Selmer groups for elliptic curves with isogenies of prime degree

James Michael Mailhot

A dissertation submitted in partial fulfillment
of the requirements for the degree of

Doctor of Philosophy

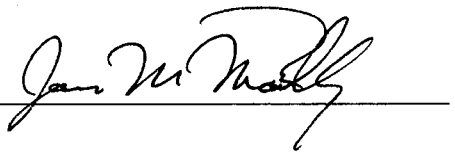
University of Washington

2003

Program Authorized to Offer Degree: Mathematics

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

In presenting this dissertation in partial fulfillment of the requirements for the Doctoral degree at the University of Washington, I agree that the Library shall make its copies freely available for inspection. I further agree that extensive copying of this dissertation is allowable only for scholarly purposes, consistent with "fair use" as prescribed in the U.S. Copyright Law. Requests for copying or reproduction of this dissertation may be referred to Bell and Howell Information and Learning, 300 North Zeeb Road, Ann Arbor, MI 48106-1346, to whom the author has granted "the right to reproduce and sell (a) copies of the manuscript in microform and/or (b) printed copies of the manuscript made from microform."

Signature 

Date June 10, 2003

University of Washington

Graduate School

This is to certify that I have examined this copy of a doctoral dissertation by

James Michael Mailhot

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Chair of Supervisory Committee:

Ralph Greenberg

Reading Committee:

Ralph Greenberg

Sándor Kovács

John Sullivan

Date: June 10, 2003

University of Washington

Abstract

Selmer groups for elliptic curves with isogenies of prime degree

by James Michael Mailhot

Chair of Supervisory Committee:

Professor Ralph Greenberg
Mathematics

The Mordell-Weil theorem states that the points of an elliptic curve defined over a number field form a finitely generated, abelian group. The rank of this group, generally referred to as the rank of the elliptic curve, is hard to study. The Selmer group, defined via Galois cohomology, gives a way of approximating the rank of an elliptic curve. The Selmer group is, itself, difficult to study in general.

We examine the Selmer group for an elliptic curve which admits an isogeny degree p, for an odd prime p. Using the kernel of the isogeny, and the kernel of its dual isogeny, we give upper and lower bounds on the p-rank of the Selmer group in terms of the arithmetic of certain number fields. We show, by way of examples, that these bounds can be computed for families of quadratic twists of an elliptic curve.

For elliptic curves defined over the rational numbers, we examine the relationship between these bounds on the p-rank of the Selmer group and the algebraic Iwasawa invariants associated to the elliptic curve for the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$.

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGMENTS

I would like to express my sincere appreciation to my advisor, Ralph Greenberg, for sharing his knowledge and insights. This dissertation could not have been completed without the patience and support of my wife, Jenny.

Chapter 1

BACKGROUND

1.1 Ranks and Selmer groups

An elliptic curve E is a one-dimensional abelian variety. Equivalently, an elliptic curve is a genus one curve with a specified base point. If E is an elliptic curve defined over the field K, then $E(K)$, the set of K-rational points on E, forms an abelian group, with the specified base point acting as the identity under the group operation. Of particular interest to number theorists is the case where K is a number field. In this case, the Mordell-Weil theorem (see [27]) states that $E(K)$ is a finitely generated, abelian group. That is, there is a non-negative integer r and a finite, abelian group T satisfying

$$E(K) \cong \mathbf{Z}^r \times T. \tag{1.1}$$

We call r the rank of E over K, and T the torsion subgroup of $E(K)$.

Very little is known, in general, about ranks of elliptic curves. For example, it is widely conjectured that for fixed K, the ranks of elliptic curves over K should be unbounded. Over $\mathbf{Q}$, the current record is an elliptic curve of rank at least 22, given by S. Fermigier in [9]. The naive approach to computing the rank of an elliptic curve - looking for linearly independent points in $E(K)$ - is generally fruitless. It seems that curves of high rank are very sparse; over $\mathbf{Q}$, most elliptic curves have rank 0 or 1.

In an effort to get a handle on the rank of E over K, we introduce the Selmer and

Tate-Shafarevich groups for E over K, denoted $\mathrm{Sel}_E(K)$ and $Ш_E(K)$ respectively. These groups, which arise via Galois cohomology, fit into the short exact sequence

$$0 \longrightarrow E(K) \otimes \mathbf{Q}/\mathbf{Z} \longrightarrow \mathrm{Sel}_E(K) \longrightarrow Ш_E(K) \longrightarrow 0. \tag{1.2}$$

Notice that $E(K) \otimes \mathbf{Q}/\mathbf{Z} \cong (\mathbf{Z}^r \times T) \otimes \mathbf{Q}/\mathbf{Z} \cong (\mathbf{Q}/\mathbf{Z})^r$, and, moreover, this group is injective, so (1.2) splits, and

$$\mathrm{Sel}_E(K) \cong (\mathbf{Q}/\mathbf{Z})^r \times Ш_E(K). \tag{1.3}$$

The Tate-Shafarevich group is conjectured to be finite, so full knowledge of the Selmer group would conjecturally provide full information on the rank of the elliptic curve over K. The goals of this paper are more modest. In chapter 2 we will give bounds on the number of elements of order p in the Selmer group, if p is an odd prime, E admits a K-rational isogeny of degree p, and E does not have potential supersingular reduction at any of the primes of K lying over p. In chapter 3 we will compute these bounds for some families of elliptic curves, including one case where these bounds give exact information. In chapter 4 we will discuss the connection to Iwasawa theory.

1.2 Notation

For any abelian group A and any prime number p, $A[p^\infty]$ will denote the p-primary subgroup of A, and $A[p]$ will denote the group of elements of order dividing p in A. The Pontryagin dual of A, denoted $A^\vee$ is defined to be $\mathrm{Hom}(A, \mathbf{Q}/\mathbf{Z})$.

For any Galois extension L/K of fields, $G_{L/K}$ will be used to denote the Galois group of L over K; G_K will be used to denote the absolute Galois group $G_{\bar{K}/K}$. We will use the shorthand of writing $H^i(L/K, -)$ and $H^i(K, -)$ for the Galois cohomology groups $H^i(G_{L/K}, -)$ and $H^i(G_K, -)$.

If K is a number field, and $\mathfrak{l}$ is any place of K, $K_\mathfrak{l}$ will denote the completion of K at $\mathfrak{l}$. If Σ is any finite set of places of K, K_Σ will denote the maximal extension of

K which is unramified outside Σ.

If K is any field and A is any G_K-module, we will use $A(K)$ for $H^0(K, A)$, the elements of A fixed by G_K. We will use $K(A)$ for the minimal extension of K whose absolute Galois group acts trivially on A. ($G_{K(A)}$ is precisely the kernel of the map $G_K \longrightarrow \mathrm{Aut}(A)$.) If K is a number field and if $K(A)/K$ is ramified at $\mathfrak{l}$, we will say A is ramified at $\mathfrak{l}$; $\mathrm{Ram}(A/K)$ will denote the set of all places of K at which A is ramified.

If K is a local field, we will use K_{nr} to denote the maximal unramified extension of K. For any G_K-module A and any non-negative integer i, we call elements of $H^i(K, A)$ unramified if they are in $H^i_{nr}(K, A) := \ker\left(H^i(K, A) \longrightarrow H^i(K_{nr}, A)\right)$. Suppose further that the residue field $K/\mathfrak{m}_K$ has characteristic p. Following J.-P. Serre in [24], if L/K is an abelian extension and $G_{L/K}$ has exponent p, we say the extension L/K is *peu ramifiée* if $L(\mu_p) = K(\mu_p, \sqrt[p]{\eta_1}, \ldots, \sqrt[p]{\eta_m})$ for some $\eta_1, \ldots, \eta_m \in \mathcal{O}^\times_{K(\mu_p)}$. Suppose $\#A = p$, and let L/K be the minimal extension such that $A \cong \mu_p$ as a G_L-module. We say an element of $H^1(K, A)$ is *peu ramifiée* if its image under the restriction map

$$H^1(K, A) \hookrightarrow H^1(L, A) \cong L^\times/(L^\times)^p \cong \mathbf{Z}/p\mathbf{Z} \times \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p \tag{1.4}$$

is in $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p$, and we let $H^1_{pr}(K, A)$ denote the group of such cocycles.

Lemma 1.1. *Let K be a local field with residue characteristic p, and let A be a G_K-module of order p. If $A \ncong \mu_p$ as G_K-modules, then $H^1_{pr}(K, A) = H^1(K, A)$. Otherwise, $H^1(K, A)/H^1_{pr}(K, A) = \mathbf{Z}/p\mathbf{Z}$.*

Proof. If $A \cong \mu_p$, then

$$\frac{H^1(K, A)}{H^1_{pr}(K, A)} \cong \frac{K^\times/(K^\times)^p}{\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p} \cong \mathbf{Z}/p\mathbf{Z}. \tag{1.5}$$

Suppose $A \ncong \mu_p$ as a G_K-module, and let α be the $\mathbf{Z}_p^\times$-valued character which gives the action of G_K on A. Let L be defined as above, so $A \cong \mu_p$ as a G_L-module. The degree of the extension L/K must divide $(p-1)$, so inflation-restriction gives an

isomorphism

$$\begin{aligned} H^1(K,A) &\cong H^1(L,A)^{G_{L/K}} \cong H^1(L,\mu_p)^{(\alpha)} \cong \left(L^\times/(L^\times)^p\right)^{(\alpha)} \\ &\cong \left(\mathbf{Z}/p\mathbf{Z} \times \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p\right)^{(\alpha)}. \end{aligned} \tag{1.6}$$

Since α is non-trivial, $(\mathbf{Z}/p\mathbf{Z})^{(\alpha)} = 0$. Thus, $H^1(K,A)$ is in the pre-image of $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p$, so $H^1(K,A) = H^1_{pr}(K,A)$. □

It will be useful for us to have an alternate description of $H^1_{pr}(K,A)$. Let K_{tame} be the maximal tamely ramified extension of K, and let K_{pr} be the extension of K_{tame} gotten by adjoining p^{th} roots of all elements of $\mathcal{O}^\times_{K_{tame}}$.

Lemma 1.2. $H^1_{pr}(K,A) = \ker\left(H^1(K,A) \longrightarrow H^1(K_{pr},A)\right)$.

Proof. Let L/K be the minimal extension such that $A \cong \mu_p$ as a G_L-module. Then by definition, $H^1_{pr}(K,A)$ is the pre-image of $H^1_{pr}(L,A)$ under $H^1(K,A) \hookrightarrow H^1(L,A)$. Since $[L:K]$ is relatively prime to p, $L_{tame} = K_{tame}$, and $L_{pr} = K_{pr}$.

Suppose $\sigma \in H^1(L,A)$ is represented by $x \in L^\times$. Then $\sigma \in H^1_{pr}(L,A)$ if and only if $p \mid v_L(x)$. If π_L is a uniformizer for L, we can multiply x by an appropriate power of π_L^p so that $0 \leq v_L(x) < p$. Then $\sigma \in H^1_{pr}(L,A)$ if and only if $v_L(x) = 0$.

If $v_L(x) = 0$, then $x \in \mathcal{O}_L^\times \subseteq \mathcal{O}^\times_{L_{tame}}$, so x is a p^{th} power in L_{pr}, and $\sigma \in \ker\left(H^1(L,A) \longrightarrow H^1(L_{pr},A)\right)$.

If $\sigma \in \ker\left(H^1(L,A) \longrightarrow H^1(L_{pr},A)\right)$, then x is a p^{th} power in $L^\times_{pr}$. By Kummer theory and the definition of L_{pr}, there is some $y \in \mathcal{O}^\times_{K_{tame}}$ such that $\frac{x}{y} \in (K^\times_{tame})^p$. Choose $z \in K^\times_{tame}$ satisfying $z^p = \frac{x}{y}$, and let $M = L(y,z)$.

$$v_M(x) = v_M(yz^p) = v_M(y) + p \cdot v_M(z) = p \cdot v_M(z) \equiv 0 \pmod{p}. \tag{1.7}$$

On the other hand, since M/L is a tamely ramified extension, $v_M(x) \equiv 0 \pmod{p}$ if and only if $v_L(x) \equiv 0 \pmod{p}$, which is equivalent to $\sigma \in H^1_{pr}(L,A)$.

Thus, $H^1_{pr}(L,A) = \ker\left(H^1(L,A) \longrightarrow H^1(L_{pr},A)\right)$. Since $H^1_{pr}(K,A)$ is the pre-image of $H^1_{pr}(L,A)$ under restriction, and $K_{pr} = L_{pr}$,

$$\begin{aligned} H^1_{pr}(K,A) &= \ker\left(H^1(K,A) \longrightarrow H^1(L,A)/H^1_{pr}(L,A)\right) \\ &= \ker\left(H^1(K,A) \longrightarrow H^1(L_{pr},A)\right) \\ &= \ker\left(H^1(K,A) \longrightarrow H^1(K_{pr},A)\right). \end{aligned} \tag{1.8}$$

□

Remark. If M/K is any tamely ramified extension, then $M_{pr} = K_{pr}$, so $H^1_{pr}(K,A)$ is the pre-image of $H^1_{pr}(M,A)$ under restriction.

1.3 Duality

Fix a prime p, and let A be a p-group. Let K be a local field, and assume G_K acts on A. Let $A' = \mathrm{Hom}(A, \mu_{p^\infty})$. Then the cup product induces a perfect pairing

$$\langle -,- \rangle_K : H^1(K,A) \times H^1(K,A') \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p. \tag{1.9}$$

(When $K = \mathbf{Q}_l$ we will denote this pairing $\langle -,- \rangle_l$.) We have the following orthogonality results when $\#A = p$.

Lemma 1.3. *Let L/K be a Galois extension of degree p, and suppose the residue characteristic of K is relatively prime to p. Let $\mathcal{H}(A) = \ker\left(H^1(K,A) \longrightarrow H^1(L,A)\right)$ and $\mathcal{H}(A') = \ker\left(H^1(K,A') \longrightarrow H^1(L,A')\right)$. Then $\mathcal{H}(A)$ and $\mathcal{H}(A')$ are orthogonal complements under the pairing* (1.9).

Proof. Suppose $A \ncong \mathbf{Z}/p\mathbf{Z}$ as a G_K-module. Since $[L:K] = p$ and $\#\,\mathrm{Aut}(A) = (p-1)$, $A(L) = 0$, and by inflation-restriction, $\mathcal{H}(A) \cong H^1(L/K, A(L)) = 0$. Thus $\mathcal{H}(A)^\perp = H^1(K,A')$. Since the residue characteristic of K is relatively prime to p,

the local Euler-Poincaré characteristic is $\chi(K, A') = 1$, and

$$\begin{aligned} \#H^1(K, A') &= \#H^0(K, A') \cdot \#H^2(K, A') \\ &= \#A'(K) \cdot \#A(K) = \#A'(K) \\ &= \#H^1(L/K, A'(L)) = \#\mathcal{H}(A'). \end{aligned} \tag{1.10}$$

Thus $\mathcal{H}(A') = H^1(K, A') = \mathcal{H}(A)^\perp$.

Suppose $A \cong \mathbf{Z}/p\mathbf{Z}$, in which case $A' \cong \mu_p$. Then $H^1(K, A) = \mathrm{Hom}(G_K, \mathbf{Z}/p\mathbf{Z})$ and $H^1(K, A') \cong K^\times/(K^\times)^p$. If $f \in \mathrm{Hom}(G_K, \mathbf{Z}/p\mathbf{Z})$, then $f \in \mathcal{H}(A)$ if and only if f factors through $G_{L/K}$. If $\alpha \in K^\times/(K^\times)^p$, then $\alpha \in \mathcal{H}(A')$ if and only if $\sqrt[p]{\alpha} \in L$, in which case $\alpha \in N_{L/K}(L^\times)$. By proposition XIV.2.4 of [23], $\langle f, \alpha \rangle_K = 0$ if and only if α is a norm in the extension cut out by f. Hence, we again have $\mathcal{H}(A') = \mathcal{H}(A)^\perp$. □

Lemma 1.4. *Suppose the residue characteristic of K is p. Then $H^1_{nr}(K, A)$ and $H^1_{pr}(K, A')$ are orthogonal complements under the pairing* (1.9).

Proof. If $A \ncong \mathbf{Z}/p\mathbf{Z}$, then $A' \ncong \mu_p$, so by lemma 1.1, $H^1_{pr}(K, A') = H^1(K, A')$; as in lemma 1.3, $H^1_{nr}(K, A) = 0$. Thus, $H^1_{pr}(K, A')$ and $H^1_{nr}(K, A)$ are orthogonal complements.

Suppose $A \cong \mathbf{Z}/p\mathbf{Z}$, in which case $A' \cong \mu_p$. Let L/K be the unramified extension of degree p. As before, $f \in H^1_{nr}(K, A)$ if and only if f factors through $G_{L/K}$; $\alpha \in H^1_{pr}(K, A')$ if and only if modulo p^{th} powers $\alpha \in \mathcal{O}_K^\times$, in which case $\alpha \in N_{L/K}(L^\times)$. As before, $\langle f, \alpha \rangle_K = 0$ if and only if α is a norm in the extension cut out by f, and again we have $H^1_{pr}(K, A') = H^1_{nr}(K, A)^\perp$. □

Now, suppose K is a number field, Σ is a finite set of places of K containing the infinite places, and A is a $G_{K_\Sigma/K}$-module. We define a pairing

$$\langle -, - \rangle : \prod_{\mathfrak{l} \in \Sigma} H^1(K_\mathfrak{l}, A) \times \prod_{\mathfrak{l} \in \Sigma} H^1(K_\mathfrak{l}, A') \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p \tag{1.11}$$

by $\langle -, - \rangle = \sum_{\mathfrak{l} \in \Sigma} \langle -, - \rangle_{K_\mathfrak{l}}$. Then we have the following.

Lemma 1.5. *Under the pairing* (1.11), $\mathrm{im}\left(H^1(K_\Sigma/K, A) \longrightarrow \prod_{\mathfrak{l}\in\Sigma} H^1(K_\mathfrak{l}, A)\right)$ *and* $\mathrm{im}\left(H^1(K_\Sigma/K, A') \longrightarrow \prod_{\mathfrak{l}\in\Sigma} H^1(K_\mathfrak{l}, A')\right)$ *are orthogonal complements.*

Proof. This follows immediately from the exactness at the middle term of the long exact sequence of Poitou-Tate (see [19]). □

1.4 Known results

Most approaches to examining Selmer and Tate-Shafarevich groups have focused on specific families of elliptic curves. In [17] K. Kramer examined elliptic curves given by the equation

$$E : y^2 + xy = x^3 - (16m)x^2 - (8m)x - m, \tag{1.12}$$

and proved that the 2-rank of the Tate-Shafarevich group for elliptic curves in this family is unbounded.

Theorem (K. Kramer). *Let n be a positive integer. One can choose integers $l = l_1 \cdot \ldots \cdot l_n r$ and $m = m_1 \cdot \ldots \cdot m_n s$ with the following properties:*

- *$l_1, \ldots, l_n, m_1, \ldots m_n$ are distinct odd primes with $l_i \equiv 1 \pmod 4$ for $1 \leq i \leq n$;*
- *r and s are positive, odd integers and each prime factor of r is $1 \pmod 4$;*
- *$l = 16m + 1$,*
- *$\left(\frac{m_i}{l_j}\right) = (-1)^{\delta_{ij}}$ for $1 \leq i, j \leq n$.*

Let E be the elliptic curve defined over $\mathbf{Q}$ by (1.12), *with m as above. Then*

$$\dim_{\mathbf{F}_2} (Ш_E(\mathbf{Q})[2]) \geq 2n. \tag{1.13}$$

In [10] T. A. Fisher examined elliptic curves with a rational point of order m for $m = 5$ or 7, parametrized by $X_1(m) \cong \mathbf{P}^1$. In [11] he considered a slightly more specialized case: elliptic curves whose m-torsion splits as $\mathbf{Z}/m\mathbf{Z} \times \mu_m$ for $m = 3, 4$ or 5, parametrized by the modular curves $X(m) \cong \mathbf{P}^1$. Each of these curves admits an isogeny $\alpha : E \longrightarrow E'$ with kernel $\mathbf{Z}/m\mathbf{Z}$. In the latter case, the curves also admit

isogenies $\beta : E \longrightarrow E''$, with kernel μ_m. To these isogenies (and the corresponding dual isogenies, $\hat{\alpha}$ and $\hat{\beta}$) we can associate Selmer groups $S^{(\alpha)}(E/K)$, $S^{(\beta)}(E/K)$, $S^{(\hat{\alpha})}(E'/K)$ and $S^{(\hat{\beta})}(E''/K)$; these groups group gives information about the number of elements of order m in the full Selmer group. He was able to estimate the sizes of these Selmer groups in terms of congruences involving the explicit parametrization of these curves. In particular, in the case of curves whose m-torsion splits, he was able to show $S^{(\hat{\beta})}(E''/K)$ can be arbitrarily large compared to $S^{(\alpha)}(E/K)$ and $S^{(\hat{\alpha})}(E'/K)$, proving the following.

Theorem (T. A. Fisher). *Let K be a number field and let $m = 3, 4$ or 5. Then the Tate-Shafarevich group of an elliptic curve over K may contain arbitrarily many elements of order m.*

The approach of G. Frey in [12] is somewhat more general. He examined quadratic twists of elliptic curves defined over $\mathbf{Q}$ with $\mathbf{Q}$-rational points of order p, for p odd. (Note that this forces $p = 3, 5$ or 7.) Let E be such an elliptic curve, of conductor N_E and j-invariant j_E. Let $\tilde{S}_E$ be the set of odd primes $l \mid N_E$ with $l \equiv -1 \pmod{p}$, and let $S_E \subseteq \tilde{S}_E$ be the subset consisting of primes satisfying $v_l(j_E) \not\equiv 0 \pmod{p}$ and $v_l(j_E) < 0$. For a fixed, square-free integer d, let $F = \mathbf{Q}(\sqrt{d})$, let ε_d be the quadratic character which gives the Galois action on $\sqrt{d}$ and let K be the subfield of $\mathbf{Q}(\zeta_p, \sqrt{d})$ of index 2 containing neither ζ_p nor $\sqrt{d}$. Let F' (respectively F'') be the maximal abelian extension of F of exponent p unramified outside the set S_E (resp. $\tilde{S}_E$). Let K' be the maximal abelian extension of K of exponent p unramified outside the set $\{p\} \cup S_E$, *peu ramifiée* above p, such that $G_{K/\mathbf{Q}}$ acts on $G_{K'/K}$ by $\chi_p \varepsilon_d$, where χ_p is the character which gives the Galois action on μ_p. He was able to prove the following theorem.

Theorem (G. Frey). *Let E be an elliptic curve defined over $\mathbf{Q}$ with a point P of order $p > 2$ rational over $\mathbf{Q}$. Assume E has either good or multiplicative reduction at p, and that P is not contained in the kernel of reduction modulo p (so E does not*

have supersingular reduction at p). Let $d \neq 1$ be a square-free integer relatively prime to $p \cdot N_E$ such that:

- *if $2 \mid N_E$ then $d \equiv 3 \pmod 4$;*
- *if $l \notin \{2, p\} \cup S_E$ but $l \mid N_E$ then $\left(\frac{d}{l}\right) = -1$ if E is a Tate curve over $\mathbf{Q}_l$ or $v_l(j_E) \geq 0$, and $\left(\frac{d}{l}\right) = +1$ otherwise;*
- *if $v_p(j_E) < 0$ then $\left(\frac{d}{p}\right) = -1$.*

If E^d is the quadratic twist by d of E, then

$$[F' : F] \leq \# \mathrm{Sel}_{E^d}(\mathbf{Q})[p] \leq [F'' : F] \cdot [K' : K]. \tag{1.14}$$

Frey's result demonstrates a couple of themes. First, the bounds on the p-rank of the Selmer group tend to be easily applicable to entire families of quadratic twists. Second, p-ranks of Selmer groups which admit K-rational isogenies of degree p are closely related to class groups of finite extensions of K. The results in chapter 2 extend Frey's theorem in two ways. Firstly, by tightening the upper bound on the number of elements of order p in the Selmer group, and secondly, by increasing the applicability. Frey's theorem applies only to elliptic curves defined over $\mathbf{Q}$, and with very specific Galois action on the kernel of the given isogeny. The results in chapter 2 will be applicable to elliptic curves defined over arbitrary number fields, with no condition placed on the Galois action on the kernel of the given isogeny.

In [21], E. Schaefer considered Selmer groups in the most general setting. If $\phi : A \longrightarrow A'$ is an isogeny of abelian varieties defined over the number field K, we can define a Selmer group $S^{(\phi)}(A/K) \subseteq H^1(K, A[\phi])$, where $A[\phi]$ denotes the kernel of the isogeny ϕ. If $H^1(K(A[\phi])/K, A[\phi])$ is trivial, we can use the inflation-restriction sequence to embed

$$S^{(\phi)}(A/K) \hookrightarrow \mathrm{Hom}_{G_{K(A[\phi])}}(G_{K(A[\phi])}, A[\phi]). \tag{1.15}$$

Let $C^{(\phi)}(A/K)$ be the subgroup of homomorphisms which factor through an everywhere unramified extension of $K(A[\phi])$, a group closely related to the class group

for K, and let $I^{(\phi)}(A/K) = S^{(\phi)}(A/K) \cap C^{(\phi)}(A/K)$. He examined the relative sizes of $S^{(\phi)}(A/K)$, $C^{(\phi)}(A/K)$ and $I^{(\phi)}(A/K)$ by considering local conditions. For every prime $\mathfrak{p}$ of K, we can define local cohomology groups $S^{(\phi)}(A/K_\mathfrak{p})$, $C^{(\phi)}(A/K_\mathfrak{p})$ and $I^{(\phi)}(A/K_\mathfrak{p}) \subseteq H^1(K_\mathfrak{p}, A[\phi])$. Schaefer shows that if $\mathfrak{p}$ is a prime of good reduction which doesn't divide the degree of ϕ, then $S^{(\phi)}(A/K_\mathfrak{p}) = C^{(\phi)}(A/K_\mathfrak{p}) = I^{(\phi)}(A/K_\mathfrak{p})$. Thus, he proved the following.

Theorem (E. Schaefer). *There are injective homomorphisms*

$$\begin{aligned} S^{(\phi)}(A/K)/I^{(\phi)}(A/K) &\hookrightarrow \prod_\mathfrak{p} S^{(\phi)}(A/K_\mathfrak{p})/I^{(\phi)}(A/K_\mathfrak{p}) \\ C^{(\phi)}(A/K)/I^{(\phi)}(A/K) &\hookrightarrow \prod_\mathfrak{p} C^{(\phi)}(A/K_\mathfrak{p})/I^{(\phi)}(A/K_\mathfrak{p}), \end{aligned}$$

where the product runs over the finite set of primes of bad reduction and primes dividing the degree of ϕ.

This theorem bounds the difference in sizes between the Selmer group associated to ϕ and a group related to the class group. When $\prod_\mathfrak{p} H^1(K_\mathfrak{p}, A[\phi])$ is small, this difference will be small. Unfortunately, if $\mathfrak{p}$ divides the degree of ϕ, $H^1(K_\mathfrak{p}, A[\phi])$ can grow quite large. In chapter 2, we will examine more closely the precise Selmer condition at primes of bad reduction, and at primes lying over p (the degree of the isogeny we will consider), in order to give a more precise description of the relationship between the Selmer group and class groups.

Chapter 2

BOUNDS ON THE SELMER GROUP

2.1 Set-up

Let E be an elliptic curve defined over the number field K, and suppose E admits a K-rational isogeny of odd, prime degree p. Suppose, in addition, that E has either multiplicative or good, ordinary reduction at all places of K lying over p. Our goal in this chapter is to use information about the isogeny to obtain bounds on the size of $\mathrm{Sel}_E(K)[p]$.

We recall, first, the definition of the p-primary Selmer group for E over K. For any place $\mathfrak{l}$ of K there is an injective map $\kappa_\mathfrak{l} : E(K_\mathfrak{l}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow H^1(K_\mathfrak{l}, E[p^\infty])$ defined as follows. If $P \in E(K_\mathfrak{l})$ and $Q \in E(\bar{K}_\mathfrak{l})$ satisfies $p^n Q = P$, then $\kappa_\mathfrak{l}(P \otimes \frac{1}{p^n}) \in H^1(K_\mathfrak{l}, E[p^\infty])$ is represented by the cocycle which maps σ to $(\sigma(Q) - Q)$. We say an element of $H^1(K, E[p^\infty])$ satisfies the Selmer condition at $\mathfrak{l}$ if, when restricted to $H^1(K_\mathfrak{l}, E[p^\infty])$, it is in $\mathrm{im}(\kappa_\mathfrak{l})$. Such an element is in the p-primary Selmer group if it satisfies the Selmer condition at all places. That is,

$$\mathrm{Sel}_E(K)[p^\infty] := \ker\left(H^1(K, E[p^\infty]) \longrightarrow \prod_\mathfrak{l} H^1(K_\mathfrak{l}, E[p^\infty])/\,\mathrm{im}(\kappa_\mathfrak{l})\right), \qquad (2.1)$$

where the product is taken over all places K. For $\mathfrak{l}$ not lying over p, $\mathrm{im}(\kappa_\mathfrak{l}) = 0$. For $\mathfrak{p}$ lying over p, we have excluded the possibility of potentially supersingular reduction, so we can use the description of $\mathrm{im}(\kappa_\mathfrak{p})$ given by J. Coates and R. Greenberg in [4].

On the surface, deciding whether a given element of $H^1(K, E[p^\infty])$ is in the Selmer group involves checking an infinite number of conditions. Fortunately, by exercise 2.9 of [14], we can replace this definition with an equivalent one involving only finitely

many places of K. Let Σ be any finite set of places of K which contains the infinite places, the places of bad reduction for E and the places lying over p. Then

$$\mathrm{Sel}_E(K)[p^\infty] \cong \ker\left(H^1(K_\Sigma/K, E[p^\infty]) \longrightarrow \prod_{\mathfrak{l}\in\Sigma} H^1(K_\mathfrak{l}, E[p^\infty])/\operatorname{im}(\kappa_\mathfrak{l})\right). \tag{2.2}$$

For convenience we will take Σ to be as small as possible. That is, the places in Σ are precisely the infinite places, the places of bad reduction for E and the places lying over p.

Let Ψ be the kernel of the K-rational, degree p isogeny alluded to at the start of the section. Then Ψ is a G_K-invariant, one-dimensional subspace of $E[p]$, and there is a short exact sequence

$$0 \longrightarrow \Psi \longrightarrow E[p] \longrightarrow \Phi \longrightarrow 0 \tag{2.3}$$

of G_K-modules, where $\Phi := E[p]/\Psi$. Applying Galois cohomology gives us the long exact sequence

$$\begin{aligned} 0 \longrightarrow\ & \Psi(K) \longrightarrow E(K)[p] \longrightarrow \Phi(K) \\ \longrightarrow\ & H^1(K_\Sigma/K, \Psi) \longrightarrow H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_\Sigma/K, \Phi) \\ \longrightarrow\ & H^2(K_\Sigma/K, \Psi) \longrightarrow \cdots\cdots . \end{aligned} \tag{2.4}$$

Likewise, by applying Galois cohomology to the short exact sequence

$$0 \longrightarrow E[p] \longrightarrow E[p^\infty] \xrightarrow{p} E[p^\infty] \longrightarrow 0, \tag{2.5}$$

we obtain the long exact sequence

$$\begin{aligned} 0 \longrightarrow\ & E(K)[p] \longrightarrow E(K)[p^\infty] \xrightarrow{p} E(K)[p^\infty] \\ \longrightarrow\ & H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_\Sigma/K, E[p^\infty]) \xrightarrow{p} H^1(K_\Sigma/K, E[p^\infty]) \\ \longrightarrow\ & \cdots\cdots . \end{aligned} \tag{2.6}$$

In light of (2.2) we can view $\mathrm{Sel}_E(K)[p]$ as a subgroup of $H^1(K_\Sigma/K, E[p^\infty])[p]$. We define $S_{E[p]}$ to be the preimage of $\mathrm{Sel}_E(K)[p]$ in $H^1(K_\Sigma/K, E[p])$ given by (2.6), and we define S_Ψ (respectively S_Φ) to be the preimage (resp. image) of $S_{E[p]}$ in $H^1(K_\Sigma/K, \Psi)$ (resp. $H^1(K_\Sigma/K, \Phi)$) given by (2.4).

Lemma 2.1.

$$\#\,\mathrm{Sel}_E(K)[p] = \frac{\#S_\Psi \cdot \#S_\Phi}{\#\Psi(K) \cdot \#\Phi(K)}. \tag{2.7}$$

Proof. From (2.4) and (2.6) we have the exact sequences

$$\begin{aligned} 0 \longrightarrow \Psi(K) \longrightarrow E(K)[p] \longrightarrow \Phi(K) \\ \longrightarrow S_\Psi \longrightarrow S_{E[p]} \longrightarrow S_\Phi \longrightarrow 0 \end{aligned} \tag{2.8}$$

and

$$\begin{aligned} 0 \longrightarrow E(K)[p] \longrightarrow E(K)[p^\infty] \longrightarrow E(K)[p^\infty] \\ \longrightarrow S_{E[p]} \longrightarrow \mathrm{Sel}_E(K)[p] \longrightarrow 0. \end{aligned} \tag{2.9}$$

Note that the Mordell-Weil theorem implies $E(K)[p^\infty]$ is finite. By (2.9)

$$\#\,\mathrm{Sel}_E(K)[p] = \frac{\#S_{E[p]} \cdot \#E(K)[p^\infty]}{\#E(K)[p^\infty] \cdot \#E(K)[p]} = \frac{\#S_{E[p]}}{\#E(K)[p]}. \tag{2.10}$$

By (2.8)

$$\#S_{E[p]} = \frac{\#S_\Psi \cdot \#S_\Phi \cdot \#E(K)[p]}{\#\Psi(K) \cdot \#\Phi(K)}. \tag{2.11}$$

Hence

$$\#\,\mathrm{Sel}_E(K)[p] = \frac{\#S_\Psi \cdot \#S_\Phi}{\#\Psi(K) \cdot \#\Phi(K)}. \tag{2.12}$$

□

2.2 Strategy

In practice, computation of $\#\Psi(K)$ and $\#\Phi(K)$ is trivial, so the problem of counting $\#\,\mathrm{Sel}_E(K)[p]$ reduces to an analysis of S_Ψ and S_Φ. Consider, for each $\mathfrak{l} \in \Sigma$, the commutative diagram

$$\begin{array}{ccccc} H^1(K_\Sigma/K, \Psi) & \longrightarrow & H^1(K_\Sigma/K, E[p]) & \longrightarrow & H^1(K_\Sigma/K, \Phi) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(K_\mathfrak{l}, \Psi) & \longrightarrow & H^1(K_\mathfrak{l}, E[p]) & \longrightarrow & H^1(K_\mathfrak{l}, \Phi) \\ & & \downarrow & & \\ & & H^1(K_\mathfrak{l}, E[p^\infty])/\,\mathrm{im}(\kappa_\mathfrak{l}). & & \end{array} \tag{2.13}$$

If we set $\mathcal{L}_\mathfrak{l}(\Psi) := \ker\left(H^1(K_\mathfrak{l}, \Psi) \longrightarrow H^1(K_\mathfrak{l}, E[p^\infty])/\operatorname{im}(\kappa_\mathfrak{l})\right)$, then

$$S_\Psi = \ker\left(H^1(K_\Sigma/K, \Psi) \longrightarrow \prod_{\mathfrak{l}\in\Sigma} H^1(K_\mathfrak{l}, \Psi)/\mathcal{L}_\mathfrak{l}(\Psi)\right). \tag{2.14}$$

Likewise, if we set $\mathcal{L}_\mathfrak{l}(\Phi) = \operatorname{im}\left(S_{E[p]} \longrightarrow H^1(K_\mathfrak{l}, \Phi)\right)$, then

$$S_\Phi \subseteq \ker\left(H^1(K_\Sigma/K, \Phi) \longrightarrow \prod_{\mathfrak{l}\in\Sigma} H^1(K_\mathfrak{l}, \Phi)/\mathcal{L}_\mathfrak{l}\right). \tag{2.15}$$

(Possible lack of surjectivity in the middle line of (2.4) makes it impossible to determine subgroups $\mathcal{L}_\mathfrak{l}(\Phi)$ which would give S_Φ precisely.)

As the following lemma shows, we can ignore infinite places in Σ.

Lemma 2.2. *Let $\mathfrak{l}$ be an infinite place in Σ. Then $H^1(K_\mathfrak{l}, \Psi) = H^1(K_\mathfrak{l}, \Phi) = 0$.*

Proof. If $\mathfrak{l}$ is a real place, then $K_\mathfrak{l} = \mathbf{R}$; otherwise $K_\mathfrak{l} = \mathbf{C}$. In either case, $G_{K_\mathfrak{l}}$ has order dividing 2, so for $i \geq 1$ the groups $H^i(K_\mathfrak{l}, -)$ have exponent 2. On the other hand, Ψ and Φ have order p, so for $i \geq 0$ the groups $H^i(-, \Psi)$ and $H^i(-, \Phi)$ have exponent p. In particular, since p is odd, $H^1(K_\mathfrak{l}, \Psi)$ and $H^1(K_\mathfrak{l}, \Phi)$ are trivial. □

For finite places in Σ we define $\mathcal{L}_\mathfrak{l}^\pm(\Psi)$ and $\mathcal{L}_\mathfrak{l}^+(\Phi)$ as follows.

Definition. If E has multiplicative reduction at $\mathfrak{l}$, set

- $\mathcal{L}_\mathfrak{l}^\pm(\Psi) = H^1(K_\mathfrak{l}, \Psi)$ and $\mathcal{L}_\mathfrak{l}^+(\Phi) = 0$ if Ψ corresponds to μ_p under the Tate parametrization (see section 2.3);
- $\mathcal{L}_\mathfrak{l}^\pm(\Psi) = 0$ and $\mathcal{L}_\mathfrak{l}^+(\Phi) = H^1(K_\mathfrak{l}, \Phi)$ if Ψ does not correspond to μ_p under the Tate parametrization.

If E has additive reduction at $\mathfrak{l}$, set

- $\mathcal{L}_\mathfrak{l}^-(\Psi) = 0$, $\mathcal{L}_\mathfrak{l}^+(\Psi) = H^1(K_\mathfrak{l}, \Psi)$ and $\mathcal{L}_\mathfrak{l}^+(\Phi) = H^1(K_\mathfrak{l}, \Phi)$.

If E has good, ordinary reduction at $\mathfrak{p} \in \Sigma$, in which case $\mathfrak{p} \mid p$, set

- $\mathcal{L}_\mathfrak{p}^\pm(\Psi) = H^1_{pr}(K_\mathfrak{p}, \Psi)$ and $\mathcal{L}_\mathfrak{p}^+(\Phi) = H^1_{nr}(K_\mathfrak{p}, \Phi)$ if Ψ is in the kernel of reduction modulo $\mathfrak{p}$;
- $\mathcal{L}_\mathfrak{p}^\pm(\Psi) = H^1_{nr}(K_\mathfrak{p}, \Psi)$ and $\mathcal{L}_\mathfrak{p}^+(\Phi) = H^1_{pr}(K_\mathfrak{p}, \Phi)$ if Ψ is not in the kernel of reduction modulo $\mathfrak{p}$.

Remark. Unless $\mathfrak{l} \in \Sigma$ is a place at which E has additive reduction, $\mathcal{L}_\mathfrak{l}^-(\Psi) = \mathcal{L}_\mathfrak{l}^+(\Psi)$. As we will see in section 2.7, we often have equality even for such $\mathfrak{l}$. In particular, $\mathcal{L}_\mathfrak{l}^-(\Phi) = \mathcal{L}_\mathfrak{l}^+(\Phi)$ for all $\mathfrak{l} \in \Sigma$ if $p \geq 5$.

Our goal in the next few sections is to prove the following theorem.

Theorem 2.3. *With the above definitions* $\mathcal{L}_\mathfrak{l}^-(\Psi) \subseteq \mathcal{L}_\mathfrak{l}(\Psi) \subseteq \mathcal{L}_\mathfrak{l}^+(\Psi)$ *and* $\mathcal{L}_\mathfrak{l}(\Phi) \subseteq \mathcal{L}_\mathfrak{l}^+(\Phi)$ *for all* $\mathfrak{l} \in \Sigma$. *If we set*

$$S_\Psi^\pm := \ker\left(H^1(K_\Sigma/K, \Psi) \longrightarrow \prod_{\mathfrak{l}\in\Sigma} H^1(K_\mathfrak{l}, \Psi)/\mathcal{L}_\mathfrak{l}^\pm(\Psi)\right), \tag{2.16}$$

and

$$S_\Phi^+ := \ker\left(H^1(K_\Sigma/K, \Phi) \longrightarrow \prod_{\mathfrak{l}\in\Sigma} H^1(K_\mathfrak{l}, \Phi)/\mathcal{L}_\mathfrak{l}^+(\Phi)\right), \tag{2.17}$$

then $S_\Psi^- \subseteq S_\Psi \subseteq S_\Psi^+$ *and* $S_\Phi \subseteq S_\Phi^+$. *Hence,*

$$\frac{\#S_\Psi^-}{\#\Psi(K)\cdot\#\Phi(K)} \leq \#\,\mathrm{Sel}_E(K)[p] \leq \frac{\#S_\Psi^+\cdot\#S_\Phi^+}{\#\Psi(K)\cdot\#\Phi(K)}. \tag{2.18}$$

2.3 The Selmer condition away from p

Let $\mathfrak{l} \in \Sigma$ be a finite place not lying over p. Then, by our choice of Σ, E has bad reduction at $\mathfrak{l}$. If E has additive reduction at $\mathfrak{l}$, then $\mathcal{L}_\mathfrak{l}^-(\Psi) = 0$, $\mathcal{L}_\mathfrak{l}^+(\Psi) = H^1(K_\mathfrak{l}, \Psi)$ and $\mathcal{L}_\mathfrak{l}^+(\Phi) = H^1(K_\mathfrak{l}, \Phi)$, so clearly $\mathcal{L}_\mathfrak{l}^-(\Psi) \subseteq \mathcal{L}_\mathfrak{l}(\Psi) \subseteq \mathcal{L}_\mathfrak{l}^+(\Psi)$ and $\mathcal{L}_\mathfrak{l}(\Phi) \subseteq \mathcal{L}_\mathfrak{l}^+(\Phi)$.

Suppose E has multiplicative reduction at $\mathfrak{l}$. Then E is isomorphic to a Tate curve over either $K_\mathfrak{l}$ or the unramified, quadratic extension of $K_\mathfrak{l}$. (See [28].) That is, for some $q_E \in K_\mathfrak{l}$ with $v_\mathfrak{l}(q_E) \geq 1$ there is a G_L-module isomorphism $\bar{K}_\mathfrak{l}^\times/\langle q_E\rangle \cong E(\bar{K}_\mathfrak{l})$, where $L = K_\mathfrak{l}$ if E has split, multiplicative reduction at $\mathfrak{l}$, and L is the unramified, quadratic extension of $K_\mathfrak{l}$ if E has non-split, multiplicative reduction at $\mathfrak{l}$. (We call q_E the Tate period.) If ε is the (trivial or quadratic) character corresponding to the

extension $L/K_\mathfrak{l}$, there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_p \otimes \varepsilon & \longrightarrow & E[p] & \longrightarrow & \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mu_{p^\infty} \otimes \varepsilon & \longrightarrow & E[p^\infty] & \longrightarrow & \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon & \longrightarrow & 0 \end{array} \tag{2.19}$$

of $G_{K_\mathfrak{l}}$-modules, in which the rows are exact. Applying Galois cohomology we again have a commutative diagram with exact rows,

$$\begin{array}{ccccc} H^1(K_\mathfrak{l}, \mu_p \otimes \varepsilon) & \longrightarrow & H^1(K_\mathfrak{l}, E[p]) & \longrightarrow & H^1(K_\mathfrak{l}, \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon) \\ {\scriptstyle \alpha_\mathfrak{l}}\downarrow & & \downarrow & & {\scriptstyle \beta_\mathfrak{l}}\downarrow \\ H^1(K_\mathfrak{l}, \mu_{p^\infty} \otimes \varepsilon) & \xrightarrow{\lambda_\mathfrak{l}} & H^1(K_\mathfrak{l}, E[p^\infty]) & \longrightarrow & H^1(K_\mathfrak{l}, \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon). \end{array} \tag{2.20}$$

Lemma 2.4. $\lambda_\mathfrak{l} \circ \alpha_\mathfrak{l} : H^1(K_\mathfrak{l}, \mu_p \otimes \varepsilon) \longrightarrow H^1(K_\mathfrak{l}, E[p^\infty])$ *is the zero map.*

Proof. It is obviously enough to show that $\lambda_\mathfrak{l}$ is the zero map.

Suppose that ε is the trivial character. Then

$$H^1(K_\mathfrak{l}, \mu_{p^\infty} \otimes \varepsilon) = H^1(K_\mathfrak{l}, \mu_{p^\infty}) \cong K_\mathfrak{l}^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p \cong \mathbf{Q}_p/\mathbf{Z}_p. \tag{2.21}$$

Meanwhile, the second row of (2.20) comes from the long, exact sequence

$$\begin{array}{l} 0 \longrightarrow \quad \mu_{p^\infty}(K_\mathfrak{l}) \quad \longrightarrow \quad E(K_\mathfrak{l})[p^\infty] \quad \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p \\ \quad \longrightarrow H^1(K_\mathfrak{l}, \mu_{p^\infty}) \xrightarrow{\lambda_\mathfrak{l}} H^1(K_\mathfrak{l}, E[p^\infty]) \longrightarrow \ldots\ldots, \end{array} \tag{2.22}$$

so

$$\ker(\lambda_\mathfrak{l}) \cong (\mathbf{Q}_p/\mathbf{Z}_p)/\operatorname{im}(E(K_\mathfrak{l})[p^\infty]) \cong \mathbf{Q}_p/\mathbf{Z}_p. \tag{2.23}$$

(The last isomorphism in (2.23) holds because $E(K_\mathfrak{l})_{tors}$ is finite.) Hence $\ker(\lambda_\mathfrak{l})$ is an infinite subgroup of $H^1(K_\mathfrak{l}, \mu_{p^\infty}) \cong \mathbf{Q}_p/\mathbf{Z}_p$, but $\mathbf{Q}_p/\mathbf{Z}_p$ has no infinite, proper subgroups, so $\lambda_\mathfrak{l}$ is the zero map.

Suppose, on the other hand, that ε is the nontrivial, unramified, quadratic character of $G_{K_\mathfrak{l}}$. Applying Galois cohomology to

$$0 \longrightarrow \mu_p \otimes \varepsilon \longrightarrow \mu_{p^\infty} \otimes \varepsilon \xrightarrow{p} \mu_{p^\infty} \otimes \varepsilon \longrightarrow 0 \tag{2.24}$$

gives the long exact sequence

$$\begin{aligned} 0 \longrightarrow\ & H^0(K_\mathfrak{l}, \mu_p \otimes \varepsilon) \longrightarrow H^0(K_\mathfrak{l}, \mu_{p^\infty} \otimes \varepsilon) \xrightarrow{p} H^0(K_\mathfrak{l}, \mu_{p^\infty} \otimes \varepsilon) \\ \longrightarrow\ & H^1(K_\mathfrak{l}, \mu_p \otimes \varepsilon) \longrightarrow H^1(K_\mathfrak{l}, \mu_{p^\infty} \otimes \varepsilon)[p] \longrightarrow 0. \end{aligned} \tag{2.25}$$

Since $\mathfrak{l}$ doesn't lie over p, the Euler-Poincaré characteristic $\chi(K_\mathfrak{l}, \mu_p) = 1$, and

$$\#H^1(K_\mathfrak{l}, \mu_p \otimes \varepsilon) = \#H^0(K_\mathfrak{l}, \mu_p \otimes \varepsilon) \cdot \#H^2(K_\mathfrak{l}, \mu_p \otimes \varepsilon). \tag{2.26}$$

By local duality,

$$H^2(K_\mathfrak{l}, \mu_p \otimes \varepsilon) = H^0(K_\mathfrak{l}, \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon)^\vee, \tag{2.27}$$

which is trivial, so

$$\#H^1(K_\mathfrak{l}, \mu_p \otimes \varepsilon) = \#H^0(K_\mathfrak{l}, \mu_p \otimes \varepsilon). \tag{2.28}$$

Since $H^0(K_\mathfrak{l}, \mu_{p^\infty} \otimes \varepsilon)$ is finite,

$$\#H^1(K_\mathfrak{l}, \mu_{p^\infty} \otimes \varepsilon)[p] = \frac{\#H^1(K_\mathfrak{l}, \mu_p \otimes \varepsilon)}{\#H^0(K_\mathfrak{l}, \mu_p \otimes \varepsilon)} = 1. \tag{2.29}$$

Thus $H^1(K_\mathfrak{l}, \mu_{p^\infty} \otimes \varepsilon)$ has no elements of order p and must be trivial. It follows immediately that $\lambda_\mathfrak{l}$ must be the zero map. □

Lemma 2.5. $\beta_\mathfrak{l} : H^1(K_\mathfrak{l}, \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon) \longrightarrow H^1(K_\mathfrak{l}, \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon)$ *is injective.*

Proof. By applying Galois cohomology to the short exact sequence

$$0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon \xrightarrow{p} \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon \longrightarrow 0 \tag{2.30}$$

we obtain the long exact sequence

$$\begin{aligned} 0 \longrightarrow\ & H^0(K_\mathfrak{l}, \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon) \longrightarrow H^0(K_\mathfrak{l}, \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon) \xrightarrow{p} H^0(K_\mathfrak{l}, \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon) \\ \longrightarrow\ & H^1(K_\mathfrak{l}, \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon) \xrightarrow{\beta_\mathfrak{l}} H^1(K_\mathfrak{l}, \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon) \longrightarrow \cdots\cdots. \end{aligned} \tag{2.31}$$

If ε is a non-trivial, quadratic character, then the cohomology groups in the first row of (2.31) all vanish, and $\beta_\mathfrak{l}$ is injective. If ε is trivial, the first row of (2.31) becomes

$$0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p. \tag{2.32}$$

The right-most map in (2.32) is surjective, so $\beta_\mathfrak{l}$ is injective. □

Proposition 2.6. *Suppose E has multiplicative reduction at $\mathfrak{l}$, for a prime $\mathfrak{l}$ not lying over p. Then $\mathcal{L}_\mathfrak{l}(\Psi) = \mathcal{L}_\mathfrak{l}^{\pm}(\Psi)$ and $\mathcal{L}_\mathfrak{l}(\Phi) \subseteq \mathcal{L}_\mathfrak{l}^{+}(\Phi)$.*

Proof. Suppose first that Ψ corresponds to μ_p under the Tate parametrization. Then $\mathcal{L}_\mathfrak{l}^{\pm}(\Psi) = H^1(K_\mathfrak{l}, \Psi)$. Since Ψ corresponds to μ_p, $H^1(K_\mathfrak{l}, \Psi)$ is naturally identified with $H^1(K_\mathfrak{l}, \mu_p \otimes \varepsilon)$, and the map $H^1(K_\mathfrak{l}, \Psi) \longrightarrow H^1(K_\mathfrak{l}, E[p^\infty])$ is the zero map, by lemma 2.4. Thus, $\mathcal{L}_\mathfrak{l}(\Psi) = H^1(K_\mathfrak{l}, \Psi) = \mathcal{L}_\mathfrak{l}^{\pm}(\Psi)$.

Also, $\mathcal{L}_\mathfrak{l}(\Phi) = \operatorname{im}\left(S_{E[p]} \longrightarrow H^1(K_\mathfrak{l}, \Phi)\right)$. Since Ψ corresponds to μ_p, $H^1(K_\mathfrak{l}, \Phi)$ is naturally identified with $H^1(K_\mathfrak{l}, \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon)$. Elements of $S_{E[p]}$ satisfy the Selmer conditions at all places in Σ so in particular they satisfy the Selmer condition at $\mathfrak{l}$.

$$\begin{aligned} S_{E[p]} &\subseteq \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_\mathfrak{l}, E[p^\infty])\right) \\ &\subseteq \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_\mathfrak{l}, \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon)\right) \\ &= \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_\mathfrak{l}, \Phi)\right), \end{aligned} \tag{2.33}$$

where the last equality follows from lemma 2.5. Thus, $\mathcal{L}_\mathfrak{l}(\Phi) = 0 = \mathcal{L}_\mathfrak{l}^{+}(\Phi)$.

Now suppose Ψ does not correspond to μ_p under the Tate parametrization. Then $\mathcal{L}_\mathfrak{l}^{+}(\Phi) = H^1(K_\mathfrak{l}, \Phi)$, so $\mathcal{L}_\mathfrak{l}(\Phi) \subseteq \mathcal{L}_\mathfrak{l}^{+}(\Phi)$ automatically.

Also, $\mathcal{L}_\mathfrak{l}^{\pm}(\Psi) = 0$. Since Ψ does not correspond to μ_p, $H^1(K_\mathfrak{l}, \Psi)$ is naturally identified with $H^1(K_\mathfrak{l}, \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon)$, and we have the following commutative diagram.

$$\begin{array}{ccccc} H^1(K_\mathfrak{l}, \Psi) & \xrightarrow{\sim} & H^1(K_\mathfrak{l}, \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon) & \xrightarrow{\beta_\mathfrak{l}} & H^1(K_\mathfrak{l}, \mathbf{Q}_p/\mathbf{Z}_p \otimes \varepsilon) \\ \downarrow & & \uparrow & & \uparrow \\ H^1(K_\mathfrak{l}, E[p]) & \xrightarrow{\sim} & H^1(K_\mathfrak{l}, E[p]) & \longrightarrow & H^1(K_\mathfrak{l}, E[p^\infty]) \end{array} \tag{2.34}$$

$$\begin{aligned}\mathcal{L}_{\mathfrak{l}}(\Psi) &= \ker\left(H^1(K_{\mathfrak{l}},\Psi)\longrightarrow H^1(K_{\mathfrak{l}},E[p^\infty])\right)\\ &\subseteq \ker\left(H^1(K_{\mathfrak{l}},\Psi)\longrightarrow H^1(K_{\mathfrak{l}},\mathbf{Q}_p/\mathbf{Z}_p\otimes\varepsilon)\right)\\ &= 0,\end{aligned}\tag{2.35}$$

by lemma 2.5. Thus, $\mathcal{L}_{\mathfrak{l}}(\Psi)=0=\mathcal{L}_{\mathfrak{l}}^{\pm}(\Psi)$. □

2.4 The Selmer condition at p

Suppose $\mathfrak{p}$ is a place of K lying over p at which E has either multiplicative or good, ordinary reduction. Then $E[p^\infty]$ has a $G_{K_\mathfrak{p}}$-invariant subgroup isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ as a group, which we will denote $\hat{E}[p^\infty]$. If E has multiplicative reduction at $\mathfrak{p}$, then $\hat{E}[p^\infty]$ is the image of μ_{p^∞} under the Tate parametrization $\bar{K}_\mathfrak{p}^\times/\langle q_E\rangle \xrightarrow{\sim} E(\bar{K}_\mathfrak{p})$. If E has good, ordinary reduction at $\mathfrak{p}$, then $\hat{E}[p^\infty]$ is the p-primary subgroup of the kernel of reduction modulo p. In either case we will use $\tilde{E}[p^\infty]$ to denote $E[p^\infty]/\hat{E}[p^\infty]$.

The inclusion $\hat{E}[p^\infty]\hookrightarrow E[p^\infty]$ gives a map

$$\lambda_\mathfrak{p}: H^1(K_\mathfrak{p},\hat{E}[p^\infty])\longrightarrow H^1(K_\mathfrak{p},E[p^\infty]).\tag{2.36}$$

By proposition 4.5 of [4], $\mathrm{im}(\kappa_\mathfrak{p})=\mathrm{im}(\lambda_\mathfrak{p})_{div}$.

2.4.1 Multiplicative reduction

Throughout this subsection, suppose E has multiplicative reduction at $\mathfrak{p}$. Then $\hat{E}[p^\infty]\cong\mu_{p^\infty}\otimes\varepsilon$, where ε is either the trivial character or the unramified, quadratic character of $G_{K_\mathfrak{l}}$. By the Weil pairing (see [27]), $\tilde{E}[p^\infty]\cong\mathbf{Q}_p/\mathbf{Z}_p\otimes\varepsilon$. We have the following commutative diagram, analogous to (2.20).

$$\begin{array}{ccccc} H^1(K_\mathfrak{p},\hat{E}[p]) & \longrightarrow & H^1(K_\mathfrak{p},E[p]) & \longrightarrow & H^1(K_\mathfrak{p},\tilde{E}[p])\\ {\scriptstyle\alpha_\mathfrak{p}}\downarrow & & \downarrow & & {\scriptstyle\beta_\mathfrak{p}}\downarrow\\ H^1(K_\mathfrak{p},\hat{E}[p^\infty]) & \xrightarrow{\lambda_\mathfrak{p}} & H^1(K_\mathfrak{p},E[p^\infty]) & \longrightarrow & H^1(K_\mathfrak{p},\tilde{E}[p^\infty]) \end{array}\tag{2.37}$$

By the same argument as in the proof of lemma 2.5, $\beta_\mathfrak{p}$ is injective.

Lemma 2.7. $\mathrm{im}(\lambda_{\mathfrak{p}})_{div} = \mathrm{im}(\lambda_{\mathfrak{p}})$.

Proof. For any positive integer n, the Euler-Poincaré characteristic $\chi(K_{\mathfrak{p}}, \hat{E}[p^n]) = p^{-n\cdot[K_{\mathfrak{p}}:\mathbf{Q}_p]}$. Thus,

$$\#H^1(K_{\mathfrak{p}}, \hat{E}[p^n]) = \#H^0(K_{\mathfrak{p}}, \hat{E}[p^\infty]) \cdot \#H^2(K_{\mathfrak{p}}, \hat{E}[p^\infty]) \cdot p^{n\cdot[K_{\mathfrak{p}}:\mathbf{Q}_p]}. \tag{2.38}$$

Applying Galois cohomology to the short exact sequence

$$0 \longrightarrow \hat{E}[p^n] \longrightarrow \hat{E}[p^\infty] \xrightarrow{p^n} \hat{E}[p^\infty] \longrightarrow 0 \tag{2.39}$$

gives the long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(K_{\mathfrak{p}}, \hat{E}[p^n]) &\longrightarrow H^0(K_{\mathfrak{p}}, \hat{E}[p^\infty]) \xrightarrow{p^n} H^0(K_{\mathfrak{p}}, \hat{E}[p^\infty]) \\ \longrightarrow H^1(K_{\mathfrak{p}}, \hat{E}[p^n]) &\longrightarrow H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])[p^n] \longrightarrow 0. \end{aligned} \tag{2.40}$$

Since $\hat{E}[p^\infty] \cong \mu_p \otimes \varepsilon$, $H^0(K_{\mathfrak{p}}, \hat{E}[p^\infty])$ is finite. Thus,

$$\#H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])[p^n] = \frac{\#H^1(K_{\mathfrak{p}}, \hat{E}[p^n])}{\#H^0(K_{\mathfrak{p}}, \hat{E}[p^n])} = \#H^2(K_{\mathfrak{p}}, \hat{E}[p^n]) \cdot (p^n)^{[K_{\mathfrak{p}}:\mathbf{Q}_p]}. \tag{2.41}$$

By local duality,

$$\#H^2(K_{\mathfrak{p}}, \hat{E}[p^n]) = \#H^0(K_{\mathfrak{p}}, \tilde{E}[p^n]) = \begin{cases} p^n & \text{if } \varepsilon \text{ is trivial,} \\ 1 & \text{if } \varepsilon \text{ is non-trivial.} \end{cases} \tag{2.42}$$

Thus,

$$\#H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])[p^n] = \begin{cases} (p^n)^{[K_{\mathfrak{p}}:\mathbf{Q}_p]+1} & \text{if } \varepsilon \text{ is trivial,} \\ (p^n)^{[K_{\mathfrak{p}}:\mathbf{Q}_p]} & \text{if } \varepsilon \text{ is not trivial.} \end{cases} \tag{2.43}$$

Since this is true for all n, $H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty]) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{[K_{\mathfrak{p}}:\mathbf{Q}_p]}$ or $(\mathbf{Q}_p/\mathbf{Z}_p)^{[K_{\mathfrak{p}}:\mathbf{Q}_p]+1}$. In either case, $H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])$ is divisible.

Since the image of a divisible group must be divisible, $\mathrm{im}(\lambda_{\mathfrak{p}})_{div} = \mathrm{im}(\lambda_{\mathfrak{p}})$. □

Proposition 2.8. *Suppose E has multiplicative reduction at $\mathfrak{p}$ for a prime $\mathfrak{p}$ lying over p. Then $\mathcal{L}_{\mathfrak{p}}(\Psi) = \mathcal{L}_{\mathfrak{p}}^{\pm}(\Psi)$ and $\mathcal{L}_{\mathfrak{p}}(\Phi) \subseteq \mathcal{L}_{\mathfrak{p}}^{+}(\Phi)$.*

Proof. Suppose first that Ψ corresponds to μ_p under the Tate parametrization. Then $\mathcal{L}_{\mathfrak{p}}^{\pm}(\Psi) = H^1(K_{\mathfrak{p}}, \Psi)$. Since Ψ corresponds to μ_p, $H^1(K_{\mathfrak{p}}, \Psi)$ is naturally identified with $H^1(K_{\mathfrak{p}}, \mu_p \otimes \varepsilon) = H^1(K_{\mathfrak{p}}, \hat{E}[p])$, and $\lambda_{\mathfrak{p}} \circ \alpha_{\mathfrak{p}}$ is the map $H^1(K_{\mathfrak{p}}, \Psi) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])$. Hence

$$\begin{aligned} \mathcal{L}_{\mathfrak{p}}(\Psi) &= \ker\left(H^1(K_{\mathfrak{p}}, \Psi) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\operatorname{im}(\lambda_{\mathfrak{p}})\right) \\ &= H^1(K_{\mathfrak{p}}, \Psi) \\ &= \mathcal{L}_{\mathfrak{p}}^{\pm}(\Psi). \end{aligned} \tag{2.44}$$

Also, $\mathcal{L}_{\mathfrak{p}}(\Phi) = \operatorname{im}\left(S_{E[p]} \longrightarrow H^1(K_{\mathfrak{p}}, \Phi)\right)$. Since Ψ corresponds to μ_p, $H^1(K_{\mathfrak{p}}, \Phi)$ is naturally identified with $H^1(K_{\mathfrak{l}}, \tilde{E}[p])$. Elements of $S_{E[p]}$ satisfy the Selmer conditions at all places in Σ so in particular they satisfy the Selmer condition at $\mathfrak{p}$.

$$\begin{aligned} S_{E[p]} &\subseteq \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])\right) \\ &\subseteq \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_{\mathfrak{p}}, \tilde{E}[p^\infty])\right) \\ &= \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_{\mathfrak{p}}, \Phi)\right), \end{aligned} \tag{2.45}$$

where the last equality follows from the injectivity of $\beta_{\mathfrak{p}}$. Thus, $\mathcal{L}_{\mathfrak{p}}(\Phi) = \mathcal{L}_{\mathfrak{p}}^{+}(\Phi)$.

Now suppose Ψ does not correspond to μ_p under the Tate parametrization. Then $\mathcal{L}_{\mathfrak{p}}^{+}(\Phi) = H^1(K_{\mathfrak{p}}, \Phi)$, so $\mathcal{L}_{\mathfrak{p}}(\Phi) \subseteq \mathcal{L}_{\mathfrak{p}}^{+}(\Phi)$ automatically.

Also, $\mathcal{L}_{\mathfrak{p}}^{\pm}(\Psi) = 0$. Since Ψ does not correspond to μ_p, $H^1(K_{\mathfrak{p}}, \Psi)$ is naturally identified with $H^1(K_{\mathfrak{p}}, \tilde{E}[p])$, and we have the following commutative diagram.

$$\begin{array}{ccccc} H^1(K_{\mathfrak{p}}, \Psi) & \xrightarrow{\sim} & H^1(K_{\mathfrak{p}}, \tilde{E}[p]) & \xrightarrow{\beta_{\mathfrak{p}}} & H^1(K_{\mathfrak{p}}, \tilde{E}[p^\infty]) \\ \downarrow & & \uparrow & & \uparrow \\ H^1(K_{\mathfrak{p}}, E[p]) & \xrightarrow{\sim} & H^1(K_{\mathfrak{p}}, E[p]) & \longrightarrow & H^1(K_{\mathfrak{p}}, E[p^\infty]) \end{array} \tag{2.46}$$

By the injectivity of $\beta_{\mathfrak{p}}$,

$$\begin{aligned} \mathcal{L}_{\mathfrak{p}}(\Psi) &= \ker\left(H^1(K_{\mathfrak{p}}, \Psi) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\operatorname{im}(\lambda_{\mathfrak{p}})\right) \\ &= \ker\left(H^1(K_{\mathfrak{p}}, \Psi) \longrightarrow H^1(K_{\mathfrak{p}}, \tilde{E}[p^\infty])\right) \\ &= 0. \end{aligned} \tag{2.47}$$

Thus, $\mathcal{L}_{\mathfrak{p}}(\Psi) = 0 = \mathcal{L}_{\mathfrak{p}}^{\pm}(\Psi)$. □

2.4.2 Good, ordinary reduction

Throughout this subsection, suppose E has good, ordinary reduction at $\mathfrak{p}$. Let $\theta : G_{K_{\mathfrak{p}}} \longrightarrow \mathbf{Z}_p^{\times}$ be the character which gives the Galois action on $\tilde{E}[p^{\infty}]$. Then θ is an unramified character of infinite order. If χ_p gives the Galois action on $\mu_{p^{\infty}}$, then by the Weil pairing, $\chi_p \cdot \theta^{-1}$ gives the Galois action on $\hat{E}[p^{\infty}]$. Let n be the largest integer such that $\theta \equiv 1 \pmod{p^n}$.

Lemma 2.9. $H^1(K_{\mathfrak{p}}, \hat{E}[p^{\infty}]) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{[K_{\mathfrak{p}}:\mathbf{Q}_p]} \times (\mathbf{Z}/p^n\mathbf{Z})$.

Proof. Take $m \geq n$, and consider the short exact sequence

$$0 \longrightarrow \hat{E}[p^m] \longrightarrow \hat{E}[p^{\infty}] \xrightarrow{\sim} \hat{E}[p^{\infty}] \longrightarrow 0; \tag{2.48}$$

applying Galois cohomology gives us the long exact sequence

$$\begin{aligned} 0 \longrightarrow\ & H^0(K_{\mathfrak{p}}, \hat{E}[p^m]) \longrightarrow H^0(K_{\mathfrak{p}}, \hat{E}[p^{\infty}]) \xrightarrow{p^m} H^0(K_{\mathfrak{p}}, \hat{E}[p^{\infty}]) \\ \longrightarrow\ & H^1(K_{\mathfrak{p}}, \hat{E}[p^m]) \longrightarrow H^1(K_{\mathfrak{p}}, \hat{E}[p^{\infty}])[p^m] \longrightarrow 0. \end{aligned} \tag{2.49}$$

Since $H^0(K_{\mathfrak{p}}, \hat{E}[p^{\infty}])$ is finite,

$$\begin{aligned} \#H^1(K_{\mathfrak{p}}, \hat{E}[p^{\infty}])[p^m] &= \frac{\#H^1(K_{\mathfrak{p}}, \hat{E}[p^m])}{\#H^0(K_{\mathfrak{p}}, \hat{E}[p^m])} \\ &= \#H^2(K_{\mathfrak{p}}, \hat{E}[p^m]) \cdot \Big(\chi(K_{\mathfrak{p}}, \hat{E}[p^m])\Big)^{-1} \\ &= \#H^2(K_{\mathfrak{p}}, \hat{E}[p^m]) \cdot p^{m \cdot [K_{\mathfrak{p}}:\mathbf{Q}_p]}. \end{aligned} \tag{2.50}$$

By local duality,

$$\#H^2(K_{\mathfrak{p}}, \hat{E}[p^m]) = \#H^0(K_{\mathfrak{p}}, \tilde{E}[p^m]) = p^n. \tag{2.51}$$

Thus, $\#H^1(K_{\mathfrak{p}}, \hat{E}[p^{\infty}])[p^m] = p^{m \cdot [K_{\mathfrak{p}}:\mathbf{Q}_p]+n}$ for all $m \geq n$, and the result follows. □

As in the multiplicative case, we have the commutative diagram (2.37). In contrast to that case, however, $\beta_{\mathfrak{p}}$ need not be injective.

Lemma 2.10. $\ker(\beta_{\mathfrak{p}}) = H^1_{nr}(K_{\mathfrak{p}}, \tilde{E}[p])$.

Proof. Consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1\left((K_{\mathfrak{p}})_{nr}/K_{\mathfrak{p}}, \tilde{E}[p]\right) & \xrightarrow{infl_1} & H^1\left(K_{\mathfrak{p}}, \tilde{E}[p]\right) & \xrightarrow{res_1} & H^1\left((K_{\mathfrak{p}})_{nr}, \tilde{E}[p]\right) \\ & & & & \downarrow{\scriptstyle \beta_{\mathfrak{p}}} & & \downarrow{\scriptstyle \beta_{\mathfrak{p}}^{nr}} \\ 0 & \longrightarrow & H^1\left((K_{\mathfrak{p}})_{nr}, \tilde{E}[p^\infty]\right) & \xrightarrow{infl_2} & H^1\left(K_{\mathfrak{p}}, \tilde{E}[p^\infty]\right) & \xrightarrow{res_2} & H^1\left((K_{\mathfrak{p}})_{nr}, \tilde{E}[p^\infty]\right), \end{array} \tag{2.52}$$

where the rows are exact, given by the inflation-restriction sequence. The action of $G_{(K_{\mathfrak{p}})_{nr}}$ on $\tilde{E}[p^\infty]$ is trivial, so $\ker(\beta_{\mathfrak{p}}^{nr}) \cong \tilde{E}[p^\infty]/p\tilde{E}[p^\infty] = 0$.

Since $\tilde{E}[p^\infty] \cong \mathbf{Q}_p/\mathbf{Z}_p$, $G_{(K_{\mathfrak{p}})_{nr}} \cong \hat{\mathbf{Z}}$ and $\tilde{E}(K_{\mathfrak{p}})[p^\infty]$ is finite, $H^1((K_{\mathfrak{p}})_{nr}, \tilde{E}[p^\infty]) = 0$ by exercise 2.2 of [14]. Thus, res_2 is injective. By the commutativity of (2.52), $res_2 \circ \beta_{\mathfrak{p}} = \beta_{\mathfrak{p}}^{nr} \circ res_1$. Since res_2 and $\beta_{\mathfrak{p}}^{nr}$ are injective, $\ker(\beta_{\mathfrak{p}}) = \ker(res_1) = H^1_{nr}(K_{\mathfrak{p}}, \tilde{E}[p])$. □

Lemma 2.11. $\ker\left(H^1(K_{\mathfrak{p}}, \hat{E}[p]) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\operatorname{im}(\lambda_{\mathfrak{p}})_{div}\right) = H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p])$.

Proof. It is clear from (2.37) that $\operatorname{im}(\lambda_{\mathfrak{p}} \circ \alpha_{\mathfrak{p}}) \subseteq \operatorname{im}(\lambda_{\mathfrak{p}})$. If $n = 0$, so $\theta \not\equiv 1 \pmod{p}$, $\hat{E}[p] \not\cong \mu_p$. Hence by lemma 1.1, $H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p]) = H^1(K_{\mathfrak{p}}, \hat{E}[p])$. In this case, $\operatorname{im}(\lambda_{\mathfrak{p}})$ is a divisible group, and

$$H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p]) = H^1(K_{\mathfrak{p}}, \hat{E}[p]) = \ker\left(H^1(K_{\mathfrak{p}}, \hat{E}[p]) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\operatorname{im}(\lambda)_{div}\right). \tag{2.53}$$

Suppose $n \geq 1$. Since $H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty]) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{[K_{\mathfrak{p}}:\mathbf{Q}_p]} \times (\mathbf{Z}_p/p^n\mathbf{Z}_p)$,

$$H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])_{div} = p^n \cdot H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty]). \tag{2.54}$$

Consider the following commutative diagram, with short, exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{E}[p^{n+1}] & \longrightarrow & \hat{E}[p^\infty] & \xrightarrow{p^{n+1}} & \hat{E}[p^\infty] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \| & & \\ 0 & \longrightarrow & \hat{E}[p] & \longrightarrow & \hat{E}[p^\infty] & \xrightarrow{p} & \hat{E}[p^\infty] & \longrightarrow & 0 \end{array} \tag{2.55}$$

Applying Galois cohomology, we obtain a new commutative diagram,

$$\begin{array}{ccc} H^1(K_\mathfrak{p}, \hat{E}[p^{n+1}]) & \xrightarrow{\alpha_\mathfrak{p}^{(n+1)}} & H^1(K_\mathfrak{p}, \hat{E}[p^\infty])[p^{n+1}] \\ {\scriptstyle p^n}\downarrow & & {\scriptstyle p^n}\downarrow \\ H^1(K_\mathfrak{p}, \hat{E}[p]) & \xrightarrow{\alpha_\mathfrak{p}} & H^1(K_\mathfrak{p}, \hat{E}[p^\infty])[p], \end{array} \tag{2.56}$$

in which the maps $\alpha_\mathfrak{p}$ and $\alpha_\mathfrak{p}^{(n+1)}$ are surjective. Let $\sigma \in H^1(K_\mathfrak{p}, \hat{E}[p])$ and suppose $\alpha_\mathfrak{p}(\sigma) \in p^n \cdot H^1(K_\mathfrak{p}, \hat{E}[p^\infty])$; then $\alpha_\mathfrak{p}(\sigma) = p^n \cdot \alpha_\mathfrak{p}^{(n+1)}(\tilde{\sigma})$ for some $\tilde{\sigma} \in H^1(K_\mathfrak{p}, \hat{E}[p^{n+1}])$, and $\sigma - p^n \cdot \tilde{\sigma} \in \ker(\alpha_\mathfrak{p})$.

As we will prove in lemmas 2.12 and 2.13,

$$p^n \cdot H^1(K_\mathfrak{p}, \hat{E}[p^{n+1}]) \subseteq H^1_{pr}(K_\mathfrak{p}, \hat{E}[p]) \tag{2.57}$$

and

$$\ker(\alpha_\mathfrak{p}) \subseteq H^1_{pr}(K_\mathfrak{p}, \hat{E}[p]). \tag{2.58}$$

Thus, if $\alpha_\mathfrak{p}(\sigma) \in H^1(K_\mathfrak{p}, \hat{E}[p^\infty])_{div}$, $\sigma \in H^1_{pr}(K_\mathfrak{p}, \hat{E}[p])$. That is,

$$\ker\left(H^1(K_\mathfrak{p}, \hat{E}[p]) \longrightarrow \frac{H^1(K_\mathfrak{p}, \hat{E}[p^\infty])[p]}{H^1(K_\mathfrak{p}, \hat{E}[p^\infty])_{div}[p]} \right) \subseteq H^1_{pr}(K_\mathfrak{p}, \hat{E}[p]). \tag{2.59}$$

But

$$\frac{H^1(K_\mathfrak{p}, \hat{E}[p^\infty])[p]}{H^1(K_\mathfrak{p}, \hat{E}[p^\infty])_{div}[p]} \cong \mathbf{Z}/p\mathbf{Z}, \tag{2.60}$$

and by lemma 1.1

$$H^1(K_\mathfrak{p}, \hat{E}[p])/H^1_{pr}(K_\mathfrak{p}, \hat{E}[p]) \cong \mathbf{Z}/p\mathbf{Z}, \tag{2.61}$$

so $\alpha_\mathfrak{p}(\sigma) \in H^1(K_\mathfrak{p}, \hat{E}[p^\infty])_{div}$ if and only if $\sigma \in H^1_{pr}(K_\mathfrak{p}, \hat{E}[p])$.

By proposition 4.6 of [4],

$$\#\left(\frac{\mathrm{im}(\lambda_\mathfrak{p})}{\mathrm{im}(\lambda_\mathfrak{p})_{div}} \right) = \#H^0(K_\mathfrak{p}, \tilde{E}[p^\infty]) = p^n = \#\left(\frac{H^1(K_\mathfrak{p}, \hat{E}[p^\infty])}{H^1(K_\mathfrak{p}, \hat{E}[p^\infty])_{div}} \right). \tag{2.62}$$

Thus, $\ker(\lambda_{\mathfrak{p}}) \subseteq H^1(K_{\mathfrak{p}}, \hat{E}[p])_{div}$, so

$$\sigma \in \ker\left(H^1(K_{\mathfrak{p}}, \hat{E}[p]) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\operatorname{im}(\lambda_{\mathfrak{p}})_{div}\right) \tag{2.63}$$

if and only if

$$\alpha_{\mathfrak{p}}(\sigma) \in H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])_{div}. \tag{2.64}$$

Therefore, $H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p]) = \ker\left(H^1(K_{\mathfrak{p}}, \hat{E}[p]) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\operatorname{im}(\lambda_{\mathfrak{p}})\right)$. □

Our proof of lemma 2.11 will be complete once we prove the following two lemmas.

Lemma 2.12. $p^n \cdot H^1(K_{\mathfrak{p}}, \hat{E}[p^{n+1}]) \subseteq H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p])$.

Proof. If $n = 0$, then $H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p]) = H^1(K_{\mathfrak{p}}, \hat{E}[p])$, and the result is automatically true.

Suppose $n \geq 1$, and let $L/K_{\mathfrak{p}}$ be the minimal extension such that $\theta|_{G_L} \equiv 1 \pmod{p^{n+1}}$. Then $L/K_{\mathfrak{p}}$ is the unramified extension of degree p. We have the following commutative diagram, in which the horizontal maps are given by restriction.

$$\begin{array}{ccccc} H^1(K_{\mathfrak{p}}, \hat{E}[p^{n+1}]) & \longrightarrow & H^1(L, \mu_{p^{n+1}})^{(\theta)} & = & \left(\frac{L^\times}{(L_\times)^{p^{n+1}}}\right)^{(\theta)} \\ {\scriptstyle p^n}\downarrow & & {\scriptstyle p^n}\downarrow & & {\scriptstyle p^n}\downarrow \\ H^1(K_{\mathfrak{p}}, \hat{E}[p]) & \longrightarrow & H^1(L, \mu_p)^{(\theta)} & = & \left(\frac{L^\times}{(L^\times)^p}\right)^{(\theta)} \end{array} \tag{2.65}$$

Let π be a uniformizer for $K_{\mathfrak{p}}$. Then, since $L/K_{\mathfrak{p}}$ is unramified, π is also a uniformizer for L. Since $\theta \equiv 1 \pmod{p}$,

$$\left(\frac{L^\times}{(L^\times)^p}\right)^{(\theta)} \cong \frac{\langle\pi\rangle}{\langle\pi^p\rangle} \times \left(\frac{\mathcal{O}_L^\times}{(\mathcal{O}_L^\times)^p}\right)^{(\theta)}. \tag{2.66}$$

Since $\theta \equiv 1 \pmod{p^n}$, but $\theta \not\equiv 1 \pmod{p^{n+1}}$,

$$\left(\frac{L^\times}{(L^\times)^{p^{n+1}}}\right)^{(\theta)} \cong \frac{\langle\pi^p\rangle}{\langle\pi^{p^{n+1}}\rangle} \times \left(\frac{\mathcal{O}_L^\times}{(\mathcal{O}_L^\times)^{p^{n+1}}}\right)^{(\theta)}. \tag{2.67}$$

Thus,

$$\left(\left(\frac{L^\times}{(L^\times)^{p^{n+1}}}\right)^{(\theta)}\right)^{p^n} \subseteq \left(\frac{\mathcal{O}_L^\times}{(\mathcal{O}_L^\times)^p}\right), \tag{2.68}$$

so

$$p^n \cdot H^1(K_\mathfrak{p}, \hat{E}[p^{n+1}]) \subseteq \ker\left(H^1(K_\mathfrak{p}, \hat{E}[p]) \longrightarrow H^1(L, \hat{E}[p])/H^1_{pr}(L, \hat{E}[p])\right). \tag{2.69}$$

Since $L/K_\mathfrak{p}$ is an unramified extension of degree p, it is tamely ramified. By the remark following lemma 1.2

$$, H^1_{pr}(K_\mathfrak{p}, \hat{E}[p]) = \ker\left(H^1(K_\mathfrak{p}, \hat{E}[p]) \longrightarrow H^1(L, \hat{E}[p])/H^1_{pr}(L, \hat{E}[p])\right), \tag{2.70}$$

and $p^n \cdot H^1(K_\mathfrak{p}, \hat{E}[p^{n+1}]) \subseteq H^1_{pr}(K_\mathfrak{p}, \hat{E}[p])$. □

Lemma 2.13. $\ker(\alpha_\mathfrak{p}) \subseteq H^1_{pr}(K_\mathfrak{p}, \hat{E}[p])$.

Proof. If $n = 0$, then $H^1_{pr}(K_\mathfrak{p}, \hat{E}[p]) = H^1(K_\mathfrak{p}, \hat{E}[p])$ and the statement is automatically true.

Suppose $n \geq 1$. Then $\hat{E}[p] \cong \mu_p$. Consider the following long exact sequence.

$$\begin{aligned} 0 \longrightarrow H^0(K_\mathfrak{p}, \mu_p) &\longrightarrow H^0(K_\mathfrak{p}, \hat{E}[p^\infty]) \xrightarrow{p} H^0(K_\mathfrak{l}, \hat{E}[p^\infty]) \\ \longrightarrow H^1(K_\mathfrak{p}, \mu_p) &\xrightarrow{\alpha_\mathfrak{p}} H^1(K_\mathfrak{p}, \hat{E}[p^\infty])[p] \longrightarrow 0 \end{aligned} \tag{2.71}$$

If $\mu_p \not\subseteq K_\mathfrak{p}$, then $H^0(K_\mathfrak{p}, \hat{E}[p^\infty]) = 0$, and $\alpha_\mathfrak{p}$ is injective, so the statement automatically holds. Suppose $\mu_p \subseteq K_\mathfrak{p}$, and let m be the largest integer such that $\chi_p \cdot \theta^{-1} \equiv 1 \pmod{p^m}$. Then $m \geq 1$, and $H^0(K_\mathfrak{p}, \hat{E}[p^\infty]) = H^0(K_\mathfrak{p}, \hat{E}[p^m]) \cong \mathbf{Z}/p^m\mathbf{Z}$. Take P to be a generator of $\hat{E}[p^m]$, and choose $Q \in \hat{E}[p^{m+1}]$ such that $p \cdot Q = P$. Then $\ker(\alpha_\mathfrak{p})$ is generated by the cocycle $f_Q : g \mapsto (g(Q) - Q)$.

Let $L = K_\mathfrak{p}(Q)$, a degree p extension of $K_\mathfrak{p}$, and consider the extension $L_{nr}/(K_\mathfrak{p})_{nr}$. Since $\theta|_{G_{K_\mathfrak{p}}}$ is trivial $\mu_{p^m} \subseteq (K_\mathfrak{p})_{nr}$, and $L_{nr} = (K_\mathfrak{p})_{nr}(\mu_{p^{m+1}})$. Thus, L_{nr} is gotten from $(K_\mathfrak{p})_{nr}$ by adjoining the p^{th} power of a unit, so $L \subseteq L_{nr} \subseteq (K_\mathfrak{p})_{pr}$.

$$\begin{aligned} f_Q &\in \ker\left(H^1(K_\mathfrak{p}, \hat{E}[p]) \longrightarrow H^1(L, \hat{E}[p])\right) \\ &\subseteq \ker\left(H^1(K_\mathfrak{p}, \hat{E}[p]) \longrightarrow H^1((K_\mathfrak{p})_{pr}, \hat{E}[p])\right) \\ &= H^1_{pr}(K, \hat{E}[p]), \end{aligned} \tag{2.72}$$

so $\ker(\alpha_{\mathfrak{p}}) \subseteq H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p])$. □

Lemma 2.14. *Let $L/K_{\mathfrak{p}}$ be the unramified extension of degree p. Then*

$$\mathrm{im}(\lambda_{\mathfrak{p}}) \cap \ker\left(H^1(K_{\mathfrak{p}}, E[p^\infty]) \longrightarrow H^1(L, E[p^\infty])\right) \subseteq \mathrm{im}(\lambda_{\mathfrak{p}})_{div}. \tag{2.73}$$

Proof. Consider the following commutative diagram.

$$\begin{array}{ccccc} H^1(K_{\mathfrak{p}}, \hat{E}[p]) & \xrightarrow{\alpha_{\mathfrak{p}}} & H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty]) & \xrightarrow{\lambda_{\mathfrak{p}}} & H^1(K_{\mathfrak{p}}, E[p^\infty]) \\ \downarrow{\scriptstyle \rho_1} & & \downarrow{\scriptstyle \rho_2} & & \downarrow{\scriptstyle \rho_3} \\ H^1(L, \hat{E}[p]) & \xrightarrow{\alpha_L} & H^1(L, \hat{E}[p^\infty]) & \xrightarrow{\lambda_L} & H^1(L, E[p^\infty]) \end{array} \tag{2.74}$$

Since $[L : K_{\mathfrak{p}}] = p$, $\ker(\rho_3)$ has exponent p. Let $\sigma \in \mathrm{im}(\lambda_{\mathfrak{p}}) \cap \ker(\rho_3)$, and choose $\hat{\sigma} \in H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])$ such that $\lambda_{\mathfrak{p}}(\hat{\sigma}) = \sigma$. By proposition 4.6 of [4], $\ker(\lambda_{\mathfrak{p}}) \subseteq H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])_{div}$. Thus, since σ has order dividing p, we can write $\hat{\sigma} = \sigma_d + \sigma_p$ where $\sigma_d \in H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])_{div}$ and $\sigma_p \in H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])[p]$.

By the commutativity of (2.74), $\lambda_L \circ \rho_2(\hat{\sigma}) = \rho_3(\sigma) = 0$, so $\rho_2(\hat{\sigma}) \in \ker(\lambda_L) \subseteq H^1(L, \hat{E}[p^\infty])_{div}$. Since $\rho_2(\sigma_d) \in H^1(L, \hat{E}[p^\infty])_{div}$, $\rho_2(\sigma_p) \in H^1(L, \hat{E}[p^\infty])_{div}$ as well. By construction, σ_p has order dividing p, so $\rho_2(\sigma_p)$ also has order dividing p. The maps $\alpha_{\mathfrak{p}}$ and α_L are surjective onto the elements of $H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])$ and $H^1(L, \hat{E}[p^\infty])$ of order p. Thus, we can choose $\sigma_{\mathfrak{p}} \in H^1(K_{\mathfrak{p}}, \hat{E}[p])$ and $\sigma_L \in H^1(L, \hat{E}[p])$ such that $\sigma_p = \alpha_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$ and $\rho_2(\sigma_p) = \alpha_L(\sigma_L)$.

Again using the commutativity of (2.74), $\alpha_L \circ \rho_1(\sigma_{\mathfrak{p}}) = \rho_2(\sigma_p) = \alpha_L(\sigma_L)$, so by lemma 2.13, $\sigma_L - \rho_1(\sigma_{\mathfrak{p}}) \in \ker(\alpha_L) \subseteq H^1_{pr}(L, \hat{E}[p])$. By construction, $\alpha_L(\sigma_L) \in H^1(L, \hat{E}[p^\infty])_{div}$, so $\sigma_L \in H^1_{pr}(L, \hat{E}[p])$. Hence $\rho_1(\sigma_{\mathfrak{p}}) \in H^1_{pr}(L, \hat{E}[p])$. Since $L/K_{\mathfrak{p}}$ is unramified, $H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p]) = \rho_1^{-1}\left(H^1_{pr}(L, \hat{E}[p])\right)$, and $\sigma_{\mathfrak{p}} \in H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p])$.

By the proof of lemma 2.11, $\alpha_{\mathfrak{p}}\left(H^1_{pr}(K_{\mathfrak{p}}, \hat{E}[p])\right) \subseteq H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])_{div}$, so $\sigma_p \in H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])_{div}$, whence $\hat{\sigma} = \sigma_d + \sigma_p \in H^1(K_{\mathfrak{p}}, \hat{E}[p^\infty])_{div}$, and $\sigma = \lambda_{\mathfrak{p}}(\hat{\sigma}) \in \mathrm{im}(\lambda)_{div}$.

□

Proposition 2.15. *Suppose E has good, ordinary reduction at $\mathfrak{p}$ for a prime $\mathfrak{p}$ lying over p. Then $\mathcal{L}_{\mathfrak{p}}(\Psi) = \mathcal{L}^{\pm}_{\mathfrak{p}}(\Psi)$ and $\mathcal{L}_{\mathfrak{p}}(\Phi) \subseteq \mathcal{L}^{+}_{\mathfrak{p}}(\Phi)$.*

Proof. First suppose Ψ is in the kernel of reduction modulo $\mathfrak{p}$. Then we can associate $H^1(K_\mathfrak{p}, \Psi)$ with $H^1(K_\mathfrak{p}, \hat{E}[p])$ and $H^1(K_\mathfrak{p}, \Phi)$ with $H^1(K_\mathfrak{p}, \tilde{E}[p])$, so

$$\begin{aligned}
\mathcal{L}_\mathfrak{p}^{\pm}(\Psi) &= H^1_{pr}(K_\mathfrak{p}, \Psi) \\
&= \ker\left(H^1(K_\mathfrak{p}, \Psi) \longrightarrow H^1(K_\mathfrak{p}, E[p^\infty])/\operatorname{im}(\lambda_\mathfrak{p})_{div}\right) \\
&= \ker\left(H^1(K_\mathfrak{p}, \Psi) \longrightarrow H^1(K_\mathfrak{p}, E[p^\infty])/\operatorname{im}(\kappa_\mathfrak{p})\right) \\
&= \mathcal{L}_\mathfrak{p}(\Psi). \qquad (2.75)
\end{aligned}$$

Also,

$$\begin{aligned}
S_{E[p]} &\subseteq \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_\mathfrak{p}, E[p^\infty])/\operatorname{im}(\kappa_\mathfrak{p})\right) \\
&\subseteq \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_\mathfrak{p}, E[p^\infty])/\operatorname{im}(\lambda_\mathfrak{p})\right) \\
&= \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_\mathfrak{p}, \tilde{E}[p^\infty])\right) \\
&= \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_\mathfrak{p}, \Phi)/H^1_{nr}(K_\mathfrak{p}, \Phi)\right), \qquad (2.76)
\end{aligned}$$

so $\mathcal{L}_\mathfrak{p}(\Phi) \subseteq H^1_{nr}(K_\mathfrak{p}, \Phi) = \mathcal{L}_\mathfrak{p}^{+}(\Phi)$.

Next, suppose Ψ is not in the kernel of reduction modulo $\mathfrak{p}$. Then $E[p] \cong \Psi \times \hat{E}[p]$ as a $G_{K_\mathfrak{p}}$-module, and we can associate $H^1(K_\mathfrak{p}, \Psi)$ with $H^1(K_\mathfrak{p}, \tilde{E}[p])$ and $H^1(K_\mathfrak{p}, \Phi)$ with $H^1(K_\mathfrak{p}, \hat{E}[p])$. Consider the following commutative diagram.

$$\begin{array}{ccccc}
H^1(K_\mathfrak{p}, \Phi) & \longrightarrow & H^1(K_\mathfrak{p}, E[p]) & \longleftarrow & H^1(K_\mathfrak{p}, \Psi) \\
{\scriptstyle \alpha_\mathfrak{p}}\downarrow & & \downarrow & & {\scriptstyle \beta_\mathfrak{p}}\downarrow \\
H^1(K_\mathfrak{p}, \hat{E}[p^\infty]) & \xrightarrow{\lambda_\mathfrak{p}} & H^1(K_\mathfrak{p}, E[p^\infty]) & \longrightarrow & H^1(K_\mathfrak{p}, \tilde{E}[p^\infty])
\end{array} \qquad (2.77)$$

By lemma 2.10,

$$\begin{aligned}
H^1_{nr}(K_\mathfrak{p}, \Psi) &= \ker(\beta_\mathfrak{p}) \\
&= \ker\left(H^1(K_\mathfrak{p}, \Psi) \longrightarrow H^1(K_\mathfrak{p}, E[p^\infty])/\operatorname{im}(\lambda_\mathfrak{p})\right). \qquad (2.78)
\end{aligned}$$

If $L/K_\mathfrak{p}$ is the unramified extension of degree p, then

$$\begin{aligned}
H^1_{nr}(K_\mathfrak{p}, \Psi) &\subseteq \ker\left(H^1(K_\mathfrak{p}, \Psi) \longrightarrow H^1(L, \Psi)\right) \\
&\subseteq \ker\left(H^1(K_\mathfrak{p}, \Psi) \longrightarrow H^1(L, E[p^\infty])\right). \qquad (2.79)
\end{aligned}$$

Thus, by lemma 2.14

$$\begin{aligned}\mathcal{L}_{\mathfrak{p}}^{\pm}(\Psi) &= H^1_{nr}(K_{\mathfrak{p}}, \Psi) \\ &= \ker\left(H^1(K_{\mathfrak{p}}, \Psi) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\operatorname{im}(\lambda_{\mathfrak{p}})_{div}\right) \\ &= \mathcal{L}_{\mathfrak{p}}(\Psi). \end{aligned} \tag{2.80}$$

Let $\sigma \in S_\Phi$, and choose $\sigma' \in S_{E[p]}$ such that σ is the image of σ' in $H^1(K_\Sigma/K, \Phi)$.

$$\sigma' \in \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\operatorname{im}(\lambda_{\mathfrak{p}})_{div}\right), \tag{2.81}$$

so the image of σ in $H^1(K_{\mathfrak{p}}, E[p^\infty])$ is in the subgroup generated by $\operatorname{im}(\lambda_{\mathfrak{p}})_{div}$ and $\operatorname{im}\left(H^1(K_{\mathfrak{p}}, \Psi) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])\right)$; the image of σ must also be in $\operatorname{im}(\lambda_{\mathfrak{p}})$, so by lemma 2.14 the image of σ must be in $\operatorname{im}(\lambda_{\mathfrak{p}})_{div}$.

Thus,

$$\begin{aligned} S_\Phi &\subseteq \ker\left(H^1(K_\Sigma/K, \Phi) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\operatorname{im}(\lambda_{\mathfrak{p}})_{div}\right) \\ &= \ker\left(H^1(K_\Sigma/K, \Phi) \longrightarrow H^1(K_{\mathfrak{p}}, \Phi)/H^1_{pr}(K_{\mathfrak{p}}, \Psi)\right) \\ &= \ker\left(H^1(K_\Sigma/K, \Phi) \longrightarrow H^1(K_{\mathfrak{p}}, \Phi)/\mathcal{L}_{\mathfrak{p}}^{+}(\Phi)\right), \end{aligned} \tag{2.82}$$

and $\mathcal{L}_{\mathfrak{p}}(\Phi) \subseteq \mathcal{L}_{\mathfrak{p}}^{+}(\Phi)$. □

Combining propositions 2.6, 2.8 and 2.15, we have proved theorem 2.3.

2.5 Selmer groups and class groups

Consider the cohomology groups $H^1(K_\Sigma/K, \Psi)$ and $H^1(K_\Sigma/K, \Phi)$. For notational convenience, we use Θ to denote one of the Galois-modules Ψ and Φ, and let θ denote the character which gives the Galois action on Θ. Inflation-restriction gives us an exact sequence

$$\begin{aligned} 0 \longrightarrow\ & H^1(K(\Theta)/K, \Theta) \xrightarrow{infl} H^1(K_\Sigma/K, \Theta) \xrightarrow{res} H^1(K_\Sigma/K(\Theta), \Theta)^{G_{K(\Theta)/K}} \\ \longrightarrow\ & H^2(K(\Theta)/K, \Theta). \end{aligned} \tag{2.83}$$

Since Θ has order p, $[K(\Theta) : K] \mid (p-1)$. Thus, the groups $H^1(K(\Theta)/K, \Theta)$ and $H^2(K(\Theta)/K, \Theta)$ vanish, and *res* gives an isomorphism

$$H^1(K_\Sigma/K, \Theta) \cong H^1(K_\Sigma/K(\Theta), \Theta)^{G_{K(\Theta)/K}}. \tag{2.84}$$

But, $G_{K_\Sigma/K(\Theta)}$ acts trivially on Θ, so

$$\begin{aligned} H^1\left(K_\Sigma/K(\Theta), \Theta\right)^{G_{K(\Theta)/K}} &\cong H^1(K_\Sigma/K(\Theta), \mathbf{Z}/p\mathbf{Z})^{(\theta)} \\ &\cong \mathrm{Hom}\left(G_{K_\Sigma/K(\Theta)}, \mathbf{Z}/p\mathbf{Z}\right)^{(\theta)} \\ &\cong \mathrm{Hom}\left((G_{K_\Sigma/K(\Theta)})^{ab}, \mathbf{Z}/p\mathbf{Z}\right)^{(\theta)}. \end{aligned} \tag{2.85}$$

That is, elements of $H^1(K_\Sigma/K, \Theta)$ correspond to extensions $L/K(\Theta)$ of degree p which are Galois over K, unramified outside the set of primes of $K(\Theta)$ lying over primes in Σ, and such that $G_{K(\Theta)/K}$ acts on $G_{L/K(\Theta)}$ by the character θ. The extension $L/K(\Theta)$ is unramified (resp. *peu ramifiée*) at all primes of $K(\Theta)$ lying over $\mathfrak{l}$ if and only if the corresponding element of $H^1(K_\Sigma/K, \Theta)$ is in the pre-image of $H^1_{nr}(K_\mathfrak{l}, \Theta)$ (resp. $H^1_{pr}(K_\mathfrak{l}, \Theta)$) under the map $H^1(K_\Sigma/K, \Theta) \longrightarrow H^1(K_\mathfrak{l}, \Theta)$. The primes of $K(\Theta)$ lying over $\mathfrak{l}$ split completely in $L/K(\Theta)$ if and only if the corresponding element of $H^1(K_\Sigma/K, \Theta)$ is in

$$\ker\left(H^1(K_\Sigma/K, \Theta) \longrightarrow H^1(K_\mathfrak{l}, \Theta)\right). \tag{2.86}$$

Hence, we have the following.

Definition. Let $L^{\pm}_\Psi$ (resp. L^{+}_Φ) be the maximal, abelian extensions of $K(\Psi)$ (resp. $K(\Phi)$) of exponent p which are unramified outside Σ, such that $G_{K(\Psi)/K}$ acts via ψ on $G_{L^{\pm}_\Psi/K(\Psi)}$ (resp. $G_{K(\Phi)/K}$ acts via ϕ on $G_{L^{+}_\Phi/K(\Phi)}$), and such that:

- if E has additive reduction at $\mathfrak{l} \nmid p$ then places lying above $\mathfrak{l}$ split completely in $L^{-}_\Psi/K(\Psi)$;
- if E has multiplicative reduction at $\mathfrak{l}$ and Ψ corresponds to μ_p under the Tate parametrization then places lying above $\mathfrak{l}$ split completely in $L^{+}_\Phi/K(\Phi)$;

• if E has multiplicative reduction at $\mathfrak{l}$ and Ψ does not correspond to μ_p under the Tate parametrization then places lying above $\mathfrak{l}$ split completely in $L_\Psi^\pm/K(\Psi)$;
• if E has good, ordinary reduction at $\mathfrak{p} \mid p$ and Ψ is in the kernel of reduction modulo $\mathfrak{p}$ then places lying over $\mathfrak{p}$ are unramified in $L_\Phi^+/K(\Phi)$ and *peu ramifiée* in $L_\Psi^\pm/K(\Psi)$;
• if E has good, ordinary reduction at $\mathfrak{p} \mid p$ and Ψ is not in the kernel of reduction modulo $\mathfrak{p}$ then places lying over $\mathfrak{p}$ are *peu ramifiée* in $L_\Phi^+/K(\Phi)$ and unramified in $L_\Psi^\pm/K(\Psi)$.

With these definitions, $\#S_\Psi^\pm = [L_\Psi^\pm : K(\Psi)]$, $\#S_\Phi^+ = [L_\Phi^+ : K(\Phi)]$, and we have the following.

Theorem 2.16.

$$\frac{[L_\Psi^- : K(\Psi)]}{\#\Psi(K) \cdot \#\Phi(K)} \leq \#\operatorname{Sel}_E(\mathbf{Q})[p] \leq \frac{[L_\Psi^+ : K(\Psi)] \cdot [L_\Phi : K(\Phi)]}{\#\Psi(K) \cdot \#\Phi(K)}. \tag{2.87}$$

2.6 Frey's theorem

As a consequence of theorem 2.16 we have the following strengthening of Frey's theorem (see section 1.4).

Corollary 2.17. *Let E, p, S_E, $\tilde{S}_E$, F, F', F'', K and K' be defined as in Frey's theorem, and let K''/K be the maximal subextension of K' in which the places of K lying over primes in S_E split completely. If $d \neq 1$ is a square-free integer satisfying the hypotheses of Frey's theorem, then*

$$[F' : F] \leq \#\operatorname{Sel}_{E^d}(\mathbf{Q})[p] \leq [F'' : F] \cdot [K'' : K]. \tag{2.88}$$

Remark. The bounds given in corollary 2.17 agree with the bounds given in Frey's theorem unless $K'' \neq K'$, in which case the upper bound in corollary 2.17 is stronger. A necessary (but not sufficient) condition for $K'' \neq K'$ is for S_E to be non-empty. Let $l \in S_E$. Then $l \equiv -1 \pmod{p}$; in particular, $l \not\equiv +1 \pmod{p}$, so $\dim_{\mathbf{F}_p} H^1(\mathbf{Q}_l, \Phi) \leq 1$. Thus, $[K' : K''] \leq p^{\#S_E}$, and the upper bound in corollary 2.17 differs from the upper bound in Frey's theorem by at most a factor of $p^{\#S_E}$.

Proof. Let ε_d be the quadratic character corresponding to the extension $F/\mathbf{Q}$. Because $E(\mathbf{Q})$ has a point of order p, E^d admits a $\mathbf{Q}$-rational isogeny of degree p with kernel $\Psi \cong \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon_d$, and we have the short exact sequence

$$0 \longrightarrow \Psi \longrightarrow E[p] \longrightarrow \Phi \longrightarrow 0, \tag{2.89}$$

where $\Phi \cong \mu_p \otimes \varepsilon_d$. Since $d \neq 1$, p is odd and $(d,p) = 1$, $\Psi(\mathbf{Q}) = \Phi(\mathbf{Q}) = 0$.

Let $L_\Psi^\pm$ and L_Φ^+ be the fields defined in section 2.5, noting that $F = \mathbf{Q}(\Psi)$ and $K = \mathbf{Q}(\Phi)$. We will show $F' = L_\Psi^-$, $F'' = L_\Psi^+$ and $L_\Phi^+ = K''$. The corollary will then follow directly from theorem 2.16. These fields are all defined as the maximal, abelian extensions of F or K of exponent p, with certain specified Galois action, and with specified behavior at places of F or K. In order to prove the equalities, it will be enough to show the specified behavior at all places is the same.

Let D be the discriminant of the field F, and let $\Sigma = \{l : l \mid N_E \cdot D\} \cup \{p, \infty\}$.

Suppose E^d has good reduction at $l \in \Sigma$ for some $l \neq p$. Then $l \mid D$, so Ψ and Φ are ramified at l and $H^1(\mathbf{Q}_l, \Psi) = H^1(\mathbf{Q}_l, \Phi) = 0$. Thus, places dividing l automatically split completely in extensions of F and K of exponent p with the appropriate Galois action, and the conditions on L_Ψ^- and F', L_Ψ^+ and F'', and L_Φ^+ and K'' at places dividing l are equivalent.

Suppose E^d has additive reduction at l. (By hypothesis, $l \neq p$.) Then either $l \mid D$ or $l \mid N_E$. In the former case, $H^1(\mathbf{Q}_l, \Psi) = H^1(\mathbf{Q}_l, \Phi) = 0$, and again the conditions at places dividing l are equivalent. In the latter case, $v_l(j_E) \geq 0$, since otherwise E would be isomorphic to a Tate curve over a ramified, quadratic extension of $\mathbf{Q}_l$, and $\mathbf{Z}/p\mathbf{Z}$ would then necessarily be ramified at l. By hypothesis, $\left(\frac{d}{l}\right) = -1$. If $l \not\equiv -1 \pmod{p}$, then $H^1(\mathbf{Q}_l, \Psi)$ and $H^1(\mathbf{Q}_l, \Phi)$ are trivial yet again. If $l \equiv -1 \pmod{p}$, then $l \in \tilde{S}_E - S_E$, $H^1_{nr}(\mathbf{Q}_l, \Psi) = 0$ and $H^1_{nr}(\mathbf{Q}_l, \Phi) = H^1(\mathbf{Q}_l, \Phi)$. Places of F lying over l must split completely in L_Ψ^-/F, and must be unramified in F'/F; since $H^1_{nr}(\mathbf{Q}_l, \Psi) = 0$, these conditions are equivalent. No condition is imposed on places of F lying over l for the extensions L_Ψ^+/F and F''/F. No condition is imposed on

places of K lying over l for the extension L_Φ^+/K, and these places must be unramified in K''/K. Since $H^1_{nr}(\mathbf{Q}_l, \Phi) = H^1(\mathbf{Q}_l, \Phi)$, these conditions are equivalent.

Suppose E^d has multiplicative reduction at l, for $l \neq p$, and suppose $l \notin S_E$. Then E must also have multiplicative reduction at l. If $l \not\equiv -1 \pmod{p}$, E is a Tate curve over $\mathbf{Q}_l$, so $\left(\frac{d}{l}\right) = -1$, $H^1(\mathbf{Q}_l, \Psi) = H^1(\mathbf{Q}_l, \Phi) = 0$, and the various conditions at places lying over l are equivalent. If $l \equiv -1 \pmod{p}$ and E is a Tate curve over $\mathbf{Q}_l$, then Ψ does not correspond to μ_p under the Tate parametrization. By hypothesis, $\left(\frac{d}{l}\right) = -1$, so $H^1_{nr}(\mathbf{Q}_l, \Psi) = 0$ and $H^1_{nr}(\mathbf{Q}_l, \Phi) = H^1(\mathbf{Q}_l, \Phi)$. Places of F lying over l must be unramified in F'/F and F''/F, and must split completely in $L_\Psi^\pm/F$; since $H^1_{nr}(\mathbf{Q}_l, \Psi) = 0$, these conditions are equivalent. Places of K lying over l must be unramified in K''/K and no condition is imposed in L_Φ^+/K; since $H^1_{nr}(\mathbf{Q}_l, \Phi) = H^1(\mathbf{Q}_l, \Phi)$, these conditions are equivalent. If $l \equiv -1 \pmod{p}$ and E is not a Tate curve over $\mathbf{Q}_l$, then Ψ corresponds to μ_p under the Tate parametrization. By hypothesis, $\left(\frac{d}{l}\right) = +1$, so $H^1_{nr}(\mathbf{Q}_l, \Psi) = H^1(\mathbf{Q}_l, \Psi)$ and $H^1_{nr}(\mathbf{Q}_l, \Phi) = 0$. Places of F lying over l must be unramified in F'/F and F''/F, and no condition is imposed in $L_\Psi^\pm/F$; since $H^1_{nr}(\mathbf{Q}_l, \Psi) = H^1(\mathbf{Q}_l, \Psi)$, these are equivalent. Places of K lying over l must be unramified in K''/K and split completely in L_Φ^+/K; since $H^1_{nr}(\mathbf{Q}_l, \Phi) = 0$, these are equivalent.

Suppose E^d has multiplicative reduction at l, for $l \neq p$, and suppose $l \in S_E$. Then E is not a Tate curve over $\mathbf{Q}_l$, and Ψ corresponds to μ_p under the Tate parametrization. No condition is imposed at places of F lying over l in the extensions F'/F, F''/F and $L_\Psi^\pm/F$. Places of K lying over l must split completely in the extensions K''/K and L_Φ^+/K.

Suppose E^d has multiplicative reduction at p. Then E also has multiplicative reduction at p, and Ψ does not correspond to μ_p under the Tate parametrization. By hypothesis, $\left(\frac{d}{p}\right) = -1$, so $\Psi(\mathbf{Q}_p)$ is non-trivial and $\Phi \ncong \mu_p$ as a $G_{\mathbf{Q}_p}$-module. Thus, $H^1_{nr}(\mathbf{Q}_p, \Psi) = 0$ and $H^1_{pr}(\mathbf{Q}_p, \Phi) = H^1(\mathbf{Q}_p, \Phi)$. Places of F lying over p must be unramified in F'/F and F''/F, and must split completely in $L_\Psi^\pm/F$; since $H^1_{nr}(\mathbf{Q}_p, \Psi)$

vanishes, these conditions are equivalent. Places of K lying over p must be *peu ramifiée* in K''/K, and no condition is imposed in L_Φ^+/K. Since $H^1_{pr}(\mathbf{Q}_p, \Phi) = H^1(\mathbf{Q}_p, \Phi)$, these conditions are equivalent.

Finally, suppose E^d has good, ordinary reduction at p, in which case so does E. By hypothesis, Ψ is not in the kernel of reduction modulo p. Thus, places of F lying over p must be unramified in the extensions F'/F, F''/F and $L_\Psi^\pm/F$, and places of K lying over p must be *peu ramifiée* in the extensions K''/K and L_Φ^+/K.

For all places of F and K lying over primes in Σ, the conditions on F' and L_Ψ^-, F'' and L_Ψ^+, and K'' and L_Φ^+ are equivalent. Hence, $F' = L_\Psi^-$, $F'' = L_\Psi^+$ and $K'' = L_\Phi^+$, and the result follows. □

2.7 Additive reduction

In this section, we will discuss what happens when E has additive reduction at $\mathfrak{l}$, considering separately the cases $\mathfrak{l} \nmid p$ and $\mathfrak{l} \mid p$.

2.7.1 Additive reduction away from p

Suppose E has additive reduction at $\mathfrak{l} \nmid p$. Then E has either potentially good, or potentially multiplicative reduction at $\mathfrak{l}$.

Lemma 2.18. *Suppose $\mathfrak{l}$ is a finite place of K not lying over p. Then $\mathfrak{l} \in \mathrm{Ram}(\Psi/K)$ if and only if $\mathfrak{l} \in \mathrm{Ram}(\Phi/K)$.*

Proof. Let ψ, ϕ and ω be the $\mathbf{Z}_p^\times$-valued characters which give the action of $G_{K_\mathfrak{l}}$ on Ψ, Φ and μ_p respectively. As a consequence of the Weil pairing, $\psi\phi = \omega$. Hence,

$$K_\mathfrak{l}(\Psi, \Phi) = K_\mathfrak{l}(\Psi, \mu_p) = K_\mathfrak{l}(\Phi, \mu_p). \tag{2.90}$$

Since $\mathfrak{l} \nmid p$, $K_\mathfrak{l}(\mu_p)/K_\mathfrak{l}$ is an unramified extension. Thus, $K_\mathfrak{l}(\Psi, \mu_p)/K_\mathfrak{l}$ is ramified if and only if $K_\mathfrak{l}(\Psi, \mu_p)/K_\mathfrak{l}(\mu_p)$ is ramified, which happens if and only if $\mathfrak{l} \in \mathrm{Ram}(\Psi/K)$.

Likewise, $K_\mathfrak{l}(\Phi, \mu_p)/K_\mathfrak{l}$ is ramified if and only if $\mathfrak{l} \in \mathrm{Ram}(\Phi/K)$. By (2.90), $\mathfrak{l} \in \mathrm{Ram}(\Psi/K)$ if and only if $\mathfrak{l} \in \mathrm{Ram}(\Phi/K)$. □

Lemma 2.19. *If $p \geq 5$ and E has additive, potentially good reduction at $\mathfrak{l} \nmid p$, then $\mathfrak{l} \in \mathrm{Ram}(\Psi/K) \cap \mathrm{Ram}(\Phi/K)$.*

Proof. For any integer $n \geq 3$ and relatively prime to l, E has good reduction over the field $K_\mathfrak{l}(E[n])$. Taking $n = p$, and noting that reduction type doesn't change in unramified extensions, we have that $K_\mathfrak{l}(E[p])/K_\mathfrak{l}$ is a ramified extension.

On the other hand, $K_\mathfrak{l}(E[n], E[p])/K_\mathfrak{l}(E[n])$ is an unramified extension for any choice of n subject to the above conditions, by the criterion of Néron-Ogg-Shafarevich (see [27]). Thus $e(K_\mathfrak{l}(E[p])/K_\mathfrak{l}) \mid [K_\mathfrak{l}(E[n]) : K_\mathfrak{l}]$. Taking $n = 4$ when $l = 3$ and $n = 3$ otherwise, and noting that $\#\mathrm{Aut}(E[3]) = 48$ and $\#\mathrm{Aut}(E[4]) = 96$, we have $e(K_\mathfrak{l}(E[p])/K_\mathfrak{l}) \mid 96$. Since $p \geq 5$, $p \nmid e(K_\mathfrak{l}(E[p])/K_\mathfrak{l})$.

Now $[K_\mathfrak{l}(E[p]) : K_\mathfrak{l}(\Psi, \Phi)]$ is either 1 or p, so $K_\mathfrak{l}(E[p])/K_\mathfrak{l}(\Psi, \Phi)$ is an unramified extension. It follows that $K_\mathfrak{l}(\Psi, \Phi)/K_\mathfrak{l}$ is ramified, so $\mathfrak{l} \in \mathrm{Ram}(\Psi/K) \cup \mathrm{Ram}(\Phi/K)$. Thus, by lemma 2.18, $\mathfrak{l} \in \mathrm{Ram}(\Psi/K) \cap \mathrm{Ram}(\Phi/K)$. □

Lemma 2.20. *If E has additive, potentially multiplicative reduction at $\mathfrak{l} \nmid p$, then $\mathfrak{l} \in \mathrm{Ram}(\Psi/K) \cap \mathrm{Ram}(\Psi/K)$.*

Proof. Since E has additive, potentially multiplicative reduction at $\mathfrak{l}$, E is isomorphic to a Tate curve over a ramified, quadratic extension of $K_\mathfrak{l}$. Let ε be the (ramified, quadratic) character corresponding to this extension. Thus, there is a short exact sequence

$$0 \longrightarrow \mu_p \otimes \varepsilon \longrightarrow E[p] \longrightarrow \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon \longrightarrow 0 \tag{2.91}$$

of $G_{K_\mathfrak{l}}$-modules. As $G_{K_\mathfrak{l}}$-modules $\Psi \cong \mu_p \otimes \varepsilon$ or $\Psi \cong \mathbf{Z}/p\mathbf{Z} \otimes \varepsilon$. Since ε is a ramified character we have $\mathfrak{l} \in \mathrm{Ram}(\Psi/K)$, whence by lemma 2.18, $\mathfrak{l} \in \mathrm{Ram}(\Phi/K)$ as well. □

Proposition 2.21. *Suppose E has additive reduction at $\mathfrak{l} \nmid p$. If E has potentially multiplicative reduction at $\mathfrak{l}$, or if $p \geq 5$ and E has potentially good reduction at $\mathfrak{l}$, then $H^1(K_\mathfrak{l}, \Psi)$ and $H^1(K_\mathfrak{l}, \Phi)$ are trivial.*

Proof. By lemmas 2.19 and 2.20, $\mathfrak{l} \in \mathrm{Ram}(\Psi/K) \cap \mathrm{Ram}(\Phi/K)$. Thus, $\Psi(K_\mathfrak{l})$ and $\Phi(K_\mathfrak{l})$ are trivial. By local duality, $H^2(K_\mathfrak{l}, \Psi) \cong \Phi(K_\mathfrak{l})^\vee$ and $H^2(K_\mathfrak{l}, \Phi) \cong \Psi(K_\mathfrak{l})^\vee$ are trivial.

$$\#H^1(K_\mathfrak{l}, \Psi) = \#\Psi(K_\mathfrak{l}) \cdot \#H^2(K_\mathfrak{l}, \Psi) \cdot \chi(K_\mathfrak{l}, \Psi) = 1 \tag{2.92}$$

$$\#H^1(K_\mathfrak{l}, \Phi) = \#\Phi(K_\mathfrak{l}) \cdot \#H^2(K_\mathfrak{l}, \Phi) \cdot \chi(K_\mathfrak{l}, \Phi) = 1 \tag{2.93}$$

Hence, $H^1(K_\mathfrak{l}, \Psi)$ and $H^1(K_\mathfrak{l}, \Phi)$ are trivial. □

2.7.2 Additive reduction above p

Suppose E has additive reduction at $\mathfrak{p} \mid p$. Then E has either potentially good, or potentially multiplicative reduction at $\mathfrak{p}$. If E has potentially good reduction at $\mathfrak{p}$, we assume that the reduction is potentially good, ordinary.

Lemma 2.22. *Suppose E has potentially multiplicative reduction at p. Then there is a quadratic extension of K in which E achieves multiplicative reduction at the place lying over $\mathfrak{p}$.*

Proof. Since E has additive, potentially multiplicative reduction at $\mathfrak{p}$, E is isomorphic to a Tate curve over a ramified, quadratic extension of $K_\mathfrak{p}$. We can choose a quadratic extension L/K such that E is isomorphic to a Tate curve over $LK_\mathfrak{p}$. Since reduction type doesn't change in unramified extensions, $\mathfrak{p}$ must be ramified in L/K. Thus, there is only one place $\mathfrak{P}$ of L lying over $\mathfrak{p}$. By construction, E is isomorphic to a Tate curve over $L_\mathfrak{P}$, so E has split, multiplicative reduction at $\mathfrak{P}$. □

Lemma 2.23. *Suppose $p \geq 5$, and suppose E has potentially good reduction at $\mathfrak{p}$. Then there is an extension of K of degree relatively prime to p in which E achieves good reduction at all places lying over $\mathfrak{p}$.*

Proof. By the criterion of Néron-Ogg-Shafarevich, E has good reduction at all of the places of $K(E[3])$ lying over $\mathfrak{p}$. Since $p \geq 5$ and $\#\operatorname{Aut}(E[3]) = 48$, p is relatively prime to the degree of $K(E[3])/K$. □

Suppose E has either potentially good, ordinary, or potentially multiplicative reduction at $\mathfrak{p}$ and L/K is an extension in which E achieves good, ordinary or multiplicative reduction. Let $\mathfrak{P}$ be a place of L lying over $\mathfrak{p}$. Then as before we can define a $G_{L_\mathfrak{P}}$-invariant subgroup $\hat{E}[p^\infty] \subseteq E[p^\infty]$. This subgroup is actually invariant under the action of $G_{K_\mathfrak{p}}$, so we can consider a short, exact sequence

$$0 \longrightarrow \hat{E}[p^\infty] \longrightarrow E[p^\infty] \longrightarrow \tilde{E}[p^\infty] \longrightarrow 0 \tag{2.94}$$

as before. We make the following definitions.

Definition. If E has potentially multiplicative reduction at $\mathfrak{p} \mid p$, set

- $\mathcal{L}_\mathfrak{p}^{\pm}(\Psi) = H^1(K_\mathfrak{p}, \Psi)$ and $\mathcal{L}_\mathfrak{p}^{+}(\Phi) = 0$ if $\Psi = \hat{E}[p]$;
- $\mathcal{L}_\mathfrak{p}^{\pm}(\Psi) = 0$ and $\mathcal{L}_\mathfrak{p}^{+}(\Phi) = H^1(K_\mathfrak{p}, \Phi)$ if $\Psi \neq \hat{E}[p]$.

If E has potentially good, ordinary reduction at $\mathfrak{p} \mid p$, set

- $\mathcal{L}_\mathfrak{p}^{\pm}(\Psi) = H^1_{pr}(K_\mathfrak{p}, \Psi)$ and $\mathcal{L}_\mathfrak{p}^{+}(\Phi) = H^1_{nr}(K_\mathfrak{p}, \Phi)$ if $\Psi = \hat{E}[p]$;
- $\mathcal{L}_\mathfrak{p}^{\pm}(\Psi) = H^1_{nr}(K_\mathfrak{p}, \Psi)$ and $\mathcal{L}_\mathfrak{p}^{+}(\Phi) = H^1_{pr}(K_\mathfrak{p}, \Phi)$ if $\Psi \neq \hat{E}[p]$.

Proposition 2.24. *If E has either potentially multiplicative reduction at $\mathfrak{p} \mid p$ or if E has potentially good, ordinary reduction at $\mathfrak{p} \mid p$ and achieves good reduction in an extension of degree relatively prime to p, then $\mathcal{L}_\mathfrak{p}(\Psi) = \mathcal{L}_\mathfrak{p}^{\pm}(\Psi)$ and $\mathcal{L}_\Phi \subseteq \mathcal{L}_\Phi^{+}$.*

Proof. Let L/K be an extension of degree relatively prime to p in which E achieves either good, ordinary or multiplicative reduction, and let $\mathfrak{P}$ be a place of L lying over $\mathfrak{p}$. Let $\rho : H^1(K_\mathfrak{p}, E[p^\infty]) \longrightarrow H^1(L_\mathfrak{P}, E[p^\infty])$ be the restriction map. By lemma 4.2 of [4],

$$\operatorname{im}(\kappa_\mathfrak{p}) = (\rho^{-1}(\operatorname{im}(\kappa_\mathfrak{P})))_{div}. \tag{2.95}$$

Since $[L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ and p are relatively prime, ρ is injective. Thus

$$\mathrm{im}(\kappa_{\mathfrak{p}}) = \rho^{-1}(\mathrm{im}(\kappa_{\mathfrak{P}})). \tag{2.96}$$

Consider the commutative diagram

$$\begin{array}{ccc} H^1(K,\Psi) & \xrightarrow{f_K} & H^1(K_{\mathfrak{p}}, E[p^\infty])/\mathrm{im}(\kappa_{\mathfrak{p}}) \\ \downarrow & & \tilde{\rho}\downarrow \\ H^1(L,\Psi) & \xrightarrow{f_L} & H^1(L_{\mathfrak{P}}, E[p^\infty])/\mathrm{im}(\kappa_{\mathfrak{P}}). \end{array} \tag{2.97}$$

By definition, $\mathcal{L}_{\mathfrak{p}}(\Psi) = \ker(f_K)$. Equation (2.96) implies $\tilde{\rho}$ is injective. Thus, $\mathcal{L}_{\mathfrak{p}}(\Psi) = \rho_{\Psi}^{-1}(\ker(f_L)) = \rho_{\Psi}^{-1}(\mathcal{L}_{\mathfrak{P}}(\Psi))$.

Let $\rho_\Psi : H^1(K_{\mathfrak{p}}, \Psi) \longrightarrow H^1(L_{\mathfrak{P}}, \Psi)$ be the restriction map. Since $[L : K]$ and p are relatively prime, $\rho_{\Psi}^{-1}(\mathcal{L}_{\mathfrak{P}}^{\pm}(\Psi)) = \mathcal{L}_{\mathfrak{p}}^{\pm}(\Psi)$. By propositions 2.8 and 2.15, $\mathcal{L}_{\mathfrak{P}}(\Psi) = \mathcal{L}_{\mathfrak{P}}^{\pm}(\Psi)$. Thus, $\mathcal{L}_{\mathfrak{p}}(\Psi) = \mathcal{L}_{\mathfrak{p}}^{\pm}(\Psi)$.

Elements of $S_{E[p]}$ satisfy the Selmer condition at $\mathfrak{p}$, so

$$\begin{aligned} S_{E[p]} &\subseteq \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(K_{\mathfrak{p}}, E[p^\infty])/\mathrm{im}(\kappa_{\mathfrak{p}})\right) \\ &= \ker\left(H^1(K_\Sigma/K, E[p]) \longrightarrow H^1(L_{\mathfrak{P}}, E[p^\infty])/\mathrm{im}(\kappa_{\mathfrak{P}})\right). \end{aligned} \tag{2.98}$$

Thus, $\mathrm{im}\left(S_{E[p]} \longrightarrow H^1(L_{\mathfrak{P}}, \Psi)\right) \subseteq \mathcal{L}_{\mathfrak{P}}^{+}(\Phi)$. If $\rho_\Phi : H^1(K_{\mathfrak{p}}, \Phi) \longrightarrow H^1(L_{\mathfrak{P}}, \Phi)$ is the restriction map, then $\rho_{\Phi}^{-1}(\mathcal{L}_{\mathfrak{P}}^{+}(\Phi)) = \mathcal{L}_{\mathfrak{p}}^{+}(\Phi)$, so

$$\begin{aligned} \mathcal{L}_{\mathfrak{p}}(\Phi) &= \mathrm{im}\left(S_{E[p]} \longrightarrow H^1(K_{\mathfrak{p}}, \Phi)\right) \\ &\subseteq \mathcal{L}_{\mathfrak{p}}^{+}(\Phi). \end{aligned} \tag{2.99}$$

□

Chapter 3

EXAMPLES

3.1 Introduction

In this section we compute bounds for the p-ranks of Selmer groups for elliptic curves in families of quadratic twists which satisfy the hypotheses of theorems 2.3 and 2.16. The data used in these calculations are taken from J. E. Cremona's tables [6].

3.2 Twists of 11A1 - 3

Let E_1, E_2 and E_3 be the elliptic curves 11A1, 11A2 and 11A3 respectively, given by the following equations.

$$E_1 \ : \ y^2 + y = x^3 - x^2 - 10x - 20 \tag{3.1}$$

$$E_2 \ : \ y^2 + y = x^3 - x^2 - 7\,820x - 263\,580 \tag{3.2}$$

$$E_3 \ : \ y^2 + y = x^3 - x^2 \tag{3.3}$$

These curves are related via rational isogenies of degree 5 as follows.

$$E_2 \rightleftarrows E_1 \rightleftarrows E_3 \tag{3.4}$$

Since $E_1(\mathbf{Q})_{tors} = \mathbf{Z}/5\mathbf{Z} = E_3(\mathbf{Q})_{tors}$, the kernels of the isogenies $E_3 \longrightarrow E_1$ and $E_1 \longrightarrow E_2$ are isomorphic to $\mathbf{Z}/5\mathbf{Z}$ as $G_{\mathbf{Q}}$-modules. As a consequence of the Weil pairing, the kernels of the isogenies $E_2 \longrightarrow E_1$ and $E_1 \longrightarrow E_3$ are isomorphic to μ_5 as $G_{\mathbf{Q}}$-modules. Thus

$$E_1[5] \cong \mu_5 \otimes \mathbf{Z}/5\mathbf{Z}, \tag{3.5}$$

and we have the following short exact sequences.

$$0 \longrightarrow \mu_5 \longrightarrow E_2[5] \longrightarrow \mathbf{Z}/5\mathbf{Z} \longrightarrow 0 \tag{3.6}$$

$$0 \longrightarrow \mathbf{Z}/5\mathbf{Z} \longrightarrow E_3[5] \longrightarrow \mu_5 \longrightarrow 0 \tag{3.7}$$

Since the conductor of E_1, E_2 and E_3 is 11, these curves have good reduction at all primes except 11, and multiplicative reduction at 11. If, for $l \neq 11$, we let $\tilde{E}_i$ denote the reduction of E_i modulo l and set $a_l = 1 + l - \#\tilde{E}_i(\mathbf{F}_l)$, then $a_5 = 1$. (Note that a_l does not depend on the choice of $i = 1, 2$, or 3.) In particular, $5 \nmid a_5$, so the curves E_i have good, ordinary reduction at 5. Since the $G_{\mathbf{Q}_5}$-action on $\tilde{E}[5]$ is unramified, the kernels of the isogenies $E_2 \longrightarrow E_1$ and $E_1 \longrightarrow E_3$ are contained in the kernel of reduction modulo 5, but the kernels of the isogenies $E_3 \longrightarrow E_1$ and $E_1 \longrightarrow E_2$ are not.

Since each E_i has multiplicative reduction at 11, each is isomorphic to a Tate curve over a quadratic extension of $\mathbf{Q}_{11}$. (In fact, the curves have split multiplicative reduction at 11, so each is isomorphic to a Tate curve over $\mathbf{Q}_{11}$ itself.) Let q_i denote the Tate period for E_i, so $\bar{\mathbf{Q}}_{11}^{\times}/\langle q_i \rangle \cong E_i(\bar{\mathbf{Q}}_{11})$. Since $\mathbf{Z}/5\mathbf{Z} \cong \mu_5$ as $G_{\mathbf{Q}_{11}}$-modules, it is, *a priori*, possible for any of the kernels of the various isogenies to correspond to μ_5 under the Tate isomorphism. If j_i denotes the j-invariant of E_i, then $v_{11}(q_i) = -v_{11}(j_i)$.

$$v_{11}(q_1) = 5, \tag{3.8}$$

$$v_{11}(q_2) = 1, \tag{3.9}$$

$$v_{11}(q_3) = 1. \tag{3.10}$$

For $i = 2$ or 3, $\sqrt[5]{q_i} \notin \mathbf{Q}_{11}$. Since $G_{\mathbf{Q}_{11}}$ acts trivially on the kernels of the isogenies $E_i \longrightarrow E_1$, these kernels must correspond to subgroups of $\mu_5 \times \langle \sqrt[5]{q_i} \rangle / \langle q_i \rangle$ on which $G_{\mathbf{Q}_{11}}$ acts trivially. The only possibility is for these kernels to correspond to μ_5. On the other hand, the following lemma shows that the kernels of the isogenies $E_1 \longrightarrow E_i$ for $i = 2$ or 3 do not correspond to μ_5 under the Tate parametrization.

Lemma 3.1. *Let K be a local field, and let E and E' be Tate curves defined over K, with Tate periods q and q', respectively. Suppose there is a K-rational isogeny $E \longrightarrow E'$ of degree p, and suppose the kernel of this isogeny corresponds to μ_p under the Tate parametrization $\bar{K}^\times/\langle q\rangle \xrightarrow{\sim} E(\bar{K})$. Then $v_K(q') = p \cdot v_K(q)$.*

Proof. Consider the G_K-invariant map $\bar{K}_l^\times/\langle q\rangle \longrightarrow \bar{K}_l^\times/\langle q^p\rangle$ induced by raising elements of $\bar{K}_l^\times$ to the p^{th} power. This map is surjective, with kernel μ_p. On the other hand, the composition $\bar{K}^\times/\langle q\rangle \xrightarrow{\sim} E(\bar{K}) \longrightarrow E'(\bar{K}) \xrightarrow{\sim} \bar{K}_l^\times/\langle q'\rangle$ is also G_K-invariant, with kernel μ_p, so $\bar{K}^\times/\langle q^p\rangle \cong \bar{K}^\times/\langle q'\rangle$ as G_K-modules. In particular, $K^\times/\langle q^p\rangle \cong K^\times/\langle q'\rangle$.

Notice that this isomorphism restricts to an isomorphism between $\mathcal{O}_K^\times \subseteq K^\times/\langle q^p\rangle$ and $\mathcal{O}_K^\times \subseteq K^\times/\langle q'\rangle$. Hence,

$$\mathbf{Z}/v_K(q^p)\mathbf{Z} \cong \left(K^\times/\langle q^p\rangle\right)/\mathcal{O}_K^\times \cong \left(K^\times/\langle q'\rangle\right)/\mathcal{O}_K^\times \cong \mathbf{Z}/v_K(q')\mathbf{Z}, \tag{3.11}$$

and $v_K(q') = v_K(q^p) = p \cdot v_K(q)$. □

Let $d \neq 1$ be a square-free integer, and let $E_i^{(d)}$ denote the quadratic twist by d of E_i, for $i = 1, 2$, or 3. Let $F = \mathbf{Q}(\sqrt{d})$, let D be the discriminant of F (so $D = d$ or $4d$), and let ε_d be the quadratic character which gives the action of $G_\mathbf{Q}$ on $\sqrt{d}$. Let $\Psi = \mathbf{Z}/5\mathbf{Z} \otimes \varepsilon_d$ and $\Phi = \mu_5 \otimes \varepsilon_d$. Then from (3.5),

$$E_1^{(d)}[5] \cong \Phi \times \Psi \tag{3.12}$$

and from (3.6) and (3.7) we have short exact sequences

$$0 \longrightarrow \Phi \longrightarrow E_2^{(d)}[5] \longrightarrow \Psi \longrightarrow 0 \tag{3.13}$$

$$0 \longrightarrow \Psi \longrightarrow E_3^{(d)}[5] \longrightarrow \Phi \longrightarrow 0 \tag{3.14}$$

The curves $E_i^{(d)}$ have additive reduction at all l dividing D. If $11 \nmid D$, $E_i^{(d)}$ has multiplicative reduction at 11. In this case, $\Phi \subseteq E_2^{(d)}$ and $\Psi \subseteq E_3^{(d)}$ correspond to μ_5 under the Tate parametrization for E_i over $\mathbf{Q}_{11}(\sqrt{d})$, but $\Psi, \Phi \subseteq E_1^{(d)}$ do not. If $5 \nmid D$,

$E_i^{(d)}$ has good, ordinary reduction at 5; otherwise $E_i^{(d)}$ has potentially good, ordinary reduction at 5. In either case, $\Phi \subseteq E_1^{(d)}[5]$ and $\Phi \subseteq E_2^{(d)}[5]$ are in the respective kernels of reduction modulo 5, whereas $\Psi \subseteq E_1^{(d)}$ and $\Psi \subseteq E_3^{(d)}[5]$ are not.

For each d and each i, $E_i^{(d)}$ satisfies the hypotheses of theorems 2.3 and 2.16, so we can now compute bounds for $\#\,\mathrm{Sel}_{E_i^{(d)}}(\mathbf{Q})$. Throughout this section, take $\Sigma = \{5, 11, \infty\} \cup \{l : l|D\}$, the smallest set containing $5, \infty$, and all primes of bad reduction for $E_i^{(d)}$. Note that since $d \neq 1$, $\Psi(\mathbf{Q})$ and $\Phi(\mathbf{Q})$ are trivial.

3.2.1 Twists of 11A3

First, consider the curve $E = E_3^{(d)}$, whose 5-torsion points fit into the short exact sequence (3.14). Since $F = \mathbf{Q}(\Psi)$, the lower bound for $\#\,\mathrm{Sel}_E(\mathbf{Q})[5]$ comes from the maximal abelian extension F' of F which is unramified outside Σ, which satisfies certain conditions for the primes in Σ, such that $G_{F'/F}$ has exponent 5 and $G_{F/\mathbf{Q}}$ acts as -1 on $G_{F'/F}$.

For $l \in \Sigma$, $l \nmid 5 \cdot 11$, the local cohomology groups $H^1(\mathbf{Q}_l, \Psi)$ vanish, so there is no need to impose any condition on the behavior in F'/F of the primes of F lying over l; these primes will automatically split completely in F'/F. Since, viewing E as a Tate curve over $\mathbf{Q}(\sqrt{d})$, Ψ corresponds to μ_p under the Tate parametrization, we place no restriction on the behavior in F'/F of primes of F lying over 11. Since Ψ is not in the kernel of reduction modulo 5, we insist that the primes of F lying over 5 must be unramified in F'/F.

Thus, F'/F is the maximal, abelian extension of F which is unramified outside $\{11\}$, such that $G_{F'/F}$ has exponent 5, and such that $G_{F/\mathbf{Q}}$ acts as -1 on $G_{F'/F}$. If $\mathrm{Cl}_F^{\{11\}}$ denotes the ray class group of conductor 11 for F, then $G_{F'/F} \cong \left(\mathrm{Cl}_F^{\{11\}}/5\mathrm{Cl}_F^{\{11\}}\right)^{(-)}$, and

$$\#\left(\frac{\mathrm{Cl}_F^{\{11\}}}{5\mathrm{Cl}_F^{\{11\}}}\right)^{(-)} \leq \#\,\mathrm{Sel}_E(\mathbf{Q})[5]. \tag{3.15}$$

If $\left(\frac{d}{11}\right) = -1$ or 0, then $\left(\mathrm{Cl}_F^{\{11\}}/5\mathrm{Cl}_F^{\{11\}}\right)^{(-)} \cong (\mathrm{Cl}_F/5\mathrm{Cl}_F)$. If $\left(\frac{d}{11}\right) = +1$, then $\left(\mathrm{Cl}_F^{\{11\}}/5\mathrm{Cl}_F^{\{11\}}\right)^{(-)} = (\mathrm{Cl}_F/5\mathrm{Cl}_F)$ or $(\mathrm{Cl}_F/5\mathrm{Cl}_F) \times (\mathbf{Z}/5\mathbf{Z})$, and the exact answer, which depends on d, can be easily determined computationally in each case. Thus,

$$5^{\eta_3} \cdot \# \left(\frac{\mathrm{Cl}_F}{5\mathrm{Cl}_F}\right) \leq \# \mathrm{Sel}_E(\mathbf{Q})[5], \tag{3.16}$$

where $\eta_3 = 0$ or 1, and can easily be computed.

Because the local cohomology groups $H^1(\mathbf{Q}_l, \Psi)$ vanish for all primes $l \neq 5$ at which E has additive reduction, the contribution from $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi)$ to the upper bound for $\# \mathrm{Sel}_E(\mathbf{Q})[5]$ is the same as the contribution to the lower bound, computed above. Thus, all that remains to compute the upper bound is to analyze the contribution from $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)$. We will analyze this contribution in terms of the Kummer theory of F, rather than the class field theory of $\mathbf{Q}(\Phi)$.

Inflation-restrction gives us an exact sequence

$$\begin{aligned} 0 \longrightarrow\ & H^1(F/\mathbf{Q}, \Phi(F)) \xrightarrow{infl} H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi) \xrightarrow{res} H^1(\mathbf{Q}_\Sigma/F, \Phi)^{G_{F/\mathbf{Q}}} \\ & \longrightarrow H^2(F/\mathbf{Q}, \Phi(F)). \end{aligned} \tag{3.17}$$

Since $\#G_{F/\mathbf{Q}} = 2$ and $\#\Phi = 5$, $H^1(F/\mathbf{Q}, \Phi(F))$ and $H^2(F/\mathbf{Q}, \Phi(F))$ are trivial, and *res* is an isomorphism. Since $\Phi \cong \mu_5$ as G_F-modules,

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi) \cong H^1(\mathbf{Q}_\Sigma/F, \Phi)^{G_{F/\mathbf{Q}}} \cong H^1(\mathbf{Q}_\Sigma/F, \mu_5)^{(-)} \subseteq \left(F^\times/(F^\times)^5\right)^{(-)} \tag{3.18}$$

Since 5 is odd, each element of $(F^\times/(F^\times)^5)^{(-)}$ has a representative $\alpha \in F^\times$ satisfying $N_{F/\mathbf{Q}}(\alpha) = 1$. Such an α represents an element of $H^1(\mathbf{Q}_\Sigma/F, \mu_5)^{(-)}$ if and only if $v_\mathfrak{l}(\alpha) \equiv 0 \pmod 5$ for all primes $\mathfrak{l}$ lying over $l \notin \Sigma$. The groups $H^1(\mathbf{Q}_l, \Phi)$ vanish for all $l \neq 5$ at which E has additive reduction, so $N_{F/\mathbf{Q}}(\alpha) = 1$ implies that $v_\mathfrak{l}(\alpha) \equiv 0 \pmod 5$ for all $\mathfrak{l}$ lying over $l \neq 5$ at which E has additive reduction.

Since Ψ corresponds to μ_5 under the Tate parametrization, and Ψ is not in the kernel of reduction modulo 5, α will contribute to the upper bound if and only if α corresponds to a trivial cocycle in $H^1(\mathbf{Q}_{11}, \Phi)$ and to a *peu ramifiée* cocycle in

$H^1(\mathbf{Q}_5, \Phi)$. The latter is equivalent to $v_{\mathfrak{p}}(\alpha) \equiv 0 \pmod 5$ for $\mathfrak{p} \mid 5$. The former is equivalent to $\alpha \in (F_{\mathfrak{l}}^{\times})^5$ for $\mathfrak{l} \mid 11$.

If $\left(\frac{d}{11}\right) = -1$ or 0, then $H^1(\mathbf{Q}_{11}, \Phi)$ is trivial, and $\alpha \in (F_{\mathfrak{l}}^{\times})^5$ is automatically satisfied for $\mathfrak{l} \mid 11$. In this case, α contributes to the upper bound if and only if $v_{\mathfrak{l}}(\alpha) \equiv 0 \pmod 5$ for all primes $\mathfrak{l}$ of F. Such an α can arise in two ways; either $\alpha \in \mathcal{O}_F^{\times}$, of norm 1, or the fractional ideal $(\alpha) = I^5$, where I is a fractional ideal representing an ideal class in $\mathrm{Cl}_F[5]$ such that $\sigma(I) = I^{-1}$, where σ is the non-trivial element of $G_{F/\mathbf{Q}}$. Thus, for $\left(\frac{d}{11}\right) = -1$ or 0 the upper bound is given by

$$\begin{aligned} \#\,\mathrm{Sel}_E(\mathbf{Q})[5] &\leq \#\mathrm{Cl}_F[5] \cdot \# \left(\frac{\mathrm{Cl}_F}{5\mathrm{Cl}_F} \right) \cdot \# \left(\frac{\mathcal{O}_F^{\times}}{(\mathcal{O}_F^{\times})^5} \right) \\ &= (\#\mathrm{Cl}_F[5])^2 \cdot \# \left(\frac{\mathcal{O}_F^{\times}}{(\mathcal{O}_F^{\times})^5} \right). \end{aligned} \tag{3.19}$$

If $\left(\frac{d}{11}\right) = +1$, then $H^1(\mathbf{Q}_{11}, \Phi) \cong (\mathbf{Z}/5\mathbf{Z})^2$. Cocycles in $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)$ represented by $\alpha \in F^{\times}$ of norm 1 arising as in the previous case will satisfy the Selmer condition at all $l \neq 11$, but in general, their image in $H^1(\mathbf{Q}_{11}, \Phi)$ need only be in $H^1_{nr}(\mathbf{Q}_{11}, \Phi)$. To analyze how often these cocycles will satisfy the Selmer condition at the prime 11, consider the following maps.

$$\pi_1 \;:\; H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi) \longrightarrow H^1(\mathbf{Q}_5, \Psi) \times H^1(\mathbf{Q}_{11}, \Psi) \tag{3.20}$$

$$\pi_2 \;:\; H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi) \longrightarrow H^1(\mathbf{Q}_5, \Phi) \times H^1(\mathbf{Q}_{11}, \Phi) \tag{3.21}$$

If we let $\langle -, - \rangle_5$ and $\langle -, - \rangle_{11}$ be the pairings described in section 1.3, then lemma 1.5 implies $\mathrm{im}(\pi_1)$ and $\mathrm{im}(\pi_2)$ are orthogonal complements under the pairing $\langle -, - \rangle := \langle -, - \rangle_5 + \langle -, - \rangle_{11}$. Likewise, $H^1_{nr}(\mathbf{Q}_5, \Psi)$ and $H^1_{pr}(\mathbf{Q}_5, \Phi)$ are orthogonal complements under $\langle -, - \rangle_5$, and $H^1_{nr}(\mathbf{Q}_{11}, \Psi)$ and $H^1_{nr}(\mathbf{Q}_{11}, \Phi)$ are orthogonal complements under $\langle -, - \rangle_{11}$.

Let $A = \mathrm{im}(\pi_1) \cap (H^1_{nr}(\mathbf{Q}_5, \Psi) \times H^1(\mathbf{Q}_{11}, \Psi))$, and let B be the image of $\mathrm{im}(\pi_2)$ under the map

$$H^1(\mathbf{Q}_5, \Phi) \times H^1(\mathbf{Q}_{11}, \Phi) \longrightarrow \left(\frac{H^1(\mathbf{Q}_5, \Phi)}{H^1_{pr}(\mathbf{Q}_5, \Phi)} \right) \times H^1(\mathbf{Q}_{11}, \Phi). \tag{3.22}$$

Let A' be the image of A under the projection

$$H^1_{nr}(\mathbf{Q}_5, \Psi) \times H^1(\mathbf{Q}_{11}, \Psi) \longrightarrow H^1(\mathbf{Q}_{11}, \Psi), \tag{3.23}$$

and let $B' = B \cap (\{0\} \times H^1(\mathbf{Q}_{11}, \Phi))$, viewed as a subset of $H^1(\mathbf{Q}_{11}, \Phi)$. Then A' and B' are orthogonal complements under $\langle -, - \rangle_{11}$, so $A' \subseteq H^1_{nr}(\mathbf{Q}_{11}, \Psi)$ if and only if $H^1_{nr}(\mathbf{Q}_{11}, \Phi) \subseteq B'$.

The quantity η_3 from (3.16) is nonzero if and only if $A' \not\subseteq H^1_{nr}(\mathbf{Q}_{11}, \Psi)$. In this case $H^1_{nr}(\mathbf{Q}_{11}, \Phi) \not\subseteq B'$, so the cocycle represented by α will always satisfy the Selmer condition at 11, and the upper bound is given by

$$\begin{aligned} \#\,\mathrm{Sel}_E(\mathbf{Q})[5] &\leq 5 \cdot \#\mathrm{Cl}_F[5] \cdot \# \left(\frac{\mathrm{Cl}_F}{5\mathrm{Cl}_F} \right) \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right) \\ &= 5 \cdot (\#\mathrm{Cl}_F[5])^2 \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right). \end{aligned} \tag{3.24}$$

Conversely, $\eta_3 = 0$ if and only if $A' \subseteq H^1_{nr}(\mathbf{Q}_{11}, \Psi)$, in which case $H^1_{nr}(\mathbf{Q}_{11}, \Phi) \subseteq B'$ and some cocycles represented by α will not satisfy the Selmer condition at 11. Since $H^1_{nr}(\mathbf{Q}_{11}, \Phi) \cong \mathbf{Z}/5\mathbf{Z}$, the subspace of $F^\times/(F^\times)^5$ representing cocycles which satisfy the Selmer conditons at all primes l will have one dimension less than the subspace given by all possible choices of α. Hence, in this case

$$\begin{aligned} \#\,\mathrm{Sel}_E(\mathbf{Q})[5] &\leq 5^{-1} \cdot \#\mathrm{Cl}_F[5] \cdot \# \left(\frac{\mathrm{Cl}_F}{5\mathrm{Cl}_F} \right) \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right) \\ &= 5^{-1} \cdot (\#\mathrm{Cl}_F[5])^2 \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right). \end{aligned} \tag{3.25}$$

Note that $A' \subseteq H^1_{nr}(\mathbf{Q}_{11}, \Psi)$ if and only if $\#\mathrm{Cl}_F[5] = \# \left(\left(\mathrm{Cl}_F^{\{11\}}/5\mathrm{Cl}_F^{\{11\}} \right)^{(-)} \right)$; thus, we have proved the following.

Theorem 3.2. *Let $d \neq 1$ be a square-free integer, and let E be the quadratic twist by d of the elliptic curve 11A3. Let $\eta_0 = 0$ if $d < 0$, and $\eta_0 = 1$ if $d > 1$. If $\left(\frac{d}{11}\right) = -1$ or 0, then*

$$\#\mathrm{Cl}_F[5] \leq \#\,\mathrm{Sel}_E(\mathbf{Q})[5] \leq 5^{\eta_0} \cdot (\#\mathrm{Cl}_F[5])^2. \tag{3.26}$$

If $\left(\frac{d}{11}\right) = +1$, *then let* $\eta_3 = 0$ *if* $\#\mathrm{Cl}_F[5] = \#\left(\left(\mathrm{Cl}_F^{\{11\}}/5\mathrm{Cl}_F^{\{11\}}\right)^{(-)}\right)$, *and* $\eta_3 = 1$ *otherwise. Then*

$$5^{\eta_3} \cdot \#\mathrm{Cl}_F[5] \leq \#\,\mathrm{Sel}_E(\mathbf{Q})[5] \leq 5^{\eta_0-(-1)^{\eta_3}} \cdot (\#\mathrm{Cl}_F[5])^2\,. \tag{3.27}$$

3.2.2 Twists of 11A2

In this section, let $E = E_2^{(d)}$, the quadratic twist by d of 11A2. As in the previous case of twists of 11A3, the local cohomology groups $H^1(\mathbf{Q}_l, \Psi)$ and $H^1(\mathbf{Q}_l, \Phi)$ vanish for all $l \neq 5$ dividing D. Since $\Phi \subseteq E[5]$ is in the kernel of reduction modulo 5, and corresponds to μ_5 under the Tate parametrization over $\mathbf{Q}_11$, the subgroup of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi)$ which satisfies the Selmer conditions at all primes l can be viewed as the $G_{F'/F}$, where F' is the maximal abelian extension of F which is everywhere unramified, in which the primes of F lying over 11 split completely, and such that $G_{F/\mathbf{Q}}$ acts as -1 on $G_{F'/F}$. If $\mathfrak{l}_{11}$ is a prime of F lying over 11, and if $\mathrm{cl}(\mathfrak{l}_{11})$ denotes its class in Cl_F, then the contribution from $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi)$ to the upper bound for $\dim_{\mathbf{F}_5}(\mathrm{Sel}_E(\mathbf{Q})[5])$ is $\dim_{\mathbf{F}_5}(\mathrm{Cl}_F/\langle \mathrm{cl}(\mathfrak{l}_{11}), 5\mathrm{Cl}_F\rangle)$.

As before, it is easiest to analyze the elements of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)$ which satisfy the Selmer conditions at all primes l in terms of the Kummer theory of F, elements of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)$ can be represented by $\alpha \in F^\times$ such that $N_{F/\mathbf{Q}}(\alpha) = 1$ and $v_\mathfrak{l}(\alpha) \equiv 0 \pmod 5$ for $\mathfrak{l}$ lying over primes not in Σ. Once again, this condition is automatically satisfied for $\mathfrak{l}$ lying over $l \mid D$ not equal to 5. The cocycle represented by α satisfies the Selmer condition at 5 if and only if $v_\mathfrak{p}(\alpha) \equiv 0 \pmod 5$ for $\mathfrak{p}$ lying over 5. This cocycle automatically satisfies the Selmer condition at 11. (In the notation of the previous chapter, $\mathcal{L}_{11}(\Phi) = H^1(\mathbf{Q}_{11}, \Phi)$, so the Selmer condition at 11 is vacuous.)

If $\left(\frac{d}{11}\right) = -1$ or 0, then either $\alpha \in \mathcal{O}_F^\times$, or the fractional ideal $(\alpha) = I^5$ for some fractional ideal I such that $\sigma(I) = I^{-1}$. Note that for such d, $\mathrm{cl}(\mathfrak{l}_{11}) \in 5\mathrm{Cl}_F$

automatically. In this case we have

$$\#\mathrm{Cl}_F[5] \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right) \leq \# \mathrm{Sel}_E(\mathbf{Q})[5] \leq 2 \left(\#\mathrm{Cl}_F[5]\right)^2 \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right). \tag{3.28}$$

For $\left(\frac{d}{11}\right) = +1$, it is possible that $\mathrm{cl}(\mathfrak{l}_{11}) \notin 5\mathrm{Cl}_F$. If A' and B' are defined as in the previous section, $\mathrm{cl}(\mathfrak{l}_{11}) \notin 5\mathrm{Cl}_F$ if and only if $H^1_{nr}(\mathbf{Q}_{11}, \Psi) \subseteq A'$, whence $B' \subseteq H^1_{nr}(\mathbf{Q}_{11}, \Phi)$. Thus, if $\mathrm{cl}(\mathfrak{l}_{11}) \notin 5\mathrm{Cl}_F$, then $v_{\mathfrak{l}}(\alpha) \equiv 0 \pmod 5$ for all $\mathfrak{l}$ not lying over 11 forces $v_{\mathfrak{l}_{11}}(\alpha) \equiv 0 \pmod 5$ as well, and the α described above represent all of the elements of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)$ which satisfy all of the Selmer conditions. In this case,

$$\#\mathrm{Cl}_F[5] \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right) \leq \# \mathrm{Sel}_E(\mathbf{Q})[5] \leq 5^{-1} \cdot \left(\#\mathrm{Cl}_F[5]\right)^2 \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right). \tag{3.29}$$

Conversely, if $\left(\frac{d}{11}\right) = +1$ and $\mathrm{cl}(\mathfrak{l}_{11}) \in \mathrm{Cl}_F$, then there are $\alpha \in F^\times$ with $N_{F/\mathbf{Q}}(\alpha) = 1$ such that $v_{\mathfrak{l}_{11}}(\alpha) \not\equiv 0 \pmod 5$ but $v_{\mathfrak{l}}(\alpha) \equiv 0 \pmod 5$ for all $\mathfrak{l}$ not lying over 11. Since $H^1(\mathbf{Q}_{11}, \Phi)/H^1_{nr}(\mathbf{Q}_{11}, \Phi) \cong \mathbf{Z}/5\mathbf{Z}$, the subgroup of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)$ of elements which satisfy the Selmer condition at all primes has order

$$5 \cdot \#\mathrm{Cl}_F[5] \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right), \tag{3.30}$$

and

$$5 \cdot \#\mathrm{Cl}_F[5] \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right) \leq \# \mathrm{Sel}_E(\mathbf{Q})[5] \leq 5 \cdot \left(\#\mathrm{Cl}_F[5]\right)^2 \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right). \tag{3.31}$$

Combining these statements, we have the following.

Theorem 3.3. *Let $d \neq 1$ be a square-free integer, and let E be the quadratic twist by d of the elliptic curve 11A2. Let $\eta_0 = 0$ if $d < 0$, and $\eta_0 = 1$ if $d > 1$. If $\left(\frac{d}{11}\right) = -1$ or 0, then*

$$5^{\eta_0} \cdot \#\mathrm{Cl}_F[5] \leq \# \mathrm{Sel}_E(\mathbf{Q})[5] \leq 5^{\eta_0} \cdot \left(\#\mathrm{Cl}_F[5]\right)^2. \tag{3.32}$$

If $\left(\frac{d}{11}\right) = +1$, then let $\eta_2 = 1$ if the class of one of the prime ideals of F lying over 11 is in $5\mathrm{Cl}_F$ and $\eta_2 = 0$ otherwise. Then

$$5^{\eta_0+\eta_2} \cdot \#\mathrm{Cl}_F[5] \leq \# \mathrm{Sel}_E(\mathbf{Q})[5] \leq 5^{\eta_0-(-1)^{\eta_2}} \cdot \left(\#\mathrm{Cl}_F[5]\right)^2. \tag{3.33}$$

3.2.3 Twists of 11A1

In this section, let $E = E_1^{(d)}$, the quadratic twist by d of 11A1. As in the previous sections, the local cohomology groups $H^1(\mathbf{Q}_l, \Psi)$ and $H^1(\mathbf{Q}_l, \Phi)$ vanish for all $l \neq 5$ dividing D. Since E admits two rational isogenies of degree 5, we can choose which isogeny to use when computing the bounds on $\#\,\mathrm{Sel}_E(\mathbf{Q})[5]$. We will choose the isogeny whose kernel is Ψ. Since $E[5] \cong \Psi \times \Phi$,

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, E[5]) \cong H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi) \times H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi), \tag{3.34}$$

and we can hope to compute the $\#\,\mathrm{Sel}_E(\mathbf{Q})[5]$ exactly. To do this, we must compute

$$\#S_\Psi = \#\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi) \cap \mathrm{Sel}_E(\mathbf{Q})[5]\right) \tag{3.35}$$

and

$$\#S_\Phi = \#\left(\mathrm{im}\left(\mathrm{Sel}_E(\mathbf{Q})[5] \longrightarrow H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)\right)\right). \tag{3.36}$$

Since $\Psi \subseteq E[5]$ is not in the kernel of reduction modulo 5, and doesn't correspond to μ_5 under the Tate parametrization over $\mathbf{Q}_{11}$, $L_\Psi^\pm$ is the maximal, abelian extension of F which is everywhere unramified, in which the primes of F lying over 11 split completely, and such that $G_{F/\mathbf{Q}}$ acts as -1 on $G_{L_\Psi^\pm/F}$. If $\mathfrak{l}_{11}$ is a prime of F lying over 11, and if $\mathrm{cl}(\mathfrak{l}_{11})$ denotes its class in Cl_F, then

$$\#S_\Psi = [L_\Psi^\pm : F] = \#\left(\mathrm{Cl}_F/\langle \mathrm{cl}(\mathfrak{l}_{11}), 5\mathrm{Cl}_F\rangle\right). \tag{3.37}$$

Since Φ is in the kernel of reduction modulo 5,

$$\begin{aligned} &\ker\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, E[5]) \longrightarrow H^1(\mathbf{Q}_5, E[5^\infty])/\,\mathrm{im}(\kappa_5)\right) \\ &= \ker\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi) \longrightarrow H^1(\mathbf{Q}_5, E[5^\infty])/\,\mathrm{im}(\kappa_5)\right) \\ &\times \ker\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi) \longrightarrow H^1(\mathbf{Q}_5, E[5^\infty])/\,\mathrm{im}(\kappa_5)\right). \end{aligned} \tag{3.38}$$

On the other hand, since Φ does not correspond to μ_5 under the Tate parametrization over $\mathbf{Q}_{11}$,

$$\begin{aligned} &\ker\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, E[5]) \longrightarrow H^1(\mathbf{Q}_{11}, E[5^\infty])\right) \\ &\neq \ker\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi) \longrightarrow H^1(\mathbf{Q}_{11}, E[5^\infty])\right) \\ &\times \ker\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi) \longrightarrow H^1(\mathbf{Q}_{11}, E[5^\infty])\right). \end{aligned} \tag{3.39}$$

Thus, $\tau \in H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)$ is the image of an element of $\mathrm{Sel}_E(\mathbf{Q})[5]$ if and only if it is *peu ramifiée* at 5 and there is a $\tau' \in H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi)$ which is unramified at 5 satisfying

$$(\tau', \tau) \in \ker\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Psi) \times H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi) \longrightarrow H^1(\mathbf{Q}_{11}, E[5^\infty])\right). \tag{3.40}$$

If $\left(\frac{d}{11}\right) = -1$ or 0, then $H^1(\mathbf{Q}_{11}, \Psi)$ and $H^1(\mathbf{Q}_{11}, \Phi)$ are trivial, so elements of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)$ contribute to $\#\,\mathrm{Sel}_E(\mathbf{Q})[5]$ if and only if they can be represented by $\alpha \in F^\times/(F^\times)^5$ of norm one, satisfying $v_\mathfrak{l}(\alpha) \equiv 0 \pmod 5$ for all primes $\mathfrak{l}$ of F. That is,

$$\#S_\Phi = \#\mathrm{Cl}_F[5] \cdot \#\left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5}\right). \tag{3.41}$$

Combining 3.37 and 3.41 we have

$$\#\,\mathrm{Sel}_E(\mathbf{Q})[5] = (\#\mathrm{Cl}_F[5])^2 \cdot \#\left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5}\right). \tag{3.42}$$

If $\left(\frac{d}{11}\right) = +1$, then $H^1(\mathbf{Q}_{11}, \Psi) \cong (\mathbf{Z}/5\mathbf{Z})^2 \cong H^1(\mathbf{Q}_{11}, \Phi)$, and $H^1_{nr}(\mathbf{Q}_{11}, \Psi) \cong \mathbf{Z}/5\mathbf{Z} \cong H^1_{nr}(\mathbf{Q}_{11}, \Phi)$. If $A' \subseteq H^1(\mathbf{Q}_{11}, \Psi)$ and $B' \subseteq H^1(\mathbf{Q}_{11}, \Phi)$ are defined as before, there are four possibilities.

If A' is trivial, then $B' = H^1(\mathbf{Q}_{11}, \Phi)$, $\eta_2 = 1$ and $\eta_3 = 0$. In this case, $\tau \in H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \Phi)$ is the image of an element of $\mathrm{Sel}_E(\mathbf{Q})[5]$ if and only if it is *peu ramifiée* at 5 and completely trivial in $H^1(\mathbf{Q}_{11}, \Phi)$. Since $H^1_{nr}(\mathbf{Q}_{11}, \Phi) \subseteq B'$, not every α of norm one satisfying $v_\mathfrak{l}(\alpha) \equiv 0 \pmod 5$ represents a τ which is the image of an element of $\mathrm{Sel}_E(\mathbf{Q})[5]$, and we have

$$\#\,\mathrm{Sel}_E(\mathbf{Q})[5] = 5^{-1} \cdot (\#\mathrm{Cl}_F[5])^2 \cdot \#\left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5}\right). \tag{3.43}$$

If $A' = H^1(\mathbf{Q}_{11}, \Psi)$, then B' is trivial, $\eta_2 = 0$, $\eta_3 = 1$, and τ will be the image of an element of $\mathrm{Sel}_E(\mathbf{Q})[5]$ as long as it is *peu ramifiée* at 5. Thus, (3.43) again holds.

If $A' = H^1_{nr}(\mathbf{Q}_{11}, \Psi)$, then $B' = H^1_{nr}(\mathbf{Q}_{11}, \Phi)$ by lemma 1.3, and $\eta_2 = \eta_3 = 0$. In this case, τ will again automatically be the image of an element of $\mathrm{Sel}_E(\mathbf{Q})[5]$ as long as it is *peu ramifiée* at 5, and again (3.43) holds.

If A' is a proper, non-trivial subgroup of $H^1(\mathbf{Q}_{11}, \Psi)$ which doesn't coincide with $H^1_{nr}(\mathbf{Q}_{11}, \Psi)$, then the same holds for $B' \subseteq H^1(\mathbf{Q}_{11}, \Phi)$. In this case, $\eta_2 = \eta_3 = 1$, and τ will automatically be the image of an element of $\mathrm{Sel}_E(\mathbf{Q})[5]$ as long as it is *peu ramifiée* at 5. However, in this case there are τ represented by α such that $v_{\mathfrak{l}_{11}}(\alpha) \not\equiv 0 \pmod 5$, so

$$\#S_\Phi = 5 \cdot \#\mathrm{Cl}_F[5] \cdot \# \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right), \tag{3.44}$$

and

$$\#\,\mathrm{Sel}_E(\mathbf{Q})[5] = 5 \cdot (\#\mathrm{Cl}_F[5])^2 \cdot \dim_{\mathbf{F}_5} \left(\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^5} \right). \tag{3.45}$$

Combining (3.42), (3.43) and (3.45) we have proved the following.

Theorem 3.4. *Let $d \neq 1$ be a square-free integer, and let E be the quadratic twist by d of the elliptic curve 11A1. Let $\eta_0 = 0$ if $d < 0$, and $\eta_0 = 1$ if $d > 1$. If $\left(\frac{d}{11}\right) = -1$ or 0, then*

$$\#\,\mathrm{Sel}_E(\mathbf{Q})[5] = 5^{\eta_0} \cdot (\#\mathrm{Cl}_F[5])^2. \tag{3.46}$$

If $\left(\frac{d}{11}\right) = +1$, then let $\eta_1 = \min\{\eta_2, \eta_3\}$; in this case

$$\#\,\mathrm{Sel}_E(\mathbf{Q})[5] = 5^{\eta_0 - (-1)^{\eta_1}} \cdot (\#\mathrm{Cl}_F[5])^2. \tag{3.47}$$

3.2.4 Data

If we call $\dim_{\mathbf{F}_p}(A[p])$ the p-rank of A, then from theorems 3.2, 3.3 and 3.4 we can see that the 5-ranks of the Selmer group for $E_i^{(d)}$ are roughly between the 5-rank

and twice the 5-rank of the class group of the quadratic field $F = \mathbf{Q}(\sqrt{d})$. The 5-ranks of class groups of quadratic fields are conjectured to be unbounded. This is equivalent to the conjecture that the 5-ranks of the Selmer groups of quadratic twists of the elliptic curves 11A1 - 3 are unbounded, which is in turn equivalent to the conjecture that either the ranks of these quadratic twists or the 5-ranks of their Tate-Shafarevich groups are unbounded. In the direction of the initial conjecture, J.-F. Mestre proved in [18] that there are infinitely many real quadratic fields and infinitely many imaginary quadratic fields whose class group has 5-rank at least 3. This, with theorem 3.4 gives us the following corollary.

Corollary 3.5. *There are infinitely many square-free integers $d < 0$ such that the 5-rank of the Selmer group for the quadratic twist by d of the elliptic curve 11A1 is at least 5. There are infinitely many square-free integers $d > 1$ such that the same quantity is at least 6.*

Given a non-negative integer r, it is very natural to ask what is the smallest value of d for $d > 1$ (or the smallest value of $-d$ for $d < 0$) such that the twist of 11A1 by d has 5-rank r. Table 3.1 shows the answer to this question for $d < 0$ and $r \leq 5$, computed using the PARI/GP program [1]. In [3], D. A. Buell computed the class groups of all imaginary quadratic fields with $D > -25\,000\,000$, finding only two examples where the 5-rank of the class group is 3, and none where the 5-rank of the class group is greater than 3. In both of these cases - $d = -2\,800\,905$ and $d = -18\,397\,407$ - $\left(\frac{d}{11}\right) = +1$ and $\eta_1 = 0$, so the 5-ranks of the Selmer groups of the twists of 11A1 by these d are 5. The smallest value of $-d$, for $d < 0$, for which the 5-rank of the Selmer group of the twist of 11A1 by d is at least 6 must satisfy $-D > 25\,000\,000$, if it exists.

Theorems 3.2, 3.3 and 3.4 can also be used to find values of d for which the groups $\mathrm{Sel}_{E_i^{(d)}}(\mathbf{Q})[5]$ do not all agree. If d is chosen so that $\#\mathrm{Cl}_F[5] = 5$, $\eta_1 = \eta_3 = 0$ and

Table 3.1: The first negative d for which the 5-rank of the Selmer group of the twist by d of 11A1 has rank r.

r	d
0	-1
1	-2
2	-86
3	-206
4	-4 486
5	-285 797

$\eta_2 = 1$, then

$$5^2 \leq \#\,\mathrm{Sel}_{E_2^{(d)}}(\mathbf{Q})[5] \leq 5^3, \tag{3.48}$$

but

$$\#\,\mathrm{Sel}_{E_1^{(d)}}(\mathbf{Q})[5] = \#\,\mathrm{Sel}_{E_3^{(d)}}(\mathbf{Q})[5] = 5. \tag{3.49}$$

Similarly, if $\eta_1 = \eta_2 = 0$ and $\eta_3 = 1$, then

$$5^2 \leq \#\,\mathrm{Sel}_{E_3^{(d)}}(\mathbf{Q})[5] \leq 5^3, \tag{3.50}$$

but

$$\#\,\mathrm{Sel}_{E_1^{(d)}}(\mathbf{Q})[5] = \#\,\mathrm{Sel}_{E_2^{(d)}}(\mathbf{Q})[5] = 5. \tag{3.51}$$

For $d < 0$, the first example of the former is $d = -1\,327$, and the first example of the latter is $d = -321$.

3.3 *Twists of 19A1 - 3*

Let E_1, E_2 and E_3 be the elliptic curves 19A1, 19A2 and 19A3 respectively, given by the following equations.

$$E_1 \ : \ y^2 + y = x^3 + x^2 - 9x - 15 \tag{3.52}$$

$$E_2 \ : \ y^2 + y = x^3 + x^2 - 769x - 8\,470 \tag{3.53}$$

$$E_3 \ : \ y^2 + y = x^3 + x^2 \tag{3.54}$$

This example is exactly analogous to the example in section 3.2. These curves are related via rational isogenies of degree 3 by

$$E_2 \rightleftarrows E_1 \rightleftarrows E_3 \tag{3.55}$$

Since $E_1(\mathbf{Q})_{tors} = \mathbf{Z}/3\mathbf{Z} = E_3(\mathbf{Q})_{tors}$, the kernels of the isogenies $E_3 \longrightarrow E_1$ and $E_1 \longrightarrow E_2$ are isomorphic to $\mathbf{Z}/3\mathbf{Z}$ as $G_{\mathbf{Q}}$-modules. As a consequence of the Weil pairing, the kernels of the isogenies $E_2 \longrightarrow E_1$ and $E_1 \longrightarrow E_3$ are isomorphic to μ_3 as $G_{\mathbf{Q}}$-modules. Thus

$$E_1[3] \cong \mu_3 \otimes \mathbf{Z}/3\mathbf{Z}, \tag{3.56}$$

and we have the following short exact sequences.

$$0 \longrightarrow \mu_3 \longrightarrow E_2[3] \longrightarrow \mathbf{Z}/3\mathbf{Z} \longrightarrow 0 \tag{3.57}$$

$$0 \longrightarrow \mathbf{Z}/3\mathbf{Z} \longrightarrow E_3[3] \longrightarrow \mu_3 \longrightarrow 0 \tag{3.58}$$

Since these curves have conductor 19, they have good reduction at all primes except 19, and multiplicative reduction at 19.

$$a_3 := 4 - \#\tilde{E}_i[3] = -2 \not\equiv 0 \pmod 3, \tag{3.59}$$

so the curves have good, ordinary reduction at 3. As in section 3.2, the kernels of the isogenies $E_2 \longrightarrow E_1$ and $E_1 \longrightarrow E_3$ are contained in the kernels of reduction modulo

3, but the kernels of the isogenies $E_3 \longrightarrow E_1$ and $E_1 \longrightarrow E_2$ are not. If j_i denotes the j-invariant of E_i, and q_i its Tate period over $\mathbf{Q}_{19}$, then $v_{19}(q_i) = -v_{19}(j_i)$.

$$v_{19}(q_1) = 3, \tag{3.60}$$

$$v_{19}(q_2) = 1, \tag{3.61}$$

$$v_{19}(q_3) = 1. \tag{3.62}$$

Thus, the same argument used in section 3.2, together with lemma 3.1, implies that the kernels of the isogenies $E_2 \longrightarrow E_1$ and $E_3 \longrightarrow E_1$ correspond to μ_3 under the Tate parametrizations of E_i over $\mathbf{Q}_{19}$, but the kernels of $E_1 \longrightarrow E_2$ and $E_1 \longrightarrow E_3$ do not.

If we again let $d \neq 1$ be a square-free integer, D be the discriminant of $F = \mathbf{Q}(\sqrt{d})$, and ε_d be the quadratic character corresponding to the extension $F/\mathbf{Q}$, then $E_i^{(d)}$ has additive reduction at all primes $l \mid D$. For such l, $E_i^{(d)}$ achieves good reduction (for $l \neq 19$) or multiplicative reduction ($l = 19$) over F. Since $[F : \mathbf{Q}] = 2$ is relatively prime to 3,

$$H^1(\mathbf{Q}_l, \mu_3 \otimes \varepsilon_d) = 0 = H^1(\mathbf{Q}_l, \mathbf{Z}/3\mathbf{Z} \otimes \varepsilon_d) \tag{3.63}$$

for all $l \mid D$, $l \neq 3$. If $3 \mid D$, $E_i^{(d)}$ achieves good, ordinary reduction at 3 over F, so since $F/\mathbf{Q}$ is a quadratic extension, the theorems of chapter 2 apply. All of the ingredients are exactly analogous to those in section 3.2, and we have the following analogues of theorems 3.2, 3.3 and 3.4.

Theorem 3.6. *Let $d \neq 1$ be a square-free integer, and let E be the quadratic twist by d of the elliptic curve 19A3. Let $\eta_0 = 0$ if $d < 0$, and $\eta_0 = 1$ if $d > 1$. If $\left(\frac{d}{19}\right) = -1$ or 0, then*

$$\#\mathrm{Cl}_F[3] \leq \#\,\mathrm{Sel}_E(\mathbf{Q})[3] \leq 3^{\eta_0} \cdot (\#\mathrm{Cl}_F[3])^2\,. \tag{3.64}$$

If $\left(\frac{d}{19}\right) = +1$, let $\eta_3 = 0$ if $\#\mathrm{Cl}_F[3] = \#\left(\left(\mathrm{Cl}_F^{\{19\}}/3\mathrm{Cl}_F^{\{19\}}\right)^{(-)}\right)$, and $\eta_3 = 1$ otherwise.

Then

$$3^{\eta_3} \cdot \#\mathrm{Cl}_F[3] \leq \#\,\mathrm{Sel}_E(\mathbf{Q})[3] \leq 3^{\eta_0-(-1)^{\eta_3}} \cdot \left(\#\mathrm{Cl}_F[3]\right)^2. \tag{3.65}$$

Theorem 3.7. *Let $d \neq 1$ be a square-free integer, and let E be the quadratic twist by d of the elliptic curve 19A2. Let $\eta_0 = 0$ if $d < 0$, and $\eta_0 = 1$ if $d > 1$. If $\left(\frac{d}{19}\right) = -1$ or 0, then*

$$3^{\eta_0} \cdot \#\mathrm{Cl}_F[3] \leq \#\,\mathrm{Sel}_E(\mathbf{Q})[3] \leq 3^{\eta_0} \cdot \left(\#\mathrm{Cl}_F[3]\right)^2. \tag{3.66}$$

If $\left(\frac{d}{19}\right) = +1$, let $\eta_2 = 1$ if the class of one of the prime ideals of F lying over 11 is in $3\mathrm{Cl}_F$ and $\eta_2 = 0$ otherwise. Then

$$3^{\eta_0+\eta_2} \cdot \#\mathrm{Cl}_F[3] \leq \#\,\mathrm{Sel}_E(\mathbf{Q})[3] \leq 3^{\eta_0-(-1)^{\eta_2}} \cdot \left(\#\mathrm{Cl}_F[3]\right)^2. \tag{3.67}$$

Theorem 3.8. *Let $d \neq 1$ be a square-free integer, and let E be the quadratic twist by d of the elliptic curve 19A1. Let $\eta_0 = 0$ if $d < 0$, and $\eta_0 = 1$ if $d > 1$. If $\left(\frac{d}{19}\right) = -1$ or 0, then*

$$\#\,\mathrm{Sel}_E(\mathbf{Q})[3] = 3^{\eta_0} \cdot \left(\#\mathrm{Cl}_F[3]\right)^2. \tag{3.68}$$

If $\left(\frac{d}{19}\right) = +1$, let $\eta_1 = \min\{\eta_2, \eta_3\}$; in this case

$$\#\,\mathrm{Sel}_E(\mathbf{Q})[3] = 3^{\eta_0-(-1)^{\eta_1}} \cdot \left(\#\mathrm{Cl}_F[3]\right)^2. \tag{3.69}$$

Chapter 4

IWASAWA THEORY

4.1 Introduction

Let K be a number field, and let K_∞/K be a $\mathbf{Z}_p$-extension. That is, let K_∞/K be a Galois extension with $\Gamma := G_{K_\infty/K} \cong \mathbf{Z}_p$. For each positive integer n there is a unique intermediate field K_n with $\Gamma_n := G_{K_\infty/K_n} = \Gamma^{p^n}$, and $G_{K_n/K} \cong \mathbf{Z}/p^n\mathbf{Z}$. Every number field has at least one such extension: the cyclotomic $\mathbf{Z}_p$-extension of K is the unique field $K_\infty^{cyc} \subseteq K\mathbf{Q}(\mu_{p^\infty})$ such that $G_{K_\infty^{cyc}/K} \cong \mathbf{Z}_p$. Throughout this chapter, we restrict our attention to the cyclotomic $\mathbf{Z}_p$-extension, and set $K_\infty = K_\infty^{cyc}$.

If we define the p-primary Selmer group for E over K_∞ in the same manner in which we defined the Selmer group over a number field,

$$\mathrm{Sel}_E(K_\infty)_p := \ker\left(H^1(K_\infty, E[p^\infty]) \longrightarrow \prod_{\mathfrak{l}} \left(H^1((K_\infty)_\mathfrak{l}, E[p^\infty])/\operatorname{im}(\kappa_\mathfrak{l})\right)\right) \qquad (4.1)$$

there is a natural, continuous Γ-action on $\mathrm{Sel}_E(K_\infty)_p$, making $\mathrm{Sel}_E(K_\infty)_p$ a module over the completed group ring $\Lambda := \mathbf{Z}_p[[\Gamma]]$, known as the Iwasawa algebra. If we choose a topological generator γ of Γ, then there is a (non-canonical) isomorphism $\Lambda \cong \mathbf{Z}_p[[T]]$ sending γ to $(T+1)$. Modules over the Iwasawa algebra have been extensively studied; although Λ is not a principal ideal domain, there is the following analogue to the structure theorem for finitely generated modules over principal ideal domains (see [14]).

Theorem. *Suppose X is a finitely generated Λ-module. Then there exists a Λ-module*

homomorphism

$$\sigma : X \longrightarrow \Lambda^r \times \prod_{i=1}^{t} \Lambda/(f_i(T)^{e_i}) \tag{4.2}$$

with finite kernel and cokernel, where $r \geq 0$, $f_1(T), \ldots, f_t(T)$ *are irreducible elements of* Λ, *and* $e_1, \ldots, e_t$ *are positive integers. The integer* r, *the prime ideals* $(f_i(T))$, *and the corresponding exponents* e_i *are uniquely determined by* X.

The group $\mathrm{Sel}_E(K_\infty)_p$ is generally *not* finitely generated as a Λ-module. Its Pontryagin dual $X_E(K_\infty) := \mathrm{Hom}(\mathrm{Sel}_E(K_\infty)_p, \mathbf{Q}_p/\mathbf{Z}_p)$, on the other hand, is a finitely generated Λ-module. (We say $\mathrm{Sel}_E(K_\infty)_p$ is cofinitely generated.) The following theorem of Kato and Rohrlich gives sufficient conditions for $X_E(K_\infty)$ to be a torsion Λ-module (equivalently, for $\mathrm{Sel}_E(K_\infty)_p$ to be Λ-cotorsion). (See [20].)

Theorem (Kato-Rohrlich). *Assume that* E *is defined over* $\mathbf{Q}$ *and is modular. Assume also that* E *has good, ordinary reduction or multiplicative reduction at* p, *and that* $K/\mathbf{Q}$ *is abelian. Then* $\mathrm{Sel}_E(K_\infty)_p$ *is* Λ*-cotorsion.*

Remark. All elliptic curves over $\mathbf{Q}$ are modular, as shown in [32], [29], [7], [5] and [2].

If E satisfies the hypotheses of the theorem, then $\mathrm{Sel}_E(K_\infty)_p$ is Λ-cotorsion, and the structure theorem for finitely generated Λ-modules gives a homomorphism (4.2) with $X = X_E(K_\infty)$ and $r = 0$. Let $I = (f_1(T)^{e_1} \cdot \ldots \cdot f_t(T)^{e_t})$. By the Weierstrass Preparation Theorem, we can choose a generator of I of the form $p^\mu \cdot g(T)$, where μ is a non-negative integer and $g(T)$ is a distinguished polynomial of degree λ. This allows us to define the algebraic Iwasawa invariants associated to E: $\lambda_E^{alg}(K_\infty/K) = \lambda$ and $\mu_E^{alg}(K_\infty/K) = \mu$.

Hereafter, we restrict our attention to the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty/\mathbf{Q}$. As we will not discuss the analytic Iwasawa invariants, we simplify the notation by using λ_E and μ_E to denote $\lambda_E^{alg}(\mathbf{Q}_\infty/\mathbf{Q})$ and $\mu_E^{alg}(\mathbf{Q}_\infty/\mathbf{Q})$.

4.2 *Mu invariants*

In [13], R. Greenberg made the following conjecture.

Conjecture. *Let E be an elliptic curve defined over $\mathbf{Q}$. Assume that $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ is Λ-cotorsion. Then there exists a $\mathbf{Q}$-isogenous elliptic curve E' such that $\mu_{E'} = 0$.*

Remark. M. J. Drinen showed in [8] that the conjecture need not hold if $\mathbf{Q}$ is replaced with an arbitrary number field.

If $\sigma : E \longrightarrow E'$ is an isogeny, P. Schneider [22] gives a relationship between μ_E and $\mu_{E'}$ in terms of $\Psi := \ker(\sigma)$. If $\deg(\sigma)$ is prime to p, or if σ is the multiplication-by-p map, then $\mu_E = \mu_{E'}$. If σ is a cyclic isogeny of p-power degree (that is, if $\Psi \cong \mathbf{Z}/p^n\mathbf{Z}$ for some n) the situation is more complicated. We say Ψ is ramified at p if p is ramified in $\mathbf{Q}(\Psi)/\mathbf{Q}$, and otherwise Ψ is unramified at p. We say Ψ is odd (resp. even) if complex conjugation acts non-trivially (resp. trivially) on Ψ. (For $p = 2$ we need to use a different definition of odd and even.) Suppose E has good, ordinary reduction at p. Then

$$\mu_E = \mu_{E'} + \begin{cases} n & : \ \Psi \text{ is ramified at } p \text{ and odd} \\ -n & : \ \Psi \text{ is unramified at } p \text{ and even} \\ 0 & : \ \text{otherwise} \end{cases} . \tag{4.3}$$

We can use (4.3) to rephrase the conjecture.

Conjecture. *Let E be an elliptic curve defined over $\mathbf{Q}$ with good, ordinary reduction at p. Let Ψ be the largest cyclic, $G_\mathbf{Q}$-invariant subgroup of $E[p^\infty]$ which is ramified and odd, and set $p^n = \#\Psi$. Then $\mu_E = n$.*

Suppose E is an elliptic curve defined over $\mathbf{Q}$ which admits a rational isogeny of degree p for p an odd prime, and suppose E has good, ordinary reduction at p. Let Ψ be the kernel of the isogeny. If Ψ is either ramified at p and even, or unramified at p and odd, then the conjecture predicts $\mu_E = 0$. R. Greenberg proved this in [13].

The cases where Ψ is unramified at p and even or ramified at p and odd are currently untractable. (M. Trifković has verified the conjecture for a few examples in this case in [30].) For the rest of this chapter, assume Ψ is unramified and even, and assume $E[p]$ is indecomposable as a $G_{\mathbf{Q}}$-module, in which case the conjecture predicts $\mu_E = 0$. The following lemma relates μ_E for E to the orders of the groups $\mathrm{Sel}_E(\mathbf{Q}_n)[p]$.

Lemma 4.1. *Suppose* $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ *is* Λ*-cotorsion. Then* $\#\,\mathrm{Sel}_E(\mathbf{Q}_n)[p]$ *is bounded as* $n \to \infty$ *if and only if* $\mu_E = 0$.

Proof. Mazur's Control Theorem (see [14]) states that the kernels and cokernels of the natural maps

$$\mathrm{Sel}_E(\mathbf{Q}_n)_p \longrightarrow \mathrm{Sel}_E(\mathbf{Q}_\infty)_p{}^{\Gamma_n} \tag{4.4}$$

are bounded as $n \to \infty$. Thus,

$$\dim_{\mathbf{F}_p}(\mathrm{Sel}_E(\mathbf{Q}_n)[p]) - \dim_{\mathbf{F}_p}(\mathrm{Sel}_E(\mathbf{Q}_\infty)[p])^{\Gamma_n} \tag{4.5}$$

is also bounded as $n \to \infty$.

Let $\omega_n(T) = (1+T)^{p^n} - 1 \in \Lambda$. If $X := X_E(\mathbf{Q}_\infty)$ is the Pontryagin dual of $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$, then $\tilde{X} := X/pX$ is the Pontryagin dual of $\mathrm{Sel}_E(\mathbf{Q}_\infty)[p]$, and $\tilde{X}/\omega_n(T)\tilde{X}$ is the Pontryagin dual of $(\mathrm{Sel}_E(\mathbf{Q}_\infty)[p])^{\Gamma_n}$. Let

$$X \longrightarrow \prod_{i=1}^{t} \Lambda/(f_i(T)^{e_i}) \tag{4.6}$$

be the map given in the structure theorem for finitely generated Λ-modules, with finite kernel and cokernel. (Note that X is a torsion Λ-module, so $r = 0$.) We can take each $f_i(T)$ to be either p or a distinguished polynomial of degree d_i, and relabel so that $f_i(T)$ is a distinguished polynomial for $1 \le i \le s$ and $f_i(T) = p$ for $s+1 \le i \le t$. Then

$$\Lambda/(f_i(T)^{e_i}) \cong \begin{cases} (\mathbf{Z}_p)^{d_i e_i} & : \quad 1 \le i \le s \\ (\mathbf{Z}/p^{e_i}\mathbf{Z})[[T]] & : \quad s+1 \le i \le t \end{cases}. \tag{4.7}$$

Let $\tilde{\Lambda} = \Lambda/p\Lambda$; for any $f(T) \in \Lambda$, let $\tilde{f}(T)$ be its image in $\tilde{\Lambda}$. Applying the Snake Lemma to (4.6), the kernel and cokernel of the map

$$\tilde{X} \longrightarrow \prod_{i=1}^{t} \left(\tilde{\Lambda}/(\tilde{f}_i(T)^{e_i})\right) \cong \prod_{i=1}^{s} \left(\tilde{\Lambda}/(\tilde{f}_i(T)^{e_i})\right) \times \prod_{i=s+1}^{t} \left(\tilde{\Lambda}\right) \tag{4.8}$$

are finite. Another application of the Snake Lemma shows the kernels and cokernels of

$$\tilde{X}/\tilde{\omega}_n(T)\tilde{X} \longrightarrow \prod_{i=1}^{s} \tilde{\Lambda}/(\tilde{f}_i(T)^{e_i}, \tilde{\omega}_n(T)) \times \prod_{i=s+1}^{t} \tilde{\Lambda}/(\tilde{\omega}_n(T)) \tag{4.9}$$

are finite, and of bounded order as $n \to \infty$.

For $1 \leq i \leq s$, $\tilde{f}_i^{e_i}(T) = T^{d_i e_i}$; $\tilde{\omega}_n(T) = T^{p^n}$ for all n. Thus, for $n \gg 0$, $\left(\tilde{\Lambda}/(\tilde{f}_i^{e_i}, \tilde{\omega}_n)\right) \cong (\mathbf{Z}/p\mathbf{Z})^{d_i e_i}$ and $\left(\tilde{\Lambda}/(\tilde{\omega}_n(T))\right) \cong (\mathbf{Z}/p\mathbf{Z})^{p^n}$, and

$$\sum_{i=1}^{s} d_i e_i + (t-s)p^n - \dim_{\mathbf{F}_p}\left(\tilde{X}/\omega_n(T)\tilde{X}\right) \tag{4.10}$$

is bounded as $n \to \infty$. Since $\tilde{X}/\omega_n(T)\tilde{X}$ is the Pontryagin dual of $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p^{\Gamma_n}$, (4.5) and (4.10) imply

$$(t-s)p^n - \dim_{\mathbf{F}_p}\left(\mathrm{Sel}_E(\mathbf{Q}_n)[p]\right) \tag{4.11}$$

is bounded as $n \to \infty$. That is, $\#\,\mathrm{Sel}_E(\mathbf{Q}_n)[p]$ is bounded as $n \to \infty$ if and only if $s = t$, which is equivalent to $\mu_E = 0$. □

Since Ψ is even and Φ is odd, $\mathrm{corank}_{\tilde{\Lambda}}\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi)\right) = 1$ and $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Psi)$ is finite, by lemma 5.9 of [13]. Thus, as $n \to \infty$, $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Psi)$ is bounded, but $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi)$ is unbounded.

Since E has good, ordinary reduction at p and Ψ is not ramified at p, Ψ is not in the kernel of reduction modulo p. Thus, if $\mathfrak{p}_n$ is the (unique) prime of $\mathbf{Q}_n$ lying over p, we have $\mathcal{L}_{\mathfrak{p}_n}(\Phi) = H^1_{pr}\left((\mathbf{Q}_n)_{\mathfrak{p}_n}, \Phi\right)$ in the language of chapter 2. Let Σ be as in chapter 2, and let Σ_n be the set of primes of $\mathbf{Q}_n$ lying over primes in Σ. No primes split completely in the cyclotomic extension $\mathbf{Q}_\infty/\mathbf{Q}$, so $\#\Sigma_n$ is bounded as $n \to \infty$.

Since $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Psi)$ is bounded as $n \to \infty$, so are the contributions of Ψ to both the upper and lower bounds for $\#\,\mathrm{Sel}_E(\mathbf{Q}_n)[p]$ given in theorem 2.16. On the other hand, the contribution of Φ to the upper bound is given by the size of

$$\ker\left(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi) \longrightarrow \prod_{\mathfrak{l}\in\Sigma_n} H^1\left((\mathbf{Q}_n)_\mathfrak{l}, \Phi\right)/\mathcal{L}_\mathfrak{l}(\Phi)\right). \tag{4.12}$$

The size of the cokernel of this map is bounded by

$$\begin{aligned}\#\left(\prod_{\mathfrak{l}\in\Sigma_n}\frac{H^1\left((\mathbf{Q}_n)_\mathfrak{l}, \Phi\right)}{\mathcal{L}_\mathfrak{l}(\Phi)}\right) &\leq \#\left(\frac{H^1\left((\mathbf{Q}_n)_{\mathfrak{p}_n}, \Phi\right)}{H^1_{pr}\left((\mathbf{Q}_n)_{\mathfrak{p}_n}, \Phi\right)}\right)\cdot\#\left(\prod_{\mathfrak{l}\in\Sigma_n-\{\mathfrak{p}_n\}} H^1\left((\mathbf{Q}_n)_\mathfrak{l}, \Phi\right)\right)\\ &\leq p\cdot p^{2(\#\Sigma_n-1)},\end{aligned} \tag{4.13}$$

which is bounded as $n \to \infty$. Since $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi)$ is unbounded, the contribution of Φ to the upper bound given in theorem 2.16 must be unbounded. That is, when applying theorem 2.16 to the Selmer group for E over intermediate fields in the extension $\mathbf{Q}_\infty/\mathbf{Q}$, the lower bound for $\#\,\mathrm{Sel}_E(\mathbf{Q}_n)[p]$ remains bounded as $n \to \infty$, but the upper bound does not.

For the conjecture to hold, the actual value of $\#\,\mathrm{Sel}_E(\mathbf{Q}_n)[p]$ must remain bounded, so most elements of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi)$ which satisfy the Selmer conditions at all primes must *not* actually contribute to the Selmer group. There are two possible ways for this to happen. Such an element must either not be the image of an element of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, E[p])$, or it must not be the image of an element which satisfies the Selmer conditions at all primes. As the next lemma shows, the former cannot account for much of the conjectured discrepancy.

Lemma 4.2. $\mathrm{coker}\left(H^1\left(\mathbf{Q}_\Sigma/\mathbf{Q}_n, E[p]\right) \longrightarrow H^1\left(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi\right)\right)$ *is bounded as* $n \to \infty$.

Proof. From the long, exact sequence of Galois cohomology, we have the exact sequence

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, E[p]) \longrightarrow H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi) \longrightarrow H^2(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Psi), \tag{4.14}$$

so it is enough to show $\#H^2(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Psi)$ is bounded as $n \to \infty$.

Since Ψ is even and $\mathbf{Q}_\infty$ is totally real, the Euler-Poincaré characteristic (see [19]) for Ψ is given by

$$\chi(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Psi) := \prod_{\textit{infinite places}} \frac{\#H^0(\mathbf{R}, \Psi)}{\#\Psi} = 1. \tag{4.15}$$

Thus, $\#H^2(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Psi) = \#H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Psi)/\#\Psi(\mathbf{Q}_n)$ is bounded as $n \to \infty$. □

Since $\operatorname{corank}_{\tilde{\Lambda}} H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi) = 1$ and $\tilde{\Lambda}$ is a principal ideal domain, the Pontryagin dual of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi)$ satisfies

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi)^\vee \cong \tilde{\Lambda} \times A \tag{4.16}$$

for some finite $\tilde{\Lambda}$-module A. Hence,

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi) \cong \tilde{\Lambda}^\vee \times A^\vee. \tag{4.17}$$

Let $S_{E[p]}(\mathbf{Q}_n) \subseteq H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, E[p])$ consist of those elements which satisfy the Selmer conditions at all primes of $\mathbf{Q}_n$, and let $S_\Phi(\mathbf{Q}_n) \subseteq H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi)$ be the image of $S_{E[p]}$. Define $S_{E[p]}(\mathbf{Q}_\infty)$ and $S_\Phi(\mathbf{Q}_\infty)$ in a similar manner. Then, under the restriction maps

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi) \longrightarrow H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi) \tag{4.18}$$

we have injective maps $S_\Phi(\mathbf{Q}_n) \longrightarrow S_\Phi(\mathbf{Q}_\infty)$. If $\mu_E > 0$, then $\#S_\Phi(\mathbf{Q}_n)$ is unbounded as $n \to \infty$ and $S_\Phi(\mathbf{Q}_\infty)$ is infinite. Thus, $\mu_E > 0$ if and only if $S_\Phi(\mathbf{Q}_\infty) \cap H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi)_{\tilde{\Lambda}-div}$ is non-trivial.

Let σ be a non-trivial element of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi)_{\tilde{\Lambda}-div}$. There is some n such that $\sigma \in H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi)$. Consider the commutative diagram

$$\begin{array}{ccc} H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi) & \longrightarrow & \prod_{l_n \in \Sigma_n} H^1((\mathbf{Q}_n)_{l_n}, \Phi) \\ \downarrow & & \downarrow \\ H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi) & \longrightarrow & \prod_{l_\infty \in \Sigma_\infty} H^1((\mathbf{Q}_\infty)_{l_\infty}, \Phi). \end{array} \tag{4.19}$$

If $\mathfrak{l}_n \in \Sigma_n$ is a prime not lying over p, and $\mathfrak{l}_\infty$ an extension of $\mathfrak{l}_n$ to $\mathbf{Q}_\infty$, then $H^1((\mathbf{Q}_\infty)_{\mathfrak{l}_\infty}, \Phi)$ is finite; hence, its maximal $\tilde{\Lambda}$-divisible subgroup is trivial. The image of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty)_{\tilde{\Lambda}-div}$ must be contained on the maximal $\tilde{\Lambda}$-divisible subgroup, so σ has trivial image in $H^1((\mathbf{Q}_\infty)_{\mathfrak{l}_\infty}, \Phi)$. Since

$$\ker\left(H^1((\mathbf{Q}_n)_{\mathfrak{l}_n}, \Phi) \to H^1((\mathbf{Q}_\infty)_{\mathfrak{l}_\infty}, \Phi)\right) \subseteq \ker\left(H^1((\mathbf{Q}_n)_{\mathfrak{l}_n}, \Phi) \to H^1((\mathbf{Q}_{n+1})_{\mathfrak{l}_{n+1}}, \Phi)\right), \tag{4.20}$$

we can choose n sufficiently large that σ must have trivial image in $H^1((\mathbf{Q}_n)_{\mathfrak{l}_n}, \Phi)$.

Thus, such σ will automatically satisfy the Selmer condition at all primes not lying over p. Suppose, in addition, that σ satisfies the Selmer condition at the prime of $\mathbf{Q}_n$ lying over p. If $F_n = \mathbf{Q}_n(\Psi)$, then by inflation-restriction

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, \Phi) \cong H^1(\mathbf{Q}_\Sigma/F_n, \Phi)^{G_{F_n/\mathbf{Q}_n}} \subseteq \left(\frac{F_n^\times}{(F_n^\times)^p}\right)^{(\phi)}. \tag{4.21}$$

Since σ satisfies the Selmer condition at the prime lying over p and is completely trivial at all other primes in Σ_n, we can take σ to be represented by $\alpha \in F_n^\times$ which is either an element of $\mathcal{O}_{F_n}^\times$ or a generator of the p^{th} power of an ideal. By the Ferrero-Washington Theorem (see [31]), the p-ranks of the ideal class groups of F_n are bounded. So, the subset of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi)_{\tilde{\Lambda}-div}$ represented by elements of $\mathcal{O}_{F_n}^\times$ for some n has finite index in $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi)_{\tilde{\Lambda}-div}$. The element represented by $\alpha \in \mathcal{O}_{F_n}^\times$ is in the maximal $\tilde{\Lambda}$-divisible subgroup if and only if it is a universal norm for the extension $\mathbf{Q}_\infty/\mathbf{Q}_n$.

Since σ is represented by α, σ corresponds to an extension $\mathbf{Q}_n(\Phi, \sqrt[p]{\alpha})/\mathbf{Q}_n(\Phi)$. Suppose σ is the image of $\tilde{\sigma} \in H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, E[p])$. Let $K_n = \mathbf{Q}_n(E[p])$. From the restriction map

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, E[p]) \longrightarrow H^1(\mathbf{Q}_\Sigma/K_n, E[p])^{G_{K_n/\mathbf{Q}_n}} \cong \mathrm{Hom}_{G_{K_n/\mathbf{Q}_n}}(G_{\mathbf{Q}_\Sigma/K_n}, E[p]), \tag{4.22}$$

$\tilde{\sigma}$ corresponds to an extension $L/K_n(\sqrt[p]{\alpha})$ of degree p with $G_{L/K_n} \cong E[p]$ as a $G_{K_n/\mathbf{Q}_n}$-module. By Kummer theory, $L = K_n(\sqrt[p]{\varepsilon})$, for some $\varepsilon \in K_n^\times$ such that $\langle \alpha, \varepsilon \rangle \subseteq K_n^\times/(K_n^\times)^p$ is a $G_{K_n/\mathbf{Q}_n}$-invariant submodule isomorphic to $E[p]$.

If $\tilde{\sigma}$ can be chosen to satisfy the Selmer conditions at all primes, then $\mu_E > 0$, and $\tilde{\sigma}$ can be so chosen if and only if we can choose ε so that the extension $L/K_n(\sqrt[p]{\alpha})$ is everywhere unramified.

Thus, $\mu_E = 0$ if and only if for every $\alpha \in \left(\frac{\mathcal{O}_{F_n}^\times}{(\mathcal{O}_{F_n}^\times)^p}\right)^{(\phi)}$ which is a universal norm for F_∞/F_n, there is no $\varepsilon \in \mathcal{O}_{K_n}^\times$ such that $\langle \alpha, \varepsilon \rangle \cong E[p]$ as a $G_{K_n/\mathbf{Q}_n}$-module and $K_n(\sqrt[p]{\alpha}, \sqrt[p]{\varepsilon})/K_n(\sqrt[p]{\alpha})$ is unramified at p.

BIBLIOGRAPHY

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. PARI/GP, a computer algebra package. http://www.parigp-home.de.

[2] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843 – 939, 2001.

[3] D. A. Buell. Class groups of quadratic fields, II. *Math. Comp.*, 48(177):85 – 93, 1987.

[4] J. Coates and R. Greenberg. Kummer theory for abelian varieties over local fields. *Invent. Math.*, 124(1 - 3):129 – 174, 1996.

[5] B. Conrad, F. Diamond, and R. Taylor. Modularity of certain potentially Barsotti-Tate Galois representations. *J. Amer. Math. Soc.*, 12(2):521 – 567, 1999.

[6] J. E. Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1992.

[7] F. Diamond. On deformation rings and Hecke rings. *Ann. of Math. (2)*, 144(1):137 – 166, 1996.

[8] M. J. Drinen. *Iwasawa mu-invariants of Selmer groups.* PhD thesis, University of Washington, 1999.

[9] S. Fermigier. Une courbe elliptique définie sur $\mathbf{Q}$ de rang ≥ 22. *Acta Arith.*, 82(4):359 – 363, 1997.

[10] T. A. Fisher. Some examples of 5 and 7 descent for elliptic curves over $\mathbf{Q}$. *J. Eur. Math. Soc.*, 3(2):169 – 201, 2001.

[11] T. A. Fisher. The Cassels-Tate pairing and the Platonic solids. *J. Number Theory*, 98(1):105 – 155, 2003.

[12] G. Frey. On the Selmer group of twists of elliptic curves with $\mathbf{Q}$-rational torsion points. *Can. J. Math.*, 40(3):649 – 665, 1988.

[13] R. Greenberg. Iwasawa theory for elliptic curves. *Lecture Notes in Math.*, 1716:51 – 144, 1999.

[14] R. Greenberg. Introduction to Iwasawa theory for elliptic curves. In *Arithmetic Algebraic Geometry (Park City, UT, 1999)*, volume 9 of *IAS/Park City Math. Ser.* Amer. Math. Soc., 2001.

[15] R. Greenberg and V. Vatsal. On the Iwasawa invariants of elliptic curves. *Invent. Math.*, 142(1):17 – 63, 2000.

[16] G. Hochschild and J.-P. Serre. Cohomology of group extensions. *Trans. Amer. Math. Soc.*, 74:110 – 134, 1953.

[17] K. Kramer. A family of semistable elliptic curves with large Tate-Shafarevitch groups. *Proc. Amer. Math. Soc.*, 89(3):379 – 386, 1983.

[18] J.-F. Mestre. Corps quadratiques dont le 5-rang du groupe des classes est ≥ 3. *C. R. Acad. Sci. Paris Ser. I Math.*, 315(4):371 – 374, 1992.

[19] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften*. Springer, 2000.

[20] K. Rubin. Euler systems and modular elliptic curves. In *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, volume 254 of *London Math. Soc. Lecture Note Ser.*, pages 351 – 367, 1998.

[21] E. F. Schaefer. Class groups and Selmer groups. *J. Number Theory*, 56:79 – 114, 1996.

[22] P. Schneider. The μ-invariant of isogenies. *J. Indian Math. Soc.*, 52:159 – 170, 1987.

[23] J.-P. Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer – Verlag, 1979.

[24] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54:179 – 230, 1987.

[25] J.-P. Serre. *Galois Cohomology*. Springer, 1997.

[26] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. Math.*, 68:492 – 517, 1968.

[27] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer – Verlag, 1986.

[28] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer – Verlag, 1994.

[29] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553 – 572, 1995.

[30] M. Trifković. *On mu-invariants of elliptic curves over* $\mathbf{Q}$. PhD thesis, Harvard University, 2002.

[31] L. C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer – Verlag, 1982.

[32] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443 – 551, 1995.

VITA

James Michael Mailhot was born and raised in the San Francisco Bay Area. He attended Stanford University from 1988 to 1993, earning Bachelor of Science and Master of Science degrees in Mathematics. In 2003 he earned a Doctor of Philosophy in Mathematics at the University of Washington.