FINDING ELEMENTS OF GIVEN ORDER IN TATE-SHAFAREVICH GROUPS OF ELLIPTIC CURVES

by

Stephen Donnelly

(Under the direction of Robert Rumely)

Abstract

The Tate-Shafarevich group of an elliptic curve over a number field K measures the obstruction to determing the K-rational points by the standard method, which is known as 'descent'. During the last two decades, a focal point of research in arithmetic geometry has been to better understand the structure and behaviour of Tate-Shafarevich groups. Selmer groups provide a stepping stone towards studying Tate-Shafarevich groups; the Selmer groups for the various isogenies defined on the curve encapsulate the information obtainable from local calculations about the set of K-rational points and about the Tate-Shafarevich group. We give a theorem that describes the Selmer groups for a certain kind of isogeny. We then give a method for constructing elliptic curves defined over quadratic fields that have many elements of order 7 in their Tate-Shafarevich groups; the construction shows that there can be arbitrarily many assuming a technical arithmetic hypothesis. As an ingredient in the construction, we find a model of the moduli space $X_0(14)$ with certain convenient properties.

Index words: Algebraic geometry, Arithmetic geometry, Elliptic curves, Tate-Shafarevich group, Descent, Selmer groups, Mordell-Weil group

FINDING ELEMENTS OF GIVEN ORDER IN TATE-SHAFAREVICH GROUPS OF ELLIPTIC CURVES

by

Stephen Donnelly

B. Sc., Australian National University, Australia, 1996

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2003

FINDING ELEMENTS OF GIVEN ORDER IN TATE-SHAFAREVICH GROUPS OF ELLIPTIC CURVES

by

Stephen Donnelly

Approved:

Major Professor: Robert Rumely

Committee: Matt Baker
Sybilla Beckman-Kazez
Roy Smith
Robert Varley

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
August 2003

Acknowledgments

First let me thank my advisor Professor Rumely for looking after me in many ways during my time at UGA, and showing much patience and concern.

I am fortunate in having had considerable help from many members of the department. Professor Granville gave several wonderful courses early in my time here, conveying a very sound understanding of many ideas in number theory. I thank him also for valued advice and encouragement, and for his great generosity in funding a number of expeditions including an extended visit to Montreal. I owe to Professor Smith much of what I understand of algebraic geometry; in some of the most memorable lectures I have attended, he projected a very strong and clear insight. I greatly appreciate Professor Varley's generosity and warm encouragement; however busy, he always made time to carefully talk through the questions I brought him. I was lucky to have Professor Benson, who I came to regard as my homological guru, providing quick and lucid solutions to my algebraic difficulties, and being good company in general. Not least, I've learnt a lot from Professor Lorenzini, and enjoyed his clear style.

It's a pleasure to thank my friend Sungkon Chang for many mathematical conversations which helped to make working more fun. And in the same vein I've enjoyed useful conversations regarding my work and other matters with Tom Tucker, Par Kurlberg, Adrian Iovita, Henri Darmon, Bill McCallum and Michael Stoll.

Table of Contents

Introduction

The motivating problem for my work is to show that the Tate-Shafarevich group of an elliptic curve can have arbitrarily many elements of order ℓ, for any prime ℓ, and to find methods for constructing elements of a given order. One could pose this problem for elliptic curves over $\mathbb{Q}$ or over a number field K. The Tate-Shafarevich group of an elliptic curve over a number field K is a cohomological obstruction, measuring the extent to which our standard method for determining the set of K-rational points fails. An alternative description of the Tate-Shafarevich group of E over K is that it classifies curves whose Jacobian is E, that have points over all completions of K but no points over K itself.

For an elliptic curve E with coefficients in a number field K, Mordell and Weil proved that the set of points with coordinates in K form a finitely generated subgroup $E(K)$. There is still no known algorithm to determine generators for $E(K)$. The standard approach to computing $E(K)$ is a twentieth century version of the *method of descent* invented by Fermat. For him, to solve a Diophantine equation by descent meant to show that each solution in integers leads to a smaller integer solution to a related equation, eventually leading to solutions small enough to be found by hand. For a modern arithmetic geometer to determine $E(K)$ by descent, she first chooses an integer ℓ, and isogeny $\phi : E \to E'$ of degree ℓ to another elliptic curve. There is then an exact sequence of finite groups

$$0 \to E'(K)/\phi E(K) \to \mathrm{Sel}^{\phi}(E, K) \to Ш(E, K)[\phi] \to 0$$

where the middle group is the 'Selmer group' for ϕ over K and $Ш(E, K)$ is the Tate-Shafarevich group of E over K. In principle there is a method to determine

$\mathrm{Sel}^\phi(E,K)$ but it is an open problem to give a method for identifying the image of $E'(K)/\phi E(K)$ inside it. Calculating $\mathrm{Sel}^\phi(E,K)$ involves local calculations (in completions K_v of K); basically one has to calculate $E'(K_v)/\phi E(K_v)$ for each place v of K. There is also a geometric interpretation of the exact sequence, under which elements of $\mathrm{Sel}^\phi(E,K)$ are curves whose Jacobian is E, and which have K_v-rational points for all v. Deciding whether an element is in the image of $E'(K)/\phi E(K)$ is equivalent to deciding whether the corresponding curve has a K-rational point. Thus $Ш(E,K)$ measures the obstruction to a local global principle. However the geometric interpretation is used only occasionally in this thesis. All this material is explained in detail in chapter one.

The Tate-Shafarevich group is shrouded in mystery. It is conjectured to be finite, for all E and K. While it is clear from the exact sequence that $Ш(E,K)[\ell]$ is finite for all ℓ, the conjecture is very hard to verify even for a fixed elliptic curve. And it would be almost as hard to verify that a given element in a given $Ш(E,K)$ is not infinitely divisible in the group. No example of a Tate-Shafarevich group had been calculated (provably) until the mid 1980s, when Karl Rubin made the breakthrough. Now $Ш(E,\mathbb{Q})$ can be computed for many elliptic curves by Kolyvagin's method (the proof of which rests on, among other things, the fact that elliptic curves over $\mathbb{Q}$ are modular, proved by Wiles, Taylor, Breuil, Conrad and Diamond). The quest for better information about Tate-Shafarevich groups is a focal point of current research in arithmetic geometry, and perhaps the strongest motivation is the conjecture of Birch and Swinnerton-Dyer. The order of $Ш(E,K)$ appears in the strong form of their conjecture, which bears a clear analogy to the class number formula under which the Tate-Shafarevich group corresponds to the class group.

Given the difficulty of getting solid information about Ш, researchers take an active interest in Selmer groups too. There is work on their sizes, sometimes on average, and on how to best compute them. In this thesis we primarily study Selmer

groups, as a means for finding interesting Tate-Shafarevich groups. There are basically two ways to detect nontrivial elements in Ш, and both involve comparing two different Selmer groups. The first is to use 'second descent', and this approach is illustrated in Section 1.4. The other idea is simply to do descent with two separate isogenies defined on E, say

$$E \xrightarrow{[2]} E \text{ and } E \xrightarrow{[\ell]} E\,.$$

One bounds $\mathrm{Sel}^{(2)}(E,K)$, thereby bounding the number of generators in $E(K)$ (since the torsion is bounded anyway). If $\mathrm{Sel}^{(\ell)}(E,K)$ turns out to be bigger than that bound then some of its elements must map to nontrivial elements of $Ш(E,K)[\ell]$. This is roughly our strategy in chapter 5, which presents a method for producing 7-torsion elements in the Tate-Shafarevich groups of curves over quadratic fields. In order to calculate the Selmer groups we choose to use isogenies of prime degree, even though this severely restricts which curves, and which values of ℓ, we can consider. (Just as Mazur's and Kamienny's theorems limit the possible orders of K-rational torsion points on elliptic curves to a finite list, the possible degrees of K-rational isogenies are likewise limited.) In the end one also needs to assume a technical arithmetic hypothesis to prove that the method succeeds infinitely often. The latter part of the chapter is devoted to a discussion of this hypothesis from various points of view. For more detail about exactly what is proved, see the introduction to chapter five.

Preliminary to such an undertaking, one needs to be able to accurately describe Selmer groups for the isogenies one is considering, and perhaps to do it systematically for a family of curves. This is done in chapter 3, where an explicit description is given for a certain class of isogenies of prime degree, working over any ground field. This generalises one of the main results in Fisher's thesis ([Fi], Cambridge, 2000), and the method of proof is different.

As it turns out we do not use the result in chapter 3 for our construction in chapter 5 because it is more convenient to use an old result of Cassels. In chapter 2 we explain the main ideas in Cassels argument in some detail, as well as presenting some other standard machinery.

Chapter 4 is also preparatory for chapter 5; we explicitly produce a model for the moduli space $X_0(14)$ with certain properties that are needed in the application. Our method takes advantage of the theories of complex multiplication and of modular forms.

Guide to the reader

Chapter One, mainly on descent on elliptic curves: The material on elliptic curves over local fields is intended for reference only. It is probably fruitful for anyone to start by reading the section on descent, up to where it discusses the geometric interpretation (which is not crucial for understanding most of the thesis). The example (Section 1.3) is illuminating and easy to skim, while the construction of Ш[2] (Section 1.4) is not very important.

Chapter Two, on algebraic machinery: One need not read this if one is prepared to take for granted the results when they are used later. The section on the Weil pairing may be of interest as it gives a point of view slightly different from Silverman's book.

Chapter Three, on calculating Selmer groups: this will be interesting to one who is curious about what data suffices to determine the Selmer conditions. The substance lies in several local calculations that are similar to each other, so one might for instance choose to study the proof of Lemma 3.3.1 carefully but just read the statements of everything else.

Chapter Four: the only thing to be used later is the result, which is a model for $X_0(14)$. The details of how it is found are probably of interest only to a specialist in

modular curves. However the introduction allows the reader to appreciate how the method works.

Chapter Five, constructing nontrivial $Ш(E, K)[7]$: the reader is invited to follow the steps in the construction by reading the statements of the lemmas and skipping their proofs. The discussion of the arithmetic hypothesis towards the end is of a different flavor to the rest, and might be appealing; the most interesting part to look at is probably the numerical data.

Chapter 1

Background on elliptic curves

1.1 Elliptic curves over local fields

This section rather tersely records standard facts for future reference, omitting proofs that are provided in Silverman's books [Si1] and [Si2]. Throughout this section $K_v/\mathbf{Q}_p$ will be a nonarchimedean local field with residue field k_v, and E will be an elliptic curve defined over K_v.

1.1.1 Reduction

When one writes down an explicit equation for an elliptic curve, it is usually in Weierstrass form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,.$$

The *discriminant* of E, $\Delta(E)$ is an integral polynomial in $a_1, \ldots, a_6$ defined in [Si1], Section III.1. The above equation is a model of some elliptic curve if and only if the equation is nonsingular, which holds if and only if $\Delta(E) \neq 0$. The discriminant is not an isomorphism invariant of E, but depends on the choice of model.

Definitions. A *minimal model of E at v* is a Weierstrass equation for E with coefficients $a_1, \ldots, a_6$ in the ring of integers $\mathfrak{O}_v$, and with $\operatorname{ord}_v \Delta(E)$ as small as possible. The *reduction of E at v*, denoted $\tilde{E}$, is the curve over k_v obtained by reducing the coefficients of a minimal model of E.

See [Si1], Section III.1 for the general form of a transformation between different Weierstrass models of the same curve E, which makes it clear that the reductions obtained via two different minimal models are isomorphic over k_v. Throughout this section we assume E is given by a minimal model.

When $\mathrm{ord}_v\,\Delta(E) = 0$, the reduction is an elliptic curve over k_v, the group law continues to hold, and reduction induces a homomorphism between the groups of rational points $E(K_v)$ and $E(k_v)$. In this case we say E has 'good reduction at v'.

Otherwise we say E has 'bad reduction', and it turns out there is just one singular point on $\tilde{E}$. One defines $\tilde{E}_{\mathrm{ns}}$ to be the affine variety over k_v obtained by omitting the singular point. The group law on E reduces to a group law on $\tilde{E}_{\mathrm{ns}}$. There are three possible types of bad reduction (for more information and proofs, see [Si1], section VII.5):

1. *Additive* reduction, when the singular point is a cusp. Then $\tilde{E}_{\mathrm{ns}} \cong \mathbf{G}_a$ as group varieties and $\tilde{E}_{\mathrm{ns}}(k_v)$ is a group of exponent p.

2. *Split multiplicative* reduction, when the singular point is a node (two branches of the curve crossing transversally) and the two tangent directions are defined over k_v. Then $\tilde{E}_{ns} \cong \mathbf{G}_m$ as group varieties, and so $\tilde{E}_{\mathrm{ns}}(k_v) \cong k_v^{\times}$ which is a cyclic group of order $\#k_v - 1$.

3. *Nonsplit multiplicative* reduction, when the singular point is a node and the tangent directions are not defined over k_v: they are distinct over $\overline{k_v}$, so they must be defined over the quadratic extension $\mathbb{F}/k_v$, and so the curve has split multiplicative reduction over $\mathbb{F}$, or equivalently over the unique unramified quadratic extension L_v/K_v. Over k_v, $\tilde{E}_{\mathrm{ns}}$ is the quadratic twist by $\mathbb{F}$ of $\mathbf{G}_m$. Therefore $\tilde{E}_{\mathrm{ns}}(\mathbb{F}) \cong \mathbb{F}^{\times}$ and the subgroup $\tilde{E}_{\mathrm{ns}}(k_v)$ equals the kernel of the norm $\mathrm{N}_{\mathbb{F}/k_v}$ on $\mathbb{F}^{\times}$, which is a cyclic group of order $\#k_v + 1$. Concretely, the twist

of $\mathbf{G}_m$ by $\mathbb{F} = k_v(\sqrt{d})$ is given by the Pell curve $x^2 - dy^2 = 1$, where d is any nonsquare element of $k_v^\times$.

Good and split multiplicative reduction are called 'stable' because when the ground field is extended, a minimal model remains minimal and the reduction type does not change.

Next we state the 'Weil bounds' on the number of points on an elliptic curve over a finite field, which assert that the number is close to the expected number with a square root error term. Actually Weil proved bounds for an arbitrary curve; the case of genus one is older, proved by Hasse in the 1930s.

1.1.1 Theorem. *Let E be a curve defined over k_v, with genus one. Then*

$$|\#E(k_v) - (\#k_v + 1)| \leq 2\sqrt{\#k_v}\,.$$

In particular, every curve of genus one over a finite field has a rational point over that field.

Proof: See [Si1], Theorem V.1.1. The second assertion follows by simple arithmetic from the lower bound.

The Weil bounds will help us prove the following useful fact.

1.1.2 Proposition. *Curves that are isogenous over a number field have the same type of reduction at each prime (the possible types being good, split mulitiplicative, nonsplit multiplicative and additive), and have the same number of points over each residue field.*

Proof: Isogenous curves have the same conductor, which determines the reduction type as good, multiplicative or additive. Consider the dual isogenies $\phi : E \to E'$ and $\phi' : E' \to E$. Suppose by way of contradiction that E has split reduction at v while E' has nonsplit reduction. Let $m = \deg \phi = \deg \phi'$, so $\phi' \circ \phi = [m]$. We know

that the reduction of E' will become split over a quadratic extension (unramified at v) but remains nonsplit over any L/K of odd degree, unramified at v. Denote the residue fields by k_w/k_v and let $\#k_v = q$, so that $\#k_w = q^n$ for some odd n. On the reduction, ϕ maps $\tilde{E}_{ns}(k_w) \to E'_{ns}(k_w)$, and these are cyclic groups of orders $q^n - 1$ and $q^n + 1$. However $\#E[\phi] \mid m$, so we must have $q^n - 1 \mid m(q^n + 1)$, which is absurd when n becomes large.

When the curves have additive reduction, $\#\tilde{E}_{\mathrm{ns}}(k_v) = \#k_v = \#E'_{\mathrm{ns}}(k_v)$ (counting the point at infinity). It remains to prove that $\#\tilde{E}(k_v) = \#\tilde{E}'(k_v)$ in the case of good reduction. The idea is similar to the multiplicative case in the previous paragraph. Put $m = \#\tilde{E}'(k_v)/\#\tilde{E}(k_v) \in \mathbb{Q}$ and suppose without loss that $m > 1$. Then

$$\#\left(\tilde{E}'(k_v)/\phi\tilde{E}(k_v)\right) = m\,\#\tilde{E}(k_v)[\phi]\,,$$

We will make a large extension of k_v which preserves the discrepancy, and this will contradict the Weil bounds. Choose coset representatives P_i for $\tilde{E}'(k_v)/\phi\tilde{E}(k_v)$, and let $\mathcal{S} = \{P_i - P_j : i \neq j\}$. Then the preimage $\phi^{-1}\mathcal{S}$ in $E(\overline{k_v})$ is a finite set that does not intersect $\tilde{E}(k_v)$. Let $\mathbb{F}$ be a finite extension of k_v large enough that $E(\mathbb{F})$ contains both $\phi^{-1}\mathcal{S}$ and $E(\overline{k_v})[\phi]$. Now, for a prime p not dividing the degree of $\mathbb{F}/k_v$, take $\mathbb{F}'/k_v$ to be the extension of degree p. Then $\mathbb{F} \cap \mathbb{F}' = k_v$, so $E(\mathbb{F}')$ does not intersect $\phi^{-1}\mathcal{S}$ and $E(\mathbb{F}')[\phi] = \tilde{E}(k_v)[\phi]$. Hence the $P_i \in E'(\mathbb{F}')$ are in different cosets of $\phi E(\mathbb{F}')$, so

$$\#\left(E'(\mathbb{F}')/\phi E(\mathbb{F}')\right) > \#\left(\tilde{E}'(k_v)/\phi\tilde{E}(k_v)\right) = m\,\#\tilde{E}(k_v)[\phi] = m\,\#E(\mathbb{F}')[\phi]$$

and hence $\#E'(\mathbb{F}') > m\,\#E(\mathbb{F}')$. But this is impossible for large p because according to the Weil bounds (Theorem 1.1.1) $\#E'(\mathbb{F}')/\#E(\mathbb{F}')$ tends to 1 as $\#\mathbb{F}'$ tends to infinity.

1.1.2 The structure of $E(K_v)$

In close analogy with the structure of $K_v^\times = \mathbf{G}_m(K_v)$, there is a filtration

$$E(K_v) \supset E_0(K_v) \supset E_1(K_v) \supset \cdots \supset E_n(K_v) \supset \ldots$$

defined as follows. Assume E is given by a minimal Weierstrass model at v. Then $E_0(K_v)$ consists of those points that reduce to nonsingular points of $E(k_v)$, $E_1(K_v)$ those points that reduce to the identity in $\tilde{E}_{\mathrm{ns}}(k_v)$, and more generally $E_n(K_v)$ those points that are congruent to the identity modulo (π_v^n). Here π_v denotes a uniformiser for v (an element of K_v with valuation 1).

Clearly these are subgroups of finite index. Define $c_v(E) := \#(E(K_v)/E_0(K_v))$. If E has good reduction at v then by definition $E(K_v)/E_0(K_v)$ is trivial, and $c_v(E) = 1$. In chapter 3 we will make frequent use of the following facts (for proofs see [Si1], Theorem VII.6.1):

1. If E has *split multiplicative* reduction, then $E(K_v)/E_0(K_v)$ is a cyclic group, and $c_v(E) = \mathrm{ord}_v\Delta(E)$

2. If E has *nonsplit multiplicative* reduction, then $c_v(E) = 1$ or 2.

3. If E has *additive* reduction, then $c_v(E) \leq 4$.

From the definitions one sees that $E_0(K_v)/E_1(K_v) \cong E_{ns}(k_v)$.

If $K_v/\mathbb{Q}_p$, $E_1(K_v)$ is a pro p-group, called the 'formal group' of E. In particular any isogeny of degree prime to p must restrict to an isomorphism on $E_1(K_v)$. For sufficiently large n, one may define a 'formal logarithm map' from $E_n(K_v)$ to the additive group $\mathfrak{O}_v^+$. See [Si1], chapter IV for more about this.

For a curve with stable reduction, $E_0(K_v) = E_0(\overline{K_v}) \cap E(K_v)$ since a minimal model remains minimal over $\overline{K_v}$.

From the preceding considerations we deduce a simple fact which has far reaching consequences, as we will see in Section 1.2.

1.1.3 Proposition. *Suppose E is an elliptic curve over K_v with good reduction at v. Suppose further that $E[n] \subset E(K_v)$. Then $E[n]$ injects into $E_0(K_v)/E_1(K_v) = E(k_v)$.*

1.1.3 Tate uniformisations

When E has multiplicative reduction over K_v, there is a description of $E(K_v)$ in analogy with the Weierstrass uniformisation over the complex numbers

$$\mathbb{C}/\langle 1, \tau \rangle \cong \mathbf{C}(E)\,.$$

Note that this could equivalently be expressed $\mathbb{C}^\times/q^{\mathbb{Z}} \cong \mathbb{C}(E)$ where $q = e^{2\pi i\tau}$. There is an analog of this for curves over K_v.

1.1.4 Theorem. *1. Suppose E has split multiplicative reduction at v. Then there exists a unique $q \in K_v$ with $ord_v\, q > 0$ such that*

$$K_v^\times/q^{\mathbb{Z}} \cong E(K_v)\,. \tag{1.1}$$

2. Conversely, for any $q \in K_v$ with $ord_v\, q > 0$, there is an elliptic curve

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

over K_v with split multiplicative reduction, such that $K_v^\times/q^{\mathbb{Z}} \cong E(K_v)$.

For a proof and more discussion see Section V.3 in [Si2]. The uniformisation (1.1) expresses the Weierstrass coordinates x and y as quotients of v-adic power series that converge for all $z \in K_v^\times$ outside $q^{\mathbb{Z}}$. We need $|q|_v < 1$ so that these power series converge; this corresponds in the case over $\mathbf{C}$ to the requirement that τ be in the upper half plane, so that $q = e^{2\pi i\tau}$ has $|q| < 1$.

In the second statement, $a_4(q)$ and $a_6(q)$ are power series in q which converge for $|q| < 1$. When one substitutes these series into the formulas giving the discriminant

and j-invariant of the curve in terms of the coefficients of E, one recovers the familiar q-expansions

$$\Delta(E_q) = q\prod_{n\geq 1}(1-q^n)^{24}$$

$$j(E_q) = \frac{1}{q} + 744 + 196844q + \dots$$

that hold in the complex analytic picture when q stands for $e^{2\pi i\tau}$. One difference is that over K_v there is a convergent power series inverting the function $j(q)$, expressing q as a continuous function of j. Thus there is a bijection between j-invariants and values of q. As a consequence, two curves defined over K_v having split multiplicative reduction are isomorphic over $\overline{K_v}$ if and only if they are isomorphic over K_v.

An important feature of the v-adic case is that the Tate uniformisation is Galois invariant, since an element of the Galois group may be applied to a convergent power series term by term.

For a Tate curve, the standard filtration can be written in a very natural way:

$$\begin{array}{ccccc} E(K_v) & \supset & E_0(K_v) & \supset & E_1(K_v) \\ \| & & \| & & \| \\ K_v^\times/q^{\mathbb{Z}} & \supset & O_v^\times & \supset & 1+(\pi_v)O_v \end{array}$$

At the top step of the filtration, one sees $E(K_v)/E_0(K_v)$ is cyclic of order $\operatorname{ord}_v q$. We asserted above that it is cyclic of order $\operatorname{ord}_v \Delta(E)$, implying that $\operatorname{ord}_v q = \operatorname{ord}_v \Delta(E)$. At the middle step, $E_0(K_v)/E_1(K_v) \cong k_v^\times$ as we already know. At the bottom step, the formal group equals the multiplicative formal group.

Isogenies

The Tate uniformisation implies that a curve over K_v with split multiplicative reduction has a K_v-rational isogeny of degree n for all n, because $E[n]$ has a distinguished cyclic subgroup:

$$\mu_n = \langle \zeta_n \rangle \subset \langle \zeta_n, q^{1/n} \rangle = E[n]\,.$$

We already showed in Proposition 1.1.2 that if a curve has split multiplicative reduction, then all isogenous curves do too. Using the Tate uniformisations for both curves, one sees there are only two kinds of isogeny with prime degree ℓ, because the kernel is either μ_ℓ or it is generated by some ℓth root of q. In other words, up to composition with an automorphism (multiplication by an element of $\mathfrak{O}_v^\times$), an isogeny must be either

$$K_v^\times/q^{\mathbb{Z}} \to K_v^\times/q^{\ell\mathbb{Z}} \quad \text{or} \quad K_v^\times/q^{\ell\mathbb{Z}} \to K_v^\times/q^{\mathbb{Z}}\,.$$

Clearly these are dual, their composite being $[\ell]$. The first kind is always defined over the ground field, for every Tate curve and every ℓ. This proves the following.

1.1.5 Lemma. *Let $K_v/\mathbb{Q}_\ell$ be a local field. Suppose E is an elliptic curve over K_v that has split multiplicative reduction. Then E has an isogeny $\phi : E \to E'$ of degree ℓ defined over K_v. If ϕ' denotes the dual isogeny, then $E[\phi] \subset E_0(K_v^{un})$ if and only if $E'[\phi'] \nsubseteq E_0'(K_v^{un})$.*

The last statement makes sense because a minimal model remains minimal over unramified extensions of the ground field (this holds for all types of reduction).

Nonsplit multiplicative reduction

Now suppose E has nonsplit multiplicative reduction. As noted in Section 1.1.1, it acquires split reduction over the unramified quadratic extension L_v/K_v. Therefore $E(L_v) \cong L_v^\times/q^{\mathbb{Z}}$ where q must in fact lie in K_v, not just in L_v. Moreover the subgroup $E(K_v)$ is isomorphic to the kernel of the norm N_{L_v/K_v} on $L_v^\times/q^{\mathbb{Z}}$.

As a consequence, $\#E(K_v)/E_0(K_v) \leq 2$.

1.2 Descent on Elliptic Curves

One of the central problems in the theory of elliptic curves is, given a curve $E/\mathbb{Q}$, how to determine the group of points with rational coordinates, denoted $E(\mathbb{Q})$.

1.2.1 Theorem. *(Mordell, Weil) For any elliptic curve E defined over a number field K, the set of K-rational points $E(K)$ is a finitely generated abelian group.*

Mordell proved this for $K = \mathbb{Q}$ in 1922, and in 1928 Weil extended the argument to work over any number field, and also for an arbitrary abelian variety instead of an elliptic curve.

Next arises the question of how to effectively compute the 'Mordell-Weil' group $E(K)$, and this remains unsolved, even in the case $K = \mathbb{Q}$. The standard method is based on the proof of the Mordell-Weil theorem, and is known as 'descent' because it is a twentieth century reincarnation of Fermat's method of descent. To explain the method, we give the first half of the proof of the Mordell-Weil theorem, showing that $E(K)/nE(K)$ is finite for any integer $n > 1$, a fact also known as the 'weak Mordell-Weil theorem'. This is the Galois theoretic half of the proof. It is the second half which goes by 'infinite descent': one deduces from the first half that $E(K)$ is finitely generated by showing that given a chain of points in $E(K)$, each dividing the one before, the heights of the points decrease in such a way that the chain must eventually terminate.

Proof of the weak Mordell-Weil theorem: Given a point $P \in E(K)$, consider any preimage $Q \in E(\overline{K})$ with $nQ = P$. The coordinates of Q lie in some finite extension of K, denoted $K(Q)$. The following property of $K(Q)$ will be the key to our proof.

1.2.2 Lemma. *In the preceding notation, the extension $K(Q)/K$ is unramified at all finite primes of K except possibly those dividing n and those where E has bad reduction.*

Proof: Suppose $\mathfrak{p}$ is a prime not excluded by the lemma, and choose an extension of $\mathfrak{p}$ to $\overline{K}$, still denoted $\mathfrak{p}$. Then E has good reduction at $\mathfrak{p}$, and good reduction is stable, meaning a minimal model for E at $\mathfrak{p}$ will continue to be minimal over the algebraic closure. Now suppose that $K(Q)$ is ramified at $\mathfrak{p}$; then there are two conjugates

Q and σQ that reduce to the same point of $E(\overline{k_\mathfrak{p}})$. Hence $\sigma Q - Q$ reduces to the identity O in $E(\overline{k_\mathfrak{p}})$. But $\sigma Q - Q$ is a nontrivial element of $E[n]$, so this contradicts Proposition 1.1.3, proving the lemma.

Resuming our proof, note that the set of exceptional primes in the lemma is finite. A standard theorem in number theory asserts that there are only finitely many extensions of fixed degree over K that are unramified outside a fixed, finite set of primes. Equivalently, the composite of all such extensions has finite degree. Therefore in our situation, there exists a finite extension L/K determined by E and n alone, with the property that for all $P \in E(K)$, each preimage Q lies in $E(L)$. It will be convenient to codify the Galois action on Q as a map $\sigma \mapsto \sigma Q - Q$. This maps $\mathrm{Gal}(L/K)$ to $E[n]$, the set of n torsion points in $E(\overline{K})$, since $n(\sigma Q) = \sigma(nQ) = P = nQ$. Each $P \in E(K)$ gives rise to such a map, or perhaps several since the map may depend on the choice of Q. In any case, there are only finitely many possible maps since $\mathrm{Gal}(L/K)$ and $E[n]$ are both finite. Now suppose P_1 and P_2 give rise to the same map, that is to say $\sigma Q_1 - Q_1 = \sigma Q_2 - Q_2$ for all $\sigma \in \mathrm{Gal}(L/K)$. Rearranging, $\sigma(Q_1 - Q_2) = Q_1 - Q_2$, which means $Q_1 - Q_2 \in E(K)$. But then $P_1 - P_2 \in nE(K)$. This shows $E(K)/nE(K)$ is finite, proving the weak Mordell-Weil theorem.

1.2.1 Descent with Galois cohomology

The preceding discussion can be expressed more systematically in the language of group cohomology. For descent one needs only the 0th and 1st cohomology groups, so we give a down-to-earth definition of them. See [Si1] (Appendix A) for more information in the same low-tech style. For us the group G will always be $G_K = \mathrm{Gal}(\overline{K}/K)$, and the abelian group M may be $E(\overline{K})$, $\overline{K}^\times$ or $\mu_n \subset \overline{K}^\times$, for instance. While doing cohomology one always writes the group operation on M additively, no matter how it is normally written.

Definitions. Suppose G is a group and M is an abelian group on which G acts. Then

$$\mathrm{H}^0(G,M) = M^G = \{m \in M : \sigma m = m \ \ \forall\ \sigma \in G\}$$
$$\mathrm{H}^1(G,M) = \frac{\{1\text{-cocycles}\}}{\{1\text{-coboundaries}\}} = \frac{\{\zeta \in \mathrm{Maps}(G,M) : \zeta(\sigma\tau) = \zeta(\sigma) + \sigma\zeta(\tau)\}}{\{\zeta : \zeta(\sigma) = \sigma m - m \text{ for some } m \in M\}}$$

The group operation on $\mathrm{H}^1(G,M)$ is pointwise addition of maps, using the group operation on M.

We continue to discuss the maps arising in the proof of the weak Mordell-Weil theorem, now replacing the isogeny $[n] : E \to E$ by a general isogeny $\phi : E \to E'$ defined over K. (More precisely this means E and E' are defined over K and ϕ can be written in terms of rational functions with coefficients in K.) Consider the map $G_K \to E[\phi] : \sigma \mapsto \sigma Q - Q$, where $\phi(Q) = P \in E'(K)$. One easily checks that it satisfies the cocycle property, so it represents an element of $\mathrm{H}^1(G_K, E[\phi])$, and it represents the trivial element in $\mathrm{H}^1(G_K, E)$: it is a coboundary with respect to $E(\overline{K})$ because $Q \in E(\overline{K})$. Moreover for fixed P and two different choices of preimage $Q, Q' \in \phi^* P$, the difference between the associated cocycles is

$$\sigma \mapsto \sigma Q - Q - (\sigma Q' - Q') = \sigma(Q - Q') - (Q - Q')$$

which is a 1-coboundary with respect to $E[\phi]$ because $Q - Q' \in E[\phi]$. Thus we have a well defined map $E'(K) \to \mathrm{H}^1(G_K, E[\phi])$ sending P to the cocycle $\sigma \mapsto \sigma Q - Q$, and this is clearly a homomorphism of abelian groups. The kernel is $\phi E(K)$, for if $\sigma \mapsto \sigma Q - Q$ equals a coboundary $\sigma \mapsto \sigma R - R$, where $\phi(R) = O$, then $\sigma(Q - R) = Q - R$ so $Q - R$ is K-rational and $P = \phi(Q - R) \in \phi E(K)$. The sequence below is exact, as we have shown except for the surjectivity:

$$0 \to E'(K)/\phi E(K) \to \mathrm{H}^1(G_K, E[\phi]) \to \mathrm{H}^1(G_K, E)[\phi] \to 0\,. \tag{1.2}$$

In this context E is shorthand for $E(\overline{K})$, just as $E[n]$ always means $E(\overline{K})[n]$. To prove the surjectivity, let $\zeta \in \mathrm{H}^1(G_K, E)[\phi]$, which means $\phi \circ \zeta$ is a coboundary

$\sigma R - R$, where $R \in E(\overline{K})$. It suffices find another cocycle cohomologous to ζ that takes values in $E[\phi]$. So we must find a coboundary $\sigma S - S$, where $S \in E(\overline{K})$, such that $\zeta(\sigma) - (\sigma S - S)$ is in $E[\phi]$ for all $\sigma \in G_K$. But this is trivial: for any $S \in \phi^{-1}R$,

$$\phi(\zeta(\sigma) - (\sigma S - S)) = \sigma R - R - (\sigma\phi(S) - \phi(S)) = 0$$

as required, where $\phi(\sigma S) = \sigma\phi(S)$ holds because ϕ is defined over K.

There is a geometric interpretation of (1.2), in which $\mathrm{H}^1(G_K, E)$ classifies the set of curves of genus 1 whose jacobian is E. We defer presenting this until the end of our account of descent, because it is not necessary for understanding most of this thesis (it is used only in Example 1.4 in this chapter, and in the proof of Proposition 2.3.2, but not in chapters 3,4 or 5).

One can also obtain (1.2) from more general principles, as follows. Start with the exact sequence

$$0 \longrightarrow E[\phi] \longrightarrow E(\overline{K}) \xrightarrow{\phi} E'(\overline{K}) \longrightarrow 0$$

Take the associated long exact sequence of cohomology groups; since $\mathrm{H}^0(G_K, -)$ is the fixed point functor, the long exact sequence is

$$\begin{aligned} 0 \longrightarrow\ & E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K) \longrightarrow \\ \longrightarrow\ & \mathrm{H}^1(G_K, E[\phi]) \longrightarrow \mathrm{H}^1(G_K, E) \xrightarrow{\phi} \mathrm{H}^1(G_K, E') \longrightarrow \ldots \end{aligned}$$

where ϕ induces a map on cocycles by composition. By suitably truncating the long exact sequence one recovers (1.2).

Kummer Theory

Kummer theory is essentially the same construction with E replaced by $\mathbf{G}_m$; the result is a cohomology group that classifies Kummer extensions. This will be used heavily in later chapters.

Start with the exact sequence

$$0 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{\times n} \overline{K}^\times \longrightarrow 0$$

where μ_n denotes the set of nth roots of unity. Taking cohomology one obtains the long exact sequence

$$\begin{aligned} 0 \longrightarrow \quad \mu_n(K) \quad &\longrightarrow \quad K^\times \quad \xrightarrow{\times n} K^\times \longrightarrow \\ \longrightarrow \mathrm{H}^1(G_K, \mu_n) &\longrightarrow \mathrm{H}^1(G_K, \overline{K}^\times) \longrightarrow \ \ldots \end{aligned}$$

But $\mathrm{H}^1(G_K, \overline{K}^\times)$ is trivial, a standard fact known as Hilbert's Theorem 90 (see [Si1], Appendix A). So $\mathrm{H}^1(G_K, \mu_n) \cong K^\times / K^{\times n}$, which in some sense classifies nth root extensions of K. The 'Kummer map' $K^\times / K^{\times n} \to \mathrm{H}^1(G_K, \mu_n)$ can also be defined (and shown to be an isomorphism) directly as follows:

$$\alpha \mapsto \frac{\beta^\sigma}{\beta} \text{ where } \beta^n = \alpha$$

in complete analogy with the map $E(K)/nE(K) \to \mathrm{H}^1(G_K, E[n])$.

1.2.2 Finding the Mordell-Weil group

Lemma 1.2.2, which was the origin of the finiteness in the Mordell-Weil theorem, suggests a strategy which in some cases will determine $E(K)$. Take $\phi = [n]$. Find an explicit description of $\mathrm{H}^1(G_K, E[n])$, and identify the finite subgroup of 'good cocycles', those that are unramified except at primes dividing n or where E has bad reduction. Then search for points in $E(K)$, not stopping until their images generate the 'good cocycles', in which case the points generate $E(K)/nE(K)$. In practice it is then not too difficult to find generators for $E(K)$. But the strategy doesn't work when there are good cocycles not in the image of $E(K)/nE(K)$; in such cases one would search in vain for ever, not being able to tell when all points in $E(K)/nE(K)$ had been found.

The standard method for computing Mordell-Weil groups is a refinement of this strategy, where in place of the 'good cocycles' one uses a smaller subgroup of $\mathrm{H}^1(G_K, E[\phi])$ that is still computable, the Selmer group $\mathrm{Sel}^\phi(E, K)$. The Selmer group will by definition be the closest approximation to the image of $E'(K)/\phi E(K)$ obtainable using local information, that is by doing calculations in completions of K. But we will see that in some cases local information is incapable of determining $E'(K)/\phi E(K)$, so even this refined strategy may fail.

To define $\mathrm{Sel}^\phi(E, K)$, note that the descent exact sequence (1.2) is valid for any field over which E is defined, for instance a completion K_v of K:

$$0 \to E'(K_v)/\phi E(K_v) \to \mathrm{H}^1(G_v, E[\phi]) \to \mathrm{H}^1(G_v, E)[\phi] \to 0 \tag{1.3}$$

where $G_v = \mathrm{Gal}(\overline{K_v}/K_v)$. Fixing an embedding of $\overline{K}$ into $\overline{K_v}$ determines an inclusion $G_v \hookrightarrow G_K$ (as the subgroup that fixes $K_v \cap \overline{K}$, the 'decomposition subgroup'). Thus it makes sense to restrict cocycles defined on G_K to G_v, and it is clear that coboundaries restrict to coboundaries. For each place v the restriction maps give rise to a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi E(K) & \longrightarrow & \mathrm{H}^1(G_K, E[\phi]) & \longrightarrow & \mathrm{H}^1(G_K, E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v} & & \downarrow{\scriptstyle \mathrm{res}_v} & & \\
0 & \longrightarrow & E'(K_v)/\phi E(K_v) & \longrightarrow & \mathrm{H}^1(G_v, E[\phi]) & \longrightarrow & \mathrm{H}^1(G_v, E)[\phi] & \longrightarrow & 0
\end{array}$$

We will now formally define the Selmer group to be the set of cocycles whose restrictions are in the 'local Mordell-Weil groups' for all places (including infinite places).

Definition. Given an elliptic curve E defined over a number field K and an isogeny defined over K, $\phi : E \to E'$ to another elliptic curve, the *Selmer group for ϕ over K* is $\mathrm{Sel}^\phi(E, K) := \{\zeta \in \mathrm{H}^1(G_K, E[\phi]) : \mathrm{res}_v\, \zeta \in \mathrm{Im}\, E'(K_v)/\phi E(K_v) \ \ \forall\ v\}$.

Given some explicit description of $\mathrm{H}^1(G_K, E[\phi])$, it is a finite computation to determine $\mathrm{Sel}^\phi(E, K)$. To explain this, we first translate Lemma 1.2.2 into the language we are now using.

Definitions. A G_v-module M is *unramified* if the inertia group $I_v \subset G_v$ acts trivially on M. For M unramified, we define $\mathrm{H}^1_{\mathrm{un}}(G_v, M)$ to be the subgroup $\mathrm{H}^1(G_v/I_v, M) \subset \mathrm{H}^1(G_v, M)$.

Remarks: $\mathrm{H}^1(G_v/I_v, M)$ is well defined because when M is unramified, the action of G_v factors through G_v/I_v. The inclusion is given by the inflation map on cocycles, which is clearly injective.

1.2.3 Lemma. *Suppose $\phi : E \to E'$ is an isogeny of elliptic curves defined over K. Suppose further that the curves have good reduction at v and that $v \nmid \deg \phi$. Then the image of $E'(K_v)/\phi E(K_v)$ lies in $\mathrm{H}^1_{un}(G_v, E[\phi])$.*

Proof: Same argument as Lemma 1.2.2.

In Proposition 2.3.2 will show that in fact the image of $E'(K_v)/\phi E(K_v)$ is exactly the set of unramified cocycles. So we know the Selmer condition imposed by 'good primes'. For each remaining place, one may determine the Selmer condition by calculating $E(K_v)$ in terms of the structure theory outlined in section 1.1 (or trivially for infinite places), and then finding the image of $E(K_v)$ in $\mathrm{H}^1(G_v, E[\phi])$. In many situations, one wants to use some sophistication in performing this step. For instance in chapter 3 we will do it theoretically for a moderately general class of isogenies, obtaining a clear description of the Selmer groups (which makes it very simple to give, say, a bound on the Mordell-Weil group for a given curve). Alternatively one may use Hensel's lemma to determine the Selmer condition at v, taking advantage of the geometric interpretation of the descent exact sequence.

The Tate-Shafarevich group of E encapsulates the obstructions to the method of 'descent by ϕ' successfully determining $E'(K)/\phi E(K)$, for every isogeny ϕ. It consists of those cocycles in $\mathrm{H}^1(G_K, E)$ that are 'locally trivial everywhere'.

Definition. Given an elliptic curve E defined over a number field K, the *Tate-Shafarevich group of E over K* is

$$Ш(E, K) := \{\zeta \in \mathrm{H}^1(G_K, E) : \mathrm{res}_v\ \zeta = 0 \quad \forall\ v\}\,.$$

For any $\zeta \in \mathrm{Sel}^\phi(E, K)$, $\mathrm{res}_v\,\zeta$ is in the kernel of the map induced by ϕ, by the exactness of (1.3). By the commutativity of the diagram, this means $\phi\,\zeta$ satisfies the definition of $Ш(E, K)$. Conversely for an element of $Ш(E, K)[\phi] \subset \mathrm{H}^1(G_K, E)[\phi]$, which must have a preimage in $\mathrm{H}^1(G_K, E[\phi])$, all preimages are in $\mathrm{Sel}^\phi(E, K)$. So inside the descent exact sequence (1.2), one has an exact sequence of finite groups

$$0 \to E'(K)/\phi E(K) \to \mathrm{Sel}^\phi(E, K) \to Ш(E, K)[\phi] \to 0$$

each term of which will interest us.

1.2.3 Geometric interpretation

Let us now describe the geometric interpretation of the descent exact sequence. It is easiest to start from the opposite point of view, considering an arbitrary curve of genus 1 defined over K and its jacobian. For any curve C defined over any field, one can construct a 'jacobian variety' $\mathrm{Jac}(C)$ algebraically, working over the ground field (see [Mi]); it is an abelian variety of dimension equal to the genus of the curve. By the construction, for any field F/K the F-rational points on $\mathrm{Jac}(C)$ are in one to one correspondence with $\mathrm{Pic}^0(C, F)$, the set of F-rational divisor classes on C. Hence for any chosen base point $P \in C(\overline{K})$, the map $R \mapsto (R) - (P)$ is an embedding of C into $\mathrm{Jac}(C)$ defined over $K(P)$, the field of definition of P. When C has genus one, $\mathrm{Jac}(C)$ is an elliptic curve defined over K, and the embedding is an isomorphism

over $\overline{K}$. There is a distinguished K-rational point on $\mathrm{Jac}(C)$ corresponding to the zero divisor, so there is an isomorphism $C \to \mathrm{Jac}(C)$ defined over K if and only if C has a K-rational point.

To define an action of $\mathrm{Jac}(C)$ on C note that by the Riemann-Roch theorem, given any divisor D of degree 1 on C, there is a unique point $P \in C(\overline{K})$ such that $D - (P) = 0$ in $\mathrm{Pic}^0(C)$. This yields a map $\mathrm{Jac}(C) \times C \to C$ (since adding the arguments gives a divisor of degree 1) which turns out to be K-rational, giving us a simple transitive group action of $\mathrm{Jac}(C)$ on C, making C a *principal homogeneous space* for C over K. Conversely one can show that if C is a principal homogeneous space for an elliptic curve E over K then $E \cong \mathrm{Jac}(C)$ over K.

The important point is that in this situation there is a $\overline{K}$-isomorphism $\lambda : E \cong C$ obtained by fixing $c \in C(\overline{K})$ and letting $\lambda(P) = P + c$, where $+$ denotes the action of E on C. If the isomorphism fails to be defined over K then it does not preserve the action of G_K. We will define a 1-cocycle that records the difference between the Galois actions; the corresponding element of $\mathrm{H}^1(G_K, E)$ then measures the obstruction to the existence of a K-isomorphism $E \cong C$. Let λ^σ denote $\sigma \circ \lambda \circ \sigma^{-1}$, the map obtained by applying σ to the coefficients of λ. Note that the composition $\lambda^{-1} \circ \lambda^\sigma : E \to E$ must equal τ_P, the 'translation by P' map, where $P \in E(\overline{K})$ is the unique point with $P + c = c^\sigma$. This gives us a map $G_K \to E(\overline{K}) : \sigma \mapsto P$, and one may check the map satisfies the cocycle property. Furthermore if the map is a coboundary then one may recover a K-isomorphism $E \cong C$. Thus $C \cong E$ over K if and only if the cohomology element corresponding to C is trivial.

There is an algorithmic procedure for starting with an element $\zeta \in \mathrm{H}^1(G_K, E)$ and producing a corresponding homogeneous space for E. The idea is that over $\overline{K}$ the function field $\overline{K}(C)$ equals $\overline{K}(E)$, but C as a curve over K is determined by the Galois action on $\overline{K}(C)$. Using ζ one defines a new action on $\overline{K}(E)$, namely

$\sigma \cdot f := \sigma f \circ \tau_{\zeta(\sigma)}$, giving a new curve C. (To actually compute C, compute $K(C)$ as the fixed points of the new action.)

This means we have a one to one correspondence between $\mathrm{H}^1(G_K, E)$ and the set of principal homogeneous spaces for E.

Now, if C is a principal homogeneous space with a K-rational point $c \in C(K)$, then λ will be a K-isomorphism sending the identity on E to c. Therefore a principal homogeneous space is trivial if and only if it has a K-rational point. There is no known algorithm for deciding whether this is the case, given arbitrary E and C. In fact for fixed E the problem is equivalent to finding the Mordell-Weil group $E(K)$. For given an element in a Selmer group, one could decide whether it is in the image of $E(K)$ if one could decide whether the corresponding homogeneous space has K-rational points.

1.3 Example: descent by isogenies of degree 2

Start with an elliptic curve in the simple Weierstrass form

$$E : y^2 = x(x-a)(x-b) \text{ for } a, b \in K \tag{1.4}$$

with $\Delta(E) = ab(a-b) \neq 0$. All points in $E[2]$ are K-rational, since the nontrivial 2-torsion points are $(0,0), (a,0)$ and $(b,0)$. Taking a quotient of E by any one of them would yield a K-rational isogeny of degree 2. Thus there are three ways to factor the isogeny $[2]$ as

$$E \xrightarrow{\phi} D \xrightarrow{\phi'} E\,.$$

Choosing $(0,0)$ to be the kernel of ϕ, it is possible to elegantly express the isogenies in the form

$$\begin{array}{c} C: \begin{cases} v^2 = x \\ u^2 = x - a \\ w^2 = x - b \end{cases} \\ \Big\downarrow{\scriptstyle \phi} \\ D: \begin{cases} v^2 = x \\ V^2 = (x-a)(x-b) \end{cases} \\ \Big\downarrow{\scriptstyle \phi'} \\ E: y^2 = x(x-a)(x-b) \end{array} \tag{1.5}$$

where C and D are elliptic curves and $C \cong E$ over K, and the maps are given by $V = uw$ and $y = vV$. Notice that the extension of function fields $K(D)/K(E)$ is obtained by adjoining a square root of $x \in K(E)$, and $K(C)/K(D)$ by adjoining a square root of $x - a$. Likewise the function field extension associated to any isogeny of elliptic curves is a Kummer extension, at least over $\overline{K}$, and the magic functions whose nth roots define the extension can be identified by their divisors. They are the same functions appearing in the role of 'f' in the definition of the Weil pairing (see section 2.2 for more on this).

Having described the isogenies explicitly, let us turn to descent. The Galois action on $E[\phi]$ and $D[\phi']$ is trivial, so the following groups are all the same:

$$\mathrm{H}^1(G_K, D[\phi']) = \mathrm{H}^1(G_K, \mathbb{Z}/2) = \mathrm{Hom}(G_K, \mathbb{Z}/2) = \mathrm{H}^1(G_K, \mu_2) = K^\times/K^{\times 2}$$

are in one to one correspondence with the set of quadratic extensions of K. Hence there is a map

$$E(K)/\phi' D(K) \to K^\times/K^{\times 2}\,.$$

By Lemma 1.2.3, the image consists only of cocycles unramified outside the set $\mathcal{S}$ of 'bad places' (those dividing 2, those where E has bad reduction, and for technical

reasons the infinite places). As one would surely guess, such cocycles correspond via Kummer theory to extensions of K that are unramified outside $\mathcal{S}$, the subgroup of $K^\times/K^{\times 2}$ classifying such extensions is contianed in the '$\mathcal{S}$-unit subgroup' generated by

$$\left\{\alpha \in K^\times : \operatorname{ord}_v \alpha \equiv 0 \mod 2 \ \ \forall\, v \notin \mathcal{S}\right\}.$$

This is a finite subgroup of $\mathrm{H}^1(G_K, D[\phi'])$ containing the Selmer group; in fact it is the subgroup obtained by imposing only the Selmer conditions from primes outside $\mathcal{S}$. To compute the Selmer group exactly one must find a way to check which elements satisfy the remaining conditions. The geometric interpretation presents a way to do that. Following the procedure sketched in section 1.2.3 for turning a cocycle into a principal homogeneous space, one finds that each $d \in K^\times/K^{\times 2}$ corresponds to the homogeneous space for D given by D_d below, and similarly each $(c,d) \in K^\times/K^{\times 2} \times K^\times/K^{\times 2} = \mathrm{H}^1(G_K, E[2])$ corresponds to the homogeneous space for $C \cong E$ given by $C_{c,d}$:

$$\begin{array}{c} C_{c,d}: \left\{\begin{array}{c} dv^2 = x \\ cu^2 = x - a \\ cdw^2 = x - b \end{array}\right. \\ \phi \big\downarrow \\ D_d: \left\{\begin{array}{c} dv^2 = x \\ dV^2 = (x-a)(x-b) \end{array}\right. \\ \phi' \big\downarrow \\ E: y^2 = x(x-a)(x-b) \end{array} \tag{1.6}$$

Here the first map is given by $V = cuw$ and the second by $y = dvV$. In general it is impossible to decide whether D_d or $C_{c,d}$ has a K-rational point. But it is routine to decide whether they have K_v-rational points, using Hensel's lemma, and that is equivalent to deciding whether the corresponding cocycle satisfies the Selmer condition at v. We do so in the next section, and we are even able to conclude

that some of the D_d's are nontrivial elements of $Ш(D, \mathbb{Q})$ (when a and b are chosen judiciously).

1.4 Tate-Shafarevich groups with many elements of order two

This section contains a very concrete construction of Tate-Shafarevich elements of order two, by means of 'second descent'. I worked this out as a warm up problem, and the proof turned out to look very similar to constructions made by other people, especially Ken Kramer's in [Kr].

We may rewrite the 2-to-1 covering maps $C_{c,d} \to D_d \to E$ from the previous section as

$$\begin{aligned} E &: \ y^2 = x(x-a)(x-b) \\ D_d &: \ dV^2 = (dv^2 - a)(dv^2 - b) \\ C_{c,d} &: \begin{cases} dv^2 - cu^2 = a \\ dv^2 - cdw^2 = b \end{cases} \end{aligned}$$

The first map is given by $v = v, V = uw/c$ and the second by $x = dv^2, y = vV/d$. The values $c = d = 1$ are special; $C_{1,1} \cong E$ over $\mathbb{Q}$, and D_1 is another elliptic curve over $\mathbb{Q}$. The maps $\phi : E \to D_1$ and $\phi' : D_1 \to E$ are isogenies of elliptic curves with $\phi' \circ \phi = [2]$. The D_d are the elements of $H^1(G_\mathbb{Q}, E'[\phi']) \cong \mathbb{Q}^\times/\mathbb{Q}^2$, and the $C_{c,d}$ are the elements of $H^1(G_\mathbb{Q}, E[2])$.

'Second descent' amounts to the following. The map

$$H^1(G_\mathbb{Q}, E[2]) \to H^1(G_\mathbb{Q}, E'[\phi'])$$

induced by ϕ is given by $C_{c,d} \mapsto D_d$. The subgroup $\mathrm{Sel}^2(E, \mathbb{Q})$ maps into $\mathrm{Sel}^{\phi'}(E', \mathbb{Q})$, since if $C_{c,d}$ is locally solvable over all completions of $\mathbb{Q}$ then so is D_d. On the other

hand, the Kummer maps form a commutative diagram

$$\begin{array}{ccc} E(\mathbb{Q})/2E(\mathbb{Q}) & \longrightarrow & \mathrm{Sel}^2(E,\mathbb{Q}) \\ \downarrow & & \downarrow \\ E(\mathbb{Q})/\phi' E'(\mathbb{Q}) & \longrightarrow & \mathrm{Sel}^{\phi'}(E',\mathbb{Q}) \end{array}$$

so if D_d is in the image of the Kummer map then it is also in the image of $\mathrm{Sel}^2(E,\mathbb{Q})$. Turning this around, if D_d is not in the image of $\mathrm{Sel}^2(E,\mathbb{Q})$ then it must map to a nontrivial element of $Ш(E',\mathbb{Q})[2]$. One may verify that D_d is not in the image of $\mathrm{Sel}^2(E,\mathbb{Q})$ by checking that for every c, $C_{c,d}$ is not locally solvable over some completion. We will explain how to choose a and b so that there are as many such d as desired.

It clearly suffices to take c and d to be squarefree integers. And as explained in Section 1.3 it suffices to take c and d to be units away from bad primes, which in this case are those dividing $2ab(a-b)$. So for the rest of this section c and d will denote squarefree integers dividing $2ab(a-b)$.

We now analyse the local solvability of D_d; we will only need sufficient conditions for our construction.

1.4.1 Lemma. *Let D_d be given as above, where a and b are positive integers that are odd, squarefree, and coprime. Then*

1. *D_d has solutions over $\mathbb{R}$ if $d > 0$.*
2. *D_d has solutions over $\mathbb{Q}_2$ if $a \equiv b \mod 8$ and $d \equiv 1 \mod 8$.*
3. *For odd $p \mid ab$, D_d has solutions over $\mathbb{Q}_p$*
4. *For odd $p \mid a-b$, D_d has solutions over $\mathbb{Q}_p$ if $\left(\frac{d}{p}\right) = 1$.*

1.4.2 Sublemma. *Let A and B be integers, and p an odd prime with $p \nmid AB$. Then the equation $r^2 + As^2 = B$ has a solution modulo p with r and s nonzero* $\mod p$.

Remark: The sublemma is equivalent to the 'three units lemma' that arises in the theory of quadratic forms.

Proof of the Sublemma: The assertion is clear if B is a square modulo p, or if A and B are both nonsquare. In the remaining case, where A is a square and B is a nonsquare, let n be an integer such that $\left(\frac{n}{p}\right) = -1$ but $\left(\frac{n-1}{p}\right) = 1$. (There must be such an $n < p$ otherwise all integers are squares modulo p). Then we may choose r and s such that $r^2 = n - 1$ and $As^2 = 1$, yielding a solution to $r^2 + As^2 = n$. Since B/n is a square, there is then also a solution to $r^2 + As^2 = B$.

Proof of the Lemma: (i) is clear. For (ii), take v to be any multiple of 4; we can then solve for V over $\mathbb{Z}_2$ because $\frac{1}{d}(dv^2 - a)(dv^2 - b) \equiv ab \equiv a^2$ modulo 8, which means it is a square in $\mathbb{Z}_2$. For (iii), it suffices to consider $p \mid a$. In the case $p \nmid d$, Hensel's lemma tells us that D_d is solvable if it has a solution modulo p with v and V nonzero. Reducing modulo p it becomes $V^2 = v^2(dv^2 - b)$, and this has a such a solution, for by the sublemma $t^2 = dv^2 - b$ has a solution modulo p with t and v nonzero. In the case $p \mid d$, we can write $d = pD$ with $p \nmid D$ since d is assumed to be squarefree, and likewise $a = pA$. The equation becomes $DV^2 = (Dv^2 - A)(dv^2 - b)$, and again this is solvable if it has a solution modulo p with v and V nonzero. Reducing, it becomes $DV^2 = -b(Dv^2 - A)$, or equivalently $V^2 = -bv^2 + AbD$, and by the sublemma this has a solution of the required kind. For (iv), again it is enough find a solution modulo p with v and V nonzero. Modulo p, the equation becomes $dV^2 = (dv^2 - a)^2$, which has such a solution when $\left(\frac{d}{p}\right) = 1$.

We now give necessary and sufficient conditions for the local solvability of $C_{c,d}$ at odd primes. (For our construction, we will not need 2 or the infinite place, and we'll only use that the conditions are necessary.)

1.4.3 Lemma. *For an odd prime $p \mid ab(a - b)$, $C_{c,d}$ has solutions over $\mathbb{Q}_p$ if and only if the condition given below holds.*

p divides:	a	b	$a-b$
neither c nor d	$\left(\frac{c/d}{p}\right)=1$	$\left(\frac{c}{p}\right)=1$	$\left(\frac{d}{p}\right)=1$
c only	*not solvable*	*not solvable*	$\left(\frac{a/d}{p}\right)=1$
d only	*not solvable*	$\left(\frac{-a/c}{p}\right)=1$	*not solvable*
c and d	$\left(\frac{-cd/bp^2}{p}\right)=1$	*not solvable*	*not solvable*

The symmetry in the table arises from the symmetry in u, v and w, Accordingly, the proofs of the various cases follow a similar pattern.

Proof of representative cases: We pass to projective equations

$$dv^2 - cu^2 = az^2, \quad dv^2 - cdw^2 = bz^2$$

First we treat the case $p \mid b, p \nmid c, p \nmid d$. Suppose there is a solution to $dv^2 - cdw^2 = bz^2$. Note $\operatorname{ord}_p bz^2$ is odd while $\operatorname{ord}_p dv^2$ and $\operatorname{ord}_p cdw^2$ are even; since two of the terms must have the same valuation, it follows that $\operatorname{ord}_p dv^2 = \operatorname{ord}_p cdw^2 < \operatorname{ord}_p bz^2$. After dividing through by a power of p, we have $dv^2 - cdw^2 \equiv 0 \mod p$, hence $\left(\frac{c}{p}\right) = 1$ as stated by the lemma. Now suppose $\left(\frac{c}{p}\right) = 1$. The equation $dv^2 - cu^2 = az^2$ is a nonsingular conic over $\mathbb{F}_p$. By Sublemma 1.4.2 above, it has a solution over $\mathbb{F}_p$. Therefore it is isomorphic to $\mathbf{P}^1$ over $\mathbb{F}_p$, and has $p+1$ solutions. Since $p+1 > 2$, it has a solution with $v \neq 0$. By Hensel's lemma, this lifts to a solution over $\mathbb{Z}_p$ with $v \in \mathbb{Z}_p^\times$. We then obtain a point on $C_{c,d}$ by solving for $w \in \mathbb{Z}_p$, which is possible since the equation involving w reduces modulo p to $dv^2 - cdw^2 = 0$, and $\left(\frac{c}{p}\right)$=1.

Now we treat the case $p \mid b, p \mid c, p \nmid d$. Note $p \nmid a$. In $dv^2 - cu^2 = az^2$, $\operatorname{ord}_p cu^2$ is odd while $\operatorname{ord}_p dv^2$ and $\operatorname{ord}_p az^2$ are even, which implies $\operatorname{ord}_p dv^2 = \operatorname{ord}_p az^2$ and hence $\operatorname{ord}_p v = \operatorname{ord}_p z$. But in $dv^2 - cdw^2 = bz^2$, $\operatorname{ord}_p dv^2$ is even while $\operatorname{ord}_p cdw^2$ and $\operatorname{ord}_p bz^2$ are odd, which implies $\operatorname{ord}_p dv^2 > \operatorname{ord}_p bz^2$ and $\operatorname{ord}_p v > \operatorname{ord}_p z$, a contradiction.

We now give the construction of curves with Tate-Shafarevich groups having many elements of order two.

1.4.4 Theorem. *Fix a positive integer r.*

The following procedure yields infinitely many pairs (a, b). For any such pair $D_1 : V^2 = (v^2 - a)(v^2 - b)$ is an elliptic curve with $\#Ш(D_1, \mathbb{Q})[2] \geq 2^r$.

1. *Choose an integer k with $k < 0$ and $8 \mid k$.*

2. *Choose an odd prime a_1 with $a_1 \equiv 1 \mod k$ and $\left(\frac{k}{a_1}\right) = 1$*

3. *Choose an odd prime b_1 such that $\left(\frac{a_1}{b_1}\right) = -1$ and $\left(\frac{h}{b_1}\right) = 1$ for $h = -1$ and for each $h \mid k$.*

4. *Set $R = r + \#\{$ odd primes $\ell \mid k\} + 2$ and choose odd primes d_i for $1 \leq i \leq R$, each distinct from a_1 and with $\left(\frac{-k}{d_i}\right) = 1$*

5. *Find negative integers a', b' that are odd and coprime satisfying*

$$a'a_1 - b'b_1d_1 \dots d_R = k$$

Finally define $a = a'a_1$ and $b = b'b_1d_1 \dots d_R$.

Proof: We leave it to the reader to check that steps (2) thru (4) can be carried out for any choice of k satisfying (1). We now explain why in step (5) one may take a' and b' to be odd and coprime. To see this, start with any solution (a', b') to the equation; it is standard that there is a solution since a_1 is coprime to $b_1d_1 \dots d_R$. One may then pass to the alternative solution $(a' - b_1d_1 \dots d_R, b' - a_1)$. Doing this repeatedly, eventually one finds a solution with b' negative, odd, and prime to k (since a_1 is odd and prime to k). Then the corresponding a' is negative, odd, and coprime to b' (recall that $k < 0$ and $8 \mid k$).

We now prove that $\#Ш(D_1, \mathbb{Q})[2] \geq 2^r$, by showing that $D_d \in Ш(D_1, \mathbb{Q})[2]$ for any positive d satisfying the conditions

1. $a_1 \mid d$,

2. $d \mid a_1 d_1 \dots d_R$,

3. $d \equiv 1 \mod 8$ and

4. $\left(\frac{d}{\ell}\right) = 1$ for all odd $\ell \mid k$.

Such d exist, for instance $d = a_1$ works because $a_1 \equiv 1 \mod k$. Hence the set of such d has size at least 2^r. For such d, it's clear that D_d is locally solvable everywhere, since d satisfies all the conditions of Lemma 1.4.1, and $a - b = k \equiv 0 \mod 8$.

Now fix any such d. We must show that for each squarefree $c \mid ab(a-b)$, there is some place at which $C_{c,d}$ is not locally solvable. Note that $ab(a-b) = a'a_1b'b_1d_1 \dots d_R k$. First suppose c is divisible by some prime $p \neq a_1$ that divides a'. Then $p \mid a$, while $p \nmid d$ since it is clear from the equation in step (5) that a' is prime to each d_i, and $p \neq a_1$. Thus $C_{c,d}$ is not solvable at that p according to Lemma 1.4.3. Next suppose c is divisible by some prime p dividing $b = b'b_1d_1 \dots d_R$; then $C_{c,d}$ is not solvable at that p. It remains only to deal with those c that divide $a_1 k$. If c is *not* divisible by a_1, then $C_{c,d}$ is not solvable at a_1, since $a_1 \mid d$. On the other hand if $c = \pm a_1 h$ for some $h \mid k$, then $\left(\frac{c}{b_1}\right) = -1$ because of the way b_1 was chosen, and so $C_{c,d}$ is not solvable at b_1. This completes the proof of the theorem.

Chapter 2

Some pairings and a theorem of Cassels

2.1 Introduction

This chapter introduces some standard pairings, and then gives a detailed sketch of the proof of a theorem of Cassels which will be used in chapter 5. Some of the preparatory lemmas are standard and will also be used in later chapters. The theorem was proved by Cassels in [Ca2] in the mid 1960s in order to show that the conjecture of Birch and Swinnerton-Dyer, as it was then formulated, is true for a curve if it is true for a $\mathbb{Q}$-isogenous curve. We follow Cassels' argument, putting it in modern notation and streamlining it in places by appealing to machinery that has now become standard.

2.2 The Weil pairing

This section defines the Weil pairing for elliptic curves, taking the view that its natural context is the Galois theory of the extension of function fields associated to an isogeny between elliptic curves. This approach entails some extra elaboration compared with the treatment in Silverman's book ([Si1] Section 3.8); however certain points appearing there as fortuitous calculations become very natural from the point of view taken here.

The Weil pairing is a duality between the kernels of an isogeny and its dual isogeny. Let F be any field and suppose ϕ is a separable isogeny of elliptic curves

defined over F; let $\hat{\phi}$ denote its dual:

$$\begin{array}{ccc} E & & \hat{E} \\ {\scriptstyle\phi}\big\downarrow & & \big\uparrow{\scriptstyle\hat{\phi}} \\ E' & & \hat{E}' \end{array}$$

The dual of E is defined as $\hat{E} := \mathrm{Pic}^0(E)$. As it happens, there is a canonical map from E to $\hat{E}$ mapping a point P to the divisor $P - O$. (This is special to the case of elliptic curves, whereas everything else in this section goes through for abelian varieties of any dimension.) The dual isogeny $\hat{\phi} : \hat{E}' \to \hat{E}$ is then simply the pullback map ϕ^*, mapping a divisor $\sum n_Q Q$ to $\sum n_Q \sum_{\phi P = Q} P$.

We now characterise the kernel of $\hat{\phi}$. Let $n = \deg \phi$, and suppose $P \in E[n]$, by which we mean $E(\overline{F})[n]$. Then the divisor

$$\hat{\phi}(\phi P - O) = \sum_{\phi R = O} (P + R) - R$$

is linearly equivalent to $nP - nO$, which is 0 in $\hat{E}$. Thus $\phi P - O \in \hat{E}'[\hat{\phi}]$, and in fact $\phi E[n] \cong \hat{E}'[\hat{\phi}]$.

As a consequence, $\deg \hat{\phi} = \deg \phi = n$. Moreover upon identifying $E' \cong \hat{E}'$, we see $E[\hat{\phi} \circ \phi] = E[n]$, so $\hat{\phi} \circ \phi = [n]$.

To prepare to define the Weil pairing $E[\phi] \times \hat{E}'[\hat{\phi}] \to \mu_n$, suppose $P \in E[\phi]$ and $Q - O \in \hat{E}'[\hat{\phi}]$ for some $Q \in E'$. Since $\hat{\phi}(Q - O) = 0$, $\phi^*(Q - O)$ is the divisor of a function $g_Q \in \overline{F}(E)$. Since $n(Q - O) \equiv 0$, it is the divisor of a function $f_Q \in \overline{F}(E')$. But

$$(f_Q \circ \phi) = \phi^* (nQ - nO) = \left(g_Q^n\right)$$

so after adjusting f_Q by a constant from $\overline{F}$, we can assume that $f_Q \circ \phi = g_Q^n$. Note that if the order of Q is exactly n, then for any proper divisor r of n, $rQ - rO$ is not the divisor of a function and so f_Q is not an rth power in $\overline{F}(E')$. Thus we see that

the extension of function fields associated to ϕ is the nth root extension

$$\begin{array}{l} \overline{F}(E) \cong \overline{F}(E')(\{\sqrt[n]{f_Q} : Q - O \in \hat{E}'[\hat{\phi}]\}) \\ {\scriptstyle \phi^*}\uparrow \\ \overline{F}(E') \end{array}$$

When Q is rational over F, $g_Q \in F(E')$ and so $F(E)/F(E')$ is a Kummer extension (and like any Kummer extension, it is Galois if and only if $\mu_n \subset F$).

For a point $P \in E[\phi]$, let $\tau(P)$ denote the 'translation by P' map $F(E)$, $\tau(P) : f(\cdot) \mapsto f(\cdot - P)$. When $P \in E(F)$, $\tau(P)$ is an automorphism of $F(E)$, and it clearly fixes the subfield $F(E')$. Therefore when $E[\phi] \subset E(F)$, τ identifies $E[\phi] \cong \mathrm{Gal}(F(E)/F(E'))$. To summarize, $F(E)/F(E')$ is Galois when P is F-rational, and an nth root extension when Q is F-rational. It follows that when both P and Q are F-rational, we must have $\mu_n \subset F$; this fact is usually stated as $F(E[n]) \supset F(\mu_n)$.

For any $P \in E[\phi]$ and $Q - O \in \hat{E}'[\hat{\phi}]$, not necessarily rational over F, the Weil pairing is

$$\langle P, Q \rangle = \frac{g_Q^{\tau(P)}}{g_Q}$$

This pairing must take values in μ_n by Kummer theory; in fact for fixed Q the map $P \mapsto \langle P, Q \rangle$ is the element of $\mathrm{H}^1(\mathrm{Gal}(\overline{F(E)}/\overline{F}(E')), \mu_n)$ associated to $f_Q \in \overline{F}(E')^\times/\overline{F}(E')^n$ by the Kummer map. Since $\mathrm{H}^1(\mathrm{Gal}(\overline{F(E)}/\overline{F}(E')), \mu_n) = \mathrm{Hom}(\mathrm{Gal}(\overline{F(E)}/\overline{F}(E')), \mu_n)$, the map $P \mapsto \langle P, Q \rangle$ is a homomorphism, in other words the pairing is linear in P. To see that it is linear in Q note that the divisor

$$\left(\frac{g_{Q_1+Q_2}}{g_{Q_1} g_{Q_2}}\right) = \phi^* \left((Q_1 + Q_2) - O - (Q_1 - O) - (Q_2 - O)\right) = \phi^*(0) = 0$$

which means $g_{Q_1+Q_2}$ and $g_{Q_1} g_{Q_2}$ agree up to a constant, and this constant cancels in the definition of $\langle P, Q \rangle$. It is clear from the definition that the pairing is Galois invariant (for the arithmetic Galois group $\mathrm{Gal}(\overline{F}/F)$).

The most interesting property of the Weil pairing is that for the special case of an isogeny $[m] : E \to E$ the pairing is alternating, that is $\langle P, P \rangle = 1$ for any $P \in E[m]$.

To see this, put $E' = E/P$ and consider the maps

$$\begin{array}{ccc} E & & \hat{E} \\ {\scriptstyle\phi}\downarrow & & \uparrow{\scriptstyle\hat{\phi}} \\ E' := E/P & & \hat{E}' \\ {\scriptstyle\psi}\downarrow & & \uparrow{\scriptstyle\hat{\psi}} \\ E & & \hat{E} \end{array}$$

where $E[\phi] = \langle P \rangle$. One easily calculates that $\hat{E}[\hat{\psi}] = \langle P - O \rangle$. As usual, g_P is a function on E with divisor $[m]^*(P-O)$, but in fact it is a pullback by ϕ of a function on E', since already $\hat{\psi}(P - O) = 0$. This means $g_P^{\tau(P)} = g_P$, so $\langle P, P \rangle = 1$.

2.3 The Tate pairing

Let K_v be a local field, and let G_v denote $\mathrm{Gal}(\overline{K_v}/K_v)$. Let $\phi : E \to E'$ be an isogeny of elliptic curves defined over K_v, let $n = \deg \phi$, and let ϕ' be the dual isogeny. Using the Weil pairing $E[\phi] \times E'[\phi'] \to \mu_n$, the 'cup product' gives us the Tate pairing

$$\mathrm{H}^1(G_v, E[\phi]) \times \mathrm{H}^1(G_v, E'[\phi']) \to \mathrm{H}^2(G_v, \mu_n) \subset \mathbb{Q}/\mathbb{Z}$$

where the inclusion into $\mathbb{Q}/\mathbb{Z}$ is the invariant map from local class field theory. The cup product of two cocycles $\sigma \mapsto y_\sigma$ and $\sigma \mapsto z_\sigma$ is the 2-cocycle $w_{\sigma,\tau} = \langle y_\sigma, \sigma z_\tau \rangle$ (where $\langle \cdot, \cdot \rangle$ denotes the Weil pairing). More generally this construction works, and the theorem below holds, for any two finite G_v-modules that pair into μ_n.

Definitions. A G_v-module M is *unramified* if the inertia group $I_v \subset G_v$ acts trivially on M. For an unramified module M, we define $\mathrm{H}^1_{\mathrm{un}}(G_v, M)$ to be the subgroup $\mathrm{H}^1(G_v/I_v, M) \subset \mathrm{H}^1(G_v, M)$.

Remarks: $\mathrm{H}^1(G_v/I_v, M)$ is well defined because when M is unramified, the action of G_v factors through G_v/I_v. The inclusion is given by the inflation map on cocycles, which is clearly injective.

2.3.1 Theorem. *The Tate pairing is a perfect pairing. When $E[\phi]$ and $E'[\phi']$ are unramified, the subgroups $\mathrm{H}^1_{un}(G_v, E[\phi])$ and $\mathrm{H}^1_{un}(G_v, E'[\phi'])$ are exact annihilators under the pairing.*

For a proof, see [Se] Section 5.2, Theorem 2 and Section 5.5, Proposition 19.

Simple consequences of the theorem:

(1) The finite groups $\mathrm{H}^1(G_v, E[\phi])$ and $\mathrm{H}^1(G_v, E'[\phi'])$ have the same cardinality.

(2) Moreover, $\#\,\mathrm{H}^1_{\mathrm{un}}(G_v, E[\phi]) \cdot \#\,\mathrm{H}^1_{\mathrm{un}}(G_v, E'[\phi']) = \#\,\mathrm{H}^1(G_v, E[\phi])$.

(3) Let $v \nmid n$ be a nonarchimedean place at which the curves have good reduction. Then the proposition below asserts that the images of the local Mordell-Weil groups consist of the unramified cocycles, and so by the theorem they are exact annihilators under the Tate pairing.

2.3.2 Proposition. *([Ca2]) Let K_v be a nonarchimedean local field and suppose $\phi : E \to E'$ is an isogeny of elliptic curves defined over K_v. Suppose further that the curves have good reduction at v and that $v \nmid \deg \phi$. Then the local Kummer map*

$$E'(K_v)/\phi E(K_v) \hookrightarrow \mathrm{H}^1(G_v, E[\phi])$$

has image exactly equal to $\mathrm{H}^1_{un}(G_v, E[\phi])$

Notes: (1) It is standard that the points in $E[\phi]$ are defined over unramified extensions of K under the stated hypotheses on v, so $\mathrm{H}^1_{\mathrm{un}}(G_v, E[\phi])$ makes sense.

(2) Similarly, for any $Q \in E'(K_v)$, the preimages $P \in \phi^{-1}Q$ are defined over unramified extensions of K (otherwise there would be two different $P_1, P_2 \in \phi^{-1}Q$ congruent to each other modulo a prime of some extension of K_v, but then $P_1 - P_2 \in E[\phi]$ would be congruent to O and hence ramified at that prime). Therefore the cocycle $\sigma \mapsto P^\sigma - P$, which is the image of Q under the Kummer map, is unramified at v. This shows that in the proposition, the image of the Kummer map is contained in $\mathrm{H}^1_{\mathrm{un}}(G_v, E[\phi])$.

Proof of the Proposition: Cassels' idea is to consider the usual descent sequence, but this time over the residue field k_v:

$$0 \to E'(k_v)/\phi E(k_v) \to \mathrm{H}^1(G_v/I_v, E[\phi]) \to \mathrm{H}^1(G_v/I_v, E(\overline{k_v}))$$

where we identify $\mathrm{Gal}(\overline{k_v}/k_v) \cong G_v/I_v$. Nontrivial elements of $\mathrm{H}^1(G_v/I_v, E(\overline{k_v}))$ correspond to curves of genus one over k_v that have no points over k_v. But, by the Weil bounds, every curve of genus one over a finite field has points over that field. Therefore $\mathrm{H}^1(G_v/I_v, E(\overline{k_v}))$ is trivial, so the Kummer map over k_v is an isomorphism.

We know by standard theory (or by Hensel's lemma) that since E' has good reduction, $E'(K_v)$ maps onto $E'(k_v)$ via the reduction map. Reduction commutes with the Kummer map, so the composition

$$E'(K_v) \to E'(k_v) \to \mathrm{H}^1(G_v/I_v, E[\phi]) = \mathrm{H}^1_{\mathrm{un}}(G_v, E[\phi])$$

is surjective, proving the proposition.

2.4 Cassels' theorem

This theorem will be applied in Chapter Five to show that a certain Selmer group is large.

2.4.1 Theorem. *(1965, [Ca2]) Let K be a number field. Suppose $\phi : E \to E'$ is an isogeny of elliptic curves defined over K, and let $\phi' : E' \to E$ be the dual isogeny. Then*

$$\frac{\mathrm{Sel}^{\phi}(E)}{\mathrm{Sel}^{\phi'}(E')} = \frac{\#E(K)[\phi]}{\#E'(K)[\phi']} \prod_v \frac{\int_{E'(K_v)} |\omega'|_v}{\int_{E(K_v)} |\omega|_v}$$

where ω and ω' are any differentials on the curves.

Comments about ω and ω': (i) The integrals appearing in the theorem are defined as follows. On an affine patch $T \subset E$ where the curve has a smooth coordinate t, we

may write $\omega = f(t)\,dt$. Define

$$\int_{T(K_v)} |\omega|_v := \int_{t\in T(K_v)} |f(t)|_v\,dt$$

where the second integral is with respect to the standard Haar measure on K_v.

(ii) On an elliptic curve, the set of differentials with no poles is a one dimensional vector space over K, so they are constant multiples of one another. The product over all places $\prod_v \int_{E(K_v)} |\omega|_v$ is independent of the normalisation, by the product rule $\prod_v |\alpha|_v = 1$ (which holds for all $\alpha \in K^\times$). To prove the theorem, it is convenient to choose ω and ω' so that $\omega = \phi^*\omega'$.

2.4.2 Lemma. *If $\omega = \phi^*\omega'$ then*

1. *For all v,*
$$\frac{\int_{E'(K_v)} |\omega'|}{\int_{E(K_v)} |\omega|} = \frac{\#E'(K_v)/\phi E(K_v)}{\#E(K_v)[\phi]}$$
2. *This equals 1 for all finite places $v \nmid n$ where E has good reduction. In particular, the infinite product appearing in the theorem makes sense.*

Proof: For a subset $N \subset E(K_v)$ that maps injectively to $E'(K_v)$,

$$\int_N |\omega| = \int_N |\phi^*\omega'| = \int_{\phi N} |\omega'|$$

by definition of the pullback differential. Hence

$$\int_{E(K_v)} |\omega| = \#E(K_v)[\phi] \int_{\phi E(K_v)} |\omega'|$$

while obviously

$$\int_{E'(K_v)} |\omega'| = \#E'(K_v)/\phi E(K_v) \int_{\phi E(K_v)} |\omega'|\,.$$

Dividing the last two equations yields (i).

By Proposition 1.1.2 if E has good reduction at $v \nmid n$, then so does E', and moreover $\#E(k_v) = \#E'(k_v)$, where k_v denotes the residue field. But ϕ induces

a homomorphism $E(k_v) \to E'(k_v)$, so $\#E'(k_v)/\phi E(k_v) = \#E(k_v)[\phi]$. Recall that $E(K_v)/E_1(K_v) \cong E(k_v)$, and that ϕ restricts to an isomorphism of the formal groups $E_1(K_v) \to E_1'(K_v)$ when $v \nmid n$. Thus $\#E'(K_v)/\phi E(K_v) = \#E(K_v)[\phi]$, proving (ii).

A sketch of the proof of Cassels' theorem is given below. The following corollary is a reformulation that is more convenient for some applications, and where the infinite product is replaced by a finite product. To state it, one must make some conventions to deal with the fact that E might not have an everywhere minimal model over $\mathfrak{O}_K$.

Definitions. Suppose E is an elliptic curve over a number field K. For a nonarchimedean place v, a differential ω_v on E defined over K_v is *well normalised at* v if

$$\int_{E_1(K_v)} |\omega|_v = 1/\,\mathrm{N}\, v\,.$$

Given a differential ω defined over K, define an ideal $\mathcal{A} = \mathcal{A}(\omega)$ as follows: For each finite place v let $\alpha_v \in K_v^\times$ be such that $\alpha_v\omega$ is well normalised at v; then let $\mathcal{A}$ be the ideal satisfying $\mathcal{A}\mathfrak{O}_v = \alpha_v\mathfrak{O}_v$ for each v. Define

$$\Omega(E) := \mathrm{N}\,\mathcal{A} \prod_{\text{infinite } v} \int_{E(K_v)} |\omega|_v$$

where ω is any differential on E defined over K.

Remarks showing that the definitions make sense:

(i) For each v, there exists a well normalised differential ω_v. Indeed if $y^2 = f(x)$ is a minimal Weierstrass model for E over K_v then $\frac{dx}{2y}$ is a well normalised differential at v. To see this, one checks that $s := x/y$ is a smooth coordinate on a neighbourhood of the identity $O \in E$, and that $\frac{dx}{2y}$ equals $-ds$. If the model is minimal, $E_1(K_v)$ consists of those points for which $s \in (\pi_v)$ and so

$$\int_{E_1(K_v)} |\omega|_v = \int_{s\in(\pi_v)} ds = 1/\mathrm{N}\, v\,.$$

In particular, if $y^2 = f(x)$ is an everywhere minimal Weierstrass model for E over K, the ideal $\mathcal{A}$ corresponding to $\frac{dx}{2y}$ is trivial. Thus in the case $K = \mathbb{Q}$, the above definition coincides with the standard definition of the real period $\Omega(E) := \int_{E(\mathbb{R})} \left|\frac{dx}{2y}\right|$.

(ii) In the definition, α_v exists since there exists a well normalised ω_v and any two differentials on E (over K_v) are constant multiples of one another.

(iii) Clearly, $\Omega(E)$ is independent of the choice of ω since it is unchanged when ω is replaced by a constant multiple $\alpha\omega$.

(iv) There is a more abstract way to define $\mathcal{A}$, as the ideal such that $\mathcal{A}\omega$ equals the $\mathfrak{O}_K$-module of integral differentials on E.

2.4.3 Corollary. *Let K be a number field. Suppose $\phi : E \to E'$ is an isogeny of elliptic curves defined over K, and let $\phi' : E' \to E$ be the dual isogeny. Let $n = \deg \phi$. Then*

$$\frac{\mathrm{Sel}^{\phi}(E)}{\mathrm{Sel}^{\phi'}(E')} = \frac{\#E(K)[\phi]}{\#E'(K)[\phi']} \cdot \frac{\Omega(E')}{\Omega(E)} \prod_{\text{finite } v} \frac{c_v(E')}{c_v(E)}$$

where $c_v(E) = \#\left(E(K_v)/E_0(K_v)\right)$ as usual. Moreover if n is odd then as fractional ideals of K

$$\left(\frac{1}{n^{[K:\mathbb{Q}]}}\right) \subseteq \left(\frac{\Omega(E')}{\Omega(E)}\right) \subseteq \left(n^{[K:\mathbb{Q}]}\right).$$

Note: the product in the corollary is really a finite product, since $c_v(E) = 1$ for all v where E has good reduction.

Proof of the corollary: For each finite prime v let ω_v and ω'_v be well normalised differentials over K_v, and let k_v denote the residue field. Note that

$$\int_{E_0(K_v)} |\omega_v|_v = \#E(k_v) \int_{E_1(K_v)} |\omega_v|_v = \frac{\#E(k_v)}{\mathrm{N}\, v}$$

and likewise for ω'_v. Therefore, since $\#E(k_v) = \#E'(k_v)$,

$$\int_{E_0(K_v)} |\omega_v|_v = \int_{E'_0(K_v)} |\omega'_v|_v$$

for all finite v. Now if ω is a differential on E over K

$$\int_{E(K_v)} |\omega|_v = c_v(E) \int_{E_0(K_v)} |\omega|_v = \frac{c_v(E)}{|\alpha_v|_v} \int_{E_0(K_v)} |\omega_v|_v \,.$$

where $\alpha_v \omega = \omega_v$. Since $1/|\alpha_v|_v = \#(\mathfrak{O}_v/\alpha_v) = \#(\mathfrak{O}_v/\mathcal{A}\mathfrak{O}_v)$, the product of $1/|\alpha_v|_v$ over all finite places v equals $\mathrm{N}\,\mathcal{A}$. Putting all this together,

$$\prod_v \frac{\int_{E'(K_v)} |\omega'|_v}{\int_{E(K_v)} |\omega|_v} = \frac{\mathrm{N}\,\mathcal{A}'}{\mathrm{N}\,\mathcal{A}} \cdot \prod_{\text{finite v}} \frac{c_v(E')}{c_v(E)} \prod_{\text{infinite v}} \frac{\int_{E'(K_v)} |\omega'|_v}{\int_{E(K_v)} |\omega|_v} = \frac{\Omega(E')}{\Omega(E)} \cdot \prod_{\text{finite v}} \frac{c_v(E')}{c_v(E)}$$

This shows that the first assertion of the corollary follows from Theorem 2.4.1.

For the second assertion, recall that $\Omega(E)$ is independent of the choice of ω, so without loss of generality take ω' to be well normalised at all primes dividing n, and take ω to be $\phi^*\omega'$. For primes $v \nmid n$, note that ϕ is an isomorphism $E_1(K_v) \to E_1'(K_v)$ so $\int_{E_1(K_v)} |\omega|_v = \int_{E_1'(K_v)} |\omega'|_v$. It follows that $\mathcal{A}\mathfrak{O}_v = \mathcal{A}'\mathfrak{O}_v$ for $v \nmid n$.

Now suppose $v \mid \ell$ for some prime ℓ dividing n, with ℓ^r exactly dividing n. Note that $\phi' \circ \phi = [n]$. By the theory of the formal group (see section 1.1.2), for a large enough integer m the subgroup $E_m(K_v) := \{P \in E(K_v) : P \equiv O \mod \pi_v^m\}$ is isomorphic as a group to $\mathfrak{O}_v^+$, and likewise for E'. On this subgroup, $[n]$ is an injection with image $\ell^r\mathfrak{O}_v$, which has index $r[K_v : \mathbb{Q}_\ell]$, so the image of ϕ must have index ℓ^a for some $a \leq r[K_v : \mathbb{Q}_\ell]$. Hence

$$\int_{E_m(K_v)} |\omega|_v = \int_{E_m(K_v)} |\phi^*\omega'|_v = \frac{1}{\ell^a} \int_{E_m'(K_v)} |\omega'|_v = \frac{1}{\ell^a} |\pi_v^m|_v$$

since we assumed ω' is well normalised at v. On the other hand, there is some $\alpha_v \in K_v$ such that $\alpha_v\omega$ is well normalised at v, which means

$$\int_{E_m(K_v)} |\omega|_v = \frac{1}{|\alpha_v|_v} |\pi_v^m|_v \,.$$

Hence $|\alpha_v|_v = \ell^a$ for some $a \leq r[K_v : \mathbb{Q}_\ell]$, for each $v \mid n$. Combining this with the facts that ω' is well normalised at all $v \mid n$ and that $\mathcal{A}\mathfrak{O}_v = \mathcal{A}'\mathfrak{O}_v$ for $v \nmid n$, one finds

$$\frac{\mathrm{N}\,\mathcal{A}'}{\mathrm{N}\,\mathcal{A}} = \prod_{v|n} |\alpha_v|_v \,,$$

and this is an integer dividing $n^{[K:\mathbb{Q}]}$. At each infinite place v, ϕ maps $E(K_v)$ onto $E'(K_v)$ since n is assumed to be odd. Thus

$$\frac{\int_{E'(K_v)} |\omega'|_v}{\int_{E(K_v)} |\omega|_v} = \frac{\int_{E'(K_v)} |\omega'|_v}{\int_{E(K_v)} |\phi^*\omega'|_v} = \frac{1}{\#E(K_v)[\phi]}\,.$$

For each place, $\#E(K_v)[\phi]$ divides n, so $\prod_{\text{infinite } v} \#E(K_v)[\phi]$ divides $n^{[K:\mathbb{Q}]}$. This completes the proof of the second assertion.

Sketch of the proof of Theorem 2.4.1, in the case where $\deg\phi$ *is prime:* This sketch will take up the remainder of the chapter. Suppose that ϕ has prime degree q. Let $\mathcal{S}$ be a finite set of places of K containing the infinite places, the primes where E has bad reduction and those dividing q. By Proposition 2.3.2 (which characterises unramified cocycles) $\mathrm{Sel}^\phi(E)$ sits inside the subgroup $\mathrm{H}^1_{\mathcal{S}}(G_K, E[\phi]) \subset \mathrm{H}^1(G_K, E[\phi])$ consisting of cocycles unramified except at $\mathcal{S}$. This is a finite subgroup, and when $\mathcal{S}$ is chosen large enough we can conveniently calculate its size.

2.4.4 Lemma. *When* $\mathcal{S}$ *is chosen large enough,*

$$\#\,\mathrm{H}^1_{\mathcal{S}}(G_K, E[\phi]) = \frac{\#E(K)[\phi]}{\#E'(K)[\phi']} \prod_{v\in\mathcal{S}} \#E'(K_v)[\phi']$$

A proof of the lemma is outlined later. Next we introduce a pairing that will help to determine the relative sizes of the Selmer groups. Recall that the Tate pairing on local cohomology

$$\mathrm{H}^1(G_v, E[\phi]) \times \mathrm{H}^1(G_v, E'[\phi']) \to \mathbb{Z}/q$$

is a perfect pairing, and by Theorem 2.3.1 the images of the local Mordell-Weil groups $E'(K_v)/\phi E(K_v)$ and $E(K_v)/\phi' E'(K_v)$ pair trivially. Rather formally, let

$$T = \oplus_{v\in\mathcal{S}}\, \mathrm{H}^1(G_v, E[\phi]),$$
$$T' = \oplus_{v\in\mathcal{S}}\, \mathrm{H}^1(G_v, E'[\phi']),$$

and let

$$\langle\cdot,\cdot\rangle : T \times T' \to \mathbb{Z}/q$$

be the sum of the local pairings; note that $\#T = \#T'$ and that $\langle \cdot, \cdot \rangle$ is perfect. Let $M \subseteq T$ and $M' \subseteq T'$ be the direct sums of the local Mordell-Weil groups; thus M and M' pair trivially. Also, let $D \subseteq T$ be the image of $\mathrm{H}^1_{\mathcal{S}}(G_K, E[\phi])$, mapped diagonally into T. The diagonal map will be an embedding if $\mathcal{S}$ is large enough (as one can see fairly easily from the proof of Lemma 2.4.4 sketched below). Define $D' \subseteq T'$ analogously. Then D and D' pair trivially, because the pairing restricted to $D \times D'$ can be expressed $\langle \zeta, \zeta' \rangle = \sum_v \mathrm{inv}_v (\zeta \vee \zeta'|_v)$ (since cup product commutes with restriction), but this is 0 by class field theory. As a remark, it can be shown that M and M' are exact annihilators, as are D and D', and moreover that all the inequalities below are really equalities; however we will not need to prove these things. Note that by definition

$$\#\,\mathrm{Sel}^{\phi}(E) = \#(M \cap D) = \frac{\#M\,\#D}{\#(M+D)}$$

where the second equality is merely group theory. On the other hand, $M' \cap D'$ pairs trivially with $M + D$, since M annihilates M' and D annihilates D', so

$$\#\,\mathrm{Sel}^{\phi'}(E') = \#(M' \cap D') \leq \frac{\#T}{\#(M+D)}$$

Dividing the last two equations,

$$\frac{\#\,\mathrm{Sel}^{\phi}(E)}{\#\,\mathrm{Sel}^{\phi'}(E')} \geq \frac{\#M\,\#D}{\#T} = \frac{\#E(K)[\phi]}{\#E'(K)[\phi']} \prod_v \frac{\#E'(K_v)[\phi']}{\#E(K_v)/\phi' E'(K_v)}$$

using Lemma 2.4.4 for the size of D, and since by the duality of M and M' $\#T/\#M = \#M'$, which by definition equals $\prod_v \#E(K_v)/\phi' E'(K_v)$. Hence by Lemma 2.4.2,

$$\frac{\mathrm{Sel}^{\phi}(E)}{\mathrm{Sel}^{\phi'}(E')} \geq \frac{\#E(K)[\phi]}{\#E'(K)[\phi']} \prod_v \frac{\int_{E'(K_v)} |\omega'|_v}{\int_{E(K_v)} |\omega|_v}$$

But by interchanging ϕ and ϕ' we may obtain the reverse inequality, thus proving Cassels' theorem (in the case of prime degree).

Sketch of the proof of Lemma 2.4.4 The idea is to compare $\mathrm{H}^1_{\mathcal{S}}(G_K, E[\phi])$ with $\mathrm{H}^1_{\mathcal{S}}(G_K, \mu_q)$, by first restricting to the subgroup of G_K which has the same action

on $E[\phi]$ as on μ_q. These are both cyclic groups of order q, so the actions are given by characters χ_ϕ and χ defined by

$$\sigma P = \chi_\phi(\sigma)P \quad \text{for} \quad P \in E[\phi]$$
$$\sigma\zeta = \zeta^{\chi(\sigma)} \quad \text{for} \quad \zeta \in \mu_q$$

Let $\psi = \chi_\phi\chi^{-1}$ and let L/K be the cyclic Galois extension corresponding to the subgroup $G_L := \ker(\psi) \lhd G_K$. Since $\#\operatorname{Gal}(L/K)$ is prime to q, the 'change of groups' exact sequence yields the first of the following isomorphisms:

$$\mathrm{H}^1(G_K, E[\phi]) \cong \mathrm{H}^1(G_L, E[\phi])^{\operatorname{Gal}(L/K)} \cong (L^\times/L^{\times q})^{\operatorname{Gal}(L/K)}$$

The second isomorphism is a Kummer theoretic calculation. It is important to note that the action of $G_{L/K}$ on $L^\times/L^{\times q}$ is not the natural one. For more details see Lemma 1.2.2, where a similar argument is given. There the action on $L^\times/L^{\times q}$ is calculated, and the fixed points turn out to be

$$\{\alpha \in L^\times/L^{\times q} : \sigma\alpha = \alpha^{\psi(\sigma)}\}$$

which is the eigenspace for ψ under the usual action. Now, $\mathrm{H}^1_{\mathcal{S}}(G_K, E[\phi])$ is the subgroup of this supported at primes above $\mathcal{S}$, which equals the ψ eigenspace of $L_{\mathcal{S}}^\times/L_{\mathcal{S}}^{\times q}$ (where $L_{\mathcal{S}}^\times$ denotes the elements that are units except at primes above $\mathcal{S}$) when $\mathcal{S}$ is sufficiently large that $\mathrm{Cl}(L)$ is generated by primes above $\mathcal{S}$. To calculate the size of this eigenspace, note that for a prime $\mathfrak{p} \in \mathcal{S}$, $\mathfrak{p}$ splits in L/K if and only if there is an element in the eigenspace supported at primes above $\mathfrak{p}$; this element would have the form $\prod_{\sigma\in\operatorname{Gal}(L/K)}(\sigma\mathcal{S})^{\psi(\sigma)^{-1}}$ where $\mathcal{S} \in L_{\mathcal{S}}$ generates the ideal $\mathfrak{q}^m$ for some $m \in \mathbb{Z}$ and some prime $\mathfrak{q}$ above $\mathfrak{p}$. On the other hand, by the definition of L, $\mathfrak{p}$ splits in L/K if and only if ψ is trivial on G_v, in other words $E[\phi] \cong \mu_q$ as $G_{\mathfrak{p}}$-modules. By the Galois invariance of the Weil pairing (see 2.2) this is equivalent to $E'[\phi'] \cong \mathbb{Z}/q$ as $G_{\mathfrak{p}}$-modules, or $E'[\phi'] \subset E'(K_{\mathfrak{p}})$. What we've just shown is that the place $\mathfrak{p}$ contributes 1 to the dimension of $\mathrm{H}^1_{\mathcal{S}}(G_K, E[\phi])$ if and only if $E'(K_{\mathfrak{p}})[\phi']$

is nontrivial, which explains why $\#E'(K_{\mathfrak{p}})[\phi']$ appears on the right hand side in the statement of the lemma. Finally we just remark that the factors $E(K)[\phi]$ and $E'(K)[\phi']$ are related to whether μ_q is contained in K or L. This completes our sketch of 2.4.4 and of Cassels' theorem in the case of prime degree.

The general case of Cassels' theorem can be reduced to the prime case by regarding an arbitrary isogeny as a composition of isogenies of prime degree and 'multiplication by n' maps. To make the reduction one simply manipulates the kernels and cokernels for some compositions of maps, using the nontrivial fact that

$$\#Ш(E,K)[\phi] = \#Ш(E,K)/\phi' Ш(E',K)$$

This fact follows from a duality property of the Cassels-Tate pairing.

Chapter 3

A generalization of Fisher's First Descent Theorem

3.1 Introduction

This chapter is devoted to proving a theorem that explicitly describes the Selmer groups for certain isogenies of prime degree between elliptic curves. Let K be a number field and suppose E and E' are elliptic curves defined over K, with an isogeny $\phi : E \to E'$ of prime degree $\ell \geq 5$, also defined over K. Denote the dual isogeny by $\phi' : E' \to E$. The theorem (3.4.1) will identify $\mathrm{Sel}^{\phi}(E, K)$ and $\mathrm{Sel}^{\phi'}(E', K)$ as subgroups of $L^{\times}/L^{\times \ell}$ for some finite extension L/K. It specifies them in terms of data involving only the behaviour of the kernels of the isogenies under reduction. This data is very easy to compute for a given curve, so the theorem is useful in practice for computing Selmer groups. For a very thorough treatment of how to compute Selmer groups see [S-St].

Our theorem generalises the 'First Descent Theorem' given in Tom Fisher's Cambridge thesis [Fi] in several respects. Fisher's theorem gives the same description of Selmer groups, but applies only in the special case where $K = \mathbb{Q}$ and $\ell = 5$ or 7. Both Fisher's theorem and ours impose the hypothesis that $E'[\phi']$ is contained in $E(K)$ (in other words E' corresponds to a K-rational point on $X_1(\ell)$, instead of just $X_0(\ell)$). However, it would not be too difficult to remove this hypothesis.

To prove the theorem, one first calculates the 'local Mordell-Weil groups', namely $E'(K_v)/\phi E(K_v)$ and $E(K_v)/\phi' E'(K_v)$, and then puts the local information together.

Consider the 'descent exact sequence' associated to ϕ

$$0 \to E'(K)/\phi E(K) \to \mathrm{Sel}^{\phi}(E,K) \to Ш(E,K)[\phi] \to 0,$$

and the analogous one associated to ϕ'. Each element of $\mathrm{Sel}^{\phi}(E,K)$ corresponds to a homogeneous space of E, and we must decide which of these have points over all completions of K. Fisher's proof supplies explicit equations for the homogeneous spaces as intersections of quadrics in $\mathbf{P}^{l-1}$, and uses Hensel's Lemma to decide whether they have points locally. One could say his approach concentrates on the right hand end of the sequence, whereas our approach concentrates on the left hand end. It calculates the 'local Mordell-Weil groups' using standard theory of elliptic curves over local fields, namely the formal group and Tate uniformisations. The local and global data about the curves that we discover along the way is much the same in both proofs.

One motivation for this kind of theorem is the desire to understand the ℓ-parts of Tate-Shafarevich groups, for instance how large they can be. Fisher constructs elliptic curves $E/\mathbb{Q}$ with $Ш(E,\mathbb{Q})[5]$ arbitrarily large. His strategy is to consider elliptic curves that have two different 5-isogenies, apply his theorem to both isogenies, and compare the results. (This will not work for $Ш(E,\mathbb{Q})[7]$ because curves can only have at most one 7-isogeny defined over $\mathbb{Q}$.) A related motivation for doing Selmer group calculations is the hope of extending them, working with the Cassels-Tate pairing, to a somewhat explicit description of the images of $\mathrm{Sel}^{\phi}(E,K)$ in $Ш(E,K)[\ell]$. A third motivation is for writing algorithms to perform ℓ-descent, in which computing Selmer groups is a key step (again, see also [S-St]).

3.2 A description of $\mathrm{H}^1(G,\mathbb{Z}/\ell)$

We recall some standard facts. G_K will denote $\mathrm{Gal}(\overline{K}/K)$. To say that $E[\phi] \cong \mu_\ell$ as G_K-modules (or more correctly, as $\mathbb{Z}[G_K]$-modules) means that the action of G_K on

$P \in E[\phi]$ is given by $\sigma P = \chi(\sigma)P$, where χ is the cyclotomic character defined by

$$\zeta^\sigma = \zeta^{\chi(\sigma)} \text{ for } \zeta \in \mu_\ell \text{ and } \sigma \in G_K.$$

In particular, $E[\phi] \subset E(K(\mu_\ell))$. Similarly the assumption $E'[\phi'] \subset E'(K)$ is equivalent to $E'[\phi'] \cong \mathbb{Z}/\ell$ as G_K-modules.

3.2.1 Proposition. *Suppose as above that $\phi : E \to E'$ and its dual $\phi' : E' \to E$ are defined over K. If $E'[\phi'] \cong \mathbb{Z}/\ell$ then $E[\phi] \cong \mu_\ell$ as G_K-modules.*

Proof: Choose a basis for $E'[\ell]$ in which $E'[\phi']$ is generated by $[1, 0]$. The Weil pairing $E'[\ell] \times E'[\ell] \to \mu_\ell$ is skew symmetric, so for any basis it has the form $\begin{pmatrix} 0 & -a \\ a & 0 \end{pmatrix}$. We may renormalise our basis so it becomes $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The pairing is also Galois invariant, so if $\sigma \in G_K$ and M_σ is the matrix describing its action on our basis, we have

$$M_\sigma^t \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} M_\sigma = \chi(\sigma) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

where χ records the action of σ on μ_ℓ, namely $\sigma\zeta_\ell = \zeta_\ell^{\chi(\sigma)}$. When one computes the left side and compares it with the right, one finds $\det M_\sigma = \chi(\sigma)$. Since $E'[\phi']$ is rational, each M_σ has the form $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$, and hence the form $\begin{pmatrix} 1 & * \\ 0 & \chi(\sigma) \end{pmatrix}$. The bottom right entry tells us the action on the image of $E'[\ell]$ under ϕ', which is $E[\phi]$. This shows $E[\phi] \cong \mu_\ell$.

The next lemma shows how our Selmer groups can be realized as subgroups of groups that arise from the theory of Kummer extensions.

3.2.2 Lemma. *Suppose as above that $E'[\phi'] \cong \mathbb{Z}/\ell$. Then $\mathrm{H}^1(G_K, E[\phi]) \cong K^\times/K^{\times\ell}$. Put $L = K(\mu_\ell)$ and let $\chi : G_K \to \mathbb{Z}/\ell^\times$ be the character defined by $\tau\zeta_\ell = \zeta_\ell^{\chi(\tau)}$. Then*

$$\mathrm{H}^1(G_K, E'[\phi']) \cong \left\{\alpha \in L^\times/L^{\times\ell} : \tau\alpha = \alpha^{\chi(\tau)} \quad \forall \tau \in G_K\right\}.$$

Proof: The long exact sequence for descent via ϕ comes by taking cohomology of $0 \to E'[\phi] \to E \to E' \to 0$. It tells us

$$0 \to E'(K)/\phi E(K) \to \mathrm{H}^1(G_K, E[\phi]) \to \mathrm{H}^1(G_K, E)[\phi] \to 0\,.$$

Now $\mathrm{H}^1(G_K, E[\phi]) = \mathrm{H}^1(G_K, \mu_\ell) \cong K^\times/K^{\times\ell}$ (the group of Kummer extensions of degree ℓ).

Doing the same for ϕ', we have $\mathrm{H}^1(G_K, E'[\phi']) = \mathrm{H}^1(G_K, \mathbb{Z}/\ell)$ (the group of cyclic extensions of degree ℓ). Of course, if $\mu_\ell \subset K$, this is the same as $\mathrm{H}^1(G_K, \mu_\ell)$. Otherwise, we use the 'change of groups' cohomology sequence (part of a spectral sequence). With $L = K(\mu_\ell)$, this is

$$\begin{aligned} &0 \to \mathrm{H}^1(\mathrm{Gal}(L/K), \mathbb{Z}/\ell) \to \mathrm{H}^1(G_K, \mathbb{Z}/\ell) \to \mathrm{H}^1(G_L, \mathbb{Z}/\ell)^{\mathrm{Gal}(L/K)} \\ &\to \mathrm{H}^2(\mathrm{Gal}(L/K), \mathbb{Z}/\ell) \end{aligned}$$

where the action of $\mathrm{Gal}(L/K)$ will be given below. Note first that $\deg(L/K)$ divides $\ell - 1$ so $\mathrm{H}^1(\mathrm{Gal}(L/K), \mathbb{Z}/\ell) = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Z}/\ell)$ is trivial. Also $\mathrm{H}^2(\mathrm{Gal}(L/K), \mathbb{Z}/\ell)$ is trivial because it classifies group extensions of $\mathbb{Z}/\ell$ by a cyclic group of order dividing $\ell - 1$, but by elementary group theory the only such extension is the direct product. So $\mathrm{H}^1(G_K, \mathbb{Z}/\ell) \cong \mathrm{H}^1(G_L, \mathbb{Z}/\ell)^{\mathrm{Gal}(L/K)}$. The action of $\mathrm{Gal}(L/K)$ on cocycles is canonical: for $\tau \in G_K$,

$$\tau \cdot (\sigma \mapsto \zeta_\sigma) = (\tau\sigma\tau^{-1} \mapsto \tau \cdot \zeta_\sigma)$$

and as always G_L acts trivially on its own cohomology. In the formula above and elsewhere, a dot denotes a special group action, while an action with no dot, such as $\sigma\beta$, denotes the ordinary Galois action. Since $\mu_\ell \subset L$, we know

$$\begin{aligned} &\mathrm{H}^1(G_L, \mathbb{Z}/\ell) \cong L^\times/L^{\times\ell} \\ &\text{via} \quad (\sigma \mapsto \sigma\beta/\beta) \leftrightarrow \alpha \quad \text{where} \quad \beta^\ell = \alpha \end{aligned}$$

but *only* as $\mathbb{Z}$-modules; the action of G_K on $L^\times/L^{\times\ell}$ induced by this isomorphism is a twist of the natural one. We'll compute the action of $\tau \in G_K$ by finding which

element of $L^\times/L^{\times\ell}$ the cocycle $\tau \cdot (\sigma \mapsto \sigma\beta/\beta)$ corresponds to. By definition, this is $\tau\sigma\tau^{-1} \mapsto \tau \cdot (\sigma\beta/\beta)$, or $\tau\sigma\tau^{-1} \mapsto (\sigma\beta/\beta)$ since τ acts trivially on the coefficients $\mathbb{Z}/\ell$. Making a substitution, this becomes

$$\sigma \mapsto \frac{\tau^{-1}\sigma\tau\beta}{\beta} = \tau^{-1}\left(\frac{\sigma\tau\beta}{\tau\beta}\right) = \left(\frac{\sigma\tau\beta}{\tau\beta}\right)^{\chi(\tau^{-1})} = \frac{\sigma\beta_1}{\beta_1}$$

where $\beta_1 = \tau\beta^{\chi(\tau^{-1})}$. So $\tau \cdot (\sigma \mapsto \sigma\beta/\beta)$ corresponds to

$$\alpha_1 = (\tau\beta^{\chi(\tau^{-1})})^\ell = \tau\alpha^{\chi(\tau^{-1})} \in L^\times/L^{\times\ell}.$$

The fixed points of this action are as stated in the lemma.

3.3 Finding the local Mordell-Weil groups

Notation. Throughout this section let K be a number field, and let $\phi : E \to E'$ is an isogeny of elliptic curves defined over K such that $E[\phi] \cong \mu_\ell$ as G_K-modules. Let $\phi' : E' \to E$ denote the dual isogeny; then $E'[\phi'] \cong \mathbb{Z}/\ell$ by Proposition 3.2.1.

We will calculate the local Mordell-Weil groups at each finite place v, first considering places $v \nmid \ell$ where the curves have good reduction, then in 3.3.2 places $v \nmid \ell$ where the curves have bad reduction, and finally in 3.3.3 dealing with the places above ℓ.

The first case is covered by Proposition 2.3.2. We restate the result here, as it seems worthwhile to give a more explicit proof in the case under consideration.

3.3.1 Lemma. *Suppose $v \nmid \ell$ is a place where the curves have good reduction. Then the images of the local Mordell-Weil groups $E'(K_v)/\phi E(K_v)$ and $E(K_v)/\phi' E'(K_v)$ are exactly equal to $\mathrm{H}^1_{un}(G_v, \mu_\ell)$ and $\mathrm{H}^1_{un}(G_v, \mathbb{Z}/\ell)$ respectively.*

Proof: By Lemma 1.2.3, the images of the local Mordell-Weil groups are contained in the unramified subgroups. A dimension count will show that the containments are equalities. In $\mathrm{H}^1(G_v, \mu_\ell) \cong K_v^\times/K_v^{\times\ell}$, the unramified cocycles are those corresponding

to unramified Kummer extensions, so $\mathrm{H}^1_{\mathrm{un}}(G_v, \mu_\ell)$ is the unit subgroup $\mathfrak{O}_v^\times/\mathfrak{O}_v^{\times\ell}$. Using $K_v^\times \cong \langle\pi\rangle \times k_v^\times \times \{1+\pi_v\mathfrak{O}_v\}$,

$$K_v^\times/K_v^{\times\ell} \cong \begin{cases} \langle\pi\rangle/\langle\pi^\ell\rangle \times \mu_\ell & \text{if } \mu_\ell \subset k_v^\times \\ \langle\pi\rangle/\langle\pi^\ell\rangle & \text{otherwise} \end{cases}$$

Hence $\mathrm{H}^1_{\mathrm{un}}(G_v, \mu_\ell)$ has order ℓ when $\mu_\ell \subset k_v$, and is trivial otherwise. On the other hand $\mathrm{H}^1_{\mathrm{un}}(G_v, \mathbb{Z}/\ell)$ automatically has order ℓ, since there is always exactly one non-trivial unramified cyclic extension of K_v.

Since E and E' have good reduction, $E(K_v)/E_0(K_v)$ and $E'(K_v)/E'_0(K_v)$ are both trivial. By assumption, v lies above some prime $p \neq \ell$. Since $E_1(K_v)$ and $E'_1(K_v)$ are pro-p groups, ϕ restricts to an isomorphism between them. Therefore $E'(K_v)/\phi E(K_v) \cong E'(k_v)/\phi E(k_v)$. But by 1.1.2 $E'(k_v)$ and $E(k_v)$ have the same size, so the map $\phi : E'(k_v) \to E(k_v)$ is surjective if and only if it is injective. This happens if and only if $E(\overline{k_v})[\phi] \not\subseteq E(k_v)$, which is equivalent to $\mu_\ell \not\subseteq k_v$ by the assumption $E(\overline{k_v})[\phi] \cong \mu_\ell$. Thus $E'(K_v)/\phi E(K_v)$ has order ℓ when $\mu_\ell \subset k_v$ and is trivial otherwise. This shows $E'(K_v)/\phi E(K_v)$ and $\mathrm{H}^1_{\mathrm{un}}(G_v, \mu_\ell)$ have the same order, and are therefore equal. By a similar argument, $E(K_v)/\phi' E'(K_v)$ has order ℓ, since $E'[\phi'] \subset E'(k_v)$ by the assumption $E'[\phi'] \cong \mathbb{Z}/\ell$. This shows $E(K_v)/\phi' E'(K_v)$ equals $\mathrm{H}^1_{\mathrm{un}}(G_v, \mathbb{Z}/\ell)$.

3.3.2 Lemma. *Suppose $v \nmid \ell$ is a place where the curves do not have good reduction.*

(i) When $\mu_\ell \subset K_v$, $\mathrm{H}^1(G_v, E[\phi]) \cong \langle\pi_v\rangle/\langle\pi_v^\ell\rangle \times k_v^\times/k_v^{\times\ell}$ and $\mathrm{H}^1(G_v, E'[\phi'])$ is the same. If $E'[\phi'] \subset E'_0(K_v)$ then $E'(K_v)/\phi E(K_v)$ is trivial while $E(K_v)/\phi' E'(K_v)$ is $\mathrm{H}^1(G_v, E'[\phi'])$. Otherwise the reverse holds.

(ii) When $\mu_\ell \not\subseteq K_v$, $\mathrm{H}^1(G_v, E[\phi]) \cong \langle\pi_v\rangle/\langle\pi_v^\ell\rangle$ while

$$\mathrm{H}^1(G_v, E'[\phi']) \cong K_v(\mu_\ell)^\times/K_v(\mu_\ell)^{\times\ell} \cong k_v(\mu_\ell)^\times/k_v(\mu_\ell)^{\times\ell}.$$

If $E'[\phi'] \subset E'_0(K_v)$ then $E'(K_v)/\phi E(K_v)$ is trivial and $E(K_v)/\phi' E'(K_v)$ is equal to $\mathrm{H}^1(G_v, E'[\phi'])$. Otherwise the reverse holds.

Remarks: (1) This is consistent with Tate local duality (2.3.1). In each case the dimensions of the images of local Mordell-Weil groups add up to the dimension of the local cohomology groups.

Proof of (i): In this case $\mu_\ell \subset K_v$, so $E[\phi] \subset E(K_v)$ and $E'[\phi'] \subset E'(K_v)$. Therefore the reduction cannot be additive, since if it were $E_0(K_v)$ would be a pro-p group and $\#E(K_v)/E_0(K_v)$ would be at most 4 (recall $\ell \geq 5$). Thus E and E' have multiplicative reduction. We will now show they must have split multiplicative reduction. Suppose they have nonsplit reduction; then $c_v(E) = \#E(K_v)/E_0(K_v) \leq 2$ (see Section 1.1.3). Hence $E(K_v)/E_0(K_v)$ and $E_1(K_v)$ have no ℓ-torsion. But $E(K_v)$ contains a point of order ℓ, so $E_0(K_v)/E_1(K_v) \cong E_{\mathrm{ns}}(k_v)$ must have a point of order ℓ. Under the assumption that E has nonsplit reduction, $\#E_{\mathrm{ns}}(k_v) = \#k_v + 1$, but this is not divisible by ℓ, giving a contradiction.

First suppose $E'[\phi'] \not\subseteq E'_0(K_v)$. If $c_v(E) = m$, then $c_v(E') = \ell m$. Consider the maps induced by ϕ on the terms of the exact sequence $0 \to E_{\mathrm{ns}}(k_v) \to E(K_v)/E_1(K_v) \to E(K_v)/E_0(K_v) \to 0$ (and likewise for ϕ'), as shown below.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & k_v^\times & \longrightarrow & E(K_v)/E_1(K_v) & \longrightarrow & \mathbb{Z}/m & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \ell} & & {\scriptstyle \phi}\downarrow & & \downarrow{\scriptstyle \ell} & & \\
0 & \longrightarrow & k_v^\times & \longrightarrow & E'(K_v)/E'_1(K_v) & \longrightarrow & \mathbb{Z}/\ell m & \longrightarrow & 0 \\
 & & \| & & {\scriptstyle \phi'}\downarrow & & \downarrow{\scriptstyle \bmod m} & & \\
0 & \longrightarrow & k_v^\times & \longrightarrow & E(K_v)/E_1(K_v) & \longrightarrow & \mathbb{Z}/m & \longrightarrow & 0
\end{array}$$

The isogenies restrict to isomorphisms on $E_1(K_v)$ and $E'_1(K_v)$, so $E(K_v)/\phi' E'(K_v)$ is trivial and $\dim_{\mathbb{F}_\ell} E'(K_v)/\phi E(K_v) = 2$. On the other hand if $E'[\phi'] \subset E'_0(K_v)$, it follows that $E[\phi] \not\subseteq E_0(K_v)$, as noted in Lemma 1.1.5. Then since $\mu_\ell \subset K_v$, the same argument applies with the roles of E and E' reversed.

Proof of (ii): As always $E'[\phi'] \subset E'(K_v)$; by assumption $\mu_\ell \nsubseteq K_v$ so $E[\phi] \nsubseteq E(K_v)$. As before, we cannot have additive reduction. First suppose $E'[\phi'] \subset E'_0(K_v)$; then $\ell \mid \#E'(k_v)$. Since by assumption $\ell \nmid \#k_v - 1$, the reduction cannot be split multiplicative; it must be nonsplit (and ℓ must divide $\#k_v + 1$). That means $c_v(E)$ and $c_v(E')$ are at most 2, in particular they are prime to ℓ, so the only part of the filtration where the isogenies are not isomorphisms is the middle step. Since $E'[\phi'] \subset E'_0(K_v)$, it sits in $E'_{\mathrm{ns}}(k_v)$; on the other hand since $E[\phi] \nsubseteq E_0(K_v)$, ϕ induces an isomorphism on $E_{\mathrm{ns}}(k_v)$. That is,

$$\begin{array}{ccccc} E_0(K_v)/E_1(K_v) & \xrightarrow{\phi} & E'_0(K_v)/E'_1(K_v) & \xrightarrow{\phi'} & E_0(K_v)/E_1(K_v) \\ \| & & \| & & \| \\ E_{\mathrm{ns}}(k_v) & = & E'_{\mathrm{ns}}(k_v) & \xrightarrow{\ell \text{ to } 1} & E_{\mathrm{ns}}(k_v) \end{array}$$

Hence $E'(K_v)/\phi E(K_v) = 0$ and $\dim_{\mathbb{F}_\ell} E(K_v)/\phi' E'(K_v) = 1$, matching the dimension of $\mathrm{H}^1(G_v, E'[\phi'])$.

Now suppose $E'[\phi'] \nsubseteq E'_0(K_v)$. Then $E'(K_v)/E'_0(K_v)$ must have a point of order ℓ, in other words $\ell \mid c_v(E')$, so E and E' must have split multiplicative reduction. Hence $\#E(k_v) = \#k_v - 1$, which is prime to ℓ, so the relevant part of the filtration is the top step. For some integer m,

$$\begin{array}{ccccc} E(K_v)/E_0(K_v) & \xrightarrow{\phi} & E'(K_v)/E'_0(K_v) & \xrightarrow{\phi'} & E(K_v)/E_0(K_v) \\ \| & & \| & & \| \\ \mathbb{Z}/m & \xrightarrow{\times \ell} & \mathbb{Z}/\ell m & \xrightarrow{\bmod m} & \mathbb{Z}/m \end{array}$$

Hence $\dim_{\mathbb{F}_\ell} E'(K_v)/\phi E(K_v) = 1$ while $E(K_v)/\phi' E'(K_v) = 0$. This proves (ii).

We now do it for places $v \mid \ell$, which could be of any reduction type (including good reduction).

3.3.3 Lemma. *Suppose $v \mid \ell$.*

1. *The cohomology groups $\mathrm{H}^1(G_v, E[\phi])$ and $\mathrm{H}^1(G_v, E'[\phi'])$ have dimension $1 + [K_v : \mathbb{Q}_\ell] + \delta_\ell$ over $\mathbb{F}_\ell$, where*

$$\delta_\ell := \begin{cases} 1 & \text{if } \mu_\ell \subset K_v \\ 0 & \text{otherwise} \end{cases}$$

2. *Suppose E and E' have multiplicative reduction. If $E'[\phi'] \subset E'_0(K_v)$ then $E'(K_v)/\phi E(K_v)$ is trivial while $E(K_v)/\phi' E'(K_v)$ is $\mathrm{H}^1(G_v, E'[\phi'])$. Otherwise the reverse holds.*

Note that the lemma is consistent with Tate local duality.

Proof: The standard structure theorem states that $K_v^\times = \langle \pi_v \rangle \times \mu_d \times (1 + \pi_v O_v)$, where $d = \#k_v - 1$. Note that when $\mu_\ell \subset K_v$ it is contained in $(1 + \pi_v O_v)$. Now

$$\mathrm{H}^1(G_v, E[\phi]) = K_v^\times / K_v^{\times \ell} = \langle \pi_v \rangle / \langle \pi_v^\ell \rangle \times (1 + \pi_v O_v)/(1 + \pi_v O_v)^\ell$$

has dimension $1 + [K_v : \mathbb{Q}_\ell] + \delta_\ell$. By Tate local duality (2.3.1), $\mathrm{H}^1(G_v, E'[\phi'])$ has the same size, proving (1).

To prove (2), first suppose the curves have split multiplicative reduction, so we may use Tate uniformisations. If $E'[\phi'] \subset E'_0(K_v)$, then the isogenies must be as follows.

$$\begin{array}{ccccc} E(K_v) & \xrightarrow{\phi} & E'(K_v) & \xrightarrow{\phi'} & E(K_v) \\ \| & & \| & & \| \\ K_v^\times / q^{\mathbb{Z}} & \xrightarrow{\ell} & K_v^\times / q^{\ell\,\mathbb{Z}} & \xrightarrow{\text{mod } q} & K_v^\times / q^{\mathbb{Z}} \end{array}$$

So $E(K_v)/\phi' E'(K_v) = 0$ and $E'(K_v)/\phi E(K_v) = K_v^\times / K_v^{\times \ell}$ has the same dimension as $\mathrm{H}^1(G_v, E'[\phi'])$. If $E'[\phi'] \not\subseteq E'_0(K_v)$, the situation is reversed.

Now suppose the curves have nonsplit multiplicative reduction. This is possible, but only in the unusual circumstance that $K_v(\mu_\ell)$ is the unramified quadratic extension of K_v. For let L_v/K_v be the unramified quadratic extension. Then there's a

Tate uniformisation

$$t : L_v^\times/q^{\mathbb{Z}} \cong E'(L_v)$$

for some $q \in K_v$. Recall from Section 1.1.3 that the subgroup $E'(K_v)$ equals the kernel of N_{L_v/K_v} on $L_v^\times/q^{\mathbb{Z}}$. As always $E'[\phi'] \subset E'(K_v)$, and indeed $E'[\phi'] \subset E'_0(K_v)$ since $\#E'(K_v)/E'_0(K_v) \leq 2$ when E' has nonsplit reduction. Now $E'_0(L_v)$ is the image under t of $O_{L_v}^\times$ so t identifies $E'[\phi']$ with ℓ-torsion in $O_{L_v}^\times$, which must be μ_ℓ. This implies $\mu_\ell \subset L_v$. Since $E'[\phi'] \subset E'(K_v)$, and $E'(K_v)$ is the kernel of the norm on $L_v^\times/q^{\mathbb{Z}}$, we have $\mathrm{N}_{L_v/K_v}\,\zeta_\ell = 1$. In particular $\mu_\ell \not\subseteq K_v$, so $L_v = K_v(\mu_\ell)$. The curves have split reduction over L_v, so we may use Tate uniformisations to describe ϕ and ϕ' on $E(L_v)$ and $E'(L_v)$; since $E'[\phi'] \subset E'_0(K_v) \subset E'_0(L_v)$, the isogenies must be as follows.

$$\begin{array}{ccccc} E(L_v) & \xrightarrow{\phi} & E'(L_v) & \xrightarrow{\phi'} & E(L_v) \\ \| & & \| & & \| \\ L_v^\times/q^{\ell\,\mathbb{Z}} & \xrightarrow{\text{mod } q} & L_v^\times/q^{\mathbb{Z}} & \xrightarrow{\ell} & L_v^\times/q^{\ell\,\mathbb{Z}} \end{array}$$

Next we'll check that ϕ is a surjection on K_v-points. Suppose $\alpha \in L_v^\times$ with $t(\alpha) \in E'(K_v)$. This means $\mathrm{N}_{L_v/K_v}\,\alpha = q^a$ for some $a \in \mathbb{Z}$. Since ℓ is odd, we may find $b \in \mathbb{Z}$ with $\ell \mid a + 2b$. Then αq^b is the required preimage of α, for ϕ maps it to $\alpha \mod q^{\mathbb{Z}}$, and $t(\alpha q^b) \in E(K_v)$ since $\mathrm{N}(\alpha q^b) = q^{a+2b} \in q^{\ell\mathbb{Z}}$. Therefore $E'(K_v)/\phi E(K_v) = 0$.

Finally, to determine the rank of the cokernel of ϕ' on K_v-points, consider

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'_0(K_v) & \longrightarrow & O_{L_v}^\times & \xrightarrow{\mathrm{N}} & O_{K_v}^\times & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'} & & \downarrow{\scriptstyle \ell} & & \downarrow{\scriptstyle \ell} & & \\ 0 & \longrightarrow & E_0(K_v) & \longrightarrow & O_{L_v}^\times & \xrightarrow{\mathrm{N}} & O_{K_v}^\times & \longrightarrow & 0 \end{array}$$

We can read off the cokernels of the vertical maps. They are all elementary ℓ-groups: on the right having rank $[K_v : \mathbb{Q}_\ell]$ and in the middle having rank $[L_v : \mathbb{Q}_\ell] + 1 = 2[K_v : \mathbb{Q}_\ell] + 1$ where the extra 1 is because μ_ℓ is in L_v but not K_v. By exactness the

cokernal of ϕ' has rank $[K_v : \mathbb{Q}_\ell]+1$, therefore $\dim_{\mathbb{F}_\ell} E(K_v)/\phi' E'(K_v) = [K_v : Q_\ell]+1$. This matches the dimension of $\mathrm{H}^1(G_v, E'[\phi'])$, since $\delta_\ell = 0$ as μ_ℓ is in L_v but not K_v.

3.4 Descent Theorem

The following theorem combines the local information from the previous section, giving a description of the Selmer groups.

3.4.1 Theorem. *Suppose the dual isogenies $\phi : E \to E'$ and $\phi' : E' \to E$ are defined over K, with $E[\phi] \cong \mu_\ell$ and $E'[\phi'] \cong \mathbb{Z}/\ell$ as G_K-modules, where $\ell \geq 5$ is an odd prime. Let $\mathcal{G}$ denote the set of places $v \nmid \ell$ of K where E and E' have good reduction, and partition the remaining $v \nmid \ell$ as follows:*

$$\mathcal{A} = \{v \notin \mathcal{G} : v \nmid \ell,\ E'[\phi'] \not\subseteq E'_0(K_v)\}$$
$$\mathcal{B} = \{v \notin \mathcal{G} : v \nmid \ell,\ E'[\phi'] \subset E'_0(K_v)\}$$

Then $\mathrm{Sel}^\phi(E, K)$ is the subset of $K^\times/K^{\times\ell}$ represented by

$$\left\{\alpha \in K^\times : \ell \mid ord_v\, \alpha \ \ \forall\ v \in \mathcal{G},\ \alpha \in K_v^{\times\ell}\ \forall\ v \in \mathcal{B},\ \text{and } \alpha \in \mathfrak{L}_v \ \ \forall\ v \mid \ell\right\}$$

where for each $v \mid \ell$, $\mathfrak{L}_v$ is a subgroup of $K_v^\times$ containing $K_v^{\times\ell}$.

Put $K(\mu_\ell) = L$, let χ be the cyclotomic character on G_K, and for given v let w denote an extension of v to L. Then $\mathrm{Sel}^{\phi'}(E', K)$ is the subset of $\left(L^\times/L^{\times\ell}\right)^\chi$ represented by

$$\left\{\alpha : \ell \mid ord_w\, \alpha \ \ \forall\ v \in \mathcal{G},\ \alpha \in L_w^{\times\ell} \ \ \forall\ v \in \mathcal{A},\ \text{and } \alpha \in \mathfrak{L}'_v \ \ \forall\ v \mid \ell\right\}$$

where for each $v \mid \ell$, $\mathfrak{L}'_v$ is a subgroup of $L_w^\times$ containing $L_w^{\times\ell}$.

For each given v, it does not matter which extension w one chooses. Note that for v with $\mu_\ell \not\subseteq K_v$, the condition $\alpha \in K_v^\times$ is equivalent to the unit condition $\alpha \in \mathfrak{O}_v^\times$.

Proof: Fix an embedding of $\overline{K}$ into $\overline{K_v}$, for each place. This specifies an identification of $G_v = \mathrm{Gal}(\overline{K_v}/K_v)$ with a particular subgroup of $G_K = \mathrm{Gal}(\overline{K}/K)$, namely the

subgroup fixing $\overline{K} \cap K_v \subset \overline{K_v}$. It also specifies a choice of w, and an embedding of L into L_w.

By definition, $\mathrm{Sel}^{\phi}(E, K)$ is the set of cocycles whose restrictions lie in the images of the local Mordell-Weil groups for each v:

$$\begin{array}{ccccc} & & & & \mathrm{H}^1(G, E[\phi]) \\ & & & & \Big\downarrow{\scriptstyle \mathrm{res}_v} \\ 0 & \longrightarrow & E'(K_v)/\phi E(K_v) & \longrightarrow & \mathrm{H}^1(G_v, E[\phi]) \end{array}$$

and likewise for $\mathrm{Sel}^{\phi'}(E', K)$. First consider $\mathrm{Sel}^{\phi}(E, K)$, which is less complicated. By Kummer theory $\mathrm{H}^1(G_K, E[\phi]) = \mathrm{H}^1(G_K, \mu_\ell) \cong K^\times/K^{\times \ell}$. and similarly $\mathrm{H}^1(G_v, E[\phi]) = K_v^\times/K_v^{\times \ell}$. The restriction map respects these identifications, in other words the following diagram commutes.

$$\begin{array}{ccc} K^\times/K^{\times \ell} & \longrightarrow & \mathrm{H}^1(G, \mu_\ell) \\ \Big\downarrow & & {\scriptstyle \mathrm{res}_v}\Big\downarrow \\ K_v^\times/K_v^{\times \ell} & \longrightarrow & \mathrm{H}^1(G_v, \mu_\ell) \end{array}$$

where the left vertical arrow is induced by our fixed embedding of K into K_v. To see this, recall that the first row is the Kummer map sending $\alpha \in K^\times$ to the cocycle $\sigma \mapsto \frac{\sigma\beta}{\beta}$, for some $\beta \in \overline{K}$ with $\beta^\ell = \alpha$. The second row sends α to $\sigma \mapsto \frac{\sigma\beta_v}{\beta_v}$, where we may take β_v to be the image of β in K_v. Then this cocycle is the restriction to G_v of the other cocycle.

Now we read off the Selmer condition imposed by each place from the lemmas in the previous section. For infinite places $\mathrm{H}^1(G_v, E[\phi])$ is either $\mathbb{R}^\times/\mathbb{R}^{\times \ell}$ or $\mathbb{C}^\times/\mathbb{C}^{\times \ell}$, which are both trivial since ℓ is odd. Hence $\mathrm{H}^1(G_v, E[\phi])$ is equal to $E'(K_v)/\phi E(K_v)$ for infinite places, which therefore impose no conditions for a cocycle to be in the Selmer group.

For $v \in \mathcal{G}$, by Lemma 3.3.1 the condition for $\alpha \in K_v^\times$ to be in the Selmer group is that its restriction be in

$$\mathrm{H}^1_{\mathrm{un}}(G_v, \mu_\ell) \cong \mathfrak{O}_v^\times/\mathfrak{O}_v^{\times \ell}$$

Equivalently, the image of α in K_v should be a unit times an ℓth power, in other words $\mathrm{ord}_v \alpha \equiv 0 \mod \ell$.

For $v \in \mathcal{A}$, by Lemma 3.3.2 the Selmer condition is vacuous, since every element of $\mathrm{H}^1(G_v, E[\phi])$ is in the image of $E'(K_v)/\phi E(K_v)$.

For $v \in \mathcal{B}$, by Lemma 3.3.2 the Selmer condition is that α restricts to the trivial element in $\mathrm{H}^1(G_v, E[\phi]) = K_v^\times / K_v^{\times \ell}$, in other words that the image of α is in $K_v^{\times \ell}$.

Finally for $v \mid \ell$, simply observe that $E'(K_v)/\phi E(K_v)$ must be isormorphic to *some* subgroup $\mathfrak{L}_v / K_v^{\times \ell}$ of $\mathrm{H}^1(G_v, E[\phi]) \cong K_v^\times / K_v^{\times \ell}$.

The argument for $\mathrm{Sel}^{\phi'}(E', K)$ is very similar. Lemma 3.2.2 gives an identification of $\mathrm{H}^1(G_K, E[\phi'])$ with $\left(L^\times / L^{\times \ell}\right)^\chi$, where $\chi : G \to \mathbb{Z}/\ell$ is the cyclotomic character defined by $\sigma \zeta_\ell = \zeta_\ell^{\chi(\sigma)}$. The same calculation shows $\mathrm{H}^1(G_v, E[\phi']) \cong \left(L_w^\times / L_w^{\times \ell}\right)^{\chi_v}$, where $L_w = K_v(\mu_\ell)$ and χ_v is the restriction of χ to G_v.

To see that restriction respects the Kummer maps, one checks that the following diagram commutes.

$$\begin{array}{ccccc}
\mathrm{H}^1(G, \mathbb{Z}/\ell) & = & \mathrm{H}^1(G_L, \mathbb{Z}/\ell)^{\mathrm{Gal}(L/K)} & = & \left(L^\times / L^{\times \ell}\right)^\chi \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{H}^1(G_v, \mathbb{Z}/\ell) & = & \mathrm{H}^1(G_w, \mathbb{Z}/\ell)^{\mathrm{Gal}(L_w/K_v)} & = & \left(L_w^\times / L_w^{\times \ell}\right)^{\chi_v}
\end{array}$$

where G_w is the subgroup $\mathrm{Gal}(\overline{L_w}/L_w)$.

Infinite places again impose no Selmer conditions, since $L_w^\times / L_w^{\times \ell} = \mathbb{C}^\times / \mathbb{C}^{\times \ell}$ when v is infinite.

For $v \in \mathcal{G}$, by Lemma 3.3.1 the condition imposed by v for $\alpha \in \left(L_w^\times / L_w^{\times \ell}\right)^{\chi_v}$ to be in the Selmer group is that the restriction of α lies in $\mathrm{H}^1_{\mathrm{un}}(G_v, \mathbb{Z}/\ell)$. Recall that $\mathrm{H}^1(G_v, \mathbb{Z}/\ell)$ classifies cyclic extentions of degree ℓ over K_v, and $\mathrm{H}^1_{\mathrm{un}}(G_v, \mathbb{Z}/\ell)$ classifies unramified extensions. Since $L_w = K_v(\mu_\ell)$ is unramified over K_v, $\alpha \in \mathrm{H}^1(G_v, \mathbb{Z}/\ell)$ corresponds to an unramified extension of K_v if and only if its image in $\mathrm{H}^1(G_w, \mathbb{Z}/\ell)$ corresponds to an unramified extension of L_w. But $\mathrm{H}^1(G_w, \mathbb{Z}/\ell) = \mathrm{H}^1(G_w, \mu_\ell)$ is the unit subgroup $\mathfrak{O}_w^\times / \mathfrak{O}_w^{\times \ell}$ of $L_w^\times / L_w^{\times \ell}$. So the Selmer condition is that

in $L_w^\times$, α can be written as a power of π_w^ℓ times an element of $\mathfrak{O}_w^\times$, or more simply $\mathrm{ord}_w\alpha \equiv 0 \mod \ell$ as the theorem states.

For $v \in \mathcal{A}$, by Lemma 3.3.2 the Selmer condition is that α restricts to the trivial element in $\mathrm{H}^1(G_v, E[\phi]) = K_v(\mu_\ell)^\times / K_v(\mu_\ell)^{\times\ell}$, that is $\alpha \in K_v(\mu_\ell)^{\times\ell}$.

For $v \in \mathcal{B}$, by Lemma 3.3.2 the Selmer condition is vacuous.

For $v \mid \ell$, the image of $E(K_v)/\phi' E'(K_v)$ must be *some* subgroup of $\left(L_w^\times / L_w^{\times\ell}\right)^{\chi_v}$, which in turn is a subgroup of $L_w^\times / L_w^{\times\ell}$. Any such subgroup has the form $\mathfrak{L}_v' / L_w^{\times\ell}$.

Chapter 4

A convenient model of $X_0(14)$

4.1 Introduction

This chapter performs a technical task that is needed for the next chapter, where we will look for elliptic curves that have Tate-Shafarevich groups with large 7-torsion. The method will require us to use elliptic curves with isogenies of degree 7 *and* 2, defined over quadratic extensions of $\mathbb{Q}$. Such curves are classified by the moduli space $X_0(14)$. As it happens, $X_0(14)$ is itself an elliptic curve defined over $\mathbb{Q}$, which means that it has a degree 2 map to $\mathbf{P}^1$. In this section we construct an explicit model for $X_0(14)$ and the map to $\mathbf{P}^1$ suited to the application we have in mind. In particular the model will be symmetric with respect to the Atkin-Lehner involution w_{14}.

The argument in chapter 5 could probably be done abstractly, without using the explicit model. However, one reason to do it explicitly is so that we can use the method to compute examples.

4.1.1 Outline of the method

Points on the moduli space $X_0(14)$ represent isogenies of degree 14 between elliptic curves. There is a natural involution w_{14} on $X_0(14)$ which sends an isogeny to its dual isogeny. The curve $X_0(14)$ has a map of degree 3 to $X_0(7)$; since $X_0(7)$ is isomorphic to $\mathbf{P}^1$, the map is given by a single element $p \in K(X_0(14))$. The model for $X_0(14)$ we will find is a plane curve with coordinate functions p and $p \circ w_{14}$. The $\mathbb{Q}$-rational map to $\mathbf{P}^1$ is then obtained by taking the quotient by the action of w_{14}.

Our method for finding the relationship between p and p_{14} is somewhat elaborate, meandering through several topics. The basic idea is to take advantage of the complex analytic picture of $X_0(14)$ as a quotient of the upper half plane, in which p and $p \circ w_{14}$ are modular functions. The theory gives us a formula for the q-expansions of p and $p \circ w_{14}$, and by computing the first few terms of the q-expansions we can determine the polynomial relationship between them. To reduce the number of terms needed, we first find out where the model intersects the diagonal $p = p \circ w_{14}$. The intersection points correspond to curves with a special endomorphism, so we can find them using the theory of complex multiplication.

It would be interesting to know whether there is a simpler, more direct way to find the explicit formulas we need, that does not resort to such deep and exotic considerations.

4.2 Curves with a 7-torsion point

Recall the familiar model for $E_1(7)$, the universal elliptic curve with a distinguished rational point of order 7:

$$E_1(7) \;:\; y^2 + (1 - c - c^2)xy + c^2(c+1)y = x^3 + c^2(c+1)x^2$$

for $c \neq 0$ or 1, where the distinguished 7-torsion point is $(0, 0)$. We will derive this here, because we will use the procedure later. For the sake of precision, $E_1(7)$ will denote the surface cut out by the above equation inside $\mathbf{P}^2_{x,y} \times \mathbf{A}^1_c \setminus \{0, 1\}$, and E_c will denote the fiber above c. Suppose we are given any elliptic curve defined over some field $\mathbb{F}$, with a distinguished rational 7-torsion point. We will now construct an isomorphism over $\mathbb{F}$ to one of the fibers E_c, sending the distinguished 7-torsion point to $(0, 0)$. First put the curve in Weierstrass form (which is possible over any field) and then translate the given point to $(0, 0)$. Then the curve has the form

$$y^2 + axy + by = x^3 + cx^2 + dx\,.$$

Since $(0,0)$ does not have order 2, the curve does not have a vertical tangent there, which means $b \neq 0$. The substitution $y = y + (d/b)x$ puts the curve in the form

$$y^2 + axy + by = x^3 + cx^2$$

(where a,b and c have changed). We calculate that the x coordinate of $[2](0,0)$ is $-c$, and since $(0,0)$ does not have order 3, this is different from 0. Now the scaling substitution $(x,y) = ((b/c)^2x, (b/c)^3y)$ makes $b = c$. Replace a by $1-a$ and let $C = b/a$. We calculate the x coordinate of $[3](0,0)$ is a, and that of $[4](0,0)$ is $C^2 + (1-a)C - a - b$. Since $(0,0)$ has order 7 these are the same, and it follows that $a = 1 - C - C^2$ and $b = C^2(C+1)$.

This shows that for any field K, any elliptic curve E over K and any choice $P \in E(K)[7]$, the pair (E,P) is isomorphic over K to $(E_c, (0,0))$ for some $c \in K$. In fact this value of c is unique; to see this one checks that for generic values of c there is no isomorphism of E_c to some other $E_{c'}$ sending $(0,0)$ to $(0,0)$ (see [Si1], Section III.1 for the general form of an isomorphism between two elliptic curves in Weierstrass form). Therefore there is a bijection between K-isomorphism classes of such pairs (E,P) and values of the parameter $c \in \mathbf{A}^1(K) \setminus \{0,1\}$; this $\mathbf{A}^1_c \setminus \{0,1\}$ is $X_1(7)$, the 'moduli space' for $\Gamma_1(7)$ structure.

4.2.1 Example

When we apply this procedure starting with the curve E_c and the 7 torsion point $P = [2](0,0)$, we obtain an isomorphism from E_c to $E_{c'}$ taking P to $(0,0)$, where $c' = \frac{-c-1}{c}$. The isomorphism is

$$(x,y) \to \left(\frac{x + c^2(c+1)}{c^4}, \frac{y - (c^2-1)x + c^2(c+1)^2}{c^6} \right)$$

and these maps taken together give us an automorphism of the surface $E_1(7)$,

$$\mu(c,x,y) = \left(\frac{-c-1}{c}, \frac{x + c^2(c+1)}{c^4}, \frac{y - (c^2-1)x + c^2(c+1)^2}{c^6} \right)$$

This automorphism has order 3, since μ^3 maps each fiber $(E_c, [8](0,0))$, which is $(E_c, (0,0))$, to some other $(E_{c'}, (0,0))$, but for a generic fiber the only such map is the identity map of E_c to itself, which means μ^3 is the identity map on the surface.

Note that if we applied the process starting with $(E_c, [-1](0,0))$, we would end up with the automorphism $(c, x, y) \to (c, x, -y)$ which is the inverse map on each fiber. Thus there are at most three different choices of the parameter c associated to each subgroup of order 7 on an elliptic curve which agrees with the fact that $[\Gamma_1(7) : \Gamma_0(7)] = 3$.

4.3 An 'almost universal' family $E_0(7)$

Next we construct a quotient of $E_1(7)$ by μ, which will almost be an 'universal family for $\Gamma_0(7)$ structure'. If μ maps a value c to itself, then so does μ^2, and E_c has an automorphism of order 3, which means it has complex multiplication by cube roots of unity and has j-invariant 0. This happens for only finitely many values of c, since the j invariant map $X_1(7) \to X(1) = \mathbf{A}^1_j$ has finite degree. For other values of c, μ identifies three different fibers isomorphically. Thus each fiber with $j \neq 0$ maps to an isomorphic copy in the quotient. On fibers with $j = 0$, μ restricts to an automorphism of order 3, which has at least one fixed point; therefore the quotient map restricted to this fiber has ramification and so by the Riemann-Hurwitz formula its image must have genus zero.

Remark: One cannot avoid this kind of degeneration on fibers with extra automorphisms. In fact this leads to a proof that there is *no* universal family for $X_0(7)$ and hence that $X_0(7)$ is not a 'fine moduli space'.

Earlier we identified $X_1(7)$ with a subset of $\mathbf{A}^1_c$, so in particular the function field $K(X_1(7))$ equals $K(c)$. Now, μ permutes the three values of c associated to a single 7-torsion group, in other words it permutes each fiber of the map $X_1(7) \to X_0(7)$. In

fact, the associated extension of function fields is a Galois extension of degree 3 and μ generates the Galois group. As we computed in the example, the three conjugates under μ are c, $\frac{-c-1}{c}$ and $\frac{-1}{c+1}$, so the sum of these

$$g = -\frac{c^3 + 3c^2 - 1}{c(c+1)} \tag{4.1}$$

must be in $K(c)^\mu = K(X_0(7))$. But since c has degree 3 over $K(g)$, $K(g)$ equals $K(X_0(7))$.

Now we will find a model for the quotient of $E_1(7)$ by μ, which we will call $E_0(7)$. It will be a surface fibered over $X_0(7) \subset \mathbf{A}^1_g$, with fibers E_g. The traces of x and y in $K(E_1(7))$ are in the fixed field $K(E_0(7))$.

$$\begin{aligned} s &:= \operatorname{Tr} x = x + \mu^* x + (\mu^2)^* x \\ t &:= \operatorname{Tr} y = y + \mu^* y + (\mu^2)^* y \end{aligned} \tag{4.2}$$

From the definition of μ it is clear that s is linear in x over $K(c)$, and that t is linear in x and y over $K(c)$. Thus g, s and t generate a subextension of index 3 in $K(E_1(7))$ (which is generated by c, x and y), and so they must generate $K(E_0(7))$.

By taking some resultants, using Maple, we compute the following relationship between g, s and t. Write $p = g - 5$ (this will be more convenient later). Except for the leading coefficients, this equation is a Weierstrass model for $E_0(7)$ over $\mathbf{A}^1_p$.

$$\begin{aligned} &t^2(-p^8 - 52p^7 - 1198p^6 - 15964p^5 - 134539p^4 \\ &\qquad - 734188p^3 - 2533410p^2 - 5054400p - 4465125) \\ &+st(p^{10} + 65p^9 + 1919p^8 + 33878p^7 + 395976p^6 + 3201380p^5 + 18128879p^4 \\ &\qquad + 70998135p^3 + 184026145p^2 + 285076350p + 200434500) \\ &+t(p^{11} + 72p^{10} + 2378p^9 + 47545p^8 + 639276p^7 + 6068676p^6 + 41500949p^5 \\ &+204438384p^4 + 710941648p^3 + 1662276995p^2 + 2352091950p + 1526080500) = \end{aligned}$$

$$
\begin{aligned}
&= -s^3(p^8 + 52p^7 + 1198p^6 + 15964p^5 + 134533p^4 + 734032p^3 + 2531836p^2 \\
&\qquad + 5047120p + 4452100) \\
&-s^2(-p^{11} - 72p^{10} - 2377p^9 - 47487p^8 - 637755p^7 - 6045017p^6 - 41260464p^5 \\
&\quad -202782195p^4 - 703214561p^3 - 1638726301p^2 - 2309541170p - 1491350475) \\
&\quad -s(-2p^{10} - 130p^9 - 3847p^8 - 68224p^7 - 802731p^6 - 6546312p^5 - 37466398p^4 \\
&\qquad - 148582310p^3 - 390730538p^2 - 615263810p - 440555550) \\
&\quad -2p^9 - 113p^8 - 2874p^7 - 43151p^6 - 421215p^5 - 2770668p^4 - 12275179p^3 \\
&\qquad - 35305948p^2 + 59792760p - 45403675
\end{aligned}
\tag{4.3}
$$

From the Weierstrass model for $E_1(7)$ we can compute a formula for the j-invariant of E_c. Combining that formula with (4.1) and eliminating c, we find

$$
j(g) = j(E_g) = \frac{(g^2+3g+9)(g^2-5g+1)^3}{g-5} = \frac{(p^2+13p+49)(p^2+5p+1)^3}{p} \tag{4.4}
$$

4.4 A model for $X_0(14)$

We could easily use (4.3) to make a model of $X_0(14)$, because the choice of a 2-torsion point is simply the choice of a root of the cubic in s on the right hand side of (4.3). However this would be too unwieldy; after all we know that $X_0(14)$ has genus one. We will make a model by another method clearly revealing the Atkin-Lehner involution w_{14}, which can be defined in terms of the modular interpretation of $X_0(14)$ as follows. Given a point $\mathcal{P}$ on $X_0(14)$, choose a pair $(E, C_{14} \subset E[14])$ in the isomorphism class associated to $\mathcal{P}$; this is equivalent to choosing an isogeny $(E \to E')$ whose kernel has order 14. Take the dual isogeny $(E' \to E)$, whose kernel also has order 14 and let $\mathcal{P}'$ be the associated point on $X_0(14)$. Define $w_{14}(\mathcal{P}) = \mathcal{P}'$.

4.4.1 Finding the fixed points of w_{14}

Fixed points of w_{14} arise from curves having a certain kind of complex multiplication.

4.4.1 Lemma. *Suppose $E \to E'$ is an isogeny of degree n with cyclic kernel, and that E is isomorphic to E'. Then E has complex multiplication by a ring containing an element of norm n.*

Proof: We may assume $E = \mathbb{C}/\langle 1, \tau\rangle$ and $E' = \mathbb{C}/\langle 1, \frac{\tau}{n}\rangle$. Since they are isomorphic, there must be a complex number λ such that

$$\lambda \langle 1, \frac{\tau}{n}\rangle = \langle 1, \tau\rangle$$

Thus $\lambda \in \mathrm{End}(E')$, and as a map of $\mathbb{Z}$-modules it has determinant n. Hence $N(\lambda) = n$, proving the lemma.

There are only finitely many quadratic imaginary elements of given norm, so there are only finitely many fixed points of w_n on $X_0(n)$. This also follows from the Riemann-Hurwitz formula, since the fixed points are ramification points of the quotient map. In particular for $X_0(14)$, which has genus one, there can be at most 4 fixed points.

We easily check that one fixed point is $(E = \mathbb{C}/\mathbb{Z}[\sqrt{-14}],\ P = \sqrt{-14}/14)$, which is represented by $\tau = \sqrt{-14}$ in the upper half plane. As it happens, $\mathbb{Z}[\sqrt{-14}]$ has class number 4. The theory of complex multiplication tells us that the j-invariant of this curve has degree 4 over $\mathbb{Q}$, and that the conjugates are the j-invariants of the curves $\mathbb{C}/L$ for other ideals L of $\mathbb{Z}[\sqrt{-14}]$. So the fixed point of $X_0(14)$ given above has *at least* 4 conjugates over $\mathbb{Q}$. Now $X_0(14)$ and w_{14} are defined over $\mathbb{Q}$, so all conjugates of a fixed point are also fixed. But in the previous paragraph we showed there are at most 4 fixed points, so we conclude that there are exactly 4 fixed points, all conjugate.

The computer package Pari tells us that the ideal class group is cyclic, and is generated by the ideals above (3). Therefore the four ideal classes are represented in the upper half plane by $\tau = \sqrt{-14}$, $\frac{-1-\sqrt{-14}}{3}$, $\frac{-3}{1+\sqrt{-14}}$ and $\frac{\sqrt{-14}-16}{9}$. Again using Pari, one can compute the corresponding values of the j-invariant, approximately, as complex numbers. But we know that these values $j(\tau)$ are algebraic integers, so one can then determine that their minimal polynomial is exactly

$$j^4 - 16220384512j^3 + 2059647197077504j^2 + 2257767342088912896j + 10064086044321563803648$$

Using (4.4), one finds that the values of g on $X_0(7)$ mapping to these values of j are the zeros of $g^4 - 34g^3 + 115g^2 + 214g + 2081$, and the zeros of an irreducible polynomial of degree 28. Therefore $g^4 - 34g^3 + 115g^2 + 214g + 2081$ must be the minimal polynomial of the 'g coordinates' of the 4 fixed points.

4.4.2 Using the fixed points of w_{14}

Our model of $X_0(14)$ will be a plane curve $\mathcal{C}$ with coordinate functions g and $\tilde{g} := g \circ w_{14}$. Geometrically, since $X_0(7) = \mathbf{A}^1_g$, $\mathcal{C}$ is the projection to $X_0(7) \times X_0(7)$ of the graph of w_{14} in $X_0(14) \times X_0(14)$. We claim $\mathcal{C}$ is birational to $X_0(14)$, because g and $\tilde{g}$ generate $K(X_0(14))$. If they did not we would have $K(g) = K(\tilde{g})$. However for a point $(E, C_7, P \in E[2])$ on $X_0(14)$, g gives its image (E, C_7) on $X_0(7)$, but this does not determine the value of $\tilde{g}$ because generically the j-invariants of the 14-isogenous curves $E/\langle C_7, P\rangle$ are different for the 3 choices of P.

Since w_{14} is an involution, its graph $\{(x, w_{14}(x))\} \subset X_0(14) \times X_0(14)$ is symmetric, and therefore $\mathcal{C}$ will be symmetric in the line $g = \tilde{g}$. It has degree 3 separately in g and $\tilde{g}$, because $\tilde{g}$ has degree 3 above $K(g)$ and vice versa. Therefore $\mathcal{C}$ has total degree at most 6. It intersects the line $g = \tilde{g}$ in the roots of $g^4 - 34g^3 + 115g^2 + 214g + 2081$, which we found above as the g values of the

fixed points of w_{14}. We now look for the other intersections of $\mathcal{C}$ with $g = \tilde{g}$ (which do not come from fixed points of w_{14}). We could find them by tediously examining all curves having a complex endomorphism of degree 14. The following method requires less computational work, although it takes longer to explain. Any other intersection would be a singular point of $\mathcal{C}$, since it would be the image of a point $\mathcal{P}$ of $X_0(14)$ that is *not fixed* by w_{14}, and so $\mathcal{P}$ and $w_{14}(\mathcal{P})$ would be different points with the same image on $\mathcal{C}$. Since $\deg \mathcal{C} \leq 6$, if there is another intersection it is the only one, it is rational, and has multiplicity 2. Consider the map $\mathcal{C}$ to $\mathbf{A}^2$ given by $(g, \tilde{g}) \mapsto (j(g), j(\tilde{g}))$. The image is again birational to $X_0(14)$ for the same reason that $\mathcal{C}$ is. Let $\Phi_{14}(j, j_{14})$ denote the irreducible polynomial defining it. Our hypothetical $\mathcal{P}$ would map to a rational root of $\Phi_{14}(j, j)$. By Theorem 11 on page 143 of [La], the roots of $\Phi_{14}(j, j)$ are the j-invariants of curves corresponding to imaginary quadratic orders that have elements of norm 14, and the multiplicity of the root equals the number of such elements modulo units. We can easily list all imaginary quadratic integers with norm 14, and using Pari we found that for all except two of them, the orders they generate have class number greater than 1. That means the j-invariants of the corresponding curves are not rational. The exceptions are $\frac{7+\sqrt{-7}}{2}$ and its conjugate, in the order $\mathbb{Z}[1, \frac{1+\sqrt{-7}}{2}]$, so the corresponding value $j = -3375$ is a root with multiplicity 2. Using (4.4), the values of g with $j(g) = -3375$ are $g = -2$ and the zeros of an irreducible septic. Now let $\mathcal{P} \in X_0(14)$ denote a point with $j(\mathcal{P}) = j_{14}(\mathcal{P})$. Since j and w_{14} are defined over $\mathbb{Q}$, all conjugates of $\mathcal{P}$ have the same property; if $g(\mathcal{P})$ were septic there would be at least 7 such points, but we noted already there are only two. Hence $g(\mathcal{P}) = -2$ and for the same reason $\tilde{g}(\mathcal{P}) = -2$. We conclude that $\mathcal{C}$ intersects $g = \tilde{g}$ doubly at $g = -2$, and there are no other intersections.

In coordinates $x = \frac{g+\tilde{g}}{2}$ and $y = \frac{g-\tilde{g}}{2}$, $\mathcal{C}$ must take the form

$$ay^6 + p_2(x)y^4 + p_4(x)y^2 = (x+2)^2(x^4 - 34x^3 + 115x^2 + 214x + 2081) \qquad (4.5)$$

where p_2 and p_4 are undetermined polynomials of degrees 2 and 4. To find their coefficients, we will compute part of the q-expansions of the modular functions g and $\tilde{g}$.

4.4.3 Using the q-expansions

Define functions $\eta(\tau)$ and $p(\tau)$ on the upper half plane as follows.

$$\begin{aligned} \eta(q) &= q^{1/24}\prod_{n\geq 1}(1-q^n) \text{ where } \ q = e^{2\pi i\tau}\,, \\ p(q) &= 49\ \frac{\eta(q^7)^4}{\eta(q)^4}\,. \end{aligned} \qquad (4.6)$$

From [Bi] we learn that $p(\tau)$ is a well defined function on $X_0(7)$, and its only poles and zeros on $X_0(7)$ are a single zero at the cusp $\tau = i\infty$ and a single pole at the cusp $\tau = 0$. We now show that $g - 5$ has the same poles and zeros on $X_0(7)$. The cusps on $X_0(7)$ are the points where $j = \infty$; from (4.4) the possible values of g at these points are 5 and ∞. Moreover from (4.4) one can see that the map $g \mapsto j$ is unramified at $g = 5$ and has ramification degree 7 at $g = \infty$. Now, $\tau = 0$ is a cusp of width 7 on $X_0(7)$ which means the map $X_0(7) \to j$ has ramification degree 7 there; the other cusp has width 1 and so the map is unramified there. Thus $\tau = i\infty$ is the same point on $X_0(7)$ as $g = 5$, while $\tau = 0$ is the point $g = \infty$. As mentioned above, the only zero of p is at $\tau = i\infty$ and its only pole is at $\tau = 0$. Therefore $g - 5 = Cp$ for some constant C. One may identify the constant by substituting the q-expansion $g = 5 + Cp(q)$ into (4.4); then one must take $C = 1$ in order to obtain the usual q-expansion for the j-invariant.

The involution w_{14} can be given as a function on the upper half plane by $\tau \mapsto \frac{-1}{14\tau}$. The functional equation for $\eta(\tau)$ implies that $p(\tau)p(\frac{-1}{7\tau}) = 49$. We define the function

$\tilde{p}(\tau)$ on the upper half plane as

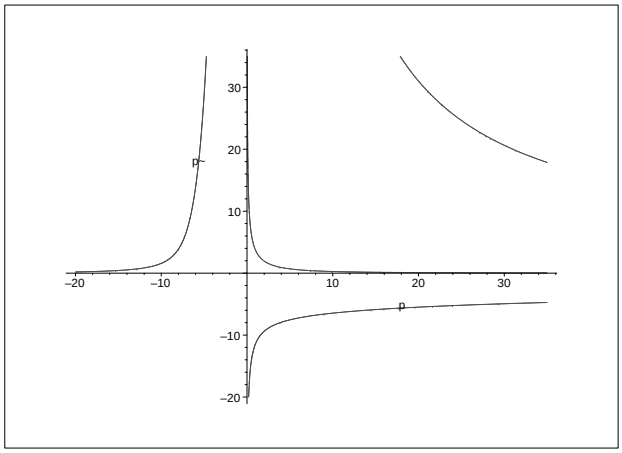
$$\tilde{p}(\tau) := p\left(\frac{-1}{14\tau}\right) = \frac{49}{p(2\tau)} = \frac{49}{p(q^2)}\,. \tag{4.7}$$

Using Maple one can compute the beginning of the q-expansion of p using (4.6), and that of $\tilde{p}$ using the (4.7). Substituting these into (4.5) determines the coefficients exactly: our model $\mathcal{C}$ of $X_0(14)$ turns out to be

$$p^3\tilde{p}^3 - 392p^2\tilde{p}^2 - 2401(p\,\tilde{p}^2 + p^2\tilde{p}) - 19208p\,\tilde{p} + 117649 = 0 \tag{4.8}$$

Note: In principle, we could obtain this relationship between p and $\tilde{p}$ from their q-expansions alone, without knowing (4.5), but this would be much more awkward to do in Maple.

Below is graph of the curve $\mathcal{C}$.



This paragraph a small digression that will be helpful in computing an example in the next chapter. When p is negative, there is just one real value of $\tilde{p}$ on the fiber over p; since the three complex values of $\tilde{p}$ correspond to the three 2-torsion points on E_p, when p is negative only one of them is real and so $E_p(\mathbb{R})$ has only one connected compontent. One can deduce directly that the 2-isogenous curve, denoted by $E_p^{(2)}$,

must have three real 2-torsion points and so $E_p^{(2)}(\mathbb{R})$ has two connected components. Another way to see this is to consider the 14-isogenous curve given by $E_{\tilde{p}}$; from the graph, it has three real 2-torsion points, since all three values of p on the fiber over $\tilde{p}$ are real. But this curve is 7-isogenous to $E_p^{(2)}$ and the 7-isogeny cannot alter the number of components.

4.5 Finding the quotient map

Taking the quotient of (4.8) by w_{14} will give us a 2 to 1 map to a line. To find it, note that the function field of the quotient consists of all functions that are constant on orbits of w_{14}, in other words the symmetric functions in p and $\tilde{p}$. The symmetric function $t = 4p\,\tilde{p}$ has degree 2 on the curve, since the inverse images are given by

$$\begin{aligned} p &= \frac{7529536 - 307328t - 1568t^2 + t^3 \pm (t-196)\sqrt{P_4(t)}}{76832t} \\ \tilde{p} &= \frac{7529536 - 307328t - 1568t^2 + t^3 \mp (t-196)\sqrt{P_4(t)}}{76832t} \end{aligned} \tag{4.9}$$

where

$$P_4(t) = t^4 - 2744t^3 + 729904t^2 - 105413504t + 1475789056\,. \tag{4.10}$$

Therefore t generates the function field of the quotient, and defines the quotient map $X_0(14) \to \mathbf{A}^1_t$.

Chapter 5

Tate-Shafarevich elements of order 7, over quadratic fields

5.1 Introduction

In this section we give a method of constructing elliptic curves E defined over quadratic extensions $K/\mathbb{Q}$, for which $Ш(E/K)[7]$ is large. For the construction to work, we need to be able to find quadratic extensions within a given family, in which a specified list of primes split in a particular way. The assertion that such extensions exist is the 'Arithmetic Hypothesis' stated below; under this hypothesis, the construction shows that $Ш(E/K)[7]$ can be arbitrarily large. Another way to view it is that one can use the construction to produce examples for which $Ш(E/K)[7]$ has any desired rank, as long as one can find instances of extensions verifying the hypothesis where the specified list of primes is large enough.

We will use the same notation as in the previous section.

5.1.1 Outline of the construction

A basic strategy to find elements of order p in Tate-Shafarevich groups is to find a curve with an isogeny $\phi : E \to E'$ of degree p, for which a structure theorem shows the Selmer group has large rank, while one can independently bound the rank of E by a 2-descent.

For $p = 7$, the previous section provides an explicit 2-to-1 map from $X_0(14)$ to $\mathbf{P}^1$, where $X_0(14)$ is written in 'natural' coordinates (meaning that for each point

$x \in X_0(14)$ one can explicitly write down the corresponding elliptic curves and isogeny, in terms of the coordinates of x). Given this map, every point $t \in \mathbf{P}^1(\mathbb{Q})$ gives rise to elliptic curves E and E^σ over a quadratic field K_t, with K_t-rational isogenies of degree 7 and degree 2.

How to make the Selmer group of ϕ large? Fix primes $p_1, \ldots, p_k$, and let $T \in \mathbf{P}^1(\mathbb{Q})$ be $p_1 \ldots p_k r$ for some $r \in \mathbb{Z}$. It turns out that each p_i splits in K_T, and one of the factors contributes a generator to the Selmer group of ϕ while its conjugate tries to impose a condition. However we may choose a twist of E that has nonsplit reduction at primes of the latter kind, and then the conditions are vacuous, so the Selmer group is big.

How to bound the rank of $E(K_T)$ by 2-descent? For this, we must bound the Selmer groups of a 2-isogeny φ *and* its dual. The same phenomenon arises: for each i, one factor of p_i contributes a generator, and the other a condition, to $\mathrm{Sel}^\varphi(E/K_T)$. For the dual Selmer group, the primes exchange roles. So we need to be able to arrange that the primes 'kill each other off', and for this we must assume an arithmetic hypothesis concerning quadratic residue symbols of prime elements in K_T. One must also arrange that the class group $C(K_T)[2]$ is small, since it contributes to the Selmer groups; this can be done using genus theory (which is the main motivation for working over quadratic fields).

5.2 The 7-descent

This will apply to everything in this chapter. Let $p_1, \ldots, p_k$ be primes, not 2 or 7. Let T denote the integer $p_1 \ldots p_k r$ where $r \in \mathbb{Z}$; we will impose more conditions on r in some of the results later. As in (4.10), let

$$P_4(t) = t^4 - 2744t^3 + 729904t^2 - 105413504t + 1475789056,$$

and put $K_T = \mathbb{Q}(\sqrt{P_4(T)})$. Let

$$p = \frac{T^3 - 1568T^2 - 307328T + 7529536 + (T-196)\sqrt{P_4(T)}}{2^5 7^4 T} \in K_T \qquad (5.1)$$

and let $\tilde{p}$ be its conjugate. Recall that under the map $X_0(14) \to \mathbf{P}^1_t$, the preimage of $t = T$ consists of the points $(p, \tilde{p})$ and $(\tilde{p}, p)$; we denote the corresponding elliptic curves by E_p and $E_{\tilde{p}}$ respectively, with $C_p, C_{\tilde{p}}$ being their distinguished 7-torsion subgroups. (At this stage, they are only determined up to $\overline{\mathbb{Q}}$-isomorphism. It makes sense to use the subscript p because the coordinate p does determine the j-invariant of the point $(p, \tilde{p})$, indeed p gives the image on $X_0(7)$ of that point.) The curves E_p and $E_{\tilde{p}}$ are 14-isogenous. As a remark, $j(p)$ is not determined by t because generically $j(E_p) \neq j(E_{\tilde{p}})$ in particular, generally $j(p) \notin \mathbb{Q}$.

5.2.1 Lemma. *For $T = p_1 \dots p_k r$, each p_i splits in $K_T/\mathbb{Q}$.*

Proof: The constant term of $P_4(t)$ is $1475789056 = 14^8 = 38416^2$. Since $p_i \mid T$, $x^2 - p_4(T) \equiv x^2 - 38416^2$ modulo p_i, which splits Therefore by Kummer's theorem, p_i splits in K_T.

Notation: Write $(p_i) = \mathcal{P}_i \mathcal{P}_i'$.

We now show that our curves have multiplicative reduction at $p_1, \dots, p_k$, at least over an extension where the reduction becomes semistable.

5.2.2 Lemma. *For each i, we have $ord_{\mathcal{P}_i}(j(p)) < 0$ and $ord_{\mathcal{P}_i'}(j(p)) < 0$.*

Proof: Recall from the previous chapter that the map $X_0(14) \to \mathbf{P}^1_t$ is given by $t = 4p\tilde{p}$, so in our case $T = 4p\tilde{p}$ and

$$\mathrm{ord}_{p_i} N_{K_T/\mathbb{Q}}(p) = \mathrm{ord}_{p_i}(T) = 1$$

From (1), p takes the form $R/(2^5 7^4 T)$ where R is an algebraic integer, and one calculates that R is not in the ideal $p_i \mathfrak{O}_{K_T}$ generated by the rational prime p_i.

However, one calculates that the numerator of p as given in (1) is not a multiple of the rational prime p_i. Therefore, possibly after interchanging $\mathcal{P}_i$ and $\mathcal{P}_i'$, we must have $\mathrm{ord}_{\mathcal{P}_i}(p) = 2 > 0$ and $\mathrm{ord}_{\mathcal{P}_i'}(p) = -1 < 0$. Then using

$$j(p) = \frac{(p^2 + 13p + 49)(p^2 + 5p + 1)^3}{p} \tag{5.2}$$

the lemma follows, since $p_i \neq 7$.

Note that given any point on $X_0(n)$, for any n, the corresponding $\overline{\mathbb{Q}}$-isomorphism class contains a whole family of quadratic twists. Indeed, if a curve $E : y^2 = f(x)$ has a Galois-stable subgroup, then the quadratic twist $E_d : dy^2 = f(x)$ does too, since $(-Y/\sqrt{d}, X)$ is the inverse of $(Y/\sqrt{d}, X)$. The next lemma shows that in our case, we can choose a curve E_p corresponding to $(p, \tilde{p}) \in X_0(14)$ that is defined over K_T and already has multiplicative reduction at each $\mathcal{P}_i$ and $\mathcal{P}_i'$.

5.2.3 Lemma. *Let K be a number field, and v a finite place with $v \nmid 6$. Suppose E is an elliptic curve defined over K with $ord_v\, j(E) < 0$. Then there is a quadratic twist of E, still defined over K and with the same j-invariant, which has multiplicative reduction at v.*

Proof: Take a minimal Weierstrass model for E at v, $y^2 = x^3 + ax + b$. Since $\mathrm{ord}_v\, j(E) < 0$, we have $\mathrm{ord}_v\, a^3 = \mathrm{ord}_v\, b^2 < \mathrm{ord}_v\, \Delta$, where $\Delta = -4a^3 - 27b^2$ is the discriminant of E. Hence $\mathrm{ord}_v\, a = 2m$ and $\mathrm{ord}_v\, b = 3m$ for some integer m. In fact since the model is minimal, m must be 0 or 1. Let $\pi \in K$ be an element with $\mathrm{ord}_v\, \pi = 1$, and twist E by π^m; the twisted curve has a Weierstrass model

$$y^2 = x^3 + (a/d^2)x + b/d^3$$

Clearly this is again a minimal model at v, in fact the coefficients are units at v. When reduced modulo v, the cubic on the right hand side cannot take the form

$(x-u)^3$, so the reduction cannot be additive. But $\mathrm{ord}_v\, j < 0$ so the reduction is multiplicative, as required.

Now that the curves have semistable reduction, it makes sense to ask whether C_p 'has good reduction', that is, whether the points in C_p reduce to nonsingular points modulo primes above $\mathcal{P}_i$.

5.2.4 Lemma. *$C_p \subset E_p^0(\overline{K_{T,\mathcal{P}_i}})$ if and only if $ord_{\mathcal{P}_i}(p) \geq 0$, and similarly for $\mathcal{P}_i'$.*

Proof: Recall that p is a coordinate for $X_0(7)$. Choose any $c \in X_1(7)(\overline{K_T})$ in the preimage of p, and any prime $\mathcal{Q}_i$ that divides $\mathcal{P}_i$ in $K_T(c)/K_T$. We need to check whether a generator of C_p lies in $E_p^0(K_T(c)_{\mathcal{Q}_i})$, and to do this we will use the standard model of an element of the moduli space $X_1(7)$. We may take c to be a $\mathcal{P}_i$-adic unit since one of $c, -\frac{c+1}{c}$ and $-\frac{1}{c+1}$ will be a unit; the standard model of the curve corresponding to $c \in X_1(7)$ is

$$E_c : y^2 + (1-c-c^2)xy + c^2(c+1)y = x^3 + c^2(c+1)x^2$$

with $(0,0)$ being the distinguished 7-torsion point. Note that E_c is a minimal model, since c is a unit. Now choose a generator P for C_p such that (E_p, P) and $(E_c, (0,0))$ correspond to the same point of $X_1(7)$. But then there must be an isomorphism defined over $K_T(c)$ between these two models, since they are in the same $\overline{\mathbb{Q}}$-isomorphism class, and $X_1(7)$ is a fine moduli space (so for any number field K, there is at most one K-isomorphism class of curves in the $\overline{\mathbb{Q}}$-isomorphism class corresponding to a particular point of $X_1(7)$).

Therefore, $C_p \subset E_p^0(\overline{K_{T,\mathcal{P}_i}})$ if and only if $(0,0) \in E_c^0(\overline{K_{T,\mathcal{Q}_i}})$, in other words $(0,0)$ reduces to a singular point modulo $\mathcal{Q}_i$ (since E_c is a minimal model). Using the equation for E_c, we compute that this happens when $\mathrm{ord}_{\mathcal{Q}_i}\, c^2(c+1) = 0$, or equivalently when $\mathrm{ord}_{\mathcal{Q}_i}\, p \geq 0$, using (4.1), and the lemma follows.

We already noted in the proof of 5.2.2 that, after interchanging $\mathcal{P}_i$ and $\mathcal{P}_i'$ if necessary, $\mathrm{ord}_{\mathcal{P}_i}\, p = 2 > 0$ and $\mathrm{ord}_{\mathcal{P}_i'}\, p = -1 < 0$. Since p and $\tilde{p}$ are conjugate,

taking conjugates gives $\mathrm{ord}_{\mathcal{P}_i'} \tilde{p} > 0$ and $\mathrm{ord}_{\mathcal{P}_i} \tilde{p} < 0$. Using 5.2.4 we see C_p has good reduction at $\mathcal{P}_i$ and bad reduction at $\mathcal{P}_i'$. The reverse holds for $C_{\tilde{p}}$.

We will now replace (E_p, C_p) by a twist as described in the next lemma, intending that for this twist, $\mathrm{Sel}^{\phi}(E_p/K_T)$ will be large.

5.2.5 Lemma. *There is a curve defined over K_T, in the isomorphism class corresponding to $(p, \tilde{p}) \in X_0(14)$, which has split multiplicative reduction at each $\mathcal{P}_i$ and nonsplit multiplicative reduction at each $\mathcal{P}_i'$.*

Proof: At this point in our argument, E_p denotes a specific curve over K_T, in just the $\overline{\mathbb{Q}}$-isomorphism class corresponding to $(p, \tilde{p})$, with multiplicative reduction at each $\mathcal{P}_i$ and $\mathcal{P}_i'$. Now choose an algebraic integer d in K_T such that

1. for each $\mathcal{P}_i$, d is a square modulo $\mathcal{P}_i$ if and only if E_p already has *split* multiplicative reduction at $\mathcal{P}_i$, and

2. for each $\mathcal{P}_i'$, d is a square modulo $\mathcal{P}_i'$ if and only if E_p already has *nonsplit* multiplicative reduction at $\mathcal{P}_i'$.

When d is a nonsquare modulo $\mathcal{P}$, twisting by d interchanges split and nonsplit multiplicative reduction: here is a simple way to see this. If $E : y^2 = f(x)$ has split reduction at $\mathcal{P}$, then $y^2 = f(x)$ has $N\mathcal{P} - 1$ solutions (x, y) over the residue field. For nonsquare d, the twisted curve $dy^2 = f(x)$ then must have $2N\mathcal{P} - (N\mathcal{P} - 1) = N\mathcal{P} + 1$ solutions over the residue field, which means it has nonsplit reduction. Therefore the twist of E_p by d will be a curve defined over K_T which satisfies the requirements of the lemma.

Consider the 7-isogeny $\phi : E_p \to E_p^{(7)}$ whose kernel is C_p, and let ϕ' be the dual isogeny. We now apply Corollary 2.4.3 to show that the Selmer group of ϕ is large.

Note first that at each $\mathcal{P}_i'$, E_p and hence also $E_p^{(7)}$ have nonsplit reduction. In that case, $c(E_p)$ and $c(E_p^{(7)})$ are 1 or 2, which means $c(E_p) = c(E_p^{(7)})$ since they could

only differ by a factor of 7. At each $\mathcal{P}_i$, they have split reduction and C_p has good reduction. Consider the Tate uniformisations of the curves: writing $K_{\mathcal{P}}$ for $K_{T,\mathcal{P}_i}$, the isogenies $E_p \to E_p^{(7)} \to E_p$ must take the form

$$K_{\mathcal{P}}^\times/q^{\mathbb{Z}} \longrightarrow^{\phi} K_{\mathcal{P}}^\times/q^{7\mathbb{Z}} \longrightarrow^{\phi'} K_{\mathcal{P}}^\times/q^{\mathbb{Z}}$$

It must be this way around because, by the theory of Tate curves, $E_0(K_{\mathcal{P}})$ equals the subgroup $\mathfrak{O}_{\mathcal{P}}^\times$ of $K_{\mathcal{P}}^\times/q^{\mathbb{Z}}$, and we know the kernel C_p of ϕ is in this subgroup. This shows $c(E_p^{(7)})/c(E_p) = \operatorname{ord} q^7/\operatorname{ord} q = 7$ at each $\mathcal{P}_i$. The other factors in Corollary 2.4.3 make only a bounded contribution, because the torsion groups have order at most 7, there are at most two infinite places v, at which the Ω_v terms are either equal or differ by a factor of 7, $c_v = 1$ at finite places of good reduction, and at each finite place of bad reduction the c_v terms are either equal or differ by a factor of 7. One computes that the primes of bad reduction are those dividing T. Therefore, we can make $\#\operatorname{Sel}^\phi(E_p/K)$ have any desired size, simply by taking $k - \#\{p \mid r\}$ large enough.

5.3 The 2-descent

Now we turn to bounding the rank of $E(K_T)$. Naturally, we will need to impose some conditions on r in order to have a bound, and in fact we will have to assume the Arithmetic Hypothesis stated below. Let $\varphi : E_p \to E_p^{(2)}$ denote the 2-isogeny whose kernel is the distinguished 2-torsion point on E_p, and let φ' denote the dual isogeny. The Selmer groups for both of these isogenies are subgroups of $H^1(K_T, \mu_2) = K_T^\times/K_T^{\times 2}$. We'll now work out the local conditions determining the Selmer groups.

5.3.1 Lemma. *Suppose $K_{\mathcal{P}}$ is a completion at one of $\mathcal{P}_i$ or $\mathcal{P}_i'$. If $E_p[\varphi] \subset E_p^0(K_{\mathcal{P}})$ then $E_p(K_{\mathcal{P}})/\varphi' E_p^{(2)}(K_{\mathcal{P}}) = 0$ and $E_p^{(2)}(K_{\mathcal{P}})/\varphi E_p(K_{\mathcal{P}}) = H^1(K_{\mathcal{P}}, E_p[\varphi]) = K_{\mathcal{P}}^\times/K_{\mathcal{P}}^{\times 2}$. If $E_p[\varphi] \not\subseteq E_p^0(K_{\mathcal{P}})$, the reverse holds.*

Proof: First we do it for the $\mathcal{P}_i$, where the reduction is split. If $E_p[\varphi] \subset E_p^0(K_\mathcal{P})$ then the isogenies $E_p \to E_p^{(2)} \to E_p$ take the form

$$K_\mathcal{P}^\times/q^\mathbb{Z} \xrightarrow{\varphi} K_\mathcal{P}^\times/q^{2\mathbb{Z}} \xrightarrow{\varphi'} K_\mathcal{P}^\times/q^\mathbb{Z}$$

where the first map is $a \mapsto a^2$. From this it is clear that the lemma is true for this case. If $E_p[\varphi] \not\subseteq E_p^0(K_\mathcal{P})$ then we have the same situation except that E_p and $E_p^{(2)}$ are interchanged.

Now we do it for the $\mathcal{P}_i'$. Note that for these primes we have $\operatorname{ord} p = -1$, so by (5.2) $\operatorname{ord} j = -7$, and so $\operatorname{ord} q = -\operatorname{ord} j$ is odd. Let $L_w/K_\mathcal{P}$ be the quadratic extension over which the reduction becomes split, in other words the unramified quadratic extension of $K_\mathcal{P}$. If $E_p[\varphi] \subset E_p^0(K_\mathcal{P})$ then the maps $E_p(L_w) \to E_p^{(2)}(L_w) \to E_p(L_w)$ again have the form

$$L_w^\times/q^\mathbb{Z} \xrightarrow{\varphi} L_w^\times/q^{2\mathbb{Z}} \xrightarrow{\varphi'} L_w^\times/q^\mathbb{Z}$$

where the first map is $a \mapsto a^2$. Furthermore, $E_p(K_\mathcal{P})$ is the kernel of the norm map $N_{L_w/K_\mathcal{P}}$ applied to $L_w^\times/q^\mathbb{Z}$, and $E_p^{(2)}(K)$ is the kernel of $N_{L_w/K_\mathcal{P}}$ applied to $L_w^\times/q^{2\mathbb{Z}}$. Choose a uniformiser π of $K_\mathcal{P}$; since $L_w/K_\mathcal{P}$ is unramified π is also a uniformiser of L_w. To show $\varphi' : E_p^{(2)}(K_\mathcal{P}) \to E_p(K_\mathcal{P})$ is surjective, take any $a \in E_p(K_\mathcal{P})$, and represent it as an element $u\pi^n$ of $L_w^\times$, where u is a unit. The condition for $a \in E_p(K_\mathcal{P})$ is that $N(a) = N(u)\pi^{2n}$ is in $q^\mathbb{Z}$, and since $\operatorname{ord} q$ is odd this means $N(a) = q^{2k}$ for some k. Therefore $a \mod q^{2\mathbb{Z}}$ is an element of $E_p^{(2)}(K_\mathcal{P})$, and it maps to $a \in E_p(K_\mathcal{P})$. This shows $E_p(K_\mathcal{P})/\varphi' E_p^{(2)}(K_\mathcal{P}) = 0$, and the assertion about $E_p^{(2)}(K_\mathcal{P})/\varphi E_p(K_\mathcal{P})$ then follows by local duality. (It can also be seen directly in a few lines.) Finally, if $E_p[\varphi] \not\subseteq E_p^0(K_\mathcal{P})$ then we have the same situation except that E_p and $E_p^{(2)}$ are interchanged. This completes the proof of the lemma.

The following lemma, which deals with the case where the curves have good reduction, is a restatement of Proposition 2.3.2.

5.3.2 Lemma. *Suppose $\mathcal{P}$ is a place not dividing 2 where E_p has good reduction. Then the images of $E_p(K_\mathcal{P})/\varphi' E_p^{(2)}(K_\mathcal{P})$ and $E_p^{(2)}(K_\mathcal{P})/\varphi E_p(K_\mathcal{P})$ are both the unit subgroup $\mathfrak{O}_\mathcal{P}^\times/\mathfrak{O}_\mathcal{P}^{\times 2}$ of $K_\mathcal{P}^\times/K_\mathcal{P}^{\times 2}$, which is the unramified subgroup of $H^1(K_\mathcal{P}, \mu_2)$.*

Notation: Let us partition the set $\{\mathcal{P}_i\} \cup \{\mathcal{P}_i'\}$ as $\mathcal{A} \cup \mathcal{B}$, where $\mathcal{A}$ consists of those places where $E_p[\varphi] \subset E_p^0(K_\mathcal{P})$. For each $(p_i) = \mathcal{P}_i\mathcal{P}_i'$, exactly one of $\mathcal{P}_i$ and $\mathcal{P}_i'$ is in $\mathcal{A}$; call it $\mathcal{P}_i^{(\mathcal{A})}$ and the other $\mathcal{P}_i^{(\mathcal{B})}$.

To describe the Selmer groups, let $K(\mathcal{A}, \mathcal{B}) \subset K^\times/K^{\times 2}$ denote the subgroup with 'generators from $\mathcal{A}$ and conditions from $\mathcal{B}$'; to be precise

$$K(\mathcal{A}, \mathcal{B}) = \{a \in K^\times/K^{\times 2} : \operatorname{ord}_v a \text{ is even for all } v \notin \mathcal{A} \text{ and } a \in K_v^{\times 2} \text{ for all } v \in \mathcal{B}\}$$

Now, $\mathrm{Sel}^\varphi(E_p/K_T)$ is close to $K_T(\mathcal{A}, \mathcal{B})$, in the following precise sense: regarding both groups as subgroups of $K_T^\times/K_T^{\times 2}$, their composite modulo their intersection is bounded in terms of $\#\{p \mid r\}$. Indeed, the two subgroups are defined by the same local conditions, except that $K_T(\mathcal{A}, \mathcal{B})$ has the 'unit' condition at places dividing ∞, 2 and r, while $\mathrm{Sel}^\varphi(E_p/K_T)$ may have some other condition. At any rate, the resulting difference in dimension cannot be more than the sum of the dimensions of $H^1(K_v, \mu_2) = K_v^\times/K_v^{\times 2}$; for $v \nmid 2$, this dimension is at most 2, and for $v \mid 2$ it is bounded independently of the value of T since K_T is always quadratic over $\mathbb{Q}$. In the same sense, $\mathrm{Sel}^{\varphi'}(E_p/K)$ is close to $K_T(\mathcal{B}, \mathcal{A})$.

We now begin to describe our arithmetic hypothesis, which basically asserts that we can arrange for $K_T(\mathcal{A}, \mathcal{B})$ and $K_T(\mathcal{B}, \mathcal{A})$ to be bounded.

Arithmetic Hypothesis, part one. *There is some number B with the following property. Given any integer k and any set of primes $p_1, \ldots, p_k$, we can find an integer r such that*

1. $\#\{p \mid r\} \leq B$
2. $\#\{p \mid P_4(p_1 \ldots p_k r)\} \leq B$

Remarks: (i) The purpose of condition (2) is that via genus theory, it implies that $C(K_T)[2] \leq 2^{B-1}$, where as usual $K_T = \mathbb{Q}(\sqrt{P_4(p_1 \dots p_k r)})$.
(ii) This hypothesis is a true statement: it is a special case of a theorem in sieve theory (for instance Theorem 9.8 in [H-R], p 261).

If r satisfies the hypothesis and $B < k$ it follows from $C(K_T)[2] < 2^B$ that we can reorder the p_j so that $\{\mathcal{P}_j : j < B\}$ generates the same subgroup of $C(K_T)/C(K_T)^2$ as $\{\mathcal{P}_j\}$ does. Note also that $\mathcal{P}'_j = \mathcal{P}_j^{-1}$ in the class group, so replacing any $\mathcal{P}_j$'s by $\mathcal{P}'_j$ would not alter the subgroup generated. Now we can find ideals $\mathfrak{a}_j$ for each j in the range $B < j \leq k$ such that

1. $\mathfrak{a}_j$ is divisible only by primes in $\{\mathcal{P}_i^{(\mathcal{A})} : i \leq j\}$,
2. $\mathcal{P}_j^{(\mathcal{A})}$ divides $\mathfrak{a}_j$, and $(\mathcal{P}_j^{(\mathcal{A})})^2$ doesn't divide $\mathfrak{a}_j$,
3. $\mathfrak{a}_j \in P_K I_K^2$ (it is a principal ideal times the square of an ideal)

We choose generators of the principal ideals appearing in (iii) as follows. For each $B < j \leq k$, define $\alpha_j^{(\mathcal{A})}$ such that $\mathfrak{a}_j \in (\alpha_j^{(\mathcal{A})}) I_K^2$. For each j, define $\alpha_j^{(\mathcal{B})}$ to be the conjugate of $\alpha_j^{(\mathcal{A})}$ which will have the corresponding properties with respect to $\mathcal{B}$. Then $\{\alpha_j^{(\mathcal{A})}, \alpha_j^{(\mathcal{B})}\}$ is a set of linearly independent elements of the $\mathbb{F}_2$-vector space $K_T^\times / K_T^{\times 2}$, otherwise some product of the $\mathfrak{a}_j$ and their conjugates would be the square of an ideal, which is impossible because of (ii).

Arithmetic Hypothesis. *As in part one, but with the following additional condition on r: that there is a choice of $\alpha_j^{(\mathcal{A})}$ and $\alpha_j^{(\mathcal{A})}$ as above such that the following $(k-B) \times (k-B)$ matrix M is nonsingular over $\mathbb{F}_2$. The entries of M are, for each pair (i,j) with $B < i \leq k$ and $B < j \leq k$,*

$$(M)_{i,j} = \frac{1}{2}\left(1 - \left(\frac{\alpha_i^{(\mathcal{A})}}{\mathcal{P}_j^{(\mathcal{B})}}\right)\right)$$

which is 1 if and only if $\alpha_i^{(\mathcal{A})}$ is a nonsquare modulo $\mathcal{P}_j^{(\mathcal{B})}$.

See the end of this chapter for a discussion of the Arithmetic Hypothesis. Its purpose is made clear in the next lemma.

5.3.3 Lemma. *Suppose $p_1, \ldots, p_k, r$ satisfy the arithmetic hypothesis. Then $\#K_T(\mathcal{A}, \mathcal{B})$ and $\#K_T(\mathcal{B}, \mathcal{A})$ are bounded in terms of B only.*

Proof. First we introduce the notation

$$K(\mathcal{A}) := \{a \in K^\times/K^{\times 2} : \mathrm{ord}_v\, a \text{ is even for all } v \notin \mathcal{A}\}$$

which is an $\mathbb{F}_2$-vector space containing $K(\mathcal{A}, \mathcal{B})$. Note that

$$\dim_{\mathbb{F}_2} K(\mathcal{A}) \leq 2 + \#\mathcal{A} + \dim C(K)[2] \leq 2 + k + B$$

To see this, if $\alpha \in K^\times$ represents an element of $K(\mathcal{A})$, we may write $(\alpha) = AI^2$, where A is an ideal supported in $\mathcal{A}$. Then the number of choices for α modulo $K^{\times 2}$ is determined by

1. the number of units, modulo squares, which contributes at most 2 to the dimension,

2. the number of choices of squarefree A, which contributes $\#\mathcal{A}$ to the dimension, and

3. the number of choices of I; this is bounded by $\#C(K)[2]$, for if we have $(\alpha_1) = AI_1^2$ and $(\alpha_2) = AI_2^2$ with α_1 and α_2 different modulo $K^{\times 2}$, then I_1 and I_2 are in different ideal classes, and $I_1 I_2^{-1} \in C(K)[2]$.

This proves the first inequality stated above, and the second follows directly from condition (2) in the Arithmetic Hypothesis.

We noted that the $\alpha_j^{(\mathcal{A})}$ are linearly independent elements of $K(\mathcal{A})$, so we may choose a basis of $K(\mathcal{A})$ consisting of the $\alpha_j^{(\mathcal{A})}$ and some other elements. The second

part of the Arithmetic Hypothesis implies that the subspace $\{\alpha \in \langle\{\beta_j\}\rangle : \alpha \in K_v^{\times 2} \text{ for all } v \in \mathcal{B}\}$ is trivial. Hence

$$\dim_{\mathbb{F}_2} K(\mathcal{A},\mathcal{B}) \leq \dim_{\mathbb{F}_2} K(\mathcal{A}) - (k-B) \leq 2 + 2B$$

as the lemma asserts. The same follows for $K(\mathcal{B},\mathcal{A})$ since the sets $\mathcal{A}$ and $\mathcal{B}$ are conjugate.

Proof of the main result: By Lemma 5.3.3, $K_T(\mathcal{A},\mathcal{B})$ and $K_T(\mathcal{B},\mathcal{A})$ are bounded in terms of B. It follows by the discussion preceding part one of the Arithmetic Hypothesis that $\mathrm{Sel}^{\varphi}(E_p^{(2)}/K)$ and $\mathrm{Sel}^{\varphi'}(E_p/K)$ are bounded in terms of B and $\#\{p \mid r\}$; then invoking condition (1), they are bounded in terms of B. Therefore the rank of $E_p(K)$ is bounded in terms of B. On the other hand, we have seen that the Selmer group for the 7-isogeny $E_p \to E_p^{(7)}$ can be made arbitrarily large, by taking k large enough. In this way, the Tate-Shafarevich group of E_p can have arbitrarily large 7-torsion.

5.4 An example of the construction

The method of construction presented in this chapter is motivated out of theoretical interest rather than its practical value in producing particular examples (certainly it is not the optimal way to produce them). So it is for the purpose of illustration that we give a numerical example here (as well as to offer some substantiation for the arithmetic hypothesis, but see Section 5.5 for much more). In principle all the theory needed to compute an example has been given already, but in practice one is led to make a finer analysis of certain terms that had no significance asymptotically, especially in the 2-descent. This uses additional arguments which will be sketched but not fully explained here.

5.4.1 Example. Set $T = -165 = -3 \cdot 5 \cdot 11$. Then the quadratic field K_T is $\mathbb{Q}(\sqrt{51808245241})$, and using (5.1)

$$p = \frac{11057731 + 361\sqrt{51808245241}}{12677280}$$

Denote by E_p the corresponding elliptic curve; a very messy equation can be obtained by substituting this value of p into (4.3). We can show that some twist E of E_p over K_T, $Ш(E, K_T)$ has nontrivial elements of order 7. Of course, assuming those elements are not infinitely divisible in $Ш(E, K_T)$, it follows that $\#Ш(E, K_T)[7] \geq 7^2$ (by a standard consequence of properties of the Cassels-Tate pairing). In this example, the 2-descent bounded the rank of $E(K_T)$ by 2, without using all of the information.

By taking $T = -3 \cdot 5 \cdot 37$ one obtains another very similar example. By taking $T = -3 \cdot 5 \cdot 37 \cdot 61$ yields an example where one can show that $\#Ш(E, K_T)[7] \geq 7^2$ without assuming any conjectures about Ш.

We now sketch the steps in the computation of the first example, where $T = -3 \cdot 5 \cdot 11$. For the 7-descent, we follow the general procedure, which is to replace the curve by a twist. It turns out that we need a twist which has split multiplicative reduction at the places dividing $(T, \sqrt{P_4(T)} - 38416)$ and nonsplit reduction at the conjugate places (in fact this is a general phenomenon). One can arrange that twisting introduces only one more bad prime, which will be a place of additive reduction. Then one finds $\#\,\mathrm{Sel}^{\phi}(E, K_T) \geq 7^2$, applying Corollary 2.4.3. At each of the three primes v dividing $(T, \sqrt{P_4(T)} - 38416)$, the factor $c_v(E)$ appearing in Corollary 2.4.3 will contribute a factor 7, and the 'additive place' introduced by twisting contributes at worst $\frac{1}{7}$. To see that the remaining factors do not contribute anything, note that $E(K_T)[\phi]$ and $E^{(7)}(K_T)[\phi']$ are trivial, and the factors $\Omega(E)$ and $\Omega(E^{(7)})$, which are both products over the two infinite places, cancel each other: this is because E and $E^{(14)}$ are conjugate, and because $\Omega(E^{(14)})$ and $\Omega(E^{(7)})$ have the same valuation at 7.

One may compute most of the 2-descent without specifying the twist (as long as the twist introduces only one additional bad prime). When T is negative, K_T is real. Further, $T < -4$ is sufficient to make p positive and $\tilde{p}$ negative. As explained at the end of Section 4.4, this means $E_p(\mathbb{R})$ has two connected components while $E_p^{(2)}(\mathbb{R})$ has one. Hence $E_p^{(2)}(\mathbb{R})/\psi E_p(\mathbb{R})$ is trivial while $E_p(\mathbb{R})/\psi' E_p^{(2)}(\mathbb{R})$ has order two. This determines the Selmer conditions for the 2-descent imposed by one of the real places, and the conjugate place imposes the reverse conditions. For odd finite places, the Selmer conditions are determined as usual by the reduction of the kernels of the isogenies. However for primes above 2 (which necessarily splits in K_T) we will use a aspect of the theory of descent that holds in general but which we have not needed elsewhere. For any isogeny ϕ, the homomorphisms

$$E'(K_v)/\phi E(K_v) \to K_v^\times / K_v^{\times \deg \phi}$$

for each place v are in fact given by a single element of the function field $K(E')$. This function can be identified as having a certain divisor. In the present case the function is $s - s_0$ where s_0 is the s coordinate of the 2-torsion point in the kernel of ψ. Using this, one finds that for one of the primes above 2 the image of $E_p^{(2)}(\mathbb{Q}_2)/\psi E_p(\mathbb{Q}_2)$ in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ is $\mathfrak{O}_2^\times/\mathfrak{O}_2^{\times 2}$, represented by $\{1,3,5,7\}$, and the image of $E_p(\mathbb{Q}_2)/\psi' E_p^{(2)}(\mathbb{Q}_2)$ is the unramified subgroup, represented by $\{1,5\}$. This determines the Selmer conditions imposed by that prime, and the conjugate prime imposes the reverse conditions. For ease of computations, I instead used $\{1,3,5,7\}$ for each of the conditions, thus obtaining upper bounds on the Selmer groups. We also have not determined the Selmer conditions at the bad prime introduced by twisting; however by Tate local duality it can at worst increase the sum of the ranks by 1. The Selmer conditions that are stated above are displayed as a matrix over $\mathbb{F}_2$, given below. Rows correspond to generators of the $\mathcal{S}$-units of K_T, where $\mathcal{S}$ consists of the primes dividing $(T, \sqrt{P_4(T)}+38416)$: K_T has class number 1, and the first three rows correspond to generators of

the ideals dividing $(T, \sqrt{P_4(T)} + 38416)$ above $3, 5$, and 11 respectively, the fourth row corresponds to a fundamental unit and the last row corresponds to -1. Columns correspond to Selmer conditions: the first three columns indicate quadratic residue symbols modulo the primes dividing $(T, \sqrt{P_4(T)} + 38416)$ above $3, 5$, and 11 respectively, the fourth column is null because that is where the condition at a prime above 2 should go, and the last column gives the condition that elements be positive at one of the real places. Note that presenting the $\mathcal{S}$-units as an $\mathbb{F}_2$ vector space entails translating everything from multiplicative notation to additive notation; thus quadratic residue symbols are translated from $1, -1$ to $0, 1$. The matrix for $\mathrm{Sel}^{\psi}(E_p, K_T)$ is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

which has rank 4. Incidentally, note that the assertion of the arithmetic hypothesis holds in this instance. The matrix for $\mathrm{Sel}^{\psi'}(E_p^{(2)}, K_T)$ looks the same, because by Tate local duality the isogenous Selmer group has the opposite Selmer conditions, and in this case that means all generators and conditions are replaced by their conjugates. Putting everything together, one sees that the ranks of $\mathrm{Sel}^{\psi}(E_p, K_T)$ and $\mathrm{Sel}^{\psi'}(E_p^{(2)}, K_T)$ add up to at most 3. (Recall that the 'additive prime' does not appear in the matrix, but as noted above it contributes at worst 1 to the sum of the ranks.) Consequently the rank of $E(K_T)$ is at most 1, since the kernels of both isogenies are both pointwise rational, which means 2-torsion in $E(K_T)$ accounts for a nontrivial part of each Selmer group.

The other examples are computed in very much the same way. In particular with $T = -3 \cdot 5 \cdot 37 \cdot 61$, the matrix for $\mathrm{Sel}^{\psi}(E_p, K_T)$ is

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

which has rank 5. For what it's worth, this is one more instance where the assertion of the arithmetic hypothesis holds.

5.5 Remarks about the Arithmetic Hypothesis

In the absence of any reason that $\mathcal{P}_i^{(A)}$ and $\mathcal{P}_i^{(B)}$ should be correlated, we expect that $\alpha_i^{(A)}$ is as likely to be a square modulo $\mathcal{P}_i^{(B)}$ as a nonsquare, as if it were a randomly chosen element of $\mathfrak{O}_{K_T} \setminus \mathcal{P}_i^{(B)}$. The same applies to the $\alpha_i^{(A)}$ modulo $\mathcal{P}_j^{(B)}$ for $i \neq j$. Note that if the symbols $\left(\frac{p_i}{p_j}\right)$ are fixed, this would *almost* determine the products $\left(\frac{\alpha_i^{(A)}}{\mathcal{P}_j^{(B)}}\right)\left(\frac{\alpha_i^{(B)}}{\mathcal{P}_j^{(B)}}\right)$ (it would determine them up to the variation resulting from multiplying the α_i's by units); however the Arithmetic Hypothesis does not seek to specify both symbols simultaneously. (Even if it did, nothing essential would by changed, since we are able to choose $p_1, \ldots, p_k$ so that $\{\left(\frac{p_i}{p_j}\right), i < j\}$ take any desired values, by the theorem on primes in arithmetic progressions.)

The Arithmetic Hypothesis is a Cebotarev-like statement, asserting that primes are somewhat equidistributed with respect to each other. Of course, Cebotarev's theorem cannot be applied because we are not working in a fixed number field; indeed we have a fixed set of primes $p_1, \ldots p_k$ and a varying number field K_T, which

is the reverse of the situation where Cebotarev applies. The Arithmetic Hypothesis is however a statement about maximal ideals in the ring $Q[t](\sqrt{P_4(t)})$.

Question. Can the Arithmetic Hypothesis be stated as a special case of some conjectural generalisation of the Cebotarev Density Theorem for certain rings of Krull dimension 2?

Under the heuristic that M is a random matrix of 0's and 1's, the probability that M is nonsingular over $\mathbb{F}_2$ is $\prod_{j=1}^{k}\left(1-\frac{1}{2^j}\right)$. To see this, note the probability that the first row is a nonzero vector is $\left(1-\frac{1}{2^k}\right)$. Given this, the probability that the second row is independent of the first row is $\left(1-\frac{2}{2^k}\right)=\left(1-\frac{1}{2^{k-1}}\right)$. One continues to argue row by row; finally the probability that the last row is not in the subspace spanned by the previous rows is $\left(1-\frac{1}{2}\right)$. As the dimension k increases to infinity, $\prod_{j=1}^{k}\left(1-\frac{1}{2^j}\right)$ must converge to a positive value (since $\sum_{j=1}^{\infty}\frac{1}{2^j}$ converges); computationally this value is $0.2887881\ldots$. So under our heuristic, for any k if $p_1,\ldots p_k$ and r are chosen at random then M will be nonsingular with probability greater then $\frac{1}{4}$. In fact there is a better chance that the Arithmetic Hypothesis holds for given $p_1,\ldots,p_k$ and r, since we have the added flexibility of multiplying the α_i's by units. When K_T is imaginary, the probability is twice as good, namely 0.58, and when K_T is real it is $\frac{8}{3}$ times as good, approximately 0.77. It is simple enough to calculate these values with the aid of the corank calculation at the end of this subsection.

Of course, we do not really need M to be nonsingular; as long as its corank is small relative to k we still get a result. As k tends to infinity, the expected corank tends to $0.85017983\ldots$ (a proof is given below). In particular the expected corank is bounded by some constant C independent of k, so in our construction for random $p_1,\ldots p_k$ and r we expect to obtain $Ш(E/K_T)[7]$ with rank $k-C$. A simple consequence is that as k tends to infinity, the probability of obtaining nontrivial $Ш[7]$ tends to 100%.

Proof of the expected corank: First, for a random matrix M, let $\mathrm{Ann}(M)$ denote the annihilator in $(\mathbb{F}_2^n)^*$ of the row space of M.

$$\begin{aligned}
&\mathrm{Prob}(M \text{ has corank } n)\\
&= (\#\text{ of choices of a subspace } S \subseteq (\mathbb{F}_2^n)^* \text{ of rank } n) \cdot \mathrm{Prob}(\mathrm{Ann}(M) = S)\\
&= \frac{\#\text{ of choices of } n \text{ independent elements in } (\mathbb{F}_2^n)^*}{\#\text{ of changes of basis}} \cdot \mathrm{Prob}(\mathrm{Ann}(M) = S)\\
&= \frac{(2^k-1)\dots(2^k-2^{n-1})}{\#\,\mathrm{GL}_n(\mathbb{F}_2)} \left(1-\frac{1}{2^k}\right)\dots\left(1-\frac{1}{2^{n+1}}\right)\left(\frac{1}{2^k}\right)^n\\
&= \frac{\left(1-\frac{1}{2^k}\right)\dots\left(1-\frac{1}{2^{k-n+1}}\right)}{(2^n-1)\dots(2^n-2^{n-1})} \left(1-\frac{1}{2^k}\right)\dots\left(1-\frac{1}{2^{n+1}}\right)
\end{aligned}$$

In the limit as $k \to \infty$, this becomes

$$\frac{\prod_{j=n+1}^{\infty}\left(1-\frac{1}{2^j}\right)}{2^{n^2}\left(1-\frac{1}{2^n}\right)\dots\left(1-\frac{1}{2}\right)} = \frac{\prod_{j=1}^{\infty}\left(1-\frac{1}{2^j}\right)}{2^{n^2}\left(1-\frac{1}{2}\right)^2\dots\left(1-\frac{1}{2^n}\right)^2}$$

Therefore the expected corank is

$$\sum_{n=0}^{\infty} n\,\mathrm{Prob}(M \text{ has corank } n) = \prod_{j=1}^{\infty}\left(1-\frac{1}{2^j}\right)\sum_{n=1}^{\infty}\frac{n}{2^{n^2}\left(1-\frac{1}{2}\right)^2\dots\left(1-\frac{1}{2^n}\right)^2}$$

which converges; computationally, it equals $0.85017983\ldots$

5.5.1 Numerical Data on the arithmetic hypothesis

After various numerical experiments with different polynomials, the arithmetic hypothesis still seems reasonable. The finer question, regarding the frequency distribution of ranks, remains unclear. One might guess that the heuristics described above are correct on average. For each particular polynomial, the frequencies are evidently skewed by some arithmetic phenomena. Perhaps the correct conjecture would adjust the heuristic by fudge factors akin to the 'twin prime constant' (a convergent product of local factors).

The polynomial $P_4(T)$ has the special property that its constant term is a square, which is the reason that odd primes dividing T necessarily split in $\mathbb{Q}(\sqrt{P_4(T)})$. Our

numerical experiments aim to investigate the claim that every irreducible polynomial whose constant term is square should satisfy the same hypothesis. The experiment that yielded the clearest data (given below) considered the family of quadratic polynomials $f_k(x) = x^2+x+k^2$. For each value of k, we set $T = 3\cdot5\cdot r$ where r is an integer such that $f_k(T)$ is prime (then by genus theory, the class number of $\mathbb{Q}(\sqrt{f_k(T)})$ is odd). We then find the rank of the matrix formed by the legendre symbols of the primes above 3 and 5, as in the arithmetic hypothesis. One obtains better data by keeping the same two primes fixed, at least for each polynomial; due to way data is selected (requiring $f_k(T)$ to be prime), varying them muddies the data considerably. The results are as follows. Here 'EXPECTED' just gives the expected frequency of ranks for random matrices, and totals are given for the set of data appearing in this table (10605 pairs of (k, T)) and for another set of data with higher values of k (18225 pairs). For each polynomial, 400 values of T are tested, so each row adds up to 400.

	$rank = 0$	$rank = 1$	$rank = 2$
'EXPECTED'	$\frac{1}{16} = 6.8\%$	$\frac{9}{16} = 56.8\%$	$\frac{3}{8} = 37.5\%$
TOTAL (THIS SET)	6.8%	54.2%	39.0%
TOTAL (2ND SET)	6.8%	54.3%	38.9%
$x^2 + x + 1$	0	158	242
$x^2 + x + 7^2$	14	222	164
$x^2 + x + 11^2$	43	205	152
$x^2 + x + 13^2$	24	230	146
$x^2 + x + 17^2$	26	222	152
$x^2 + x + 19^2$	40	207	153
$x^2 + x + 23^2$	17	227	156
$x^2 + x + 29^2$	39	214	147
$x^2 + x + 31^2$	36	217	147

	$rank = 0$	$rank = 1$	$rank = 2$
$x^2 + x + 37^2$	16	222	162
$x^2 + x + 41^2$	33	205	162
$x^2 + x + 43^2$	21	231	148
$x^2 + x + 47^2$	26	209	165
$x^2 + x + 49^2$	36	230	134
$x^2 + x + 53^2$	19	223	158
$x^2 + x + 59^2$	40	210	150
$x^2 + x + 61^2$	37	212	151
$x^2 + x + 67^2$	11	225	164
$x^2 + x + 71^2$	34	231	135
$x^2 + x + 73^2$	14	237	149
$x^2 + x + 77^2$	23	215	162
$x^2 + x + 79^2$	40	212	148
$x^2 + x + 83^2$	16	230	154
$x^2 + x + 89^2$	33	198	169
$x^2 + x + 91^2$	36	225	139
$x^2 + x + 97^2$	15	221	164

5.5.2 Units in quadratic extensions of $K[t]$

This section, of mild independent interest, closes off an obvious avenue by which one might try to verify the Arithmetic Hypothesis. The hope is that for some primes $\mathcal{P}_i$, a generator might come from a section $A(t)+\sqrt{P_4(t)}B(t)$, by virtue of a polynomial identity $A(t)^2 - P_4(t)B(t)^2 = p_i$. We show this does not happen.

In general let K be a number field and let $f \in K[t]$. The units $A + \sqrt{f}B$ of $K[t](\sqrt{f})$ must satisfy $A^2 - fB^2 \in K^\times$ since the unit group of $K[t]$ equals $K^\times$.

Question. How large can the unit group of $K[t](\sqrt{f})$ be, and how can it be determined?

A partial answer is given by the next two lemmas, which rule out certain kinds of units.

5.5.1 Lemma. *There are no solutions to $A^2 - fB^2 = pm^2$ if p is any prime such that f takes a nonsquare value modulo p, and $m \in \mathbb{Z}$.*

Proof: We may assume A and B are in $\mathfrak{O}_K[t]$ with content prime to p, by clearing denominators and replacing m by another value. Suppose $f(x) = n$, with $\left(\frac{n}{\mathfrak{p}}\right) = -1$ for some $\mathfrak{p} \mid p$. Reducing modulo $\mathfrak{p}$, we have $\overline{A}^2 - f\overline{B}^2 = 0$ in $\mathbb{F}_{\mathfrak{p}}[t]$, although $\overline{A}$ and $\overline{B}$ are nonzero. Divide out the largest power of $(T - x)$ dividing both $\overline{A}$ and $\overline{B}$ in $\mathbb{F}_{\mathfrak{p}}[t]$. Then either $\overline{A}(x) \neq 0$ or $\overline{B}(x) \neq 0$. But we must have $\overline{B}(x) = 0$, otherwise $f(x)$ would be a square in $\mathbb{F}_{\mathfrak{p}}$. Now it follows that $\overline{A}(x) = 0$, a contradiction.

5.5.2 Lemma. *Let $K = \mathbb{Q}$. There are no solutions to $A^2 - fB^2 = pm^2$ for any prime $p \geq (\deg f + 2)^2$ such that f has distinct roots modulo p.*

Proof: If there is a solution, then by 5.5.1 $f(x)$ is a square modulo p for every $x \in \mathbb{F}_p$. Let $d = \deg f$; then there are at least $2p - d$ solutions to $y^2 = f(x)$ over $\mathbb{F}_p$, since $f(x)$ equals 0 for at most d values of x. But since f has distinct roots, $y^2 = f(x)$ is a curve of genus $\lceil \frac{d}{2} \rceil$ over $\mathbb{F}_p$, so the number of solutions is less than $p + 1 + 2\lceil \frac{d}{2} \rceil \sqrt{p}$, by the Weil bound. After some simple manipulation, one obtains $p \leq (d + 2)^2$ as required.

In particular there can only be solutions for at most finitely many primes. In our case, where $f = P_4$, we need only consider $p < 36$ since the only primes dividing the discriminant of f are 2 and 7. By a short computer search, we find that f takes a nonsquare value modulo each prime $p < 36$ except for 2 and 7, so 5.5.1 rules these out too. We are not interested in 2 or 7, since we cannot use them as p_i's.

Bibliography

[B-O] Balog, A. and Ono, K. *Elements of class groups and Shafarevich-Tate groups of elliptic curves*, to appear.

[Be] Beaver, C. *5-torsion in the Shafarevich-Tate group of a family of elliptic curves*. J. Number Theory **82** (2000), No. 1, 25–46.

[Bi] Birch, B. J. *Some calculations of modular relations*. Modular Functions in One Variable, I. Proc. Internat. Summer School, Univ. Antwerp, 1972. Lecture notes in Mathematics **320** (1973), 175–186.

[Bo] Bolling, *Die Ordnung der Schafarewitsch-Tate Gruppe kann beliebig gross werden*. Math. Nachr. **76** (1975), 157–179.

[Ca1] Cassels, J. W. S. *Arithmetic on curves of genus 1 (VI): The Tate-Šafarevič group can be arbitrarily large*. J. Reine Agnew. Math. **214/215** (1964), 65–70.

[Ca2] Cassels, J. W. S. *Arithmetic on curves of genus 1 (VIII): On the conjectures of Birch and Swinnerton-Dyer*. J. Reine Agnew. Math. **217** (1965), 180–199.

[Fi] Fisher, T. *Some examples of 5 and 7 descent for elliptic curves over* $\mathbb{Q}$. J. Eur. Math. Soc. **3** (2001), No. 2, 169–201.

[H-R] Halberstam, H. and Rickert, H. E. *Sieve Methods*. Academic Press, London (1974), L.M.S. monographs No. 4.

[K-S] Kloosterman, R. and Schaefer, E. *Selmer groups of elliptic curves that can be arbitrarily large*. J. Number Theory **99** (2003), No. 1, 148–163.

[Kr] Kramer, K. *A family of semistable elliptic curves with large Tate-Shafarevich groups*. Proc. Amer. Math. Soc. **89** (1983), No. 3, 379–386.

[La] Lang, S. *Elliptic Functions,* Springer-Verlag, Berlin, New York (1987).

[L] Lemmermeyer, F. *On Tate-Shafarevich groups of some elliptic curves* in Algebraic number theory and Diophantine analysis (Graz 1998), de Gruyter, Berlin (2000), 182–194.

[Mi] Milne, J. S. *Abelian varieties* in Arithmetic Geometry, edited by G. Cornell and J. Silverman, Springer-Verlag, New York (1986), 103–150.

[Ono] Ono, Ken *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves* . J. Reine Agnew. Math. **533** (2001), 81–97.

[S-St] Schaefer, E. and Stoll, M. *How to do a p-descent on an elliptic curve.* to appear in Trans. Amer. Math. Soc.

[Se] Serre, J. P. *Galois Cohomology,* Springer-Verlag, Berlin, New York (1986).

[Si1] Silverman, J. H. *The Arithmetic of Elliptic Curves,* Springer-Verlag, Berlin, New York (1997).

[Si2] Silverman, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves,* Springer-Verlag, Berlin, New York (1994).

[Wo] Wong, Siman *Elliptic curves and class number divisibility.* Internat. Math. Res. Notices (1999), No. 12, 661–672.