K(_2) and L-series of elliptic curves over real quadratic fields

Michael Alexander Young

K_2 and L-series of elliptic curves over real quadratic fields

Michael Alexander Young

A thesis submitted in part fulfillment
of the requirements for the degree
of Doctor of Philosophy

September 29, 1995

Department of Mathematical Sciences
University of Durham
South Road, Durham
England, DH1 3LE

Abstract

This thesis examines the relationship between the L-series of an elliptic curve evaluated at $s = 2$ and the image of the regulator map when the curve is defined over a real quadratic field with narrow class number one, thus providing numerical evidence for Beilinson's conjecture. In doing so it provides a practical formula for calculating the L-series for modular elliptic curves over real quadratic fields, and in outline for more general totally real fields, and also provides numerical evidence for the generalization of the Taniyama-Weil-Shimura conjecture to real quadratic fields.

Preface

No part of this thesis has previously been submitted by me to fulfil the requirements for a degree at this or any other university, and no part of it is the result of joint research by me and any other person.

In particular, the last two sections of Chapter 4 and the whole of Chapter 5 are my own original work, as are the contents of the Appendices (except that some of the results in Appendix A have already been calculated to lower precision by Bloch and Grayson [4] as explained at the start of Section 3.3). Also, the calculations at the end of Section 2.2 are original, and the contents of the first two sections of Chapter 3 may be known to others, but I don't think they have been written out before.

I would like to acknowledge the help of my supervisor Tony Scholl in preparing this thesis, and the support of many others during my time at Durham.

Contents

List of Tables

Chapter 1

Introduction

The basis of this thesis is a conjecture first made by Beilinson [2] (though Bloch was also working along these lines, see for example [5]) relating the value of the L-function of a smooth projective curve V over $\mathbb{Q}$ evaluated at zero to the value obtained from the determinant of the image of the regulator map r. More precisely if l is the leading coefficient of the Taylor expansion of the L-function of V at zero then Beilinson conjectured

$$\begin{aligned} & r\left(\mathrm{K}_2(V)\right) \text{ is a lattice in } H^1(V \otimes \mathbb{C}, \mathbb{R}(1))^+ \\ & \text{and } \det r\left(\mathrm{K}_2(V)\right) = l \det H^1(V \otimes \mathbb{C}, \mathbb{Q}(1))^+ \end{aligned} \tag{1.1}$$

(the notation is explained more fully in Chapter 2).

Computer calculations by Bloch and Grayson [4] on elliptic curves with small conductor and appropriate torsion points, led them to modify the conjecture slightly. The corrected conjecture is as follows:

Conjecture 1. *Let $E_{\mathbb{Z}}$ be the Neron minimal model for an elliptic curve E. Then the rank of $\mathrm{K}_2(E_{\mathbb{Z}}) = 1$, and the image of a generator of $\mathrm{K}_2(E_{\mathbb{Z}})$ under the regulator map is a non-zero rational multiple of $L(E,2)$.*

Note that the important difference is that Bloch and Grayson consider the K-group of the Neron minimal model, in other words they consider the curve over the

integers rather than over the rationals. They also define their regulator differently, in terms of Eisenstein-Kronecker-Lerch series, but their definition is equivalent to Beilinson's apart from a few factors of 2 and π, and they use the value of the L-series at 2, but again this is the same as l above (at least for modular curves) apart from factors of 2 and π. They also explained the rest of the image of $\mathrm{K}_2(E)$ (I cover these matters more fully in chapter 2).

Beilinson extended the conjecture to more general algebraic varieties and more values of the L-function in a later paper [3].

In some cases, partial proofs of the above conjecture are known. For elliptic curves over $\mathbb{Q}$ with complex multiplication there are two papers which show that there are elements of $K_2(E_{\mathbb{Z}})$ with the correct image under the regulator map. Rohrlich [16] gives a proof (building on the work of Bloch) that

Theorem. *If E is an elliptic curve over $\mathbb{Q}$ with complex multiplication and $f, g \in \mathbb{Q}(E)$ have divisors supported on the points of order dividing n (where $\mathbb{Q}(E)$ is the function field of E over $\mathbb{Q}$ and n is an integer) then*

$$r(f \otimes g) = a_{f,g} L'(E, 0)$$

where $a_{f,g} \in n^{-1}\mathbb{Z}$ and $a_{f,g}$ is not zero for some choice of f, g and n.

Note that $L'(E,0)$ means $\frac{d}{ds}\Big|_{s=0} L(E,s)$, and is another way of writing l above. Also Deninger and Wingberg [8] give a proof of a theorem due to Beilinson and Bloch which states

Theorem. *If E is an elliptic curve over $\mathbb{Q}$ with complex multiplication and conductor N, then there exists $\psi \in \mathrm{K}_2(E_{\mathbb{Z}})$ and $\phi \in H^1(E \otimes \mathbb{C}, \mathbb{Q}(1))^+$ such that*

$$r(\psi) = \frac{N}{4\pi^2} L(E, 2)\phi$$

Note that the latter theorem does not require the curve to have any torsion points.

Also Ross in [19] has shown that

Theorem. *For all but finitely many elliptic curves $E/\mathbb{Q}$ which are isogenous to an elliptic curve defined over $\mathbb{Q}$ with a rational torsion point of order at least 3, $K_2(E)$ contains an element of infinite order.*

which confirms that $K_2(E)$ is usually large enough to contain the conjectured rank 1 image of $K_2(E_{\mathbb{Z}})$. He has also proved a similar result for Fermat curves [18] and as a result constructs an element of $K_2(E)$ supported on non-torsion points for the elliptic curve $y^2 + y = x^3$, whose image under the regulator Grayson has shown to be equal to $4L'(E, 0)$ to 100 decimal places.

Further calculations have also been made for elliptic curves over $\mathbb{Q}$ with non-torsion points in unpublished work by Grayson and Schappacher [10], and Nekovář and improved upon by Rolshausen [17] in his thesis.

There seem to be two ways of generalizing this problem. One is to consider higher regulators, related to $L(Sym^k E, k + 1)$. Mestre and Schappacher [13] have verified this numerically for $k = 2$. The other is to consider larger fields than $\mathbb{Q}$, and this thesis aims to examine the numerical evidence in this case, when the fields concerned are real quadratic fields of narrow class number 1.

To do this I need on the one hand to calculate the L-series, and on the other to calculate the regulator. Chapter 4 shows how to calculate the L-series for elliptic curve over real quadratic fields of narrow class number 1. This assumes the curve is modular but a consequence of my calculations will be to provide numerical evidence for this assumption. Chapter 2 defines the regulator by means of Eisenstein-Kronecker-Lerch series, which it also defines, and it starts by defining enough K-theory to describe the various maps and exact sequences around which Beilinson's conjectures are based.

Chapter 3 is concerned with describing the image of the regulator map acting on $K_2(E)$, and explaining that part of the image which doesn't come from elements of $K_2(E_{\mathcal{O}})$, and then moves on to analyse the results of my extension of the calculations of Bloch and Grayson, of the relationship between elements in the

image the regulator map and $L(E,2)$ for rational elliptic curves. These results are presented in Appendix A.

Chapter 5 examines the results from my calculations of the relationship between E-K-L series and $L(E,2)$ for elliptic curves over some real quadratic fields, which are given in Appendix B, and summarizes the main conclusions of this thesis, and where the work might be extended. Finally Appendix C lists the two main programs used in my calculations.

Chapter 2

K-Theory, Regulators and E-K-L series

The purpose of this chapter is to establish enough background mathematics to be able to define the regulator map and thus to state Beilinson's conjecture, and also to define and establish facts about Eisenstein-Kronecker-Lerch series, which we will link to the image of the regulator map.

First we go through enough category theory to define the K-theory groups, and then go through enough K-theory to establish the exact sequences which Beilinson's conjecture relies on in the case we are considering.

Then we switch to defining E-K-L series, and then manipulating them to establish a functional equation, and linked to that an efficient way of evaluating the E-K-L series. We conclude this section by bounding above the sum of all but finitely many terms, and thus establishing the accuracy obtained by adding together sufficiently many of the larger terms, which is what we will calculate in practice.

Finally in this chapter we define the regulator map, and process it in order to link it to the E-K-L series, and in the process connect the various differing definitions of the regulator map in the literature. We conclude the chapter with a

precise statement of Beilinson's conjecture in the cases we consider.

2.1 K-Theory

First we briefly run through the Algebraic K-theory necessary to construct two exact sequences of abelian groups, which will be used to construct and to calculate the regulator. We start with Quillen's Q-construction of the K-groups of a small, exact category. This follows Srinivas's book [23] (see also articles by Quillen [15] and Grayson [11]). We start with some definitions from category theory.

Definition. A **small** category is a category whose objects and morphisms form sets.

Definition. An **additive** category is a category satisfying the following:

Given any two objects a and b, the maps $a \to b$ form an abelian group $\hom(a, b)$, which is distributive under composition. That is, if $f, f' \colon a \to b$ and $g, g' \colon b \to c$ then

$$(g + g') \circ (f + f') = g \circ f + g \circ f' + g' \circ f + g' \circ f'$$

The category contains a null object 0. That is, for any object a, there exist unique maps $a \to 0$ and $0 \to a$.

There is a biproduct for each pair of objects. That is given any two objects a and b, there is an object c and maps $a \underset{p_1}{\overset{i_1}{\rightleftarrows}} c \underset{p_2}{\overset{i_2}{\leftrightarrows}} b$ such that $p_1 i_1 = 1_a$, $p_2 i_2 = 1_b$ and $i_1 p_1 + i_2 p_2 = 1_c$.

Definition. An **abelian** category is an additive category that also satisfies:

Every map has a kernel and a co-kernel. That is, given a map $a \xrightarrow{f} b$ there exists a kernel map $s \xrightarrow{k} a$ such that $fk = 0$ and any map h such that $fh = 0$ factors uniquely through k, and a co-kernel map $b \xrightarrow{c} t$ such that $cf = 0$ and any map h such that $hf = 0$ factors uniquely through c.

Every monic map is the kernel of some map, and every epic map is the co-kernel of some map. (A map $a \xrightarrow{f} b$ is monic if whenever there are maps $g, g' \colon b \to c$ such that $gf = g'f$ then $g = g'$, and is epic if whenever there are maps $g, g' \colon c \to a$ such that $fg = fg'$ then $g = g'$).

Definition. Given a small category $\mathcal{C}$ define $\mathrm{B}\mathcal{C}$, the **classifying space** of $\mathcal{C}$ as follows:

Construct a simplicial set where the n-simplices are the sequences

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \ldots \xrightarrow{f_n} A_n$$

where $A_i \in \mathrm{Ob}\,\mathcal{C}$ and $f_i \in \mathrm{Mor}\,\mathcal{C}$, the ith face of this simplex is the $(n-1)$-simplex

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \ldots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_{i+1} \circ f_i} A_{i+1} \xrightarrow{f_{i+2}} \ldots \xrightarrow{f_n} A_n$$

and the ith degenerate $(n+1)$-simplex is

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \ldots \xrightarrow{f_i} A_i \xrightarrow{1} A_i \xrightarrow{f_{i+1}} \ldots \xrightarrow{f_n} A_n$$

Then the classifying space is defined by

$$\mathrm{B}\mathcal{C} = \left(\coprod_{n \geq 0} (\text{set of } n\text{-simplices with discrete topology}) \times \Delta_n \right) \Big/ \sim$$

where

$$\Delta_n = \left\{ (t_0, \ldots, t_n) \in \mathbb{R}^{n+1} \;\middle|\; t_i \geq 0, \sum_{i=0}^{n} t_i = 1 \right\}$$

and the equivalence relation is generated by the equivalences:

If G is an n-simplex and F its ith face then $\forall (t_0, \ldots, t_{n-1}) \in \Delta_{n-1}$

$$(F, (t_0, \ldots, t_{n-1})) \sim (G, (t_0, \ldots, t_{i-1}, 0, t_i, \ldots, t_{n-1}))$$

If G is an n-simplex and D its ith degenerate then $\forall (t_0, \ldots, t_n) \in \Delta_n$

$$(G, (t_0, \ldots, t_n)) \sim (D, (t_0, \ldots, t_{i-1}, t_i + t_{i+1}, t_{i+2}, \ldots, t_n))$$

Definition. An **exact** category is an additive category that embeds as a full subcategory of an abelian category (i.e. if two objects are in the subcategory, all the maps between them are as well), such that if $0 \to a \to c \to b \to 0$ is an exact sequence in the abelian category with a and b in the subcategory, then there exists an object isomorphic to c in the subcategory. (A sequence $\cdot \xrightarrow{f} c \xrightarrow{g} \cdot$ is exact at c if $\ker(g) = \ker(\mathrm{coker}(f))$ and a sequence is exact in the subcategory if it is exact everywhere in the abelian category).

Definition. Given a small exact category $\mathcal{C}$, we define a new category $Q\mathcal{C}$ where the objects of $Q\mathcal{C}$ are the objects of $\mathcal{C}$ and a morphism $a \to b$ in $Q\mathcal{C}$ is an isomorphism class of diagrams $a \overset{s}{\twoheadleftarrow} c \overset{i}{\hookrightarrow} b$ such that the following diagrams in $\mathcal{C}$ are exact for some objects d and e in $\mathcal{C}$.

$$0 \to c \overset{i}{\hookrightarrow} b \to d \to 0$$

$$0 \leftarrow a \overset{s}{\twoheadleftarrow} c \leftarrow e \leftarrow 0$$

(Two diagrams $a \overset{s}{\twoheadleftarrow} c \overset{i}{\hookrightarrow} b$ and $a \overset{t}{\twoheadleftarrow} f \overset{j}{\hookrightarrow} b$ are isomorphic if there exists an isomorphism $c \overset{\sim}{\to} f$ such that the diagram

$$\begin{array}{ccccc} a & \overset{s}{\twoheadleftarrow} & c & \overset{i}{\hookrightarrow} & b \\ \| & & \| \wr & & \| \\ a & \overset{t}{\twoheadleftarrow} & f & \overset{j}{\hookrightarrow} & b \end{array}$$

commutes). The identity morphism is clearly $a \overset{id}{\twoheadleftarrow} a \overset{id}{\hookrightarrow} a$. Morphisms $a \twoheadleftarrow d \hookrightarrow b$ and $b \twoheadleftarrow e \hookrightarrow c$ are composed via the following diagram

$$\begin{array}{ccccc} d \times_b e & \hookrightarrow & e & \hookrightarrow & c \\ \downarrow & & \downarrow & & \\ d & \hookrightarrow & b & & \\ \downarrow & & & & \\ a & & & & \end{array}$$

where $d \times_b e$ is the pullback in the abelian category containing $\mathcal{C}$, that is, if f is the biproduct of d and e, then $d \times_b e$ is the kernel of difference of the maps $f \to d \to b$

and $f \to e \to b$, which is defined up to isomorphism. (Note that $d \times_b e \to d$ is epic, as $e \twoheadrightarrow b$ is and $d \times_b e \to e$ is monic as $d \hookrightarrow b$ is). This diagram is *a priori* only defined in the abelian category containing $\mathcal{C}$, but as $\ker(d \times_b e \to d) = \ker(e \twoheadrightarrow b) \in \mathcal{C}$ then $d \times_b e \in \mathcal{C}$ (up to isomorphism) because $\mathcal{C}$ is exact. Moreover the compositions of $d \times_b e \hookrightarrow e \hookrightarrow c$ and of $d \times_b e \twoheadrightarrow d \twoheadrightarrow a$ are part of appropriate exact sequences in $\mathcal{C}$, so it is valid to define

$$(b \twoheadleftarrow e \hookrightarrow c) \circ (a \twoheadleftarrow d \hookrightarrow b) = a \twoheadleftarrow d \times_b e \hookrightarrow c$$

The other condition to verify to show that $Q\mathcal{C}$ is a category is the associativity of morphisms, and this is similarly checked.

We are now in the position to state Quillen's Q-definition of the K-theory of a small exact category.

Definition. If $\mathcal{C}$ is a small exact category, let 0 be a zero object of $\mathcal{C}$ (so $\{0\} \in \mathrm{BQ}\mathcal{C}$). Define

$$\mathrm{K}_i(\mathcal{C}) = \pi_{i+1}(\mathrm{BQ}\mathcal{C}, \{0\}) \tag{2.1}$$

where π_i is the ith homotopy group.

In fact, we will want to define the category of a scheme X, so we need to associate a category to it, and in some cases we can do this in two ways.

Definition. If X is a scheme, let $\mathcal{P}(X)$ denote the category of locally free sheaves (of $\mathcal{O}_X$-modules) of finite rank on X. Thus for any sheaf $\mathcal{F} \in \mathcal{P}(X)$, X is covered by open sets U such that $\mathcal{F}|_U \cong (\mathcal{O}_X|_U)^r$ for some integer r. Define

$$\mathrm{K}_i(X) = \mathrm{K}_i(\mathcal{P}(X))$$

If X is a noetherian scheme, let $\mathcal{M}(X)$ denote the category of coherent sheaves on X. Thus for any sheaf $\mathcal{F} \in \mathcal{M}(X)$, X is covered by open affine sets $U = \operatorname{Spec} A$

such that $\mathcal{F}|_U = \widetilde{M}$, for some finitely -generated A-module M. ($\widetilde{M}$ is the $\mathcal{O}_{\operatorname{Spec} A}$-module arising naturally from M, i.e. $\widetilde{M}(V) = M \otimes_A \mathcal{O}_{\operatorname{Spec} A}(V)$). Define

$$\mathrm{K}'_i(X) = \mathrm{K}_i(\mathcal{M}(X))$$

In fact you can show that if X is a regular scheme, then $\mathrm{K}_i(X) = \mathrm{K}'_i(X)$. Also, if $X = \operatorname{Spec} R$ for some ring R, then these groups correspond to those obtained from the "classical" K-theory of R (see [14] for the definition, and [23] shows they are equivalent).

For example, if $X = \operatorname{Spec} F$ for a field F, then $\mathcal{P}(X) = \mathcal{M}(X)$ is the category of finite dimensional F-vector spaces. Using this fact you can show that $\mathrm{K}_0(X) = \mathbb{Z}$, which agrees with the result from classical K-theory. Classical K-theory also shows that $\mathrm{K}_1(X) = F^*$ and $\mathrm{K}_2(X)$ is the abelian group

$$\mathrm{K}_2(X) = \frac{F^* \otimes_{\mathbb{Z}} F^*}{(f \otimes (1-f))_{f \neq 0,1}}$$

by Matsumoto's theorem (see [14]). We denote by $\{f, g\}$ the element of $\mathrm{K}_2(X)$ corresponding to the coset in $F^* \otimes_{\mathbb{Z}} F^*$ containing $f \otimes g$. Note that it is a consequence of the definition that $\{\cdot, \cdot\}$ is anti-symmetric, i.e. $\{f, g\} = -\{g, f\}$. It is also true that if F is a number field then $\mathrm{K}_2(F)$ is a torsion group (this is essentially a result of Garland [9] drawing on results of Bass and Tate, but his paper does not state this result. See for example [25] to fill the gap).

We now move on to consider maps between K-groups arising from functors between exact categories, with the aim of establishing the required exact sequences.

Definition. A functor $F\colon \mathcal{C} \to \mathcal{D}$ between exact categories $\mathcal{C}$ and $\mathcal{D}$ is **exact** if, whenever $0 \to a \xrightarrow{g} b \xrightarrow{h} c \to 0$ is an exact sequence in $\mathcal{C}$, the sequence $0 \to F(a) \xrightarrow{F(g)} F(b) \xrightarrow{F(h)} F(c) \to 0$ is exact in $\mathcal{D}$.

Note that an exact functor between exact categories $F\colon \mathcal{C} \to \mathcal{D}$ induces a functor between categories $QF\colon Q\mathcal{C} \to Q\mathcal{D}$, and hence a continuous map between simplicial complexes $\mathrm{B}QF\colon \mathrm{B}Q\mathcal{C} \to \mathrm{B}Q\mathcal{D}$, and thus a homomorphism between $\mathrm{K}_i(\mathcal{C})$ and $\mathrm{K}_i(\mathcal{D})$.

Definition. A **Serre** subcategory of a small abelian category $\mathcal{C}$ is a full, additive subcategory $\mathcal{D}$ where for any exact sequence $0 \to a \to b \to c \to 0$ in $\mathcal{C}$, $b \in \mathrm{Ob}\,\mathcal{D}$ if and only if $a \in \mathrm{Ob}\,\mathcal{D}$ and $c \in \mathrm{Ob}\,\mathcal{D}$. In particular any object isomorphic to an object in $\mathcal{D}$ is in $\mathcal{D}$, and $\mathcal{D}$ must be abelian as $\mathcal{C}$ is.

Definition. Given a small abelian category $\mathcal{C}$ with a Serre subcategory $\mathcal{D}$ define the **quotient** category $\mathcal{C}/\mathcal{D}$ to be the category whose objects are the objects of $\mathcal{C}$, and where if $a, b \in \mathrm{Ob}\,\mathcal{C}/\mathcal{D}$ then the group of morphisms from a to b is

$$\hom_{\mathcal{C}/\mathcal{D}}(a,b) = \varinjlim \hom_{\mathcal{C}}(a', b/b') \quad \text{such that} \quad a/a', b' \in \mathcal{D}$$

where the partial ordering on the groups is given by setting $\hom_{\mathcal{C}}(a', b/b') \leq \hom_{\mathcal{C}}(a'', b/b'')$ if $a'' \hookrightarrow a' \hookrightarrow a$ and $b \twoheadrightarrow b/b' \twoheadrightarrow b/b''$, and we obtain the map $\hom_{\mathcal{C}}(a', b/b') \to \hom_{\mathcal{C}}(a'', b/b'')$ by sending $a' \xrightarrow{f} b/b'$ to $a'' \twoheadrightarrow a' \xrightarrow{f} b/b' \twoheadrightarrow b/b''$.

Composing morphisms involves a lot of chasing around diagrams, but essentially relies on the isomorphism $(b' \cup b'')/b' \equiv b''/(b' \times_b b'')$, where $b' \cup b''$ is the smallest object such that $b' \hookrightarrow b$ and $b'' \hookrightarrow b$ factor through $(b' \cup b'') \hookrightarrow b$, because given maps $a' \to b/b'$ and $b'' \to c/c'$, we can map these under the partial ordering to maps $(a'' \to b/b') = (a'' \to (b' \cup b'')/b' \hookrightarrow b/b')$ and $(b'' \to c/c'') = (b'' \twoheadrightarrow b''/(b' \times_b b'') \to c/c'')$, and define the composition to be the image of the map $a'' \to c/c''$ via the isomorphism. Also note that the natural map $\mathcal{C} \to \mathcal{C}/\mathcal{D}$ is exact, and $\mathcal{C}/\mathcal{D}$ is an abelian category.

Finally, we can construct an exact sequence of K-groups.

Theorem 2.1. *If $\mathcal{D}$ is a Serre subcategory of an abelian category $\mathcal{C}$, then the natural exact functors $\mathcal{D} \to \mathcal{C}$ and $\mathcal{C} \to \mathcal{C}/\mathcal{D}$ induce the exact sequence of group homomorphisms*

$$\cdots \to \mathrm{K}_i(\mathcal{D}) \to \mathrm{K}_i(\mathcal{C}) \to \mathrm{K}_i(\mathcal{C}/\mathcal{D}) \to \mathrm{K}_{i-1}(\mathcal{D}) \to \ldots$$

Proof. See [23]. □

In particular we can use this to deduce the following

Theorem 2.2. *Let X be a noetherian scheme, and Z a closed subscheme with U its open complement. Then we have the following exact sequence*

$$\cdots \to \mathrm{K}'_i(Z) \to \mathrm{K}'_i(X) \to \mathrm{K}'_i(U) \to \mathrm{K}'_{i-1}(Z) \to \ldots$$

Proof. Observe that $\mathcal{M}(X)$ is an abelian category, with Serre subcategory $\mathcal{M}_Z(X)$ (the category of coherent sheaves supported on Z), and that $\mathcal{M}(U) \equiv \mathcal{M}_U(X) = \mathcal{M}(X)/\mathcal{M}_Z(X)$, thus we have an exact sequence

$$\cdots \to \mathrm{K}_i(\mathcal{M}_Z(X)) \to \mathrm{K}'_i(X) \to \mathrm{K}'_i(U) \to \mathrm{K}_{i-1}(\mathcal{M}_Z(X)) \to \ldots$$

but for any sheaf $\mathcal{F} \in \mathcal{M}_Z(X)$ there is a filtration $0 = \mathcal{F}_0 \subset \mathcal{F}_1 \subset \cdots \subset \mathcal{F}_N = \mathcal{F}$ such that each $\mathcal{F}_n/\mathcal{F}_{n-1}$ is in a category isomorphic to $\mathcal{M}(Z)$, and these are precisely the conditions required to apply the devissage theorem (see [23] again) and we deduce $\mathrm{BQ}\mathcal{M}_Z(X)$ is homotopic to $\mathrm{BQ}\mathcal{M}(Z)$, hence the result. □

Also note that if Z' is another closed subset of X such that $Z \subset Z'$ and where U' is the open complement of Z' then we have the following commutative diagram

$$\begin{array}{ccccccc} & \mathrm{K}'_i(Z) & \longrightarrow & \mathrm{K}'_i(X) & \longrightarrow & \mathrm{K}'_i(U) & \longrightarrow & \mathrm{K}'_{i-1}(Z) & \\ \cdots & \downarrow & & \downarrow{\scriptstyle l} & & \downarrow & & \downarrow & \cdots \\ & \mathrm{K}'_i(Z') & \longrightarrow & \mathrm{K}'_i(X) & \longrightarrow & \mathrm{K}'_i(U') & \longrightarrow & \mathrm{K}'_{i-1}(Z') & \end{array}$$

and thus we take the direct limit of such diagrams. In particular let X be the scheme associated to the elliptic curve E_k over number field k, then we may take the direct limit of sequences given by taking Z to be a finite number of closed points on E_k to obtain

$$\ldots \to \coprod_{\substack{P \in E_k \\ P \text{ closed}}} \mathrm{K}_i(k(P)) \to \mathrm{K}_i(E_k) \to \mathrm{K}_i(k(E)) \xrightarrow{\partial} \coprod_{\substack{P \in E_k \\ P \text{ closed}}} \mathrm{K}_{i-1}(k(P)) \to \ldots$$

But if F is a number field then $\mathrm{K}_2(F)$ is a torsion group, and by [12] we know an explicit expression for the map ∂: $\mathrm{K}_2(k(E))_{\mathbb{Q}} \to \coprod_{\substack{P \in E_k \\ P \text{ closed}}} k(P)^*$ and so, if we denote $K_i(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$ by $K_i(\mathcal{C})_{\mathbb{Q}}$ we conclude

Theorem 2.3. *For an elliptic curve E over a number field k, the sequence*

$$\text{(2.2)} \qquad \textit{torsion} \to \mathrm{K}_2(E_k) \to \mathrm{K}_2(k(E)) \xrightarrow{\partial} \coprod_{\substack{P \in E_k \\ P \text{ closed}}} k(P)^* \to \dots$$

is exact where ∂ is given by

$$\partial = \coprod_{\substack{P \in E_k \\ P \text{ closed}}} \partial_P \qquad \textit{where} \qquad \partial_P(\{f,g\}) = (-1)^{ord_P(f)ord_P(g)} \frac{f^{ord_P(g)}}{g^{ord_P(f)}}(P)$$

In particular,

$$\text{(2.3)} \qquad \mathrm{K}_2(E_k)_{\mathbb{Q}} = \ker \left(\mathrm{K}_2(k(E)) \xrightarrow{\partial} \coprod_{\substack{P \in E_k \\ P \text{ closed}}} k(P)^* \right)_{\mathbb{Q}}$$

Hence every non-torsion element of $\mathrm{K}_2(E_k)$ may be identified with a $\mathbb{Q}$-linear combination of elements of $\mathrm{K}_2(k(E))$.

This Theorem allows us to define the regulator map on the torsion free part of $\mathrm{K}_2(E_k)$ by considering it a subgroup of $\mathrm{K}_2(k(E))$.

The second exact sequence we require is obtained by letting X be the scheme corresponding to a regular model of the elliptic curve E over the ring of integers $\mathcal{O}_k$ of k, denoted $E_{\mathcal{O}}$, and taking the direct limit over those closed subsets corresponding to finitely many reduced curves. Thus we have

$$\dots \to \coprod_{\mathfrak{p} \text{ prime in } k} \mathrm{K}'_i(E_{\mathfrak{p}}) \to \mathrm{K}'_i(E_{\mathcal{O}}) \to \mathrm{K}'_i(E_k) \to \coprod_{\mathfrak{p} \text{ prime in } k} \mathrm{K}'_{i-1}(E_{\mathfrak{p}}) \to \dots$$

In particular we want the following piece of this sequence

Theorem 2.4. *Let $E_{\mathcal{O}}$ be a minimal regular model for an elliptic curve E over a number field k. Then the sequence*

$$\text{(2.4)} \qquad \mathrm{K}_2(E_{\mathcal{O}}) \to \mathrm{K}_2(E_k) \to \coprod_{\mathfrak{p} \textit{ prime in } k} \mathrm{K}'_1(E_{\mathfrak{p}})$$

is exact at $\mathrm{K}_2(E_k)$.

This will allow us to state Beilinson's conjecture, once we have defined the regulator.

2.2 E-K-L series

This section will define Eisenstein-Kronecker-Lerch series, and establish some basic properties needed elsewhere such as the functional equation. It is based on material in the book by Weil [27]. Throughout this section Λ will be a lattice over $\mathbb{C}$ generated by u and v. First we define some quantities that will be used extensively in what follows.

Definition. Define $\tau = \delta v/u$, where $\delta = \pm 1$ is chosen such that $\mathrm{Im}(\tau) > 0$. Define

$$A = \frac{\mathrm{Im}(\tau)u\overline{u}}{\pi} = \frac{\delta(v\overline{u} - u\overline{v})}{2\pi i}$$

For $x_0, w \in \mathbb{C}$, define the character $\chi(w)$ by

$$\chi(w) = \chi(w; x_0) = e^{(\overline{x_0}w - \overline{w}x_0)/A}$$

Definition. If $a \in \mathbb{Z}_{\geq 0}$, define the Eisenstein-Kronecker-Lerch series for $\mathrm{Re}(s) > \frac{a}{2} + 1$ as

$$K_a(x, x_0, s) = \sum_{\substack{w \in \Lambda \\ w \neq -x}} \frac{\chi(w)(\overline{x+w})^a}{|x+w|^{2s}} \tag{2.5}$$

This may be continued analytically to the whole of the s-plane as follows. For $\mathrm{Re}(s) > \frac{a}{2} + 1$, we have

$$\Gamma(s)K_a(x, x_0, s) = \int_0^\infty \Theta_a^*(t, x, x_0)t^{s-1}dt$$

where

$$\Theta_a^*(t, x, x_0) = \sum_{\substack{w \in \Lambda \\ w \neq -x}} e^{-t|x+w|^2}\chi(w)(\overline{x+w})^a$$

Define Θ_a to be the result of extending the sum in the definition of Θ_a^* to all $w \in \Lambda$. So

$$\Theta_a(t, x, x_0) = \begin{cases} \Theta_a^*(t, x, x_0) + \chi(-x) & \text{if } a = 0 \text{ and } x \in \Lambda \\ \Theta_a^*(t, x, x_0) & \text{otherwise} \end{cases}$$

Observe that the function $\chi(x)\Theta_a(t,x,x_0)$ is doubly periodic in x, that is if $x = \alpha u + \beta v$ then $\chi(x)\Theta_a(t,x,x_0)$ has period 1 in α and β. Assume for the moment that $a = 0$. We may then use a Fourier Transform to write

$$\chi(x)\Theta_0(t,x,x_0) = \sum_{\epsilon,\eta\in\mathbb{Z}} e^{2\pi i(\alpha\epsilon+\beta\eta)} f(\epsilon,\eta)$$

where

$$f(\epsilon,\eta) = \int_0^1 \int_0^1 \chi(\alpha u+\beta v)\Theta_0(t,\alpha u+\beta v,x_0)e^{-2\pi i(\alpha\epsilon+\beta\eta)}d\alpha d\beta$$

But if $y = \delta(-\epsilon v + \eta u) \in \Lambda$ for integer ϵ and η, then

$$2\pi i(\alpha\epsilon+\beta\eta) = (x\overline{y} - y\overline{x})/A = ((x+w)\overline{y} - y(\overline{x+w}))/A$$

for any $w \in \Lambda$, and as $d\alpha d\beta = (d\overline{x}\wedge dx)/\delta(v\overline{u} - u\overline{v})$ we may combine the sum and integral to get

$$\begin{aligned} f(\epsilon,\eta) &= \frac{1}{\delta(v\overline{u}-u\overline{v})}\int_{\mathbb{C}} e^{-tx\overline{x}+x(\overline{x_0-y})/A-\overline{x}(x_0-y)/A} d\overline{x}\wedge dx \\ &= \frac{1}{At}e^{-(x_0-y)(\overline{x_0-y})/A^2t} \end{aligned}$$

so

$$\begin{aligned} \Theta_0(t,x,x_0) &= \chi(-x)\frac{1}{At}\sum_{-y\in\Lambda} e^{-(x_0-y)(\overline{x_0-y})/A^2t}e^{-(x\overline{y}-y\overline{x})/A} \\ &= \chi(-x)\frac{1}{At}\Theta_0(A^{-2}t^{-1},x_0,x) \end{aligned}$$

and differentiating both sides a times with respect to x gives

$$\Theta_a(t,x,x_0) = \chi(-x)(At)^{-a-1}\Theta_a(A^{-2}t^{-1},x_0,x) \tag{2.6}$$

Now we use this to get the analytic continuation of K_a. For $T > 0$ let

$$\begin{aligned} I(T,a,x,x_0,s) &= \int_T^\infty \Theta_a^*(t,x,x_0)t^{s-1}dt \\ &= \sum_{\substack{w\in\Lambda \\ w\neq -x}} \frac{\chi(w)(\overline{x+w})^a}{|x+w|^{2s}}\int_{T|x+w|^2}^\infty e^{-t}t^{s-1}dt \end{aligned}$$

This is absolutely convergent for all s, and defines a holomorphic function on $\mathbb{C}$. Thus

$$\begin{aligned}\Gamma(s)K_a(x,x_0,s) - I(T,a,x,x_0,s) &= -\lambda\chi(-x)\frac{T^s}{s} + \int_0^T \Theta_a(t,x,x_0)t^{s-1}dt \\ &= -\lambda\chi(-x)\frac{T^s}{s} + \int_0^T (At)^{-a-1}\Theta_a(A^{-2}t^{-1},x_0,x)\chi(-x)t^{s-1}dt \\ &= -\lambda\chi(-x)\frac{T^s}{s} - \mu\frac{T^{s-a-1}}{(a-s+1)A^{a+1}} + \frac{\chi(-x)}{A^{2s-a-1}}\int_{1/A^2t}^{\infty}\Theta_a^*(t,x_0,x)t^{a-s}dt\end{aligned}$$

so

Theorem 2.5. *For K,χ and I as above, we have*

$$\begin{aligned}(2.7)\quad \Gamma(s)K_a(x,x_0,s) &= I(T,a,x,x_0,s) - \lambda\chi(-x)\frac{T^s}{s} \\ &\quad - \mu\frac{T^{s-a-1}}{(a-s+1)A^{a+1}} + \frac{\chi(-x)}{A^{2s-a-1}}I\left(\frac{1}{A^2T},a,x_0,x,a-s+1\right)\end{aligned}$$

where

$$\lambda = \begin{cases} 1 & \text{if } a=0 \text{ and } x\in\Lambda \\ 0 & \text{otherwise}\end{cases} \quad \text{and } \mu = \begin{cases} 1 & \text{if } a=0 \text{ and } x_0\in\Lambda \\ 0 & \text{otherwise}\end{cases}$$

and since the right hand side of this equation is defined for all s, as is $\Gamma(s)$, this defines the analytic continuation of the E-K-L series to the whole of the s-plane.

Note that since $\Gamma(s)$ has no zeroes, the only possible poles of the E-K-L series are simple poles at $s=0$ if $a=0$ and $x\in\Lambda$, and at $s=1$ if $a=0$ and $x_0\in\Lambda$. We will mostly be using equation (2.7) when $a=1$, $x=0$, $s=2$ and $T=A^{-1}$ to give a rapidly convergent way of calculating the E-K-L series in this case. Hence

Corollary 2.6.

$$\begin{aligned}(2.8)\quad & K_1(0,x_0,2) \\ &= \sum_{w\in\Lambda\smallsetminus\{0\}}\frac{\chi(w)}{w^2\overline{w}}\left(\frac{|w|^2}{A}+1\right)e^{-|w|^2/A} + \frac{1}{A^2}\sum_{\substack{w\in\Lambda\\ w\neq -x_0}}(\overline{x_0+w})\,\mathrm{Ei}\left(\frac{|x_0+w|^2}{A}\right)\end{aligned}$$

Also observe that if we set $T = A^{-1}$, then the right hand side of (2.7) is fixed by multiplying by $A^{2s-a-1}\chi(x)$ and then exchanging x for x_0 and replacing s by $a+1-s$. Thus we get the following functional equation for the E-K-L series

Theorem 2.7.

$$\Gamma(s)K_a(x,x_0,s) = \chi(-x)A^{a+1-2s}\Gamma(a+1-s)K_a(x_0,x,a+1-s) \tag{2.9}$$

This will also be useful later.

Since we will want to evaluate $K_1(0,x_0,2)$ for various real elliptic curves, when x_0 corresponds to various real points, it is useful to have some idea of which terms we need to evaluate and which we can ignore to obtain a sufficiently accurate result. Recall

$$K_1(0,x_0,2) = \sum_{w\in\Lambda\smallsetminus\{0\}} e^{(\overline{x}_0 w - \overline{w}x_0)/A}\frac{1}{w^2\overline{w}}$$

Observe that for any Λ and any x_0, $K_1(0,x_0,2)$ is antisymmetric in x_0, so $K_1(0,-x_0,2) = -K_1(0,x_0,2)$, and if $y\in\Lambda$, $K_1(0,x_0+y,2) = K_1(0,x_0,2)$, which shows that $K_1(0,x_0,2) = 0$ if $x_0 \in \frac{1}{2}\Lambda$, so we know the result exactly in this case.

More generally, if we assume Λ corresponds to a real elliptic curve and x_0 is a real point, we know that $\Lambda = \overline{\Lambda}$, $x \equiv \overline{x} \mod \Lambda$, and thus $K_1(0,x_0,2)$ is real. By equation (2.8) we have

$$\begin{aligned} &K_1(0,x_0,2) \\ &= \sum_{w\in\Lambda\smallsetminus\{0\}} \left(\frac{|w|^2}{A}+1\right)\frac{e^{(\overline{x}_0 w-\overline{w}x)/A}e^{-|w|^2/A}}{w^2\overline{w}} + \frac{1}{A^2}\sum_{\substack{w\in\Lambda\\ w\neq -x_0}} (\overline{x_0+w})\,\mathrm{Ei}\left(\frac{|x_0+w|^2}{A}\right) \end{aligned}$$

and we use this equation to calculate the E-K-L series when we don't know the answer exactly. Clearly the modulus of each term depends only on $|w|$ for the first sum and $|x_0+w|$ for the second, and strictly decreases very rapidly as these increase. Moreover it is easy to see that if $t>0$, $\mathrm{Ei}(t) \le e^{-t}/t$, so if we set $r = |w|$

in the first case and $r = |x_0 + w|$ in the second, then in either case the modulus of the term in w is bounded by

$$e^{-r^2/A}\left(\frac{1}{rA} + \frac{1}{r^3}\right)$$

Since this depends only on r, it seems reasonable to calculate those terms in a disc, of radius R say, and then bound the remaining terms by summing over annuli of increasing diameter. In this case all we need to do is to come up with a good bound on the number of points in an annulus, and to choose how thick to make the annuli to facilitate this.

Let the generators of the lattice Λ be u and v, where u is the least positive real element of Λ, and $\mathrm{Re}(v) = 0$ or $= \frac{1}{2}u$. Consider a fundamental parallelogram which maximizes the smaller of the distances between the two pairs of parallel sides, d say. If $\mathrm{Re}(v) = 0$ one such parallelogram has vertices $0, u, u+v$ and v, and if $\mathrm{Re}(v) = \frac{1}{2}u$ then such a parallelogram has vertices $0, \overline{v}, u$ and v.

For a circle of radius r' consider the union of the tesselations of the parallelogram which intersect the interior of the circle. The border of this contains all the extra lattice points within a larger concentric circle of radius r'' if r'' is sufficiently close to r', for example if $r'' = r' + d$. There are at most $8\lceil r'/d \rceil$ lattice points on the border, because the border has the same length as that of the smallest parallelogram with sides parallel to the parallelogram above containing the circle.

Thus the sum of the terms of the sum outside a circle of radius R are bounded in modulus by

$$(2.10)\quad 2\sum_{n=0}^{\infty} 8(R+(n+1)d)e^{-(R+nd)^2/A}\left(\frac{1}{(R+nd)A} + \frac{1}{(R+nd)^3}\right) \leq 16e^{-R^2/A}\frac{(R+d)\left(\frac{1}{RA}+\frac{1}{R^3}\right)}{1-e^{-2Rd/A}}$$

where $d = \min(1, \mathrm{Im}(\tau))$ if $\mathrm{Im}(v) = 0$, and $d = \mathrm{Im}(\tau)/\sqrt{1/4 + \mathrm{Im}(\tau)^2}$ otherwise. As the dominant term in this expression is a power of e^{-R^2}, we should only need to calculate in the order of 1000 terms to get very good accuracy, hence justifying

the claim that the series converges very rapidly, and thus we can afford surplus accuracy at this stage, since other stages of my calculations take considerably longer (in practice this calculation takes a matter of seconds, but other calculations take minutes or even hours).

2.3 Regulators

This section will define the regulator, and link it to E-K-L series. On the way, it will also show that the definition given here is equivalent to various other definitions given in the literature. We begin by defining a map $r_\sigma\colon \mathrm{K}_2(E_k)_\mathbb{Q} \longrightarrow H^1(E_\sigma(\mathbb{C}), 2\pi i\mathbb{R})$ for each embedding $k \xhookrightarrow{\sigma} \mathbb{C}$. Recall by Theorem 2.3, that we may identify $\mathrm{K}_2(E_k)_\mathbb{Q}$ with the kernel of the map ∂ tensored with $\mathbb{Q}$. So

Definition. Let E be an algebraic curve over k, let E_σ be the curve over $\mathbb{C}$ given by the embedding $k \xhookrightarrow{\sigma} \mathbb{C}$ and let γ be a loop on $E_\sigma(\mathbb{C})$ based at a point α. Define the homomorphism $r_\sigma\colon \mathrm{K}_2(E_k)_\mathbb{Q} \to H^1(E_\sigma(\mathbb{C}), 2\pi i\mathbb{R})$ by defining the image of an element $\sum_j \{f_j, g_j\} \in \ker\partial$ to be

(2.11)
$$r_\sigma\Big(\sum_j \{f_j, g_j\}\Big)(\gamma) = 2\pi i \sum_j \mathrm{Re}\left(\frac{\int_\gamma \ln f_{j\sigma}\, d\ln g_{j\sigma} - \ln(g_{j\sigma}(\alpha)) \int_\gamma d\ln f_{j\sigma}}{2\pi i}\right)$$

and extending linearly.

Proof (Well Defined). First observe that

$$\begin{aligned}\mathrm{Re}\left(\frac{1}{i}\int_\gamma \ln f_{j\sigma}\, d\ln g_{j\sigma}\right) &= \int_\gamma \ln|f_{j\sigma}|\, d\arg g_{j\sigma} + \int_\gamma \arg f_{j\sigma}\, d\ln|g_{j\sigma}| \\ &= \int_\gamma \ln|f_{j\sigma}|\, d\arg g_{j\sigma} + \Big[\arg f_{j\sigma} \ln|g_{j\sigma}|\Big]_\gamma - \int_\gamma \ln|g_{j\sigma}|\, d\arg f_{j\sigma}\end{aligned}$$

and

$$\begin{aligned}\mathrm{Re}\left(\frac{1}{i}\ln(g_{j\sigma}(\alpha)) \int_\gamma d\ln f_{j\sigma}\right) &= \ln|g_{j\sigma}(\alpha)| \Big[\arg f_{j\sigma}\Big]_\gamma + \arg(g_{j\sigma}(\alpha))\Big[\ln|f_{j\sigma}|\Big]_\gamma \\ &= \Big[\arg f_{j\sigma} \ln|g_{j\sigma}|\Big]_\gamma\end{aligned}$$

thus

$$(2.12) \qquad r_\sigma\Big(\sum_j \{f_j, g_j\}\Big)(\gamma) = \oint_\gamma i \sum_j \left(\ln|f_{j\sigma}|\, d\arg g_{j\sigma} - \ln|g_{j\sigma}|\, d\arg f_{j\sigma}\right)$$

so in particular the definition is independent of choice of α, and r_σ is anti-symmetric if we exchange the f_j with the g_j.

To show that the definition depends only on the homotopy class of γ, it is enough to show that if γ is a contractible loop then $r_\sigma\left(\sum_j \{f_j, g_j\}\right)(\gamma) = 0$. But by Cauchy's Theorem on (2.11), this will equal the sum of the residues at the zeroes and poles of the $f_{j\sigma}$ and $g_{j\sigma}$ enclosed by γ. However the zeroes and poles of the $f_{j\sigma}$ and $g_{j\sigma}$ are just the images under σ of poles and zeroes in $\bar{k}$ of the f_j and g_j. Let P be a pole or zero of one of the f_j or g_j. Using local co-ordinates about P_σ, let γ_P be a circle with radius r and centre P_σ, which is small enough so that no pole or zero of the $f_{j\sigma}$ or $g_{j\sigma}$ other than P_σ is inside. Write $f_{j\sigma}(re^{i\theta} + P_\sigma) = \left(re^{i\theta}\right)^{m_j} \hat{f}_j(re^{i\theta})$ and $g_{j\sigma}(re^{i\theta} + P_\sigma) = \left(re^{i\theta}\right)^{n_j} \hat{g}_j(re^{i\theta})$, where $\hat{f}_j$ and $\hat{g}_j$ have neither poles nor zeroes at $r = 0$ (i.e. at P_σ). Then, by using Cauchy's formula and Cauchy's theorem, we have

$$\begin{aligned}
\int_{\gamma_P} \ln f_{j\sigma}\, d\ln g_{j\sigma} &= \int_{\theta=0}^{2\pi} \left(m_j \ln r + i m_j \theta + \ln \hat{f}_j\right)\left(d(i n_j \theta) + d\ln \hat{g}_j\right) \\
&= m_j n_j \left(2\pi i \ln r - 2\pi^2\right) + 2\pi i n_j \ln \hat{f}_j(0) \\
&\qquad + \left[m_j(\ln r + i\theta)\ln \hat{g}_j\right]_{\theta=0}^{2\pi} - \int_{\theta=0}^{2\pi} \ln \hat{g}_j\, d(i m_j \theta) + 0 \\
&= m_j n_j \left(2\pi i \ln r - 2\pi^2\right) + 2\pi i n_j \ln \hat{f}_j(0) \\
&\qquad + 2\pi i m_j \ln \hat{g}_j(r) - 2\pi i m_j \ln \hat{g}_j(0)
\end{aligned}$$

and

$$\begin{aligned}
\ln(g_{j\sigma}(\alpha)) \int_{\gamma_P} d\ln f_{j\sigma} &= (n_j \ln r + \ln \hat{g}_j(r))\left[m_j \ln r + i m_j \theta + \ln \hat{f}_j\right]_{\theta=0}^{2\pi} \\
&= 2\pi i m_j n_j \ln r + 2\pi i m_j \ln \hat{g}_j(r)
\end{aligned}$$

thus

$$\begin{aligned} r_\sigma\Big(\sum_j\{f_j,g_j\}\Big)(\gamma_P) &= 2\pi i\sum_j \mathrm{Re}\left(\pi i m_j n_j + \ln\left(\frac{\hat{f}_j(0)^{n_j}}{\hat{g}_j(0)^{m_j}}\right)\right) \\ &= 2\pi i\sum_j \mathrm{Re}\left(\ln\left((-1)^{m_jn_j}\frac{f^{n_j}}{g^{m_j}}(P)\right)_\sigma\right) \\ &= 2\pi i \ln\Big|\partial_P\Big(\sum_j\{f_j,g_j\}\Big)_\sigma\Big| = 0 \end{aligned}$$

since $\sum_j\{f_j,g_j\}\in\ker\partial$. Thus if γ is contractible, $r_\sigma\left(\sum_j\{f_j,g_j\}\right)(\gamma)=0$. Hence the image of r_σ is contained in $H^1(E_\sigma(\mathbb{C}),2\pi i\mathbb{R})$.

We still have to show that r_σ is a homomorphism, and that the image does not depend on the choice of the f_j and g_j in an element $\sum_j\{f_j,g_j\}$.

It is clear from the definition that r_σ is a homomorphism, so to show that the image does not depend on the choice of the f_j and g_j in an element $\sum_j\{f_j,g_j\}$ we need to show that r_σ preserves bimultiplicity, and that $r_\sigma(\{f,1-f\})(\gamma)=0$ $\forall f\not\equiv 0$ or 1.

The former is straightforward, for example

$$\begin{aligned} r_\sigma(\{f,gh\})(\gamma) &= \oint_\gamma i\left(\ln|f_\sigma|\,d\arg g_\sigma h_\sigma - \ln|g_\sigma h_\sigma|\,d\arg f_\sigma\right) \\ &= \oint_\gamma i\left(\ln|f_\sigma|\,d\arg g_\sigma - \ln|g_\sigma|\,d\arg f_\sigma\right) \\ &\qquad + \oint_\gamma i\left(\ln|f_\sigma|\,d\arg h_\sigma - \ln|h_\sigma|\,d\arg f_\sigma\right) \\ &= r_\sigma(\{f,g\})(\gamma) + r_\sigma(\{f,h\})(\gamma) \\ &= r_\sigma(\{f,g\}+\{f,h\})(\gamma) \end{aligned}$$

Similarly,

$$r_\sigma(\{fh,g\})(\gamma) = r_\sigma(\{f,g\}+\{h,g\})(\gamma)$$

To complete the proof we must show that $r_\sigma(\{f,1-f\})(\gamma)=0$ for any $f\not\equiv 0$ and $\not\equiv 1$, and any γ. By replacing γ by a homotopic path, we may assume that f

and $1-f$ have no poles or zeroes on γ. Now

$$r_\sigma(\{f,1-f\})(\gamma) = -i\,\mathrm{Im}\left(\int_\gamma \ln f_\sigma d\ln(1-f_\sigma) - \ln(1-f_\sigma(\alpha))\int_\gamma d\ln f_\sigma\right)$$

thus if $\gamma' = f_\sigma(\gamma)$, and $\alpha' = f_\sigma(\alpha)$ it is enough to show that

$$\mathrm{Im}\left(\int_{\gamma'}(\ln x)d\ln(1-x) - \ln(1-\alpha')\int_{\gamma'} d\ln x\right) = 0$$

and by considering homotopies of γ', it is enough to show this when γ' is a small loop about either $x=0$ or $x=1$. This is easy at $x=1$, since both integrals are zero in this case, and the $x=0$ case follows by anti-symmetry, replacing x by $1-x$. $\square$

Most of the above follows the ideas of Beilinson's paper [2]. Note that if σ is a real embedding, and thus σ factors $\sigma\colon k \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ then we can deduce from the definition of r_σ that $r_\sigma(\sum_j\{f_j,g_j\})(\overline{\gamma}) = \overline{r_{\overline{\sigma}}(\sum_j\{f_j,g_j\})(\gamma)}$, hence the image of r_σ is contained in $H^1(E_\sigma(\mathbb{C}),2\pi i\mathbb{R})^+$, which is the $+1$ eigenspace when complex conjugation acts simultaneously on $E_\sigma(\mathbb{C})$ and on $2\pi i\mathbb{R}$. $H^1(E_\sigma(\mathbb{C}),2\pi i\mathbb{R})^+$ is a one dimensional real vector space, and thus it may be identified with $\mathbb{R}$ if we choose an element of $H^1(E_\sigma(\mathbb{C}),2\pi i\mathbb{R})^+$ to map to $1\in\mathbb{R}$. The natural choice for such an element is the element of $H^1(E_\sigma(\mathbb{C}),2\pi i\mathbb{R})^+$ which maps the real period of $E_\sigma(\mathbb{C})$ to zero, and the imaginary period to $2\pi i$.

An alternative way of mapping this space to $\mathbb{R}$ is by means of differential forms. By (2.12) we see that $r_\sigma(\sum_j\{f_j,g_j\})$ can be identified with a closed differential 1-form, thus we can assign a value to it via the bilinear pairing of closed 1-forms

$$\langle\eta,\omega\rangle = \pi i\int_{E_\sigma(\mathbb{C})}\eta\wedge\omega$$

Observe that

$$\begin{aligned} i\left(\ln|f_\sigma|\,d\arg g_\sigma - \ln|g_\sigma|\,d\arg f_\sigma\right) & \\ &= \ln|f_\sigma|\left(d\ln g_\sigma - d\ln|g_\sigma|\right) + \ln|g_\sigma|\left(\overline{d\ln f_\sigma} - d\ln|f_\sigma|\right) \\ &= \ln|g_\sigma|\,\overline{d\ln f_\sigma} + \ln|f_\sigma|\,d\ln g_\sigma - d\left(\ln|f_\sigma|\ln|g_\sigma|\right) \end{aligned}$$

So if ω is a closed holomorphic 1-form (for example dx but not $\overline{dx}$), we deduce from (2.12) that

$$\begin{aligned}(2.13)\quad &\Big\langle r_\sigma\Big(\sum_j\{f_j,g_j\}\Big),\omega\Big\rangle \\ &\qquad = \pi i\int_{E_\sigma(\mathbb{C})} r_\sigma\Big(\sum_j\{f_j,g_j\}\Big)\wedge\omega = \sum_j \pi i\int_{E_\sigma(\mathbb{C})}\ln|g_{j\sigma}|\,\overline{d\ln f_{j\sigma}}\wedge\omega\end{aligned}$$

which brings us to Rohrlich's [16] definition of the regulator if we take $k=\mathbb{Q}$ and $\sigma\colon \mathbb{Q}\hookrightarrow\mathbb{C}$ to be the natural embedding. For a rational elliptic curve E, he defines the regulator map $r\colon \mathbb{Q}(E)^*\otimes\mathbb{Q}(E)^*\to\mathbb{R}$ to be

$$r(f\otimes g)=\frac{\int_{E(\mathbb{C})}\ln|f|\,\overline{dg/g}\wedge\omega}{\pi i\int_{E(\mathbb{R})^\circ}\omega}$$

where $E(\mathbb{R})^\circ$ is the connected component of $E(\mathbb{R})$ containing zero, and ω is a holomorphic 1-form. With the above assumption, this r is equivalent to $2r_\sigma\in H^1(E_\sigma(\mathbb{C}),2\pi i\mathbb{R})^+$ under the identification of $H^1(E_\sigma(\mathbb{C}),2\pi i\mathbb{R})^+$ with $\mathbb{R}$ as above.

We return to the general case. The main reason why we introduce the bilinear pairing $\langle\cdot,\cdot\rangle$ is because if we take $\omega=dx$, then we can express $\langle r_\sigma(\sum_j\{f_j,g_j\}),dx\rangle$ only in terms of the poles and zeroes of the $f_{j\sigma}$ and $g_{j\sigma}$.

Lemma 2.8. If Λ is the period lattice of $E_\sigma(\mathbb{C})$ then

$$(2.14)\qquad \Big\langle r_\sigma\Big(\sum_j\{f_j,g_j\}\Big),dx\Big\rangle=(\pi A)^2\sum_j\sum_{z,w\in\mathbb{C}/\Lambda}\mathrm{ord}_w(f_{j\sigma})\mathrm{ord}_z(g_{j\sigma})\overline{K_1(0,z-w,2)}$$

Proof. First observe that

$$\Big\langle r_\sigma\Big(\sum_j\{f_j,g_j\}\Big),dx\Big\rangle=\sum_j\pi i\int_{E_\sigma(\mathbb{C})}\ln|g_{j\sigma}|\,\overline{d\ln f_{j\sigma}}\wedge dx$$

and the integrals on the right hand side are defined not only for $\sum_j\{f_j,g_j\}\in\ker\partial$ but for any set of $f_j\otimes g_j\in k(E)^*\otimes k(E)^*$. Thus it is enough to show that

$$\pi i\int_{E_\sigma(\mathbb{C})}\ln|g_\sigma|\,\overline{d\ln f_\sigma}\wedge dx=(\pi A)^2\sum_{z,w\in\mathbb{C}/\Lambda}\mathrm{ord}_w(f_\sigma)\mathrm{ord}_z(g_\sigma)\overline{K_1(0,z-w,2)}$$

where $f, g \in k(E)^*$.

Observe that $\ln|g_\sigma|$ is periodic with respect to the lattice Λ (where $E_\sigma(\mathbb{C}) = \mathbb{C}/\Lambda$). Thus we can again use Fourier Transforms to write

$$\ln|g_\sigma(x)| = \sum_{y\in\Lambda} e^{(x\overline{y}-y\overline{x})/A} G(y)$$

where if $y \neq 0$

$$\begin{aligned} G(y) &= \int_{\mathbb{C}/\Lambda} e^{-(x\overline{y}-y\overline{x})/A} \ln|g_\sigma(x)| \frac{d\overline{x}\wedge dx}{2\pi i A} \\ &= \left(\frac{A}{-\overline{y}}\right)^3 \int_{\mathbb{C}/\Lambda} e^{-(x\overline{y}-y\overline{x})/A} \frac{\partial^3}{\partial x^3}(\ln|g_\sigma(x)|) \frac{d\overline{x}\wedge dx}{2\pi i A} \end{aligned}$$

But in this case, we can write g_σ in terms of the sigma function, so

$$g_\sigma(x) = c \prod_{z\in\mathbb{C}/\Lambda} \mathrm{ord}_z(g_\sigma)\sigma(x-z) \qquad \text{where} \qquad \sigma(x) = x \prod_{\substack{\lambda\in\Lambda \\ \lambda\neq 0}} \left(1+\frac{x}{\lambda}\right) e^{-x/\lambda + x^2/2\lambda^2}$$

for some constant c. Now

$$\frac{\partial^3}{\partial x^3}(\ln|g_\sigma(x)|) = \sum_{z\in\mathbb{C}/\Lambda} \mathrm{ord}_z(g_\sigma) \sum_{w\in\Lambda} \frac{1}{(x-z+w)^3}$$

which gives

$$\begin{aligned} G(y) &= -\frac{A^3}{\overline{y}^3} \int_{\mathbb{C}/\Lambda} e^{-(x\overline{y}-y\overline{x})/A} \sum_{z\in\mathbb{C}/\Lambda} \mathrm{ord}_z(g_\sigma) K_3(x-z,0,3) \frac{d\overline{x}\wedge dx}{2\pi i A} \\ &= -\frac{A^3}{\overline{y}^3} \sum_{z\in\mathbb{C}/\Lambda} \mathrm{ord}_z(g_\sigma) \int_{\mathbb{C}/\Lambda} e^{-(x\overline{y}-y\overline{x})/A} \frac{\Gamma(1)}{A^2\Gamma(3)} K_3(0,x-z,1) \frac{d\overline{x}\wedge dx}{2\pi i A} \end{aligned}$$

as K_3 is bounded in any choice of $\mathbb{C}/\Lambda$. But if $\mathrm{Re}(s) > \frac{5}{2}$

$$\begin{aligned} &\int_{\mathbb{C}/\Lambda} e^{-(x\overline{y}-y\overline{x})/A} K_3(0,x-z,s) \frac{d\overline{x}\wedge dx}{2\pi i A} \\ &\qquad = e^{(z\overline{y}-y\overline{z})/A} \int_{\mathbb{C}/\Lambda} \sum_{\substack{w\in\Lambda \\ w\neq 0}} e^{((w+y)\overline{x}-x(\overline{w+y}))/A} \frac{\overline{w}^3}{|w|^{2s}} \frac{d\overline{x}\wedge dx}{2\pi i A} \\ &\qquad = -e^{-(z\overline{y}-y\overline{z})/A} \frac{\overline{y}^3}{|y|^{2s}} \end{aligned}$$

so by analytic continuation, if $y \neq 0$

$$G(y) = \frac{A}{2\,|y|^2} \sum_{z \in \mathbb{C}/\Lambda} \mathrm{ord}_z(g_\sigma) e^{-(z\overline{y} - y\overline{z})/A}$$

Thus we conclude

$$\ln |g_\sigma(x)| = \ln |c| + \frac{A}{2} \sum_{z \in \mathbb{C}/\Lambda} \mathrm{ord}_z(g_\sigma) K_0(0, z - x, 1)$$

where we consider $1/|y|^2$ as $\lim_{s \downarrow 1}(1/|y|^{2s})$. Similarly,

$$\overline{d \ln f_\sigma(x)} = 2\frac{\partial}{\partial \overline{x}} (\ln |f_\sigma(x)|)\, d\overline{x} = -\sum_{z \in \mathbb{C}/\Lambda} \mathrm{ord}_z(f_\sigma) \overline{K_1(0, x - z, 1)}$$

and as for $\mathrm{Re}(s) > \frac{3}{2}$

$$\begin{aligned}
&\int_{\mathbb{C}/\Lambda} K_0(0, z_1 - x, s) \overline{K_1(0, x - z_2, s)} d\overline{x} \wedge dx \\
&\qquad = \int_{\mathbb{C}/\Lambda} \sum_{\substack{w,y \in \Lambda \\ w \neq 0 \neq y}} e^{\left((x(\overline{w+y}) - (w+y)\overline{x}) + (w\overline{z}_1 - z_1\overline{w}) + (y\overline{z}_2 - z_2\overline{y})\right)/A} \frac{y}{|wy|^s} d\overline{x} \wedge dx \\
&\qquad = 2\pi i A \sum_{\substack{y \in \Lambda \\ y \neq 0}} e^{(y(\overline{z_2 - z_1}) - (z_2 - z_1)\overline{y})/A} \frac{y}{|y|^{2s}}
\end{aligned}$$

so by analytic continuation

$$\pi i \int_{E_\sigma(\mathbb{C})} \ln |g_\sigma|\, \overline{d \ln f_\sigma} \wedge dx = (\pi A)^2 \sum_{z,w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f_\sigma) \mathrm{ord}_z(g_\sigma) \overline{K_1(0, z - w, 2)}$$

as required. □

The above proof is essentially the approach in [8] using the properties of E-K-L series to make it more explicit. For an alternate approach see [16].

Similarly, as

$$\left\langle r_\sigma\left(\sum_j \{f_j, g_j\}\right), d\overline{x} \right\rangle = \sum_j \pi i \int_{E_\sigma(\mathbb{C})} \ln |f_{j\sigma}|\, d \ln g_{j\sigma} \wedge d\overline{x}$$

we deduce that

$$\left\langle r_\sigma\left(\sum_j \{f_j, g_j\}\right), d\overline{x} \right\rangle = (\pi A)^2 \sum_j \sum_{z,w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f_{j\sigma}) \mathrm{ord}_z(g_{j\sigma}) K_1(0, z - w, 2)$$

In particular if σ is a real embedding $k \xrightarrow{\sigma} \mathbb{R} \to \mathbb{C}$, then E_σ will be a real curve, thus $\Lambda = \overline{\Lambda}$, also if x is a pole or zero of one of the $f_{j\sigma}$ or $g_{j\sigma}$ then $x \equiv \overline{x} \mod \Lambda$, and these two conditions imply that if $z - w$ is as in (2.14) then

$$K_1(0, z-w, 2) = \overline{K_1(0, z-w, 2)}$$

and so

$$\Big\langle r_\sigma\Big(\sum_j \{f_j, g_j\}\Big), dx\Big\rangle = \Big\langle r_\sigma\Big(\sum_j \{f_j, g_j\}\Big), \overline{dx}\Big\rangle$$

in this case.

Note that $\langle r_\sigma(\sum_j \{f_j, g_j\}), dx\rangle$ depends on the choice of scaling of lattice, namely it is proportional to the real period of the curve (i.e. $\int_{E(\mathbb{R})^\circ} dx$), so define

$$R_\sigma\Big(\sum_j \{f_j, g_j\}\Big) = \frac{\Big\langle r_\sigma\Big(\sum_j \{f_j, g_j\}\Big), dx\Big\rangle}{\int_{E(\mathbb{R})^\circ} dx}$$

Thus R_σ does not depend on the choice of scaling. If we identify $H^1(E_\sigma(\mathbb{C}), 2\pi i\mathbb{R})^+$ with $\mathbb{R}$ as we did above, then $R_\sigma = 2(\pi i)^2 r_\sigma$. Alternatively, if we consider $r_\sigma \in H^1(E_\sigma(\mathbb{C}), (\pi i)^{-1}\mathbb{R})^+$ then R_σ is the image of r_σ under the natural identification of $H^1(E_\sigma(\mathbb{C}), (\pi i)^{-1}\mathbb{R})^+$ to $\mathbb{R}$. If $k = \mathbb{Q}$ and σ is the natural embedding $\sigma\colon \mathbb{Q} \hookrightarrow \mathbb{C}$, then R_σ is the same as the regulator map of Bloch and Grayson [4], which they call M.

We are now able to define the regulator map. As you will by now have gathered, the choice of the constant in front of the regulator map doesn't seem to be universally agreed, so I will adopt the constant which most suits the problem in hand, which generalizes that of Bloch and Grayson.

Definition. For an elliptic curve E over a totally real number field k of dimension n over $\mathbb{Q}$, define the regulator map $R\colon \mathrm{K}_2(E_k)_\mathbb{Q} \to \mathbb{R}^n$ by

$$R\Big(\sum_j \{f_j, g_j\}\Big) = \left(R_{\sigma_1}\Big(\sum_j \{f_j, g_j\}\Big), \ldots, R_{\sigma_n}\Big(\sum_j \{f_j, g_j\}\Big)\right)$$

where $\sigma_1, \ldots, \sigma_n$ are all the real embeddings of $k \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$. We also denote by R the map $\mathrm{K}_2(E_{\mathcal{O}}) \to \mathbb{R}^n$ obtained by composing the map $\mathrm{K}_2(E_{\mathcal{O}}) \to \mathrm{K}_2(E_k)$ in equation (2.4) with R.

Note that we may also extend the definition of R to a map $\mathrm{K}_2(k(E)) \to \mathbb{R}^n$ by using either the integral expression (2.13) or the E-K-L series expression (2.14) for each $\langle r_\sigma(\sum_j \{f_j, g_j\}), dx \rangle$, since these are defined even if $\sum_j \{f_j, g_j\} \notin \mathrm{K}_2(E_k)$.

Now we can state the version of Beilinson's conjecture that we will verify.

Conjecture 2. *Let E be an elliptic curve over a totally real number field k of dimension n over $\mathbb{Q}$. Then $R(\mathrm{K}_2(E_{\mathcal{O}}))$ is a rank n lattice in $\mathbb{R}^n$, whose volume $\det(R(\mathrm{K}_2(E_{\mathcal{O}})))$ is a rational multiple of $L(E, 2)$.*

Chapter 3

The image of the regulator and results in the rational case

So far we have constructed the regulator map, and thus been able to state Beilinson's conjecture for the situation we are studying, which relates the image of $K_2(E_{\mathcal{O}})$ under the regulator map to the L-series. This chapter considers how this image is contained in the image of $K_2(E_k)$ under the regulator map, and what can be said about the rest of the image. This provides enough background to analyse my first set of results which extend the calculations of Bloch and Grayson, and so this chapter finishes with an analysis of those results. Most of the first two sections of this chapter is the natural generalization to totally real fields of material stated in outline in the paper by Bloch and Grayson [4], but may not have been written down before. Tony Scholl showed me how to prove Theorem 3.3 when we couldn't find a good reference.

3.1 E-K-L series and the image of the regulator map

In this section we will show that there is a $\mathbb{Q}$-vector space in $\mathbb{R}^n$ which is generated by vectors whose components are essentially E-K-L series evaluated at the points of a finite group $T \subset E$, and which is contained in the image under the regulator of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$. This will give us a vector space which has a spanning set that is easy to calculate and which may contain the image under the regulator of $\mathrm{K}_2(E_{\mathcal{O}})$. If it does then a consequence of Conjecture 2 is that $L(E,2)$ will be a rational combination of the determinants of n-tuples of the vectors corresponding to points of T. Thus we may test the conjecture by calculating these quantities.

Let k be a totally real number field of degree n over $\mathbb{Q}$, let $\sigma_1, \ldots, \sigma_n$ be the embeddings $k \hookrightarrow \mathbb{C}$ and let E be an elliptic curve over k. Recall we have the following extract of an exact sequence

$$\text{torsion} \to \mathrm{K}_2(E_k) \to \mathrm{K}_2(k(E)) \xrightarrow{\partial} \coprod_{\substack{P \in E_k \\ P \text{ closed}}} k(P)^* \to \ldots$$

and the regulator map $R\colon \ker \partial \to \mathbb{R}^n$, which can be extended to a map $R\colon k(E)^* \otimes k(E)^* \to \mathbb{R}^n$, and equally to a map $R\colon \mathrm{K}_2(E_k) \to \mathbb{R}^n$, since $R(f \otimes (1-f)) = \mathbf{0}$ for any $f \in k(E)$. Let T be a finite group of torsion points of E defined over k. Let $\mathcal{O}(E \setminus T)^* \subset k(E)$ denote the set of functions on E over k which only have poles and zeroes at points of T.

We start by showing that the image of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^* \subset k(E)^* \otimes k(E)^*$ under the regulator map is contained in the image of $\mathrm{K}_2(E_k)$. This is Bloch's lemma (see [5]).

Lemma 3.1. If $f, g \in \mathcal{O}(E \setminus T)^*$, and the number of elements in T is N, then there exist $h_j \in \mathcal{O}(E \setminus T)^*$, and $c_j \in k^*$ such that

$$N\{f,g\} + \sum_j \{h_j, c_j\} \in \ker \partial$$

Hence the image under the regulator map R of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ is contained in the image under R of the part of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$ generated by elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$.

Proof. If $P \notin T$ then $\partial_P(N\{f,g\} + \sum_j \{h_j, c_j\}) = 1$ for any $c_j \in k^*$ and any $h_j \in \mathcal{O}(E \setminus T)^*$, since none of the functions have any poles or zeroes at P. If $P \in T$ then

$$\partial_P(N\{f,g\}) = \left((-1)^{\mathrm{ord}_P(f)\mathrm{ord}_P(g)} \frac{f^{\mathrm{ord}_P(g)}}{g^{\mathrm{ord}_P(f)}}(P)\right)^N$$

So for each point $P \in T$ other than the origin, let h_P be the function with a zero of order N at P and a pole of order N at 0. Such a function exists in $k(E)$ because P is defined over k and the order of P divides N. Put

$$c_P = (-1)^{\mathrm{ord}_P(f)\mathrm{ord}_P(g)} \frac{f^{\mathrm{ord}_P(g)}}{g^{\mathrm{ord}_P(f)}}(P)$$

Then $\partial_P(N\{f,g\} + \sum_{Q \in T \setminus \{0\}} \{h_Q, c_Q\}) = 1$ for $P \in T \setminus \{0\}$, so it only remains to show that this is true at 0. But then

$$\partial_0 \left(N\{f,g\} + \sum_{Q \in T \setminus \{0\}} \{h_Q, c_Q\} \right) = \left(\prod_{Q \in T} (-1)^{\mathrm{ord}_Q(f)\mathrm{ord}_Q(g)} \frac{f^{\mathrm{ord}_Q(g)}}{g^{\mathrm{ord}_Q(f)}}(Q) \right)^N$$

and by the calculations in section 2.3 we know that for any embedding $k \overset{\sigma}{\hookrightarrow} \mathbb{C}$,

$$\ln \left(\prod_{Q \in T} (-1)^{\mathrm{ord}_Q(f)\mathrm{ord}_Q(g)} \frac{f^{\mathrm{ord}_Q(g)}}{g^{\mathrm{ord}_Q(f)}}(Q) \right)_\sigma = \left(\frac{\int_\gamma \ln f_\sigma d \ln g_\sigma - \ln(g_\sigma(\alpha)) \int_\gamma d \ln f_\sigma}{2\pi i} \right)$$

where γ is the boundary of any fundamental domain for $E_\sigma(\mathbb{C})$ which contains the images of the points of T under σ in its interior, and α is any point on γ. But the right hand side of this equation is zero because γ is the union of sides of a fundamental domain and these cancel. So $\partial_0 \left(N\{f,g\} + \sum_{Q \in T \setminus \{0\}} \{h_Q, c_Q\} \right) = 1$. So the first part of the lemma is proved. The rest is immediate consequence of the first part when you observe that $R(\{h_j, c_j\}) = \mathbf{0}$ for any $c_j \in k^*$ and any $h_j \in k(E)^*$. $\square$

Thus we have shown that the image under the regulator of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ is contained in that of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$. Now we establish what this image is in terms of E-K-L series.

Definition. For each point $P \in T$, define the vector $\mathbf{v}_P \in \mathbb{R}^n$, by setting its jth component to be

$$(\mathbf{v}_P)_j = \left(\pi A_{\sigma_j}\right)^2 \frac{K_1\left(0, P_{\sigma_j}, 2; E_{\sigma_j}(\mathbb{C})\right)}{\int_{E_{\sigma_j}(\mathbb{R})^\circ} dx}$$

where $K_1\left(0, P_{\sigma_j}, 2; E_{\sigma_j}(\mathbb{C})\right)$ is the E-K-L series $K_1(0, P_{\sigma_j}, 2)$ on the elliptic curve $E_{\sigma_j}(\mathbb{C})$, and A_{σ_j} is the constant A defined for the elliptic curve $E_{\sigma_j}(\mathbb{C})$ in Section 2.2.

Lemma 3.2. For each $P \in T$, there is an element of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ in $\ker \partial$ whose image under R is a rational multiple of $\mathbf{v}_P$. Hence the image of the part of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$ generated by elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ is the $\mathbb{Q}$-vector space in $\mathbb{R}^n$ generated by the vectors $\mathbf{v}_P$ for all $P \in T$.

Proof. First observe that for any elliptic curve, $K_1(0, x, 2) = -K_1(0, -x, 2)$, so for any $P \in T$, $\mathbf{v}_P = -\mathbf{v}_{-P}$. Thus $\mathbf{v}_P = \mathbf{0}$ if $P = 0$. Also $K_1(0, x, 2)$ is fixed under the addition to x of elements of the lattice of the elliptic curve, and so $\mathbf{v}_P = \mathbf{0}$ if P has order 2. So in these case $\mathbf{v}_P$ is the image of the identity.

Otherwise, let $h_P \in \mathcal{O}(E \setminus T)^*$ be a function with a zero of order $N = |T|$ at P and a pole of order N at the origin as in the previous lemma. Then

$$\begin{aligned} R(h_{-P} \otimes h_P) &= N^2(\mathbf{v}_{2P} - 2\mathbf{v}_P + \mathbf{v}_0) \\ &= N^2(\mathbf{v}_{2P} - 2\mathbf{v}_P) \end{aligned}$$

So if $P \in T$ has odd order $m > 1$, we can choose u such that $2^u \equiv 1 \mod m$, and then

$$\begin{aligned} R\left(\sum_{j=0}^{u-1} 2^{u-1-j}(h_{-2^jP} \otimes h_{2^jP})\right) &= N^2\left(\mathbf{v}_{2^uP} - 2^u\mathbf{v}_P\right) \\ &= N^2(1 - 2^u)\mathbf{v}_P \end{aligned}$$

so if $P \in T$ has odd order, there is an element of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ whose image under R is a multiple of $\mathbf{v}_P$ (note we have already done the case when P has order 1). If however $P \in T$ has order $2^w m$ where m is odd, then

$$R\left(\sum_{j=0}^{w-1} 2^{w-1-j}(h_{-2^j P} \otimes h_{2^j P})\right) = N^2\left(\mathbf{v}_{2^w P} - 2^w \mathbf{v}_P\right)$$

and since $2^w P$ has odd order, we already know that some multiple of $\mathbf{v}_{2^w P}$ is the image of an element of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ under R, thus the same is true of $\mathbf{v}_P$. Finally we multiply by N, and apply Lemma 3.1, to find an element in $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ and in $\ker \partial$, whose image under R is a multiple of $\mathbf{v}_P$ for each $P \in T$.

The second part follows because by the definition of R and equation (2.14), the jth component of the image under R of an element $(\sum_i f_i \otimes g_i) \in \mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ is given by

$$\begin{aligned}
&\left(R\Big(\sum_i f_i \otimes g_i\Big)\right)_j \\
&\quad = \frac{(\pi A_{\sigma_j})^2}{\int_{E_{\sigma_j}(\mathbb{R})^\circ} dx} \sum_i \sum_{P,Q \in T} \mathrm{ord}_{P_{\sigma_j}}(f_{i\sigma_j})\mathrm{ord}_{Q_{\sigma_j}}(g_{i\sigma_j}) K_1(0, Q_{\sigma_j} - P_{\sigma_j}, 2; E_{\sigma_j}(\mathbb{C})) \\
&\quad = \left(\sum_i \sum_{P,Q \in T} \mathrm{ord}_P(f_i)\mathrm{ord}_Q(g_i)\mathbf{v}_{Q-P}\right)_j
\end{aligned}$$

so

$$R\Big(\sum_i f_i \otimes g_i\Big) = \sum_{P,Q \in T} \left(\sum_i \mathrm{ord}_P(f_i)\mathrm{ord}_P(g_i)\right) \mathbf{v}_{Q-P} \tag{3.1}$$

and so $R(\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*)$ is contained in the space spanned by the $\mathbf{v}_P$ for $P \in T$, so the required result follows from the previous lemma. □

Thus the $\mathbb{Q}$ -vector space generated by the $\mathbf{v}_P$ is the image under R of the part of $\mathrm{K}_2(E_k)_\mathbb{Q}$ generated by symbols $\sum_i \{f_i, g_i\}$ where $f_i, g_i \in \mathcal{O}(E \setminus T)^*$. And if the image of $\mathrm{K}_2(E_\mathcal{O})$ in $\mathrm{K}_2(E_k)_\mathbb{Q}$ is contained in the part of $\mathrm{K}_2(E_k)_\mathbb{Q}$ generated by such symbols, then Beilinson's conjecture says that $L(E, 2)$ is a rational multiple of the

determinant of a matrix whose columns are rational combinations of the vectors $\mathbf{v}_P$ for $P \in T$. Thus to confirm the conjecture, we can look for linear relations over $\mathbb{Q}$ between $L(E,2)$, and a generating set for the determinants of matrices whose columns are the vectors $\mathbf{v}_P$.

However, we can get better information on when we are likely to get such a linear relation over $\mathbb{Q}$ by considering the exact sequence in equation (2.4), because this says that the torsion free part of $\mathrm{K}_2(E_k)$ is a combination of the image of $\mathrm{K}_2(E_{\mathcal{O}})$ and elements which are not killed by mapping into the $\mathrm{K}_1'(E_{\mathfrak{p}})$. We consider this map in the next section.

3.2 Split multiplicative reduction and the image of the regulator

Recall that the sequence

$$\mathrm{K}_2(E_{\mathcal{O}}) \to \mathrm{K}_2(E_k) \to \coprod_{\mathfrak{p} \text{ prime in } k} \mathrm{K}_1'(E_{\mathfrak{p}})$$

is exact at $\mathrm{K}_2(E_k)$. Denote by $\partial_{\mathfrak{p}}$ the corresponding map $\mathrm{K}_2(E_k) \to \mathrm{K}_1'(E_{\mathfrak{p}})$. We established in the last section that the image under the regulator map of the part of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$ generated by elements $\sum_j \{f_j, g_j\} \in \mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ is the space generated by vectors related to E-K-L series. In this section we will establish more information about this part of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$, and in particular when we can expect it to contain the image of $\mathrm{K}_2(E_{\mathcal{O}})$.

First we need to observe what the groups $\mathrm{K}_1'(E_{\mathfrak{p}})$ actually are. Clearly since we are only interested in the K-groups up to torsion, it is only the non-torsion part of $\mathrm{K}_1'(E_{\mathfrak{p}})$ which will interest us. It fact we have the following

Theorem 3.3. *The group $\mathrm{K}_1'(E_{\mathfrak{p}})$ is torsion unless E has split multiplicative reduction at $\mathfrak{p}$ in which case $\mathrm{K}_1'(E_{\mathfrak{p}})$ is isomorphic to $\mathbb{Z}$ upto torsion.*

Proof. By Soulé [22], $\mathrm{K}_1(E_\mathfrak{p}) = \mathrm{K}_1'(E_\mathfrak{p})$ is torsion if E has good reduction at $\mathfrak{p}$.

If E has additive reduction at $\mathfrak{p}$, we follow [8] which uses the devissage theorem of Quillen (see [23]) to deduce that $\mathrm{K}_1'(E_\mathfrak{p}) = \mathrm{K}_1'({E_\mathfrak{p}}^{red})$, where ${E_\mathfrak{p}}^{red}$ is the same as $E_\mathfrak{p}$ except all the fibres have multiplicity one. But then ${E_\mathfrak{p}}^{red} = X$ is a simply connected (or more precisely the corresponding graph is simply connected) union of copies of $\mathbb{P}^1$, and we use Theorem 2.2 with $U = \mathbb{A}^1(\mathbb{F})$ and $Z = X \setminus U$ to get the exact sequence

$$(\text{torsion}) = \mathrm{K}_2(\mathbb{A}^1(\mathbb{F})) \to \mathrm{K}_1'(Z) \to \mathrm{K}_1'(X) \to \mathrm{K}_1'(\mathbb{A}^1(\mathbb{F})) = (\text{torsion})$$

(where $\mathbb{F} = \mathcal{O}_k/\mathfrak{p}$) and thus deduce $\mathrm{K}_1'(Z) \cong \mathrm{K}_1'(X)$ up to torsion, and so by induction $\mathrm{K}_1'(E_\mathfrak{p})$ is isomorphic to K_1' of a point up to torsion and hence $\mathrm{K}_1'(E_\mathfrak{p})$ is also torsion.

If E has non-split multiplicative reduction at $\mathfrak{p}$, then $E_\mathfrak{p}$ is an M-gon which can be considered as the disjoint union of Z which is a simply connected union of copies of $\mathbb{P}^1$, and U which is the non-singular fibre of $E_\mathfrak{p}$ (which is a copy of $\mathbb{P}^1$) minus a closed point over $\mathbb{F}$ which consists of the union of two conjugate points over the quadratic extension of $\mathbb{F}$. Then by Theorem 2.2 again and by what we have shown above, we have the exact sequence

$$(\text{torsion}) = \mathrm{K}_1'(Z) \to \mathrm{K}_1'(E_\mathfrak{p}) \to \mathrm{K}_1'(U) = (\text{torsion})$$

and so $\mathrm{K}_1'(E_\mathfrak{p})$ is again torsion.

Finally if E has split multiplicative reduction at $\mathfrak{p}$, we see that $E_\mathfrak{p}$ is an M-gon which can be considered as the disjoint union of Z which is a simply connected union of copies of $\mathbb{P}^1$, and $U = \mathbb{G}_m$ which is $\mathbb{P}^1$ minus two points and so we have the sequence

$$(\text{torsion}) = \mathrm{K}_1'(Z) \to \mathrm{K}_1'(E_\mathfrak{p}) \to \mathrm{K}_1'(\mathbb{G}_m) \to \mathrm{K}_0'(Z) \hookrightarrow \mathrm{K}_0'(X)$$

but $\mathrm{K}_1'(\mathbb{G}_m) = K_1(\mathbb{G}_m) = \mathbb{F}[t, t^{-1}]^*$ is isomorphic to $\mathbb{Z}$ upto torsion, and therefore so also is $\mathrm{K}_1'(E_\mathfrak{p})$. $\square$

Moreover, if E has split multiplicative reduction at $\mathfrak{p}$ we know by [20] precisely what the map $\partial_{\mathfrak{p}}$ is. Recall (from [21] for example) that at a prime $\mathfrak{p}$ where $E_{\mathcal{O}}$ has split multiplicative reduction, the reduced curve $E_{\mathfrak{p}}$ consists of an M-gon of copies of $\mathbb{P}^1(\mathcal{O}_k/\mathfrak{p})$, where M is the least power of the prime ideal $\mathfrak{p}$ which contains the ideal generated by the discriminant of the curve $E_{\mathcal{O}}$, i.e. $M = \mathrm{ord}_{\mathfrak{p}}(\Delta)$. We associate the sides of this M-gon to $\mathbb{Z}/M\mathbb{Z}$, by associating the non-singular fibre, i.e. the side which contains the image of the identity ($[0 : 1 : 0]$ in projective coordinates) with zero, and numbering the sides consecutively from there. Then by [20],

Lemma 3.4. Let $\mathfrak{p}$ be a prime where $E_{\mathcal{O}}$ has split multiplicative reduction, let M be the number of fibres on the reduced curve $E_{\mathfrak{p}}$, and if $f \in \mathcal{O}(E \setminus T)^*$, let $d_\mu(f)$ be the sum of the orders of the zeroes minus the orders of the poles of f on the μth fibre, i.e. $d_\mu(f) = \sum_{P \in T \text{ on } \mu} \mathrm{ord}_P(f)$. Then if $\sum_j \{f_j, g_j\} \in \mathrm{K}_2(E_k)$ where $f_j, g_j \in \mathcal{O}(E \setminus T)^*$, the map $\partial_{\mathfrak{p}}$ is given by

$$\partial_{\mathfrak{p}}\Big(\sum_j \{f_j, g_j\}\Big) = \pm \frac{1}{3M} \sum_{\mu,\nu=0}^{M-1} \left(\sum_j d_\mu(f_j) d_\nu(g_j) \right) \mathbf{B}_3\left(\left\langle \frac{\nu - \mu}{M} \right\rangle \right) \Phi^1_{1\mathfrak{p}} \tag{3.2}$$

where $\Phi^1_{1\mathfrak{p}}$ is a fixed generator of $\mathrm{K}'_1(E_{\mathfrak{p}})_{\mathbb{Q}}$, $\langle x \rangle$ is the fractional part of x, (i.e. $0 \leq \langle x \rangle < 1$ and $x - \langle x \rangle \in \mathbb{Z}$) and $\mathbf{B}_3(x)$ is the third Bernoulli polynomial, $\mathbf{B}_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x$.

Note that an immediate consequence of this is that if $M = 1$ or 2 or all the points of T are on the 0th or $(M/2)$th fibres, then the image of $\partial_{\mathfrak{p}}$ is zero, since $\mathbf{B}_3(0) = \mathbf{B}_3(1/2) = \mathbf{B}_3(1) = 0$.

Thus we know that the image of the part of $\mathrm{K}_2(E_k)$ generated by the elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ under the map $\partial_{\mathfrak{p}}$ is non-trivial if E has split multiplicative reduction at $\mathfrak{p}$ and the points of T map onto at least 3 different fibres. So if we label the prime ideals with such reduction $\mathfrak{p}_j$, then we can consider the image of this part of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$ under the combined map $\coprod_{\mathfrak{p} \text{ prime}} \partial_{\mathfrak{p}}$ as a $\mathbb{Q}$ -vector space, with a basis consisting of the $\Phi^1_{1\mathfrak{p}_j}$.

But now observe that because of the similarly between the regulator map as in equation (3.1) and the map $\partial_{\mathfrak{p}_j}$ as in equation (3.2), we deduce that

Lemma 3.5. If $v = \sum_{P\in T} a_P \mathbf{v}_P \in \mathbb{R}^n$ with $a_P \in \mathbb{Q}$, then there is an element z in the part of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$ generated by elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ with $R(z) = v$ and

$$\partial_{\mathfrak{p}_j}(z) = \pm\frac{1}{3M_j}\sum_{\mu=0}^{M_j-1}\Big(\sum_{\substack{P\in T\\ P \text{ on } \mu}} a_P\Big)\mathbf{B}_3\Big(\frac{\mu}{M_j}\Big)\Phi^1_{1\mathfrak{p}_j}$$

Proof. By Lemma 3.2 there is an element $z = c\sum_i\{f_i, g_i\} \in \mathrm{K}_2(E_k)_{\mathbb{Q}}$ with $c \in \mathbb{Q}$ and $f_i, g_i \in \mathcal{O}(E \setminus T)^*$, such that $R(z) = v$. Thus

$$a_P = c\sum_{Q\in T}\Big(\sum_i \mathrm{ord}_{Q-P}(f_i)\mathrm{ord}_Q(g_i)\Big)$$

However the coefficient of the term in $\pm\frac{1}{3M_j}\mathbf{B}_3\big(\frac{\mu}{M_j}\big)\Phi^1_{1\mathfrak{p}_j}$ of $\partial_{\mathfrak{p}_j}(z)$ is

$$\begin{aligned} c\sum_{\nu=0}^{M-1}\Big(\sum_i d_{\nu-\mu}(f_i)d_\nu(g_i)\Big) &= c\sum_{\nu=0}^{M-1}\sum_i\Big(\sum_{\substack{Q\in T\\ Q \text{ on } \nu-\mu}}\mathrm{ord}_Q(f_i)\Big)\Big(\sum_{\substack{Q\in T\\ Q \text{ on } \nu}}\mathrm{ord}_Q(g_i)\Big)\\ &= c\sum_{\substack{P\in T\\ P \text{ on } \mu}}\sum_{Q\in T}\Big(\sum_i \mathrm{ord}_{Q-P}(f_i)\mathrm{ord}_Q(g_i)\Big) = \sum_{\substack{P\in T\\ P \text{ on } \mu}} a_P \end{aligned}$$

as required. □

In particular, if we take one $a_P = 1$ and all the rest zero, then there is an element of the part of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$ generated by elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$, whose image under the combined map $\coprod_{\mathfrak{p}\text{ prime}}\partial_{\mathfrak{p}}$ is the vector whose jth component is

$$\pm\frac{1}{3M_j}\mathbf{B}(\mu_{P,j}/M_j)$$

where P is on the $\mu_{P,j}$th fibre on the M_j-gon which is the curve $E_{\mathfrak{p}_j}$. And it is clear that the image of this part of $\mathrm{K}_2(E_k)_{\mathbb{Q}}$ under the map $\coprod_{\mathfrak{p}\text{ prime}}\partial_{\mathfrak{p}}$ is spanned by these vectors. So

Theorem 3.6. *The dimension of the image of the part of* $\mathrm{K}_2(E_k)_{\mathbb{Q}}$ *generated by the elements of* $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ *under the map* $\coprod_{\mathfrak{p}\ prime} \partial_{\mathfrak{p}}$ *is the rank of the matrix whose* (i,j)*th entry is* $\mathbf{B}(\mu_{P,j}/M_j)$*, where* P *is the* i*th point of* T*, and* P *is on the* $\mu_{P,j}$*th fibre on the* M_j*-gon of the curve* $E_{\mathfrak{p}_j}$*.*

Proof. This is immediate from the previous discussion because the image is generated by vectors with components $\pm 1/(3M_j)\mathbf{B}(\mu_{P,j}/M_j)$, and all we do is form a matrix with these columns and cancel the common factor $\pm 1/(3M_j)$ from each row (noting the choice of $+/-$ is consistent). □

Clearly each column of this matrix which corresponds to a point of order 1 or 2 is $\mathbf{0}$. Also if a point P is mapped onto fibre μ on an M-gon, then $-P$ is mapped onto fibre $M-\mu$, and as $\mathbf{B}_3(\mu/M) = -\mathbf{B}_3((M-\mu)/M)$, the column corresponding to P is -1 times the column corresponding to $-P$. So we may reduce to the case where we have one column for each pair of points $P, -P$ where $P \neq -P$. Let m be the number of such pairs of points. It so happens that m is also the maximum number of different rows obtainable up to sign, and the set of possible rows is linearly independent. (It is easy to verify this for all the groups T which occur in my results, for example if $T = C_7$, then the possible rows for the matrix are up to multiplication by a constant $(5,5,2)$, $(5,-2,-5)$ and $(2,-5,5)$, which are linearly independent. See Table 3.1 for all the relevant Bernoulli numbers).

So if we consider two reductions the same if they give rise the the same row up to sign, then the rank of the matrix is the number of distinct reductions. Let this number be m'. Note that for the reductions at prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ to be the same, it is not necessary that $M_1 = M_2$, merely that the number of fibres which contain points of T for each reduction must be the same, and also we must either have $\mu_{P,1}/M_1 = \mu_{P,2}/M_2$ for each point $P \in T$, or $\mu_{P,1}/M_1 = -\mu_{P,2}/M_2$ for each point $P \in T$.

So the image of the part of $K_2(E_k)_{\mathbb{Q}}$ generated by elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ under $\coprod_{\mathfrak{p}\ \mathrm{prime}} \partial_{\mathfrak{p}}$ has rank m' equal to the number of different split

multiplicative reductions where the elements of T map onto at least 3 different fibres.

But the sequence

$$\mathrm{K}_2(E_{\mathcal{O}}) \to \mathrm{K}_2(E_k) \xrightarrow{\coprod_{\mathfrak{p} \text{ prime}} \partial_{\mathfrak{p}}} \coprod_{\mathfrak{p} \text{ prime in } k} \mathrm{K}_1'(E_{\mathfrak{p}})$$

is exact at $\mathrm{K}_2(E_k)$, thus an element of $\mathrm{K}_2(E_k)$ is the image of an element of $\mathrm{K}_2(E_{\mathcal{O}})$ if it is mapped to $\mathbf{0}$ by $\coprod_{\mathfrak{p} \text{ prime}} \partial_{\mathfrak{p}}$. And thus, by Lemma 3.5, the image in $\mathbb{R}^n$ under the regulator R of elements of the part of $\mathrm{K}_2(E_k)$ generated by symbols $\sum_i \{f_i, g_i\}$ where $f_i, g_i \in \mathcal{O}(E \setminus T)^*$ which are the image of elements of $\mathrm{K}_2(E_{\mathcal{O}})$, consists of those elements

$$(3.3) \quad \sum_{P \in T} a_P \mathbf{v}_P \in \mathbb{R}^n \quad \text{such that} \quad \sum_{\mu=0}^{M_j-1} \Big(\sum_{\substack{P \in T \\ P \text{ on } \mu}} a_P \Big) \mathbf{B}_3\Big(\frac{\mu}{M_j}\Big) = 0 \quad \text{for each } j$$

This imposes m' independent linear conditions on the $\mathbf{v}_P$, for elements in the image of $\mathrm{K}_2(E_{\mathcal{O}})$. But since $\mathbf{v}_P = 0$ if P has order 1 or 2, and $\mathbf{v}_P = -\mathbf{v}_{-P}$ otherwise, this means that the dimension of the space spanned by the $\mathbf{v}_P$ is at most m. Thus the dimension of the image of $\mathrm{K}_2(E_{\mathcal{O}})$ under the regulator map is at most $m - m'$. So in summary we have

Theorem 3.7. *If m is the number of pairs of points $P, -P \in T$ where $P \neq -P$, and m' is the rank of the matrix in Theorem 3.6, then the dimension of the image of the regulator of the part of $\mathrm{K}_2(E_{\mathcal{O}})$ corresponding to elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ in $\mathrm{K}_2(E_k)$ is equal to $m - m'$ minus the number of additional linear relations which are independent of the equations (3.3) taken together with the simple relations on the $\mathbf{v}_P$ (i.e. $\mathbf{v}_P = 0$ if P has order 1 or 2 and $\mathbf{v}_P = -\mathbf{v}_{-P}$).*

If this dimension is equal to n then this should determine $L(E, 2)$ precisely in terms of determinants consisting of E-K-L series.

3.3 Analysis of results over the rational numbers

As a warm up for the case of real quadratic fields, I first tested the above theory on rational curves for all the elliptic curves in Cremona's tables [7] with sufficient torsion, extending the results of Bloch and Grayson [4]. Their results essentially cover the elliptic curves with a single real component and conductor less than 200, though they don't cover all such curves with 3 or 4 torsion points, and they only claim that the linear dependencies are correct to 25 decimal places, whereas my results are correct to about 70 decimal places. The full tables of such results are given in Appendix A, but here I will summarize the main features of the tables. Note that each curve is labelled by Cremona's system, that is the label for each curve consists of the conductor, a letter indicating its isogeny class, and another number to distinguish curves within the isogeny class with the curve 1 being the strong Weil curve. For curves with conductor less than 200 this is followed by a letter in brackets indicating the label of the curve in Swinnerton-Dyer's tables [24] in the Antwerp proceedings. For example 11A1(B) corresponds to the curve 11B in those tables, and is the strong Weil curve. Also I have labelled the rational points by the corresponding point on the natural fundamental domain when the curve is considered as a quotient $\mathbb{C}/\Lambda$ with Λ scaled so that the real period of the curve is 1. Thus Λ is generated by 1 and τ, and the rational points are of the form $\frac{x}{y}$ or $\frac{x}{y}+\frac{1}{2}\tau$.

The tables tabulate the linear dependencies between the product of the conductor N and $L(E,2)$, and the $\mathbf{v}_P = (\pi \mathrm{Im}\tau)^2 K_1(0,P,2)$ for the rational points $P \in T$, bearing in mind that $\mathbf{v}_P = -\mathbf{v}_{-P}$. I consider $NL(E,2)$ rather than $L(E,2)$ because I found (as did Bloch and Grayson) that in all cases there is a linear combination of the $\mathbf{v}_P$ which is equal to N times $L(E,2)$ up to a few small factors. Thus I presented the table to take account of this, and show up more clearly when there are any extra factors.

My results appear to agree entirely with those of Bloch and Grayson except

that their table assumes that curve 15A4(F) has 4 torsion points when it actually has 8.

The tables also show that in every case, the number of distinct split multiplicative reductions m' plus the dimension of the part of the image of $\mathrm{K}_2(E_{\mathbb{Z}})$ in the space spanned by the $\mathbf{v}_P$ is equal to the dimension of the space spanned by the $\mathbf{v}_P$. This shows that there are no elements in $\mathrm{K}_2(E_{\mathbb{Q}})$ generated by symbols $\sum_i \{f_i, g_i\}$ where $f_i, g_i \in \mathcal{O}(E \setminus T)^*$ which map to a non-torsion element under $\coprod_{p \text{ prime}} \partial_p$ but map to zero (up to torsion) under R. In other words R is injective on the part of $\mathrm{K}_2(E_{\mathbb{Q}})$ we considered modulo $\ker \coprod_{p \text{ prime}} \partial_p$ up to torsion, or alternatively $\coprod_{p \text{ prime}} \partial_p$ factors through R (up to torsion) for the part of $\mathrm{K}_2(E_{\mathbb{Q}})$ we considered.

One can also check that the linear dependencies in the tables satisfy appropriate linear conditions imposed at primes with split multiplicative reduction, that is they are perpendicular to the appropriate permutation of Bernoulli numbers, which are given in Table 3.1. I have in fact checked that all the dependencies are perpendicular to the appropriate number of Bernoulli relations, though not that these relations are in fact the correct relations.

	x	$\frac{1}{\cdot}$	$\frac{2}{\cdot}$	$\frac{3}{\cdot}$	$\frac{4}{\cdot}$	$\frac{5}{\cdot}$	$\frac{6}{\cdot}$	$\frac{7}{\cdot}$
$\frac{\cdot}{3}$	$\frac{1}{27}$	1						
$\frac{\cdot}{4}$	$\frac{3}{64}$	1	0					
$\frac{\cdot}{5}$	$\frac{3}{125}$	2	1					
$\frac{\cdot}{6}$	$\frac{1}{108}$	5	4	0				
$\frac{\cdot}{7}$	$\frac{3}{343}$	5	5	2				
$\frac{\cdot}{8}$	$\frac{3}{512}$	7	8	5	0			
$\frac{\cdot}{9}$	$\frac{1}{729}$	28	35	27	10			
$\frac{\cdot}{10}$	$\frac{3}{500}$	6	8	7	4	0		
$\frac{\cdot}{12}$	$\frac{1}{1728}$	55	80	81	64	35	0	
$\frac{\cdot}{15}$	$\frac{1}{3375}$	91	143	162	154	125	81	28

Table 3.1: Bernoulli numbers $\mathbf{B}_3(\cdot)/x$

Also, in almost every case where there are few enough relations imposed by split

multiplicative reductions (i.e. $m' \leq |T|-1$) so that we would expect some relations between the v_P and $L(E,2)$, there is in fact such a relation. The exceptions are the curves 27A3(A), 108A1(A), 225B1, 243A2, 243B1, 441B1, 675C1, 900C1, 972A2, 972B2, 972C1 and 972D1, which each have $K_1(0,\frac{1}{3},2) = 0$ when the curves are normalized so that the real period is 1. In fact after normalization these curves are the same and each have $\tau = 1/2 + i/(2\sqrt{3})$ (as does 36A1(A), but in that case the point of order 6 gives an E-K-L series related to the L-series). In particular, if we put $\omega = \frac{1}{2} + \frac{i\sqrt{3}}{2}$, this means that they all have complex multiplication by $\mathbb{Z}[\omega]$. A consequence of this is that for this value of τ, the E-K-L series is zero at the point $\frac{1}{3}$ is because it lies on a symmetry of the lattice Λ, in other words, the set $\frac{1}{3} + \Lambda$ is fixed when the lattice is rotated by $2\pi/3$ radians. But this rotation corresponds to multiplying the E-K-L series by $\bar{\omega}$. By the same sort of argument we can show that the corresponding elements in $\mathrm{K}_2(E_{\mathbb{Q}})$ and in $\mathrm{K}_2(\mathbb{Q}(E))$ are zero. For example, if $f \in \mathbb{Q}(E)$ has a pole of order 3 at zero, and a zero of order 3 at $1/3$, and $g \in \mathbb{Q}(E)$ has a pole of order 2 at zero and zeroes of order 1 at $1/3$ and $2/3$, then $f(z) \otimes g(z) = f(\omega z) \otimes g(\omega z)$ by symmetry. However, from K-theory you can show that for any functions $f, g \in \mathbb{Q}(E)$ $f(\omega z) \otimes g(\omega z) = \omega f(z) \otimes g(z)$, so the symbol $f(z) \otimes g(z) = 0$. Thus the E-K-L series is zero because the part of $K_2(E_{\mathbb{Q}})$ generated by elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ is zero.

Thus the tables of results suggest that R is injective on the part of $K_2(E_{\mathbb{Q}})$ generated by elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ because R is injective on the part which is not killed by $\coprod_{p \text{ prime}} \partial_p$, and also the image of R has the largest possible dimension, given the restrictions explained above. The only way R might not be injective in the cases calculated would be if there were some element of $K_2(E_{\mathbb{Z}})$ whose image in $K_2(E_{\mathbb{Q}})$ was not a torsion element, but which was killed the regulator map, which would incidentally contradict Beilinson's conjecture. But it should be possible to check that no such element exists on the part of $K_2(E_{\mathbb{Q}})$ considered by calculating its dimension.

We have already observed that a linear combination of the E-K-L series seems to be a rational multiple of the conductor times $L(E,2)$. Now we move on to consider these linear combinations more closely. It is easy to check that each entry in the table lies on appropriate planes given by Bernoulli numbers. Also, in almost all cases, the linear combinations of the E-K-L series have a common factor which is the number of torsion points $|T|$ (Bloch and Grayson also observed this). Thus we have equations of the form

$$c_1 |T| \sum_{P \in T} a_P K_1(0,P,2) + c_2 N L(E,2) = 0$$

where the a_P are coprime numbers which satisfy the appropriate equations with Bernoulli numbers, and c_1, c_2 are coprime integers. Note that when there are linear dependencies between the E-K-L series, there is some choice over what values the coefficients a_P take and in the tables I have chosen the values which minimize c_2 and maximize c_1.

The tables show that $c_2 = 1$ in almost all cases. The exceptions are given in Table 3.2 following. The tables suggest that the normal value of c_1 is $c_1 = 2^?$ if

Curve	50A1(E)	15A7(D)	42A4(D)	63A5(F)	99B1(H)
Torsion group	C_3	C_4	C_4	C_4	C_4
c_2	5	11	3	7	3
Curve	11A1(B)	57C1(F)	14A1(C)	14A2(D)	30A4(D)
Torsion group	C_5	C_5	C_6	C_6	C_6
c_2	25	3	3	6	3
Curve	30A5(E)	34A1(A)	34A2(B)	90C8(K)	210E4
Torsion group	C_6	C_6	C_6	C_6	C_8
c_2	5	3	3	3	3
Curve	54B3(B)	90C3(G)	15A1(C)	42A1(B)	90C6(J)
Torsion group	C_9	C_{12}	$C_4 \times C_2$	$C_4 \times C_2$	$C_6 \times C_2$
c_2	3	3	3	3	3

Table 3.2: Exceptional values of c_2

$|T|$ is a power of 2 (and possibly this case should be extended to include all cases

where $|T|$ is not a multiple of 3, though the evidence from the tables is less clear), and $c_1 = 2^?3^?$ otherwise. The exceptions to this are given in Table 3.3.

Curve	605B1	690K1	690K2	891F1	973B1	550K3	606F1
Torsion group	C_4	C_8	$C_4 \times C_2$	C_3	C_3	C_5	C_5
c_1	2^43	2^23	2^33	2^23^25	2^23^15	2^25	2^211

Table 3.3: Exceptional values of c_1

The cases where c_2 is not 1, would be explained if the part of $K_2(E_{\mathbb{Q}})$ generated by elements of $\mathcal{O}(E \setminus T)^* \otimes \mathcal{O}(E \setminus T)^*$ was a subgroup of the full group $K_2(E_{\mathbb{Q}})$ of index c_2, and thus our method of calculation would be missing elements of $K_2(E_{\mathbb{Q}})$ whose image under R would correspond to $L(E,2)$, and not a multiple of it. So it is probable that nothing exciting is going on in these cases.

If c_1 is not 1, this suggests that there are elements of the part of $K_2(E_{\mathbb{Q}})$ we are studying which are not in the image of $K_2(E_{\mathbb{Z}})$ but some finite multiple of these elements is. Such elements would map under $\coprod_{p \text{ prime}} \partial_p$ to the torsion part of $\coprod_{\mathfrak{p} \text{ prime in } k} \mathrm{K}_1'(E_{\mathfrak{p}})$, which presumably correspond to primes with additive or non-split multiplicative reduction. And indeed there seems to be some correlation between the factors of 2 and 3 in c_1 and such reduction. However it is harder to explain the bigger factors, particularly since the corresponding curves do not seem to have any exceptional types of reduction. Any unexplainable factors would be analogous to the group Ш in the Birch-Swinnerton Dyer conjecture. It is also worth noting that exceptional values of c_2 occur for small values of the conductor, and exceptional values of c_1 occur for larger values of the conductor.

Before we can repeat these calculations for real quadratic fields, we must work out how to calculate the L-series of an elliptic curve over a real quadratic field, and this is the subject of the next chapter.

Chapter 4

Calculating L-series

It seems that the easiest way to calculate the L-series of an elliptic curve over a real quadratic field effectively is to assume that the curve corresponds to a Hilbert modular form, use this to calculate the L-series at a particular value, and then check numerically that the assumption is almost certainly valid.

So the first section will describe what a Hilbert modular form is, define its L-series, and explain how this might correspond to the the L-series of an elliptic curve. For simplicity it will assume we are working over a totally real field of narrow class number one.

The next section will establish practical formulae for calculating the L-series of an elliptic curve under the assumption that it corresponds to the L-series of a Hilbert modular form, and explain how these can be used to verify the assumption numerically. As these formulae are infinite sums, it will also give a bound for the error caused by ignoring all sufficiently small terms, and thus show which terms need to be calculated to achieve a given accuracy.

The final section will explain how to implement these calculations.

But first we establish some notation that will be used frequently in this chapter. Let k be a totally real number field of degree n over $\mathbb{Q}$. There are n distinct embeddings $k \hookrightarrow \mathbb{R}$ which we will denote by $i_1, \ldots, i_n$. If we are working over a

real quadratic field and if $\nu \in k$, it will often be convenient to abbreviate $i_1(\nu)$ by ν_1 or even just ν, and $i_2(\nu)$ by ν_2 or $\overline{\nu}$, depending on the circumstances.

Let $\mathfrak{h} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$ be the upper half plane. We will often be doing arithmetic with a combination of vectors in $\mathbb{R}^n$ or $\mathfrak{h}^n$ and of elements of k, in which case we will identify an element $\nu \in k$ with the vector $\{i_1(\nu), \ldots, i_n(\nu)\}$. Moreover it is convenient to define multiplication and division of such vectors to be the vectors obtained by multiplying and dividing componentwise. Thus for example if $a, b, c, d \in k$ and $\mathbf{z} \in \mathfrak{h}^n$ then we take $\dfrac{a\mathbf{z} + b}{c\mathbf{z} + d}$ to be the vector whose jth component is $\dfrac{i_j(a)z_j + i_j(b)}{i_j(c)z_j + i_j(d)}$.

We will also use the standard trace and norm functions interchangeably on ideals in k and on vectors in $\mathbb{R}^n$ and $\mathfrak{h}^n$. So for example, $\operatorname{Tr}(a\mathbf{z}) = \sum_{j=1}^n i_j(a)z_j$ and $\mathbf{N}(a\mathbf{z}) = \prod_{j=1}^n i_j(a)z_j = \mathbf{N}((a))\mathbf{N}(\mathbf{z})$. It is also convenient to take $\mathbf{N}(d\mathbf{y})$ to mean $dy_1 \ldots dy_n$.

4.1 Hilbert modular forms

Hilbert modular forms are a natural generalization of modular forms over $\mathbb{Q}$ to totally real number fields, and many of the properties of modular forms generalize directly to Hilbert modular forms. We start by constructing the space over which Hilbert modular forms are defined. (Most of this section is stongly based on the first chapter of the book by van der Geer [26]).

Definition. An element $x \in k$ is **totally positive** (written $x \gg 0$) if $i_j(x) > 0$ for all $1 \leq j \leq n$.

Let $\mathrm{GL}_2^+(k)$ denote the group of non-singular 2 by 2 matrices over k with totally positive determinant, and $\mathrm{GL}_2^+(\mathbb{R})$ denote the 2 by 2 matrices over $\mathbb{R}$ with strictly positive determinant. Each embedding i_j extends in a natural way to an embedding $\mathrm{GL}_2^+(k) \hookrightarrow \mathrm{GL}_2^+(\mathbb{R})$ which we will also call i_j, i.e. i_j: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} i_j(a) & i_j(b) \\ i_j(c) & i_j(d) \end{pmatrix}$.

Now $GL_2^+(\mathbb{R})$ acts on $\mathfrak{h}$ by fractional linear transformations, that is, if $z \in \mathfrak{h}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{R})$ then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \dfrac{az+b}{cz+d}$. Hence we can make $A \in \mathrm{GL}_2^+(k)$ act on $\mathfrak{h}^n$ by letting $i_j(A)$ act on the jth coordinate of $\mathfrak{h}^n$ for each j. That is, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(k)$ and $\mathbf{z} \in \mathfrak{h}^n$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mathbf{z} = \dfrac{a\mathbf{z}+b}{c\mathbf{z}+d}$ and this is in $\mathfrak{h}^n$ because $ad - bc \gg 0$. Note that scalar matrices in $\mathrm{GL}_2^+(\mathbb{R})$ fix $\mathfrak{h}$, so scalar matrices in $\mathrm{GL}_2^+(k)$ fix $\mathfrak{h}^n$. Thus the action of $\mathrm{PGL}_2^+(k)$ on $\mathfrak{h}^n$ is the same as that of $\mathrm{GL}_2^+(k)$.

The reason for such a construction is that discrete subgroups of $\mathrm{PGL}_2^+(k)$, in particular $\mathrm{PSL}_2(\mathcal{O}_k)$ and related groups, act on $\mathfrak{h}^n$ properly discontinuously, thus the resulting quotient will be a manifold (and in fact an algebraic variety in the cases we will consider), except that a finite number of points corresponding to points on the boundary of $\mathfrak{h}^n$ need to be added on, and there are also a finite number of cosets of points on $\mathfrak{h}^n$ which are fixed by non-trivial elements of the group, and these correspond to finitely many branch points on the quotient, so local charts in neighbourhoods about such points on the quotient need to be replaced for the quotient to be a manifold. We now focus on such groups.

Definition. Two groups are **commensurable** if they have a common subgroup, which has finite index in each group.

Fix a group Γ which is a subgroup of $\mathrm{PGL}_2^+(k)$ commensurable with $\mathrm{PSL}_2(\mathcal{O}_k)$. This means that Γ acts on $\mathfrak{h}^n$ properly discontinuously. Γ also acts on $\mathbb{P}^1(k)$ by letting an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ map $(e:f) \in \mathbb{P}^1(k)$ to $(ae+bf : ce+df)$. Observe that an element $(e:f) \in \mathbb{P}^1(k)$ can be identified with the point on the boundary of $\mathfrak{h}^n$ given by $(i_1\left(\frac{e}{f}\right), \ldots, i_n\left(\frac{e}{f}\right))$, with the exception of $(1:0)$ which may be identified with the point given by $\lim_{y\to\infty}(iy, \ldots, iy)$, and the action of Γ is preserved by this identification in the sense that if a series of points in $\mathfrak{h}^n$ tend to the point on the boundary of $\mathfrak{h}^n$ associated to an element of $\mathbb{P}^1(k)$, then the image under Γ of these points tend to the point on the boundary identified with the image under Γ of the

element in $\mathbb{P}^1(k)$.

Definition. The **cusps** of Γ are the orbits of Γ when acting on $\mathbb{P}^1(k)$.

The cusps of Γ are the points mentioned above on the boundary of $\mathfrak{h}^n$ which are missing from the quotient $\Gamma\backslash\mathfrak{h}^n$.

Now note that any element $(e : f) \in \mathbb{P}^1(k)$ is the image of $(1 : 0)$ when acted on by $\begin{pmatrix} e & e^* \\ f & f^* \end{pmatrix} \in \mathrm{SL}_2(k)$, where $ef^* - fe^* = 1$ and $e^*, f^* \in (e, f)^{-1}$ ($(e, f)^{-1}$ isthe ideal inverse of the ideal generated by e and f). This can be used to deduce which elements of $\mathbb{P}^1(k)$ are equivalent under the action of Γ, by considering the product of a matrix of this form with the inverse of a different matrix of this form, and considering when the matrices can be choosen so that the product gives a matrix in Γ. For example, if $\Gamma = \mathrm{PSL}_2(\mathcal{O}_k)$, then we deduce that the cusps of Γ are in one to one correspondence with the elements of $Cl(k)$, the class group of k. The correspondence is given by associating an element $(e : f) \in \mathbb{P}^1(k)$, where e and f can be assumed to be algebraic integers, with the ideal class containing (e, f).

Also, it is often easier to study the action of Γ on a cusp, represented by $(e : f)$ say, by looking at the action of $\begin{pmatrix} e & e^* \\ f & f^* \end{pmatrix} \Gamma \begin{pmatrix} e & e^* \\ f & f^* \end{pmatrix}^{-1}$ on $(1 : 0)$. This is because if γ maps $(1 : 0)$ to itself, then $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, for some $a, b, d \in k$. The action of Γ at the cusp $(1 : 0)$ is essentially determined by the two groups we are about to define, and which we will refer to later. Define $M = \left\{ \frac{b}{a} \;\middle|\; \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \Gamma \right\}$ and $V = \left\{ \frac{a}{d} \;\middle|\; \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \Gamma \right\}$.

For each Γ, V is a multiplicative group, and since Γ is commensurable with $\mathrm{PSL}_2(\mathcal{O}_k)$, V is commensurable with U_k^+, the totally positive units of $\mathcal{O}_k$. But each element of V must be totally positive, and some finite power of this element must be a unit, so it is itself a totally positive unit and $V \subset U_k^+$. Also, M is a free

$\mathbb{Z}$ -module of rank n, commensurable as an additive group with $\mathcal{O}_k$, and acted on by sums of elements of V. Usually, M will be a fractional k-ideal.

Definition. A **Hilbert modular form** of weight $\mathbf{k} = (k_1, \ldots, k_n) \in \mathbb{Z}^n$ on Γ is a holomorphic function $f\colon \mathfrak{h}^n \to \mathbb{C}$, such that $f|_{\mathbf{k}}\gamma = f \ \forall \gamma \in \Gamma$, where for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(k)$,

$$(f|_{\mathbf{k}}\gamma)(\mathbf{z}) = \left(\prod_{j=1}^{n} \frac{i_j(\det\gamma)^{k_j/2}}{(i_j(c)z_j + i_j(d))^{k_j}}\right) f(\gamma\mathbf{z})$$

If $\gamma = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ then $(f|_{\mathbf{k}}\gamma)(\mathbf{z}) = f(\mathbf{z} + \frac{b}{a})$, so we can write f as the Fourier expansion about $(1:0)$,

$$f(\mathbf{z}) = \sum_{\nu \in M^\vee} a_\nu e^{2\pi i \operatorname{Tr}(\nu\mathbf{z})}$$

where $M^\vee = \{\lambda \in k \mid \operatorname{Tr}(\lambda\mu) \in \mathbb{Z} \quad \forall \mu \in M\}$. Thus M is related to the Fourier expansion of f at $(1:0)$.

If $\mathbf{k} = (l, \ldots, l)$, the expression for $(f|_{\mathbf{k}}\gamma)(\mathbf{z})$ simplifies to

$$(f|_{\mathbf{k}}\gamma)(\mathbf{z}) = \left(\frac{\mathbf{N}(\det\gamma)^{l/2}}{\mathbf{N}(c\mathbf{z} + d)^l}\right) f(\gamma\mathbf{z})$$

But in this case, if $\gamma = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ then $(f|_{\mathbf{k}}\gamma)(\mathbf{z}) = f(\frac{a}{d}\mathbf{z})$, so if $\epsilon \in V$, $f(\epsilon\mathbf{z}) = f(\mathbf{z})$, and hence $a_{\epsilon\nu} = a_\nu$ by equating expansions. (For general $\mathbf{k}$, $a_{\epsilon\nu} = ca_\nu$ for some positive c depending on ϵ but not ν). Thus V is the group of elements of k which fix f.

If we assume $n \neq 1$, a consequence of this action of V is that if $\nu \in M^\vee$ is not totally positive and non-zero, then $a_\nu = 0$. If this were not true, say $a_\nu \neq 0$ where $i_j(\nu) < 0$, then we could choose a unit $\epsilon \in V$ with $i_j(\epsilon) > 1$ and $i_m(\epsilon) < 1$ for $m \neq j$, and then $\operatorname{Re}\left(a_{\epsilon^m\nu} e^{2\pi i \operatorname{Tr}(\epsilon^m\nu\mathbf{z})}\right) \to \infty$ as $m \to \infty$ for any $\mathbf{z} \in \mathfrak{h}^n$, so the sum cannot converge because $a_{\epsilon^m\nu} = a_\nu$ does not depend on m since $\mathbf{k} = (l, \ldots, l)$.

(Note for general $\mathbf{k}$, the change in a_ν is dominated by the exponential term as m increases, so the same conclusion holds).

Definition. f is called a **cusp form** if a_0 vanishes in the Fourier expansion at each cusp. (If $n = 1$ we need the additional condition that $a_\nu = 0$ for $\nu < 0$. The equivalent condition for $n \geq 2$ is always satisfied by the above argument).

Thus if f is a cusp form, it may be written as

$$f(\mathbf{z}) = \sum_{\substack{\nu \in M^\vee \\ \nu \gg 0}} a_\nu e^{2\pi i \operatorname{Tr}(\nu \mathbf{z})}$$

To simplify what follows, we now make various assumptions. First assume k has narrow class number one. If this is not the case, then to get an L-series we have to consider cusp forms on a set of different groups Γ, one for each element of the narrow class group. The assumption also means that Γ will have a simpler form. Next, we assume that $\mathbf{k} = (l, \ldots, l)$, so that the integrals become simpler. Finally, we set $\Gamma = \Gamma_0(\mathfrak{n})$ which is defined to be $\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_k) \;\middle|\; c \in \mathfrak{n} \right\}$, where $\mathfrak{n}$ is an integral ideal of $\mathcal{O}_k$.

For this Γ, $M = \mathcal{O}_k$ and $V = U_k^+ = U_k^2$. If f is a cusp form then

$$f(\mathbf{z}) = \sum_{\substack{\nu \in \delta^{-1} \\ \nu \gg 0}} a_\nu e^{2\pi i \operatorname{Tr}(\nu \mathbf{z})}$$

where δ is the different. By convention, since any scalar multiple of a cusp form f is still a cusp form, it is convenient to normalize f by assuming that if ν generates δ^{-1} then $a_\nu = 1$.

Definition. We define the **L-series** associated to f to be

$$L(f, s) = \sum_{\substack{\nu \in \delta^{-1}/U_k^+ \\ \nu \gg 0}} a_\nu \mathrm{N}(\nu\delta)^{-s}$$

for those $s \in \mathbb{C}$ where the series converges, and by analytic continuation as far as possible.

The definition assumes that $a_{\epsilon\nu} = a_\nu \; \forall \epsilon \in U_k^+$ (hence we are using $\mathbf{k} = (l, \ldots, l)$ here), or else the series wouldn't be well defined. Equivalently, we may write the series as

$$L(f,s) = \sum_{\text{ideals } \mathfrak{m}} b_{\mathfrak{m}} \mathbf{N}(\mathfrak{m})^{-s}$$

where $b_{\mathfrak{m}} = a_\nu$ if $(\nu) = \mathfrak{m}\delta^{-1}$. This expression strongly resembles the L-series of an elliptic curve.

We can get $L(f,s)$ in terms of f as follows. For $\nu \in \delta^{-1}$ with $\nu \gg 0$, we have

$$\mathbf{N}(\nu\delta)^{-s} = D^{-s}\left(\frac{(2\pi)^s}{\Gamma(s)}\right)^n \int_0^\infty \cdots \int_0^\infty e^{-2\pi \operatorname{Tr} \nu \mathbf{y}} \mathbf{N}(\mathbf{y})^{s-1} \mathbf{N}(d\mathbf{y})$$

where $\mathbf{y} \in \mathbb{R}_+^n$, and D, the discriminant, equals $\mathbf{N}(\delta)$. So, for those s where the L-series converges absolutely, we have

$$L(f,s) = D^{-s}\left(\frac{(2\pi)^s}{\Gamma(s)}\right)^n \int_{\mathbb{R}_+^n/U_k^+} f(i\mathbf{y}) \mathbf{N}(\mathbf{y})^{s-1} \mathbf{N}(d\mathbf{y})$$

where we have changed the region of integration because the sum implicit in f is over all totally positive $\nu \in \delta^{-1}$, rather than one for each coset of U_k^+, as is the case for the sum in $L(f,s)$. Thus $L(f,s)$ is essentially the Mellin transform of f.

The cusp forms on Γ are acted on by various Hecke operators, which arise from various double cosets of $\Gamma_0(\mathfrak{n})$ acting on $\Gamma_0(\mathfrak{n})\backslash\mathfrak{h}^n$. The L-series of eigenforms of such operators have additional properties.

Definition. Let f be a cusp form on $\Gamma_0(\mathfrak{n})$, and $\nu \in \mathcal{O}_k$ generate a prime ideal. If $\mathfrak{n} \not\subseteq (\nu)$, define T_ν by

$$f\big|_{\mathrm{T}_\nu} = f\big|_{\left(\begin{smallmatrix}\nu & 0\\ 0 & 1\end{smallmatrix}\right)} + \sum_{j=0}^{\mathbf{N}(\nu)-1} f\big|_{\left(\begin{smallmatrix}1 & j\\ 0 & \nu\end{smallmatrix}\right)}$$

If $\mathfrak{n} \subseteq (\nu)$, define U_ν and W_ν by

$$f\big|_{\mathrm{U}_\nu} = \sum_{j=0}^{\mathbf{N}(\nu)-1} f\big|_{\left(\begin{smallmatrix}1 & j\\ 0 & \nu\end{smallmatrix}\right)} \qquad \text{and} \qquad f\big|_{\mathrm{W}_\nu} = f\big|_{\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)}$$

where if m is the biggest power of ν such that $\mathfrak{n} \subseteq (\nu^m)$, then $c \in \mathfrak{n}$, $a, d \in (\nu^m)$ and $ad - bc = \nu^m$. Finally, define N to be a totally positive generator of $\mathfrak{n}$, and define W_N by

$$f|_{\mathrm{W}_N} = f|_{\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)}$$

noting that W_N is the product of all the different W_ν, since this is true of the matrices which define these operators upto multiplication by an element of $\Gamma_0(\mathfrak{n})$.

Lemma 4.1. T_μ commutes with $\mathrm{U}_\nu, \mathrm{W}_\nu$ and T_λ. U_ν commutes with U_λ, and with W_μ if $(\mu) \neq (\nu)$. W_μ commutes with W_ν. Thus the T_ν and the W_μ have common eigenspaces, as do the T_ν and the U_μ.

Also, $f = \left(f|_{\mathrm{W}_N}\right)|_{\mathrm{W}_N}$ and $f = \left(f|_{\mathrm{W}_\nu}\right)|_{\mathrm{W}_\nu}$. Thus the eigenvalues of the W_ν and of W_N are ± 1.

Proof. Just algebra, or see [1] which generalizes directly to the case under consideration. □

We will soon be considering common eigenforms to all the $\mathrm{T}_\nu, \mathrm{U}_\mu$ and W_λ, and some of these will correspond to elliptic curves. Any common eigenspace of the T_ν which has dimension 1 must also be an eigenspace of the U_μ and the W_λ by the above lemma, and hence consists of common eigenforms to all the $\mathrm{T}_\nu, \mathrm{U}_\mu$ and W_λ. Such spaces may be explicitly determined by decomposing the space of Hilbert modular forms of weight 2 on each group $\Gamma_0(\mathfrak{n})$ into eigenspaces, and looking for any eigenspace which is common to all the $\mathrm{T}_\nu, \mathrm{U}_\mu$ and W_λ. Note that in any common eigenspace of the T_ν which has dimension 2 or more, there is nothing forcing the eigenvectors of the U_μ and the W_μ to coincide. We now establish some properties of eigenforms.

If f is a cusp form which is also an eigenform of W_N, say with eigenvalue $w = \pm 1$, then we can express $L(f, s)$ as an integral with better convergence properties. (Note in the special case where $\mathfrak{n} = \mathcal{O}_k$, all cusp forms are eigenforms of the operator W_1 with eigenvalue 1, since $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \Gamma_0(\mathcal{O}_k)$).

Choose a fundamental domain for $\mathbb{R}_+^n/U_k^+$, and divide it into two subsets, A and B. Let $C = \left\{\mathbf{y} \in \mathbb{R}_+^n \;\middle|\; (\frac{1}{i_1(N)y_1}, \ldots, \frac{1}{i_n(N)y_n}) \in B\right\}$. Define

$$\Lambda(f,s) = D^s \mathbf{N}(\mathfrak{n})^{s/2} \left(\frac{\Gamma(s)}{(2\pi)^s}\right)^n L(f,s) \tag{4.1}$$

and note that $\mathbf{N}(\mathfrak{n}) = \mathbf{N}(N)$. Then

$$\Lambda(f,s) = \int_{A+B} f(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^{s-1}\mathbf{N}(d\mathbf{y})$$

But as

$$wf(\mathbf{z}) = f\big|_{W_N}(\mathbf{z}) = \frac{1}{\mathbf{N}(N)^{l/2}\mathbf{z}^l} f\left(\frac{-1}{N\mathbf{z}}\right)$$

we have

$$\begin{aligned}\int_B f(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^s \mathbf{N}\left(\frac{d\mathbf{y}}{\mathbf{y}}\right) &= \int_C f\left(\frac{i}{N\mathbf{y}}\right)\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}\left(\frac{1}{N\mathbf{y}}\right)^s \mathbf{N}\left(\frac{d\mathbf{y}}{\mathbf{y}}\right) \\ &= \int_C wf(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{(l-s)/2}\mathbf{N}(\mathbf{y})^{(l-s)-1}\mathbf{N}(i)^l\mathbf{N}(d\mathbf{y})\end{aligned}$$

So

$$\begin{aligned}\Lambda(f,s) = \Big(&\int_A f(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^{s-1}\mathbf{N}(d\mathbf{y}) \\ &+ i^{ln} w \int_C f(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{(l-s)/2}\mathbf{N}(\mathbf{y})^{(l-s)-1}\mathbf{N}(d\mathbf{y})\Big)\end{aligned} \tag{4.2}$$

A sensible choice for the regions A and B is one where $A = C$, so that the two integrals are essentially the same. Since we obtain C from B by the map $\mathbf{y} \mapsto \frac{1}{N\mathbf{y}}$, one such choice is to partition A and B by the hypersurface $\mathbf{N}(\mathbf{y}) = \mathbf{N}(\mathfrak{n})^{-1/2}$.

Lemma 4.2. Let f be a cusp form on $\Gamma_0(\mathfrak{n})$, and let A be the intersection of a fundamental domain for $\mathbb{R}_+^n/U_k^+$ with the region $\mathbf{N}(\mathbf{y}) \geq \lambda\mathbf{N}(\mathfrak{n})^{-1/2}$ where $\lambda \in \mathbb{R}_+$. Then the integral $\int_A f(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^{s-1}\mathbf{N}(d\mathbf{y})$ converges absolutely for all s.

Proof. Let $E \subset \mathbb{R}_+^n$ be the set $E = \left\{\mathbf{y} \in \mathbb{R}_+^n \;\middle|\; \mathbf{N}(\mathbf{y}) \geq \lambda\mathbf{N}(\mathfrak{n})^{-1/2}\right\}$. Then

$$\int_A f(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^{s-1}\mathbf{N}(d\mathbf{y}) = \int_E \sum_{\substack{\nu \in \delta^{-1}/U_k^+ \\ \nu \gg 0}} a_\nu e^{-2\pi \operatorname{Tr}(\nu\mathbf{y})}\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^{s-1}\mathbf{N}(d\mathbf{y}) \tag{4.3}$$

But for $\nu \gg 0$, if $F = \left\{\mathbf{y} \in \mathbb{R}^n_+ \;\middle|\; \mathbf{N}(\mathbf{y}) \geq (2\pi)^n \lambda \mathbf{N}(\nu)\mathbf{N}(\mathfrak{n})^{-1/2}\right\}$, then by substituting $\mathbf{y}$ for $2\pi\nu\mathbf{y}$ we get

$$(*) \quad \int_E \left|a_\nu e^{-2\pi \operatorname{Tr}(\nu\mathbf{y})}\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^{s-1}\right| \mathbf{N}(d\mathbf{y})$$
$$= \left|a_\nu \mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\nu)^{-s}(2\pi)^{-ns}\right| \int_F \left|e^{-\operatorname{Tr}(\mathbf{y})}\mathbf{N}(\mathbf{y})^{s-1}\right| \mathbf{N}(d\mathbf{y})$$

But as $\nu \gg 0$, $\operatorname{Tr}(\mathbf{y}) \geq n\mathbf{N}(\mathbf{y})^{1/n}$, and so we deduce that $F \subset \left\{\mathbf{y} \in \mathbb{R}^n_+ \;\middle|\; \operatorname{Tr}(\mathbf{y}) \geq 2\pi n(\lambda \mathbf{N}(\nu)\mathbf{N}(\mathfrak{n})^{-1/2})^{1/n}\right\}$. Let $G = 2\pi n(\lambda \mathbf{N}(\nu)\mathbf{N}(\mathfrak{n})^{-1/2})^{1/n}$, and observe that if $x \geq z \geq 1$ then $0 \leq \int_x^\infty e^{-t}t^{z-1}dt \leq e^{-x}x^z$. Thus, if $\operatorname{Re} s \geq 1$ then using the substitution $Y = \operatorname{Tr}(\mathbf{y})$

$$\begin{aligned}
(*) &\leq \left|a_\nu \mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\nu)^{-s}(2\pi)^{-ns}n^{n(1-s)}\right| \int_F e^{-\operatorname{Tr}(\mathbf{y})} \left|\operatorname{Tr}(\mathbf{y})^{n(s-1)}\right| \mathbf{N}(d\mathbf{y}) \\
&\leq \left|a_\nu \mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\nu)^{-s}(2\pi)^{-ns}n^{n(1-s)}\right| \int_G^\infty \frac{Y^{n-1}}{(n-1)!} e^{-Y} Y^{n(\operatorname{Re}(s)-1)} dY \\
&\leq \left|a_\nu \mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\nu)^{-s}(2\pi)^{-ns}\frac{n^{n(1-s)}}{(n-1)!}\right| e^{-G}G^{n\operatorname{Re}(s)} \\
&= \lambda^{\operatorname{Re}(s)} |a_\nu| \frac{n^n}{(n-1)!} e^{-2\pi n(\lambda \mathbf{N}(\nu)\mathbf{N}(\mathfrak{n})^{-1/2})^{1/n}}
\end{aligned}$$

provided $2\pi(\lambda \mathbf{N}(\nu)\mathbf{N}(\mathfrak{n})^{-1/2})^{1/n} \geq \operatorname{Re} s$, which is true for all $\nu \in \delta^{-1}/U_k^+$ with sufficiently large norm, that is for all but finitely many cosets of U_k^+. On the other hand, if $\operatorname{Re} s \leq 1$ then, again setting $Y = \operatorname{Tr}(\mathbf{y})$

$$\begin{aligned}
(*) &\leq \left|a_\nu \mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\nu)^{-s}(2\pi)^{-ns}\right| \int_F e^{-\operatorname{Tr}(\mathbf{y})} \left|\left((2\pi)^n \lambda \mathbf{N}(\nu)\mathbf{N}(\mathfrak{n})^{-1/2}\right)^{s-1}\right| \mathbf{N}(d\mathbf{y}) \\
&\leq \lambda^{\operatorname{Re}(s)-1} \left|a_\nu \mathbf{N}(\mathfrak{n})^{1/2}\mathbf{N}(\nu)^{-1}(2\pi)^{-n}\right| \int_G^\infty \frac{Y^{n-1}}{(n-1)!} e^{-Y} dY \\
&\leq \lambda^{\operatorname{Re}(s)-1} \left|a_\nu \mathbf{N}(\mathfrak{n})^{1/2}\mathbf{N}(\nu)^{-1}(2\pi)^{-n}\right| e^{-G}G^n \\
&= \lambda^{\operatorname{Re}(s)} |a_\nu| \frac{n^n}{(n-1)!} e^{-2\pi n(\mathbf{N}(\nu)\mathbf{N}(\mathfrak{n})^{-1/2})^{1/n}}
\end{aligned}$$

if $2\pi(\lambda \mathbf{N}(\nu)\mathbf{N}(\mathfrak{n})^{-1/2})^{1/n} \geq 1$, which is again true for all $\nu \in \delta^{-1}/U_k^+$ with sufficiently large norm, so again the bound is valid for all but finitely many cosets of U_k^+.

Now, as f is a Hilbert modular form, a_ν is bounded by a polynomial in $\mathbf{N}(\nu)$ for given l, as is the number of totally positive $\nu \in \delta^{-1}/U_k^+$ for each fixed norm $\mathbf{N}(\nu)$, so

$$\sum_{\substack{\nu \in \delta^{-1}/U_k^+ \\ \nu \gg 0}} \lambda^{\mathrm{Re}(s)} |a_\nu| \frac{n^n}{(n-1)!} e^{-2\pi n(\mathbf{N}(\nu)\mathbf{N}(\mathfrak{n})^{-1/2})^{1/n}}$$

converges, so

$$\sum_{\substack{\nu \in \delta^{-1}/U_k^+ \\ \nu \gg 0}} \int_E a_\nu e^{-2\pi \,\mathrm{Tr}(\nu \mathrm{y})} \mathbf{N}(\mathfrak{n})^{s/2} \mathbf{N}(\mathrm{y})^{s-1} \mathbf{N}(d\mathrm{y})$$

converges absolutely, and thus we may exchange the $\sum$ and $\int$ to get the right hand side of (4.3), hence the left hand side of this equation converges absolutely, as required. □

Corollary 4.3. If f is a Hilbert modular cusp form on $\Gamma_0(\mathfrak{n})$ which is an eigenform of W_N, then (4.2) with the above choice of A and C together with (4.1) defines $\Lambda(f,s)$ and $L(f,s)$ for all s and

$$\Lambda(f,s) = i^{ln} w \Lambda(f, l-s) \tag{4.4}$$

Proof. By the above lemma with $\lambda = 1$, with the above choice of A and C, the first term of the right hand side of (4.2) converges absolutely for each s and so does the second term (by replacing s with $l-s$). Hence (4.2) defines $\Lambda(f,s)$ for all s, and since (4.1) expresses $\Lambda(f,s)$ in terms of $L(f,s)$, this shows $L(f,s)$ is defined for all s. Also substituting s for $l-s$ in (4.2) and multiplying by $i^{ln}w$ fixes this equation, so we deduce

$$\Lambda(f,s) = i^{ln} w \Lambda(f, l-s)$$

□

We can also use the Hecke operators to produce a product expansion for the L-series of a common eigenform. Let δ^{-1} be generated by ξ. If f is an eigenform

of T_ν, so $f\big|_{\mathrm{T}_\nu} = \mu f$, then looking at the Fourier expansion of f gives that

$$\mu a_\lambda = \begin{cases} a_{\lambda\nu}\mathbf{N}(\nu)^{1-l/2} & \text{if } \lambda \notin (\nu\xi) \\ a_{\lambda\nu}\mathbf{N}(\nu)^{1-l/2} + \mathbf{N}(\nu)^{l/2}a_{\lambda/\nu} & \text{if } \lambda \in (\nu\xi) \end{cases}$$

hence $\mu a_\xi = a_{\nu\xi}\mathbf{N}(\nu)^{1-l/2}$, but $a_\xi = 1$ by our choice of normalization, so $\mu = a_{\nu\xi}\mathbf{N}(\nu)^{1-l/2}$. This means that

$$(1 - a_{\nu\xi}\mathbf{N}(\nu)^{-s} + \mathbf{N}(\nu)^{(l-1)-2s})L(f,s) = \sum_{\substack{\mu \in \delta^{-1}/U_k^+ \\ \mu \gg 0 \\ \mu \notin (\nu\xi)}} a_\mu \mathbf{N}(\mu\delta)^{-s}$$

Similarly, if f is an eigenform of U_ν, so $f\big|_{\mathrm{U}_\nu} = \mu f$, then looking at the Fourier expansion of f gives that $\mu a_\lambda = a_{\lambda\nu}\mathbf{N}(\nu)^{1-l/2}$, so again $\mu = a_{\nu\xi}\mathbf{N}(\nu)^{1-l/2}$, and

$$(1 - a_{\nu\xi}\mathbf{N}(\nu)^{-s})L(f,s) = \sum_{\substack{\mu \in \delta^{-1}/U_k^+ \\ \mu \gg 0 \\ \mu \notin (\nu\xi)}} a_\mu \mathbf{N}(\mu\delta)^{-s}$$

thus we have

Theorem 4.4. *If f is a common eigenform for all the T_ν and all the U_ν, and if* $c_\nu = \begin{cases} 1 & \text{if } \nu \notin \mathfrak{n} \\ 0 & \text{if } \nu \in \mathfrak{n} \end{cases}$ *then*

$$L(f,s) = \prod_{\substack{(\nu) \text{ prime} \\ (\nu \gg 0)}} \left(1 - a_{\nu\xi}\mathbf{N}(\nu)^{-s} + c_\nu \mathbf{N}(\nu)^{(l-1)-2s}\right)^{-1} \tag{4.5}$$

Note that a consequence of this theorem is that a common eigenspace of all the T_ν and all the U_ν must have dimension 1, since the eigenvalues of these operators determine the fourier series expansion upto multiplication by a constant.

Also if $l = 2$, (4.5) is precisely the form of the L-series $L(E,s)$ of an elliptic curve E over $\mathcal{O}_k$, with conductor $\mathfrak{n}$, and with the number of points on the reduced curve E_ν over $\mathcal{O}_k/(\nu) \cong \mathbb{F}_{\mathbf{N}(\nu)}$ equal to $1 + \mathbf{N}(\nu) - a_{\nu\xi}$. This leads us to the following conjecture.

Conjecture 3. *Let E be a global minimal elliptic curve over $\mathcal{O}_k$, with conductor $\mathfrak{n}$. Then the coefficients of the L-series $L(E,s)$ are the coefficients of the Fourier series expansion of a Hilbert modular form f on $\Gamma_0(\mathfrak{n})$ of weight 2, which is a common eigenform of the Hecke operators T_ν, U_μ and W_λ, as above. (Thus $L(E,s) = L(f,s)$).*

This is a generalization of the Taniyama-Weil-Shimura conjecture to totally real number fields. The conjecture has recently been proved in many cases over $\mathbb{Q}$ by Andrew Wiles, Richard Taylor, and Fred Diamond (see [28]).

4.2 Calculating L-Series

We now assume **Conjecture 3** to provide an efficient method to calculate the L-series of an elliptic curve with coefficients in $\mathcal{O}_k$. In fact it will emerge that this assumption is almost certainly valid, since the methods used provide an easy way to verify numerically that what we are assuming is a modular form almost certainly is a modular form with the correct conductor.

Recall the equation (4.2)

$$\Lambda(f,s) = \Big(\int_A f(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^{s-1}\mathbf{N}(d\mathbf{y}) + i^{ln}w\int_C f(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{(l-s)/2}\mathbf{N}(\mathbf{y})^{(l-s)-1}\mathbf{N}(d\mathbf{y})\Big)$$

where A and B were a partition for a fundamental domain for $\mathbb{R}_+^n/U_k^+$ and C was the image of B under the map $\mathbf{y} \mapsto \frac{1}{N\mathbf{y}}$. Here $l = 2$, and we need to choose A and B so that we can integrate each term of (4.2) over the resulting regions. This is where our previous choice of A and B runs into trouble. If we set $E = \left\{\mathbf{y} \in \mathbb{R}_+^n \;\middle|\; \mathbf{N}(\mathbf{y}) \geq \mathbf{N}(\mathfrak{n})^{-1/2}\right\}$, we have to integrate expressions like

$$(\dagger) \qquad \int_E e^{-2\pi\,\mathrm{Tr}(\nu\mathbf{y})}\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^{s-1}\mathbf{N}(d\mathbf{y})$$

where $\nu \in \delta^{-1}/U_k^+$ and is totally positive. The problem is that I have found no way to integrate this expression completely, except when $n = 2$ and $s > 0$ is

an integer. Since the case we will be considering requires this expression to be evaluated for $s = 2$ and for $s = 0$ this is insufficient. (You can integrate once to get an expression in terms of Bessel K functions or Ei functions, and then (at least for $n = 2$) integrate numerically, but this is prohibitively slow for even a small number of decimal places).

The obstruction comes from the curved hyperplane boundary $\mathbf{N}(\mathbf{y}) = \mathbf{N}(\mathfrak{n})^{-1/2}$, which introduces terms which do not appear to be integrable into the expression obtained after integrating with respect to one coordinate. So the way around this problem is to choose A and B so we have a "nice" boundary between them. It would also be convenient to have $A = C$, particularly since this means the two integrals have a similar rate of convergence. My solution is to bound these regions by hyperplanes perpendicular to one of the axes, that is, by regions with one of the y_i constant.

The main advantages of this approach are that the map $\mathbf{y} \mapsto \frac{1}{N\mathbf{y}}$ maps hyperplanes with one coordinate fixed, to hyperplanes with one coordinate fixed, so we should be able to find regions with $A = C$, and that integration is vastly simplified, since each region will be a union of hypercuboids, and so we can integrate with respect to each y_i separately, which reduces the problem to evaluating the product of various incomplete Gamma functions.

The slight disadvantage is that the rate of convergence will be slightly worse since this essentially depends on the coefficient of the exponential in (†) at the point of the region where this is largest. As the exponential may be bounded above by $-2\pi\mathbf{N}(\nu\mathbf{y})^{1/n}$ with equality at one point, it means that our previous choice of region would be optimal if we could integrate over it.

If we restrict to the case where k is a real quadratic field (with narrow class number one) then we can make this explicit. Since the units of such a field form a rank 1 $\mathbb{Z}$-module under multiplication with torsion $\{\pm 1\}$, there is a unit, u say, with $i_1(u)$ taking the least possible value greater than 1. Then u and -1 generate the

group of units, and u^2 generates U_k^+, the group of totally positive units. Identify $u \in \mathbb{R}$ with $i_1(u)$, and write N_j for $i_j(N)$. Then we can choose our fundamental region of $\mathbb{R}_+^2/U_k^+$ to be $\left\{\mathbf{y} \in \mathbb{R}_+^2 \;\middle|\; u^{-1}N_1^{-1/2} \le y_1 < uN_1^{-1/2}\right\}$. Thus we can take $A = C = \left\{\mathbf{y} \in \mathbb{R}_+^2 \;\middle|\; u^{-1}N_1^{-1/2} \le y_1 < uN_1^{-1/2} \text{ and } N_2^{-1/2} \le y_2\right\}$.

Then as $U_k^+ A \subset \left\{\mathbf{y} \in \mathbb{R}_+^n \;\middle|\; \mathbf{N}(\mathbf{y}) \ge u^{-1}\mathbf{N}(\mathfrak{n})^{-1/2}\right\}$, by Lemma 4.2 we can rearrange integrals and sums to get

$$\begin{aligned}
&\int_A f(i\mathbf{y})\mathbf{N}(\mathfrak{n})^{s/2}\mathbf{N}(\mathbf{y})^{s-1}\mathbf{N}(d\mathbf{y}) \\
&\qquad = \mathbf{N}(\mathfrak{n})^{s/2} \sum_{\substack{\nu \gg 0 \\ \nu \in \delta^{-1}}} a_\nu \int_{N_2^{-1/2}}^{\infty} e^{-2\pi\nu_2 y_2} y_2^{s-1} dy_2 \int_{u^{-1}N_1^{-1/2}}^{uN_1^{-1/2}} e^{-2\pi\nu_1 y_1} y_1^{s-1} dy_1 \\
&\qquad = \sum_{\substack{\nu \gg 0 \\ \nu \in \delta^{-1}}} a_\nu \frac{\mathbf{N}(\mathfrak{n})^{s/2}}{(2\pi)^{2s}\mathbf{N}(\nu)^s} \Gamma\left(s, \frac{2\pi\nu_2}{\sqrt{N_2}}\right)\left[\Gamma\left(s, \frac{2\pi\nu_1}{u\sqrt{N_1}}\right) - \Gamma\left(s, \frac{2\pi\nu_1 u}{\sqrt{N_1}}\right)\right]
\end{aligned}$$

where $\Gamma(s,x) = \int_x^\infty e^{-y}y^{s-1}dy$. Replacing s with $2-s$ gives the other integral in (4.2) so finally we have

Theorem 4.5. *Let f be a Hilbert modular cusp form on $\Gamma_0(\mathfrak{n})$ over a real quadratic field k with narrow class number one, let u be the least positive real embedding of a unit of k which is greater than one, and let $N \in k$ be a totally positive generator of $\mathfrak{n}$. Then*

(4.6)

$$\begin{aligned}
L(f,s) = \frac{1}{D^s\Gamma(s)^2} \sum_{\substack{\nu \gg 0 \\ \nu \in \delta^{-1}}} a_\nu \Bigg(&\mathbf{N}(\nu)^{-s}\Gamma\left(s, \frac{2\pi\nu_2}{\sqrt{N_2}}\right)\left[\Gamma\left(s, \frac{2\pi\nu_1}{u\sqrt{N_1}}\right) - \Gamma\left(s, \frac{2\pi\nu_1 u}{\sqrt{N_1}}\right)\right] \\
+ w(2\pi)^{4s-4}&\left(\frac{\mathbf{N}(\mathfrak{n})^{1-s}}{\mathbf{N}(\nu)^{2-s}}\right)\Gamma\left(2-s, \frac{2\pi\nu_2}{\sqrt{N_2}}\right)\left[\Gamma\left(2-s, \frac{2\pi\nu_1}{u\sqrt{N_1}}\right) - \Gamma\left(2-s, \frac{2\pi\nu_1 u}{\sqrt{N_1}}\right)\right]\Bigg)
\end{aligned}$$

where $\Gamma(s,x) = \int_x^\infty e^{-y}y^{s-1}dy$.

This expression is valid for all s, but for our calculations we will want $s = 2$, so we can simplify this further using $\Gamma(2,x) = (x+1)e^{-x}$ and $\Gamma(0,x) = \mathrm{Ei}(x)$ where by definition $\mathrm{Ei}(x) = \int_x^\infty e^{-y}\frac{dy}{y}$. So

Corollary 4.6. Under the same conditions as the previous theorem

$$(4.7)\quad L(f,2) = \frac{1}{D^2}\sum_{\substack{\nu \gg 0 \\ \nu\in\delta^{-1}}} a_\nu \left(\left(\frac{2\pi}{\nu_2\sqrt{N_2}} + \frac{1}{\nu_2^2} \right) e^{-2\pi\nu_2/\sqrt{N_2}} \right.$$
$$\left[\left(\frac{2\pi}{u\nu_1\sqrt{N_1}} + \frac{1}{\nu_1^2} \right) e^{-2\pi\nu_1/u\sqrt{N_1}} - \left(\frac{2\pi u}{\nu_1\sqrt{N_1}} + \frac{1}{\nu_1^2} \right) e^{-2\pi u\nu_1/\sqrt{N_1}} \right]$$
$$\left. + \left(\frac{(2\pi)^4 w}{\mathbf{N}(\mathfrak{n})} \right) \mathrm{Ei}\left(\frac{2\pi\nu_2}{\sqrt{N_2}} \right) \left[\mathrm{Ei}\left(\frac{2\pi\nu_1}{u\sqrt{N_1}} \right) - \mathrm{Ei}\left(\frac{2\pi\nu_1 u}{\sqrt{N_1}} \right) \right] \right)$$

This process can be generalized to real cubic fields (of narrow class number 1) or beyond, but constructing a fundamental domain becomes more and more complicated, and there is a choice to be made of which domain gives the best convergence. The best approach seems to be to consider the lattice formed by the logarithms of the coordinates of the units, ignoring one coordinate to give a lattice in $\mathbb{R}^{n-1}$. Any fundamental domain in this bounded by hyperplanes perpendicular to an axis will correspond to a fundamental domain in $\mathbb{R}^n_+$ bounded by hyperplanes perpendicular to an axis. I have have used this to construct such a fundamental domain for the real cubic field case as follows.

Let $-1, \mathbf{u}$ and $\mathbf{v}$ generate the unit group of $\mathcal{O}_k$ where k is a real cubic field with narrow class number one. So $\mathbf{u}^2$ and $\mathbf{v}^2$ generate U_k^+. Let $U_j = \ln|u_j|$ and $V_j = \ln|v_j|$, where $j \in \{1,2\}$. Assume (by change of basis of the unit group) that (U_1, U_2) is an element of minimal length in the lattice generated by (U_1, U_2) and (V_1, V_2) in $\mathbb{R}^2$, that $U_1 > 0$ and $U_1V_2 - V_1U_2 > 0$ (by replacing $\mathbf{u}$ by $\frac{1}{\mathbf{u}}$ and $\mathbf{v}$ by $\frac{1}{\mathbf{v}}$ if necessary) and that $0 \le V_1 < U_1$ (by multiplying $\mathbf{v}$ by a power of $\mathbf{u}$). Note that means that $V_2 > 0$, since either U_2 is positive, and then $V_2 > 0$ is a consequence of $U_1V_2 - V_1U_2 > 0$, or else U_2 is negative, and so $V_2 > 0$ as otherwise (U_1, U_2) is not minimal.

Then the region R is a fundamental domain for $\mathbb{R}^2$ modulo the lattice generated

by $2(U_1, U_2)$ and $2(V_1, V_2)$ where if $U_2 \leq 0$

$$\begin{aligned} R = &\Big\{(x,y) \,\Big|\, (-U_1 \leq x \leq U_1) \text{ and } (-V_2 \leq y \leq V_2)\Big\} \\ &\cup \Big\{(x,y) \,\Big|\, (-U_1 \leq x \leq 2V_1 - U_1) \text{ and } (V_2 \leq y \leq V_2 - U_2)\Big\} \\ &\cup \Big\{(x,y) \,\Big|\, (-2V_1 + U_1 \leq x \leq U_1) \text{ and } (-V_2 + U_2 \leq y \leq -V_2)\Big\} \end{aligned}$$

and if $U_2 \geq 0$

$$\begin{aligned} R = &\Big\{(x,y) \,\Big|\, (-U_1 \leq x \leq U_1) \text{ and } (-V_2 \leq y \leq V_2)\Big\} \\ &- \Big\{(x,y) \,\Big|\, (-U_1 \leq x \leq 2V_1 - U_1) \text{ and } (V_2 \geq y \geq V_2 - U_2)\Big\} \\ &- \Big\{(x,y) \,\Big|\, (-2V_1 + U_1 \leq x \leq U_1) \text{ and } (-V_2 + U_2 \geq y \geq -V_2)\Big\} \end{aligned}$$

If we consider the equivalent region in $\mathbb{R}^3_+$ we obtain

Theorem 4.7. *Let f be a Hilbert modular cusp form over $\Gamma_0(\mathfrak{n})$ corresponding to an elliptic curve over a real cubic field k with narrow class number one, let $N \in k$ be a totally positive generator of $\mathfrak{n}$ and let $\mathbf{u}$ and $\mathbf{v}$ be generators with -1 of the unit group of $\mathcal{O}_k$ such that*

(i) $\mathbf{u}$ has $|u_1| > 1$ and minimizes $(\ln|u_1|)^2 + (\ln|u_2|)^2$ over the unit group

(ii) $\mathbf{v}$ is such that $\ln|u_1|\ln|v_2| > \ln|v_1|\ln|u_2|$ and $1 < |v_1| < |u_1|$

Then

$$\begin{aligned} (4.8)\quad L(f,s) = \frac{1}{D^s\Gamma(s)^3} \sum_{\substack{\nu \gg 0 \\ \nu \in \delta^{-1}}} a_\nu \Bigg(&\mathbf{N}(\nu)^{-s} g_3(1) \left(g_1\left(\frac{1}{u_1}\right)\left[g_2\left(\frac{1}{v_2}\right) - g_2\left(\frac{v_2}{u_2}\right)\right]\right. \\ &+ g_1\left(\frac{v_1^2}{u_1}\right)\left[g_2\left(\frac{v_2}{u_2}\right) - g_2(v_2)\right] + g_1(u_1)\left[g_2(v_2) - g_2\left(\frac{u_2}{v_2}\right)\right] + g_1\left(\frac{u_1}{v_1^2}\right)\left[g_2\left(\frac{u_2}{v_2}\right)\right. \\ &\left.\left. - g_2\left(\frac{1}{v_2}\right)\right]\right) - w(2\pi)^{6s-6}\left(\frac{\mathbf{N}(\mathfrak{n})^{1-s}}{\mathbf{N}(\nu)^{2-s}}\right) h_3(1)\left(h_1\left(\frac{1}{u_1}\right)\left[h_2\left(\frac{1}{v_2}\right) - h_2\left(\frac{v_2}{u_2}\right)\right] + h_1\left(\frac{v_1^2}{u_1}\right)\right. \\ &\left.\left[h_2\left(\frac{v_2}{u_2}\right) - h_2(v_2)\right] + h_1(u_1)\left[h_2(v_2) - h_2\left(\frac{u_2}{v_2}\right)\right] + h_1\left(\frac{u_1}{v_1^2}\right)\left[h_2\left(\frac{u_2}{v_2}\right) - h_2\left(\frac{1}{v_2}\right)\right]\right)\Bigg) \end{aligned}$$

where $g_j(x) = \Gamma(s, |x|2\pi\nu_j/\sqrt{N_j})$ and $h_j(x) = \Gamma(2-s, |x|2\pi\nu_j/\sqrt{N_j})$.

In fact, this expression will work for any choice of $\mathbf{u}$ and $\mathbf{v}$ which generate the unit group with -1, possibly after swapping $\mathbf{u}$ and $\mathbf{v}$ so that $\ln|u_1|\ln|v_2| > \ln|v_1|\ln|u_2|$, and not just the ones constructed above. This may be seen by showing that the regions R obtained by fixing one of $\mathbf{u}$ and $\mathbf{v}$ and varying the other are the same upto translations of parts of the region by lattice elements. Hence every such region is a fundamental domain, provided we interpret suitably negative parts of the region caused when the boundary self-intersects (the region is a fundamental domain in the sense that in each equivalence class of points (under the action of the lattice) which has no points on the boundary, there is precisely one more point in the positive parts of the region than in the negative parts). The formula above still works even if it corresponds to a region with negative parts.

The choice of $\mathbf{u}$ and $\mathbf{v}$ given above need not be optimal in terms of convergence, and exchanging the first and second coordinates may also improve the convergence. However the above construction gives an explicit way of constructing a "not too bad" region.

The issue of which fundamental domain to choose is only a matter of rate of convergence, any choice of fundamental domain will (conjecturally) converge to the same value. This is because, if ϵ is a totally positive unit then $f(\mathbf{z}) = f(\epsilon\mathbf{z})$, so f is periodic modulo totally positive units. The individual exponential terms however will not in general have this behaviour, so if you evaluate the L-series for two different fundamental domains and the results are the same to within an expected error due to approximations in calculation, this provides strong evidence that f does indeed have the conjectural periodic behaviour. Moreover this will also confirm that f has expected conductor, since the conductor is involved in the calculation.

There is a slight modification to the above method, which may improve the rate of convergence, particularly for those fields which have minimal units with large coefficients. Rather than using one integration region for each fundamental domain,

we can use an integer number of them. This is equivalent to replacing the coefficients of the units above, by their integer roots. In other words, instead of integrating over a fundamental domain for $\mathbb{R}_+^n/U_k^+$ we will be integrating over a fundamental domain for $\mathbb{R}_+^n/(U_k^+)^{1/m}$ for some positive integer m, and this will work since m^n of the smaller domains together will make a fundamental domain for $\mathbb{R}_+^n/U_k^+$. (By $(U_k^+)^{1/m}$ we mean the set $(U_k^+)^{1/m} = \left\{(i_1(v)^{1/m}, \ldots, i_n(v)^{1/m}) \text{ for } v \in U_k^+\right\}$, where we take the real positive mth root).

For example, in equations (4.6) and (4.7), we can replace $u = i_1(u)$ with $\sqrt[m]{u}$, where $u \in \mathcal{O}_k$ is a minimal unit in the sense described above and m is a positive integer, and the sum is over totally positive $\nu \in \delta^{-1}(U_k^+)^{1/m}$. Then the generalization of Corollary 4.6 is

Theorem 4.8. *Under the conditions of Theorem 4.5*

$$L(f,2) = \sum_{\substack{\nu \gg 0 \\ \nu \in \delta^{-1}(U_k^+)^{1/m}}} \frac{1}{D^2} a_\nu \left(\left(\frac{2\pi}{\nu_2\sqrt{N_2}} + \frac{1}{\nu_2^2} \right) e^{-2\pi\nu_2/\sqrt{N_2}} \right. \tag{4.9}$$
$$\left[\left(\frac{2\pi}{\sqrt[m]{u}\nu_1\sqrt{N_1}} + \frac{1}{\nu_1^2} \right) e^{-2\pi\nu_1/\sqrt[m]{u}\sqrt{N_1}} - \left(\frac{2\pi\sqrt[m]{u}}{\nu_1\sqrt{N_1}} + \frac{1}{\nu_1^2} \right) e^{-2\pi\nu_1\sqrt[m]{u}/\sqrt{N_1}} \right]$$
$$\left. + \left(\frac{(2\pi)^4 w}{\mathbf{N}(\mathfrak{n})} \right) \mathrm{Ei}\left(\frac{2\pi\nu_2}{\sqrt{N_2}} \right) \left[\mathrm{Ei}\left(\frac{2\pi\nu_1}{\sqrt[m]{u}\sqrt{N_1}} \right) - \mathrm{Ei}\left(\frac{2\pi\nu_1\sqrt[m]{u}}{\sqrt{N_1}} \right) \right] \right)$$

where $a_\nu \in \delta^{-1}(U_k^+)^{1/m} \setminus \delta^{-1}$ is defined to be equal to a_μ for any $\mu \in \delta^{-1}$ which, when considered as an element of $\delta^{-1}(U_k^+)^{1/m}$, is in the same $(U_k^+)^{1/m}$ coset as ν.

Note that we already know that a_ν for $\nu \in \delta^{-1}$ is constant on cosets of U_k^+, thus the final condition of the theorem merely extends the definition of a_ν to $\nu \in \delta^{-1}(U_k^+)^{1/m}$ by insisting it is constant on cosets of $(U_k^+)^{1/m}$. Also we may generalize Theorems 4.5 and 4.7 in exactly the same way. Equation (4.9) is the one I use in my program to calculate $L(f,2)$.

The best choice of m will depend on the relative efficiency of evaluating each term of the sum and of calculating the coefficients a_ν. Roughly speaking, to obtain a given accuracy as m increases, the number of terms you need to evaluate in the

sum will increase, but the number of different a_ν you need to evaluate will decrease. We will return to the question of choosing m later when we have established error bounds for truncating the series.

By evaluating $L(f,2)$ for two different values of m, we can also verify numerically that f has the predicted periodicity, and this is also more practical (from the point of view of programming and of convergence) than varying the choice of fundamental domain. In fact, this is one of the methods I used to check for programming and calculation errors when I was writing my program.

We finish this section by considering how many terms in equation (4.9) we need to calculate to obtain a given accuracy.

Proposition 4.9. Let $\nu \in (U_k^+)^{1/m}$ be totally positive. If $T = 2\pi\left(\nu_1/\sqrt[m]{u}\sqrt{N_1} + \nu_2/\sqrt{N_2}\right)$ then the term in ν in equation (4.9) is bounded in modulus by

$$\left((1+T) + \frac{(2\pi)^2}{D\mathbf{N}(\mathfrak{n})^{1/2}}\left(\sqrt[m]{u} + \frac{1}{\sqrt[m]{u}}\right)\right)e^{-T} \tag{4.10}$$

Proof. Each term of (4.9) consists of a_ν/D^2 multiplied by the sum of two more complicated terms. Since $(1+x)e^{-x}$ is a decreasing function in x, we deduce for the first term

$$0 \le \frac{1}{\mathbf{N}(\nu)^2}\left(1+\frac{2\pi\nu_2}{\sqrt{N_2}}\right)e^{-2\pi\nu_2/\sqrt{N_2}}\left[\left(1+\frac{2\pi\nu_1}{\sqrt[m]{u}\sqrt{N_1}}\right)e^{-2\pi\nu_1/\sqrt[m]{u}\sqrt{N_1}} - \left(1+\frac{2\pi\nu_1\sqrt[m]{u}}{\sqrt{N_1}}\right)e^{-2\pi\nu_1\sqrt[m]{u}/\sqrt{N_1}}\right] \le \left(\frac{1}{\mathbf{N}(\nu)^2}(1+T) + \frac{(2\pi)^2}{\sqrt[m]{u}\mathbf{N}(\mathfrak{n})^{1/2}\mathbf{N}(\nu)}\right)e^{-T}$$

and for the second term, since $\mathrm{Ei}(x) \le \frac{1}{x}e^{-x}$ (for $x > 0$) is a decreasing function, we have

$$0 \le \left|\frac{(2\pi)^4 w}{\mathbf{N}(\mathfrak{n})}\right|\mathrm{Ei}\left(\frac{2\pi\nu_2}{\sqrt{N_2}}\right)\left[\mathrm{Ei}\left(\frac{2\pi\nu_1}{\sqrt[m]{u}\sqrt{N_1}}\right) - \mathrm{Ei}\left(\frac{2\pi\nu_1\sqrt[m]{u}}{\sqrt{N_1}}\right)\right] \le \frac{(2\pi)^2\sqrt[m]{u}}{\mathbf{N}(\mathfrak{n})^{1/2}\mathbf{N}(\nu)}e^{-T}$$

Thus as $\mathbf{N}(\nu) \ge 1/D$, the result follows by the following lemma, which gives a bound for a_ν which though not optimal, is the most useful in this situation. □

Lemma 4.10. $|a_\nu| \le D\mathbf{N}(\nu)$

Proof. We use the product expansion of the L-series of an elliptic curve as in equation (4.5) and following. Using a well known bound on the number of points on an elliptic curve over a finite field, we have that if $\nu \in \delta^{-1}$ is totally positive and generates a prime ideal then,

$$|a_{\nu\xi}| \leq 2\mathbf{N}(\nu)^{1/2}$$

This gives the required result in this case if $\mathbf{N}(\nu) \geq 4$. (Recall ξ generates δ^{-1} as a fractional ideal and $\mathbf{N}(\xi) = D^{-1}$, also that $a_{v\mu} = a_\mu$ for any totally positive unit v and any totally positive $\mu \in \delta^{-1}$). Now if μ and ν are coprime (totally positive) algebraic integers, we have $a_{\mu\nu\xi} = a_{\mu\xi}a_{\nu\xi}$ so by induction we need only look at $a_{\nu^t\xi}$ where ν generates a prime ideal in $\mathcal{O}_k$. But then

$$a_{\nu^t\xi} - a_{\nu\xi}a_{\nu^{t-1}\xi} + \mathbf{N}(\nu)a_{\nu^{t-2}\xi} = 0$$

(except if there is bad reduction at ν, but then $a_{\nu^t\xi} = 0$ or ± 1 so we may ignore this case). Then solving the recurrence relation, using the facts that $a_{\nu\xi}$ and $\mathbf{N}(\nu)$ are integers, and that $a_\xi = 1$ gives

$$|a_{\nu^t\xi}| \leq \begin{cases} 2\mathbf{N}(\nu)^{(t+1)/2} & \text{if}(a_{\nu\xi})^2 \neq 4\mathbf{N}(\nu) \\ (t+1)\mathbf{N}(\nu)^{t/2} & \text{if}(a_{\nu\xi})^2 = 4\mathbf{N}(\nu) \end{cases}$$

The second case can only occur when $\mathbf{N}(\nu)$ is a square, hence $\mathbf{N}(\nu) \geq 4$ and we have the required result for $t \geq 2$. In the first case $\mathbf{N}(\nu) \geq 2$, so this gives the required result for $t \geq 3$, and for $t = 2$ unless $\mathbf{N}(\nu) \leq 3$. We have already covered the case where $t = 1$ for $\mathbf{N}(\nu) \geq 4$, so all that remains when $t = 1$ or 2 and $\mathbf{N}(\nu) \leq 3$. But, $a_{\nu\xi}$ is an integer, and the integer part of $2\sqrt{2}$ is 2, and of $2\sqrt{3}$ is 3, so the lemma is true for $t = 1$. Finally, $a_{\nu^2\xi} = (a_{\nu\xi})^2 - \mathbf{N}(\nu)$, so if $\mathbf{N}(\nu) = 2$, $-2 \leq a_{\nu^2\xi} \leq 2$ and if $\mathbf{N}(\nu) = 3$, $-3 \leq a_{\nu^2\xi} \leq 6$, which covers the remaining cases. □

Next we need to estimate how many totally positive $\nu \in \delta^{-1}(U_k^+)^{1/m}$ there are such that $T = 2\pi\left(\nu_1/\sqrt[m]{u}\sqrt{N_1} + \nu_2/\sqrt{N_2}\right)$ lies within narrow limits, and use this

to deduce a bound in modulus for all the terms of (4.9) where ν is such that T is bigger than a given bound, M say. Here it is easier to consider each δ^{-1} coset of $\delta^{-1}(U_k^+)^{1/m}$ in turn. We can write the cosets of δ^{-1} as $((\sqrt[m]{u})^{2q}, (\sqrt[m]{u})^{-2q})\,\delta^{-1}$ for $q = 0, \ldots, m-1$.

Proposition 4.11. Let $\{g, h\}$ be a $\mathbb{Z}$-basis for δ^{-1} so that g is totally positive and $g_1h_2 - g_2h_1 > 0$. Let $x = 2\pi\left(g_1/(\sqrt[m]{u})^{1+2q}\sqrt{N_1} + g_2/(\sqrt[m]{u})^{-2q}\sqrt{N_2}\right)$, and let $r \geq 0$ be an integer. Then the number of totally positive $\nu \in ((\sqrt[m]{u})^{2q}, (\sqrt[m]{u})^{-2q})\,\delta^{-1}$ with $M + rx \leq T < M + (r+1)x$, where $T = 2\pi\left(\nu_1/\sqrt[m]{u}\sqrt{N_1} + \nu_2/\sqrt{N_2}\right)$, is at most

$$\frac{\sqrt{D}\,\sqrt[m]{u}\mathbf{N}(\mathfrak{n})^{1/2}x}{(2\pi)^2}\,(M + (r+1)x) + 1 \tag{4.11}$$

Proof. Observe that $\nu \in ((\sqrt[m]{u})^{2q}, (\sqrt[m]{u})^{-2q})\,\delta^{-1}$ if and only if $\nu_1 = (\sqrt[m]{u})^{-2q}(ag_1 + bh_1)$ and $\nu_2 = (\sqrt[m]{u})^{2q}(ag_2 + bh_2)$ for some $a, b \in \mathbb{Z}$. Let $y = 2\pi\left(h_1/(\sqrt[m]{u})^{1+2q}\sqrt{N_1} + h_2/(\sqrt[m]{u})^{-2q}\sqrt{N_2}\right)$. Then for this ν, $T = ax + by$ and so we wish to bound the number of a and b such that $M + rx \leq ax + by < M + (r+1)x$ and such that ν is totally positive, i.e. $ag_1 + bh_1 > 0$ and $ag_2 + bh_2 > 0$.

But by our choice of bounds, for each value of b, there is precisely one a such that $M + rx \leq ax + by < M + (r+1)x$. So all we need to do is to eliminate a from the above inequalities, and the required result is the number of b which satisfy the resulting inequalities.

As $g \gg 0$, $a > -bh_1/g_1$ and $a > -bh_2/g_2$. Thus

$$-bx\frac{h_2}{g_2} + by < M + (r+1)x \quad \text{and} \quad -bx\frac{h_1}{g_1} + by < M + (r+1)x$$

Rearranging this gives

$$\frac{2\pi b(h_1g_2 - h_2g_1)}{g_2(\sqrt[m]{u})^{1+2q}\sqrt{N_1}} < M + (r+1)x \quad \text{and} \quad \frac{2\pi b(g_1h_2 - g_2h_1)}{g_1(\sqrt[m]{u})^{-2q}\sqrt{N_2}} < M + (r+1)x$$

but as $\{g, h\}$ is a $\mathbb{Z}$-basis for δ^{-1} and $g_1h_2 - g_2h_1 > 0$, then $g_1h_2 - g_2h_1 = 1/\sqrt{D}$, and so

$$-(M + (r+1)x)g_2(\sqrt[m]{u})^{1+2q}\sqrt{N_1}\sqrt{D} < 2\pi b < (M + (r+1)x)g_1(\sqrt[m]{u})^{-2q}\sqrt{N_2}\sqrt{D}$$

However $\sqrt[m]{u}\mathbf{N}(\mathfrak{n})^{1/2}x = 2\pi\sqrt{D}\left(g_1(\sqrt[m]{u})^{-2q}\sqrt{N_2} + g_2(\sqrt[m]{u})^{1+2q}\sqrt{N_1}\right)$ and so the number of totally positive ν in this coset such that $M + rx \leq T < M + (r+1)x$ is at most

$$\frac{\sqrt{D}\,\sqrt[m]{u}\mathbf{N}(\mathfrak{n})^{1/2}x}{(2\pi)^2}\,(M + (r+1)x) + 1$$

as required. □

Note that the bound above depends only on the value of x, which depends on g but not h. Thus for the moment we will treat the bounds as functions of x. We combine the last two propositions to give

Corollary 4.12. If x is as defined in the previous proposition, then the sum of the terms in (4.9) corresponding to totally positive $\nu \in ((\sqrt[m]{u})^{2q}, (\sqrt[m]{u})^{-2q})\,\delta^{-1}$ where $T = 2\pi\left(\nu_1/\sqrt[m]{u}\sqrt{N_1} + \nu_2/\sqrt{N_2}\right) \geq M$ is bounded in modulus by

(4.12)
$$\frac{e^{-M}}{(2\pi)^2(1-e^{-x})}\left(\left(K_2 + M + \frac{x}{1-e^{-x}}\right)\left(1 + MK_1x + \frac{K_1x^2}{1-e^{-x}}\right) + K_1\frac{x^3e^{-x}}{(1-e^{-x})^2}\right)$$

where $K_1 = \sqrt{D}\,\sqrt[m]{u}\mathbf{N}(\mathfrak{n})^{1/2}$ and $K_2 = 1 + (2\pi)^2(\sqrt[m]{u} + (\sqrt[m]{u})^{-1})/D\mathbf{N}(\mathfrak{n})^{1/2}$.

Proof. We see from Proposition 4.11 that we may bound the number of totally positive $\nu \in ((\sqrt[m]{u})^{2q}, (\sqrt[m]{u})^{-2q})\,\delta^{-1}$ where $M + rx \leq T < M + (r+1)x$ by $K_1x(2\pi)^{-2}\,(M + (r+1)x) + 1$, and by Proposition 4.9 we know that for those ν such that T is in this range, the term in ν of (4.9) is bounded by $(K_2 + (M + (r+1)x))e^{-(M+rx)}$, so the sum of the terms in (4.9) with totally positive ν in this coset of δ^{-1} with $T \geq M$ is bounded in modulus by

$$\frac{e^{-M}}{(2\pi)^2}\sum_{r=0}^{\infty} e^{-rx}\,(K_2 + M + (r+1)x)\,((M + (r+1)x)K_1x + 1) =$$
$$\frac{e^{-M}}{(2\pi)^2(1-e^{-x})}\left(\left(K_2 + M + \frac{x}{1-e^{-x}}\right)\left(1 + MK_1x + \frac{K_1x^2}{1-e^{-x}}\right) + K_1\frac{x^3e^{-x}}{(1-e^{-x})^2}\right)$$

as required. □

This corollary gives a bound which depends only on x, so the obvious question is for what value of x is this bound optimal, and since we cannot specify x exactly, what is the most appropriate choice of range so that we can guarantee to find a permissible x in this range, and so that the bound is close to optimal for all x in this range. Now M, K_1 and K_2 do not depend on g or x, so very basic analysis says that the bound is optimal when x is small but x not too small. Our choice of range is actually determined by the following theorem.

Theorem 4.13. *There is a totally positive $g \in \delta^{-1}$ which satisfies the conditions in Proposition 4.11 for some h, such that if as before we set $x = 2\pi\left(g_1/(\sqrt[n]{u})^{1+2q}\sqrt{N_1} + g_2/(\sqrt[n]{u})^{-2q}\sqrt{N_2}\right)$, then $4\pi/(\sqrt{D}\sqrt[n]{u}\mathbf{N}(\mathfrak{n})^{1/2}) \leq x \leq 2\pi$.*

Proof. To show we can find such a g we use various properties of continued fractions. The following lemma establishes the required properties.

Lemma 4.14. Let $z = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \mod 4$ and $z = \sqrt{d}$ otherwise. Define $z_0 = z$, $p_0 = 1$ and $q_0 = 0$, and by induction define $z_r = 1/(z_{r-1} - \lfloor z_{r-1} \rfloor)$. Then there are coprime integers p_r and q_r so that $p_r - zq_r = -(p_{r-1} - zq_{r-1})/z_r$. Moreover if we set $y_r = p_r - zq_r$, and $c_r = (-1)^r\mathbf{N}(y_r)$, then $0 < c_r < \sqrt{D}$,

$$z_r = \frac{\sqrt{D} + \sqrt{D - 4c_rc_{r-1}}}{2c_r} = \frac{2c_{r-1}}{\sqrt{D} - \sqrt{D - 4c_rc_{r-1}}}$$

and $(-1)^r y_r \downarrow 0$ and $\overline{y_r}$ increases as $r \to \infty$. Also $\{y_r, y_{r+1}\}$ is a $\mathbb{Z}$ -basis for $\mathcal{O}_k$.

Proof. $-(p_0 - zq_0)/z_1 = -(1)(z_0 - \lfloor z_0 \rfloor) = \lfloor z_0 \rfloor - z$, so $p_1 = \lfloor z_0 \rfloor$ and $q_1 = 1$. Note $p_1q_0 - q_1p_0 = -1$. Now by induction,

$$\begin{aligned} -(p_{r-1} - zq_{r-1})/z_r &= (p_{r-1} - zq_{r-1})(\lfloor z_{r-1} \rfloor - z_{r-1}) \\ &= (p_{r-1} - zq_{r-1})\lfloor z_{r-1} \rfloor + (p_{r-2} - zq_{r-2}) \end{aligned}$$

so $p_r = \lfloor z_{r-1} \rfloor p_{r-1} + p_{r-2}$, $q_r = \lfloor z_{r-1} \rfloor q_{r-1} + q_{r-2}$ and thus $p_rq_{r-1} - q_rp_{r-1} = -(p_{r-1}q_{r-2} - q_{r-1}p_{r-2}) = (-1)^r$ so p_r and q_r are coprime integers. c_r is positive since

z_r is positive and so by induction $(-1)^r y_r$ is positive, and since $c_r = (-1)^r y_r(p_r - \overline{z}q_r)$, where $(p_r - \overline{z}q_r)$ is positive.

The next part is mostly algebraic manipulation. Assume $d \not\equiv 1 \mod 4$ (the other case is similar). Then

$$z_r = \frac{-(p_{r-1} - \sqrt{d}q_{r-1})(p_r + \sqrt{d}q_r)}{(-1)^r c_r} = \frac{1}{2c_r}\left(\sqrt{D} + (-1)^r 2(q_r q_{r-1} d - p_r p_{r-1})\right)$$

and $4(q_r q_{r-1} d - p_r p_{r-1})^2 = D - 4c_r c_{r-1}$, so the only thing to verify is the sign of the final term. But if $z_r = \left(\sqrt{D} - \sqrt{D - 4c_r c_{r-1}}\right)/2c_r$, then as $z_r > 1$

$$\frac{\sqrt{D}}{2c_r} \geq \frac{\sqrt{D} - \sqrt{D - 2c_r c_{r-1}}}{2c_r} > 1 \text{ and } 1 < \frac{2c_{r-1}}{\sqrt{D} + \sqrt{D - 2c_r c_{r-1}}} < \frac{2c_{r-1}}{\sqrt{D}}$$

so $2c_r > \sqrt{D}$ and $2c_{r-1} > \sqrt{D}$. But this is impossible because $D \geq 4c_r c_{r-1}$. Hence we have the required expressions for z_r, and $c_r < \sqrt{D}$ because $2\sqrt{D}/2c_r > z_r > 1$. Thus z_r takes only finitely many values as c_r and c_{r-1} do, so $z_r \geq B > 1$ for some B and so by induction $0 < (-1)^r y_r < B^{-r} \to 0$ as $r \to \infty$, and y_r decreases as r increases because $z_r > 1$. It is clear that $\overline{y_r}$ increases as r increases, since p_r and q_r do and $-\overline{z}$ is positive.

Finally as $y_{r+1} = \lfloor z_r \rfloor y_r + y_{r-1}$, it is clear that y_r and y_{r+1} generate the same subgroup as y_{r-1} and y_r, and hence by induction as $y_0 = 1$ and $y_1 = \lfloor z \rfloor - z$, that is as 1 and z, but these generate $\mathcal{O}_k$ as a $\mathbb{Z}$ -basis. □

We apply this immediately as follows:

Lemma 4.15. Suppose $w_1 > w_2 > 0$ and $w_1 w_2 \leq 1/D$. Then there is a totally positive $y \in \mathcal{O}_k$ with

$$y w_1 + \overline{y} w_2 \leq 1$$

and $y' \in \mathcal{O}_k$ such that $\{y, y'\}$ is a $\mathbb{Z}$ -basis for $\mathcal{O}_k$.

Proof. Consider the y_r obtained in the previous lemma. $y_0 = \overline{y_0} = 1$ and $(-1)^r y_r$ decreases and $\overline{y_r}$ increases as r increases, so there is a greatest even r such that

$y_r w_1 > \overline{y_r} w_2$. If $y_r w_1 + \overline{y_r} w_2 \leq 1$ taking $y = y_r$ and $y' = y_{r+1}$ gives the result, so assume not. Then

$$1 < y_r w_1 + \overline{y_r} w_2 \leq y_r w_1 + \frac{c_r}{D y_r w_1}$$

so solving the quadratic equation in $y_r w_1$ gives

$$y_r w_1 > \frac{\sqrt{D} + \sqrt{D - 4c_r}}{2\sqrt{D}} \text{ or } y_r w_1 < \frac{\sqrt{D} - \sqrt{D - 4c_r}}{2\sqrt{D}}$$

but the latter is impossible because of our choice of y_r, since it would imply that $y_r w_1 \leq \frac{1}{2}$. Now $y_{r+2} = y_r / x_{r+1} x_{r+2}$ so

$$y_{r+2} w_1 > \frac{\sqrt{D} + \sqrt{D - 4c_r}}{2\sqrt{D}} \left(\frac{\sqrt{D} - \sqrt{D - 4c_{r+2} c_{r+1}}}{\sqrt{D} + \sqrt{D - 4c_{r+1} c_r}} \right) \geq \frac{\sqrt{D} - \sqrt{D - 4c_{r+2}}}{2\sqrt{D}}$$

as $c_{r+1} \geq 1$. But then by choice of y_r

$$y_{r+2} w_1 < \overline{y_{r+2}} w_2 \leq \frac{c_{r+2}}{D y_{r+2} w_1} < \frac{\sqrt{D} + \sqrt{D - 4c_{r+2}}}{2\sqrt{D}}$$

and so combining these two expressions for $y_{r+2} w_1$ in a quadratic equation gives

$$y_{r+2} w_1 + \overline{y_{r+2}} w_2 \leq y_{r+2} w_1 + \frac{c_{r+2}}{D y_{r+2} w_1} < 1$$

so we can take $y = y_{r+2}$ and $y' = y_{r+3}$. □

The required result is now almost a direct consequence of this lemma. Choose an integer s so that $u^{2s+1} / (\sqrt{D} (\sqrt[m]{u})^{1+2q} \sqrt{N_1}) > u^{-2s-1} / (\sqrt{D} (\sqrt[m]{u})^{-2q} \sqrt{N_2})$. Set

$$w_1 = \frac{u^{2s+1}}{\sqrt{D} (\sqrt[m]{u})^{1+2q} \sqrt{N_1}} \quad \text{and} \quad w_2 = \frac{u^{-2s-1}}{\sqrt{D} (\sqrt[m]{u})^{-2q} \sqrt{N_2}}$$

and observe that $w_1 w_2 = 1/(D \sqrt[m]{u} \mathbf{N}(\mathfrak{n})^{1/2}) \leq 1/D$, so there is a totally positive $y \in \mathcal{O}_k$ such that $u^{2s+1} y / (\sqrt{D} (\sqrt[m]{u})^{1+2q} \sqrt{N_1}) + u^{-2s-1} \overline{y} / (\sqrt{D} (\sqrt[m]{u})^{-2q} \sqrt{N_2}) < 1$, and a $y' \in \mathcal{O}_k$ such that $\{y, y'\}$ is a $\mathbb{Z}$ -basis for $\mathcal{O}_k$.

But there is an element $t \in \delta^{-1}$ such that $i_1(t) = u^{2s+1}/\sqrt{D}$ and $i_2(t) = u^{-2s-1}/\sqrt{D}$. Clearly t is totally positive and generates δ^{-1} as a $\mathcal{O}_k$-module. Therefore if $g = ty$, then $g \in \delta^{-1}$ is totally positive, and $x = 2\pi \left(g_1 / (\sqrt[m]{u})^{1+2q} \sqrt{N_1} \right.$

$+g_2/(\sqrt[m]{u})^{-2q}\sqrt{N_2}\Big) \leq 2\pi$. Also by the AM-GM inequality, since g is totally positive, we have

$$x = 2\pi\left(g_1/(\sqrt[m]{u})^{1+2q}\sqrt{N_1} + g_2/(\sqrt[m]{u})^{-2q}\sqrt{N_2}\right)$$
$$\geq 4\pi\sqrt{\frac{\mathbf{N}(g)}{\sqrt[m]{u}\mathbf{N}(\mathfrak{n})^{1/2}}} \geq \frac{4\pi}{\sqrt{D}\sqrt[m]{u}\mathbf{N}(\mathfrak{n})^{1/2}}$$

Finally if $h = \pm ty'$ choosing the sign so that $g_1h_2 - g_2h_1 > 0$, then $\{g, h\}$ is a $\mathbb{Z}$ -basis for δ^{-1}. □

Finally, we are in a position to bound all terms with $T \geq M$.

Theorem 4.16. *The sum of all terms in equation (4.9) with totally positive $\nu \in \delta^{-1}(U_k^+)^{1/m}$ such that $T = 2\pi\left(\nu_1/\sqrt[m]{u}\sqrt{N_1} + \nu_2/\sqrt{N_2}\right) \geq M$ is bounded in modulus by*

(4.13)
$$\frac{e^{-M}m\sqrt[m]{u}\sqrt{D}\mathbf{N}(\mathfrak{n})^{1/2}}{2\pi(1-e^{-2\pi})}\left(1+(M+8)\left(M+8+\frac{(2\pi)^2(\sqrt[m]{u}+(\sqrt[m]{u})^{-1})}{D\mathbf{N}(\mathfrak{n})^{1/2}}\right)\right)$$

Proof. By Corollary 4.12 we know that, for x as in the corollary, the sum of the terms for $\nu \in ((\sqrt[m]{u})^{2q}, (\sqrt[m]{u})^{-2q})\,\delta^{-1}$ with $T \geq M$ is bounded in modulus by (4.12), that is by

$$\frac{e^{-M}}{(2\pi)^2(1-e^{-x})}\left(\left(K_2+M+\frac{x}{1-e^{-x}}\right)\left(1+MK_1x+\frac{K_1x^2}{1-e^{-x}}\right)+K_1\frac{x^3e^{-x}}{(1-e^{-x})^2}\right)$$

where $K_1 = \sqrt{D}\sqrt[m]{u}\mathbf{N}(\mathfrak{n})^{1/2}$ and $K_2 = 1+(2\pi)^2(\sqrt[m]{u}+(\sqrt[m]{u})^{-1})/D\mathbf{N}(\mathfrak{n})^{1/2}$. Now observe (for example by comparing derivatives) that

$$1-e^{-x} \geq \left(\frac{1-(1+\pi)e^{-2\pi}}{\pi}\right)x - \left(\frac{1-(1+2\pi)e^{-2\pi}}{4\pi^2}\right)x^2$$

for $0 \leq x \leq 2\pi$ with equality at $x = 2\pi$. Thus

$$(4.12) \leq \frac{e^{-M}}{(2\pi)^2}\left(\frac{(K_2+M+7)(1+MK_1x+7K_1x)}{1-e^{-2\pi}}+1.7K_1\right)$$
$$\leq \frac{e^{-M}}{(2\pi)^2}\left(\frac{4\pi^2(K_2+M+7)(1+MK_1x+7K_1x)}{4\pi(1-(1+\pi)e^{-2\pi})x-(1-(1+2\pi)e^{-2\pi})x^2}+1.7K_1\right)$$

for $0 < x \leq 2\pi$. But by comparing this with the value at $x = 2\pi$, this is at most

$$\frac{e^{-M}}{(2\pi)^2}\left(\frac{(K_2+M+7)(1+2\pi K_1(M+7))}{1-e^{-2\pi}}+2K_1\right)$$
$$\text{if } \left(\frac{2\pi(1-e^{-2\pi})}{(1-(1+2\pi)e^{-2\pi})(1+2\pi K_1(M+7))}\right) \leq x \leq 2\pi$$

which is certainly true if $4\pi/K_1 \leq x \leq 2\pi$. But by Theorem 4.13 precisely such an x exists, and hence, combining all the cosets of δ^{-1} and simplifying we deduce that the sum of those terms with $T \geq M$ is bounded in modulus by

$$\frac{e^{-M}m\sqrt[m]{u}\sqrt{D}\mathbf{N}(\mathfrak{n})^{1/2}}{2\pi(1-e^{-2\pi})}\left(1+(M+8)\left(M+8+\frac{(2\pi)^2(\sqrt[m]{u}+(\sqrt[m]{u})^{-1})}{D\mathbf{N}(\mathfrak{n})^{1/2}}\right)\right)$$

as required. □

In practice, we will want to know how big to choose M so that this is less than a given value, L say. But if M_0 is a good approximation to M then a good approximation to $M^2 + AM + B$ is

$$\left(M_0^2+AM_0+B\right)e^{(M-M_0)(2M_0+A)/(M_0^2+AM_0+B)}$$
$$\geq (M^2+AM+B)+(M-M_0)^2\left(1+\frac{A^2-4B}{2(M_0^2+AM_0+B)}\right) \geq M^2+AM+B$$

provided $1+(A^2-4B)/2(M_0^2+AM_0+B) > 0$. In our case this is certainly satisfied if $M_0 > 0$. So to determine M set

(4.14)

$$M_0 = \ln\left(\frac{m\sqrt[m]{u}\sqrt{D}\mathbf{N}(\mathfrak{n})^{1/2}}{2\pi(1-e^{-2\pi})L}\right) \qquad K_3 = 2M_0+16+\frac{(2\pi)^2(\sqrt[m]{u}+(\sqrt[m]{u})^{-1})}{D\mathbf{N}(\mathfrak{n})^{1/2}}$$
$$K_4 = 1+(M_0+8)\left(M_0+8+\frac{(2\pi)^2(\sqrt[m]{u}+(\sqrt[m]{u})^{-1})}{D\mathbf{N}(\mathfrak{n})^{1/2}}\right) \qquad M = M_0+\frac{\ln K_4}{1-K_3/K_4}$$

This will give a close approximation to M if M is close to M_0, that is if $\ln K_4$ is small compared with M_0. But this will be the case if L is reasonably small.

Note that the value of M that (4.14) gives turns out in practice to be significantly bigger than it need be. This is probably because some of the approximations used to give a reasonably simple result are fairly loose for some terms. Note also

that the bound assumes that the individual terms are calculated to sufficient accuracy to make the error from this source negligible.

It is also useful to know the number of terms that this bound leaves us to calculate. But by (4.11) the number of terms required in each coset is

$$\sum_{r=1}^{\lceil M/x\rceil}\left(rx^2 2\pi\sqrt{D}\,\sqrt[m]{u}\mathrm{N}(\mathfrak{n})^{1/2}+1\right)=x^2\sqrt{D}\,\sqrt[m]{u}\mathrm{N}(\mathfrak{n})^{1/2}\frac{1}{2}\left\lceil\frac{M}{x}\right\rceil\left(\left\lceil\frac{M}{x}\right\rceil+1\right)+\left\lceil\frac{M}{x}\right\rceil$$
$$\leq\frac{\sqrt{D}}{2}\sqrt[m]{u}\mathrm{N}(\mathfrak{n})^{1/2}(M+1)(M+2)+M\frac{\sqrt{D}\sqrt{\sqrt[m]{u}\mathrm{N}(\mathfrak{n})^{1/2}}}{4\pi}$$

Thus the total number of terms to be calculated is at most

$$\frac{1}{2}\sqrt{D}m\,\sqrt[m]{u}\mathrm{N}(\mathfrak{n})^{1/2}(M^2+4M+2) \tag{4.15}$$

This equation, (4.13), and (4.14) all suggest that the optimal choice of m is approximately that which minimizes $m\sqrt[m]{u}$, that is $m\approx\ln u$. However, the coefficients a_ν that need to be calculated will be those where $M>T=2\pi(\nu_1/\sqrt[m]{u}\sqrt{N_1}+\nu_2/\sqrt{N_2})$, that is for those ν where $\mathrm{N}(\nu)<\sqrt[m]{u}\mathrm{N}(\mathfrak{n})^{1/2}(M/4\pi)^2$. This bound for $\mathrm{N}(\nu)$ is roughly proportional to $\sqrt[m]{u}\ln(m\sqrt[m]{u})^2$ and the number of a_ν will be a monotonicly increasing function of this, and $\sqrt[m]{u}\ln(m\sqrt[m]{u})^2$ is minimal for $m>\ln u$, so the optimal value of m will be slightly bigger than $\ln u$, though precisely how much bigger will depend on what proportion of the time is taken by calculating the a_ν.

4.3 Implementation

This section will tidy up a few bits and pieces I haven't mentioned yet, and give some idea of how I programmed some of the above where I think it needs comment. One of the things I haven't mentioned yet is how to determine the sign w of the operator W_N in (4.2) and following equations. In fact guessing is a reasonable option, since there are only two choices, and the right one is the one which gives results consistent with the other calculations, or the one which gives the same

answer to appropriate precision when m is changed. But if we restrict attention to semi-stable elliptic curves, we can calculate w directly, assuming the curve comes from a Hilbert modular form (as we are already doing).

Lemma 4.17. Let f be a Hilbert modular cusp form over $\Gamma_0(\mathfrak{n})$ corresponding to an elliptic curve over a real quadratic field k with semi-stable reduction. Then the eigenvalue w of the operator W_N equals $\prod(-a_{\nu\xi})$, where each ν in the product generates a different prime ideal dividing $\mathfrak{n}$.

Proof. Recall that $W_N = \prod W_\nu$ where the product is over a set of ν which generate all the distinct prime ideals (ν) dividing $(\mathfrak{n})$. But if $(\mathfrak{n})$ is the product of distinct prime ideals (i.e. the conductor of the corresponding curve is squarefree, so the curve is semi-stable), then you can show that for any cusp form f on $\Gamma_0(\mathfrak{n})$, $\left(f\big|_{U_\nu}\big|_{W_\nu} + f\right)$ is a cusp form on $\Gamma_0(\mathfrak{n}/(\nu))$ (compare with [1]). So if f is a non-trivial common eigenfunction of the W_ν and the U_ν, then $\left(f\big|_{U_\nu}\big|_{W_\nu} + f\right)$ is a scalar multiple of f, and so either f is a cusp form on $\Gamma_0(\mathfrak{n}/(\nu))$ or $f\big|_{U_\nu}\big|_{W_\nu} = -f$.

The former case is impossible since the matrix in the definition of W_ν may be written as $\alpha\left(\begin{smallmatrix}\nu & 0\\ 0 & 1\end{smallmatrix}\right)$, where $\alpha \in \Gamma_0(\mathfrak{n}/(\nu))$, hence $f\big|_{W_\nu} = f\big|_{\left(\begin{smallmatrix}\nu & 0\\ 0 & 1\end{smallmatrix}\right)} = \pm f$, but then by comparing the fourier series of f and $f\big|_{\left(\begin{smallmatrix}\nu & 0\\ 0 & 1\end{smallmatrix}\right)}$, we can deduce that

$$\pm a_\lambda = \begin{cases} \mathrm{N}(\nu) a_{\lambda/\nu} & \text{if } \lambda \in (\nu\xi) \\ 0 & \text{otherwise} \end{cases}$$

and hence by induction that $f \equiv 0$.

But the latter implies that $w_\nu = -u_\nu$ where $f\big|_{U_\nu} = u_\nu f$ and $f\big|_{W_\nu} = w_\nu f$. However $u_\nu = a_{\nu\xi}$, and $w = \prod w_\nu$, so $w = \prod(-a_{\nu\xi})$ where the product is over a set of ν which generate the distinct prime ideals dividing $\mathfrak{n}$, as required. □

I haven't yet found a way of calculating w when the curve is not semi-stable, so any of my results which are in this case have been calculated by using the 'guess and check' method.

My programs use routines provided by the PARI package [6]. I decided that the easiest and most efficient way to implement the calculation of the L-series was first to calculate and store the values of $a_{\nu\xi}$ for sufficiently many generators ν of powers of prime ideals. This was done by calculating $a_{\nu\xi}$ for each prime ideal (ν), by counting points on the reduced elliptic curve, often by fairly crude methods, and then using the recurrence relation given by the product formula in Theorem 4.4 to calculate $a_{\nu\xi}$ for sufficiently many of those ν which generate powers of this prime ideal. Thus, again by Theorem 4.4, since $a_{\nu\xi}$ depends only on the ideal (ν), every $a_{\nu\xi}$ could be calculated by taking a product of stored values.

Next I calculated the terms of the L-series in order of increasing $\mathbf{N}(\nu)$ (that is $\mathbf{N}(\nu) = 1/D, \mathbf{N}(\nu) = 2/D, \ldots$) ignoring those which were too small. I did this because it allowed me to calculate together all the required terms with the same value of $a_{\nu\xi}$ by choosing a generator ν for each fractional ideal in δ^{-1} with the appropriate norm, and then evaluating all sufficiently large terms corresponding to ν multiplied by roots of units. Thus I only needed to evalute each value of $a_{\nu\xi}$ once. It was also easy to find each fractional ideal in δ^{-1} with a given norm, because each such fractional ideal is just ξ times an ideal of $\mathcal{O}_k$. Thus I considered in turn all possible ideals of $\mathcal{O}_k$ with norm 1,2,3, etc. by considering all possible products of prime ideals with this norm, and then calculating the corresponding terms.

I could have calculated w (at least in the semi-stable case) in terms of the $a_{\nu\xi}$ for those ν where bad reduction occurs. However in this case $a_{\nu\xi} = \pm 1$ where the sign depends on whether the reduction at (ν) is split or non-split multiplicative, and (for primes not above 2) this reduction may also be determined by seeing whether $-c_6$ is a quadratic residue or not with respect to this prime ideal (c_6 is the usual function of elliptic curve coefficients, see Silverman [21] for example). Thus w may be evaluated by evaluating the symbol $(-c_6/(\text{bad primes not above } 2))$ which is the natural generalization of the Legendre and Jacobi symbols to real quadratic

fields of narrow class number 1.

Chapter 5

Analysis of Results and Generalizations

This chapter assesses the results from my calculations of the linear dependencies between the L-series of a real quadratic elliptic curve at $s = 2$, and determinants of pairs of elements in the image of the regulator map, but first it explains how I obtained the lists of elliptic curves in the first part of Appendix B and how the information in the second set of tables is laid out. Finally there is a section for conclusions and suggestions on how this work might be extended.

5.1 Explanation of tables for curves over real quadratic fields

We now know how to calculate the L-series for an elliptic curve over a real quadratic field k (or at least conjecturally, and provided k has narrow class number 1). But first we need some curves. These will have to have a torsion group with order at least 5, because we are expecting the image of $K_2(E_{\mathcal{O}})$ to have rank 2, and thus we need at least two independent vectors from the v_P to stand a chance of having this image in the part of the image of the regulator map we are studying. And we

need at least 5 torsion points because $\mathbf{v}_P = 0$ if P has order 2, and $\mathbf{v}_P = -\mathbf{v}_{-P}$ for any $P \in T$.

Fortunately, there are 1-parameter families of elliptic curves with each such torsion group, provided the group is not too big, so it is easy to find examples.

So for example we have

Lemma 5.1. Every elliptic curve defined over $\mathcal{O}_k$ with 5-torsion, may be written in the form

$$y^2 + (r+s)xy + (rs^2)y = x^3 + (rs)x^2 \tag{5.1}$$

where (at least for quadratic fields) $r, s \in \mathcal{O}_k$, and this curve is in global minimal form if r and s are coprime.

Proof. Suppose we have an elliptic curve defined over $\mathcal{O}_k$ with a point of order 5 (over k). Change co-ordinates so that this point is at the origin and has tangent $y = 0$. Thus the curve has equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2$$

where $a_1, a_2, a_3 \in k$. For any equation of this form we have $-(0,0) = (0, -a_3)$ and $-2(0,0) = (-a_2, 0)$. The line joining these two points is $a_2y + a_3x + a_2a_3 = 0$. This intersects the curve when

$$\begin{aligned} 0 &= {a_2}^2x^3 + {a_2}^3x^2 - {a_3}^2(x+a_2)^2 + a_2a_3(a_1x + a_3)(x + a_2) \\ &= x(x+a_2)\left({a_2}^2x + a_3(a_1a_2 - a_3)\right) \end{aligned}$$

but because $(0,0)$ has order 5, the line is tangent to the curve at $x = -a_2$, and so

$$-{a_2}^3 + a_1a_2a_3 - {a_3}^2 = 0$$

and thus if we set $r = {a_2}^2/a_3$ and $s = a_3/a_2$ we get the above equation. If we express the usual elliptic curve qualities c_4 and Δ as homogeneous polynomials in r and s, we see by polynomial manipulation that as fractional ideals

$$125\,(r,s)^{23} \subset \left(\Delta, {c_4}^3\right)(r,s)^{11}$$

But the original curve was defined over $\mathcal{O}_k$ and so we have $\Delta, {c_4}^3 \in \mathcal{O}_k$ as these have not changed, so $125\,(r,s)^{12} \subset \mathcal{O}_k$, and as (125) is not contained in the twelfth power of any prime ideal when k is quadratic (or rational), we deduce that $r, s \in \mathcal{O}_k$. Moreover if r and s are coprime, then $(125) \in (\Delta, {c_4}^3)$ and thus the curve is in global minimal form because (125) is not contained in the twelfth power of any prime ideal and so the curve is minimal for each prime ideal. □

There are similar results giving equations for curves with larger torsion groups, but we don't always have the stronger condition that the resulting curve is minimal. This does not however provide many problems since it will only fail to be minimal for very small prime ideals and because we assume narrow class number one, it is still easy to find a global minimal equation.

Observe that if we replace y with $u^{-3}y$ and x in equation (5.1), with $u^{-2}x$, we get the equation

$$y^2 + u(r+s)xy + u^3(rs^2)y = x^3 + u^2(rs)x^2$$

so we are in effect replacing (r,s) by (ur,us). This transformation does change the real periods of the two embeddings of the elliptic curve into $\mathbb{C}$ (each real period is divided by the appropriate embedding of u in $\mathbb{R}$) but it does not affect the normalized lattices for each embedding $k \to \mathbb{C}$. Hence the curves corresponding to (r,s) and (ur,us) are really the same, and so the curve is parameterized by the 1-dimensional projective coordinates $[r:s]$. But note that if u is a unit, the coordinates (r,s) and (ur,us) give us alternate global minimal forms for the curve, and it may not be apparent from the equations of these two global minimal forms that they are in fact the same.

The 5-torsion points of the curve (5.1) are $(0,0)$, $(-rs,r^2s)$, $(-rs,0)$, and $(0,-rs^2)$, and if we change co-ordinates in turn so that each each point is mapped to $(0,0)$ with tangent $y=0$ we get the curves corresponding to the projective co-ordinates $[r:s]$, $[s:-r]$, $[-s:r]$ and $[-r:-s]$ respectively, so $[r:s] = [-r:-s]$

and $[s : -r] = [-s : r]$ all give the same curve. Thus only one such curve is listed in my tables.

It is also fairly easy to see from the form of the torsion points that, assuming there are no extra torsion points, the primes where there is non-trivial split multiplicative reduction are precisely those which divide r and s. Moreover $(0, 0)$ lies on the fibres corresponding to $\pm\mathbf{B}_3(\frac{2}{5})$ for each prime dividing r, and on the fibres corresponding to $\pm\mathbf{B}_3(\frac{1}{5})$ for each prime dividing s. Thus m' is 0 if both r and s are units, 1 if only one is a unit, and 2 otherwise.

The tables of 5-torsion points which start Appendix B were obtained by listing all the curves with 5-torsion with sufficiently small r and s and sorting those with small enough conductor into isogeny classes (and adding any obvious missing isogenous curves), discarding the multiple copies of each curve as described above, for each of the fields $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{13})$. It is followed by tables of 6-torsion curves and 7-torsion curves for the same fields, the curves being obtained by using the same sort of methods as above. Note that these tables are by no means guaranteed to be complete. I do not claim to have found every isogeny and every conductor in the range considered.

The entries in each such table indicates the conductor of the curve, a label in the style of Cremona with a letter indicating the isogeny class of the curve and a number to distinguish curves (however unlike Cremona's tables the first curve in each isogeny class need not be a strong Weil curve, since it is not clear that such a concept exists for curves over real quadratic fields, and even if it does, we are only considering curves with a given torsion subgroup and this may not include any strong Weil curve in an isogeny class). Note that I haven't calculated the L-series corresponding to every curve listed in these tables. This is partly due to lack of time, and partly because my program started running out of memory space for curves with larger conductors, for the precision of the L-series I was working at.

After this first set of tables, there are further tables which first list linear depen-

dencies amongst the vectors $\mathbf{v}_P$ which consist of components $(\pi \mathrm{Im}(\tau))^2 K_1(0, P_\sigma, 2)$ for each real embedding $\sigma\colon k \to \mathbb{C}$, where P_σ is on the normalized lattice Λ_σ. Note that the columns of this table are indexed by the actual points P unlike the rational tables. This is because it will often be the case that P embeds at different points on the normalized lattices, which of course need not be the same anyway. The second set of columns show linear dependencies between determinants of matrices consisting of pairs of these vectors $\mathbf{v}_P$. The columns are labelled with entries of the form '$\det_{12}$' by which I mean the determinant of the matrix whose columns correspond to the first and second points listed in the first part of the table. For example,

Curve	m'	P	$2P$	$3P$	$4P$	$\det_{23}$	$\det_{24}$	$\det_{34}$	L
6A1	0	2	-4	-2	1		-5		9
		2	1	2	4				

indicates that for the curve 6A1 (over $\mathbb{Q}(\sqrt{5})$), if P is the point of order 10 such that 2P=(0,0), then

$$-2\mathbf{v}_P + 4\mathbf{v}_{2P} + 2\mathbf{v}_{3P} - 1\mathbf{v}_{4P} = 0 \qquad \text{and} \qquad 2\mathbf{v}_P + 1\mathbf{v}_{2P} + 2\mathbf{v}_{3P} + 4\mathbf{v}_{4P} = 0$$

and also

$$-5 \det(\mathbf{v}_{2P} \mid \mathbf{v}_{4P}) + 9L(E, 2) = 0$$

These linear dependencies are of course only established numerically, so it is not proven that such dependencies exist, merely that the linear combinations listed give a very small result. However in all the cases I checked the dependencies are correct to at least 50 decimal places, and the error is of the sort of magnitude explainable by approximations made in calculation.

Note that there is only one entry in the results tables for each pair of conjugate curves, since these are the same except that the real embeddings of k have been exchanged, and hence the linear dependencies will be the same, apart from a minus sign in the determinants. Such pairs of curves will occur when the conductor is

not rational, and we get one curve corresponding to the conductor, and one to its conjugate. If the conductor of a curve is rational, or generates an ideal that is fixed by conjugation, then the conjugate of the curve can either be an isogeny of the original curve, or the same curve after multiplying by units. For example over $\mathbb{Q}(\sqrt{5})$ in the 6-torsion table, x+7A1 is the conjugate of -x+8A1, and 4x+8A2 is the conjugate of 4x+8A3.

Finally a word of caution. Whereas most of my rational results where done by passing files directly from one computer program to another and have been fairly carefully checked where this was not true, in the quadratic case more of the calculations have been done by programs with manually entered data, and the tables have been manually typed. Thus although I don't know of any errors, I would be the first to admit that the probability that there is some minor slip, in particular an errant minus sign, is probably quite high.

5.2 Analysis of results for real quadratic fields

The first thing to observe is that we do in fact have some results, i.e. there are linear dependencies (up to expected calculation error) between the determinants of pairs of elements of the image of the regulator map and the L-series at $s = 2$ for various elliptic curves. Thus something along the lines of Beilinson's conjecture must be true, and unless we are the victim of an extraordinary coincidence, all the elliptic curves where we get such linear dependencies are modular, because of the way we calculate the L-series.

The clearest aspect of the results is that the dimensions of the various parts that make up the image of the regulator map are what we would expect from what has been said so far. Thus when there is some linear dependency between the L-series and the determinants from elements making up the image of the regulator map, we find that the dimension over $\mathbb{Q}$ of the image of the regulator map (from the

part of $K_2(E_k)$ we consider) minus m', the number of distinct split multiplicative reductions of E is exactly 2, and if there isn't any linear dependency, the dimension minus m' is 1 or zero. Moreover, whenever we would expect from the value of m' that there might be some linear dependency between the determinants and the L-series there is such a relation, except when the curve is rational and all the points over k are in fact over $\mathbb{Q}$. In this latter case, the two real embeddings are identical so all the $\mathbf{v}_P$ are real multiples of $(1,1)^T$, but the $\mathbb{Q}$-dimension minus m' is always 1 or 0 anyway because of what happens in the rational case. These results again suggests that the regulator map is injective.

Thus as we have stated it, Beilinson's conjecture holds numerically in the cases we would expect to be able to verify via this method. But the results still have something to say on the form of the linear dependency involved.

Having said that, the evidence from the quadratic case is less clear than the rational case, simply because things are more complicated, since linear dependencies between the $\mathbf{v}_P$ correspond to quadratic dependencies between the determinants. Thus for example it is harder to say whether the dependencies do in fact correspond to the conditions which the image of $K_2(E_{\mathcal{O}})$ should satisfy because of the various split multiplicative reductions. The easiest such case to check is where we have the torsion group C_7 (in the cases of C_5 and C_6 we must have $m' = 0$ to have any dependency between the L-series and the determinants). Assume we are considering a curve with torsion group C_7, and where $P = (0,0)$ maps onto the fibre corresponding to $\pm\mathbf{B}_3(\frac{1}{7})$ under split multiplicative reduction for all primes where split multiplicative reduction occurs. Then for an element $a\mathbf{v}_P + b\mathbf{v}_{2P} + c\mathbf{v}_{3P} \in \mathrm{Im}R$ to be in the image of $K_2(E_{\mathcal{O}})_{\mathbb{Q}}$ we must have $5a + 5b + 2c = 0$, hence the image of $K_2(E_{\mathcal{O}})_{\mathbb{Q}}$ is generated by $\mathbf{v}_P - \mathbf{v}_{2P}$ and $2\mathbf{v}_{2P} - 5\mathbf{v}_{3P}$. Thus the L-series should be a rational multiple of

$$\det(\mathbf{v}_P - \mathbf{v}_{2P} \mid 2\mathbf{v}_{2P} - 5\mathbf{v}_{3P}) = 2\det_{12} - 5\det_{13} + 5\det_{23}$$

and the other possible split multiplicative reductions should be (up to the sign of

each term) a permutation of this. This is precisely what does occur in the curves with torsion group C_7.

For larger torsion groups there are more cases to consider as there are more types of split multiplicative reduction, and there may be linear dependencies between the $\mathbf{v}_P$, and these don't seem to fit into any pattern from one curve to the next. Nevertheless, if we just look for linear dependencies of the L-series and the determinants formed from the minimal number of $\mathbf{v}_P$ likely to give a result (i.e. $2+m'$ of them), this makes things as simple as possible, and it is possible to check that the linear dependencies obtained do correspond to the determinant of a pair of vectors made up of the $\mathbf{v}_P$ which satisfy the linear dependencies imposed by the split multiplicative reductions.

However there is sometimes a further complication, namely extra linear dependencies between the determinants for some of these larger groups. These seem to arise when some of the E-K-L series in the two different embeddings $k \to \mathbb{C}$ are in fact the same. This will be the case when the two embeddings give the same normalized lattice, and so the E-K-L series from one embedding will be a permutation of those from the other, and this quite often leads to pairs of determinants being equal up to sign, or in the case of curves which are in fact rational curves, to pairs of parallel $\mathbf{v}_P$. For this sort of situation I have only listed the dependencies in the case where they they do not obviously fit into this pattern (i.e. for the curve 6A2 over $\mathbb{Q}(\sqrt{13})$).

There is one more interesting case, namely the curve 6A3 over $\mathbb{Q}(\sqrt{13})$. In this case one of the embeddings gives a normalized lattice which has index 4 in the other normalized lattice, and whereas I haven't fully explained the dependencies in this case, I do observe that if we look for linear dependencies between all the E-K-L series from both embeddings, we do find linear dependencies, and at least some are explained because they correspond (up to a factor of $\sqrt{2}$) to E-K-L series in the lattice between the two under consideration (namely the relations

$2(\mathbf{v}_P - \mathbf{v}_{4P})_2 = (\mathbf{v}_{2P} - \mathbf{v}_{3P})_1$ and $-2(\mathbf{v}_{2P} - \mathbf{v}_{3P})_2 = (\mathbf{v}_P - \mathbf{v}_{4P})_1$).

As well as checking that the linear dependencies are consistent with the predicted form, we can also look at some of the factors involved in any linear dependency between determinants of the $\mathbf{v}_P$, and the L-series. Recall in the rational case we had the equation

$$c_1 |T| \sum_{P \in T} a_P K_1(0, P, 2) + c_2 NL(E, 2) = 0$$

where the a_P were coprime. From the results I conclude that the corresponding equation in the quadratic case is probably

$$c_1 |T|^3 \sum_{i,j} a_{ij} \det{}_{ij} + c_2 \mathrm{N}(\mathfrak{n}) D^2 L(E, 2) = 0 \tag{5.2}$$

where the a_{ij} have no common factors, $\mathrm{N}(\mathfrak{n})$ is the norm of the conductor, and D is the discriminant of the quadratic field.

The results are in fact rather ambiguous about the power of $|T|$ which should appear in this equation, as you can also argue that $|T|^2$ should replace $|T|^3$. This would reduce the number of factors in the various values of c_2, but introduce extra factors into various of the values of c_1. However, if we recall what happened in the rational case, we saw there that c_2 tended to have stray factors for smaller conductors, and c_1 tended to have stray factors only for larger values. This is most consistent with the above choice of power of $|T|$.

Even if we assume the above equation, the true values of c_1 and c_2 are not as obvious as they at first might seem, because for simplicity and to save space, I have only listed linear combinations between the L-series, and the least number of determinants which could be expected to give a result considering the linear combinations that exist between the $\mathbf{v}_P$. However it is often possible to use these linear combinations to cancel factors of c_2 and increase c_1. The true case to consider is when we maximize c_1 and minimize c_2 because this corresponds to finding generators for the whole $\mathbb{Z}$-lattice which is the image of $\mathrm{K}_2(E_O)_{\mathbb{Q}}$ in $\mathrm{K}_2(E_k)$ (or more precisely the image of this under the regulator map).

For example, consider the curve 6A1 over $\mathbb{Q}(\sqrt{5})$ which has torsion group C_{10}, we have

$$-5\det_{24} + 9L(E,2) = 0$$

which suggests that $c_1 = 1$ and $c_2 = 2$. However, we can deduce from the linear dependencies on the $\mathbf{v}_P$ that $5\det_{24} + 4\det_{34} = 0$ and $10\det_{13} - 17\det_{34} = 0$ from which we can deduce that $-5\det_{24} = 120\det_{13} - 200\det_{34}$ so in fact we actually have

$$120\det_{13} - 200\det_{34} + 9L(E,2) = 0$$

so in fact we really have $c_1 = 4$ and $c_2 = 1$. Note that we have to ensure that this does actually correspond to the determinant of appropriate combinations of the $\mathbf{v}_P$. In this case we have

$$-120\det_{13} + 200\det_{34} = 40\det(\mathbf{v}_3 \mid 3\mathbf{v}_1 + 5\mathbf{v}_4)$$

On the other hand we could have equally obtained the equation

$$40\det_{13} + 80\det_{24} + 9L(E,2) = 0$$

which does not arise as a determinant.

The above example is made easier because $m' = 0$. When m' is not zero, we must also ensure that all the linear combinations of determinants we obtain arise from a determinant of combinations of $\mathbf{v}_P$ which satisfy the conditions imposed by split multiplicative reduction.

Tables 5.1 to 5.3 give the real values of c_1 and c_2 I obtained in the curves where a linear relation between determinants and the L-series exists over each field.

Note that c_1 consists only of factors of 2 and also factors of 3 if 3 divides $|T|$, though this is partly ensured by the way I choose the power of $|T|$ to put in equation (5.2). However c_2 is less well behaved, quite often containing extra factors from the number of torsion points, or the norm of the conductor, or the

Curve	c_1	c_2	$\lvert T\rvert$	Curve	c_1	c_2	$\lvert T\rvert$	Curve	c_1	c_2	$\lvert T\rvert$
7A1	16	5	5	2x+14A1	2	5	10	9A1	2	3	6
2x+8A1	16	5	5	2x+14A2	4	5	10	9A3	4	3	6
10B1	16	1	5	10A1	12	25	15	x+7A1	3	2	12
10B2	2	1	5	x+7A2	2	1	6	4x+8A1	3	2	12
2x+10A1	16	1	5	x+7A3	6	11	6	x+6A1	1	1	7
3x+13A1	16	5	5	x+7A4	6	25	6	2x+10A1	8	35	7
15B1	16	1	5	x+8A1	2	1	6	3x+11A1	16	133	7
22A1	16	1	5	x+8A2	2	1	6	3x+24A1	8	21	7
6A1	4	1	10	4x+8A2	3	4	6	11x+27A1	16	7	7
6A2	1	1	10								

Table 5.1: c_1 and c_2 for curves over $\mathbb{Q}(\sqrt{5})$

Curve	c_1	c_2	$\lvert T\rvert$	Curve	c_1	c_2	$\lvert T\rvert$	Curve	c_1	c_2	$\lvert T\rvert$
4x+11A1	8	1	5	3x+12A2	1	5	10	7A1	4	1	6
13A1	32	1	5	2x+5A1	2	3	6	2x+6A4	3	2	12
3A1	4	1	10	2x+5A2	4	3	6	2x+6A1	3	1	12
3A2	2	1	10	2x+6A2	6	11	6	x+10A1	2	7	7
x+8A1	2	5	10	2x+6A3	3	2	6	x+10A2	16	7	7
x+8A2	2	5	10	x+6A1	3	2	6	x+12A1	4	7	7
3x+12A1	1	5	10	x+6A2	3	4	6	x+16A1	16	7	7

Table 5.2: c_1 and c_2 for curves over $\mathbb{Q}(\sqrt{2})$

discriminant of the field. But there are other extra factors, like a factor of 19 in curve 3x+11A1 over $\mathbb{Q}(\sqrt{5})$, or 31 in curve 2A1 over $\mathbb{Q}(\sqrt{2})$. But of course extra factors in c_2 are probably just because our method doesn't consider all of $\mathrm{K}_2(E_k)$. There are no stray factors in c_1 but by analogy with the rational case, I suspect this is because we have not calculated any curves with big enough conductor.

Curve	c_1	c_2	$\lvert T\rvert$	Curve	c_1	c_2	$\lvert T\rvert$
2A1	16	31	5	6A3	2	45	10
2A2	2	1	5	6A2	1	10	20
6A1	2	5	10				

Table 5.3: c_1 and c_2 for curves over $\mathbb{Q}(\sqrt{13})$

5.3 Conclusions and areas for further study

In this thesis, I have provided a way of calculating the L-series of a modular elliptic curve over a real quadratic field with narrow class number 1, and used it to confirm numerically aspects of Beilinson's conjecture, in the process showing that a number of real quadratic curves are almost certainly modular with the expected conductor. In particular, I have shown that the image under the regulator map of $\mathrm{K}_2(E_{\mathcal{O}})$ has rank at least 2, and probably exactly 2, for various elliptic curves over some real quadratic fields, and in these cases shown that this image has a volume which agrees with a simple rational multiple of the L-series $L(E,2)$ to around 50 decimal places. I have also detailed the linear dependencies involved in this, and conjectured a formula analogous to the Birch Swinnerton-Dyer conjecture for this case.

I have also confirmed and extended Bloch and Grayson's calculations for the analogous case for curves over the rational numbers, and found curves which may correspond to a non-trivial group Ш. I have also produced a formula for calculating the L-series of modular elliptic curves over real cubic fields with narrow class number one, and outlined how to construct this for general curves of narrow class number one.

There are various obvious areas in which this work can be extended. First it should be possible to remove the restriction to fields of narrow class number one. This assumption mainly assures that the modular form associated to the L-series lies on one connected component of the appropriate space. It should be possible

to remove this assumption by considering fourier series expansions for some cusp on each connected component and combining them somehow to get the L-series. The tricky part may be finding the appropriate functional equation, but I think it must be along the lines of what I have here.

Second, we can consider the same problem over bigger fields. The real cubic case is just a matter of implementing the formula I have given, and the only bar to going higher than that is working out a fundamental domain of the appropriate sort.

It should also be fairly easy to carry out calculations using a mixture of torsion and non-torsion points, providing you can find appropriate curves.

Appendix A

Results from Rational Calculations

This will be a table of results, explanation will be in chapter 3.

These tables indicate linear dependencies (to about 70 d.p.) between values of E-K-L series and the L-series evaluated at $s = 2$. N is the conductor of the curve, and m' is the number of different split multiplicative reductions as explained in Chapter 3. The other columns are labelled by a point which corresponds to a multiple of the E-K-L series evaluated at that point on the curve when normalized so that the real period is 1. For example

Curve	m'	$\frac{1}{3}$	NL
19A3(A)	0	-12	1

indicates that on the curve 19A3(A),

$$-12\left((\pi \mathrm{Im}(\tau))^2 K_1(0, \tfrac{1}{3}, 2)\right) + 1(19L(E,2)) = 0$$

The results of chapter 3 are as follows.

Curve	m'	Curve	m'	Curve	m'	Curve	m'	Curve	m'
19A1(B)	1	234E3	1	426C1	1	585B1	1	754A1	1
26A1(B)	1	246F1	1	430C1	1	585D1	1	756B2	1
35A1(B)	1	254A1	1	430C2	1	590A1	1	756E2	1
37B1(C)	1	254A2	1	434B1	1	594H2	1	762F1	1
38A1(D)	1	267A1	1	434B2	1	612B1	1	774A1	1
51A1(A)	1	270B1	1	435A1	1	614B1	1	774F1	1
54B1(A)	1	270C2	1	450B2	1	618C1	1	780D1	1
77B1(D)	1	270D1	1	450B4	1	618D1	1	786F1	1
91B2(C)	1	278B1	1	459C2	1	627B1	1	794B1	1
106A1(B)	1	286A1	1	460C1	1	635A1	1	794D1	1
106C1(E)	1	294D1	1	466B1	1	642B1	1	794D2	1
110B1(A)	1	300B1	1	470B1	1	650L1	1	795C1	1
110C1(E)	1	315A2	1	470D1	1	651E1	1	801C2	1
140A1(A)	1	315A3	1	485A1	1	651E2	1	806E1	1
142D1(C)	1	318B1	1	486D2	1	657C2	1	806E2	1
153B2(B)	1	326C1	1	486E2	1	658C1	1	807A1	1
158D1(B)	1	333A2	1	486F1	1	666C2	1	810A1	1
162B1(G)	1	342A2	1	490C1	1	670B1	1	810B1	1
162B3(I)	1	342A3	1	490E1	1	682A1	1	810C1	1
162D1(E)	1	350B1	1	506C1	1	682A2	1	810D1	1
170C1(F)	1	354B1	1	516D1	1	693C2	1	810E1	1
170D1(D)	1	355A1	1	522C1	1	693C3	1	810F1	1
171B2(B)	1	358B1	1	522H1	1	702E1	1	810G1	1
174A1(I)	1	366F1	1	522M2	1	702H2	1	810H1	1
178A1(A)	1	370C1	1	530A1	1	702N1	1	813B1	1
182B1(A)	1	372C1	1	537C1	1	702N3	1	813B2	1
182B2(B)	1	378A1	1	540B2	1	702P1	1	814A1	1
187A1(A)	1	378A2	1	540E2	1	702P2	1	815A1	1
189B2(D)	1	378B1	1	540F1	1	705C1	1	819E2	1
189C1(F)	1	378E1	1	546D1	1	714I2	1	819E3	1
190C1(A)	1	378E3	1	546D2	1	715A1	1	822C1	1
209A1	1	378F2	1	555B1	1	730B1	1	825C1	1
214D1	1	396C2	1	558B1	1	730K1	1	828D2	1
218A1	1	402D1	1	558F1	1	735D1	1	830A1	1
219B1	1	402D2	1	564B1	1	738J2	1	854B2	1
222A1	1	405A1	1	572A1	1	740B1	1	858D1	1
234E2	1	406B1	1	574F1	1	753B1	1	858J1	1

Table A.1: Curves with torsion group C_3 and no relations (part 1)

Curve	m'	Curve	m'	Curve	m'	Curve	m'	Curve	m'
862D1	1	903B2	1	918G1	1	938D1	1	973B2	1
866A1	1	906C1	1	918I1	1	938D2	1	978H1	1
874F1	1	906C2	1	918J1	1	940C1	1	986A1	1
882F1	1	906D1	1	921B1	1	946B1	1	988D1	1
882H2	1	910B1	1	924G1	1	948C1	1	990F2	1
891B1	1	910E1	1	924H1	1	954E2	1	990L2	1
894C1	1	910E2	1	930I1	1	954F2	1	994D1	1
901C1	1	918D2	1	934B1	1	954K2	1	995B1	1
902B1	1	918E2	1	935B1	1	966K1	1	996C1	1
903B1	1	918F1	1						

Table A.2: Curves with torsion group C_3 and no relations (part 2)

Curve	m'	$\frac{1}{3}$	NL	Curve	m'	$\frac{1}{3}$	NL	Curve	m'	$\frac{1}{3}$	NL
19A3(A)	0	-12	1	225B1	0	1	0	540D1	0	-324	1
26A3(A)	0	-36	1	236B1	0	216	1	550D1	0	-324	1
27A1(B)	0	-12	1	242B1	0	-108	1	594C1	0	162	1
27A3(A)	0	1	0	243A2	0	1	0	612A1	0	324	1
27A4(C)	0	12	1	243B1	0	1	0	620A1	0	324	1
35A3(A)	0	36	1	270A1	0	324	1	650G1	0	324	1
37B3(B)	0	-12	1	278B3	0	72	1	675C1	0	1	0
38A3(C)	0	18	1	324A1	0	-108	1	676C1	0	-216	1
44A1(A)	0	-27	1	324B1	0	-216	1	700I1	0	-324	1
50A1(E)	0	-108	5	324C1	0	-108	1	702E3	0	108	1
50A3(G)	0	54	1	324D1	0	216	1	702H1	0	-108	1
54A1(E)	0	-54	1	325A1	0	-108	1	722A1	0	-324	1
54A3(D)	0	36	1	326C3	0	-36	1	756D1	0	-324	1
77B3(C)	0	36	1	333A3	0	-36	1	756F1	0	-648	1
91B1(B)	0	36	1	370C3	0	108	1	854B1	0	-108	1
92A1(A)	0	-108	1	378B3	0	108	1	882A1	0	324	1
108A1(A)	0	1	0	378F1	0	108	1	891F1	0	540	1
116B1(A)	0	216	1	404B1	0	-108	1	892B1	0	-216	1
124A1(B)	0	108	1	405B1	0	-108	1	900C1	0	1	0
158D3(A)	0	-36	1	441B1	0	1	0	900F2	0	324	1
162A1(K)	0	108	1	459F1	0	324	1	916D1	0	-216	1
162C1(A)	0	-108	1	485A3	0	-72	1	972A2	0	1	0
162C3(D)	0	54	1	486A2	0	216	1	972B2	0	1	0
171B3(C)	0	36	1	486B2	0	-108	1	972C1	0	1	0
172A1(A)	0	108	1	486C1	0	-108	1	972D1	0	1	0
189B1(C)	0	-36	1	490A1	0	-324	1	973B1	0	-180	1
189C3(H)	0	-36	1	540A1	0	324	1	980A1	0	648	1
196B1(C)	0	-108	1	540C1	0	324	1				

Table A.3: Curves with torsion group C_3 with relations

Curve	m'	Curve	m'	Curve	m'	Curve	m'	Curve	m'
17A1(C)	1	210C1	1	395A1	1	552D3	1	720J8	1
33A3(D)	1	210C4	1	402B3	1	552E1	1	744B3	1
39A3(D)	1	210E6	1	410B1	1	560D4	1	759B1	1
40A4(C)	1	222C4	1	410B4	1	561D4	1	759B4	1
55A3(C)	1	231A4	1	423C4	1	570E4	1	760E1	1
57B3(C)	1	234D1	1	429B1	1	570G1	1	770C4	1
62A1(A)	1	238C1	1	435C4	1	570I1	1	770E4	1
66B1(E)	1	240A6	1	435D1	1	570M1	1	777A4	1
70A1(A)	1	240D6	1	435D4	1	582D1	1	777D1	1
75B8(K)	1	240D8	1	438F1	1	590B4	1	777E3	1
78A4(D)	1	246E1	1	438F4	1	609B1	1	782E1	1
80A4(G)	1	254D1	1	440C4	1	609B4	1	791C1	1
90C1(E)	1	258D1	1	448B4	1	610B4	1	792E4	1
96A4(G)	1	264C1	1	455B4	1	616E3	1	798I4	1
102B4(I)	1	272B4	1	462F1	1	624C4	1	805C1	1
105A4(C)	1	282A1	1	465B3	1	624F3	1	816B4	1
112B4(C)	1	285C4	1	480B3	1	624F4	1	816H5	1
114C1(G)	1	291B4	1	480D4	1	624H4	1	816H6	1
120A4(G)	1	294C1	1	480F4	1	624I4	1	822E1	1
129B3(C)	1	312C1	1	480G4	1	630J1	1	840B1	1
130B1(A)	1	312D4	1	480H3	1	651D1	1	840C1	1
130B4(C)	1	330B1	1	480H4	1	663B4	1	840D3	1
138C1(A)	1	330B4	1	490H1	1	665B3	1	840F4	1
141C1(A)	1	330C1	1	496F4	1	666F1	1	840G4	1
150C1(I)	1	330C4	1	504G1	1	672E4	1	840J1	1
150C3(K)	1	330D1	1	510D1	1	672F3	1	858E1	1
154B1(E)	1	330E3	1	510E1	1	672H3	1	858H1	1
161A3(C)	1	336B4	1	510E4	1	678E1	1	870D4	1
168A3(C)	1	336C4	1	510E6	1	681B3	1	870G1	1
168B1(E)	1	336D6	1	514A1	1	690F4	1	870G4	1
182A1(E)	1	336E6	1	514A4	1	690G1	1	880C3	1
192B4(C)	1	345D1	1	522K1	1	690K4	1	880C4	1
192C6(O)	1	366E4	1	528B4	1	705F4	1	880I4	1
195A4(C)	1	377A4	1	528H4	1	714F1	1	885B3	1
195A6(F)	1	385A1	1	528J4	1	714G4	1	888B1	1
205A4	1	390B1	1	545A4	1	720E4	1	888B4	1
210B8	1	390B4	1	546C3	1	720J5	1	890H1	1

Table A.4: Curves with torsion group C_4 and no relations (part 1)

Curve	m'	Curve	m'	Curve	m'	Curve	m'	Curve	m'
890H4	1	912K4	1	960E5	1	960O5	1	987B3	1
897B1	1	915B4	1	960E8	1	960O8	1	990J1	1
897C3	1	930O1	1	960H4	1	960P4	1	990K1	1
897E1	1	960C4	1	960K4	1	966G1	1	994F3	1
912G4	1	960D3	1	960N3	1	966I1	1		

Table A.5: Curves with torsion group C_4 and no relations (part 2)

Curve	m'	$\frac{1}{4}$	$\frac{1}{4}+\frac{\tau}{2}$	NL	Curve	m'	$\frac{1}{4}$	$\frac{1}{4}+\frac{\tau}{2}$	NL
15A7(D)	0	-16		11	288B3	0	-64		1
15A8(A)	0	-16		1	288C3	0	-64		1
17A4(A)	0		-8	1	289A1	0	-64		1
21A4(A)	0	-8		1	291B3	0		-32	1
24A3(D)	0	-4		1	312D1	0		-64	1
24A4(A)	0	-16		1	336E5	0	-32		1
32A1(B)	0	-16		1	360D1	0	-256		1
32A4(D)	0		-8	1	363A1	0		-64	1
40A3(A)	0		-16	1	387D1	0		-64	1
42A4(D)	0	-16		3	392A1	0	-128		1
48A5(F)	0	-8		1	400A3	0	-64		1
56A1(C)	0	-64		1	408B1	0		-128	1
63A5(F)	0		-64	7	429B4	0	-32		1
64A3(D)	0	-16		1	440C1	0		-64	1
72A1(A)	0	-32		1	448A4	0	-64		1
80A3(H)	0		-16	1	455B1	0		-64	1
96B3(B)	0		-32	1	480E3	0		-64	1
99B1(H)	0	-64		3	480F3	0		-64	1
117A1(A)	0	-64		1	504F1	0		-128	1
120A1(E)	0	-32		1	507C1	0	-128		1
144B4(H)	0		-32	1	525A1	0		-128	1
147A1(C)	0	-64		1	600A1	0		-128	1
171A1(D)	0		-64	1	600F1	0	-256		1
192A3(T)	0		-32	1	605B1	0	-192		1
192D5(J)	0		-32	1	663B1	0	-64		1
195A1(A)	0	-32		1	672C3	0	-128		1
200C1(G)	0	-64		1	680A1	0	-128		1
205A1	0		-32	1	784C4	0		-128	1
225C1	0	-64		1	792D1	0		-256	1
231A1	0	-32		1	840F1	0	-128		1
240A5	0	-32		1	840G1	0	-128		1
240D7	0	-32		1	840J4	0	-128		1
272B3	0		-32	1	936E3	0		-128	1
275A1	0	-128		1					

Table A.6: Curves with torsion group C_4 with relations

Curve	m'	$\frac{1}{5}$	$\frac{2}{5}$	NL	Curve	m'	$\frac{1}{5}$	$\frac{2}{5}$	NL
11A1(B)	1	-8	-4	5	302A1	1	-60	120	1
11A3(A)	0	2	3	0	325E1	1	-40	-20	1
		0	10	1	366B1	2			
38B1(A)	1	-40	-20	1	395C1	1	-60	120	1
50B1(A)	1	-20	40	1	426A1	2			
50B2(B)	1	-20	-10	1	537E1	1	-80	160	1
57C1(F)	1	-40	-20	3	550K2	2			
58B1(B)	1	-40	-20	1	550K3	1	-100	200	1
75C1(C)	1	-40	-20	1	574J1	1	-160	-80	1
110A1(C)	1	-40	-20	1	606F1	1	-220	440	1
118B1(B)	1	-40	80	1	665D1	2			
123A1(A)	1	-20	40	1	710D1	2			
155A1(D)	1	-40	-20	1	786M1	2			
158C1(H)	1	-40	-20	1	806F1	1	-160	320	1
175A2(A)	1	-20	40	1	834G1	2			
186B1(B)	1	-120	-60	1	862E1	1	-160	320	1
203A1	1	-40	-20	1	874E1	2			
246B1	2				885D1	1	-120	-60	1
286D1	2				890G1	2			

Table A.7: Curves with torsion group C_5

Curve	m'	Curve	m'	Curve	m'	Curve	m'	Curve	m'
90C7(L)	2	370D2	2	570F1	2	660D1	2	870C1	2
114A1(A)	2	390C1	2	570F2	2	660D2	2	870C2	2
114A2(B)	2	390C2	2	570K1	2	770F1	2	910J3	2
126A3(C)	2	390D1	2	570K2	2	770F2	2	910J4	2
126A4(D)	2	390D2	2	630F7	2	770G1	2	930N1	2
198B3(G)	2	414A3	2	630F8	2	770G2	2	930N2	2
198B4(H)	2	414A4	2	630H1	2	798E3	2	966F1	2
210A1	2	438A1	2	630H2	2	798E4	2	966F2	2
210A5	2	438A2	2	630I3	2	858B1	2	990H3	2
210B4	2	462G1	2	630I8	2	858B2	2	990H4	2
306A3	2	462G2	2	646E1	2	870B1	2	994G1	2
306A4	2	510G1	2	646E2	2	870B2	2	994G2	2
370D1	2	510G2	2						

Table A.8: Curves with torsion group C_6 and no relations

Curve	m'	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{6}+\frac{\tau}{2}$	$\frac{2}{3}+\frac{\tau}{2}$	NL
14A1(C)	1	-2	-2			1
14A2(D)	1		-5	4		1
14A4(A)	0	2	5			0
		0	18			1
14A6(B)	0		8	-7		0
			18	-18		1
20A1(B)	0	5	-13			0
		-36	72			1
20A2(A)	0		11	-16		0
			-48	60		1
30A1(A)	1	-12	-12			1
30A4(D)	1		-10		8	1
30A5(E)	1	-12	-12			5
34A1(A)	1		-10		8	1
34A2(B)	1	-4	-4			1
36A1(A)	0	0	1			0
		-24	0			1
36A2(B)	0		1	-1		0
			-12	0		1
66A1(A)	1		-12	-12		1
66A2(B)	1	-48	60			1
84A1(C)	1	-24	-24			1
84A2(D)	1		-60	48		1
90A1(M)	1	-24	-24			1
90A2(N)	1		-60	48		1
90B1(A)	1	-48	60			1
90B2(B)	1		-12	-12		1
90C8(K)	1	-8	-8			1
102C1(A)	1		-12	-12		1
102C2(B)	1	-48	60			1
126A5(E)	1	-48	60			1
126A6(F)	1		-12	-12		1
130A1(E)	1		-12	-12		1
130A2(F)	1	-48	60			1
138B1(G)	1	-48	60			1
138B2(H)	1		-12	-12		1
156B1(A)	1		-60		48	1
156B2(B)	1	-24	-24			1
170B1(H)	1		-12	-12		1
170B2(I)	1	-48	60			1
180A3(C)	1		-24	-24		1

Table A.9: Curves with torsion group C_6 with relations (part 1)

Curve	m'	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{6}+\frac{\tau}{2}$	$\frac{2}{3}+\frac{\tau}{2}$	NL
180A4(D)	1	-96	120			1
198C1(M)	1		-60		48	1
198C2(N)	1	-24	-24			1
198D1(A)	1	-24	-24			1
198D2(B)	1		-60		48	1
210A4	1	-24	-24			1
210B1	1	-24	-24			1
220A1	1	-24	-24			1
220A2	1		-60		48	1
252A3	1	-96	120			1
252A4	1		-24	-24		1
306B3	1	-24	-24			1
306B4	1		-60		48	1
310B1	1	-96	120			1
310B2	1		-24	-24		1
342C3	1		-24	-24		1
342C4	1	-96	120			1
410C1	1		-60		48	1
410C2	1	-24	-24			1
420C1	1		-72	-72		1
420C2	1	-288	360			1
438D1	1		-60		48	1
438D2	1	-24	-24			1
468D3	1	-48	-48			1
468D4	1		-120		96	1
630A1	1		-72	-72		1
630A2	1	-288	360			1
630F3	1	-48	-48			1
630I7	1	-48	-48			1
660C1	1	-288	360			1
660C2	1		-72	-72		1
770B1	1	-144	180			1
770B2	1		-36	-36		1
798E1	1	-72	-72			1
798E2	1		-180		144	1
910C1	1	-72	-72			1
910C2	1		-180		144	1
910J1	1		-180		144	1
910J2	1	-72	-72			1
990B1	1		-72	-72		1
990B2	1	-288	360			1

Table A.10: Curves with torsion group C_6 with relations (part 2)

Curve	m'	$\frac{1}{7}$	$\frac{2}{7}$	$\frac{3}{7}$	NL
26B1(D)	1	5	10	8	0
		0	28	28	1
174B1(G)	2	-140	-140	-84	1
258F1	2	-140	-140	-84	1
294B2	2	-140	84	140	1
490K2	2	-140	-140	-84	1
546F1	2	-140	-140	-84	1
574I1	2	-70	-70	-42	1
678D1	2	-280	168	280	1
762G1	2	-140	-140	-84	1
858K1	3				

Table A.11: Curves with torsion group C_7

Curve	m'	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{3}{8}$	$\frac{1}{8}+\frac{\tau}{2}$	$\frac{3}{8}+\frac{\tau}{2}$	NL
15A4(F)	1	-19	10	25			0
		40	-24	-56			1
21A3(C)	1		4		-23	21	0
			-8		32	-32	1
42A1(A)	1	1	5	5			0
		-16	32	48			1
48A6(E)	1	-1	2	3			0
		-8	-40	-40			1
102B1(G)	2		-24		-16	-16	1
210E1	2	-64	-96	-64			1
210E4	2	-64	-96	-64			3
336D5	2	-32	-48	-32			1
690K1	2	-384	96	384			1
714G1	2	-64	-96	-64			1
930O4	3						
966G4	2		-96		-64	-64	1

Table A.12: Curves with torsion group C_8

Curve	m'	$\frac{1}{9}$	$\frac{2}{9}$	$\frac{1}{3}$	$\frac{4}{9}$	NL
54B3(B)	1	1	10	10	0	0
		0	8	7	-1	0
		0	-60	0	48	1
714I1	3	-324	-432	-468	-108	1

Table A.13: Curves with torsion group C_9

Curve	m'	$\frac{1}{10}$	$\frac{1}{5}$	$\frac{3}{10}$	$\frac{2}{5}$	$\frac{1}{10}+\frac{\tau}{2}$	$\frac{3}{10}+\frac{\tau}{2}$	$\frac{3}{5}+\frac{\tau}{2}$	$\frac{4}{5}+\frac{\tau}{2}$	NL
66C1(I)	2		-4		-1	4	6			0
			-20		-10	0	0			1
66C2(J)	2	-2	0	3	4					0
		0	-20	-40	-40					1
150A3(C)	2	0	1	2	2					0
		-80	0	120	160					1
150A4(D)	2		3		1	-2	-3			0
			-40		-20	0	0			1
570L1	3	-80	-120	-120	-80					1
570L2	3		-280		-100	160	240			1
870I1	3		-280		-100			160	240	1
870I2	3	-80	-120	-120	-80					1

Table A.14: Curves with torsion group C_{10}

Curve	m'	$\frac{1}{12}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{5}{12}$	NL
90C3(G)	2	1	0	-1	1	2	0
		0	1	2	3	2	0
		0	0	16	144	144	1
210B5	3	-2	-1	1	4	3	0
		0	-24	-48	-72	-48	1

Table A.15: Curves with torsion group C_{12}

Curve	m'	$\frac{1}{4}$	$\frac{1}{4}+\frac{\tau}{2}$	NL	Curve	m'	$\frac{1}{4}$	$\frac{1}{4}+\frac{\tau}{2}$	NL
15A1(C)	1	-8	-8	3	330C2	2			
15A3(B)	0	5	-6	0	336D4	2			
		-16	16	1	336E4	1	-32	-32	1
21A1(B)	1	-8	8	1	390B2	2			
24A1(B)	0	3	-5	0	429B2	1	-32	-32	1
		8	-24	1	510E2	1	-64	-64	1
42A2(B)	1	-16	-16	3	510E3	2			
48A3(C)	1	-8	-8	1	609B2	1	-32	-32	1
102B2(H)	2				663B2	1	-64	-64	1
120A2(F)	1	-32	-32	1	690K2	1	-96	-96	1
195A2(B)	1	-32	-32	1	714G2	2			
195A3(D)	2				759B2	2			
210C2	2				816H3	1	-64	-64	1
210E3	2				840F2	1	-128	-128	1
231A2	1	-32	-32	1	840G2	1	-128	-128	1
240A3	1	-32	-32	1	840J2	1	-128	-128	1
240D4	2				930O2	2			
240D5	1	-32	-32	1	966G2	2			
330B2	2								

Table A.16: Curves with torsion group $C_4 \times C_2$

Curve	m'	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{6}+\frac{\tau}{2}$	$\frac{2}{3}+\frac{\tau}{2}$	NL
30A2(B)	1	2	-3	2	2	0
		0	5	-5	1	0
		12	12	-24	24	1
90C6(J)	2	2	-3	2	2	0
		0	-20	0	16	1
210A2	2	2	-3	2	2	0
		0	60	0	-48	1
210B2	2	2	-3	2	2	0
		0	-60	0	48	1
630F6	2	2	-3	2	2	0
		0	-120	0	96	1
630I6	2	2	-3	2	2	0
		0	-120	0	96	1

Table A.17: Curves with torsion group $C_6 \times C_2$

Curve	m'	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{3}{8}$	$\frac{1}{8}+\frac{\tau}{2}$	$\frac{1}{4}+\frac{\tau}{2}$	$\frac{3}{8}+\frac{\tau}{2}$	NL
210E2	3	2	-1	-2	2	0	-2	0
		0	-2	-2	3	3	1	0
		-32	-48	-32	0	0	0	1

Table A.18: Curves with torsion group $C_8 \times C_2$

Appendix B

Results from Quadratic Calculations

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
6	A1	x+1	x	x	0	0	10	2:2
6	A2	x+5	-x	-x+2	0	0	10	2:1
7	A1	2	-x	1	0	0	5	
2x+8	A1	3	1	x+1	0	0	5	
-2x+10	A1	3	1	-x+2	0	0	5	
10	A1	3	2	2	0	0	15	3:2
10	A2	7	-8	8	0	0	5	3:1
10	B1	x-1	-x	x	0	0	5	3:2
10	B2	x+5	-x	-5x-3	0	0	5	3:1
2x+10	A1	1	-1	-x	0	0	5	
-2x+12	A1	1	-1	x-1	0	0	5	
11	A1	0	-1	1	0	0	5	5:2
11	A2	10	-11	11	0	0	5	5:1
3x+13	A1	4	-1	-2x-1	0	0	5	
-3x+16	A1	4	-1	2x-3	0	0	5	
2x+14	A1	4x-5	-5	5x	0	0	10	2:2
2x+14	A2	2x+3	2x-1	5x+5	0	0	10	2:1
-2x+16	A1	-4x-1	-5	-5x+5	0	0	10	2:2
-2x+16	A2	-2x+5	-2x+1	-5x+10	0	0	10	2:1
15	A1	2	-3	3	0	0	5	
15	B1	2x	x	1	0	0	5	
6x+18	A1	x+3	-2x	2	0	0	5	
6x+18	B1	-3x+2	3x-3	-3x+3	0	0	5	
-6x+24	A1	-x+4	2x-2	2	0	0	5	
-6x+24	B1	3x-1	-3x	3x	0	0	5	
8x+18	A1	3x-4	-4	4x	0	0	5	
-8x+26	A1	-3x-1	-4	-4x+4	0	0	5	
22	A1	x+3	x	x-1	0	0	5	5:2
22	A2	x+9	-11x	-11x+44	0	0	5	5:1
x+22	A1	2x-4	x-3	2x-1	0	0	5	
-x+23	A1	-2x-2	-x-2	-2x+1	0	0	5	
8x+22	A1	-3x+3	-2	2x+2	0	0	5	
-8x+30	A1	3x	-2	-2x+4	0	0	5	
30	A1	1	-12	36	0	0	10	2:2
30	A2	17	18	-18	0	0	10	2:1

Table B.1: Curves over $\mathbb{Q}(\sqrt{5})$ with 5-torsion where x=$\frac{1+\sqrt{5}}{2}$

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
3	A1	x	-x-1	x+1	0	0	10	2:2
3	A2	x+4	-x-1	1	0	0	10	2:1
x+8	A1	x+3	-2	2x-2	0	0	10	2:2
x+8	A2	5x-1	x	3x+4	0	0	10	2:1
-x+8	A1	-x+3	-2	-2x+2	0	0	10	2:2
-x+8	A2	-5x-1	-x	-3x+4	0	0	10	2:1
3x+10	A1	3	x	x+2	0	0	5	
-3x+10	A1	3	-x	-x+2	0	0	5	
4x+11	A1	2	-1	-x-1	0	0	5	
-4x+11	A1	2	-1	x-1	0	0	5	
11	A1	0	-1	1	0	0	5	5:2
11	A2	10	-11	11	0	0	5	5:1
3x+12	A1	x+7	-4x-2	-4x+12	0	0	10	2:2
3x+12	A2	x-9	x-10	x-10	0	0	10	2:1
-3x+12	A1	-x+7	4x-2	4x+12	0	0	10	2:2
-3x+12	A2	-x-9	-x-10	-x-10	0	0	10	2:1
x+12	A1	3x+1	-x-2	2	0	0	5	
-x+12	A1	-3x+1	x-2	2	0	0	5	
13	A1	x+2	x+1	x+1	0	0	5	
6x+17	A1	4	2x+1	3x+5	0	0	5	
-6x+17	A1	4	-2x+1	-3x+5	0	0	5	
3x+18	A1	-5x+3	5x-4	-5x+4	0	0	5	
-3x+18	A1	5x+3	-5x-4	5x+4	0	0	5	
3x+20	A1	-x+1	x-2	-x+2	0	0	5	
-3x+20	A1	x+1	-x-2	x+2	0	0	5	

Table B.2: Curves over $\mathbb{Q}(\sqrt{2})$ with 5-torsion where x=$\sqrt{2}$ (part 1)

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
9x+24	A1	2x+5	2x-10	24x-28	0	0	5	
-9x+24	A1	-2x+5	-2x-10	-24x-28	0	0	5	
x+22	A1	-x+1	-x	2	0	0	5	
-x+22	A1	x+1	x	2	0	0	5	
11x+28	A1	2x+1	-2x-2	2x+2	0	0	5	
-11x+28	A1	-2x+1	2x-2	-2x+2	0	0	5	
3x+24	A1	1	x-2	-2x+2	0	0	5	
3x+24	B1	-4x+3	4x-4	-4x+4	0	0	5	
-3x+24	A1	1	-x-2	2x+2	0	0	5	
-3x+24	A1	4x+3	-4x-4	4x+4	0	0	5	
13x+30	A1	5	2x-2	4	0	0	5	
-13x+30	A1	5	-2x-2	4	0	0	5	
25	A1	3x+2	x+1	1	0	0	5	
19x+38	A1	1	-2	2	0	0	5	
9x+30	A1	2x+5	-x-2	x	0	0	5	
9x+30	B1	-2x+3	2x-4	-2x+4	0	0	5	
-9x+30	A1	-2x+5	x+2	-x	0	0	5	
-9x+30	B1	2x+3	-2x-4	2x+4	0	0	5	
13x+34	A1	x+5	-2x	-2x+4	0	0	5	
-13x+34	A1	-x+5	2x	2x+4	0	0	5	

Table B.3: Curves over $\mathbb{Q}(\sqrt{2})$ with 5-torsion where x=$\sqrt{2}$ (part 2)

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
2	A1	3	-1	x-2	0	0	5	3:2
2	A2	x	-x-1	x+1	0	0	5	3:1,3
2	A3	3	-1	-x-1	0	0	5	3:2
6	A1	x+4	-3x-3	3x+6	0	0	10	2:2
6	A2	3x+10	-9x-9	9x+27	0	0	20	2:1,3,4
6	A3	3x-17	3x-18	3x-18	0	0	10	2:2
6	A4	-3x-14	-3x-15	-3x-15	0	0	10	2:2
8x+14	A1	-x-3	2x+2	-4x-4	0	0	5	
-8x+22	A1	x-4	-2x+4	4x-8	0	0	5	
11	A1	0	-1	1	0	0	5	
11	A2	10	-11	11	0	0	5	
2x+13	A1	4	-x+1	-2x+5	0	0	5	
-2x+15	A1	4	x	2x+3	0	0	5	
14	A1	x+2	x+1	x+1	0	0	5	
2x+18	A1	x+5	-x	-x+3	0	0	5	
-2x+16	A1	-x+6	x-1	x+2	0	0	5	
4x+18	A1	x-4	-x+3	x-3	0	0	5	
-4x+22	A1	-x-3	x+2	-x-2	0	0	5	
x+20	A1	-2	-x-2	4x+5	0	0	5	
-x+21	A1	-2	x-3	-4x+9	0	0	5	
14x+28	A1	x+4	-x-5	x+5	0	0	5	
-14x+42	A1	-x+5	x-6	-x+6	0	0	5	
25	A1	2x+6	-x-1	1	0	0	5	
6x+26	A1	2x-3	2x-4	2x-4	0	0	5	
-6x+32	A1	-2x-1	-2x-2	-2x-2	0	0	5	
14x+30	A1	x-2	x-3	x-3	0	0	5	
14x+30	B1	4x+1	-4x-2	4x+2	0	0	5	
-14x+44	A1	-x-1	-x-2	-x-2	0	0	5	
-14x+44	B1	-4x+5	4x-6	-4x+6	0	0	5	
2x+30	A1	3x-1	-2x	4x-6	0	0	5	
-2x+32	A1	-3x+2	2x-2	-4x-2	0	0	5	
8x+30	A1	x-1	-x	x	0	0	5	
-8x+38	A1	-x	x-1	-x+1	0	0	5	

Table B.4: Curves over $\mathbb{Q}(\sqrt{13})$ with 5-torsion where x=$\frac{1+\sqrt{13}}{2}$

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
x+7	A1	-3	-x-1	4x+3	0	0	12	2:2,3,4
x+7	A2	2x-1	-x	-1	0	0	6	2:1
x+7	A3	-3x+9	2	-7x+17	0	0	6	2:1
x+7	A4	7x+6	2x	25x+15	0	0	6	2:1
-x+8	A1	-3	x-2	-4x+7	0	0	12	2:2,3,4
-x+8	A2	-2x+1	x-1	-1	0	0	6	2:1
-x+8	A3	3x+6	2	7x+10	0	0	6	2:1
-x+8	A4	-7x+13	-2x-2	-25x+40	0	0	6	2:1
x+8	A1	x+4	2x	9x+1	0	0	6	2:2
x+8	A2	-x+2	-x	1	0	0	6	2:1
-x+9	A1	-x+5	-2x+2	-9x+10	0	0	6	2:2
-x+9	A2	x+1	1-x	1	0	0	6	2:1
4x+8	A1	0	-2	2	0	0	12	2:2,3,4
4x+8	A2	2x-6	-4x	8x-12	0	0	6	2:1
4x+8	A3	-2x-4	4x-4	-8x-4	0	0	6	2:1
4x+8	A4	6	4	20	0	0	6	2:1
9	A1	5x+2	-2	-9x-6	0	0	6	2:3 5:2
9	A2	-5x+7	-2	9x-15	0	0	6	2:4 5:1
9	A3	4x-3	-x+2	6x-9	0	0	6	2:1 5:4
9	A4	-4x+1	x+1	-6x-3	0	0	6	2:2 5:3
x+9	A1	x-2	-1	1	0	0	6	2:2
x+9	A2	5x-4	2	9x-8	0	0	6	2:1
-x+10	A1	-x-1	-1	1	0	0	6	2:2
-x+10	A2	-5x+1	2	-9x+1	0	0	6	2:1
2x+9	A1	3x-1	x-3	-2x+1	0	0	12	2:2,3,4
2x+9	A2	5x-1	10x-10	15x+10	0	0	6	2:1
2x+9	A3	9x-5	-2x+6	43x-44	0	0	6	2:1
2x+9	A4	3x-3	-2x+1	4x-7	0	0	6	2:1
-2x+11	A1	-3x+2	-x-2	2x-1	0	0	12	2:2,3,4
-2x+11	A2	-5x+4	-10x	-15x+25	0	0	6	2:1
-2x+11	A3	-9x+4	2x+4	-43x-1	0	0	6	2:1
-2x+11	A4	-3x	2x-1	-4x-3	0	0	6	2:1

Table B.5: Curves over $\mathbb{Q}(\sqrt{5})$ with 6-torsion where x=$\frac{1+\sqrt{5}}{2}$ (part 1)

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
4x+10	A1	5x+3	2x	16x+9	0	0	6	2:3 3:2
4x+10	A2	5x+8	20x-12	132x-82	0	0	6	2:4
4x+10	A3	3x-2	-x+1	2x-4	0	0	6	2:1 3:4
4x+10	A4	7x-8	-10x+6	60x-98	0	0	6	2:2
-4x+14	A1	-5x+8	-2x+2	-16x+25	0	0	12	2:3 3:2
-4x+14	A2	-5x+13	-20x+8	-132x+50	0	0	6	2:4
-4x+14	A3	-3x+1	x	-2x-2	0	0	6	2:1 3:4
-4x+14	A4	-7x-1	10x-4	-60x-38	0	0	6	2:2
3x+12	A1	-3x+2	6x-12	3x+3	0	0	6	2:2
3x+12	A2	3x-8	-3x+6	30x-51	0	0	6	2:1
-3x+15	A1	3x-1	-6x-6	-3x+6	0	0	6	2:2
-3x+15	A2	-3x-5	3x+3	-30x-21	0	0	6	2:1
4x+12	A1	2x-2	-2x	2x-2	0	0	6	2:2
4x+12	A2	4x+2	4x	20x+16	0	0	6	2:1
-4x+16	A1	-2x	2x-2	-2x	0	0	6	2:2
-4x+16	A2	-4x+6	-4x+4	-20x+36	0	0	6	2:1
6x+12	A1	5	-3	-6	0	0	12	2:2,3,4
6x+12	A2	13	6	75	0	0	6	2:1
6x+12	A3	5	3	12	0	0	12	2:1
6x+12	A4	-5	-18	9	0	0	6	2:1
14	A1	-3	-2	7	0	0	6	2:2
14	A2	3	1	2	0	0	6	2:1
4x+13	A1	-3x+4	-2	7x-8	0	0	6	2:2
4x+13	A2	3x-2	1	2x-1	0	0	6	2:1
-4x+17	A1	3x+1	-2	-7x-1	0	0	6	2:2
-4x+17	A2	-3x+1	1	-2x+1	0	0	6	2:1
5x+13	A1	4x+1	3x-1	12x+7	0	0	6	2:2
5x+13	A2	2x-7	-6x+2	21x-29	0	0	6	2:1
-5x+18	A1	-4x+5	-3x+2	-12x+19	0	0	6	2:2
-5x+18	A2	-2x-5	6x-4	-21x-8	0	0	6	2:1
2x+14	A1	3x+4	6x-2	26x+17	0	0	6	2:2
2x+14	A2	3x-4	-3x+1	8x-10	0	0	6	2:1

Table B.6: Curves over $\mathbb{Q}(\sqrt{5})$ with 6-torsion where x=$\frac{1+\sqrt{5}}{2}$ (part 2)

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
2x+14	B1	-x+5	-2x-4	6x-13	0	0	12	2:2,3,4
2x+14	B2	9x-1	10x	80x+65	0	0	6	2:1
2x+14	B3	9x-18	-6x-2	18x-29	0	0	6	2:1
2x+14	B4	5x-1	x+2	12x+4	0	0	6	2:1
-2x+16	A1	-3x+7	-6x+4	-26x+43	0	0	6	2:2
-2x+16	A2	-3x-1	3x-2	-8x-2	0	0	6	2:1
-2x+16	B1	x+4	2x-6	-6x-7	0	0	12	2:2,3,4
-2x+16	B2	-9x+8	-10x+10	-80x+145	0	0	6	2:1
-2x+16	B3	-9x-9	6x-8	-18x-11	0	0	6	2:1
-2x+16	B4	-5x+4	-x+3	-12x+16	0	0	6	2:1
4x+18	A1	-x+3	-x	-2x	0	0	6	2:2 3:3
4x+18	A2	-3x+8	2x-2	16x-23	0	0	6	2:1 3:4
4x+18	A3	5x-5	-8x+2	22x-34	0	0	6	2:4 3:1
4x+18	A4	7x+5	16x-4	130x+110	0	0	6	2:3 3:2
-4x+22	A1	x+2	x-1	2x-2	0	0	6	2:2 3:3
-4x+22	A2	3x+5	-2x	-16x-7	0	0	6	2:1 3:4
-4x+22	A3	-5x	8x-6	-22x-12	0	0	6	2:4 3:1
-4x+22	A4	-7x+12	-16x+12	-130x+240	0	0	6	2:3 3:2
4x+20	A1	2	-2	-2x-2	0	0	6	2:2
4x+20	A2	6x-4	4	20x-16	0	0	6	2:1
-4x+24	A1	2	-2	2x-4	0	0	6	2:2
-4x+24	A2	-6x+2	4	-20x+4	0	0	6	2:1
8x+21	A1	1	-x-2	2x-1	0	0	6	2:2
8x+21	A2	6x-1	2x+4	29x+8	0	0	6	2:1
-8x+29	A1	1	x-3	-2x+1	0	0	6	2:2
-8x+29	A2	-6x+5	-2x+6	-29x+37	0	0	6	2:1
10x+26	A1	7x+2	-x-1	-8x-4	0	0	6	2:2 3:3
10x+26	A2	10x+1	2	18x+5	0	0	6	2:1 3:4
10x+26	A3	-x-3	4x-20	20x-24	0	0	6	2:4 3:1
10x+26	A4	x-21	-8x+40	164x-744	0	0	6	2:3 3:2
-10x+36	A1	-7x+9	x-2	8x-12	0	0	6	2:2 3:3
-10x+36	A2	-10x+11	2	-18x+23	0	0	6	2:1 3:4
-10x+36	A3	x-4	-4x-16	-20x-4	0	0	6	2:4 3:1
-10x+36	A4	-x-20	8x+32	-164x-580x	0	0	6	2:3 3:2
4x+28	A1	2x-4	-4	-12x+16	0	0	6	2:2
4x+28	A2	4x-2	2	6x-2	0	0	6	2:1
-4x+32	A1	-2x-2	-4	12x+4	0	0	6	2:2
-4x+32	A2	-4x+2	2	-6x+4	0	0	6	2:1

Table B.7: Curves over $\mathbb{Q}(\sqrt{5})$ with 6-torsion where x=$\frac{1+\sqrt{5}}{2}$ (part 3)

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
2x+5	A1	x	-x-2	1	0	0	6	2:2
2x+5	A2	3x+2	x+2	7x+9	0	0	6	2:1
-2x+5	A1	-x	x-2	1	0	0	6	2:2
-2x+5	A2	-3x+2	-x+2	-7x+9	0	0	6	2:1
2x+6	A1	3x	-x	x-4	0	0	12	2:2,3,4
2x+6	A2	-3x-6	2x	-10x-14	0	0	6	2:1
2x+6	A3	2x	-2x-2	-2	0	0	6	2:1
2x+6	A4	5x-4	-2x+4	26x-34	0	0	12	2:1
-2x+6	A1	-3x	x	-x-4	0	0	12	2:2,3,4
-2x+6	A2	3x-6	-2x	10x-14	0	0	6	2:1
-2x+6	A3	-2x	2x-2	-2	0	0	6	2:1
-2x+6	A4	-5x-4	2x+4	-26x-34	0	0	12	2:1
x+6	A1	-3x+1	1	-2x	0	0	6	2:2
x+6	A2	-3x+5	-2	7x-9	0	0	6	2:1
-x+6	A1	3x+1	1	2x	0	0	6	2:2
-x+6	A2	3x+5	-2	-7x-9	0	0	6	2:1
7	A1	x+2	x	2x+1	0	0	6	2:2
7	A2	-x+2	-x	-2x+1	0	0	6	2:1
5x+12	A1	x+3	x+1	3x+4	0	0	6	2:2
5x+12	A2	-4x+5	-2x+2	-17x+25	0	0	6	2:1
-5x+12	A1	-x+3	-x+1	-3x+4	0	0	6	2:2
-5x+12	A2	4x+5	2x+2	17x+25	0	0	6	2:1
7x+14	A1	-3	-2	7	0	0	12	2:2,3,4 3:5
7x+14	A2	3	1	2	0	0	6	2:1 3:6
7x+14	A3	9x-11	-2x+2	40x-57	0	0	6	2:1 3:7
7x+14	A4	-9x-11	2x+2	-40x-57	0	0	6	2:1 3:8
7x+14	A5	3	-14	7	0	0	12	2:6,7,8 3:1
7x+14	A6	9	7	56	0	0	6	2:5 3:2
7x+14	A7	4x-13	-28x-14	154x-217	0	0	6	2:5 3:3
7x+14	A8	-4x-13	28x-14	-154x-217	0	0	6	2:5 3:4
10	A1	0	-2	2	0	0	6	2:2
10	A2	3x	2	5x	0	0	6	2:1
18	A1	4	2	6	0	0	6	2:2
18	A2	-2	-4	12	0	0	6	2:1

Table B.8: Curves over $\mathbb{Q}(\sqrt{2})$ with 6-torsion where x=$\sqrt{2}$

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
x+6	A1	0	-x	x	0	0	7	
-x+7	A1	0	x-1	-x+1	0	0	7	
2x+10	A1	3	-2x	-2x+4	0	0	7	
-2x+12	A1	3	2x-2	2x+2	0	0	7	
3x+11	A1	6x-4	-3x-1	3x-4	0	0	7	
-3x+14	A1	-6x+2	3x-4	-3x-1	0	0	7	
3x+24	A1	6x-2	3x+3	3x-6	0	0	7	
-3x+27	A1	-6x+4	-3x+6	-3x-3	0	0	7	
26	A1	1	2	-2	0	0	7	
11x+27	A1	2x	x+2	x-3	0	0	7	
-11x+38	A1	-2x+2	-x+3	-x-2	0	0	7	

Table B.9: Curves over $\mathbb{Q}(\sqrt{5})$ with 7-torsion where x=$\frac{1+\sqrt{5}}{2}$

n	label	a_1	a_2	a_3	a_4	a_6	$\|T\|$	isogenies
x+10	A1	4x-1	-2x+4	2x+4	0	0	7	3:2
x+10	A2	1	-x	-x+2	0	0	7	3:1
-x+10	A1	-4x-1	2x+4	-2x+4	0	0	7	3:2
-x+10	A2	1	x	x+2	0	0	7	3:1
x+12	A1	4x+1	2x-2	2x+2	0	0	7	
-x+12	A1	-4x+1	-2x-2	-2x+2	0	0	7	
x+16	A1	3	x+2	-x	0	0	7	
-x+16	A1	3	-x+2	x	0	0	7	
13x+26	A1	1	2	-2	0	0	7	
9x+30	A1	5x+3	-6x-6	6x-6	0	0	7	
9x+30	A2	-5x+3	6x-6	-6x-6	0	0	7	

Table B.10: Curves over $\mathbb{Q}(\sqrt{2})$ with 7-torsion where x=$\sqrt{2}$

Curve	m'	(0,0)	2(0,0)	$\det_{12}$	L
7A1	0			-16	49
2x+8A1	0			4	19
10A2	1				
10B1	0			4	5
10B2	0			1	10
2x+10A1	0			20	29
11A1	0	3	-2		
11A2	1				
3x+13A1	0			16	199
15A1	1				
15B1	0			16	45
6x+18A1	1				
6x+18B1	1				
8x+18A1	1				
22A1	0			-20	121
22A2	2				
x+22A1	1				
8x+22A1	1				

Table B.11: Curves with torsion group C_5 over $\mathbb{Q}(\sqrt{5})$

Curve	m'	P	2P	3P	4P	$\det_{23}$	$\det_{24}$	$\det_{34}$	L
6A1	0	2	-4	-2	1		-5		9
		2	1	2	4				
6A2	0	6	-4	3	-5		-2		81
		3	5	-6	-4				
2x+14A1	1	5	0	-2	-4	-16	28	-32	275
2x+14A2	1	4	-4	2	1	-4	2	2	55
30A1	2	0	1	2	2				
30A2	2	-2	2	-3	3				

Table B.12: Curves with torsion group C_{10} over $\mathbb{Q}(\sqrt{5})$ where 2P=(0,0) and P$\neq$3(0,0)

Curve	m'	P	2P	3P	4P	5P	6P	7P	$\det_{35}$	$\det_{45}$	L
10A1	1	0	1	1	0	0	2	1	81	162	125
		0	0	2	3	3	-1	0			
		1	0	0	1	2	0	0			
		0	4	10	12	17	0	0			

Table B.13: Curve 10A1 with torsion group C_{15} over $\mathbb{Q}(\sqrt{5})$ with P=(2+4x,-12-20x)

Curve	m'	(0,0)	2(0,0)	$\det_{12}$	L
3x+10A1	1				
4x+11A1	0			125	712
11A1	0	3	-2		
11A2	1				
x+12A1	1				
13A1	0			-125	338
6x+17A1	1				
3x+18A1	1				
3x+20A1	1				

Table B.14: Curves with torsion group C_5 over $\mathbb{Q}(\sqrt{2})$

Curve	m'	P	2P	3P	4P
3A1	0	3	-5	3	4
		-3	4	3	5
3A2	0	1	17	-23	-4
		0	-79	106	15
x+8A1	1	8	-4	-4	3
x+8A2	1	-11	-4	8	13
3x+12A1	2				
3x+12A2	2				

Curve	$\det_{12}$	$\det_{13}$	$\det_{14}$	$\det_{23}$	$\det_{24}$	$\det_{34}$	L
3A1					125		324
3A2					-125		3816
x+8A1				100	-175	200	1984
x+8A2				-25	-50	-50	2728
3x+12A1	-50	-100	-100	-75	-100	-50	1008
3x+12A2	75	0	-150	50	25	100	1008

Table B.15: Curves with torsion group C_{10} over $\mathbb{Q}(\sqrt{2})$ where 2P=(0,0) and P$\neq$3(0,0)

Curve	m'	(0,0)	2(0,0)	$\det_{12}$	L
2A1	0			-500	5239
2A2	0			125	338
8x+14A1	1				
11A1	0	3	-2		
11A2	1				

Table B.16: Curves with torsion group C_5 over $\mathbb{Q}(\sqrt{13})$

Curve	m'	P	2P	3P	4P	$\det_{12}$	$\det_{13}$	$\det_{14}$	$\det_{23}$	$\det_{24}$	$\det_{34}$	L
6A1	2					100	100	0	0	-100	-100	1521
6A3	2					-300	0	600	-200	-100	-400	13689
						-5	-1	2	0	-11	5	0
						-2	-13	2	3	-18	3	0

Table B.17: Curves with torsion group C_{10} over $\mathbb{Q}(\sqrt{13})$ where 2P=(0,0) and P$\neq$3(0,0)

Curve	m'	P	2P	3P	4P	P+Q	2P+Q	3P+Q	4P+Q
6A2	2	0	-2	2	1	0	-2	2	0
		1	1	-3	1	-3	2	0	0
		0	0	-2	-2	2	3	1	1
		2	-1	0	-2	2	0	0	-2

$\det_{23}$	$\det_{26}$	$\det_{27}$	$\det_{36}$	$\det_{37}$	$\det_{67}$	L
700	-900	-100	-200	600	-800	4563
4	-1	1	-2	6	-4	0
-1	5	5	-4	0	4	0

Table B.18: Curve 6A2 with torsion group $C_{10} \times C_2$ over $\mathbb{Q}(\sqrt{13})$ where P=(−9x,54+27x) and Q=(−4+x,2 − 5x)

Curve	m'	(0,0)	2(0,0)	$\det_{12}$	L
x+7A2	0			-432	1375
x+7A3	0			-1296	15125
x+7A4	0			1296	34375
x+8A1	0			-432	1775
x+8A2	0			-432	1775
4x+8A2	0			-81	1000
4x+8A4	0	5	-13		
9A1	0			-16	225
9A3	0			32	225

Table B.19: Curves with torsion group C_6 over $\mathbb{Q}(\sqrt{5})$

Curve	m'	(0,0)	2(0,0)	(0,0)+P	2(0,0)+P	$\det_{24}$	L
x+7A1	0	2	-3	2	-2	432	1375
		1	29	-2	26		
4x+8A1	0	2	-3	2	-2	-81	1000
		1	5	-7	7		

Table B.20: Curves with torsion group $C_6 \times C_2$ over $\mathbb{Q}(\sqrt{5})$ where 2P=0 and P$\neq$3(0,0)

Curve	m'	(0,0)	2(0,0)	$\det_{12}$	L
2x+5A1	0			9	68
2x+5A2	0			-9	34
2x+6A2	0			81	1232
2x+6A3	0			81	448
x+6A1	0			-81	544
x+6A2	0			-81	1088
7A1	0			-27	98

Table B.21: Curves with torsion group C_6 over $\mathbb{Q}(\sqrt{2})$

Curve	m'	P	2P	3P	4P	5P	$\det_{34}$	$\det_{45}$	L
2x+6A4	1	-1	0	2	4	3	81	-81	280
		0	-5	7	20	7			

Table B.22: Curves with torsion group C_{12} over $\mathbb{Q}(\sqrt{2})$ where 2P=(0,0)

Curve	m'	(0,0)	2(0,0)	(0,0)+P	2(0,0)+P	$\det_{24}$	L
2x+6A1	0	2	-3	2	-2	-81	448
		0	6	4	7		

Table B.23: Curves with torsion group $C_6 \times C_2$ over $\mathbb{Q}(\sqrt{2})$ where 2P=0 and P$\neq$3(0,0)

Curve	m'	(0,0)	2(0,0)	3(0,0)	$\det_{12}$	$\det_{13}$	$\det_{23}$	L
x+6A1	0	-16	10	1			343	1025
2x+10A1	1				-196	490	-490	3625
3x+11A1	1				-1568	3920	-3920	68875
3x+24A1	1				784	-1960	1960	47925
26A1	1	-10	8	5				
11x+27A1	1				1568	-3920	3920	22625

Table B.24: Curves with torsion group C_7 over $\mathbb{Q}(\sqrt{5})$

Curve	m'	(0,0)	2(0,0)	3(0,0)	$\det_{12}$	$\det_{13}$	$\det_{23}$	L
x+10A1	1				-2	5	-5	64
x+10A2	1				-2	5	-5	8
x+12A1	1				-98	245	-245	2272
x+16A1	1				-98	245	-245	1016
13x+26A1	1	-10	8	5				

Table B.25: Curves with torsion group C_7 over $\mathbb{Q}(\sqrt{2})$

Appendix C

Programs

This is the listing of the basic program I use to calculate the L-series for real quadratic fields of narrow class number one. I do make minor changes to run it as a batch job, and also when we have non-semi stable reduction, I modify the conductor finding routine, and also running keep totals for both possible signs of the functional equation, so I can find the correct sign by doing a second run with a different value of m. Unfortunately the the variables do not match the conventions used in my thesis, although the user interface pretends they do.

```
/* this version has changes to improve efficiency, including reordering in main loop
   to reduce the number of repiles by calculating the coefficient table first */
#include <stdio.h>
#include <genpari.h>

#define TRUE 1
#define G(a,i) (long*)(*(a+(i)))
#define GG(a,i,j) (long*)(*((long*)(*(a+(i)))+(j)))
#define lGG(a,i,j) (*((long*)(*(a+(i)))+(j)))

long prec;

GEN conductor();
GEN hcf();
int legsym();
GEN mnorm();
GEN aterm();
GEN t1();
GEN t2();
GEN ppcoeff();
GEN ratred();
GEN quadred();
GEN spos();
GEN coadd();
GEN cogen();

GEN normC,F,twopi,Lim;
GEN l1a,l21a,l2ua,l1b,l21b,l2ub;

main()
{
        GEN A,c,C,D,e,f,L,H,m,nf,N,S,u,v,rootC1,rootC2,rootF;
        char s[512];
        long lbot,ltop,dec;
```

```
        int i,j,sgn;

/* set precision and initialize */
        printf("precision required? ");
        scanf("%d",&prec);
        init(1500000,50000);
        setprecr((long) (prec/K1));
        constpi(prec+2);
        twopi=gmul(gpi,gdeux);
        polx[0]=lisexpr("x");
        printf("%d\n",prec);

/* get quadratic field and check it has narrow class number one */
/* D is the discriminant of m, and nf is the corresponding number field */
        printf("discriminant of quadratic field? ");
        s[0]=0;
        while(!s[0]) gets(s);
        D=lisexpr(s);
        m=quadpoly(D);
        printf("polynomial is: ");
        outbeaut(m);
        nf=initalg(m,prec);
        ltop=avma;
        if (gcmp1(classno(D))!=TRUE) {
                printf("Class number not 1\n");
                exit(1);
                }
        v=fundunit(D);
        if (gcmp_1(gnorm(v))!=TRUE) {
                printf("Narrow class number not 1\n");
                exit(1);
                }
/* u is the real embedding >1 of the fundamental unit */
/* c is a totally positive generator of the inverse different (polynomial) */
        c=gdiv(v,gadd(gmul(gdeux,quadgen(D)),truecoeff(m,1)));
        outbeaut(c);
        c=gadd(greal(c),gmul(polx[0],gimag(c)));
        u=gadd(greal(v),gmul(GG(nf,6,2),gimag(v)));
        lbot=avma;
        c=gcopy(c);
        u=gcopy(u);
        dec=lpile(ltop,lbot,0)/4;
        c+=dec;
        u+=dec;
                printf("Minimal unit is ");
                outbeaut(u);


/* get elliptic curve, simplify coefficients */
        printf("elliptic curve? ");
        s[0]=0;
        while(!s[0]) gets(s);
        ltop=avma;
        e=lisexpr(s);
        e=gmodulcp(e,m);
        e=smallinitell(e);
        lbot=avma;
        e=gerepile(ltop,lbot,lift(e));

/* get conductor C and test for semi-stable reduction */
        C=conductor(e,m,nf,D,c);
        normC=mnorm(C,m);
        ltop=avma;
        rootC1=gsqrt(gsubst(C,0,GG(nf,6,2)),prec+2);
        rootC2=gsqrt(gsubst(C,0,GG(nf,6,1)),prec+2);
        lbot=avma;
        rootC1=gcopy(rootC1);
        rootC2=gcopy(rootC2);
        dec=lpile(ltop,lbot,0)/4;
        rootC1+=dec;
        rootC2+=dec;
                printf("Conductor is ");
                outbeaut(C);


/* F will be the mth root of u squared. The bound on the mth root of u should be about e for optimal preformance */
        printf("Upper limit on mth root of u? (close to e recommended) ");
        s[0]=0;
        while(!s[0]) gets(s);
        ltop=avma;
        F=lisexpr(s);
        v=gceil(gdiv(glog(u,prec),glog(F,prec)));
        rootF=gpui(u,gdiv(gun,v),prec);
        /* naive limit on number of terms. N.B. low accuracy permissible */
        Lim=gmul(glog(gdeux,3),stoi(32*(prec-2)));
        Lim=gsub(Lim,glog(twopi,3));
```

```
        Lim=gadd(Lim,glog(gdiv(gmul(v,rootF),gsub(gun,gexp(gneg(twopi),3))),3));
        Lim=gadd(Lim,gdiv(glog(gmul(D,normC),3),gdeux));
        /* now adjust for polynomial in Lim */
        v=gdiv(gmul(gsqr(twopi),gadd(rootF,gdiv(gun,rootF))),gmul(D,gsqrt(normC,3)));
        F=gadd(gun,gmul(gadd(Lim,stoi(8)),gadd(gadd(Lim,stoi(8)),v)));
        v=gdiv(gadd(gadd(gmul(gdeux,Lim),stoi(16)),v),F);
        Lim=gadd(Lim,gdiv(glog(F,3),gsub(gun,v)));
        lbot=avma;
        rootF=gcopy(rootF);
        Lim=gcopy(Lim);
        dec=lpile(ltop,lbot,0)/4;
        rootF+=dec;
        Lim+=dec;
        F=gsqr(rootF);
        printf("F= ");
        outbeaut(F);


        l1a=gdiv(gun,rootC1);
        ltop=avma;
        l2la=gmul(rootF,rootC2);
        lbot=avma;
        l2la=gerepile(ltop,lbot,gdiv(gun,l2la));
        l2ua=gdiv(rootF,rootC2);
        l1b=gdiv(l1a,F);
        l2lb=l2ua;
        l2ub=gmul(l2lb,F);

/* now get the sign of the functional equation */
/* this may need to be modified if 2|D and D!=8 */
/* or if C is not coprime to 2 */
        ltop=avma;
        /* first remove 2 from conductor as 2 is awkward */
        if (gcmp0(gmod(normC,gdeux))==TRUE)
                v=gmod(gdiv(C,hcf(C,gdeux,m,GG(nf,6,2))),m);
        else v=C;
        sgn=logsym(gneg(compo(e,11)),v,m);
        /* now treat the 2 case (a1!=0 as reduction is not additive) */
        if (gcmp0(gmod(normC,gdeux))==TRUE) {
                v=gmod(gadd(compo(e,3),gmul(compo(e,2),compo(e,1))),m);
                /* first consider the case where 2 is not split or two */
                /* different primes above 2 are in the conductor */
                if ((gcmp0(gmod(normC,stoi(4)))==TRUE)||
                        (gegal(gmod(D,stoi(8)),stoi(5))==TRUE)) {
                        if (gcmp0(gmod(truecoeff(v,1),gdeux))!=TRUE) sgn=-sgn;
                        }
                /* otherwise there is only one prime above two */
                /* reduce v modulo this prime and invert sgn if this */
                /* is not 0 mod 2 */
                else  {
                        v=simplify(gmod(v,hcf(C,gdeux,m,GG(nf,6,2))));
                        if (gcmp0(gmod(v,gdeux))!=TRUE) sgn=-sgn;
                        }
                }
        /* now multiply this by (-1)^$(prime factors of C) */
        if (bigomega(normC)%2!=0) sgn*=-1;
        /* but non-split primes have been counted twice */
        /* fix this if there is an odd number of them */
        v=gdiv(normC,content(C));
        v=gdiv(v,ggcd(v,D));
        /* this next line would fail for 2|v and D=(3 or 7) mod 8 */
        sgn*=kronecker(D,v);
        printf("sgn=%d\n",sgn);
        lbot=avma;
        gerepile(ltop,lbot,0);

/* L is the number of terms to be calculated, if this is too high you have a chance to interupt the program here */
        ltop=avma;
        L=gmul(gsqr(gdiv(Lim,gmul(stoi(4),gpi))),gmul(gmul(D,rootF),gmul(rootC1,rootC2)));
        lbot=avma;
        L=gerepile(ltop,lbot,gfloor(L));
        printf("L= ");
        outbeaut(L);
        printf("okay to start?");
        s[0]=0;
        while(!s[0]) gets(s);

/* loop to initialize prime power coefficient table */
        ltop=avma;
        for(j=1;gcmp(prime(j),L)<=0;j++);
        lbot=avma;
        A=gerepile(ltop,lbot,cgetg(j,17));
        for(i=1;i<j;i++){
                ltop=avma;
                N=prime(i);
                lbot=avma;
                A[i]=(long)gerepile(ltop,lbot,ppcoeff(m,N,e,L));
```

```
                }

/* first term */
        ltop=avma;
        S=aterm(nf,gun,m,c,sgn);
        H=gdeux;

        while(gcmp(H,L)<=0){
/* add on the coefficient */
                f=factor(H);
                H=cogen(A,H,f,m,c,L);
                for(i=1;i<lg(H[1]);i++) {
                        lbot=avma;
                        S=gadd(S,aterm(nf,gcoeff(H,i,2),m,gcoeff(H,i,1),sgn));
                        }
                H=gadd(H,gun);
                dec=lpile(ltop,lbot,0)/4;
                S+=dec;
                H+=dec;
                }
/* normalize the result and output it */
        S=gmul(S,gdiv(gpui(twopi,stoi(4),0),gsqr(D)));
        outbeaut(S);
}

int legsym(p,q,m)
        GEN p,q,m;
/* calculate natural extension of legendre symbol to quadratic field */
{
        GEN e,f,t;
        int s;
        long ltop,lbot;

        ltop=avma;
        e=content(p);
        p=gdiv(p,e);
        f=content(q);
        q=gdiv(q,f);
        s=kronecker(mnorm(p,m),f)*kronecker(e,mnorm(q,m));
        t=gmul(truecoeff(q,1),gsub(gmul(truecoeff(q,1),truecoeff(p,0)),gmul(truecoeff(p,1),truecoeff(q,0))));
        s=s*kronecker(t,mnorm(q,m));
        lbot=avma;
        gerepile(ltop,lbot,0);
        return(s);
}

GEN conductor(e,m,nf,D,c)
        GEN e,m,nf,D,c;
/* This gets the conductor of e. At the moment it requires e to be semi-stable */
{
        GEN f,v,C;
        long ltop,lbot;
        int i;

        ltop=avma;
        if (gcmpi(hcf(compo(e,10),compo(e,12),m,GG(nf,6,2)))!=TRUE) {
                printf("curve not semi-stable\n");
                exit(1);
                }
        f=factor(mnorm(compo(e,12),m));
        v=gun;
        i=0;
        while(i<lg(f[1])-1) {
        i++;
                v=gmul(v,gcoeff(f,i,1));
                }
        if (gcmpi(ggcd(v,D))!=TRUE)
                v=gmod(gdiv(v,hcf(v,gmul(c,gdiv(D,ggcd(D,gdeux))), m,GG(nf,6,2))),m);
        /* v is the squarefree part over the quadratic field of the */
        /* norm of the determinant assuming D=2 or D=1 mod 4*/
        C=hcf(compo(e,12),v,m,GG(nf,6,2));
        lbot=avma;
        return(gerepile(ltop,lbot,gcopy(C)));
}

GEN hcf(p1,p2,m,r)
        GEN p1,p2,m,r;
/* finds highest common factor of two algebraic integers */
/* this assumes class number 1 (pari's routine is/was unreliable) */
{
        GEN cp,H,p,v,n,a,q1,q2,q;
        long ltop,lbot;

        ltop=avma;
        v=cgetg(3,18);
        v[1]=(long)truecoeff(p1,0);
        v[2]=(long)truecoeff(p1,1);
```

```
        H=gtomat(v);
        v[1]=(long)truecoeff(p2,0);
        v[2]=(long)truecoeff(p2,1);
        H=concat(H,v);
        p=gmod(gmul(p1,polx[0]),m);
        v[1]=(long)truecoeff(p,0);
        v[2]=(long)truecoeff(p,1);
        H=concat(H,v);
        p=gmod(gmul(p2,polx[0]),m);
        v[1]=(long)truecoeff(p,0);
        v[2]=(long)truecoeff(p,1);
        H=concat(H,v);
        lbot=avma;
        H=gerepile(ltop,lbot,hnf(H));
        n=gcoeff(H,1,1);
        p=gadd(gmul(gcoeff(H,2,2),polx[0]),gcoeff(H,1,2));
        cp=content(p);
        if (gegal(n,cp)==TRUE) {
                lbot=avma;
                return(gerepile(ltop,lbot,gcopy(n)));
                }
        cp=gmul(cp,n);
        v=p;
        q=gdiv(p,n);
        p2=gzero;
        q2=gun;
        p1=gun;
        q1=gzero;
        while (gegal(cp,mnorm(v,m))!=TRUE) {
                a=gfloor(gsubst(q,0,r));
                v=gadd(gmul(p1,a),p2);
                p2=p1;
                p1=v;
                v=gadd(gmul(q1,a),q2);
                q2=q1;
                q1=v;
                q=gmod(gdiv(gun,gsub(q,a)),m);
                v=gsub(gmul(p,q1),gmul(p1,n));
                }
        if (gcmp(gsubst(v,0,r),gzero)<0) v=gneg(v);
        lbot=avma;
        return(gerepile(ltop,lbot,gcopy(v)));
}

GEN mnorm(p,m)
        GEN p,m;
/* this calculates the norm of p */
{
        GEN p0,p1,t0,t1;
        long ltop,lbot;

        ltop=avma;
        p0=truecoeff(p,0);
        p1=truecoeff(p,1);
        t0=gmul(gsub(p0,gmul(truecoeff(m,1),p1)),p0);
        t1=gmul(gsqr(p1),truecoeff(m,0));
        lbot=avma;
        return(gerepile(ltop,lbot,gadd(t0,t1)));
}

GEN aterm(nf,a,m,nu,sgn)
        GEN a,m,nf,nu;
        int sgn;
/* this calculates the term in nu with coefficient a */
{
        GEN r,s1,s2,l1,l2l,l2u,e1,e2,z1,z2,u1,u2l,u2u;
        long dec,ltop,lbot,ltop1,lbot1;
        int i;

        ltop=avma;
        if(gcmp0(a)==TRUE) return(gzero);
        r=G(nf,6);
/* e1 and e2 are the exponents l1, l2l, and l2u are the limits */
        e1=gmul(twopi,gsubst(nu,0,G(r,2)));
        e2=gmul(twopi,gsubst(nu,0,G(r,1)));

        ltop1=avma;
        l1=l1a;
        l2l=l2la;
        l2u=l2ua;
/* change limits to ensure our choices upto units don't miss the first region */
        u1=gmul(e1,l1);
        u2l=gmul(e2,l2l);
        if(gcmp(gadd(u1,u2l),Lim)>0)
                while((gcmp(u1,u2l)<0)&&(gcmp(gadd(u1,u2l),Lim)>0)) {
                        lbot1=avma;
                        l1=gmul(l1,F);
```

```
                        l2u=gcopy(l2l);
                        l2l=gdiv(l2l,F);
                        dec=lpile(ltop1,lbot1,0)/4;
                        l1+=dec;
                        l2u+=dec;
                        l2l+=dec;
                        u1=gmul(e1,l1);
                        u2l=gmul(e2,l2l);
                        }

/* now the calculations for the first region */
        s1=gzero;
        s2=gzero;
        while (gcmp(gadd(u1,u2l),Lim)<=0) {
                u2u=gmul(e2,l2u);
        /* don't calculate stray term if it is too small */
                if(gcmp(gadd(u1,u2u),Lim)<=0) {
                    z1=gmul(t1(e1,l1),gsub(t1(e2,l2l),t1(e2,l2u)));
                    z2=gmul(t2(u1),gsub(t2(u2l),t2(u2u)));
                    }
                else {
                    z1=gmul(t1(e1,l1),t1(e2,l2l));
                    z2=gmul(t2(u1),t2(u2l));
                    }
                lbot1=avma;
                s1=gadd(s1,z1);
                s2=gadd(s2,z2);
                l1=gmul(l1,F);
                l2u=gcopy(l2l);
                l2l=gdiv(l2l,F);
                dec=lpile(ltop1,lbot1,0)/4;
                l1+=dec;
                l2u+=dec;
                l2l+=dec;
                s1+=dec;
                s2+=dec;
                u1=gmul(e1,l1);
                u2l=gmul(e2,l2l);
                }
        lbot1=avma;
        s1=gcopy(s1);
        s2=gcopy(s2);
        dec=lpile(ltop1,lbot1,0)/4;
        s1+=dec;
        s2+=dec;

/* set limits for the second region */
        ltop1=avma;
        l1=l1b;
        l2l=l2lb;
        l2u=l2ub;
/* change limits again if necessary */
        u1=gmul(e1,l1);
        u2l=gmul(e2,l2l);
        if(gcmp(gadd(u1,u2l),Lim)>0)
                while((gcmp(u1,u2l)>0)&&(gcmp(gadd(u1,u2l),Lim)>0)) {
                        lbot1=avma;
                        l1=gdiv(l1,F);
                        l2l=gcopy(l2u);
                        l2u=gmul(l2u,F);
                        dec=lpile(ltop1,lbot1,0)/4;
                        l1+=dec;
                        l2l+=dec;
                        l2u+=dec;
                        u1=gmul(e1,l1);
                        u2l=gmul(e2,l2l);
                        }

/* calculations for the second region */
        while (gcmp(gadd(u1,u2l),Lim)<=0) {
                u2u=gmul(e2,l2u);
        /* don't calculate stray term if it is too small */
                if(gcmp(gadd(u1,u2u),Lim)<=0) {
                    z1=gmul(t1(e1,l1),gsub(t1(e2,l2l),t1(e2,l2u)));
                    z2=gmul(t2(u1),gsub(t2(u2l),t2(u2u)));
                    }
                else {
                    z1=gmul(t1(e1,l1),t1(e2,l2l));
                    z2=gmul(t2(u1),t2(u2l));
                    }
                lbot1=avma;
                s1=gadd(s1,z1);
                s2=gadd(s2,z2);
                l1=gdiv(l1,F);
                l2l=gcopy(l2u);
                l2u=gmul(l2u,F);
                dec=lpile(ltop1,lbot1,0)/4;
```

```
                l1+=dec;
                l2l+=dec;
                l2u+=dec;
                s1+=dec;
                s2+=dec;
                u1=gmul(e1,l1);
                u2l=gmul(e2,l2l);
                }
        if (sgn==1) s1=gadd(s1,gdiv(s2,normC));
        else s1=gsub(s1,gdiv(s2,normC));
        lbot=avma;
        return(gerepile(ltop,lbot,gmul(a,s1)));
}

/* these next two routines evaluate individual terms. If you want to evaluate the L-series at s not equal two,
   these routines are essentially all you need to change (you might also need to look at what accuracy you get) */
GEN t1(x,l)
        GEN x,l;
{
        GEN z0,z1;
        long ltop,lbot;

        ltop=avma;
        z0=gadd(gdiv(l,x),gdiv(gun,gsqr(x)));
        z1=gexp(gneg(gmul(l,x)),prec);
        lbot=avma;
        return(gerepile(ltop,lbot,gmul(z0,z1)));
}

GEN t2(x)
        GEN x;
{
        return(eint1(x,prec));
}

GEN ppcoeff(m,p,e,L)
        GEN m,p,e,L;
/* calculate points on each reduced curve mod primes above p */
/* and corresponding prime power coefficients */
{
        GEN p1,r,s;
        long ltop,lbot;
        int i;

        ltop=avma;
        r=cgetg(3,17);
        r[1]=(long)p;
        p1=lift(factmod(m,p));
        if(lg(p1[1])==3){
/* p is split */
                p1=spos(p,m,p1);
                s=cgetg(3,19);
                for(i=1;i<=2;i++){
                        s[i]=(long)ratred(e,p,gcoeff(p1,i,1),gcoeff(p1,i,2));
                        s[i]=(long)gtrans(coadd(s[i],p,L));
                        }
                r[2]=(long)gtrans(s);
                }
        else if(gegal(gcoeff(p1,1,2),gdeux)==TRUE){
/* p is ramified */
                p1=spos(p,m,p1);
                s=ratred(e,p,gcoeff(p1,1,1),gcoeff(p1,1,2));
                r[2]=(long)gtomat(coadd(s,p,L));
                }
        else {
/* p is non-split */
                s=quadred(e,p,m,L);
                r[2]=(long)gtomat(coadd(s,gsqr(p),L));
                }
        lbot=avma;
        return(gerepile(ltop,lbot,gcopy(r)));
}

GEN ratred(e,p,m1,p1)
        GEN e,p,m1,p1;
/* reduced curve is equivalent to one over Q at p, calculate */
/* number of points and reduction */
{
        GEN n,s;
        long ltop,lbot;

        ltop=avma;
        e=gcopy(e);
        setlg(e,6);
        e=simplify(gmod(e,m1));
        e=smallinitell(e);
        n=apell(e,p);
```

```
        if (gcmp0(gmod(compo(e,12),p))==TRUE)
                s=concat(p1,concat(gzero,n));
        else    s=concat(p1,concat(gun,n));
        lbot=avma;
        return(gerepile(ltop,lbot,gcopy(s)));
}

GEN quadred(e,p,m,L)
        GEN e,p,m,L;
/* calculate reduction and number of points over F_{p^2} */
{
        GEN p2,n,s,x,y,z;
        long ltop,lbot,ltop1,lbot1;
        int i,j,k,l,q;

        ltop=avma;
        p2=gsqr(p);
        if(gcmp(p2,L)>0){
/* p is too big to matter */
                s=concat(gzero,gzero);
                lbot=avma;
                s=concat(p,s);
                }
        else if(gegal(p,gdeux)==TRUE){
/* 2 is awkward (naive count of points) */
                e=gcopy(e);
                setlg(e,6);
                e=smallinitell(gmodulcp(gmul(e,gmodulcp(gun,p)),m));
                n=gun;
                q=gtolong(p);
                for (i=0;i<q;i++) {
                  for (j=0;j<q;j++) {
                    x=gmodulcp(gadd(stoi(i),gmul(stoi(j),polx[0])),m);
                    z=gadd(compo(e,5),gmul(x,gadd(compo(e,4),gmul(x,gadd(compo(e,2),x)))));
                    for (k=0;k<q;k++) {
                      for (l=0;l<q;l++) {
                        y=gmodulcp(gadd(stoi(k),gmul(stoi(l),polx[0])),m);
                        if(gegal(z,gmul(y,gadd(y,gadd(gmul(compo(e,1),x),compo(e,3)))))==TRUE) {
                                n=gadd(n,gun);
                                }
                        }
                      }
                    }
                  }
                n=gsub(gadd(p2,gun),n);
                if (gcmp0(lift(lift(compo(e,12))))==TRUE)
                        s=concat(p,concat(gzero,n));
                else    s=concat(p,concat(gun,n));
                }
        else {
/* default */
/* p is non-split and not large (get curve in form y^2=f(x)), mark values on
   RHS and add those which occur on LHS */
                ltop1=avma;
                e=gcopy(e);
                setlg(e,6);
                e=smallinitell(gmodulcp(gmul(e,gmodulcp(gun,p)),m));
                x=concat(concat(gun,gzero),concat(gdiv(compo(e,1),gneg(gdeux)),gdiv(compo(e,3),gneg(gdeux))));
                lbot1=avma;
                e=coordch(e,x);
                e=gerepile(ltop1,lbot1,e);
                ltop1=avma;
                q=gtolong(p);
                s=gscalsmat(0,q);

                for (i=0;i<q;i++) {
                  for (j=0;j<q;j++) {
                    x=gmodulcp(gmul(gmodulcp(gun,p),gadd(stoi(i),gmul(stoi(j),polx[0]))),m);
                    z=gadd(compo(e,5),gmul(x,gadd(compo(e,4),gmul(x,gadd(compo(e,2),x)))));
                    y=lift(lift(z));
                    k=1+gtolong(truecoeff(y,0));
                    l=1+gtolong(truecoeff(y,1));
                    lGG(s,k,l)=(long)gadd(gun,compo(compo(s,k),l));
                    }
                  lbot1=avma;
                  s=gerepile(ltop1,lbot1,gcopy(s));
                  }
                ltop1=avma;
                n=gun;
                for (i=0;i<q;i++) {
                  for (j=0;j<q;j++) {
                    x=gmodulcp(gmul(gmodulcp(gun,p),gadd(stoi(i),gmul(stoi(j),polx[0]))),m);
                    z=gmul(x,x);
                    y=lift(lift(z));
                    k=1+gtolong(truecoeff(y,0));
                    l=1+gtolong(truecoeff(y,1));
                    n=gadd(n,compo(compo(s,k),l));
```

```
                }
                lbot1=avma;
                n=gerepile(ltop1,lbot1,gcopy(n));
                }
              n=gsub(gadd(gsqr(p),gun),n);
              if (gcmp0(lift(lift(compo(e,12))))==TRUE)
                    s=concat(p,concat(gzero,n));
              else        s=concat(p,concat(gun,n));
              }
        return(gerepile(ltop,lbot,s));
}

GEN spos(p,m,p1)
        GEN p,m,p1;
/* get totally positive generators for ideals over p */
/* This assumes narrow class number one and uses trial and error method */
{
        GEN n,f;
        long ltop,lbot;
        int i;

        ltop=avma;
        n=gun;
        f=factor(gsub(p,m));
        while(gcmpi(compo(matsize(f),1))==TRUE) {
              n=gadd(n,gun);
                        if(gcmp(n,stoi(100))>=0) printf("!");
              f=factor(gsub(p,gmul(gsqr(n),m)));
              }
        n=gcoeff(f,1,1);
        if(lg(p1[1])==3) {
              if(gcmp0(gmod(subres(gcoeff(p1,1,1),n),p))==TRUE) i=0;
              else i=1;
              if(gsigne(truecoeff(n,0))>0)
                    coeff(p1,1+i,2)=(long)n;
              else        coeff(p1,1+i;2)=(long)gneg(n);
              n=gcoeff(f,2,1);
              if(gsigne(truecoeff(n,0))>0)
                    coeff(p1,2-i,2)=(long)n;
              else        coeff(p1,2-i,2)=(long)gneg(n);
              }
        else {
              if(gsigne(compo(n,1))*gsigne(compo(n,2))<0)
                    n=gcoeff(f,2,1);
              if(gsigne(truecoeff(n,0))>0)
                    coeff(p1,1,2)=(long)n;
              else        coeff(p1,1,2)=(long)gneg(n);
              }
        lbot=avma;
        return(gerepile(ltop,lbot,gcopy(p1)));
}

GEN coadd(s,q,L)
        GEN s,q,L;
/* add coefficients of the prime powers */
{
        GEN c,v;
        long ltop,lbot;
        int i;
        ltop=avma;
        c=gsqr(q);
        if(gcmp(c,L)<=0) {
            i=(gexpo(L)+1)/gexpo(q);
            v=cgetg(i+1,17);
            if(gcmp0(compo(s,2))==TRUE)
                for(i=1;gcmp(c,L)<=0;i++){
                    if (i%2==0) v[i]=(long)compo(s,3);
                    else        v[i]=(long)gsqr(compo(s,3));
                    c=gmul(q,c);
                    }
                else for(i=1;gcmp(c,L)<=0;i++){
                    if (i==1)       v[1]=(long)gsub(gsqr(compo(s,3)),q);
                    else if (i==2) v[2]=(long)gmul(compo(s,3),gsub(compo(v,1),q));
                    else v[i]=(long)gsub(gmul(compo(s,3),compo(v,i-1)),gmul(q,compo(v,i-2)));
                    c=gmul(q,c);
                    }
                setlg(v,i);
                lbot=avma;
                v=concat(s,v);
                }
        else {
                lbot=avma;
                v=gcopy(s);
                }
        return(gerepile(ltop,lbot,v));
}
```

```
GEN cogen(A,N,f,m,c,L)
        GEN A,N,f,m,c,L;
/* generate coefficients for a composite number */
{
        GEN H,p,pp,pm,r1,r2,s,s2;
        long ltop,lbot,ltop1,lbot1;
        int i,j,k,kk,l;

        ltop=avma;
        l=lg(f[1])-1;
        H=N;
        for(i=1;i<=l;i++) {
                p=gcoeff(f,i,1);
                for(j=1;gegal(p,compo(compo(A,j),1))!=TRUE;j++);
                pp=GG(A,j,1);
                pm=GG(A,j,2);
                if((lg(pm[1])!=3)&&(gegal(pp,gcoeff(pm,1,1))==TRUE)) H=gmul(H,gpui(pp,gcoeff(f,i,2),0));
                }
        if(gcmp(H,L)>0) {
                H=concat(gun,gzero);
                lbot=avma;
                return(gerepile(ltop,lbot,gtomat(H)));
                }
        H=gtomat(concat(c,gun));

        for(i=1;i<=l;i++) {
                p=gcoeff(f,i,1);
                k=gtolong(gcoeff(f,i,2));
                for(j=1;gegal(p,compo(compo(A,j),1))!=TRUE;j++);
                pp=GG(A,j,1);
                pm=GG(A,j,2);
                if(lg(pm[1])==2) {
                    r1=gmod(gmul(G(H,1),gpui(gcoeff(pm,1,1),gcoeff(f,i,2),0)),m);
                    r2=gmul(G(H,2),gcoeff(pm,1,k+2));
                    }
                else {
                        ltop1=avma;
                        lbot1=avma;
                        r1=gtrans(G(pm,1));
                        while(lg(r1)<(k+2)) {
                                s=gmod(gmul(G(r1,lg(r1)-1),gcoeff(pm,2,1)),m);
                                r1=gmod(gmul(r1,gcoeff(pm,1,1)),m);
                                lbot1=avma;
                                r1=concat(r1,s);
                                }
                        if(ltop1!=lbot1) r1=gerepile(ltop1,lbot1,r1);
                        if(k==1) r2=gtrans(G(pm,3));
                        else {
                            ltop1=avma;
                            r2=gcoeff(pm,1,k+2);
                            for(kk=1;kk<k;kk++)
                                r2=concat(r2,gmul(gcoeff(pm,1,k+2-kk),gcoeff(pm,2,2+kk)));
                            lbot1=avma;
                            r2=gerepile(ltop1,lbot1,concat(r2,gcoeff(pm,2,k+2)));
                            }
                        s=gmod(gmul(G(H,1),r1),m);
                        s2=gmul(G(H,2),r2);
                        r1=compo(s,1);
                        r2=compo(s2,1);
                        for(kk=1;kk<lg(s)-1;kk++) {
                                r1=concat(r1,G(s,kk+1));
                                r2=concat(r2,G(s2,kk+1));
                                }
                        }
                r1=gtomat(r1);
                lbot=avma;
                H=gerepile(ltop,lbot,concat(r1,r2));
                }
        return(H);
}
```

Now we have my program for calculating Eisenstein-Kronecker-Lerch series for real elliptic curves.

```
/* calculates chi(x_0) to specified precision on lattice generated by 1 and tau */

#include <stdio.h>
#include <genpari.h>

#define TRUE 1

long prec;
GEN chi();
GEN tm1();
GEN tm2();

main()
{
        GEN A,x,w,t,tau,lim,m,n;
        char s[512];
        long lbot,ltop,dec;

        prec=8;
        init(1000000,2);
        setprecr((long) (prec/K1));
        constpi(prec);
        polx[0]=lisexpr("x");

        printf("lattice generator(other than 1)?");
        s[0]=0;
        while(!s[0]) gets(s);
        tau=lisexpr(s);
        if(gcmp(gimag(tau),gzero)<0) tau=gneg(tau);
        printf("x0?");
        s[0]=0;
        while(!s[0]) gets(s);
        x=lisexpr(s);

        ltop=avma;
        x=gsub(x,gmul(gfloor(gdiv(gimag(x),gimag(tau))),tau));
        x=gsub(x,gfloor(greal(x)));
        lbot=avma;
        x=gerepile(ltop,lbot,gcopy(x));

        ltop=avma;
        A=gdiv(gimag(tau),gpi);
        lbot=avma;
        A=gerepile(ltop,lbot,gcopy(A));

        lim=gsqrt(gmul(gmul(glog(gdeux,prec),stoi(prec*32)),A),prec);
        t=gzero;
        ltop=avma;
        n=gfloor(gdiv(lim,gimag(tau)));
        while (gcmp_1(n)==0) {
                m=gsqrt(gsub(gsqr(lim),gsqr(gmul(n,gimag(tau)))),prec);
                if (gcmp0(n)==0) w=gsub(gmul(n,tau),gfloor(gadd(m,gmul(n,greal(tau)))));
                else w=gun;
                while (gcmp(m,greal(w))!=-1) {
                        t=gadd(t,tm1(w,x,A));
                        t=gadd(t,tm1(gneg(w),x,A));
                        w=gadd(w,gun);
                        }

                n=gsub(n,gun);
                lbot=avma;
                t=gcopy(t);
                n=gcopy(n);
                dec=lpile(ltop,lbot,0)/4;
                t+=dec;
                n+=dec;
                }

        n=gneg(gfloor(gdiv(gadd(lim,gimag(x)),gimag(tau))));
        while (gcmp(gadd(gmul(n,gimag(tau)),gimag(x)),lim)!=1) {
                m=gsqrt(gsub(gsqr(lim),gsqr(gadd(gmul(n,gimag(tau)),gimag(x)))),prec);
                w=gsub(gmul(n,tau),gfloor(gadd(gadd(m,greal(x)),gmul(n,greal(tau)))));
                while (gcmp(m,gadd(greal(w),greal(x)))!=-1) {
                        t=gadd(t,tm2(w,x,A));
                        w=gadd(w,gun);
                        }

                n=gadd(n,gun);
                lbot=avma;
                t=gcopy(t);
                n=gcopy(n);
```

```
                dec=lpile(ltop,lbot,0)/4;
                t+=dec;
                n+=dec;
                }
        t=gmul(gsqr(gimag(tau)),t);
        outbeaut(t);
}

GEN chi(w,x,A)
        GEN w,x,A;
{
        GEN y,z;

        z=gimag(gdiv(gmul(gmul(w,gconj(x)),gdeux),A));
        if (expo(z)<-prec*16) y=gadd(gun,gmul(z,gi));
        else                  y=gexp(gmul(z,gi),prec);
        return(y);
}

GEN tm1(w,x,A)
        GEN w,x,A;
{
        GEN t,e,ms;

        ms=greal(gmul(w,gconj(w)));
        e=gexp(gneg(gdiv(ms,A)),prec);
        t=gmul(gmul(chi(w,x,A),e),gdiv(gadd(gun,gdiv(ms,A)),gmul(w,ms)));
        return(t);
}

GEN tm2(w,x,A)
        GEN w,x,A;
{
        GEN t,ms,xaw;

        xaw=gadd(x,w);
        ms=greal(gmul(xaw,gconj(xaw)));
        t=gdiv(gmul(gconj(xaw),eint1(gdiv(ms,A),prec)),gmul(A,A));
        return(t);
}
```

Bibliography

[1] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Mathematische Annalen **185** (1970), 134–160.

[2] A. A. Beilinson, *Higher regulators and values of L-functions of curves*, Functional Analysis and its Applications **14** (1980), 116–118.

[3] ———, *Higher regulators and values of L-functions*, Journal of Soviet Mathematics **30** (1985), 2036–2070.

[4] S. Bloch and D. Grayson, K_2 *and L-functions of elliptic curves, computer calculations*, Applications of algebraic K-theory to algebraic geometry and number theory, part I, Boulder 1983, Contemporary Mathematics, vol. 55, pp. 79–88.

[5] Spencer Bloch, *Algebraic K-theory and zeta functions of elliptic curves*, Proceedings of the International Congress of Mathematicians, Helsinki 1978, vol. 2, pp. 511–515.

[6] H. Cohen C. Batut, D. Bernardi and M. Olivier, *PARI*, available via anonymous ftp at megrez.math.u-bordeaux.fr/pub/pari/.

[7] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1992.

[8] C. Deninger and K. Wingberg, *On the Beilinson conjectures for elliptic curves with complex multiplication*, Beilinson's conjectures on special values of L-functions, Perspectives in mathematics, vol. 4, pp. 249–272.

[9] Howard Garland, *A finiteness theorem for K_2 of a number field*, Annals of Mathematics **94** (1971), 534–548.

[10] Dan Grayson and Norbert Schappacher, *On symbols in $K_2(E)\otimes\mathbb{Q}$ from points of infinite order*, very preliminary version.

[11] Daniel R. Grayson, *Higher algebraic K-theory: II (after Daniel Quillen)*, Algebraic K-theory, Evanston 1976, Lecture Notes in Mathematics, vol. 551, pp. 217–240.

[12] ———, *Localization for flat modules in algebraic K-theory*, Joural of Algebra **61** (1979), 463–496.

[13] Jean-François Mestre and Norbert Schappacher, *Séries de Kronecker et fonctions L des puissances symétriques de courbes elliptiques sur $\mathbb{Q}$*, Arithmetic Algebraic Geometry, (Texel 1989), Progress in Mathematics, vol. 89, pp. 209–245.

[14] John Milnor, *Introduction to algebraic K-theory*, Annals of Mathematics Studies, vol. 72, Princeton University Press, 1971.

[15] D. Quillen, *Higher algebraic K-theory: I*, Algebraic K-theory I, Battelle Institute conference 1972, Lecture Notes in Mathematics, vol. 341, pp. 85–147.

[16] David E. Rohrlich, *Elliptic curves and values of L-functions*, Number theory, Proceedings of the 1985 Montreal Conference held June 17-29, 1985, Canadian Mathematical Society Conference Proceedings, vol. 7, pp. 371–387.

[17] Klaus Rolshausen, Ph.D. thesis, Strasbourg, 1995, Preliminary version.

[18] Raymond Ross, *K_2 of Fermat curves and values of L-functions*, Comptes rendus, Académie des Sciences, Paris **312** (1991), 1–5.

[19] ———, *K_2 of elliptic curves with sufficient torsion over $\mathbb{Q}$* , Compositio Mathematica **81** (1992), 211–221.

[20] Norbert Schappacher and Anthony J. Scholl, *The boundary of the Eisenstein symbol*, Mathematische Annalen **290** (1991), 303–321,815.

[21] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate texts in mathematics, vol. 106, Springer-Verlag, 1986.

[22] C. Soulé, *Groupes de Chow et K-théorie de variétés sur un corps fini*, Mathematische Annalen **268** (1984), 317–345.

[23] V. Srinivas, *Algebraic K-theory*, Progress in Mathematics, vol. 90, Birkhäuser, 1991.

[24] H.P.F. Swinnerton-Dyer et al., *Table 1*, Modular Functions of One Variable IV, Antwerp 1972, Lecture Notes in Mathematics, vol. 476, pp. 81–113.

[25] John Tate, *Symbols in arithmetic*, Actes du Congrès International des Mathématiciens, Nice 1970, vol. 1, pp. 201–211.

[26] Gerard van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete; 3. Folge, vol. 16, Springer-Verlag, 1988.

[27] André Weil, *Elliptic functions according to Eisenstein and Kronecker*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 88, Springer-Verlag, 1976.

[28] Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), 443–551.