Modular Forms and Elliptic Curves over Imaginary Quadratic Fields

J. E. Cremona

April 1998

1 Introduction

The talk given at the conference was a survey describing the almost entirely conjectural correspondence between certain modular forms and elliptic curves defined over imaginary quadratic fields. Most of this work, apart from some recent examples computed over the field $\mathbb{Q}(\sqrt{-5})$ with class number 2, has already appeared in print. Here we give a summary with references to published papers for more details.

Most of the work described here was carried out by the author together with his students E. Whitley and J.S. Bygott.

1.1 Overall goals

The overall goal of this project is to develop a better understanding of, and a more explicit description of, a Shimura-Taniyama-Weil type correspondence between elliptic curves and modular forms defined over number fields other than $\mathbb{Q}$, and particularly over imaginary quadratic fields. The project has been under way since the early 1970s, and lays a particular emphasis on explicit constructions and the computation of particular examples. As is often the case in number theory, the understanding of specific examples in detail often plays an important part in guiding more theoretical developments, and in the formulation of explicit conjectures.

1.2 Some specific questions

Let K be a number field. We are interested in the following questions concerning modular forms and elliptic curves defined over K.

1. What do modular forms over K look like?
2. Can they be computed explicitly (say for given weight and level)?
3. Do they have associated L-series, with functional equations and interesting arithmetic properties, such as Fourier coefficients of number-theoretical interest or significant special values?
4. Do they have associated Galois representations?
5. What does it mean for an elliptic curve defined over K to be modular?

6. Are all elliptic curves over K modular?
7. Is it possible to construct modular elliptic curves over K explicitly?
8. If E is a modular elliptic curve over K, can we use the associated modular form to obtain arithmetic information about $E(K)$, in line with the Birch–Swinnerton-Dyer conjectures?

Over the field $\mathbb{Q}$, these questions are very well understood, as are most of the answers. Much has been proved, notably the recent results of Wiles and Taylor-Wiles concerning the modularity of "most" elliptic curves over $\mathbb{Q}$: see Diamond's talk for the latest results on this. However, even over $\mathbb{Q}$ there are substantial outstanding questions such as the Birch–Swinnerton-Dyer conjectures, for which almost nothing has been proved for curves of rank greater than 1.

Over a totally real field K, there is a well-developed theory of Hilbert Modular Forms. Their study requires adelic methods to deal efficiently with the infinite unit group and (possibly) nontrivial ideal class group. The same is true for general number fields. Nevertheless, one of our reasons for beginning with imaginary quadratic fields of class number one was that these complications do not arise, and a non-adelic treatment is possible.

In greater generality we may consider modular forms over general global fields. There is a wide literature concerning these "automorphic forms for GL(2)", and also for more general algebraic groups. See, for examples Weil's 1971 book [15] and also Gelbart [8] for the GL(2) case. Finally, one can go further and replace automorphic forms by automorphic representations, where again there is a vast literature.

One of our aims has been to specialize this general theory to the case of an imaginary quadratic field, in order to arrive at as concrete a description as possible of automorphic forms over these fields, amenable to explicit computations.

1.3 Recent history of the problem

1970s and 1980s: Mennicke, Grunewald, Elstrodt and others carried out some explicit computations over $\mathbb{Q}(\sqrt{-d})$ for $d = 1, 2, 3$, for split prime levels and weight 2. They produced tables of newforms and corresponding examples of curves. See [10] for a description of some of this work and further references.

1970s: Kurčanov [13] extended some of Manin's results over $\mathbb{Q}$, including the Manin-Drinfeld Theorem, to imaginary quadratic fields. The duality between spaces of cusp forms of weight 2 and the homology of quotients of hyperbolic 3-space is clearly set up, together with the definition of generalized modular symbols giving explicit generators for the homology.

From 1978: Cremona extended the work of Mennicke et al. to all five Euclidean fields ($d = 1, 2, 3, 7, 11$) and arbitrary levels, using more hyperbolic geometry and modular symbols. Extensive tables of newforms and associated elliptic curves were produced: see [3].

1987–1990: Cremona's student Whitley extended this to the four other fields of class number 1 ($d = 19, 43, 67, 163$) and produced more tables.

1990–1993: Cremona and Whitley looked more closely at arithmetic aspects of the newform–curve correspondence, computing and comparing periods, analytic ranks and other data appearing in the Birch–Swinnerton-Dyer conjectures.

Early 1990s: R. Taylor succeeded in constructing ℓ-adic Galois representations associated to automorphic forms over $K = \mathbb{Q}(\sqrt{-3})$. Explicit examples, computed with Cremona, showed that certain elliptic curves defined over K (and not over $\mathbb{Q}$) were modular in a weak sense.

From 1993: Cremona's student Bygott extends the methods of Cremona and Whitley to fields of higher class number, and produces tables of newforms over $\mathbb{Q}(\sqrt{-5})$ (class number 2).

2 The correspondence between elliptic curves and modular forms

2.1 The correspondence over $\mathbb{Q}$

The relevant modular forms over $\mathbb{Q}$ are newforms $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z}$ for $\Gamma_0(N)$ of weight 2 and rational integer coefficients a_n. Such a form has an L-series

$$\Lambda(f,s) = \int_0^\infty y^{s-1} f(iy)dy$$

which is analytic for all complex s and for $\Re(s) > 3/2$ is given by a Dirichlet series:

$$\Lambda(f,s) = (2\pi)^{-s}\Gamma(s)L(f,s)$$

where

$$L(f,s) = \sum_{n\geq 1} a_n n^{-s}.$$

The coefficients a_n are determined by multiplicative relations from the a_p for prime p; these multiplicative relations can be summarized by the statement that $L(f,s)$ has an Euler product

$$L(f,s) = \prod_p^{*} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where the product is over all primes and the * indicates that the factors for p dividing N need modification. So this Dirichlet series has analytic continuation to $\mathbb{C}$, and $\Lambda(f,s)$ satisfies a functional equation linking its values at s and $2-s$, easily derived from the action of the Fricke involution $z \mapsto -1/Nz$ on $f(z)$.

On the other hand, we consider isogeny classes of elliptic curves defined over $\mathbb{Q}$ with conductor N, which also have an L-series $L(E,s)$ defined for $\Re(s) > 3/2$, of exactly the same form as that just given for $L(f,s)$. Now the coefficients a_p in the Euler product are determined by the reduction of the curve E modulo p.

Unlike the situation for $L(f,s)$, it is not known in general that $L(E,s)$ has an analytic continuation to the whole complex plane and satisfies a functional equation, though this has long been conjectured. Essentially the only way of proving this is to show that E is modular, so that $L(E,s) = L(f,s)$ for a suitable newform f. The exception is the case of elliptic curves with complex multiplication (CM) where the conjectured properties were proved directly by Weil and Deuring. The Shimura-Taniyama-Weil conjecture states that all elliptic curves are modular in the above sense. At the time of the conference this was known to be true provided that the conductor N is not divisible by 27: see Diamond's talk for details of this result, which extends the earlier results of Wiles, Taylor-Wiles and Diamond.

Given a rational newform $f(z)$ (of weight 2 for $\Gamma_0(N)$ as above) the construction of Eichler and Shimura associates to f the elliptic curve $E_f = \mathbb{C}/\Lambda_f$ where Λ_f is the lattice of periods of the differential $2\pi i f(z)dz$. It is a deep result that this elliptic curve E_f is defined over $\mathbb{Q}$, has conductor N, and the L-series $L(E_f, s)$ and $L(f, s)$ coincide. See Knapp's book [12] for a detailed account of this. On the practical side, for reasonably small levels N one can find all the newforms f and hence construct the modular elliptic curves E_f explicitly: see the author's book [6] for details of this.

In the other direction, given an elliptic curve E, Weil's converse to Hecke theory states (essentially) that provided that $L(E, s)$ and sufficiently many of its twists $L(f, \chi, s)$ satisfy the appropriate functional equations, then $L(E, s) = L(f, s)$ for a newform f. It then follows by the isogeny theorem of Serre-Faltings that E is isogenous to E_f, so that E is modular.

2.2 Cusp forms of weight 2 over an imaginary quadratic field

Before we describe the (much more fragmentary) picture over the field $K = \mathbb{Q}(\sqrt{-d})$, we must first briefly describe what cusp forms of weight 2 look like over such a field. For simplicity we assume here that K has class number 1. See [7] for a little more detail and further references.

We denote by $\mathcal{H}_3$ hyperbolic 3-space, which plays the same role as the upper half-plane in the classical situation:

$$\mathcal{H}_3 = \mathbb{C} \times \mathbb{R}_+ = \{(z, t) \mid z \in \mathbb{C}, t > 0\}.$$

The group $\mathrm{GL}(2, \mathbb{C})$ acts on $\mathcal{H}_3$ via hyperbolic isometries. The action is most concisely written using quaternion notation: identifying the point (z, t) with the quaternion $q = z + tj$, the action is given by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : q \mapsto (\alpha q + \beta)(\gamma q + \delta)^{-1}.$$

Let R be the ring of integers of K, and $\Gamma = \mathrm{PSL}(2, R)$ the so-called Bianchi group. Then Γ acts discretely on $\mathcal{H}_3$, with a fundamental region of finite volume bounded by various geodesic planes. (These fundamental regions were first studied systematically by Bianchi in [1].) For an ideal $\mathfrak{n}$ of R we define the congruence subgroup $\Gamma_0(\mathfrak{n})$ in the usual way, as the subgroup consisting of matrices congruent to $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ modulo $\mathfrak{n}$.

A cusp form of weight 2 for $\Gamma_0(\mathfrak{n})$ is a vector-valued function

$$F = (F_0, F_1, F_2) : \mathcal{H}_3 \to \mathbb{C}^3$$

such that $-F_0 \frac{dz}{t} + F_1 \frac{dt}{t} + F_2 \frac{d\bar{z}}{t}$ is a $\Gamma_0(\mathfrak{n})$-invariant harmonic differential on $\mathcal{H}_3$, well-behaved at the cusps. (More generally, forms of weight k take values in $\mathbb{C}^{k+1}$.) Such a function F has a Fourier expansion (about the cusp $(0, \infty)$) of the form

$$F(z, t) = \frac{16\pi^2 w_K}{|D_K|} \sum_{\mathfrak{a}} c(\mathfrak{a}) t^2 \mathbf{K}(4\pi |\eta|^{-1} |\alpha| t) \psi(\eta^{-1} \alpha z)$$

where D_K denotes the discriminant of K, w_K the number of units, η generates the different of K, $\psi(z) = \exp(2\pi i(z + \overline{z}))$, $\mathbf{K}(t)$ is the vector-valued K-Bessel function

$$\mathbf{K}(t) = (-\frac{1}{2}iK_1(t), K_0(t), \frac{1}{2}iK_1(t))$$

and $\mathfrak{a} = \alpha R$ runs over all the (nonzero) ideals of R.

It may be helpful to compare this expansion with the Fourier expansion of an ordinary cusp form over $\mathbb{Q}$, separating the real and imaginary parts of the variable $z = x + yi$ in the upper half-plane:

$$2\pi i f(z) = 2\pi i f(x,y) = 2\pi i \sum_n a_n \exp(-2\pi n y)\exp(2\pi i n x),$$

where the sum is over the integral ideals $n\mathbb{Z}$ of $\mathbb{Z}$, we have a rapidly decaying negative exponential term $\exp(-2\pi n y)$ instead of the K-Bessel function, and the real additive character $\exp(2\pi i x)$ instead of the complex additive character $\psi(z)$.

2.3 The correspondence over an imaginary quadratic field

On the modular forms side, we consider newforms $F(z,t)$ for $\Gamma_0(\mathfrak{n})$ with rational integer Fourier coefficients $c(\alpha)$. These are eigenforms of a suitable Hecke algebra, and via Mellin transform we obtain an L-series which analytically continues a Dirichlet series with Euler product, all just as in the rational case:

$$\Lambda(F,s) = \int_0^\infty t^{2s-2}F_1(0,t)dt = \frac{w_K}{4}|D_K|^{s-1}(2\pi)^{-2s}\Gamma(s)^2 L(F,s)$$

where

$$L(F,s) = \sum_{\mathfrak{a}} c(\mathfrak{a})N(\mathfrak{a})^{-s}.$$

So the Dirichlet series $L(F,s)$ has an analytic continuation, and using a Fricke-type involution we may easily derive a functional equation for $\Lambda(F,s)$. (See [7] for the details.)

On the other hand, we have isogeny classes of elliptic curves E defined over K of conductor $\mathfrak{n}$, which have L-series of the same form

$$L(E,s) = \sum_{\mathfrak{a}} c(\mathfrak{a})N(\mathfrak{a})^{-s}$$

defined as usual by an Euler product which converges for $\Re(s) > 3/2$. The adjusted series $\Lambda(E,s)$ is obtained by multiplying by the same gamma factors as for $\Lambda(F,s)$, and is conjectured to have an analytic continuation to the whole complex plane and to satisfy a functional equation.

As before, provided that $\Lambda(E,s)$ and sufficiently many of its twists do indeed satisfy functional equations, one can show that $L(E,s) = L(F,s)$ for a suitable modular form. This is proved (in greater generality) in Weil's book [15]. But there are essentially no cases for which these functional equations are known to hold, apart from curves which are defined over $\mathbb{Q}$ or their twists (this includes CM curves defined over K, since we are currently assuming that K has class number 1).

One exceptional case is worth mentioning here: if the curve E has CM by an order in the field K itself, then it is known that $L(E,s) = L(F,s)$ where F is not a cusp form but an Eisenstein series. For in this situation we have (up to twist) that E is defined over $\mathbb{Q}$, and it known that the base-change lift from $\mathbb{Q}$ to K of a cusp form f is again a cusp form except in this one case, when f has CM in K itself.

In the other direction, there is no analogue of the Eichler-Shimura construction to construct an elliptic curve from a cusp form of weight 2 with rational Fourier coefficients, say via periods. This lack is one of the biggest mysteries in this area. We can define (and explicitly compute, see below) the periods of (the harmonic differential associated to) F, but these form a 1-dimensional lattice in $\mathbb{R}$ rather than a 2-dimensional lattice in $\mathbb{C}$. The generator $\Omega(F)$ of this lattice does seem to be related to the period lattice of an associated elliptic curve (when we have one), as we will see in the examples below, but the periods of the form F do not appear to contain enough information to construct an elliptic curve. Such a construction (described as a "pipe dream" by Mennicke in [10]) would be a very significant breakthrough. However, there are cases, which are well understood, in which a newform F has no associated elliptic curve E defined over K. We give an example of this below, taken from [5]. Any general construction would need to allow for such exceptions.

Based on general philosophy, the situation over $\mathbb{Q}$, the computational evidence and the known exceptions, we can state the following open question:

Open Question: For each newform F for $\Gamma_0(\mathfrak{n})$ with rational Fourier coefficients, is there *either* an elliptic curve E defined over K with conductor $\mathfrak{n}$ such that $L(F,s) = L(E,s)$, *or* a quadratic twist ϵ such that $F \otimes \epsilon$ is the lift from $\mathbb{Q}$ to K of a modular form f over $\mathbb{Q}$?

3 Computational methods, results and examples

3.1 The modular symbol method

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field, which for the moment we assume to have class number 1. Let R be its ring of integers and $\mathfrak{n}$ a nonzero ideal of R, and define the congruence subgroup $\Gamma_0(\mathfrak{n})$ as above. Let $X_0(\mathfrak{n}) = \Gamma_0(\mathfrak{n})\backslash\mathcal{H}_3$; provided that $\Gamma_0(\mathfrak{n})$ has no nontrivial elements of finite order, this is a 3-manifold.

Instead of computing the space $S_2(\mathfrak{n})$ of cusp forms of weight 2 for $\Gamma_0(\mathfrak{n})$ directly, we compute the 1-homology $H(\mathfrak{n}) = H_1(X_0(\mathfrak{n}), \mathbb{R})$ via modular symbols and then use the fact that $S_2(\mathfrak{n})$ and $H(\mathfrak{n})$ are dual to one another. This is a duality not just of real vector spaces, but of modules for the Hecke algebra, so that we may use the Hecke action on $H(\mathfrak{n})$ to obtain information about eigenforms and eigenvalues on $S_2(\mathfrak{n})$. This is very similar to the situation over $\mathbb{Q}$, except that there the action of complex conjugation plays a role. This means that (over $\mathbb{Q}$) the homology has twice the dimension of the space of cusp forms unless we restrict to the homology classes fixed by conjugation.

To compute the 1-homology of a quotient of $\mathcal{H}_3$, we first tessellate $\mathcal{H}_3$ with hyperbolic polyhedra. See [3] for some pictures for the five Euclidean fields: for example, when $d = 1$ the tessellation is by (hyperbolic) octahedra, all translates of a basic octahedron with vertices at the cusps $0, 1, i, 1+i, (1+i)/2$ and ∞. This octahedron consists of 12 copies of the fundamental region for $\mathrm{PSL}_2(\mathbb{Z}[i])$ glued together. The tessellation for $\mathbb{Q}(\sqrt{-163})$ consists of 5 different polyhedra in 25 Γ-orbits: 11 tetrahedra, 8 triangular prisms, 3 square pyramids, 2 hexagonal caps and 1 cuboctahedron. (See [16] for the details!)

The vertices of the tessellation are the "principal" cusps $\frac{\alpha}{\beta} \in \mathbb{P}^1(K) = K \cup \{\infty\}$ where $\alpha, \beta \in R$ are coprime: $(\alpha, \beta) = R$. The Bianchi group $\Gamma = \mathrm{PSL}_2(R)$ acts on $\mathbb{P}^1(K)$ with exactly h orbits, where h is the class number of K, and the principal cusps are just the orbit of the cusp ∞.

The edges of the tessellation consist of certain geodesic paths between cusps, which again fall into a finite number of Γ-orbits, including the orbit of the path from 0 to ∞, traditionally denoted $\{0, \infty\}$. The edges of the tessellation will generate the homology of each quotient of H_3: by abuse of notation, we use the same symbol $\{\alpha, \beta\}$ to denote a path in $\mathcal{H}_3$, a path in the quotient $X_0(\mathfrak{n})$, or the image of the path in the relative homology $H_1(X_0(\mathfrak{n}), \mathbb{Z}; \mathrm{cusps})$.

Each edge orbit leads to one type of modular symbol in the computation. In the Euclidean case there is only one edge orbit (as is the case over $\mathbb{Q}$), which simplifies the computation of homology considerably.

The faces of the tessellation lead to relations between the generating modular symbols. Again, there is a finite number of face orbits, so we have a finite number of types of relation. (Over $\mathbb{Q}$ there is just one 3-term relation arising this way). We also obtain 2-term relations from the gluing together of the different polyhedra.

Finally, the polyhedra themselves lead to relations between the face relations which gives some redundancy in our presentation of the homology.

So for each field K, we first compute once and for all the geometry of the tessellation, which gives us a list of types of modular symbol and the relations between them. Then to compute $H(\mathfrak{n})$ for a specific level $\mathfrak{n}$, or indeed $H_1(\Gamma_0 \backslash \mathcal{H}_3)$ for any subgroup Γ_0 of Γ of finite index, we have to take one modular symbol generator for each coset representative of Γ_0 in Γ, for each type, and factor out all the face relations. For the case of a congruence subgroup such as $\Gamma_0(\mathfrak{n})$, this computation reduces almost entirely to arithmetic modulo $\mathfrak{n}$ and linear algebra.

3.2 Results for class number one fields

First we give a table showing, for each field $K = \mathbb{Q}(\sqrt{-d})$, the range of levels $\mathfrak{n}$ covered and the number of rational newforms F found. The bounds on the norm $N(\mathfrak{n})$ are taken from [3] and [16]. Here we only count one of each pair of conjugate levels $\mathfrak{n}$, $\overline{\mathfrak{n}}$.

d	1	2	3	7	11	19	43	67	163
Bound on $N(\mathfrak{n})$	500	300	500	300	200	500	230	265	100
Number of forms F	39	36	27	17	17	55	7	6	0

Note that no rational newforms were found over $\mathbb{Q}(\sqrt{-163})$ at the levels considered.

In all cases except one (see below), for each newform F at level $\mathfrak{n}$ we also found an elliptic curve E defined over K with conductor $\mathfrak{n}$, such that the L-series $L(E, s)$ and $L(F, s)$ agree to at least the first 500 Euler factors. This is checked by comparing the Hecke eigenvalue $a_{\mathfrak{p}}(F)$, which is computed via modular symbols, with the trace of Frobenius $a_{\mathfrak{p}}(E) = 1 + N(\mathfrak{p}) - \#E(R/\mathfrak{p})$, computed by counting the points on E modulo $\mathfrak{p}$.

The exceptional newform is at level $\mathfrak{a} = (\alpha)^2$ where $\alpha = \frac{1}{2}(1+\sqrt{-43})$ over $K = \mathbb{Q}(\sqrt{-43})$. It is a quadratic twist of a base-change lift from $\mathbb{Q}$ to K of a newform f of weight 2 for $\Gamma_0(43^2)$ over $\mathbb{Q}$. This newform f has coefficients in $\mathbb{Q}(\sqrt{6})$ and has "extra twist" by $\sqrt{-43}$. It corresponds to an abelian variety A_f of dimension 2 whose endomorphism algebra is the quaternion algebra $\left(\frac{(6,-43)}{\mathbb{Q}}\right)$, which is non-split, so that A_f is absolutely simple. So although the original newform F over K—which does have rational Fourier coefficients—has no corresponding elliptic curve defined over K, it does correspond to a modular abelian variety of higher dimension. For more details of this situation, see [5].

3.3 Numerical evidence for the Birch–Swinnerton-Dyer Conjecture

Here we give two examples, taken from [7], of numerical computations which appear to support the Birch–Swinnerton-Dyer conjecture for elliptic curves defined over K, assuming that the L-series $L(E,s)$ is equal to $L(F,s)$ for the newform F we have found.

In the examples below, for an elliptic curve E defined over K we set $\Omega(E) = \int_{E(\mathbb{C})} \omega_E$, the "volume" of E, which is real: it is the area of the fundamental parallelogram for the period lattice of E. We also define $\Omega^*(E) = 2\Omega(E)/\sqrt{|D_K|}$.

3.3.1 Example 1

Field: $K = \mathbb{Q}(\sqrt{-2})$. Level: $\mathfrak{n} = (13+8\theta) = (1-\theta)^2(3+\theta)$, where $\theta = \sqrt{-2}$. There are two rational newforms at this level.

For the first newform F we compute $\Lambda(F,1)/\Omega(F) = 1/3$ exactly using modular symbols, and $\Lambda(F,1) \approx 0.58775231$ to 8 decimal places (using the series (2.8) from [7] with 50 primes). Hence $\Omega(F) \approx 1.76325694$. We found an isogeny class of three curves of conductor $(13+8\theta)$ corresponding to F (in the sense that the first 50 $a_{\mathfrak{p}}$ for the curves agree with those of F):

	a_1	a_2	a_3	a_4	a_6	$\lvert T\rvert$	$\prod c_{\mathfrak{p}}/\lvert T\rvert^2$	Ω^*
E_1	0	$-1+\theta$	1	$1-\theta$	θ	3	1/9	5.289771
E_2	0	$-1+\theta$	1	$11-11\theta$	$-27+3\theta$	3	1/3	1.763257
E_3	0	$-1+\theta$	1	$-9+39\theta$	$-210-39\theta$	1	1	0.5877523

Here $T = E(K)_{\text{tors}}$. The curves are linked by 3-isogenies:

$$E_1 \stackrel{3}{\longleftrightarrow} E_2 \stackrel{3}{\longleftrightarrow} E_3$$

In each case we have

$$\Omega^*(E)\frac{\prod c_{\mathfrak{p}}}{|T|^2} \approx 0.58775231 \approx \Lambda(F,1)$$

to 8 decimal places, agreeing with th value predicted by the Birch–Swinnerton-Dyer conjecture for $L(E,1)$; moreover for curve E_2 we also have exact equality of the ratios $\prod c_{\mathfrak{p}}/|T|^2 = \Lambda(F,1)/\Omega(F) = 1/3$, and $\Omega^*(E_2) \approx 1.7632569 \approx \Omega(F)$ to 8 decimal places. Thus we might say that curve E_2 is the 'strong' curve in the class.

3.3.2 Example 2

Field: $K = \mathbb{Q}(\sqrt{-1})$. Level: $\mathfrak{n} = (13+8i)$ (a prime), where $i = \sqrt{-1}$. The unique rational newform F at level $\mathfrak{n}$ has $\Lambda(F,1) = 0$, with the sign of the functional equation being -1. Twisting by the quadratic character modulo the prime $\lambda = 3$, we have $\Lambda(F,\chi,1)|\lambda|/\Omega(F) = 2$, and compute $\Lambda(F,\chi,1) \approx 5.87129440$. Hence $\Omega(F) \approx 8.80694160$. The unique curve we found of conductor $(13+8i)$ is as follows:

	a_1	a_2	a_3	a_4	a_6	$\|T\|$	$\prod c_{\mathfrak{p}}/\|T\|^2$	Ω^*
E	0	$1-i$	i	$-i$	0	1	1	8.80694161

Again, we observe that $\Omega^*(E) \approx \Omega(F)$ to 8 decimal places. In this case we expect the curve to have rank 1, and the rank is certainly positive since the point $P = (0,0)$ has infinite order. Finally, we have computed $\Lambda'(F,1) \approx 0.20277292$, which again agrees with the value predicted by the Birch–Swinnerton-Dyer conjecture, using the value $\hat{h}(P) \approx 0.023024215$ for the canonical height of the point P, assuming that $E(K)$ does indeed have rank 1, and that $\#\text{Ш}(E/K) = k^2$ where $k = [E(K) : \langle P\rangle]$. (We have not proved that $k = 1$, though this is presumably true.)

3.4 Taylor's construction of ℓ-adic representations

Here we refer to the papers [9], [14] by R. Taylor et al. for all details and merely sketch the one explicit example from [14] for which we provided the numerical input.

Let $K = \mathbb{Q}(\sqrt{-3})$ and let $\mathfrak{n} = (\frac{1}{2}(17+\sqrt{-3}))$ of norm 73. There is a unique newform F at this level, with associated elliptic curve E with Weierstrass coefficients $[a_1,a_2,a_3,a_4,a_6] = [1, \frac{1}{2}(3+\sqrt{-3}), 0, \frac{1}{2}(1+\sqrt{-3}), 0]$. Here "associated" initially means in the empirical sense used above, that E has conductor $\mathfrak{n}$ and the first few Euler factors of the L-series agree.

In the papers cited, it is proved that there exists a cuspidal automorphic representation π for $\mathrm{GL}(2,\mathbb{A}_K)$ with L-series $L(\pi,s) = \prod_v L(\pi_v,s)$ such that, for all valuations v outside a set of Dirichlet density zero, we have

$$L(\pi_v,s) = \left(1 - a_v N(v)^{-s} + N(v)^{1-2s}\right)^{-1},$$

where $a_v = 1 + N(v) - \#E(\mathbb{F}_v)$. This representation π is constructed via a Galois representation associated to the newform F. To prove (using the method of Livné and Serre) that this representation does indeed come from the (dual of the) Tate module of E, it was necessary to check the equality $a_{\mathfrak{p}}(F) = a_{\mathfrak{p}}(E)$ for 32 carefully chosen primes $\mathfrak{p}$.

If this result can be completed and generalized, it would be significant in the following way. Even with no explicit construction of elliptic curves from these newforms, if there was always an associated Galois representation, then one might be able to prove in each case that the Galois representations attached to the newform and the curve (found independently) were isomorphic, thus establishing the equality of $L(F,s)$ and $L(E,s)$, and showing that the curve E was really modular in a well-defined sense.

3.5 Recent work on fields with higher class number

We finish with a few words about the extension of the modular symbol method of computation to imaginary quadratic fields of class number greater than 1. This work will be described in detail in the thesis [2].

Working with a field K whose ring of integers R is not a principal ideal domain obviously involves many arithmetical complications in practice, which must be overcome. Most of these are merely tiresome, but there are some interesting features: for example, although we obviously do not have a Euclidean algorithm for R, we can replace it by something just as useful in practice using the geometry of hyperbolic 3-space $\mathcal{H}_3$ (just as the usual Euclidean algorithm for $\mathbb{Z}$ can be described in terms of the geometry of the ordinary upper half-plane).

The geometry of the tessellation of $\mathcal{H}_3$ becomes more complicated also, as Γ no longer acts transitively on the cusps so the the fundamental region for Γ has cusps other than ∞. The number of cusps (orbits of Γ on $\mathbb{P}^1(K)$) is equal to the class number h_K. It is possible, and rather useful in practice, to enlarge Γ to

$$\tilde{\Gamma} = N_{\mathrm{PGL}(2,K)}(\Gamma)$$

which contains Γ as a normal subgroup of finite index, with quotient $\tilde{\Gamma}/\Gamma$ isomorphic to the subgroup of ambiguous classes (classes whose square is trivial) in the ideal class group C_K of K. (See [4] for an elementary proof of this.)

If C_K is an elementary abelian 2-group, then $\tilde{\Gamma}$ is transitive on the cusps, and the geometry becomes similar to the class number one case. This is true of the field $\mathbb{Q}(\sqrt{-5})$, with class number 2, for example.

The domain of the modular forms F is in general a disjoint union of h_K copies of $\mathcal{H}_3$, indexed by the ideal classes. To see why this is so, one has to first define modular forms for K as functions on the adele group $\mathrm{GL}(2,\mathbb{A}_K)$, which has h_K components given by the ideal class of the determinant idele. However, we have discovered that it is possible to obtain all the information about the cusp forms F at level $\mathfrak{n}$ by looking exclusively at the homology of the principal component, which is simply the space $X_0(\mathfrak{n})$ defined above. This is essentially because the Hecke operators $T_\mathfrak{p}$ permute the components according to the regular action of the ideal class $[\mathfrak{p}]$ of the prime $\mathfrak{p}$. The details will appear in [2].

Bygott has computed a large number of forms for $\mathbb{Q}(\sqrt{-5})$ in this way, tables of which will also appear in [2]. The space $H(\mathfrak{n})$ defined above is in fact dual to the space of cusp forms for $\Gamma_0(\mathfrak{n})$ which either have trivial character or have unramified quadratic character. We denote by $H^+(\mathfrak{n})$ the subspace of $H(\mathfrak{n})$ which is dual to the space of forms with trivial character, which we expect to correspond to elliptic curves. For some of these we have matching elliptic curves, but we have not yet systematically generated extensive tables of elliptic curves defined over this field to attempt to match all the newforms. We restrict here to giving some details of the very first newform with trivial character in Bygott's table.

3.6 The first example over $\mathbb{Q}(\sqrt{-5})$

Let $K = \mathbb{Q}(\sqrt{-5})$, with ring of integers $R = \mathbb{Z}[\sqrt{-5}]$ and class number 2. The ideal $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$ is the unique prime above 2 (which is ramified) and represents the unique class of non-principal ideals. The space $H(\mathfrak{p}_2^3)$ has dimension 1, so there is a newform F_- at this level, which has non-trivial character. At level $\mathfrak{n} = \mathfrak{p}_2^4$ we find that $H(\mathfrak{p}_2^4)$ has dimension 3, consisting of a two-dimensional "old part" and a one-dimensional new part, which is in fact $H^+(\mathfrak{p}_2^4)$, so there is a newform F at level $\mathfrak{n}$ with trivial character. This form F is the quartic twist of F_- by the quartic idele class character modulo $\mathfrak{p}_2^2$. In fact, there is a related *pair* of newforms at level $\mathfrak{n}$, since it turns out that each Hecke eigenspace in $H(\mathfrak{n})$ corresponds to *two* newforms, which are twists of each other by the unramified quadratic character.

The eigenvalues of the Hecke operators $T_\mathfrak{p}$ for the principal primes $\mathfrak{p} = (\pi)$ are computed in the usual way using $N(\mathfrak{p}) + 1$ upper triangular matrices of determinant π. We find the following eigenvalues for the first few principal primes. Here $\mathfrak{p}_p$ denotes a prime above the rational prime $\mathfrak{p}$: in each case the eigenvalues of $T_\mathfrak{p}$ and $T_{\overline{\mathfrak{p}}}$ are the same for this form F.

$\mathfrak{p}$	$\mathfrak{p}_5$	$\mathfrak{p}_{29}$	$\mathfrak{p}_{41}$	$\mathfrak{p}_{61}$	$\mathfrak{p}_{89}$	$\dots$	$\mathfrak{p}_{11}$	$\dots$
$a_\mathfrak{p}$	2	-2	-2	10	-6	$\dots$	-6	$\dots$

Computing the eigenvalues for non-principal primes requires more thought. In fact, when $\mathfrak{p}$ is not principal the operator $T_\mathfrak{p}$ does not even act on the space $H(\mathfrak{n})$, since this only represents the principal component. However we can compute $T_{\mathfrak{p}^2}$ since $\mathfrak{p}^2$ is principal, and hence determine first $a_{\mathfrak{p}^2}$ and then $(a_\mathfrak{p})^2$. This gives rise to two possible values for $a_\mathfrak{p}$ which differ by sign. But we can also compute $T_{\mathfrak{p}_1\mathfrak{p}_2} = T_{\mathfrak{p}_1}T_{\mathfrak{p}_2}$ for each pair of non-principal primes $\mathfrak{p}_1$, $\mathfrak{p}_2$ since their product is principal, so we know the sign of $a_{\mathfrak{p}_1}a_{\mathfrak{p}_2}$. Thus once we have fixed the sign of $a_\mathfrak{p}$ for one non-principal prime $\mathfrak{p}$, the others are all determined uniquely.

This leads to two consistent sets of eigenvalues for each one-dimensional Hecke eigenspace in $H(\mathfrak{n})$. In fact, both sets are valid, and there are two newforms corresponding to this one-dimensional eigenspace, which are twists of each other by the unramified quadratic character χ whose value is $+1$ at principal primes and -1 at non-principal primes. In the case $\mathfrak{n} = \mathfrak{p}_2^4$ we find the following values for one set of eigenvalues at the non-principal primes:

$\mathfrak{p}$	$\mathfrak{p}_3$	$\overline{\mathfrak{p}_3}$	$\mathfrak{p}_7$	$\overline{\mathfrak{p}_7}$	$\mathfrak{p}_{23}$	$\overline{\mathfrak{p}_{23}}$	$\mathfrak{p}_{43}$	$\overline{\mathfrak{p}_{43}}$	$\dots$
$a_{\mathfrak{p}^2}$	1	1	-3	-3	-19	-19	-7	-7	$\dots$
$a_\mathfrak{p}$	2	-2	2	-2	2	-2	-6	6	$\dots$

Remarks

1. There are examples (at level $\mathfrak{p}_2^6$, for example) where all the eigenvalues at the non-principal primes are 0, so that there is only one newform associated to the one-dimensional eigenspace in $H(\mathfrak{n})$. This newform is therefore of CM-type, being its own quadratic twist by the unramified character.

2. The newforms described here at level $\mathfrak{p}_2^4$ are not stable under Galois, so are not base-change lifts from $\mathbb{Q}$ to K. However, it appears that a suitable quadratic twist is a base-change lift, so is attached to an elliptic curve defined over $\mathbb{Q}$. We have not yet identified an elliptic curve defined over K associated

with these newforms, but hope to do so.

References

[1] L. Bianchi, *Sui gruppi di sostituzioni lineari con coefficienti appartenenti a corpi quadratici immaginari*, Math. Ann. **40** (1892), 332–412.

[2] J. S. Bygott, *Modular forms and elliptic curves over imaginary quadratic number fields of*, Ph.D. thesis, University of Exeter, 1998.

[3] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Mathematica **51** (1984), 275–323.

[4] ______, *On* $\mathrm{GL}(n)$ *of a Dedekind domain*, Quart. J. Math. Oxford (2) **39** (1988), 423–426.

[5] ______, *Abelian varieties with extra twist, cusp forms and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2) **45** (1992), 404–416.

[6] ______, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, 1997.

[7] J. E. Cremona and E. Whitley, *Periods of cusp forms and elliptic curves over imaginary quadratic fields*, Mathematics of Computation **62** (1994), no. 205, 407–429.

[8] S. Gelbart, *Automorphic forms on adele groups*, Annals of Mathematics Studies, no. 83, Princeton University Press, 1975.

[9] Michael Harris, David Soudry, and Richard Taylor, *ℓ-adic representations associated to modular forms over imaginary quadratic fields. I*, Invent. Math. **112** (1993), 377–411.

[10] J.Elstrodt, F.Grunewald, and J.Mennicke, *On the group* $\mathrm{PSL}_2(\mathbb{Z}[i])$, In J.V.Armitage [11].

[11] J.V.Armitage (ed.), *Journées arithmétiques 1980*, London Mathematical Society Lecture Notes Series, vol. 56, Cambridge University Press, 1980.

[12] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, no. 40, Princeton University Press, 1992.

[13] P. F. Kurčanov, *Cohomology of discrete groups and Dirichlet series connected with Jacquet–Langlands cusp forms*, Math. USSR Izv. **12** (1978), no. 3, 543–555.

[14] Richard Taylor, *ℓ-adic representations associated to modular forms over imaginary quadratic fields. II*, Invent. Math. **116** (1994), 619–643.

[15] A. Weil, *Dirichlet series and automorphic forms*, Lecture Notes in Mathematics, no. 189, Springer-Verlag, 1971.

[16] E. Whitley, *Modular forms and elliptic curves over imaginary quadratic number fields of class number one*, Ph.D. thesis, University of Exeter, 1990.