COMPOSITIO MATHEMATICA

J. E. CREMONA

Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields

Compositio Mathematica, tome 51, n^o 3 (1984), p. 275-324.

<http://www.numdam.org/item?id=CM_1984__51_3_275_0>

Compositio Mathematica 51 (1984) 275–323

HYPERBOLIC TESSELLATIONS, MODULAR SYMBOLS, AND ELLIPTIC CURVES OVER COMPLEX QUADRATIC FIELDS

J.E. Cremona *

1. Introduction

In [22], Weil presented the conjecture that every elliptic curve defined over Q is a quotient of one of the modular curves $X_0(N)$ as an open question, and recommended its solution to the interested reader. This conjecture has since been generalized and forms part of the "Langlands Philosophy", that "every zeta function associated with any algebraic variety is some sort of transform of a modular form on a semisimple or reductive algebraic group" [20]. In particular, if E is an elliptic curve defined over a global field K, with zeta function $L(E, s)$, it follows from the results in [13,23] that $L(E, s)$ is the transform of a certain automorphic form for K provided that $L(E, s)$, and sufficiently many of its character twists, satisfy appropriate analytic conditions: that they have analytic continuations, satisfy functional equations, and are bounded in vertical strips. These conditions have been proved in certain cases (for example, when K is a function field, or when E has complex multiplication) and are conjectured to hold generally. For further examples and comments, see [24] and [23], Chapter X.

In this paper we consider the case where K is a complex quadratic field. If E is an elliptic curve over K whose L-series $L(E, s)$ satisfies the analytic conditions referred to above (see [23] for details) then $L(E, s)$ is the Mellin transform of an automorphic form F of weight 2 for the congruence subgroup $\Gamma_0(\mathfrak{a})$ of $SL(2, \mathfrak{o}_K)$, where $\mathfrak{a}$ is the conductor of E: see below for the notation. This form F is even a cusp form, except in the case when E has complex multiplication by an order in K itself, when F is an Eisenstein series (see [24], penultimate paragraph, or [5], Theorem 2(b)). In the former case F is (essentially) a harmonic differential 1-form on the quotient of hyperbolic 3-space H_3 by $\Gamma_0(\mathfrak{a})$. By duality the space of such differentials is isomorphic to $H_1(\Gamma_0(\mathfrak{a})\backslash H_3^*, C)$, where $H_3^* = H_3 \cup \{\text{cusps}\}$. This latter space can be calculated by means of modular symbols, as was described by Grunewald, Mennicke and others in

* This work was supported by a grant from the Science Research Council.

[8,9,10] in the cases $K=\boldsymbol{Q}(\sqrt{-1})$, $\boldsymbol{Q}(\sqrt{-2})$, $\boldsymbol{Q}(\sqrt{-3})$ and $\mathfrak{a}$ a prime ideal of degree 1.

Here we show how to extend the calculations with modular symbols to arbitrary ideals $\mathfrak{a}$ in all five Euclidean complex quadratic fields: the ones above and $\boldsymbol{Q}(\sqrt{-7})$, $\boldsymbol{Q}(\sqrt{-11})$. By duality we are thus calculating the space of cuspidal automorphic forms for $\Gamma_0(\mathfrak{a})$. Secondly we produce tables of elliptic curves defined over each such K with small conductor (found by computer search), and observe the correspondence, as predicted by the Weil conjectures. The correspondence is described in more detail below.

This approach follows closely the work of Tingley [21] who carried out the same procedure over $\boldsymbol{Q}$; however, Tingley was able to go much further and construct elliptic curves directly from newforms $f(z)$ by calculating the two periods of $2\pi i f(z)\mathrm{d}z$. In the present case the differential attached to a cusp form F on H_3 has only a single period. This period has been calculated numerically in several cases by the author, and is related to $L(E,1)$ for the corresponding curve E in the way predicted by the Birch Swinnerton Dyer conjectures, but as a single (real) number is insufficient for determining the curve E.

For a down-to-earth description of cusp forms of weight 2 for $\Gamma_0(\mathfrak{a})$ over a complex quadratic field K, see [4], Chapter 3.

Let d be a square-free positive integer, and K the complex quadratic field $\boldsymbol{Q}(\sqrt{-d})$; denote the ring of integers in K by $\mathfrak{o}_d$ and set $\Gamma_d = SL(2,\mathfrak{o}_d)$. For an ideal $\mathfrak{a}$ of $\mathfrak{o}_d$ define

$$\Gamma_0(\mathfrak{a}) := \left\{\begin{pmatrix} a & b \\ c & e\end{pmatrix} \in \Gamma_d : c \in \mathfrak{a}\right\}.$$

Let H_3 be hyperbolic three-space:

$$H_3 := \{(z,t) : z\in \boldsymbol{C},\quad t\in\boldsymbol{R},\quad t>0\}.$$

H_3 is equipped with a hyperbolic structure given by

$$ds^2 = \frac{dx^2+dy^2+dt^2}{t^2} \qquad (z=x+iy).$$

Its group of isometries is $PGL(2,\boldsymbol{C})$ which acts according to the formulae

$$\begin{pmatrix} a & b \\ c & e\end{pmatrix} : (z,t) \mapsto (z^*, t^*) \quad \text{where}$$

$$z^* = \frac{(az+b)(\overline{cz+e}) + (at)(\overline{ct})}{|cz+e|^2+|c|^2t^2}$$

and

$$t^* = \frac{|ae - bc|t}{|cz + e|^2 + |c|^2 t^2}.$$

[We write elements of $PGL(2, \mathbb{C})$ as 2×2 matrices throughout]. The action of Γ_d and of subgroups of finite index in Γ_d is discrete: that is, every compact subset of H_3 meets only a finite number of its images under the action (see [2]).

Let H_3^* denote the extended space $H_3 \cup K \cup \{\infty\}$ obtained by including the cusps, and set

$$V(\mathfrak{a}) := H_1(\Gamma_0(\mathfrak{a}) \backslash H_3^*, \mathbb{Q}).$$

If ε is a generator of the unit group $\mathfrak{o}^*$ of $\mathfrak{o}_d$, then

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

normalizes $\Gamma_0(\mathfrak{a})$ for every ideal $\mathfrak{a}$, and hence induces an automorphism J of $V(\mathfrak{a})$, which is an involution. Hence we can decompose $V(\mathfrak{a})$ as

$$V(\mathfrak{a}) = V^+(\mathfrak{a}) \oplus V^-(\mathfrak{a})$$

where $V^+(\mathfrak{a})$ and $V^-(\mathfrak{a})$ are the $+1$ and -1 eigenspaces for J, respectively.

Acting on $V(\mathfrak{a})$ one also has the algebra of Hecke operators T_π, for prime elements π of $\mathfrak{o}$ not dividing $\mathfrak{a}$, and involutions W_π for each prime π dividing $\mathfrak{a}$. These are defined as follows. If π is a prime then T_π acts firstly on the free abelian group on the cusps $\Gamma_0(\mathfrak{a}) \backslash K \cup \{\infty\}$ via

$$T_\pi : [\alpha] \mapsto \sum_{x \bmod \pi} \left[\frac{\alpha + x}{\pi}\right] + [\pi\alpha];$$

here $[\alpha]$ denotes the equivalence class of $\alpha \in K \cup \{\infty\}$ under the action of $\Gamma_0(\mathfrak{a})$. This action extends to $H_1(\Gamma_0(\mathfrak{a}) \backslash H_3^*, \mathbb{Q})$, since clearly the homology is generated by paths between cusps.

Secondly, if π divides $\mathfrak{a}$ to the exact power r, and α is a generator for the ideal $\mathfrak{a}$, let W_π be a matrix of the form

$$W_\pi = \begin{pmatrix} \pi^r x & y \\ \alpha z & \pi^r w \end{pmatrix}$$

which has determinant π^r. Then W_π normalizes $\Gamma_0(\mathfrak{a})$ and so induces an action on $\Gamma_0(\mathfrak{a}) \backslash H_3^*$, which is independent of the matrix chosen. This is an involution since W_π^2 is (modulo a scalar matrix) in $\Gamma_0(\mathfrak{a})$.

We use the notation T_π rather than $T_\mathfrak{p}$ for a prime ideal $\mathfrak{p}$, since $T_{\varepsilon\pi} = JT_\pi$, and so T_π and $T_{\varepsilon\pi}$ only coincide on V^+.

These operators all commute, and therefore there exists a basis for $V(\mathfrak{a})$ consisting of eigenvectors for J and all the T_π and W_π. Of special interest will be one-dimensional eigenspaces with rational eigenvalues for all the T_π.

Conjecture [1]: There is a one-one correspondence between

(i) One-dimensional rational eigenspaces of $V^+(\mathfrak{a})$, and

(ii) Isogeny classes of elliptic curves E defined over K with conductor $\mathfrak{a}$, which do not have complex multiplication by an order in K.

Now $V^+(\mathfrak{a})$ is isomorphic (as a module for the Hecke algebra) to the space of cuspidal automorphic forms for $\Gamma_0(\mathfrak{a})$ mentioned above. We shall abuse language and borrow some of the terminology from the theory of automorphic forms to describe certain subspaces of $V(\mathfrak{a})$.

If $\mathfrak{b}$ divides $\mathfrak{a}$, then for an element k in $\mathfrak{O}$ dividing $\mathfrak{a}\mathfrak{b}^{-1}$ we have

$$\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} \Gamma_0(\mathfrak{a}) \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}^{-1} \subset \Gamma_0(\mathfrak{b})$$

and thus $(z, t) \mapsto (kz, t)$ induces a map from $V(\mathfrak{b})$ to $V(\mathfrak{a})$. "Newforms" in $V(\mathfrak{a})$ are one-dimensional eigenspaces for J and for all the T_π and W_π. A newform for $\Gamma_0(\mathfrak{b})$ will appear several times in $V(\mathfrak{a})$, as a set, or "oldclass", of "oldforms", one for each ideal divisor (k) of $\mathfrak{a}\mathfrak{b}^{-1}$. Each oldform in the same oldclass has the same Hecke eigenvalues for each T_π (with π not dividing $\mathfrak{a}$) as the original newform in $V(\mathfrak{b})$.

In practice, oldforms can be recognized not only because of their multiplicity, but also because in any systematic calculation we will have already met them as newforms for $\Gamma_0(\mathfrak{b})$, for some $\mathfrak{b}$ dividing $\mathfrak{a}$.

The theory of oldforms and newforms in the general context of automorphic forms for an arbitrary global field can be found in [16], which generalizes the classical results of [1].

The conjecture only mentions $V^+(\mathfrak{a})$. As for the V^- spaces, we show that they are connected with the V^+ spaces via twisting operators which are simple generalizations of the R_χ operators of [1]. More precisely:

THEOREM: *Let χ be a quadratic character of K modulo the ideal $\mathfrak{q}$. Then there is an operator R_χ which acts on $V(\mathfrak{a})$ provided that $\mathfrak{q}^2$ divides $\mathfrak{a}$, and satisfies*

(i) $R_\chi J = \chi(\varepsilon) J R_\chi$;

(ii) $R_\chi T_\pi = \chi(\pi) T_\pi R_\chi$ *if* $(\pi) \nmid \mathfrak{a}$; *and*

(iii) $R_\chi W_\pi = \chi(\pi^e) W_\pi R_\chi$ *if* $(\pi)^e \| \mathfrak{a}$.

In particular, if we choose χ so that $\chi(\varepsilon) = -1$, then (i) shows that R_χ

[1] See end of paper.

maps $V^+(\mathfrak{a})$ into $V^-(\mathfrak{a})$ and vice versa; also, from (ii) and (iii), R_χ preserves the eigenvalues of T_π and W_π provided that we choose generators π of each prime ideal $\mathfrak{p}$ with $\chi(\pi) = +1$: this can be done, again because $\chi(\varepsilon) = -1$.

In Section 2 below we give algorithms for computing $V(\mathfrak{a})$ in the five Euclidean cases: $d = 1, 2, 3, 7$ and 11. These algorithms are similar to one given by Manin [15] for the rational case of the subgroup $\Gamma_0(N)$ of the modular group $SL(2, \mathbb{Z})$ acting on the upper half-plane. When $d = 1, 2,$ or 3 the Hecke eigenvalues on $V(\mathfrak{p})$, for $\mathfrak{p}$ a prime of degree 1, have been calculated for $N_\mathfrak{p} < 1500$ in [8]: of course at a prime level the twists R_χ do not operate, and there are no oldforms.

The author has computed the full space $V(\mathfrak{a})$ for all ideals $\mathfrak{a}$ with norm less than a bound B_K (depending on K) for each of the five euclidean fields. The values of B_K are as follows.

K	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-7})$	$\mathbb{Q}(\sqrt{-11})$
B_k	500	300	500	200	200

As observed in [8], the behaviour of dim $V(\mathfrak{a})$ is very erratic: in particular the figures suggest that dim $V(\mathfrak{a}) = 0$ infinitely often for each field. By contrast, the result of [11] shows that for almost all d,

$$\dim H_1(G \backslash H_3, \mathbb{C}) \neq 0$$

for all subgroups G of finite index in Γ_d.

For each space $V(\mathfrak{a})$ with positive dimension we have computed the action of the Hecke operators T_π on $V(\mathfrak{a})$ for each prime π not dividing $\mathfrak{a}$ and $N(\pi) < 50$, and the action of the involution W_π for each prime π dividing $\mathfrak{a}$. We have thus found a basis for $V(\mathfrak{a})$ consisting of eigenvectors for every T_π and W_π.

In Section 3 we provide tables of the results of these computations, giving the dimension of each $V(\mathfrak{a})$, $V^+(\mathfrak{a})$ and $V^-(\mathfrak{a})$, the field over which the Hecke action splits, and a list of the Hecke eigenvalues for $N(\pi) < 50$ and all one-dimensional rational eigenspaces in V^+. We also describe the outcome of a systematic computer search for curves of small conductor defined over K, for each Euclidean K. The conductors were found using Tate's algorithm [19] and the Traces of Frobenius by counting points over residue fields. We remark on the numerical coincidences between the tables of one-dimensional eigenspaces in $V^+(\mathfrak{a})$ and the tables of elliptic curves with conductor $\mathfrak{a}$.

In Section 4 we prove the theorem stated above relating V^+ and V^- by means of twisting operators. This holds for arbitrary complex quadratic fields, not just the Euclidean ones. We conclude with some remarks about extending the computations themselves to the non-Euclidean fields.

2. The algorithms

2.1. Review of the rational case

Let

$$S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \quad\text{and}\quad T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

be the usual generators for $\Gamma = SL(2, \mathbb{Z})$, and $H_2^* = H_2 \cup \mathbb{Q} \cup \{\infty\}$ the extended upper half-plane. Let G be a subgroup of Γ of finite index. The network of geodesic lines joining $\gamma(0)$ to $\gamma(\infty)$ for γ in Γ forms a tesselation of H_2^* by triangles. If we denote by $\{\alpha, \beta\}_G$ the image of the geodesic path between two cusps α and β in the quotient space $X_G = G\backslash H_2^*$ then clearly the set of all paths of the form $\{\gamma(0), \gamma(\infty)\}_G$ forms a triangulation of X_G: now it is only necessary for γ to run over a complete set of right coset representatives for G in Γ.

To calculate the homology of this quotient space, first note that the triangles of the triangulation are just the transforms of the *basic triangle* with vertices at 0, ∞ and 1, whose edges consist of $\{\gamma(0), \gamma(\infty)\}$ for $\gamma = I$, $\gamma = TS$, and $\gamma = (TS)^2$. If we denote $\{\gamma(0), \gamma(\infty)\}_G$ by the symbol (γ) for short, then we see that $H_1(X_G, \mathbb{Q})$ is generated by

$$\{(\gamma) : \gamma \in [\Gamma : G]\}$$

and that for any γ the relation

$$(\gamma) + (\gamma TS) + \left(\gamma (TS)^2\right) = 0$$

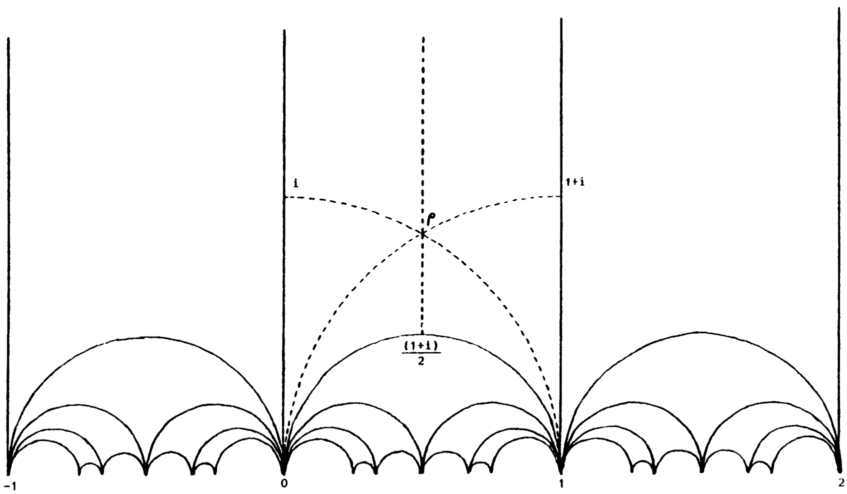


Figure 2.1

holds. We also have a second type of relation from the gluing together of the translates of the basic triangle. Since S identifies the edge $\{0, \infty\}$ with itself in the opposite orientation, we have for each γ the relation

$$(\gamma)+(\gamma S)=0.$$

So let $C(G)$ be the $\mathbb{Q}$-vector space with basis the symbols (γ) for each γ in $[\Gamma : G]$; the natural right coset action of Γ on $[\Gamma : G]$ extends by linearity to an action of the group ring $\mathbb{Z}\Gamma$ on $C(G)$. Define the *relation ideal* $\mathscr{R}$ to be the left ideal of $\mathbb{Z}\Gamma$ generated by $I+S$ and $I+TS+(TS)^2$, and let $B(G) := C(G)\mathscr{R}$. If $H_0(G)$ denotes the free abelian group on the cusps of G (that is, on the orbits of $\mathbb{Q} \cup \{\infty\}$ under the action of G) then we have the *boundary map* ∂: $C(G) \to H_0(G)$ defined by

$$\partial : (\gamma) \mapsto [\gamma(\infty)] - [\gamma(0)]$$

where $[\alpha]$ denotes the cusp equivalence class containing α. Let $Z(G) :=$ ker ∂. It is easy to see that $B(G) \subset Z(G)$, and Manin's result is [15]:

THEOREM 1: *Define $H(G) := Z(G)/B(G)$. Then $H(G)$ is isomorphic to $H_1(X_G, \mathbb{Q})$, the isomorphism being given by*

$$(\gamma) \mapsto \{\gamma(0), \gamma(\infty)\}_G. \tag{2.1.1}$$

Below we will show how this resul can be extended to subgroups of finite index in $\Gamma_d = SL(2, \mathfrak{o}_d)$: the main difficulty is determining the correct "relation ideal" $\mathscr{R}$ from the geometry. Before we do this, we will discuss the question of how to convert the theorem into an algorithm.

First we need a convenient way of writing down the coset representatives for G in Γ. In the case $G = \Gamma_0(N)$, these are in one-one correspondence with the elements $(c:d)$ of $P^1(N)$, where $P^1(N) = P^1(\mathbb{Z}/N\mathbb{Z})$ is the projective line over the ring of integers modulo N. We recall the definition: see [15] or [4]. Form the set of ordered pairs $(c, d) \in \mathbb{Z}^2$ such that $g.c.d.\ (c, d, N) = 1$, and factor out by the equivalence relation $\sim$, where

$$(c_1, d_1) \sim (c_2, d_2) \Leftrightarrow \exists u\colon g.c.d.(u, N) = 1,$$

$$c_1 u \equiv c_2, \qquad d_1 u \equiv d_2 \pmod N.$$

The equivalence class of (c, d) will be denoted $(c:d)$, and such symbols will be called *M-symbols.* Notice that c and d are only determined modulo N, and that we can always assume that $g.c.d.(c, d) = 1$. The correspondence is given by

$$(c:d) \leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{2.1.2}$$

where a and b are any integers chosen so that $ad - bc = 1$.

It is thus a simple matter to list the elemens of $P^1(N)$ and compute the action of Γ:

$$(c:d)\begin{pmatrix} p & q \\ r & s \end{pmatrix} = (cp + dr : cq + ds). \tag{2.1.3}$$

The boundary map ∂ has the form

$$\partial : (c:d) \mapsto \left[\frac{b}{d}\right] - \left[\frac{a}{c}\right]$$

and we can decide when two cusps are equivalent by means of the following easy Lemma.

LEMMA 2.1.5: *Let p_1/q_1 and p_2/q_2 be rational numbers in their lowest terms. Then the following are equivalent.*

(i) $\exists \gamma \in \Gamma_0(N) : \gamma(p_1/q_1) = p_2/q_2$;

(ii) $s_1 q_2 \equiv s_2 q_1 (\mathrm{mod}\ g.c.d.(q_1 q_2, N))$ *where* $p_j s_j \equiv 1 (\mathrm{mod}\ q_j)$ *for* $j = 1, 2$.

Lastly we recall the definition of the Hecke operators T_p. These act, first, on the free abelian group on the points of H_2^*, and hence on modular symbols $\{\alpha, \beta\}_G$ via

$$T_p : \{\alpha, \beta\} \mapsto \sum_{k \bmod p} \left\{\frac{\alpha + k}{p}, \frac{\beta + k}{p}\right\} + \{p\alpha, p\beta\}. \tag{2.1.6}$$

Thus we cannot compute the action of T_p on $H(G)$ directly but instead we convert to modular symbols via the isomorphism (2.1.1) which now has the form

$$(c:d) \mapsto \left\{\frac{b}{d}, \frac{a}{c}\right\}_G, \tag{2.1.7}$$

then compute the action of T_p on the modular symbol $\{b/d, a/c\}_G$, and lastly convert back to M-symbols. This last step is achieved by expressing an arbitrary modular symbol $\{\alpha, \beta\}_G$ as a sum of symbols of the special form $\{\gamma(0), \gamma(\infty)\}_G$ for γ in Γ, by means of continued fractions (see [15]).

A similar process must be used to calculate the W_q-involutions, for whose definition we refer to the Introduction.

Hence, given any integer N we can (given enough time) calculate the dimension of the space $H_1(\Gamma_0(N)\backslash H_2^*, \mathbb{Q})$, split it into simultaneous eigenspaces for all the W_q (for q dividing N) and T_p (for p dividing N), and calculate the eigenvalue of any of these operators. This was done by Tingley [21] for $N \leqslant 300$, and the first eight primes.

2.2. Euclidean complex quadratic fields

Let K be one of the Euclidean fields $\mathbb{Q}(\sqrt{-d})$ for $d = 1, 2, 3, 7$ or 11, let $\mathfrak{o}$ be the ring of integers of K, $\mathfrak{o}^*$ the group of units, ε a fundamental unit, and $\Gamma = SL(2, \mathfrak{o})$.

Γ acts discretely on the hyperbolic upper half-space $H_3 = \mathbb{C} \times \mathbb{R}^+$ which we extend by including the K-rational cusps $K \cup \{\infty\}$ on the boundary of H_3 to form $H_3^* := H_3 \cup K \cup \{\infty\}$. As in the two-dimensional case the set of geodesic paths of the form $\{\gamma(0), \gamma(\infty)\} = \{b/d, a/c)$ with

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in Γ, forms a network which is the 1-skeleton of a tesselation of H_3^* by hyperbolic polyhedra. This will be described in detail for the five fields, in the next subsection. There is a *basic polyhedron* B whose edges are the transforms of $\{0, \infty\}$ by a certain finite subgroup G_P, and whose transforms fill the space, just as in the 2-dimensional case we had a "basic triangle" with vertices at 0, ∞ and 1.

So, as in the rational case, we can generate the homology of $G \backslash H_3^*$, where G is a subgroup of finite index in Γ, by means of paths $(\gamma) = \{\gamma(0), \gamma(\infty)\}$ for γ in Γ. Clearly

$$(g\gamma) = (\gamma)$$

for every g in G. Other relations among these generators arise in two ways: from considering which transforms of B meet at the edge $\{0, \infty\}$; and from the edges around each face of the polyhedron B. The latter can be determined by calculating the orbits of G_P on the edges of B.

It turns out to be more natural to consider the action of the larger group $\tilde{\Gamma}$, where

$$\tilde{\Gamma} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathfrak{o}, \quad ad - bc \in \mathfrak{o}^* \right\}.$$

This group contains Γ with index $|\mathfrak{o}^*|$; the corresponding projective groups $P\Gamma$ and $P\tilde{\Gamma}$, obtained by factoring out the scalar matrices (which act trivially on H_3), always satisfy $|P\tilde{\Gamma} \colon P\Gamma| = 2$ since $|\mathfrak{o}^* : (\mathfrak{o}^*)^2| = 2$ in every case. Note that

$$J = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}$$

normalizes $\Gamma_0(\mathfrak{a})$ for every ideal $\mathfrak{a}$ of $\mathfrak{o}$, and that its image in $P\tilde{\Gamma}$ lies in the second coset $P\tilde{\Gamma} \backslash P\Gamma$. The definition of the symbol $(\gamma) =$

$\{\gamma(0), \gamma(\infty)\}_G$ extends to γ in $\tilde{\Gamma}$, and clearly $(\gamma)=(\gamma J)$ since J fixes 0 and ∞. (These extra symbols will make computations and formulae tidier.)

So, given a group G of finite index in Γ, let $C(G)$ denote the $\mathbb{Q}$-vector space spanned by symbols (γ) where γ runs through a complete set of right coset representatives for G in Γ. By means of the rules

$$\text{(i) } (\gamma)=(g\gamma) \qquad \text{for} \quad g \in G;$$

$$\text{(ii) } (\gamma)=(\gamma J) \tag{2.2.1}$$

we can identify any symbol (γ) for γ in $\tilde{\Gamma}$ with a unique basis element of $C(G)$, and thus define an action of $\mathbb{Z}\tilde{\Gamma}$ on $C(G)$ via

$$\tilde{\gamma}: (\gamma) \mapsto (\gamma\tilde{\gamma}) \tag{2.2.2}$$

for $\tilde{\gamma}$ in $\tilde{\Gamma}$, extended to $\mathbb{Z}\tilde{\Gamma}$ by linearity.

From the geometry we will determine a "relation ideal" $\mathscr{R}$ of $\mathbb{Z}\tilde{\Gamma}$, and then set $B(G):=C(G)\mathscr{R}$ and $Z(G):=\ker\partial$ where ∂ is given by

$$\partial:(\gamma) \mapsto [\gamma(\infty)]-[\gamma(0)], \tag{2.2.3}$$

the boundary map from $C(G)$ to $H_0(G)$, the free abelian group on the cusps of G. It will be clear from the definition of $\mathscr{R}$ that $B(G) \subset Z(G)$, and we will then have the following result.

THEOREM 2: *The map* $\xi:(\gamma) \mapsto \{\gamma(0), \gamma(\infty)\}_G$ *induces an isomorphism from* $H(G)$ *to* $H_1(G\backslash H_3^*, \mathbb{Q})$, *where* $H(G):=Z(G)/B(G)$.

We postpone the precise determination of the ideal $\mathscr{R}$ until the next subsection.

Note that the J involution acts on the symbols via

$$J:(\gamma) \mapsto (J^{-1}\gamma J) \tag{2.2.4}$$

which from 2.2.1 (i) is well-defined provided that J normalizes G.

From the theorem we obtain an algorithm for computing $H_1(\Gamma_0(\mathfrak{a})\backslash H_3^*, \mathbb{Q})$ explicitly for any ideal $\mathfrak{a}$ as follows. It is a simple matter to define the set $P^1(\mathfrak{a})$ of M-symbols $(c:d)$ which are in one-one correspondence with the coset representatives for $\Gamma_0(\mathfrak{a})$ in Γ via (2.1.2), with Γ-action given by (2.1.3). To extend this to an action of $\tilde{\Gamma}$ we proceed as follows: a set of coset representatives for $\Gamma_0(\mathfrak{a})$ in $\tilde{\Gamma}$ is $\{\gamma\} \cup \{J\gamma\}$, where $\{\gamma\}$ is a set of representatives for $\Gamma_0(\mathfrak{a})$ in Γ: thus we need to extend the M-symbols to a set twice the size. If we (temporarily) write $(c:d)^+$ for a coset representative

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with determinant 1, and $(c:d)^-$ for the representative

$$J\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \varepsilon a & \varepsilon b \\ c & d \end{pmatrix}$$

of determinant ε, then the action of a matrix

$$g = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

is still given by (2.1.3), except that if $\det g$ is not a square than g also changes the sign in the superscript.

In practice, however, these extra symbols are superfluous:

LEMMA 2.2.5: *Under the map ξ the M-symbols $(c:d)^-$ and $(\xi c:d)^+$ have the same image.*

PROOF: Choose a and b so that $ad - bc = 1$. Then on the one hand $(c:d)^-$ corresponds to

$$\begin{pmatrix} a\varepsilon & b\varepsilon \\ c & d \end{pmatrix}$$

whose image under ξ is $\{b\varepsilon/d, a\varepsilon/c\}$. On the other hand, since $ad - (\varepsilon^{-1}b)(\varepsilon c) = 1$ the symbol $(\varepsilon c:d)^+$ corresponds to

$$\begin{pmatrix} a & \varepsilon^{-1}b \\ \varepsilon c & d \end{pmatrix}$$

whose image under ξ is

$$\left\{\frac{b}{\varepsilon d}, \quad \frac{a}{\varepsilon c}\right\}.$$

The images are equal since

$$\begin{pmatrix} \varepsilon^{-1} & 0 \\ 0 & \varepsilon \end{pmatrix}$$

is in $\Gamma_0(\mathfrak{a})$ and sends $b\varepsilon/d$ to $b/\varepsilon d$ and $a\varepsilon/c$ to $a/\varepsilon c$. $\square$

We can therefore identify $(c:d)^-$ with $(\varepsilon c:d)^+$ with no loss. Thus henceforth we will drop the superscripts, the formulae for the action of

$\tilde{\Gamma}\setminus\Gamma$ being given by the following.

LEMMA 2.2.6:

(i) $(c:d)J=(\varepsilon^2c:d)$;

(ii) *If* $ps-qr=\varepsilon$ *then* $(c:d)\begin{pmatrix} p & q \\ r & s\end{pmatrix}=(\varepsilon(cp+dr):cq+ds)$.

PROOF:

(i) $(c:d)^+J=(\varepsilon c:d)^-=(\varepsilon^2c:d)^+$.

(ii) Write γ for $\begin{pmatrix} p & q \\ r & s\end{pmatrix}$. Then

$$(c:d)^+\gamma=(c:d)^+J(J^{-1}\gamma)=(\varepsilon c:d)^-(J^{-1}\gamma)$$

$$=(\varepsilon c:d)^-\begin{pmatrix} \varepsilon^{-1}p & \varepsilon^{-1}q \\ r & s\end{pmatrix}$$

$$=(cp+dr:cq+ds)^-=(\varepsilon(cp+dr):cq+ds)^+. \quad \square$$

The action of the J-involution on M-symbols is given by

$$(c:d)\mapsto(\varepsilon c:d) \tag{2.2.7}$$

since

$$J^{-1}\begin{pmatrix} a & b \\ c & d\end{pmatrix}J=\begin{pmatrix} a & \varepsilon^{-1}b \\ \varepsilon c & d\end{pmatrix}.$$

To decide on the equivalence of cusps under the action of $\Gamma_0(\mathfrak{a})$, we have to modify Lemma 2.1.5 slightly as follows.

LEMMA 2.2.7: *Let* p_1/q_1 *and* p_2/q_2 *be elements of* K *written in their lowest terms, so that* $(p_1,q_1)=(p_2,q_2)=\mathfrak{v}$. *Then the following are equivalent*:

(i) $\exists\gamma\in\Gamma_0(\mathfrak{a}):\gamma(p_1/q_1)=p_2/q_2$;

(ii) $\exists u\in\mathfrak{v}^*: s_1q_2\equiv u^2s_2q_1$ (modulo $(q_1q_2)+\mathfrak{a}$), *where* $p_ks_k\equiv 1$ (mod (q_k)) *for* $k=1,2$.

PROOF: For $k=1,2$ choose r_k and s_k such that $p_ks_k-r_kq_k=1$. Then

$$\gamma_1=\begin{pmatrix} q_1 & -p_1 \\ s_1 & -r_1\end{pmatrix}$$

is in Γ, and

$$\gamma_1(p_1/q_1)=0,$$

while

$$\gamma_2=\begin{pmatrix} -r_2 & p_2 \\ -s_2 & q_2\end{pmatrix}$$

is in Γ and $\gamma_2(0)=p_2/q_2$. Any element of Γ fixing 0 has the form

$$\begin{pmatrix} u & 0 \\ x & u^{-1} \end{pmatrix}$$

for $u \in \mathfrak{o}^*$, $x \in \mathfrak{o}$; so the general element in Γ taking p_1/q_1 to p_2/q_2 is

$$\gamma_2\begin{pmatrix} u & 0 \\ x & u^{-1} \end{pmatrix}\gamma_1 = \begin{pmatrix} * & * \\ xq_1q_2 + u^{-1}\left(s_1q_2 - u^2q_1s_2\right) & * \end{pmatrix}.$$

Thus (i) holds if and only if we can solve the congruence

$$xq_1q_2 + u^{-1}\left(s_1q_2 - u^2q_1s_2\right) \equiv 0 \pmod{\mathfrak{a}}$$

for some u, which is if and only if (ii) holds. □

Of course, if $d \neq 1, 3$ we have $u^2 = 1$ for all $u \in \mathfrak{o}^*$ anyway; if $d = 1$ we have $u^2 = \pm 1$, while if $d = 3$ then $u^2 = 1$, ρ^2 or ρ^4 where $\rho = \frac{1}{2}(1 + \sqrt{-3}\,)$.

The definition of Hecke operators T_π for prime elements π of $\mathfrak{o}$ is straightforward: on the cusps we have

$$T_\pi\colon [\alpha] \mapsto \sum_{x \bmod \pi} \left[\frac{\alpha + x}{\pi}\right] + [\pi\alpha]. \tag{2.2.8}$$

We have to define T_π for a prime *element* π rather than for a prime *ideal* since in general $T_\pi \neq T_{\varepsilon\pi}$. In fact we have

$$T_{\varepsilon\pi} = JT_\pi \tag{2.2.9}$$

as a simple computation will verify. On modular symbols $\{\alpha, \beta\}$, we have

$$T_\pi\colon \{\alpha, \beta\} \mapsto \sum_{x \bmod \pi} \left\{\frac{\alpha + x}{\pi}, \frac{\beta + x}{\pi}\right\} + \{\pi\alpha, \pi\beta\}. \tag{2.2.10}$$

So again we work with M-symbols but convert to modular symbols via the map ξ to compute the Hecke action. The conversion back from modular symbols to M-symbols is achieved as before using continued fractions (in K) to express an arbitrary modular symbol $\{\alpha, \beta\}$ as a sum of symbols of the type $\{\gamma(0), \gamma(\infty)\}$ for γ in Γ. We can use continued fractions because K is Euclidean, and so every element of K is equivalent modulo $\mathfrak{o}$ to an element with norm less than 1.

When the subgroup G is normalized by J (in particular, when $G = \Gamma_0(\mathfrak{a})$ for some ideal $\mathfrak{a}$), the space $H(G)$ decomposes according to the eigenvalues of the J involution as

$$H(G) = H^+(G) \oplus H^-(G) \tag{2.2.11}$$

where J acts as $+1$ on H^+ and as -1 on H^-. In the case of $G = \Gamma_0(\mathfrak{a})$ we will denote $H(G)$, $H^+(G)$ and $H^-(G)$ by $V(\mathfrak{a})$, $V^+(\mathfrak{a})$ and $V^-(\mathfrak{a})$ respectively.

In practice it is more convenient (that is, faster and requires less storage space) to compute $H^+(G)$ (resp. $H^-(G)$) separately as the quotient space $H(G)/H^-(G)$ (resp. $H(G)/H^+(G)$), by including extra relations

$$(\gamma) = (J^{-1}\gamma J) \qquad \text{or} \qquad (\gamma) = -(J^{-1}\gamma J), \tag{2.2.12}$$

or, in the case $G = \Gamma_0(\mathfrak{a})$,

$$(c:d) = (\varepsilon c:d) \qquad \text{or} \qquad (c:d) = -(\varepsilon c:d). \tag{2.2.12$'$}$$

This will enable us to give a simpler set of generators for the relation ideal $\mathscr{R}$ in the case $d = 1$ and $d = 3$.

To distinguish between the conjugation action of J, given in (2.2.4), (2.2.7), which induces the main involution, and the right coset action of J (which is trivial by 2.2.1 (ii)) we extend $\mathbb{Z}\tilde{\Gamma}$ by adding an extra element J^* to represent the conjugation action. This element J^* satisfies the relation $(J^*)^{-1}XJ^* = J^{-1}XJ$ for any X in $\mathbb{Z}\tilde{\Gamma}$. Then $\mathbb{Z}\tilde{\Gamma}$ together with J^* generates a larger ring of operators which we denote $\mathscr{A}$.

So the relation ideal $\mathscr{R}$ always contains $I - J$ by (2.2.1) (ii)); to enforce (2.2.12) we include either $I - J^*$ (for H^+) or $I + J^+$ (for H^-) in $\mathscr{R}$. Hence we define

$$\mathscr{R}^+ := \mathscr{R} + \langle I - J^* \rangle$$

and

$$\mathscr{R}^- := \mathscr{R} + \langle I + J^* \rangle$$

as left relation ideals in $\mathscr{A}$, and let $B^+(G) := C(G)\mathscr{R}^+$ (resp. $B^-(G) = C(G)\mathscr{R}^-$). Now $B^+(G)$ is not contained in ker ∂, since $\partial(\gamma) \neq \partial(J^{-1}\gamma J)$ in general. Clearly we must replace ∂ by $\partial^+ := \partial \circ (I + J^*)$ and define $Z^+(G) := \ker \partial^+$, so that $B^+(G) \subset Z^+(G)$. Similarly $\partial^- := \partial \circ (I - J^*)$ and $Z^-(G) := \ker \partial^-$. Hence we have the following result.

THEOREM 3: *Let G be a subgroup of finite index in Γ which is normalized by J. Then for either choice of sign $s = \pm$ we have an isomorphism*

$$\xi^s : H^s(G) := \frac{Z^s(G)}{B^s(G)} \to H_1^s(G \backslash H_3^*, \mathbb{Q})$$

where ξ is given by Theorem 2 *and*

$$\xi^+ = \xi \circ (I + J^*); \qquad \xi^- = \xi \circ (I - J^*);$$

here H_1^s denotes the subspace of H_1 on which the main involution acts with sign s.

We now turn to look more closely at the geometry of the five Euclidean fields, and determine the relation ideal $\mathscr{R}$ in each case.

2.3. Some hyperbolic geometry

Recall that $H_3 = \{(z, T) : z \in \mathbb{C}, t \in \mathbb{R}, t > 0\}$. Denote by j the point (0, 1) in H_3, and by P the unique point at the intersection of the three unit hemispheres centred at (0, 0), (1, 0), and (α, 0), where

$$\alpha = \begin{cases} \sqrt{-d} \text{ if } d = 1 \text{ or } 2; \\ \frac{1}{2}(1 + \sqrt{-d}) \text{ if } d = 3, 7 \text{ or } 11, \end{cases}$$

so that $\mathfrak{v} = \mathbb{Z} + \mathbb{Z}\alpha$ in all cases. The following finite subgroups of $\tilde{\Gamma}$ will be important:

$$G_j := \{\gamma \in \tilde{\Gamma} : \gamma(j) = j\};$$

$$G_P := \{\gamma \in \tilde{\Gamma} : \gamma(P) = P\}.$$

The group G_j is easily determined: the stabilizer of j in $GL(2, \mathbb{C})$ is

$$U(2) = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} : |u|^2 + |v|^2 \neq 0 \right\}$$

and thus its intersection with $\tilde{\Gamma}$ is

$$\left\{ \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}, \begin{pmatrix} 0 & u \\ v & 0 \end{pmatrix} : u, v \in \mathfrak{v}^* \right\}$$

(modulo scalars as usual) which is generated by

$$J = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

and thus has order $2w$ where $w = |\mathfrak{v}^*|$. The subgroup generated by J consists of those matrices in $\tilde{\Gamma}$ which fix 0 and ∞; the other coset in G_j consists of the matrices which interchange 0 and ∞.

Determining the subgroup G_P requires some computation which we omit since it is straightforward but long, and has been done by others (see [7,12]). In each case G_P is generated by

$$TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},$$

of order 3, and a further element X_d; the transforms of the geodesic $\{0, \infty\}$ under the action of G_P form the edges of the basic polyhedron B. We summarize the facts in the following table.

d	P	X_d	$o(X_d)$	$\lvert G_p \rvert$	Shape of B
1	$\left(\frac{1}{2}(1+\alpha), \frac{1}{\sqrt{2}}\right)$	$\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$	3	12	Octahedron
2	$\left(\frac{1}{2}(1+\alpha), \frac{1}{2}\right)$	$\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$	4	24	Cuboctahedron
3	$\left(\frac{1}{3}(1+\alpha), \sqrt{\frac{2}{3}}\right)$	$\begin{pmatrix} 1 & \alpha-1 \\ \alpha & 0 \end{pmatrix}$	3	12	Tetrahedron
7	$\left(\frac{1}{7}(3\alpha+2), \sqrt{\frac{3}{7}}\right)$	$\begin{pmatrix} -1 & \alpha \\ \alpha-1 & 1 \end{pmatrix}$	2	6	Triangular Prism
11	$\left(\frac{1}{11}(3+5\alpha), \sqrt{\frac{2}{11}}\right)$	$\begin{pmatrix} -1 & \alpha \\ \alpha-1 & 2 \end{pmatrix}$	3	12	Truncated Tetrahedron

The first types of relations in homology between symbols (γ) consist of 2-term relations and come from the elements of G_j: they are generated by $I+S$ and $I-J$. Secondly, each polyhedron B has a triangular face whose edges are the transforms of $\{0, \infty\}$ under I, TS and $(TS)^2$, so the relation ideal will always contain $I + TS + (TS)^2$. Thus for each field the relation ideal always contains the ideal $\mathscr{R}_0$, where

$$\mathscr{R}_0 = \langle I+S, I-J, I+TS+(TS)^2 \rangle.$$

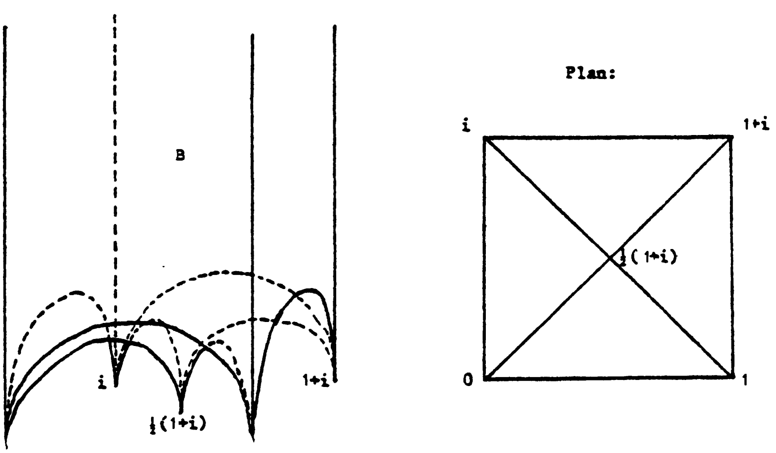


Figure 2.3.1

Also, let $\mathscr{R}_0^+ := \mathscr{R}_0 + \langle \mathrm{I} - \mathrm{J}^* \rangle$ and $\mathscr{R}_0^- := \mathscr{R}_0 + \langle \mathrm{I} + \mathrm{J}^* \rangle$ be the larger ideals used in calculating the eigenspaces for the J involution separately. There will be one more generator for $\mathscr{R}$, which we determine for each field in turn.

Case $d = 1$: We write $i = \sqrt{-1}$. Here

$$X = \begin{pmatrix} i & 1 \\ 1 & 0 \end{pmatrix}$$

which has order 3, and B has triangular faces which are the orbits of X (Fig. 2.3.1). The images of $\{0, \infty\}$ under X and X^2 are $\{\infty, i\}$ and $\{i, 0\}$, and so we get a relation $I + X + X^2$. Hence in this case,

$$\mathscr{R} = \mathscr{R}_0 + \langle I + X + X^2 \rangle.$$

LEMMA: $I + X + X^2 \in \mathscr{R}_0^{\pm}$.

PROOF: $\mathscr{R}_0^+$ contains $I + TS + (TS)^2$ and $I - J^*$; since $J^{-1}XJ = TS$ we have $XJ^* = J^*TS$, so

$$(I + X + X^2)J^* = J^*\left(I + TS + (TS)^2\right).$$

Hence

$$I + X + X^2 = (I + X + X^2)(I - J^*) + J^*\left(I + TS + (TS)^2\right)$$

is in the left ideal $\mathscr{R}_0^+$. The case of $\mathscr{R}_0^-$ is similar.

COROLLARY: *$\mathscr{R}^+ = \mathscr{R}_0^+$ and $\mathscr{R}^- = \mathscr{R}_0^-$.*

For instance, to calculate $V^+(\mathfrak{a})$ we start with the M-symbols $P^1(\mathfrak{a})$ and factor out by the relations

(i) $(c : d) = (ic : d)$;

(ii) $(c : d) + (-d : c) = 0$;

(iii) $(c : d) + (c + d : -c) + (d : -c - d) = 0$.

Notice that we have just added one extra relation ((i)) to the "rational relations" (ii), (iii).

Case $d = 2$: Now

$$X = \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}$$

which has order 4, and B has quadrilateral, as well as the usual triangu-

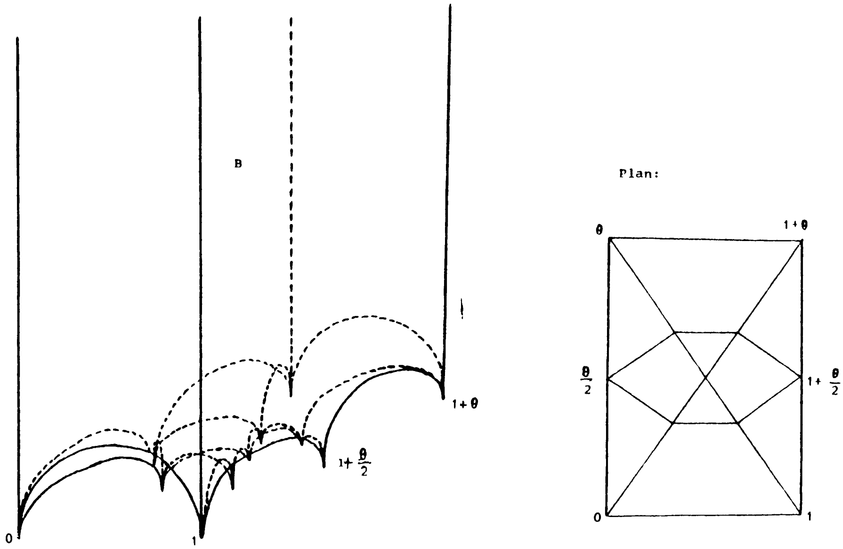


Figure 2.3.2. ($\alpha=\theta=\sqrt{-2}$)

lar, faces (Fig. 2.3.2). The orbit of $\{0, \infty\}$ under powers of X is $\{0, \infty\}$, $\{\infty, \alpha\}$, $\{\alpha, \frac{1}{2}\alpha\}$, $\{\frac{1}{2}\alpha, 0\}$ and so the extra relation is $I+X+X^2+X^3$:

$$\mathscr{R}=\mathscr{R}_0+\langle I+X+X^2+X^3\rangle.$$

No simplification occurs in $\mathscr{R}^{\pm}$, and so $\mathscr{R}^{\pm}=\mathscr{R}+\mathscr{R}_0^{\pm}$.

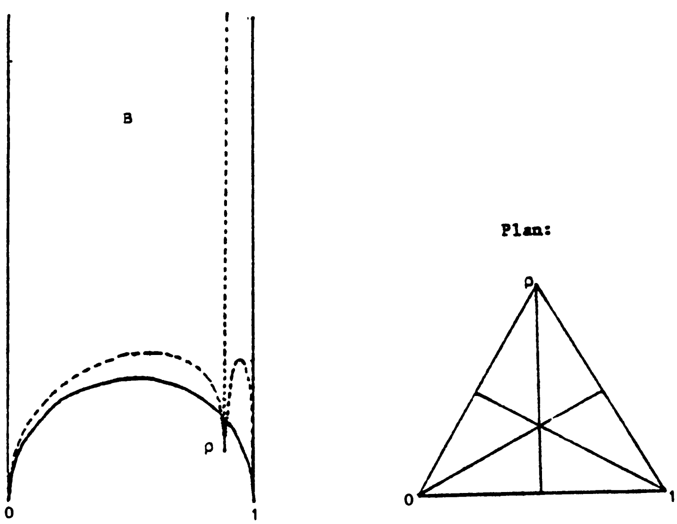


Figure 2.3.3. ($\alpha=\rho=\frac{1}{2}(1+\sqrt{-3})$)

Case $d=3$: Here

$$X=\begin{pmatrix}1 & \alpha-1\\ \alpha & 0\end{pmatrix}$$

which has order 3, and we have the relation $I+X+X^2$. B is a tetrahedron (Fig. 2.3.3). As for $\mathbb{Q}(i)$ we have $J^{-1}XJ=TS$, and hence

$$\mathscr{R}=\mathscr{R}_0+\langle I+X+X^2\rangle;$$

$$\mathscr{R}^{\pm}=\mathscr{R}_0^{\pm}.$$

Case $d=7$: Now

$$X=\begin{pmatrix}-1 & \alpha\\ \alpha-1 & 1\end{pmatrix}$$

and has order 2. The basic polyhedron B is a triangular prism (Fig. 2.3.4) whose triangular faces have vertices $\{0,\infty,1\}$ and $\{\alpha,\tfrac12(1+\alpha),\tfrac12\alpha\}$: orbits of TS. The square faces are not given by orbits of a single matrix as in previous cases: the square face with one edge $\{0,\infty\}$ has vertices $\{0,\infty,\alpha,\tfrac12\alpha\}$, and edges $\{0,\infty\}$;

$$\{\infty,\alpha\}=\{U(\infty),U(0)\}=-(U);$$

$$\{\alpha,\tfrac12\alpha\}=\{X(0),X(\infty)\}=(X);$$

and

$$\{\tfrac12\alpha,0\}=\{XU(\infty),XU(0)\}=-(XU),$$

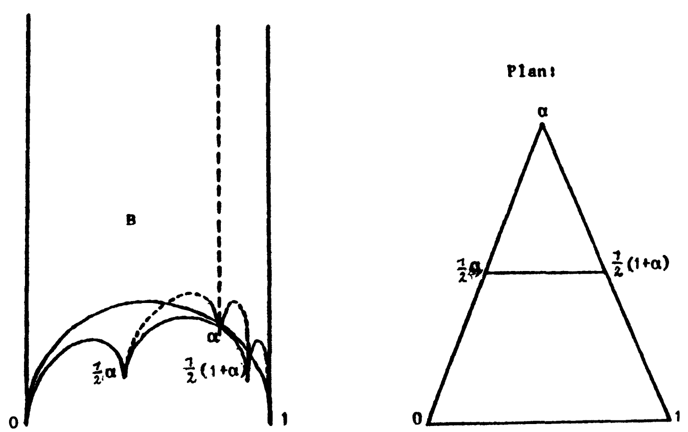


Figure 2.3.4

where

$$U = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

So the extra relation is now $I - U + X - XU$, or $(I + X)(I - U)$. Hence

$$\mathscr{R} = \mathscr{R}_0 + \langle (I + X)(I - U) \rangle$$

and $\mathscr{R}^{\pm} = \mathscr{R} + \mathscr{R}_0^{\pm}$.

Case $d = 11$. Here finally

$$X = \begin{pmatrix} -1 & \alpha \\ \alpha - 1 & 2 \end{pmatrix}$$

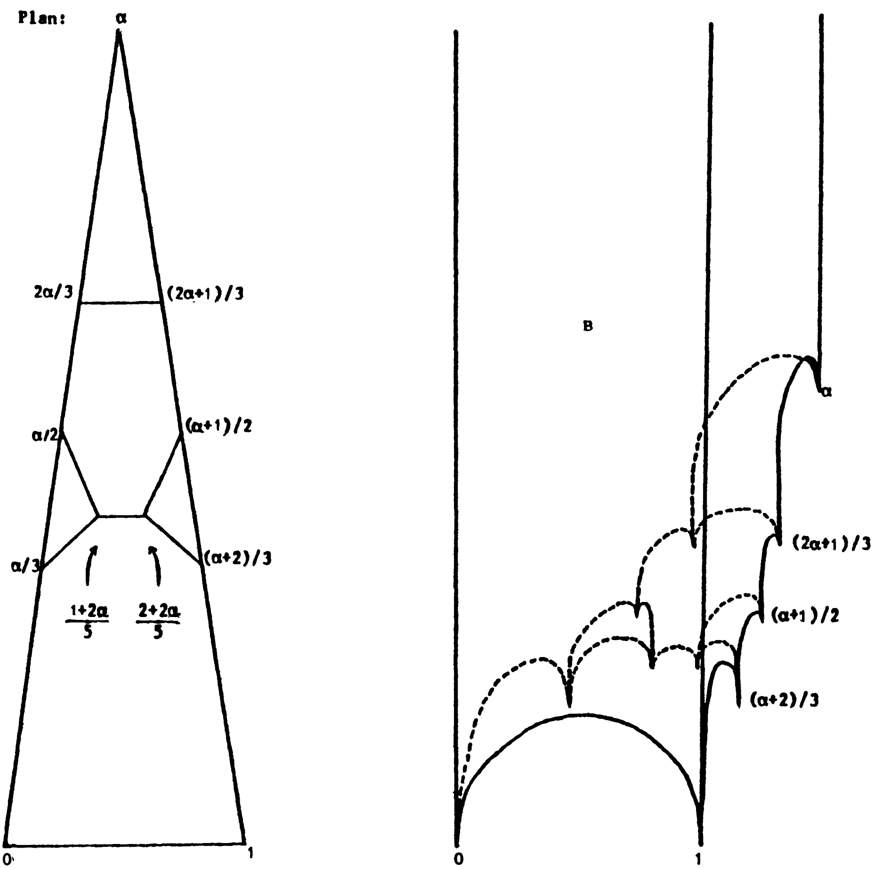


Figure 2.3.5

which has order 3. The polyhedron B is a truncated tetrahedron (Fig. 2.3.5) whose triangular faces come from the orbits of TS as usual. The hexagonal face which includes $\{0, \infty\}$ as an edge has edges $\{0, \infty\}$;

$$\{\infty, \alpha\} = \{U(\infty), U(0)\} = -(U);$$

$$\{\alpha, \tfrac{2}{3}\alpha\} = \{X^2(0), X^2(\infty)\} = (X^2);$$

$$\{\tfrac{2}{3}\alpha, \tfrac{1}{2}\alpha\} = \{X^2U(\infty), X^2U(0)\} = -(X^2U);$$

$$\{\tfrac{1}{2}\alpha, \tfrac{1}{3}\alpha\} = \{X(0), X(\infty)\} = (X);$$

and

$$\{\tfrac{1}{3}\alpha, 0\} = \{XU(\infty), XU(0)\} = -(XU).$$

So the extra relation is $I - U + X^2 - X^2U + X - XU$, or $(I + X + X^2)(I - U)$, and we have

$$\mathscr{R} = \mathscr{R}_0 + \langle (I + X + X^2)(I - U) \rangle;$$

$$\mathscr{R}^{\pm} = \mathscr{R} + \mathscr{R}_0^{\pm}.$$

We sum up the results of this section in the following table (where $X = X_d$ depends on the field as above).

d	$\mathscr{R}$	$\mathscr{R}^+$
1	$\mathscr{R}_0 + \langle I + X + X^2 \rangle$	$\mathscr{R}_0^+$
2	$\mathscr{R}_0 + \langle I + X + X^2 + X^3 \rangle$	$\mathscr{R} + \mathscr{R}_0^+$
3	$\mathscr{R}_0 + \langle I + X + X^2 \rangle$	$\mathscr{R}_0^+$
7	$\mathscr{R}_0 + \langle (I + X)(I - U) \rangle$	$\mathscr{R} + \mathscr{R}_0^+$
11	$\mathscr{R}_0 + \langle (I + X + X^2)(I - U) \rangle$	$\mathscr{R} + \mathscr{R}_0^+$
	$\mathscr{R}_0 = \langle I - J, I + S, I + TS + (TS)^2 \rangle$	
	$\mathscr{R}_0^+ = \mathscr{R}_0 + \langle I - J^* \rangle$	

3. The computations and results

3.1. Introduction to the tables

For each of the five Euclidean fields discussed in the previous section, computer programs have been written in Algol 68 which carry out the algorithms presented there, in terms of M-symbols. These programs have been run on an ICL 2980 computer at the Oxford University Computing Service. Thus we have been able to calculate, for each field K and each ideal $\mathfrak{a}$ of $\mathfrak{o}_K$ such that $N\mathfrak{a}$ is not too large, the following data:

(i) the dimension of $V(\mathfrak{a})$;
(ii) the action of the main involution J on $V(\mathfrak{a})$ and the dimensions of $V^+(\mathfrak{a})$ and $V^-(\mathfrak{a})$;
(iii) the action of the W_π involution for each prime π dividing $\mathfrak{a}$;
(iv) the action of the Hecke operator T_π for a prime π not dividing $\mathfrak{a}$;
(v) the splitting of $V(\mathfrak{a})$ into one-dimensional subspaces which are eigenspaces for all of the above operators, and their eigenvalues on each subspace;
(vi) the splitting of $V(\mathfrak{a})$ into "newforms" and "oldforms".

Remark on (vi): We can easily determine which eigenspaces in $V(\mathfrak{a})$ correspond to oldforms, since we will have already met them as newforms for $\Gamma_0(\mathfrak{b})$ for some $\mathfrak{b}$ dividing $\mathfrak{a}$.

For each field we give first a table showing, for each ideal $\mathfrak{a}$ with $N\mathfrak{a} \leqslant B_K$, the dimensions of $V(\mathfrak{a})$, $V^+(\mathfrak{a})$ and $V^-(\mathfrak{a})$, and an indication of the splitting of each space into newforms and oldforms. Then, for each $\mathfrak{a}$ such that there are newforms for $\Gamma_0(\mathfrak{a})$ in $V^+(\mathfrak{a})$ we list the first fifteen Hecke eigenvalues for each *rational* newform (with rational eigenvalues). We have omitted non-rational eigenvalues for simplicity: instead, when there is a conjugate set of newforms defined over a number field L we just give this "splitting field" L. In the range covered by the tables, a quadratic splitting field occurs 19 times, a cubic field 3 times, and over $\mathbb{Q}(\sqrt{-11})$ a quintic splitting field is required for $V((13))$. [The splitting field is always totally real, since the Hecke operators are self-adjoint with respect to a Hermitian inner product which generalizes the Petersson inner product: see [16].] The undiagonalized matrices for the first fifteen Hecke operators are available on computer printout for these cases.

Thus, two limits (B_K and 15) had to be set for each field. These were decided on by consideration of how much computer time was available. In all cases the physical limitations (storage space needed and size of integers encountered) would have allowed the computations to be extended much further. For example, for $K = \mathbb{Q}(i)$, the systematic coverage of all levels stops at $N\mathfrak{a} = 500$, but a few isolated levels were calculated up to $\mathfrak{a} = (1+i)^{12}$ with norm 4096. These sporadic cases were chosen for two reasons: firstly to gather evidence for Theorem 4 before this was proved; and secondly when it was known that there existed elliptic curves with the corresponding conductor. For instance, R.J. Stroeker's thesis [17] gives tables of all elliptic curves over $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$ with bad reduction only at the primes dividing 2. For $\mathbb{Q}(\sqrt{-1})$, extra calculations were done with powers of $(1+i)$.

The results of these extra computations are recorded in [4] or are available from the author. He can also provide explicit bases for each $V(\mathfrak{a})$ in terms of modular symbols.

For the first three fields, some of these calculations have been previously carried out by Mennicke and Grunewald, working in Bielefeld. They only work with prime ideals of degree one, for which the M-symbols just reduce to elements of the projective line over the finite field $GF(p)$, for a rational prime p. The relations they use are derived in an algebraic rather than a geometric way, described in [10] for the case $\mathbb{Q}(\sqrt{-1})$. In that paper they also give results for $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-3})$ which agree with the tables given here insofar as they overlap.

We have also made a systematic search for elliptic curves with small conductor over each of the five fields. Here we implement on the computer Tate's algorithm, given in [19], to determine the type of reduction of an elliptic curve at a prime $\mathfrak{p}$, given its coefficients a_1, a_2, a_3, a_4 and a_6. It is easily seen from the formulae given by Tate [19] that we may assume that a_1, a_2 and a_3 are reduced modulo 2, 3 and 2 respectively. So the search consists of a systematic stepping through an enumeration of the pairs (a_4, a_6). For each pair, all 144 sets of values of a_1 and a_3 (modulo 2) and a_2 (modulo 3) are considered.

In the following five subsections we give three tables for each field. The contents of each, and notation used, are as follows.

Table 1. For each $\mathfrak{a}$ with $N\mathfrak{a} \leqslant B_K$ such that $r(\mathfrak{a})(= \dim V(\mathfrak{a})) > 0$ we give $r(\mathfrak{a})$ and indicate how this splits between $V^+(\mathfrak{a})$ and $V^-(\mathfrak{a})$. In each of the columns headed "+" and "−",

(i) an entry of "**1**" (bold face 1) denotes a rational "newform", that is, a one-dimensional eigenspace with rational eigenvalues;

(ii) an entry of "***n***" (bold face n) for $n \geqslant 2$ denotes an n-dimensional subspace spanned by a set of n "newforms", defined and conjugate over a number field of degree n;

(iii) an entry of "n" in ordinary typeface denotes an n-dimensional "oldclass": that is, an n-dimensional subspace spanned by n "oldforms" which have the same eigenvalue for all T_π where π does not divide $\mathfrak{a}$.

Levels $\mathfrak{a}$ with $\dim V(\mathfrak{a}) = 0$ have been omitted for brevity. Also, only one ideal from each conjugate pair $\mathfrak{a}$, $\bar{\mathfrak{a}}$ is given, since obviously conjugation induces an isomorphism from $V(\mathfrak{a})$ to $V(\bar{\mathfrak{a}})$, and thus the data for $\mathfrak{a}$ and $\bar{\mathfrak{a}}$ are identical.

Table 2. For each rational "newform" in $V^+(\mathfrak{a})$ with $N\mathfrak{a} \leqslant B_K$ we give: the eigenvalue ± 1 of all the W_π-involutions (for each π dividing $\mathfrak{a}$) as "+" or "−"; the eigenvalue of T_π for all other π with $N\pi < 50$. For conjugate sets of newforms with not all eigenvalues rational we just give the splitting field.

Table 3. A list of elliptic curves defined over K whose conductors have norm less than B_K, in order of the conductor norm. For each curve we give the coefficients, the conductor $\mathfrak{f}$, and indicate whether the curve has complex multiplication by an order in K. Only one curve from each isomorphism class is included. Curves conjugate to listed curves are usually omitted. Isogenies between given curves are shown: they are 2-isogenies unless otherwise indicated.

No claim of completeness is made for this list of curves. There are certainly more curves with small conductor with coefficients outside the search region. In particular, no attempt was made to find all curves isogenous to given ones. A more complete list is in preparation.

The search regions for (a_4, a_6) were as follows:

Field	Region searched
$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$	$\{x + y\alpha \mid -3 \leqslant x, y \leqslant 3\}$
$\mathbb{Q}(\sqrt{-7})$	$\{x + y\alpha \mid -3 \leqslant x \leqslant 2,\ -2 \leqslant y \leqslant 3\}$
$\mathbb{Q}(\sqrt{-11})$	$\{x + y\alpha \mid -2 \leqslant x, y \leqslant 2\}$

A few curves are included with coefficients outside these ranges, either as a result of a program overruning, or from existing tables of elliptic curves defined over $\mathbb{Q}$ with small conductor.

In the tables we write "i" for $\sqrt{-1}$, "θ" for $\sqrt{-2}$, "ρ" for $\frac{1}{2}(1+\sqrt{-3})$ and "α" for either $\frac{1}{2}(1+\sqrt{-7})$ or $\frac{1}{2}(1+\sqrt{-11})$.

3.7. Comments on the results in the tables

The tables of results of computations for the five Euclidean fields give support to the Main Conjecture, stated in the Introduction, which we restate now in greater detail.

MAIN CONJECTURE [2] (i) *For every rational newform in $V^+(\mathfrak{a})$ there corresponds an isogeny class of elliptic curves defined over K with conductor $\mathfrak{a}$.*

(ii) *For primes $\mathfrak{p}$ not dividing $\mathfrak{a}$, the Trace of Frobenius of the curve at $\mathfrak{p}$ is equal to the eigenvalue of $T_{\mathfrak{p}}$ acting on the space generated by the newform.*

(iii) *For primes $\mathfrak{p}$ dividing $\mathfrak{a}$: if $\mathfrak{p}^2$ divides $\mathfrak{a}$ then the Trace of Frobenius of the curve at $\mathfrak{p}$ is 0; otherwise (if $\mathfrak{p}$ divides $\mathfrak{a}$ exactly) it is minus the corresponding eigenvalue of $W_{\mathfrak{p}}$.*

(iv) *Every elliptic curve defined over K corresponds to a newform in $V^+(\mathfrak{a})$ (where $\mathfrak{a}$ is the conductor of the curve) in this way, except when the curve has complex multiplication by an order in K.*

Regarding the second and third parts of the conjecture: for each of the curves listed above, the Trace of Frobenius $a_{\mathfrak{p}}$ at each prime $\mathfrak{p}$ with $N\mathfrak{p} < 50$ was calculated by counting the number of points $M_{\mathfrak{p}}$ on the curve modulo $\mathfrak{p}$ (including the point at infinity):

$$a_{\mathfrak{p}} = 1 + N\mathfrak{p} - M_{\mathfrak{p}}.$$

In each case the conjecture was verified. The tables of $a_{\mathfrak{p}}$ were given in [4]: they have been omitted here for the sake of brevity.

[2] See end of paper.

TABLE 3.2.1
Ideals $\mathfrak{a}$ of $\mathbb{Z}[\sqrt{-1}]$ with dim $V(\mathfrak{a}) > 0$ and $N\mathfrak{a} \leqslant 500$

$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	+	−	$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	+	−	$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	+	−
$(7+4i)$	65	1	**1**		$(14+8i)$	260	3	3		$(17+9i)$	370	3		**1**+2
$(8+2i)$	68	1		**1**	$(16+2i)$	260	2	2		$(16+11i)$	377	4	**1+2**	**1**
$(6+6i)$	72	1	**1**		$(16+3i)$	265	1	**1**		$(18+8i)$	388	4	2+2	
$(7+7i)$	98	1	**1**		$(16+4i)$	272	4	**1**	3	$(14+14i)$	392	5	**1+1**+3	
(10)	100	1	**1**		$(15+7i)$	274	2		2	$(15+13i)$	394	1		**1**
$(9+5i)$	106	1	**1**		$(14+9i)$	277	1	**1**		(20)	400	7	2+3	**1+1**
(11)	121	1	**1**		$(12+12i)$	288	5	3	2	$(17+11i)$	410	2	**1+1**	
$(9+7i)$	130	1	**1**		(17)	289	1	**1**		$(19+7i)$	410	2	**1**	**1**
$(11+3i)$	130	2	2		$(17+i)$	290	5	**1**	4	$(18+10i)$	424	4	3	**1**
$(10+6i)$	136	2		2	$(13+11i)$	290	2		2	$(19+8i)$	425	2	**1**	**1**
$(11+4i)$	137	1		**1**	$(15+9i)$	306	1		**1**	$(17+12i)$	433	2		**2**
(12)	144	3	2	**1**	$(17+5i)$	314	1	**1**		(21)	441	1	**1**	
$(9+8i)$	145	2		**1+1**	$(16+8i)$	320	4	2	2	$(19+9i)$	442	2	**1**	**1**
$(12+i)$	145	1		**1**	(18)	324	1	**1**		$(18+11i)$	445	2		**2**
$(12+4i)$	160	2	**1**	**1**	$(15+10i)$	325	3	2	**1**	$(15+15i)$	450	3	**1**+2	
$(10+8i)$	164	1	**1**		$(17+6i)$	325	1		**1**	$(21+3i)$	450	2	**1**	**1**
$(12+6i)$	180	1		**1**	$(18+i)$	325	3	2	**1**	$(16+4i)$	452	1		**1**
$(13+4i)$	185	1		**1**	$(18+2i)$	328	3	2	**1**	$(17+13i)$	458	1		**1**
$(13+5i)$	194	2	**1+1**		$(13+13i)$	338	2	**1+1**		$(21+5i)$	466	2	2	
(14)	196	2	2		$(18+4i)$	340	2		2	$(18+12i)$	468	1		**1**
$(10+10i)$	200	3	**1**+2		$(14+12i)$	340	3	**1**	2	(22)	484	4	**1**+3	
$(14+4i)$	212	2	2		$(18+6i)$	360	4	2	2	$(17+14i)$	485	2	**2**	
(15)	225	1	**1**		(19)	361	3	**1**	**1+1**	$(21+7i)$	490	2	2	
$(13+8i)$	233	1	**1**		$(19+i)$	362	2	**1**	**1**	$(18+13i)$	493	1		**1**
$(11+11i)$	242	2	2		$(15+12i)$	369	1		**1**	$(20+10i)$	500	3	2	**1**
$(16+i)$	257	1	**1**											

TABLE 3.2.2
$\mathbb{Q}(\sqrt{-1})$: Newforms in $V^+(\mathfrak{a})$

$\mathfrak{a}$	$1+i$	$2+i$	$2-i$	3	$3+2i$	$3-2i$	$1+4i$	$1-4i$	$5+2i$	$5-2i$	$1+6i$	$1-6i$	$5+4i$	$5-4i$	7	other W
$(7+4i)$	0	+	0	−2	−4	−	6	0	−6	6	2	2	0	6	−4	
$(6+6i)$	+	−2	−2	−	−2	−2	2	2	6	6	6	6	−6	−6	−14	
$(7+7i)$	+	0	0	−2	−4	−4	6	6	−6	−6	2	2	6	6	−	
(10)	−	+	+	−2	2	2	−6	−6	6	6	2	2	6	6	−10	
$(9+5i)$	−	−3	−3	1	−4	5	0	0	−6	3	2	2	6	−3	5	$+(7-2i)$
(11)	−2	1	1	−5	4	4	−2	−2	0	0	3	3	−8	−8	−10	$-(11)$
$(9+7i)$	+	0	+	4	−4	−	−6	0	−6	0	2	2	−6	6	14	
$(12+4i)$	+	−	−2	2	−2	−2	2	−6	−2	−2	−2	6	−6	10	2	
$(10+8i)$	−	0	0	−2	2	−4	6	−6	6	0	8	−4	+	−6	2	
$(13+5i)$	+	3	−3	4	−4	−4	3	0	6	−3	−7	−7	0	−9	−4	$-(9-4i)$
$(13+5i)$	−	−1	−1	−4	0	0	−3	4	2	9	3	−11	0	7	8	$+(9-4i)$
$(10+10i)$	−	−	−	−6	−2	−2	2	2	−2	−2	6	6	−6	−6	2	
(15)	−1	−	−	−	−2	−2	2	2	−2	−2	−10	−10	10	10	−14	
$(13+8i)$	−2	−3	−2	−4	3	−3	−4	−3	6	−7	4	4	12	−5	1	$+(13+8i)$
$(16+i)$	−1	−2	2	2	6	−2	2	2	−6	−6	−10	−6	10	2	2	$-(16+i)$
$(16+3i)$	0	0	−	4	2	2	−6	−6	6	−6	2	−4	0	−6	2	$+(7-2i)$
$(16+4i)$	+	2	−2	2	−6	2	2	−	−6	−2	2	−2	2	−6	2	
$(14+9i)$	−1	−4	−1	−1	−4	−6	−1	2	1	5	−6	−1	6	6	−1	$+(14+9i)$

(17)	−1	−2	−2	−6	−2	−2	−	−	6	6	−2	−2	−6	−6	2	
$(17+i)$	−	0	+	−2	−4	2	0	0	+	0	−10	8	−6	6	−10	
$(17+5i)$	+	−4	−3	−1	−3	−1	−7	5	2	−6	−2	−2	−5	4	4	$+(11-6i)$
(18)	−	0	0	+	2	2	0	0	0	0	−10	−10	0	0	2	
$(13+13i)$	+	−3	−3	−5	−	−	−3	−3	6	6	−7	−7	0	0	−13	
$(13+13i)$	−	−1	−1	3	+	+	−3	−3	2	2	3	3	0	0	−13	
$(14+12i)$	−	0	+	4	2	−4	6	+	−6	−6	−10	2	0	−6	−4	
(19)	0	3	3	−2	−4	−4	−3	−3	6	6	2	2	−6	−6	−13	−(19)
$(19+i)$	+	0	3	−2	5	−4	−6	3	−9	6	2	−7	6	9	−4	$-(9+10i)$
$(16+11i)$	0	3	0	−2	5	−	−3	0	3	+	−7	−7	−9	−3	−4	
$(16+11i)$	$\mathbb{Q}(\sqrt{2})$															
$(14+14i)$	−	−4	−4	−2	0	0	−2	−2	2	2	−6	−6	−2	−2	−	
$(14+14i)$	+	2	2	−6	2	2	−6	−6	6	6	−2	−2	2	2	−	
$(17+11i)$	+	0	−	4	−4	2	0	−6	6	6	2	−4	6	+	−10	
$(17+17i)$	+	−4	+	−4	0	−6	0	2	−6	−2	−2	8	6	+	−2	
$(19+7i)$	−	−2	−	2	−2	−2	2	−6	−2	6	−10	−2	−	10	2	
$(19+8i)$	2	0	−	−4	0	2	+	0	6	2	−4	6	8	−4	−4	
(21)	−1	−2	−2	−	−2	−2	−6	−6	−2	−2	6	6	2	2	−	
$(19+9i)$	+	0	3	−5	5	−	3	+	−6	0	−7	2	3	−3	14	
$(15+15i)$	+	+	+	−	2	2	6	6	−6	−6	2	2	−6	−6	2	
$(21+3i)$	−	1	+	+	−6	−1	3	−7	0	5	3	8	12	2	−5	
(22)	−	−3	−3	−5	−4	−4	6	6	0	0	−1	−1	0	0	−10	−(11)
$(17+14i)$	$\mathbb{Q}(\sqrt{2})$															

TABLE 3.2.3
Elliptic Curves defined over $\mathbb{Q}(\sqrt{-1})$ with small conductor

a_1	a_2	a_3	a_4	a_6	$CM(1)$?	$\mathfrak{f}$	$N\mathfrak{f}$	Isogenies
$1+i$	i	i	0	0	√	$(3-4i)$	25	
0	0	0	-1	0	√	(8)	64	
$1+i$	i	$1+i$	$2-i$	$-i$	√	(8)	64	
$1+i$	0	1	0	0		$(7+4i)$	65	
$1+i$	$1+i$	i	$-1+i$	-1		$(7+4i)$	65	
0	1	0	1	0		$(6+6i)$	72	
$1+i$	0	$1+i$	$1-i$	0		$(6+6i)$	72	
i	0	i	0	0		$(7+7i)$	98	
0	1	0	-1	0		(10)	100	
$1+i$	$-i$	$1+i$	$-1-i$	0		(10)	100	
1	$-1+i$	$1+i$	$-1-i$	0		$(9+5i)$	106	
0	-1	1	0	0		(11)	121	
i	$1-i$	i	$-i$	0		$(9+7i)$	130	
0	$-1-i$	0	1	$-1-i$		$(12+4i)$	160	
0	$-1+i$	0	$1+2i$	$-3-i$		$(12+4i)$	160	
$1-i$	$1+i$	$1-i$	$-5+4i$	$2-3i$		$(12+4i)$	160	
$1+i$	$1+i$	0	i	0		$(10+8i)$	164	
1	$-1+i$	$-i$	$-4-3i$	$-4i$		$(13+5i)$	194	
$-i$	i	$-i$	$-i$	1		$(13+5i)$	194	
$1+i$	i	0	1	0		$(10+10i)$	200	
0	0	0	2	1		$(10+10i)$	200	
$1+i$	i	$1+i$	$-4-i$	$2i$		$(10+10i)$	200	
1	1	1	0	0		(15)	225	
1	1	1	-5	2		(15)	225	
0	$1-i$	i	$-i$	0		$(13+8i)$	233	
0	0	0	1	0		(16)	256	
1	i	$-i$	i	0		$(16+i)$	257	
$1-i$	0	$-i$	$-1+i$	i		$(16+3i)$	265	
$1-i$	$-1-i$	1	$-4+2i$	$3+i$		$(16+3i)$	265	
$1-i$	$1+i$	$1-i$	$-1+i$	-1		$(16+4i)$	272	
0	$1+i$	0	$2i$	-1		$(16+4i)$	272	
1	$1+i$	$1+i$	i	0		$(14+9i)$	277	
i	1	i	0	0		(17)	289	
1	1	$-i$	1	1		$(17+i)$	290	
1	$1+i$	i	0	0		$(17+5i)$	314	
0	0	0	0	1		(18)	324	
$1+i$	i	0	3	$-i$		(18)	324	
1	0	1	0	0		$(13+13i)$	338	
i	1	i	-2	-3		$(13+13i)$	338	
0	i	0	$-1+2i$	$-1-i$		$(14+12i)$	340	
$1-i$	$-1-i$	$1-i$	$1-i$	$-4+i$		$(14+12i)$	340	
0	1	1	1	0		(19)	361	
1	$-1+i$	1	i	0		$(19+i)$	362	
0	$-i$	i	i	1		$(16+11i)$	377	
$1+i$	$-i$	$1+i$	$-i$	0		$(14+14i)$	392	
$1+i$	i	$1+i$	$4-i$	$-2i$		$(14+14i)$	392	
$1+i$	i	0	-1	0		$(14+14i)$	392	
1	$1-i$	1	$-i$	0		$(17+11i)$	410	
1	$-i$	$-i$	$1+i$	$-i$		$(19+7i)$	410	
1	0	0	-4	-1		(21)	441	
1	0	0	1	0		(21)	441	
i	-1	0	$2-i$	i		$(19+9i)$	442	
1	0	1	1	2		$(15+15i)$	450	
$-i$	$-1+i$	$1-i$	0	0		$(21+3i)$	450	
0	$-i$	$1+i$	-1	0		(22)	484	

TABLE 3.3.1
Ideals $\mathfrak{a}$ of $\mathbb{Z}[\sqrt{-2}]$ with dim $V(\mathfrak{a}) > 0$ and $N\mathfrak{a} \leqslant 300$

$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	+	−
(4θ)	32	1	**1**	
(6)	36	1		**1**
$(3+4\theta)$	41	1		**1**
(7)	49	1		**1**
$(7+\theta)$	51	1	**1**	
$(2+5\theta)$	54	2	**1**	**1**
(8)	64	2	2	
$(8+\theta)$	66	1		**1**
(6θ)	72	3	**1**	2
$(5+5\theta)$	75	1		**1**
$(8+3\theta)$	82	2		2
$(8+4\theta)$	96	2	2	
(7θ)	98	3	**1**	2
$(9+3\theta)$	99	1	**1**	
(10)	100	3	**1**	**2**
$(2+7\theta)$	102	2	2	
$(10+2\theta)$	108	4	2	2
$(6+6\theta)$	108	3	**1**	2
$(4+7\theta)$	114	2	**1**	**1**
(11)	121	2	**1**	**1**
$(11+\theta)$	123	3		**1**+2
$(5+7\theta)$	123	2		2
(8θ)	128	5	3	**1**+**1**
$(11+2\theta)$	129	2		**1**+**1**
$(10+4\theta)$	132	1		**1**
$(2+8\theta)$	132	2		2
$(6+7\theta)$	134	1		**1**

$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	+	−
$(8+6\theta)$	136	1		**1**
(12)	144	7	**1**+2	**1**+3
$(12+\theta)$	146	1		**1**
$(7+7\theta)$	147	2		2
$(10+5\theta)$	150	2		2
$(9+6\theta)$	153	2	2	
$(5+8\theta)$	153	3	2	**1**
$(12+3\theta)$	162	4	2	2
$(8+7\theta)$	162	4	2	2
$(6+8\theta)$	164	4	**1**	3
$(2+9\theta)$	166	1		**1**
(13)	169	2		**2**
$(3+9\theta)$	171	1		**1**
$(4+9\theta)$	178	1	**1**	
$(8+\theta)$	192	4	4	
$(12+5\theta)$	194	2	**1**	**1**
(14)	196	7	2	**2**+3
$(10+7\theta)$	198	3	**1**	2
$(6+9\theta)$	198	5	2	**1**+2
(10θ)	200	7	**1**+2	2+2
$(14+2\theta)$	204	3	3	
$(2+10\theta)$	204	2		**2**
$(12+6\theta)$	216	9	2+2	**1**+4
$(4+10\theta)$	216	6	3	3
$(11+7\theta)$	219	1	**1**	
(15)	225	7	**1**	**1**+**1**+2+2
$(5+10\theta)$	225	3	**1**	2

$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	+	−
$(14+4\theta)$	228	4	2	2
$(12+7\theta)$	242	2	**1**	**1**
(11θ)	242	4	2	2
$(14+5\theta)$	246	4	4	
$(2+11\theta)$	246	9	**1**	**1**+**1**+2+4
$(7+10\theta)$	249	1	**1**	
(16)	256	11	**1**+**1**+4	**1**+2+2
$(16+\theta)$	258	1	**1**	
$(4+11\theta)$	258	4		2+2
$(16+2\theta)$	264	5	**1**	**1**+3
$(8+10\theta)$	264	2		2
$(13+7\theta)$	267	2	**2**	
$(5+11\theta)$	267	1	**1**	
$(14+6\theta)$	268	2		2
$(12+8\theta)$	272	3		**1**+2
$(6+11\theta)$	278	1		**1**
$(16+4\theta)$	288	4	3	**1**
(12θ)	288	19	**1**+**1**+**1**+**1**+2+3+4	2+4
(17)	289	5	**1**	**1**+**1**+**2**
$(2+12\theta)$	292	2		2
$(14+7\theta)$	294	9	2	**1**+**1**+**1**+4
$(15+6\theta)$	297	5	**1**+2	**1**+**1**
$(13+8\theta)$	297	4	**1**+**1**	**1**+**1**
$(3+12\theta)$	297	5	**1**+2	**1**+**1**
$(10+10\theta)$	300	9	2	3+2+2

$(\theta = \sqrt{-2})$.

TABLE 3.3.2
$Q(\sqrt{-2})$: Newforms in $V^+(\mathfrak{a})$

$\mathfrak{a}$	θ	$1+\theta$	$1-\theta$	$3+\theta$	$3-\theta$	$3+2\theta$	$3-2\theta$	$1+3\theta$	$1-3\theta$	5	$3+4\theta$	$3-4\theta$	$5+3\theta$	$5-3\theta$	7	Other W
(4θ)	−	0	0	0	0	2	2	0	0	−6	10	10	0	0	−14	
$(7+\theta)$	−2	+	−2	−2	−4	−6	+	−4	0	−2	−2	−2	10	−2	−2	
$(2+5\theta)$	+	−	1	3	0	−6	−3	2	2	−1	0	−3	8	−10	−4	
(6θ)	−	+	+	4	4	2	2	−4	−4	−6	−6	−6	4	4	−14	
(7θ)	+	−2	−2	0	0	6	6	2	2	−10	6	6	8	8	−	
$(9+3\theta)$	−1	+	−	+	4	−6	2	4	4	2	−6	−6	12	4	−6	
(10)	−	−2	−2	0	0	−6	−6	−4	−4	−	6	6	−10	−10	−10	
$(6+6\theta)$	−	−	−	0	0	−6	6	−4	−4	2	−6	6	−4	−4	2	
$(4+7\theta)$	−	+	0	4	4	−2	−6	0	+	−2	−10	6	−4	0	2	
(11)	−2	−1	−1	−	−	−2	−2	0	0	−9	−8	−8	−6	−6	−10	
(12)	−	−	−	−4	−4	2	2	4	4	−6	−6	−6	−4	−4	−14	
$(6+8\theta)$	−	0	−2	−4	−6	2	−2	4	−2	−2	−	−6	−2	−2	10	
$(4+9\theta)$	−	1	1	0	−3	−6	3	−4	5	8	0	−9	8	8	2	$+(9-2\theta)$
$(12+5\theta)$	+	0	−1	3	−6	−5	−6	−4	6	−3	−6	10	4	4	2	$+(5-6\theta)$
$(10+7\theta)$	+	−	−2	−	−6	0	0	−4	−4	−4	6	−6	−4	2	−10	
(10θ)	+	0	0	4	4	2	2	4	4	−	−6	−6	−8	−8	2	

$(11+7\theta)$	0	0	+	−2	0	−2	−2	−2	−6	−2	6	−6	4	−10	−2	$+(1-6\theta)$
(15)	−1	+	+	−4	−4	2	2	4	4	−	10	10	4	4	−14	
$(5+10\theta)$	2	0	−	2	6	−2	2	−6	2	+	−6	6	−4	−8	−6	
$(12+7\theta)$	+	−1	2	3	−	0	6	−2	5	4	0	6	4	−4	−5	
$(2+11\theta)$	+	−	−3	−3	−4	1	−7	−5	1	4	−12	−	−2	1	−11	
$(7+10\theta)$	−1	+	1	−2	−5	−1	−7	2	4	−6	9	−11	−7	11	−4	$+(9+\theta)$
(16)	−	2	2	−2	−2	−2	−2	2	2	−6	−6	−6	6	6	2	
(16)	+	−2	−2	2	2	−2	−2	−2	−2	−6	−6	−6	−6	−6	2	
$(16+\theta)$	−	+	2	4	−2	−6	0	−6	4	−2	0	6	+	−2	−6	
$(16+2\theta)$	+	2	+	2	−	−4	0	8	4	−8	2	−2	10	−12	2	
$(13+7\theta)$	$\mathbb{Q}(\sqrt{5})$															
$(5+11\theta)$	0	−	−2	0	0	−6	6	2	8	2	−6	6	2	8	−10	$+(9+2\theta)$
(12θ)	−	−	−	4	4	−6	−6	−4	−4	−6	2	2	4	4	2	
(12θ)	+	+	+	−4	−4	−6	−6	4	4	−6	2	2	−4	−4	2	
(12θ)	+	+	−	4	−4	2	2	4	−4	10	−6	−6	4	−4	2	
(12θ)	+	−	+	−4	4	2	2	−4	4	10	−6	−6	−4	4	2	
(17)	−1	0	0	0	0	−	−	−4	−4	−6	−6	−6	4	4	2	
$(15+6\theta)$	0	+	−	0	+	6	6	−4	2	2	0	12	−4	2	−10	
$(13+8\theta)$	0	−2	−	+	3	3	−3	−7	2	8	6	12	−1	8	−4	
$(13+8\theta)$	2	2	−	+	−5	3	5	1	−2	−4	6	0	−9	4	12	
$(3+12\theta)$	2	+	−	+	4	0	−4	−2	−8	2	6	6	6	−8	6	

TABLE 3.3.3
Elliptic Curves with small conductor defined over $\mathbb{Q}(\sqrt{-2})$

a_1	a_2	a_3	a_4	a_6	CM(2)?	$\mathfrak{f}$	$N\mathfrak{f}$	Isogenies
θ	$1-\theta$	1	-1	0	√	$(1-2\theta)$	9	
0	0	0	1	0		(4θ)	32	
0	0	0	-1	0		(4θ)	32	
θ	-1	θ	-1	0		(4θ)	32	
θ	-1	0	-2	3		(4θ)	32	
$-\theta$	$-1+\theta$	1	0	0		$(7+\theta)$	51	
$-\theta$	$-1+\theta$	$1-\theta$	$2-\theta$	θ		$(7+\theta)$	51	
$1-\theta$	θ	1	-1	0		$(2+5\theta)$	54	3
1	$1-\theta$	0	$-1-\theta$	-1		$(2+5\theta)$	54	
θ	1	θ	0	0		(6θ)	72	
0	-1	0	1	0		(6θ)	72	
1	0	1	-1	0		(7θ)	98	
$1+\theta$	$1-\theta$	$1+\theta$	-2θ	$-\theta$		$(9+3\theta)$	99	
0	1	0	-1	0		(10)	100	
θ	0	θ	2	0		(10)	100	
1	$-\theta$	θ	$-\theta$	0		$(4+7\theta)$	114	
0	-1	1	0	0		(11)	121	
θ	1	1	$3-3\theta$	$-3-\theta$	√	$(7-6\theta)$	121	
θ	0	θ	0	1		(12)	144	
0	1	0	1	0		(12)	144	
$-\theta$	$1-\theta$	$-\theta$	2	$1-\theta$		$(6+8\theta)$	164	
0	$-1-\theta$	0	$1+2\theta$	$2-\theta$		$(6+8\theta)$	164	
$1-\theta$	$-1-\theta$	$1-\theta$	$-1+\theta$	$1+\theta$		$(4+9\theta)$	178	
1	θ	1	-1	0		$(12+5\theta)$	194	
1	$1-\theta$	$-\theta$	$2+\theta$	$2-2\theta$		$(10+7\theta)$	198	3
$1-\theta$	θ	$1-\theta$	$1+3\theta$	$2+2\theta$		$(10+7\theta)$	198	
0	0	0	-2	1		(10θ)	200	
θ	-1	θ	0	2		(10θ)	200	
θ	θ	$1+\theta$	θ	0		$(11+7\theta)$	219	
1	1	1	0	0		(15)	225	
$1-\theta$	0	$1-\theta$	$-\theta$	θ		$(2+11\theta)$	246	
1	$-1+\theta$	1	$-1+\theta$	$-2-\theta$		$(7+10\theta)$	249	
0	θ	0	1	θ	√	(16)	256	
0	$-\theta$	0	1	$-\theta$	√	(16)	256	
0	-1	0	-2	2		(16)	256	
0	-1	0	1	-1		(16)	256	
0	1	0	-2	-2		(16)	256	
0	1	0	1	1		(16)	256	
$1-\theta$	$-\theta$	$-\theta$	1	$-1-\theta$		$(16+\theta)$	258	
$-\theta$	1	$-\theta$	$-1-2\theta$	$-1-2\theta$		$(16+2\theta)$	264	
$-\theta$	0	$1-\theta$	$-\theta$	$-1-2\theta$		$(5+11\theta)$	267	
0	1	0	-2	0		(12θ)	288	
θ	0	0	2	-1		(12θ)	288	
0	-1	0	-2	0		(12θ)	288	
0	θ	0	1	3θ		(12θ)	288	
0	$-\theta$	0	1	-3θ		(12θ)	288	
1	-1	1	-1	0		(17)	289	
θ	$1-\theta$	$1+\theta$	$-1-\theta$	1		$(15+6\theta)$	297	
$-\theta$	$1-\theta$	$1-\theta$	$1+2\theta$	0		$(15+6\theta)$	297	
0	$-1+\theta$	1	$1-\theta$	θ		$(13+8\theta)$	297	
0	$1-\theta$	1	$2-2\theta$	1		$(13+8\theta)$	297	

TABLE 3.4.1
Ideals $\mathfrak{a}$ of $\mathbf{Z}[\frac{1}{2}(1+\sqrt{-3})]$ with $\dim V(\mathfrak{a})>0$ and $N\mathfrak{a}\leqslant 500$ ($\rho=\frac{1}{2}(1+\sqrt{-3})$).

$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	+	−	$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	+	−	$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	+	−
(7)	49	1		**1**	$(14+2\rho)$	228	1	**1**		$(15+7\rho)$	379	1	**1**	
$(8+\rho)$	73	1	**1**		$(15+\rho)$	241	2	**1**	**1**	$(17+5\rho)$	399	1	**1**	
$(5+5\rho)$	75	1	**1**		$(16+\rho)$	273	1	**1**		$(13+10\rho)$	399	2		**1**+**1**
(10)	100	1		**1**	$(11+8\rho)$	273	1	**1**		(20)	400	3	**1**	2
(11)	121	2	**1**	**1**	$(13+6\rho)$	283	1	**1**		$(18+4\rho)$	412	1	**1**	
$(10+2\rho)$	124	2	**1**	**1**	(17)	289	2	**1**	**1**	$(16+7\rho)$	417	2	**1**	**1**
$(7+7\rho)$	147	3	**1**	2	$(16+2\rho)$	292	2	2		$(18+5\rho)$	439	1		**1**
(13)	169	1		**1**	$(10+10\rho)$	300	5	**1**+2	2	(21)	441	7	**1**+2	**1**+3
$(9+6\rho)$	171	2	**1**	**1**	(18)	324	2	**1**	**1**	$(13+12\rho)$	469	2		**2**
$(8+8\rho)$	192	1	**1**		$(15+5\rho)$	325	1		**1**	$(15+10\rho)$	475	2	**1**	**1**
(14)	196	3	**1**	2	$(14+7\rho)$	343	3	**1**	2	$(16+9\rho)$	481	3	**1**	**2**
$(11+5\rho)$	201	1		**1**	(19)	361	3	**1**	**2**	(22)	484	5	2	**1**+2
$(10+7\rho)$	219	2	2		$(11+11\rho)$	363	5	**1**+2	2	$(17+8\rho)$	489	1		**1**
(15)	225	3	2	**1**	$(14+8\rho)$	372	4	2	2	$(20+4\rho)$	496	4	2	2

TABLE 3.4.2
$\mathbb{Q}(\sqrt{-3})$: Newforms in $V^{+}(\mathfrak{a})$

$\mathfrak{a}$	$1+\rho$	2	$1+2\rho$	$2+\rho$	$3+\rho$	$1+3\rho$	$3+2\rho$	$2+3\rho$	5	$5+\rho$	$1+5\rho$	$3+4\rho$	$4+3\rho$	$1+6\rho$	$6+\rho$	Other W
$(8+\rho)$	-2	-1	2	-4	2	2	2	2	2	-4	-10	2	2	2	-4	$-(8+\rho)$
$(5+5\rho)$	$+$	-3	0	0	-2	-2	4	4	$-$	0	0	-10	-10	4	4	
(11)	-1	0	-2	-2	4	4	0	0	-9	7	7	3	3	-6	-6	$-(11)$
$(10+2\rho)$	-1	$+$	-2	3	-1	-6	0	5	1	$-$	7	3	-2	4	-6	
$(7+7\rho)$	$-$	-3	$+$	$+$	-2	-2	4	4	-6	0	0	6	6	-4	-4	
$(9+6\rho)$	$+$	-1	-4	2	-4	2	$-$	2	-4	2	8	2	2	8	-4	
$(8+8\rho)$	$+$	$-$	0	0	-2	-2	-4	-4	-6	8	8	6	6	4	4	
(14)	-2	$-$	$-$	$-$	-4	-4	2	2	-10	-4	-4	2	2	8	8	
$(14+2\rho)$	$-$	$+$	-2	-2	-6	4	0	$+$	6	-8	2	-2	8	4	4	
$(15+\rho)$	0	1	0	-4	-2	6	-4	0	10	0	4	-2	6	-8	-4	$-(15+\rho)$
$(16+\rho)$	$+$	1	0	$+$	$-$	-2	4	-4	-6	-8	0	6	6	12	-4	
$(11+8\rho)$	$-$	-1	$-$	-4	$-$	2	-4	-4	2	8	-4	-10	2	8	8	
$(13+6\rho)$	-3	-3	-2	-3	0	-2	5	-4	-4	-1	-7	-3	4	4	-8	$+(13+6\rho)$
(17)	0	-3	4	4	-2	-2	-4	-4	-6	4	4	-2	-2	4	4	$-(17)$
$(10+10\rho)$	$-$	$-$	-4	-4	2	2	-4	-4	$-$	8	8	2	2	-4	-4	
(18)	$+$	$-$	-1	-1	-4	-4	2	2	-1	5	5	2	2	-10	-10	
$(14+7\rho)$	0	1	$+$	$-$	-2	2	4	-4	2	4	-4	-2	-2	4	4	
(19)	-2	-4	-1	-1	-4	-4	$-$	$-$	-1	-4	-4	2	2	-1	-1	
$(11+11\rho)$	$+$	-3	4	4	-2	-2	0	0	-6	-8	-8	6	6	0	0	$-(11)$
$(15+7\rho)$	-2	-3	-5	-1	4	1	-2	-7	1	2	0	-8	-8	1	-4	$+(15+7\rho)$
$(17+5\rho)$	$+$	1	0	$-$	-2	-2	$+$	4	2	0	0	-2	-10	-12	4	
(20)	-2	$+$	2	2	2	2	-4	-4	$-$	-4	-4	2	2	-10	-10	
$(18+4\rho)$	-3	$+$	-3	-4	1	-5	1	0	-2	2	-2	1	-4	-11	12	$+(9+2\rho)$
$(16+7\rho)$	$-$	-2	1	1	0	0	-8	-1	-2	4	4	10	-4	-12	-5	$+(3+10\rho)$
(21)	$-$	-1	$-$	$-$	2	2	-4	-4	2	-4	-4	2	2	-4	-4	
$(15+10\rho)$	0	1	4	-4	6	-2	$+$	-4	$-$	0	0	-10	-2	8	0	
$(16+9\rho)$	-2	-3	-2	0	-6	$+$	0	-4	-2	-2	10	$+$	10	-6	0	

TABLE 3.4.3
Elliptic curves with small conductor defined over $\mathbb{Q}(\sqrt{-3})$

a_1	a_2	a_3	a_4	a_6	$CM(3)$?	$\mathfrak{f}$	$N\mathfrak{f}$	Isogenies
0	$1+\rho$	ρ	ρ	0	√	$(3+5\rho)$	49	
1	$1+\rho$	0	ρ	0		$(8+\rho)$	73	
$-1+\rho$	$-\rho$	1	0	0		$(5+5\rho)$	75	
0	0	1	0	0	√	(9)	81	
0	-1	1	0	0		(11)	121	
$-\rho$	$-1+\rho$	$1-\rho$	0	0		$(10+2\rho)$	124	
0	0	0	0	1	√	(12)	144	
$-1+\rho$	0	0	$-1+\rho$	0		$(7+7\rho)$	147	
ρ	0	0	4ρ	-1		$(7+7\rho)$	147	
$-1+\rho$	ρ	ρ	ρ	0		$(9+6\rho)$	171	
0	ρ	0	$-1+\rho$	0		$(8+8\rho)$	192	
ρ	0	1	0	0		(14)	196	
$-1+\rho$	$1+\rho$	1	0	$-\rho$		$(14+2\rho)$	228	
$-1+\rho$	$1-\rho$	ρ	0	0		$(15+\rho)$	241	
0	$2-\rho$	0	$1-\rho$	0	√	(16)	256	
0	$1+\rho$	0	ρ	0	√	(16)	256	
$-1+\rho$	1	$-1+\rho$	0	0		$(16+\rho)$	273	
1	$1+\rho$	1	$-1+\rho$	-1		$(11+8\rho)$	273	
$-\rho$	$1+\rho$	$1-\rho$	$5-3\rho$	-2ρ		$(11+8\rho)$	273	
ρ	ρ	ρ	0	0		$(13+6\rho)$	283	
ρ	$1-\rho$	1	0	0		(17)	289	
1	0	1	1	2		$(10+10\rho)$	300	
$-1+\rho$	ρ	1	$-1+\rho$	-1		(18)	324	3
ρ	$1-\rho$	0	3ρ	3		(18)	324	
0	$-\rho$	1	$-1+\rho$	0		(19)	361	
1	1	0	-11	0		$(11+11\rho)$	363	
$-\rho$	$1+\rho$	1	ρ	0		$(15+7\rho)$	379	
$1-\rho$	$-1+\rho$	$1-\rho$	$-4+2\rho$	$-2+\rho$		$(15+5\rho)$	399	
0	$-1+\rho$	0	ρ	0		(20)	400	
ρ	$1-\rho$	ρ	0	0		$(18+4\rho)$	412	
0	$-\rho$	$-\rho$	-2ρ	$-1+\rho$		$(16+7\rho)$	417	
$-\rho$	ρ	$-\rho$	$-2+2\rho$	$-1+\rho$		$(15+10\rho)$	475	
$-\rho$	$1+\rho$	0	ρ	0		$(16+9\rho)$	481	

TABLE 3.5.1
Ideals $\mathfrak{a}$ of $\mathbf{Z}[\frac{1}{2}(1+\sqrt{-7})]$ with dim $V(\mathfrak{a}) > 0$ and $N\mathfrak{a} \leqslant 200$

$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	$+$	$-$	$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	$+$	$-$	$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	$+$	$-$
(5)	25	1		**1**	$(6+4\alpha)$	92	2	2		$(7+6\alpha)$	163	1		**1**
$(2-4\alpha)$	28	1	**1**		(10)	100	5		**1**+4	(13)	169	5		**2+3**
(6)	36	1		**1**	$(5+5\alpha)$	100	3		3	$(11+3\alpha)$	172	2	2	
$(2+4\alpha)$	44	1	**1**		$(8+3\alpha)$	106	1		**1**	$(10+4\alpha)$	172	4	2+2	
$(-1+5\alpha)$	46	1	**1**		$(4+6\alpha)$	112	4	3	**1**	$(1+9\alpha)$	172	2	2	
(5α)	50	2		2	$(-4+8\alpha)$	112	4	4		$(5-10\alpha)$	175	5	**1+2**	2
$(6+2\alpha)$	56	2	2		$(2+7\alpha)$	116	1		**1**	$(12+2\alpha)$	176	8	3+2+2	**1**
$(3-6\alpha)$	63	1	**1**		$(2-8\alpha)$	116	1		**1**	$(9+5\alpha)$	176	3	2	**1**
(8)	64	1		**1**	(11)	121	3	**1**	**2**	$(6+7\alpha)$	176	3	2	**1**
(6α)	72	2		2	$(9+3\alpha)$	126	2		2	$(4+8\alpha)$	176	6	4+2	
$(1+6\alpha)$	79	1		**1**	(8α)	128	3	**1**	2	$(4-10\alpha)$	176	5	3+2	
$(4+5\alpha)$	86	1	**1**		(12)	144	5		**1**+4	$(8+6\alpha)$	184	4	3	**1**
$(3-7\alpha)$	86	1	**1**		$(6+6\alpha)$	144	4		**1**+3	$(2+9\alpha)$	184	3	3	
$(8+2\alpha)$	88	2	2		$(8+5\alpha)$	154	1		**1**	$(2-10\alpha)$	184	6	**1**+2+2	**1**
$(7+3\alpha)$	88	1	**1**		$(1-9\alpha)$	154	1		**1**	(14)	196	5	**1**+2	2
$(2+6\alpha)$	88	3	**1**+2		$(12+\alpha)$	158	3	**1**	2	$(3+9\alpha)$	198	1		**1**
$(2-7\alpha)$	88	1	**1**		$(5+7\alpha)$	158	2		2	$(10+5\alpha)$	200	5	**1**	4
$(9+\alpha)$	92	2	2		$(3+8\alpha)$	161	1	**1**		(10α)	200	8		6+2

TABLE 3.5.2
$\mathbb{Q}(\sqrt{-7})$: Newforms in $V^{+}(\mathfrak{a})$

$\mathfrak{a}$	α	$1-\alpha$	$1-2\alpha$	3	$1+2\alpha$	$3-2\alpha$	$3+2\alpha$	$5-2\alpha$	5	$-1+4\alpha$	$3-4\alpha$	$1+4\alpha$	$5-4\alpha$	$5+2\alpha$	$7-2\alpha$	Other W
$(2-4\alpha)$	+	+	−	−2	0	0	0	0	−10	−6	−6	2	2	8	8	
$(2+4\alpha)$	+	−	−4	−2	+	0	0	0	2	6	6	2	−10	−4	−4	
$(1-5\alpha)$	−1	−	0	2	−4	−4	−8	+	2	6	−2	−2	6	4	−4	
$(3-6\alpha)$	−1	−1	+	−	4	0	0	−6	−2	−2	6	6	−4	−4		
$(4+5\alpha)$	+	0	−1	4	3	3	−6	−3	−1	6	−6	−7	−7	8	−	
$(3-7\alpha)$	1	−	−4	2	−4	4	0	0	−2	−6	−2	6	−2	0	+	
$(7+3\alpha)$	1	−	4	−2	+	0	−8	0	−6	6	−2	2	−2	4	−4	
$(2+6\alpha)$	+	−	2	4	−6	+	0	0	2	6	−6	2	−4	−4	−4	
$(2-7\alpha)$	−	−1	0	2	+	4	8	0	−6	−2	−10	6	−2	−4	4	
(11)	−2	−2	−2	−5	−	−	−1	−1	−9	0	0	3	3	−6	−6	
(8α)	+	−	0	2	−4	4	0	0	2	−2	−2	−10	−10	4	−4	
$(12+\alpha)$	+	−2	−1	−1	−6	−3	1	−8	−3	3	−4	10	4	2	−8	$+(7-6\alpha)$
$(3+8\alpha)$	0	0	−	4	−3	6	3	+	−1	−6	3	−7	2	−1	8	
$(5-10\alpha)$	0	0	−	−5	−3	−3	−6	−6	−	3	3	2	2	−10	−10	
$(5-10\alpha)$	$\mathbb{Q}(\sqrt{17})$															
$(2-10\alpha)$	+	−	−4	4	6	0	0	+	−4	6	0	2	2	−4	8	
(14)	−	−	−	−4	−2	−2	−4	−4	−2	2	2	10	10	2	2	
$(10+5\alpha)$	+	−2	−4	−1	−3	−1	−8	−4	+	9	−3	4	−8	−6	2	

TABLE 3.5.3
Elliptic Curves with small conductor defined over $\mathbb{Q}(\sqrt{-7})$

a_1	a_2	a_3	a_4	a_6	$CM(7)$?	$\mathfrak{f}$	$N\mathfrak{f}$	Isogenies
α	$2-\alpha$	α	$2-2\alpha$	$1-\alpha$	√	$(2-3\alpha)$	16	
1	0	1	-1	0		$(2-4\alpha)$	28	
1	α	$-1+\alpha$	1	α		$(2-4\alpha)$	28	
1	$1-\alpha$	0	1	1		$(2+4\alpha)$	44	
1	1	$-\alpha$	$2-\alpha$	$2-\alpha$		$(2+4\alpha)$	44	
1	$-\alpha$	$-\alpha$	$-2+\alpha$	1		$(1-5\alpha)$	46	
0	$-1+\alpha$	$-1+\alpha$	0	0		$(1-5\alpha)$	46	
1	-1	0	-2	-1	√	(7)	49	
1	$1-\alpha$	$-1+\alpha$	α	0		$(3-6\alpha)$	63	
1	0	0	1	0		$(3-6\alpha)$	63	
$-1+\alpha$	$2-\alpha$	1	-1	0		$(4+5\alpha)$	86	
1	$2-\alpha$	1	$-\alpha$	-1		$(3-7\alpha)$	86	
1	$1+\alpha$	0	$2+\alpha$	1		$(3-7\alpha)$	86	
1	$-\alpha$	1	$-1-2\alpha$	$-3+2\alpha$		$(3-7\alpha)$	86	
$-1+\alpha$	α	$-1+\alpha$	α	1		$(7+3\alpha)$	88	
$1-\alpha$	0	$1-\alpha$	$-1+\alpha$	α		$(2+6\alpha)$	88	
$-1+\alpha$	$-1+\alpha$	0	$-3+2\alpha$	$-1+\alpha$		$(2+6\alpha)$	88	
$-\alpha$	$-1+\alpha$	0	1	0		$(2-7\alpha)$	88	
$-\alpha$	α	$-\alpha$	$-\alpha$	$1-\alpha$		$(2-7\alpha)$	88	
0	-1	1	0	0		(11)	121	
0	$1-\alpha$	0	$-2+\alpha$	0		(8α)	128	
0	$-\alpha$	0	$-1-\alpha$	0		(8α)	128	
0	$-1+\alpha$	0	$-4+2\alpha$	$-2+\alpha$		(8α)	128	
0	α	0	$-2-\alpha$	$1+\alpha$		(8α)	128	
$1-\alpha$	$-\alpha$	1	$-1+\alpha$	0		$(12+\alpha)$	158	
0	$2-\alpha$	1	$-\alpha$	-1		$(3+8\alpha)$	161	
0	1	1	-1	0		$(5-10\alpha)$	175	
$1-\alpha$	$2-\alpha$	$1-\alpha$	$2-\alpha$	$-\alpha$		$(2-10\alpha)$	184	
$1-\alpha$	α	$1-\alpha$	2	0		$(2-10\alpha)$	184	
0	$1-\alpha$	$-\alpha$	-1	0		$(10+5\alpha)$	200	

TABLE 3.6.1
Ideals $\mathfrak{a}$ of $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-11})]$ with $\dim V(\mathfrak{a})>0$ and $N\mathfrak{a} \leqslant 200$

$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	$+$	$-$	$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	$+$	$-$	$\mathfrak{a}$	$N\mathfrak{a}$	$r(\mathfrak{a})$	$+$	$-$
(3)	9	1		$\mathbf{1}$	(5α)	75	2		2	$(3+6\alpha)$	135	8	$\mathbf{1}+2$	$\mathbf{1}+4$
$(1-2\alpha)$	11	1	$\mathbf{1}$		(9)	81	9	$2+2$	$\mathbf{1}+4$	$(6+5\alpha)$	141	3	2	$\mathbf{1}$
(5)	25	1		$\mathbf{1}$	$(6+3\alpha)$	81	5	2	3	$(1-7\alpha)$	141	2	2	
(3α)	27	3	$\mathbf{1}$	2	$(2+5\alpha)$	89	2	$\mathbf{1}$	$\mathbf{1}$	(12)	144	5		$2+3$
$(5+\alpha)$	33	2	2		$(8+2\alpha)$	92	1	$\mathbf{1}$		(7α)	147	6		$3+3$
(6)	36	3		$\mathbf{1}+2$	$(3+5\alpha)$	99	6	$\mathbf{1}+3$	$\mathbf{1}+\mathbf{1}$	$(9+4\alpha)$	165	5	4	$\mathbf{1}$
$(2-4\alpha)$	44	2	2		$(3-6\alpha)$	99	7	$\mathbf{1}+4$	2	$(2+7\alpha)$	165	8	$\mathbf{1}+\mathbf{2}+4$	$\mathbf{1}$
$(3+3\alpha)$	45	2		2	(10)	100	5		$\mathbf{1}+\mathbf{1}+\mathbf{1}+2$	(13)	169	5		$\mathbf{5}$
$(5+2\alpha)$	47	1	$\mathbf{1}$		$(6+4\alpha)$	108	4	$\mathbf{1}+\mathbf{1}$	$\mathbf{1}+\mathbf{1}$	$(4-8\alpha)$	176	4	$\mathbf{1}+3$	
(7)	49	3		$\mathbf{3}$	(6α)	108	9	$\mathbf{1}+2$	$2+4$	$(3+7\alpha)$	177	1	$\mathbf{1}$	
$(4+3\alpha)$	55	2	2		$(9+2\alpha)$	111	4	$\mathbf{2}$	$\mathbf{2}$	$(6+6\alpha)$	180	7	$\mathbf{1}$	$2+4$
(8)	64	1		$\mathbf{1}$	(11)	121	5	$\mathbf{1}+2$	$\mathbf{1}+\mathbf{1}$	$(1-8\alpha)$	185	3	$\mathbf{3}$	
$(2-5\alpha)$	69	2		$\mathbf{1}+\mathbf{1}$	$(5+5\alpha)$	125	3		$\mathbf{1}+2$	$(10+4\alpha)$	188	2	2	
$(1-5\alpha)$	71	2		$\mathbf{2}$	$(10+2\alpha)$	132	4	4		(8α)	192	2		2
$(7+2\alpha)$	75	2		2	$(9+3\alpha)$	135	6	2	4	(14)	196	9	$\mathbf{1}$	$\mathbf{2}+3+3$

TABLE 3.6.2
$\mathbb{Q}(\sqrt{-11})$: Newforms in $V^{+}(\mathfrak{a})$

$\mathfrak{a}$	2	α	$1-\alpha$	$1+\alpha$	$2-\alpha$	$-1+2\alpha$	$4+\alpha$	$5-\alpha$	$1+3\alpha$	$4-3\alpha$	$2+3\alpha$	$5-3\alpha$	$5+2\alpha$	$7-2\alpha$	7	Other W
$(1-2\alpha)$	0	−1	−1	1	1	−	−1	−1	7	7	3	3	8	8	−10	
(3α)	1	−	+	−2	2	0	4	−4	0	0	−2	−2	8	−8	−6	
$(5+2\alpha)$	0	1	−3	−3	−1	−4	−3	3	5	−5	7	7	+	0	2	
$(2+5\alpha)$	−1	0	2	2	2	−4	0	6	4	−2	−6	2	−8	12	10	$-(2+5\alpha)$
$(8+2\alpha)$	−	−2	1	0	3	3	+	0	−4	5	−7	2	−6	3	5	
$(3+5\alpha)$	3	+	2	−2	−2	−	−4	8	−2	4	−12	0	−4	2	8	
$(3-6\alpha)$	−3	+	+	−2	−2	−	8	8	−8	−8	6	6	8	8	2	
$(6+4\alpha)$	−	−	−2	0	−3	−3	−6	−6	5	−4	−7	−7	0	3	−4	
$(6+4\alpha)$	−	+	1	0	3	−6	3	0	−4	5	2	11	−6	−6	−4	
(6α)	−	−	−	0	0	0	−6	6	−4	−4	2	2	6	−6	14	
$(9+2\alpha)$	$\mathbb{Q}(\sqrt{5})$															
(11)	−3	2	2	1	1	−	2	2	−2	−2	−3	−3	2	2	−10	
$(3+6\alpha)$	−1	−	+	0	+	6	6	6	−4	8	−10	2	0	0	2	
$(2+7\alpha)$	3	−2	+	−	4	+	0	−6	−4	0	−2	−8	−12	4	0	
$(2+7\alpha)$	$\mathbb{Q}(\sqrt{5})$															
$(4-8\alpha)$	+	1	1	−3	−3	+	−3	−3	5	5	−1	−1	0	0	−10	
$(3+7\alpha)$	−2	−	0	−3	0	2	−5	−7	−3	4	−8	−6	2	8	−5	$-(8-\alpha)$
$(6+6\alpha)$	−	+	+	+	2	4	−4	4	−8	8	−2	−2	4	12	2	
$(1-8\alpha)$	$\mathbb{Q}(x^3-4x-2)$															
(14)	−	−2	−2	0	0	0	0	0	−4	−4	2	2	−12	−12	−	

TABLE 3.6.3
Elliptic Curves with small conductor defined over $\mathbb{Q}(\sqrt{-11})$

a_1	a_2	a_3	a_4	a_6	$\mathfrak{f}$	$N\mathfrak{f}$	Isogenies
0	-1	1	0	0	$(1-2\alpha)$	11	
$-\alpha$	α	$1-\alpha$	$-\alpha$	$2-\alpha$	(3α)	27	
0	$1-\alpha$	1	-1	0	$(5+2\alpha)$	47	
$-\alpha$	α	0	-1	0	$(2+5\alpha)$	89	
$1-\alpha$	α	1	-1	0	$(8+2\alpha)$	92	
1	$2-\alpha$	0	-2α	-1	$(3+5\alpha)$	99	
1	1	0	-11	0	$(3-6\alpha)$	99	
$-\alpha$	0	1	α	0	$(6+4\alpha)$	108	3
1	$-1+\alpha$	α	$-\alpha$	1	$(6+4\alpha)$	108	
$1-\alpha$	$2-\alpha$	1	1	0	$(6+4\alpha)$	108	
1	1	0	-2	-7	(11)	121	
α	$1+\alpha$	α	α	0	$(3+6\alpha)$	135	
0	1	0	3	-1	$(4-8\alpha)$	176	
0	$1-\alpha$	α	α	0	$(3+7\alpha)$	177	
1	0	1	-1	0	(14)	196	

It will be noticed that, although in the majority of cases we were able to find a curve with conductor $\mathfrak{a}$ to correspond to each rational newform in $V(\mathfrak{a})$, there are a few values of $\mathfrak{a}$ for which no such curve was found. However, the search region was really very small. Also, there is some precedent for this situation in the rational case: for some conductors, for example 78, no curves were found by any systematic search. We list these "missing conductors" in the following table.

Missing Conductors

	$\mathbb{Q}(\sqrt{-1})$	$(17+11i)$, $(19+8i)$
	$\mathbb{Q}(\sqrt{-2})$	$(6+6\theta)$, $(5+10\theta)$, $(12+7\theta)$, $(3+12\theta)$
	$\mathbb{Q}(\sqrt{-3})$	$(14+7\rho)$, (21)
	$\mathbb{Q}(\sqrt{-7})$	(14)
	$\mathbb{Q}(\sqrt{-11})$	(6α), $(2+7\alpha)$, $(6+6\alpha)$

In [8] and [9], Mennicke and Grunewald also discuss the question of a correspondence between elliptic curves with conductor $\mathfrak{a}$ and one-dimensional rational eigenspaces in $V(\mathfrak{a})$. Their computations of newforms at level $\mathfrak{p}$, where $\mathfrak{p}$ is a prime of degree 1, give some support for the Main Conjecture. They also remark that, as in part (iv) of the Conjecture, one would not expect a cusp form to correspond to an elliptic curve with complex multiplication by the ground field K. According to [6] it can be proved that the curves with complex multiplication in K itself correspond to cohomology classes in $H^1(\Gamma_0(\mathfrak{a}), \mathbb{Q})/H^1\ \mathrm{cusp}(\Gamma_0(\mathfrak{a}), \mathbb{Q})$: that is, to non-cuspidal automorphic forms for $\Gamma_0(\mathfrak{a})$. They also suggest that in certain cases a newform may exist in $V^+(\mathfrak{a})$ for some ideal $\mathfrak{a}$ without a corresponding curve with conductor $\mathfrak{a}$. [3] Of course, it would be highly desirable to have a procedure for constructing an elliptic curve directly from a newform, as Tingley did [21] in the rational case by means of calculating the periods of the differential $2\pi i f(z)dz$, where $f(z)$ is a newform. Efforts in this direction have so far been unsuccessful. In the rational case the quotient of the upper half-plane by $\Gamma_0(N)$ has, as well as a complex structure, an algebraic structure as an algebraic curve $X_0(N)$. Elliptic curves then arise as one-dimensional factors of the Jacobian variety $J_0(N)$. By contrast we have no complex or algebraic structure on $\Gamma_0(\mathfrak{a})\backslash \mathrm{H}_3^*$ by means of which to generalize this construction.

4. Twisting

According to the Main Conjecture it is only the newforms in $V^+(\mathfrak{a})$ which are related to elliptic curves. However the V^+ and V^- spaces are linked by certain "twisting" operators, which in fact provide a one-one correspondence between the newforms in V^+ and those in V^-, not necessarily at the same level. In the case of $\mathbb{Q}(i)$, for example, if the related levels are $\mathfrak{a}_1$ and $\mathfrak{a}_2$ then *either* $\mathfrak{a}_1 = \mathfrak{a}_2 \cap (1+i)^4$ *or* $\mathfrak{a}_2 = \mathfrak{a}_1 \cap (1+i)^4$. (Recall that intersecting ideals gives their least common multiple.)

To make this correspondence clearer, we give some examples. There is a newform in $V^+((6+6i))$ which grows into two oldforms in $V^+((12))$; in $V^-((12))$ there is a newform also. These two newforms have the same eigenvalue for T_π if $\pi \equiv 1$ (modulo 2), and hence eigenvalues of opposite sign for T_π if $\pi \equiv i$ (modulo 2) by (2.2.9). Note that $(12) = (6+6i) \cap (1+i)^4$. In the other direction, there is a newform in $V^-((8+2i))$, which grows into two oldforms in $V^-((10+6i))$ and three oldforms in $V^-((16+4i))$. Now $(16+4i) = (8+2i) \cap (1+i)^4$, and there is a newform in $V^+(16+4i))$ whose eigenvalues correspond as before.

One other example: in [8] Mennicke observed that there is a newform in $V^-((11+4i))$, but (apparently) no elliptic curve with conductor $(11+4i)$. Having calculated $V^\pm(\mathfrak{a})$ for $\mathfrak{a} = (11+4i)$, $(11+4i)(1+i)$, $(11+4i)(1+i)^2$, $(11+4i)(1+i)^3$ and $(11+4i)(1+i)^4$, we eventually find, as well as five oldforms in $V^-((11+4i)(1+i)^4)$, a newform in $V^+((11+4i)(1+i)^4)$, as predicted. Moreover there is an elliptic curve with conductor $(11+4i)(1+i)^4$, which Mennicke had found, whose Traces of Frobenius correspond as in the Main Conjecture.

Precisely, we have the following result.

THEOREM 4: *Let* $\mathfrak{a}$ *be an ideal of* $\mathbb{Z}[i]$ *such that* $(1+i)^4$ *divides* $\mathfrak{a}$. *Then there is a map* R_2: $V(\mathfrak{a}) \to V(\mathfrak{a})$ *such that*

(i) $R_2 J = -J R_2$;

[3] See end of paper.

(ii) $R_2 T_\pi = (\pi/2) T_\pi R_2$ *if* π *is prime*;
(iii) $R_2 W_\pi = (\pi/2)^e W_\pi R_2$ *if* π *is a prime dividing* $\mathfrak{a}$ *to the power* e, $(\pi) \neq (1+i)$.

Here $(\pi/2)$ denotes the quadratic residue symbol modulo (2): it is $+1$ if $\pi \equiv 1$ (modulo 2) and -1 if $\pi \equiv \mathrm{i}$ (modulo 2). It follows from (i) that R_2 maps $V^+(\mathfrak{a})$ into $V^-(\mathfrak{a})$ and vice versa. Then from (ii) and (iii) it follows that R_2 preserves the eigenvalues of T_π and W_π provided that $\pi \equiv 1$ (modulo 2). Note that every nonzero prime ideal of $\mathbb{Z}[i]$ has four generators, of which two are congruent to 1 and two congruent to i (modulo 2). So we can always choose a generator in such a way that R_2 preserves eigenvalues.

This Theorem is a special case of a more general result proved below (see Corollary 4.2.5) which is applicable to any complex quadratic field. For any quadratic character χ of $\mathfrak{o}$ modulo an ideal $\mathfrak{q}$ we will define an operator R_χ which will act on $V(\mathfrak{a})$ provided that $\mathfrak{q}^2$ divides $\mathfrak{a}$. For suitable χ the operator R_χ will interchange $V^+(\mathfrak{a})$ and $V^-(\mathfrak{a})$.

4.1. Quadratic characters

By a quadratic character χ of $\mathfrak{o}_K$ we mean an arithmetic character of order 2 defined modulo an ideal $\mathfrak{q}$ of $\mathfrak{o}$. That is, χ is a surjective homomorphism from the multiplicative group $(\mathfrak{o}/\mathfrak{q})^\times$ to $\{\pm 1\}$, extended to elements of $\mathfrak{o}$ relatively prime to $\mathfrak{q}$ in the obvious way, and finally extended to the whole of $\mathfrak{o}$ by defining $\chi(x) = 0$ for x in $\mathfrak{o}$ not relatively prime to $\mathfrak{q}$.

For each odd prime $\mathfrak{p}$ of $\mathfrak{o}$ (that is, each prime not containing 2) there is a unique quadratic character modulo $\mathfrak{p}$ given by the quadratic residue symbol $x \mapsto (x/\mathfrak{p})$. Indeed, it is easy to see that these are the only primitive characters modulo prime powers. (A character modulo $\mathfrak{q}$ is *primitive* if it is not induced from a character modulo any proper divisor of $\mathfrak{q}$.) The situation modulo powers of even primes is more complicated. For the present purposes we will be particularly interested in *odd* quadratic characters: that is, those χ such that $\chi(\varepsilon) = -1$, where ε as usual denotes the fundamental unit of K. Hence we will limit the discussion to a determination of the simplest such character in each complex quadratic field.

First we deal with the two fields with $\varepsilon \neq -1$.

Case 1: $K = \mathbb{Q}(\sqrt{-1})$. Here (2) ramifies: $(2) = (1+i)^2$. Clearly $(\mathfrak{o}/(1+i))^\times$ is the trivial group, but $(\mathfrak{o}/(1+i)^2)^\times$ is cyclic of order 2, generated by i. So we have an odd character χ_1 defined modulo (2) by:

$$\chi_1(x) = \begin{cases} +1 & \text{if } x \equiv 1 \pmod 2, \\ -1 & \text{if } x \equiv i \pmod 2, \\ 0 & \text{otherwise.} \end{cases}$$

Case 2: $K = \mathbb{Q}(\sqrt{-3})$. Here (2) is prime and $(\mathfrak{o}/(2))^{\times}$ is thus cyclic of order 3 with no quadratic characters. However $(\mathfrak{o}/(2)^2)^{\times} = \langle \rho \rangle \times \langle 1 + 2\rho \rangle$ where $\rho = \frac{1}{2}(1 + \sqrt{-3})$ has order 6 and $1 + 2\rho$ has order 2; there are thus three quadratic characters modulo 4. One, χ_ρ, has kernel $\langle \rho \rangle$ (this is, in fact, the character $x \mapsto (\rho/x)$). The others are both odd: $\chi_3^{(1)}$ has kernel $\langle \rho^2 \rangle \times \langle 1 + 2\rho \rangle$ and $\chi_3^{(2)} = \chi_\rho \chi_3^{(1)}$.

In all other fields $\varepsilon = -1$ and we seek a character χ such that $\chi(-1) = -1$. There will be such a character modulo $\mathfrak{a}$ provided that -1 is not a square modulo $\mathfrak{a}$; so for instance if $\mathfrak{p}$ is an odd prime with $N\mathfrak{p} \equiv 3 \pmod 4$ then $x \mapsto (x/\mathfrak{p})$ is an odd character modulo $\mathfrak{p}$. Modulo powers of even primes we continue to proceed case by case.

Recall our terminology: $K = \mathbb{Q}(\sqrt{-d})$ with d squarefree, and from now on $d \neq 1$, $d \neq 3$.

Case 3: $d \equiv 3 \pmod 8$. Here (2) remains prime and the situation is exactly as in the case $d = 3$. There are no quadratic characters modulo (2) but three modulo (4), of which two are odd: $(\mathfrak{o}/(4))^{\times} \cong C_3 \times C_2 \times C_2$ with three elements of order 2, namely -1, $\sqrt{-d}$ and $2 + \sqrt{-d}$.

Case 4: $d \equiv 7 \pmod 8$. Now (2) splits as $\mathfrak{p}_2 \bar{\mathfrak{p}}_2$ and $\mathfrak{o}/\mathfrak{p}_2^k \cong \mathbb{Z}/(2)^k \cong \mathfrak{o}/\bar{\mathfrak{p}}_2^k$. Hence there are two odd characters $\chi_d^{(1)}$ and $\chi_d^{(2)}$ modulo $\mathfrak{p}_2^2$ and $\bar{\mathfrak{p}}_2^2$ respectively. Explicitly, $\mathfrak{p}_2 = (2, \alpha)$ and $\mathfrak{p}_2^2 = (4, 2\alpha, \alpha - n)$ with $n = (1 + d)/4$, so $\alpha \equiv n \pmod{\mathfrak{p}_2^2}$. Therefore $\chi_d^{(1)}$ is given by

$$\chi_d^{(1)}(x + y\alpha) = \begin{cases} +1 & \text{if } x + yn \equiv 1 \pmod 4, \\ -1 & \text{if } x + yn \equiv -1 \pmod 4, \\ 0 & \text{otherwise.} \end{cases}$$

Case 5: $d \equiv 2 \pmod 4$. Here (2) is ramified: $(2) = \mathfrak{p}^2$ with $\mathfrak{p} = (2, \alpha)$. Modulo $\mathfrak{p}^3$ we have $(1 + \alpha)^2 \equiv -1$; but $(\mathfrak{o}/\mathfrak{p}^4)^{\times} = \langle -1 \rangle \times \langle 1 + \alpha \rangle$, so there is an odd character χ_d modulo (4) with kernel $\langle 1 + \alpha \rangle = \{1, 1 + \alpha, -1 + 2\alpha, -1 + \alpha\} \pmod 4$.

Case 6: $d \equiv 1 \pmod 4$, $d > 1$. Again (2) is ramified. Let the power of 2 dividing $1 - d$ be 2^n; so $n \geqslant 2$. Then modulo $\mathfrak{p}^{2n}$ we have $-1 \equiv -d = \alpha^2$ so that there are no odd quadratic characteris modulo $\mathfrak{p}^{2n}$. Hence if $\mathfrak{p}^k$ is the smallest power of $\mathfrak{p}$ modulo which there is an odd character we must have $k \geqslant 2n + 1$. [Such a k must exist, for otherwise there would be a square root of -1 in the completion $K_{\mathfrak{p}} = \mathbb{Q}_2(\sqrt{-d})$ which is false if $d > 1$.]

4.2. Twisting operators

Let χ be a quadratic character of $\mathfrak{o}$ defined modulo the ideal $\mathfrak{q}$. Assume that $\mathfrak{q}$ is principal, generated by an element q. Let

$$R_q = \begin{pmatrix} q & 1 \\ 0 & q \end{pmatrix};$$

then for $\lambda \in \mathbb{Z}$ we have

$$R_q^\lambda = \begin{pmatrix} q & \lambda \\ 0 & q \end{pmatrix},$$

modulo scalars as always. We extend the definition to cover all λ in $\mathfrak{o}$:

$$R_q^\lambda := \begin{pmatrix} q & \lambda \\ 0 & q \end{pmatrix} \tag{4.2.1}$$

so that $R_q^1 = R_q$, and $R_q^q = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = T$. The law of exponents holds: $R_q^\lambda R_q^\mu = R_q^{\lambda+\mu}$. Observe also that if $\lambda \equiv \mu \pmod{\mathfrak{q}}$ then $R_q^\lambda (R_q^\mu)^{-1}$ is a power of T, so that $R_q^\lambda \equiv R_q^\mu (\bmod\ \Gamma_0(\mathfrak{a}))$ since $T \in \Gamma_0(\mathfrak{a})$ for any $\mathfrak{a}$.

Now let $\mathfrak{a}$ be an ideal such that $\mathfrak{q}^2$ divides $\mathfrak{a}$. If

$$\gamma = \begin{pmatrix} a & b \\ q^2 c & d \end{pmatrix}$$

is an element of $\Gamma_0(\mathfrak{a})$, and λ and μ are in $\mathfrak{o}$, we have

$$R_q^\lambda \gamma R_q^{-\mu} = \begin{pmatrix} a + \lambda q c & b + \dfrac{\lambda d - \mu a}{q} - \lambda \mu c \\ q^2 c & d - \mu q c \end{pmatrix}$$

which is in $\Gamma_0(\mathfrak{a})$ provided that $\lambda d \equiv \mu a (\bmod\ \mathfrak{q})$. Since $ad - bcq^2 = 1$ we have $ad \equiv 1 (\bmod\ \mathfrak{q})$, so an equivalent condition is that

$$\mu \equiv \lambda d^2 (\bmod\ \mathfrak{q}). \tag{4.2.2}$$

Hence for a given γ in $\Gamma_0(\mathfrak{a})$ and a given λ, we can find a μ such that $R_q^\lambda \gamma (R_q^\mu)^{-1} \in \Gamma_0(\mathfrak{a})$; moreover μ is unique modulo $\mathfrak{q}$, and so R_q^μ is unique modulo $\Gamma_0(\mathfrak{a})$.

We define R_χ to be a particular element of the group algebra of $PGL(2, K)$:

$$R_\chi := \sum_{\lambda \bmod q} \chi(\lambda) R_q^\lambda. \tag{4.2.3}$$

PROPOSITION 4.2.4: *Let* $\mathfrak{q}$, $\mathfrak{a}$ *and* χ *be as in the preceding discussion. Then*

(i) R_χ *acts on* $V(\mathfrak{a})$;

(ii) *If* $(\mathfrak{v}/\mathfrak{q})^\times$ *has exponent* 2 *then for any* λ *the matrix* R_q^λ *normalizes* $\Gamma_0(\mathfrak{a})$ *and hence* R_q^λ *itself acts on* $V(\mathfrak{a})$;

(iii) *If* $\mathfrak{p}=(\pi)$ *is a prime ideal dividing* $\mathfrak{a}$ *to the exact power e but not dividing* $\mathfrak{q}$ *then* $R_\chi W_\pi = \chi(\pi^e) W_\pi R_\chi$;

(iv) *If* $\mathfrak{p}=(\pi)$ *is a prime not dividing* $\mathfrak{a}$ *then* $R_\chi T_\pi = \chi(\pi) T_\pi R_\chi$;

(v) $R_\chi J = \chi(\varepsilon) J R_\chi$.

PROOF: The proofs of parts (i) – (iv) are almost identical to the proofs given in [1] (Lemmas 29-33) in the rational case. As for part (v), first note that

$$R_q^\lambda J = J R_q^{\varepsilon^{-1}\lambda}.$$

Then

$$R_\chi J = \sum_{\lambda \bmod q} \chi(\lambda) R_q^\lambda J = \sum_\lambda \chi(\lambda) J R_q^{\varepsilon^{-1}\lambda} = J \sum_\lambda \chi(\lambda) R_q^{\varepsilon^{-1}\lambda}.$$

A change of variables $\lambda = \mu\varepsilon$ shows that the latter sum is $\chi(\varepsilon) J R_\chi$ as required.

Note: As remarked in the Introduction, the homology space $V(\mathfrak{a})$ we have been working with is isomorphic to a certain space of cuspidal automorphic forms for $\Gamma_0(\mathfrak{a})$. These forms have Fourier expansions as in the case of modular forms for subgroups of $SL(2, \mathbb{Z})$, and the action of the operators J, T_π and R_χ can be seen directly on the Fourier coefficients. If the form F has coefficients $\{c(\alpha): \alpha \in \mathfrak{v}\}$ then

$F \mid J$ has coefficients $\{c(\alpha\varepsilon)\}$;
$F \mid T_\pi$ has coefficients $\{N(\pi)c(\alpha\pi) + c(\alpha/\pi)\}$;
$F \mid R_\chi$ has coefficients $\{\chi(\alpha)c(\alpha)\}$; (up to a constant scalar factor). See [4] for more details of this aspect.

COROLLARY 4.2.5: *Let* χ *be an odd quadratic character modulo* $\mathfrak{q}$ *and* $\mathfrak{a}$ *an ideal divisible by* $\mathfrak{q}^2$. Then

(i) R_χ *maps* $V^+(\mathfrak{a})$ *into* $V^-(\mathfrak{a})$ *and vice versa*;

(ii) *For each prime ideal* $\mathfrak{p}$ *of* $\mathfrak{v}$ *choose a generator* π *such that* $\chi(\pi)=1$; *then* R_χ *commutes with each* T_π *(for* $\mathfrak{p} \nmid \mathfrak{a}$*) and* W_π *(for* $\mathfrak{p} \mid \mathfrak{a}$*), and hence preserves the Hecke eigenvalues.*

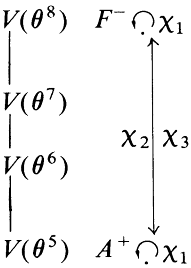
PROOF: Part (i) follows from part (v) of the Proposition since if $\chi(\varepsilon) = -1$ then $JR_\chi = -R_\chi J$. Similarly, part (ii) follows from parts (ii) and (iii) of the Proposition. □

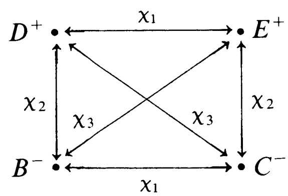
As a special case of the Corollary we obtain Theorem 4 by setting $R_2 = R_\chi$, where χ is the odd character χ_1 defined in subsection 4.1.

4.3. Other examples from the tables

Examples of the twist R_2 for $\mathbb{Q}(\sqrt{-1})$ have already been given. As another example for $\mathbb{Q}(\sqrt{-1})$, the 3-twist R_3 operates on $V(18)$; since i is a square modulo 3 ($i \equiv (1-i)^2$), R_3 preserves $V^+(18)$ which is one-dimensional. By Proposition 4.2.4 (ii) this implies that the eigenvalue of T_π on $V^+(18)$ is 0 whenever π is not a square modulo 3, which is verified by the calculations. There is also an example of a $1+2i$-twist in $V(18+i)$.

In $\mathbb{Q}(\sqrt{-2})$ set $\theta = \sqrt{-2}$. There is a primitive even character χ_1 modulo θ^2 and two primitive odd characters, χ_2 (defined in subsection 1 above) and $\chi_3 = \chi_1\chi_2$, modulo $(\theta^4) = (4)$. In $V^+(\theta^5)$ there is a newform A^+ which is its own χ_1-twist (and thus has eigenvalue 0 for T_π whenever $\chi_1(\pi) = -1$, or $\pi \equiv 1+\theta \pmod 2$). The χ_2-twist F^- of this newform appears in $V^-(\theta^8)$, and is also its own χ_1-twist. Also, in $V^-(\theta^7)$ there are two newforms, B^- and C^- which are χ_1-twists of each other; their χ_2-twists D^+ and E^+ appear in $V^+(\theta^8)$. We illustrate all this in the following diagram.





The corresponding elliptic curves are as follows:

$E_1: y^2 = x^3 + x$	has conductor (θ^5) and corresponds to A^+;
$E_2: y^2 = x^3 - x^2 + x - 1$	has conductor (θ^8) and corresponds to D^+;
$E_3: y^2 = x^3 + x^2 + x + 1$	has conductor (θ^8) and corresponds to E^+.

Note that E_1 has complex multiplications by $\mathbb{Z}[\sqrt{-1}]$ and so is its own χ_1-twist, while E_2 and E_3 are χ_1-twists of each other.

We give a final example from $\mathbb{Q}(\sqrt{-1})$ to show how twisting of newforms corresponds to twisting of curves. At level (10) for $\mathbb{Q}(i)$ there is a newform in $V^+((10))$ and a corresponding curve $y^2 = x^3 + x^2 - x$ with conductor (10). Applying the $(2i-1)$-twist, we obtain a newform at level $(10) \cap (2i-1)^2 = (20i-10)$, and because i is not a square modulo $(2i-1)$ this newform is in $V^-((20i-10))$. There is no corresponding curve with this conductor. If we then apply R_2 (in order to obtain a newform in V^+) to the latter, we find, as expected, a newform at level $(20i-10) \cap (1+i)^4 = (40i-20)$, in $V^+((40i-20))$. Moreover, if we twist the original curve by $2i-1$ we obtain the curve

$$y^2 = x^3 + (2i-1)x^2 - (2i-1)^2 x$$

which has conductor $(40i-20)$ and corresponds to the latter newform.

Numerous other examples of these and other twists abound in the tables. For brevity we omitted tables of the Hecke eigenvalues on V^-: these can be found in [4].

5. Other quadratic fields

The results proved in Section 4 apply to all complex quadratic fields, although numerical data has only been collected for the Euclidean fields. In the case of a non-Euclidean field with class number one, the tesselation of hyperbolic space consists of more than one kind of polyhedron. The case of $\mathbb{Q}(\sqrt{-19})$ has been described by Grunewald, Gushoff, and Mennicke in [7] and also by Hatcher [12], who also works out the picture for $\mathbb{Q}(\sqrt{-43})$. In the former tesselation there are two types of polyhedron; in the latter, four.

When the field K has class number greater than one the situation is further complicated by the fact that $PSL(2, \mathfrak{o}_K)$ no longer acts transitively on the cusps $K \cup \{\infty\}$ which form the vertices of the tesselation: the number of orbits is equal to the class number. It may be appropriate in these cases to consider the action of a larger group than $PSL(2, \mathfrak{o}_K)$, the action of which on the cusps is transitive. No work has yet been carried out on these tesselations, or possible applications and connections with elliptic curves, although for some of the fields the geometry was worked out by Swan [18], or Bianchi [3] in the last century.

References

[1] A.O.L. Atkin and J. Lehner: Hecke operators on $\Gamma_0(m)$. *Math. Ann. 185* (1970) 134–160.

[2] A.F. Beardon: The geometry of discrete groups. In: *Discrete Groups and Automorphic Functions,* Academic Press, London 1977.

[3] L. Bianchi: Sui Gruppi di Sostituzioni Lineari con Coefficienti appartenenti a Corpi quadratici immaginari. *Math. Ann.* 40 (1892) 332–412.

[4] J.E. Cremona: *Modular Symbols*, Oxford D. Phil. Thesis 1981.

[5] P. Gérardin and J.P. Labesse: Base change problem for $GL(2)$. In: Automorphic Forms, Representations and L-Functions, *Proc. Symp. Pure Math.* XXXIII(2), ed. A. Borel and W. Casselman.

[6] F. Grunewald: personal communication, November 1981.
[7] F. Grunewald, A.-C. Gushoff and J. Mennicke, *Komplex-quadratische Zahlkörper kleiner Diskriminante und Pflasterungen des dreidimensionalen hyperbolischen Raumes,* preprint.
[8] J. Elstrodt, F. Grunewald and J. Mennicke, On the group $PSL_2(\mathbf{Z}[i])$. In: *Lect. Notes 60*, London Math. Soc. 1981.
[9] F. Grunewald, H. Helling and J. Mennicke: $SL_2(\mathfrak{O})$ over complex quadratic numberfields I. *Algebra i Logica 17* (1978) 512–580.
[10] F. Grunewald and J. Mennicke: $SL_2(\mathfrak{O})$ and Elliptic Curves. Preprint, Bielefeld 1978.
[11] F. Grunewald and J. Schwermer: Arithmetic quotients of hyperbolic 3-space, cusp forms, and link complements. *Duke Math. J. 48* (1981) 351–358.
[12] A. Hatcher: *Hyperbolic Structures of Arithmetic type on some link complements.* Preprint.
[13] H. Jacquet and R.P. Langlands: Automorphic forms on $GL(2)$. *Lect. Notes Math. 114*, Berlin-Heidelberg-New York, 1970.
[14] 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.
[15] J.I. Manin: Parabolic points and zeta functions of modular curves. *Math. USSR Izv. 6* (1972) No. 1, 19–64.
[16] T. Miyake: On automorphic forms on GL_2 and Hecke operators. *Ann. Math. 94* (1971) 174–189.
[17] R.J. Stroeker: *Elliptic Curves defined over Imaginary Quadratic Fields,* Amsterdam Doctoral Thesis 1975.
[18] R.G. Swan: Generators and relations for certain special linear groups. *Advances in Math. 6* (1971) 1–77.
[19] J. Tate: Algorithm for determining the singular fiber in an elliptic pencil. In: Modular Functions of one Variable IV. *Lect. Notes Math. 476* Berlin-Heidelberg-New York 1975.
[20] J. Tate: The arithmetic of elliptic curves. *Inv. Math. 23* (1974) 179–206.
[21] D.J. Tingley: *Elliptic Curves uniformized by Modular Functions,* Oxford D. Phil. Thesis 1975.
[22] A. Weil: Über die Bestimmung Dirichletscher Reihen durch Functionalgleichungen. *Math. Ann. 168* (1967) 149–156.
[23] A. Weil: Dirichlet series and automorphic forms. *Lect. Notes Math. 189,* Berlin-Heidelberg-New York 1971.
[24] A. Weil: Zeta functions and Mellin transforms. *Colloquium on Algebraic Geometry*, Bombay 1968, 409–426.

(Oblatum 22-IV-1982)

Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
USA

from March, 1983:
Department of Mathematics
Dartmouth College
Bradley Hall
Hanover, NH 03755
USA

Note added in proof

Since this paper was accepted, new evidence has suggested that the "Main Conjecture" of (3.7) might need to be modified: in certain special cases a rational newform in $V^+(a)$ may correspond to an abelian variety of dimension 2 rather than an elliptic curve. See forthcoming papers for details and examples.