MODULAR SYMBOLS FOR $\Gamma_1(N)$ AND ELLIPTIC CURVES WITH EVERYWHERE GOOD REDUCTION

J. E. CREMONA

Abstract. The modular symbols method developed by the author in [4] for the computation of cusp forms for $\Gamma_0(N)$ and related elliptic curves is here extended to $\Gamma_1(N)$. Two applications are given: the verification of a conjecture of Stevens [14] on modular curves parametrised by $\Gamma_1(N)$; and the study of certain elliptic curves with everywhere good reduction over real quadratic fields of prime discriminant, introduced by Shimura and related to Pinch's thesis [10].

1. Introduction

In [4] a method was presented for the computation of the space $S_2(G)$ of cusp forms of weight 2 for a subgroup G of finite index in the modular group $\Gamma = PSL(2,\mathbb{Z})$. A detailed algorithm was given, in the case $G = \Gamma_0(N)$, for computing the 1-homology $H_1(\Gamma_0(N),\mathbb{C})$ (which is isomorphic to $S_2(\Gamma_0(N))$ as a Hecke module) explicitly in terms of certain "M-symbols" (see [4] and §2 below); finding one-dimensional rational eigenspaces for the Hecke algebra and hence finding rational newforms $f(z)$; computing numerically the period lattice of the differential $2\pi i f(z)dz$; and hence computing (approximately) the coefficients of the corresponding modular elliptic curve E_f.

In this paper we extend the M-symbol method to the cases $\Gamma_1(N)$ and $\Gamma_\chi(N)$ where χ is a quadratic character modulo N. It is hoped that we will hence be able systematically to compile tables of cusp forms of weight 2 for $\Gamma_1(N)$, or equivalently the spaces $S_2(N,\chi)$ of cusp forms of weight 2 with arbitrary character χ for $\Gamma_0(N)$. So far we have looked at the following two situations.

1. For each rational newform $f(z)$ for $\Gamma_0(N)$ computed in [4], we can compute the $\Gamma_1(N)$-period lattice $\Lambda_1(f)$ of the differential $2\pi i f(z)dz$, and hence compute an (approximate) equation for the corresponding elliptic curve $E_f^{(1)}$ parametrized by modular functions on $\Gamma_1(N)$. Clearly $\Lambda_1(f)$ has finite index in the $\Gamma_0(N)$-period lattice $\Lambda_0(f)$, so that $E_f^{(1)}$ is isogenous to E_f. To carry out this computation we only had to make certain modifications to the $\Gamma_0(N)$ computer programs used to compile the tables in [4], specifically in that part of the computation in which a

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

basis for the period lattice is computed. We have carried this out only for $N \leq 100$ and in this range we have an independent verification of the results of Stevens [14]. Stevens shows that in each isogeny class of elliptic curves over $\mathbb{Q}$ there is a unique curve with minimal period lattice (with respect to inclusion), and conjectures that this minimal curve is always the $\Gamma_1(N)$ curve. Using a different method Stevens has verified this for $N \leq 200$, the range of the tables in [2].

2. Let N be a prime congruent to 1 modulo 4, and χ the quadratic character modulo N, so that $\chi(-1) = 1$. Set

$$\Gamma_\chi(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid \chi(d) = 1 \right\},$$

and let $X_\chi(N)$ be the corresponding modular curve with Jacobian $J_\chi(N)$. Set $\overline{J_\chi(N)} = J_\chi(N)/J_0(N)$. The $\mathbb{Q}$-simple factors A of $\overline{J_\chi(N)}$ have even dimension $2d$ and split over $\mathbb{Q}(\sqrt{N})$ as $A = A' \times A''$ (up to isogeny) where $\dim A' = \dim A'' = d$, and A' is isogenous to A''. It is known ([12,7.7.6], [3,Theorem 1.1], [6, V.3.7(ii)]) that the factors A' and A'' have everywhere good reduction over $\mathbb{Q}(\sqrt{N})$. In the case $d = 1$ this gives a construction of elliptic curves of everywhere good reduction over $\mathbb{Q}(\sqrt{N})$ ([10], [11]). In [10], Pinch speculated that the curves he found and tabulated might all be of this form. Using our methods we have been able to find all such 2-dimensional A for $N < 1000$, and compute equations for the curves A' in all 16 cases. (The situation here is in fact very similar to the case of 2-dimensional factors of $J_0(N)$ with 'extra twist', as studied in [5].) We find some curves not in Pinch's tables (for $N = 461$ and $N = 509$), and show that two of his curves could not arise in this way, as each is not isogenous to its Galois conjugate.

The cases $N = 29, 37, 41$ have previously been worked out by Shiota [13] using manual computations with modular symbols. These cases are considerably simpler, since the genus is 2, so $A = \overline{J_\chi(N)}$ and it is not necessary to find and split off particular 2-dimensional factors. Also, Shiota computes the j-invariants of the curves A' rather than the actual equations; these j-invariants are known to be integral, and so can be computed exactly. One interesting feature of our computations is that the models which we obtain for the curves are *not* always minimal models, in striking contrast to the situation with $\Gamma_0(N)$ elliptic curves where in all known cases one obtains a minimal model from the period lattice of the normalised newform (this is Manin's "$c = 1$" conjecture). Indeed, in some of our cases here the class number of $\mathbb{Q}(\sqrt{N})$ is greater than 1 and no minimal equation exists for the curve. This phenomenon is not noticed in [13], although it first occurs at level 37.

We present the results of these computations below in section 6 together with a conjecture concerning the minimality of the models at the primes above 2 and 3. Work is in progress to extend these computations to composite N and χ a primitive character modulo N, and to imprimitive χ.

In §2 we review general aspects of the modular symbol method from [4]; in §3 we show how to define M-symbols for $\Gamma_1(N)$. The first application, to $\Gamma_1(N)$ modular

curves, occupies §4. In §5 we discuss the computation of $S_2(N,\chi)$ for characters χ in general, and in the specific case described above, where N is prime and χ quadratic. The results in the latter case are given in §6.

2. The modular symbol method: generalities

In this section we outline the basic modular symbol method which may be used to compute the 1-homology $H_1(G\backslash\mathcal{H}^*,\mathbb{Q})$ for any subgroup G of finite index in the modular group Γ. Here $\mathcal{H}^* = \mathcal{H}\cup\mathbb{Q}\cup\{\infty\}$, the extended upper half-plane. For more details on this, see [4].

We have $H_1 = H_1^+\oplus H_1^-$, where $H_1^\pm$ denote the $\pm$-eigenspaces for the conjugation involution $*$ induced by $z\mapsto\overline{-z}$, and $\dim H_1^+ = \dim H_1^- = g$, the genus of the Riemann surface $X_G = G\backslash\mathcal{H}^*$. There is a duality between homology and the space of holomorphic differentials on X_G. These differentials (or, more precisely, their pullbacks to $\mathcal{H}$) have the form $2\pi i f(z)dz$ where $f(z)$ is a cusp form of weight 2 for G, and the bilinear pairing

$$S_2(G)\times H_1(X_G,\mathbb{C})\longrightarrow\mathbb{C}$$

given by

$$(f,\gamma)\mapsto\langle f,\gamma\rangle = \int_\gamma 2\pi i f(z)dz$$

induces an isomorphism of complex vector spaces

$$S_2(G)\cong H_1^+(X_G,\mathbb{C}).$$

This isomorphism is also an isomorphism of modules for the Hecke algebra $\mathbb{T}$ (when G is a congruence subgroup), since we then have

$$\langle Tf,\gamma\rangle = \langle f,T\gamma\rangle$$

for all $T\in\mathbb{T}$.

To compute $H = H_1(X_G,\mathbb{C})$ we represent homology classes by modular symbols $\{\alpha,\beta\}_G$ with $\alpha,\beta\in\mathcal{H}^*$. The symbol $\{\alpha,\beta\}$ denotes a geodesic path from α to β in $\mathcal{H}^*$, and $\{\alpha,\beta\}_G$ its image in X_G, or its homology class. To generate H it suffices to take α and β to be cusps, i.e. $\alpha,\beta\in\mathbb{Q}\cup\{\infty\}$. Moreover each symbol $\{\alpha,\beta\}$ may be expressed as a sum of symbols of the special form $\{\gamma(0),\gamma(\infty)\} = \{b/d, a/c\}$ with $\gamma = \begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma$, using continued fractions in $\mathbb{Q}$.

Let (γ) denote the special symbol $\{\gamma(0),\gamma(\infty)\}_G$ for each $\gamma\in\Gamma$. These symbols generate H, while satisfying the relations

$$(g\gamma) = (\gamma) \qquad \text{for } g\in G; \tag{1}$$

$$(\gamma)+(\gamma S) = 0; \tag{2}$$

$$(\gamma)+(\gamma TS)+(\gamma(TS)^2) = 0; \tag{3}$$

where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are the usual generators of Γ. In view of (1) we may generate $H_1(X_G, \mathbb{Q})$ using the finite number of symbols (γ) as γ ranges over a set $\mathcal{R}$ of right coset representatives for G in Γ. Let $C(G)$ be the $\mathbb{Q}$-vector space spanned by symbols (γ) with $\gamma \in \mathcal{R}$, and $B(G)$ the subspace spanned by the left-hand sides of the relations (2) and (3).

Denote by $H_0(G)$ the $\mathbb{Q}$-vector space with basis the equivalence classes $[\alpha]$ of cusps $\alpha \in \mathbb{Q} \cup \{\infty\}$ under the action of G. Define the 'boundary map' $\delta\colon C(G) \to H_0(G)$ by

$$\delta((\gamma)) = [\gamma(\infty)] - [\gamma(0)],$$

extended by linearity, and set $Z(G) = \ker(\delta)$. It is easy to see that $B(G) \subseteq Z(G)$. Finally set $H(G) = Z(G)/B(G)$. The fundamental result, first formulated in this way by Manin [8], is the following.

Theorem 2.1 (Manin). *$H(G)$ is isomorphic to $H_1(X_G, \mathbb{Q})$, the isomorphism being given by*

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

The flexibility of this result comes from the fact that the homology relations (2), (3) do not depend on which subgroup G of Γ is being considered. Only the generators change, coming from a set of right coset representatives of G in Γ. To apply this result in practice, we thus need to determine these coset representatives explicitly in an easily computable form. We also need to be able to determine when two cusps are equivalent modulo G in order to compute $\ker \delta$.

In the case $G = \Gamma_0(N)$ considered in [4], we represented the right cosets of G in Γ by means of so-called M-symbols $(c : d)$, where $c, d \in \mathbb{Z}$, $\gcd(c, d, N) = 1$, and $(c : d) = (c' : d') \iff cd' \equiv c'd \pmod{N}$. The correspondence with coset representatives is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longleftrightarrow (c : d)$$

where a and b are any integers such that $ad - bc = 1$; the boundary map becomes

$$\delta((c : d)) = [a/c] - [b/d].$$

It is often desirable to compute $H_1^+(G\backslash\mathcal{H}^*, \mathbb{Q})$ directly rather than as the $+1$-eigenspace of the $*$-involution (given by $(\gamma) \mapsto (J\gamma)$ where $J = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$), in order to work in a space of dimension g rather than $2g$. To do this, define $C(G)$ as before but enlarge the relation subspace to $B^+(G)$, spanned by $B(G)$ and the extra relations $(\gamma) = (J\gamma)$ for $\gamma \in \Gamma$. Similarly, we replace $Z(G)$ by $Z^+(G) = \ker \delta^+$ where

$$\begin{aligned} \delta^+((\gamma)) &= \delta((\gamma)) + \delta((J\gamma)) \\ &= [\gamma(\infty)] - [\gamma(0)] + [-\gamma(\infty)] - [-\gamma(0)]. \end{aligned}$$

Then $B^+(G) \subseteq Z^+(G)$ and

$$H^+(G) = Z^+(G)/B^+(G) \cong H_1^+(G\backslash\mathcal{H}^*, \mathbb{Q}).$$

Alternatively we may set $H_0^+(G)$ to be the quotient of $H_0(G)$ by the relations $[\alpha] = [J(\alpha)]$, that is $[\alpha] = [-\alpha]$, and define $\overline{\delta}\colon C(G) \to H_0^+(G)$ by

$$\overline{\delta}(\gamma) = [\pm\gamma(\infty)] - [\pm\gamma(0)],$$

where $[\pm\alpha]$ denotes the equivalence class of $[\alpha]$ in $H_0^+(G)$. Then clearly $\ker\delta^+ = \ker\overline{\delta} = Z^+(G)$, and $H^+(G) = Z^+(G)/B^+(G)$ as before.

This gives an explicit representation of the space $H_1^+(G\backslash\mathcal{H}^*, \mathbb{C}) = H_1^+(G\backslash\mathcal{H}^*, \mathbb{Q})\otimes\mathbb{C}$, which is isomorphic to the space of cusp forms $S_2(G)$, and on which we may compute the actions of Hecke and other operators. As the dimension is half that of the whole space H_1, there is some saving in machine storage and computation time with this approach.

3. Symbols for $\Gamma_1(N)$

3.1. First we adapt the definition of M-symbols to give convenient coset representatives for $\Gamma_1(N)$ in Γ.

Lemma 3.1. *For $i = 1, 2$ let $\gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \Gamma$. The matrices γ_1 and γ_2 lie in the same right coset of $\Gamma_1(N)$ if and only if $c_1 \equiv \varepsilon c_2$ and $d_1 \equiv \varepsilon d_2 \pmod N$, where $\varepsilon = \pm 1$.*

Proof. We have

$$\gamma_1\gamma_2^{-1} = \begin{pmatrix} a_1d_2 - b_1c_2 & * \\ c_1d_2 - d_1c_2 & a_2d_1 - b_2c_1 \end{pmatrix},$$

which is in $\Gamma_1(N)$ if and only if

$$c_1d_2 - d_1c_2 \equiv 0 \pmod N$$

and

$$a_2d_1 - b_2c_1 \equiv a_1d_2 - b_1c_2 \equiv \varepsilon \pmod N$$

with $\varepsilon = \pm 1$. Suppose that these congruences hold. Then

$$\begin{aligned} c_2\varepsilon &\equiv a_2d_1c_2 - b_2c_1c_2 \\ &\equiv a_2d_2c_1 - b_2c_2c_1 && \text{since } d_1c_2 \equiv d_2c_1 \pmod N \\ &\equiv c_1 && \text{since } a_2d_2 - b_2c_2 = 1 \end{aligned}$$

and $d_2\varepsilon \equiv d_1$ similarly. Conversely if $c_1 \equiv \varepsilon c_2$ and $d_1 \equiv \varepsilon d_2 \pmod N$, with $\varepsilon = \pm 1$ then the congruences follow easily. □

Thus we can represent each coset uniquely by a symbol (c,d) with $c,d \in \mathbb{Z}/N\mathbb{Z}$ provided that we identify (c,d) with $(-c,-d)$. Such symbols will be called M1-symbols. The correspondence between M1-symbols, coset representatives, and modular symbols is given by

$$(c,d) \leftrightarrow \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow (\gamma) = \{b/d, a/c\} \tag{3.1}$$

where $a,b \in \mathbb{Z}$ are chosen so that $ad-bc=1$. (A different choice of a,b has the effect of multiplying γ on the left by a power of T which does not change the symbol (γ) since $T \in \Gamma_1(N)$ for all N.)

The right coset action of Γ on M1-symbols is given by

$$(c,d)\begin{pmatrix} p & q \\ r & s \end{pmatrix} = (cp+dr, cq+ds). \tag{3.2}$$

The boundary map δ has the form

$$\delta((c,d)) = [a/c] - [b/d]. \tag{3.3}$$

We may test the equivalence of cusps by the following lemma.

Lemma 3.2. *For $i=1,2$ let $\alpha_i = p_i/q_i$ be cusps written in lowest terms. The following are equivalent:*
(1) $\alpha_2 = \gamma(\alpha_1)$ for some $\gamma \in \Gamma_1(N)$;
(2) $q_2 \equiv \varepsilon q_1 \pmod N$ and $p_2 \equiv \varepsilon p_1 \pmod{\gcd(q_1,N)}$, with $\varepsilon = \pm 1$.

Proof. That (1) implies (2) is easy. For the converse we use Lemma 3.1. Assume (2), and write $p_1 s_1' - q_1 r_1' = p_2 s_2 - q_2 r_2 = 1$ with $s_1', r_1', s_2, r_2 \in \mathbb{Z}$. Then $p_1 s_1' \equiv 1 \pmod{q_1}$ and $p_2 s_2 \equiv 1 \pmod{q_2}$. Also $\gcd(q_1,N) = \gcd(q_2,N) = N_0$, say, since $q_2 \equiv \pm q_1 \pmod N$. Now $p_2 \equiv \varepsilon p_1 \pmod{N_0}$ implies $s_1' \equiv \varepsilon s_2 \pmod{N_0}$, so we may find $x \in \mathbb{Z}$ such that $xq_1 \equiv s_1' - \varepsilon s_2 \pmod N$. Set $s_1 = s_1' - xq_1$ and $r_1 = r_1' - xp_1$. Then $p_1 s_1 - q_1 r_1 = 1$ and now $s_2 \equiv \varepsilon s_1 \pmod N$. By Lemma 3.1 there exists $\gamma \in \Gamma_1(N)$ such that $\begin{pmatrix} p_2 & r_2 \\ q_2 & s_2 \end{pmatrix} = \gamma \begin{pmatrix} p_1 & r_1 \\ q_1 & s_1 \end{pmatrix}$, and so $\gamma(p_1/q_1) = p_2/q_2$ as required. □

Let $X_1(N) = \Gamma_1(N)\backslash\mathcal{H}^*$. We may now compute $H_1(X_1(N),\mathbb{Q})$ using Theorem 2.1 as follows.

(1) Form the $\mathbb{Q}$-vector space with basis a set of M1-symbols modulo N. A pairwise inequivalent set of symbols is

$$\{(c,0) \mid 1 \le c \le N/2\} \cup \{(c,d) \mid -N/2 < c \le N/2, 1 \le d \le N/2\}.$$

(2) Factor out by the relations

$$(c,d) + (-d,c) = 0$$
$$(c,d) + (c+d,-c) + (-d,c+d) = 0$$

(3) Restrict to $\ker\delta$, where δ is defined by (3.3) and cusp equivalence is tested via Lemma 3.2.

The result is a $\mathbb{Q}$-basis for $H_1(X_1(N),\mathbb{Q})$ given explicitly in terms of M1-symbols.

3.2 Character decomposition. Recall that the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$ acts on the space of cusp forms $S_2(\Gamma_1(N))$ as follows (see [7]). For each $u \in (\mathbb{Z}/N\mathbb{Z})^*$, let $\gamma_u \in \Gamma$ be a matrix such that

$$\gamma_u \equiv \begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix} \pmod{N}.$$

Then γ_u acts on the modular forms $f(z) \in S_2(\Gamma_1(N))$ in the usual way, and we obtain a decomposition

$$S_2(\Gamma_1(N)) = \bigoplus_{\chi} S_2(N, \chi) \tag{3.4}$$

where χ ranges over all the even characters modulo N. Here $S_2(N, \chi)$ is the subspace of forms $f(z)$ such that $f|\gamma_u = \chi(u)f$, which is zero if $\chi(-1) = -1$ since we always have $\gamma_{-1} \in \Gamma_1(N)$.

On $H_1(X_1(N), \mathbb{C})$, given in terms of M1-symbols, the action of γ_u is

$$\gamma_u \colon (c, d) \mapsto (uc, ud) \tag{3.5}$$

and similarly we have a decomposition

$$H_1(X_1(N), \mathbb{C}) = \bigoplus_{\chi} H_1(N, \chi). \tag{3.6}$$

To compute this decomposition we use (3.5) to compute the action of each γ_u with respect to an M1-symbol basis as a $2g \times 2g$ matrix, where g is the genus of $X_1(N)$, and simultaneously diagonalize these matrices. Clearly it suffices to work with γ_u for a set of u which generates $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$; in particular, when N is a prime power this group is cyclic, and we merely have to diagonalize the matrix γ_u for a primitive root u.

The eigenvalues of γ_u will be roots of unity of order dividing $\varphi(N)$, so the splitting (3.5) will be defined over the cyclotomic field $\mathbb{Q}(\mu_{\varphi(N)})$.

3.3 Hecke action. For primes p not dividing N the action of the Hecke operator T_p is given by

$$T_p = \sum_{a \pmod{p}} \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} + \gamma_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence we may compute the action of T_p on modular symbols:

$$T_p(\{\alpha, \beta\}) = \sum \left\{ \frac{\alpha + a}{p}, \frac{\beta + a}{p} \right\} + \{\gamma_p(p\alpha), \gamma_p(p\beta)\}. \tag{3.7}$$

In practice we convert the generating M1-symbols to modular symbols via (3.1) once and for all, then apply (3.7), and reconvert using continued fractions, as in the $\Gamma_0(N)$ case. On the χ-eigenspace (3.7) becomes, more simply,

$$T_p(\{\alpha, \beta\}) = \sum \left\{ \frac{\alpha + a}{p}, \frac{\beta + a}{p} \right\} + \chi(p)\{p\alpha, p\beta\}. \tag{3.8}$$

3.4 Computing eigenspaces separately. It is more efficient in practice to compute the χ-eigenspaces of $H_1(X_0(N),\mathbb{C})$ separately, instead of computing the whole space first and then diagonalizing the γ_u matrices as described in §3.2. We may do this by including extra relations between the symbols of the form

$$(\gamma_u\gamma) = \chi(u)(\gamma); \tag{3.9}$$

or, in terms of M1-symbols,

$$(uc, ud) = \chi(u)(c, d). \tag{3.10}$$

Also we have to replace $H_0(\Gamma_1(N))$ by $H_0^\chi(\Gamma_1(N))$, obtained from $H_0(\Gamma_1(N))$ by factoring out by relations of the form

$$[\gamma_u(\alpha)] = \chi(u)[\alpha] \tag{3.11}$$

on the cusp equivalence classes. As a special case, when χ is the trivial character, the symbols reduce precisely to M-symbols for $\Gamma_0(N)$. The advantage of this approach is that we will (in general) be working in spaces of smaller dimension from the start, with a corresponding gain in computation time and saving in machine storage at each stage of the computation. The technique is in fact very similar to the idea of working in H_1^+, as at the end of §2. Moreover, using (3.10) we may cut down the initial set of M1-symbols by a factor of $[\Gamma_0(N) : \Gamma_1(N)] = \frac{1}{2}\varphi(N)$ (if $N > 2$), and just use (in effect) the M-symbols $(c : d)$ which are in one-one correspondence with the coset representatives for $\Gamma_0(N)$ in Γ, and satisfy

$$(c_1 : d_1) = (c_2 : d_2) \iff c_1d_2 \equiv c_2d_1 \pmod N.$$

In practice whenever we compare a given M1-symbol (c, d) with our standard list of M-symbols and find (say) $(c : d) = (c_0 : d_0)$, then we may replace (c, d) by $\chi(u)(c_0, d_0)$ where u is such that $c \equiv uc_0$ and $d \equiv ud_0 \pmod N$.

The method described in this subsection has so far only been implemented in the case where χ is quadratic, so that $\chi(u) = \pm1$ for all $u \in (\mathbb{Z}/N\mathbb{Z})^*$. In this case we can work entirely with rational coefficients, which makes programming much simpler. This will be described in more detail (for prime N) in §5, with the results in §6.

4. $\Gamma_1(N)$ modular curves and Stevens' conjecture

In [4] we computed numerically the period lattice

$$\Lambda_0(f) = \left\{ \int_0^{\gamma(0)} 2\pi i f(z)dz \mid \gamma \in \Gamma_0(N) \right\}$$

for rational newforms $f \in S_2(\Gamma_0(N))$, in order to find the corresponding 'strong Weil curves' $E_f = \mathbb{C}/\Lambda_0(f)$. This was carried out for all $N \le 1000$. Each such f is,

of course, also a newform for $\Gamma_1(N)$, and we may also consider the $\Gamma_1(N)$ period lattice

$$\Lambda_1(f) = \left\{ \int_0^{\gamma(0)} 2\pi i f(z)dz \mid \gamma \in \Gamma_1(N) \right\}$$

and the curve $E_f^1 = \mathbb{C}/\Lambda_1(f)$. In [14] Stevens conjectured that E_f^1 is always the unique curve in its isogeny class with minimal period lattice (ordered by inclusion), and verified this in all cases for which data were then available in the Antwerp IV tables [2], namely for all cases where $N \leq 200$.

As an application of the method of the previous section, we checked Stevens' results for $N \leq 100$. In each case we already had on computer files the Hecke eigenvalues of each rational newform $f \in S_2(\Gamma_0(N))$. Now we adapted the computer programs, used in [4] to compute $\Lambda_0(f)$, to compute $\Lambda_1(f)$ instead. We first computed a basis for $H_1(X_1(N), \mathbb{C})$ in terms of M1-smbols and found a pair of eigencycles with the same eigenvalues as f. Then we used the same method as in [4] (with very minor changes) to obtain a pair of generating periods for $\Lambda_1(f)$. From these we computed the c_4 and c_6 covariants of $\Lambda_1(f)$, and found them to be very close to integers, integers which were indeed the covariants of the minimal model of a curve E_f^1 of conductor N.

While this was a simple procedure in principle, in practice it became very time-consuming since the number of M1-symbols grows rapidly with N. This number is the index $[\Gamma : \Gamma_1(N)] = \frac{1}{2}N^2 \prod_{p|N}(1 - p^{-2})$ for $N > 2$, which is $\frac{1}{2}\varphi(N)$ times the number of M-symbols. Hence this method does not seem a practical way of verifying Stevens' conjecture much past $N = 200$. However, a more efficient algorithm is currently being implemented by the author, using which it is hoped to carry the verification much further, perhaps for N up to 1000, the range of [4].

5. Computation of elliptic curves with everywhere good reduction

5.1 Modular symbols. From now on N will be a prime congruent to 1 modulo 4, and χ the quadratic character modulo N, so that $\chi(-1) = 1$. Set

$$\Gamma_\chi(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid \chi(d) = 1 \right\},$$

a normal subgroup of index 2 in $\Gamma_0(N)$. The space of cusp forms for $\Gamma_\chi(N)$ is a subspace of $S_2(\Gamma_1(N))$ and splits as

$$S_2(N, \chi) \oplus S_2(N);$$

we will be concerned with the χ-eigenspace only. As described in §3.4, we have

$$\begin{aligned} S_2(N, \chi) &\cong H_1(\Gamma_\chi(N)\backslash\mathcal{H}^*, \mathbb{C})/H_1(\Gamma_0(N)\backslash\mathcal{H}^*, \mathbb{C}) \\ &= H_1^\chi(N), \end{aligned}$$

say, which may be computed using M1-symbols (c,d) modulo N with the extra relations

$$(gc, gd) = -(c, d)$$

where g is a primitive root modulo N. These relations reduce the generating set of symbols to $N+1$ since

$$(c,d) = \begin{cases} \chi(d)(cd^{-1}, 1) & \text{if } d \not\equiv 0 \pmod N, \\ \chi(c)(1,0) & \text{if } d \equiv 0 \pmod N. \end{cases}$$

Then we impose the usual homology relations from §3.1. The boundary map δ^χ is given by

$$\delta^\chi(c,d) = \delta(c,d) - \delta(gc, gd)$$

with δ given by (3.3). It is easy to see that there are four cusp equivalence classes, since N is prime:

$$\begin{aligned} \mathcal{C}_1 &= \{p/q \in \mathbb{Q} \cup \infty \mid \chi(q) = 0, \chi(p) = +1\}; \\ \mathcal{C}_2 &= \{p/q \in \mathbb{Q} \cup \infty \mid \chi(q) = 0, \chi(p) = -1\}; \\ \mathcal{C}_3 &= \{p/q \in \mathbb{Q} \cup \infty \mid \chi(q) = +1\}; \\ \mathcal{C}_4 &= \{p/q \in \mathbb{Q} \cup \infty \mid \chi(q) = -1\}. \end{aligned}$$

We have $\delta^\chi((1,0)) = \mathcal{C}_3 - \mathcal{C}_1 - \mathcal{C}_4 + \mathcal{C}_2$, while

$$\begin{aligned} \delta^\chi((c,1)) &= \begin{cases} 0 & \text{if } \chi(c) = +1 \\ 2(\mathcal{C}_4 - \mathcal{C}_3) & \text{if } \chi(c) = -1 \end{cases} \\ &= (1 - \chi(c))(\mathcal{C}_4 - \mathcal{C}_3). \end{aligned}$$

Thus $H_1^\chi(N) = \ker(\delta^\chi)$ may be computed.

5.2. Hecke eigenspaces. Let p denote a prime with $\chi(p) = +1$, and q a prime with $\chi(q) = -1$. Then (see [7]) the Hecke operator T_p is Hermitian, while T_q is skew-Hermitian, so the eigenvalues a_p, a_q are real and pure imaginary respectively. We also have the Fricke involution $W = W_N$ induced by $z \mapsto -1/Nz$, which satisfies

$$WT_p = T_pW, \qquad WT_q = -T_qW.$$

Since N is square-free there cannot be any complex multiplication. It follows that simultaneous eigenforms for all T_p, T_q come in pairs $\{f_1, f_2\}$, with eigenvalues as follows:

$$\begin{aligned} T_p(f_1) = a_pf_1, \quad T_p(f_2) = a_pf_2 \qquad & \text{with } a_p \in \mathbb{R}; \\ T_q(f_1) = a_qf_1, \quad T_p(f_2) = -a_qf_2 \qquad & \text{with } a_q \in i \cdot \mathbb{R}. \end{aligned}$$

Moreover, $W(f_1)$ is a scalar multiple of f_2 and vice versa. These scalars are called "pseudo-eigenvalues" in [1]. In our case we have (see [13, §2.1] or [9, Lemma 2]):

$$W(f_1) = \frac{\overline{a_N}}{\sqrt{N}} f_2, \qquad W(f_2) = \frac{a_N}{\sqrt{N}} f_1$$

where a_N and $\overline{a_N}$ are the T_N-eigenvalues of f_1 and f_2, which satisfy $|a_N| = N$.

5.3. The elliptic curves. Suppose that $f_1 = \sum_{n=1}^{\infty} a_n \exp(2\pi i n z)$ and f_2 are a conjugate pair of eigenforms, as above, normalized so that $a_1 = 1$, and such that $a_p \in \mathbb{Z}$. Then each a_q has the form $b_q\sqrt{-d}$ with $b_q \in \mathbb{Z}$ and d a square-free positive integer depending only on f_1, f_2 but not on q. From such a pair of forms we may construct elliptic curves defined over $\mathbb{Q}(\sqrt{N})$, which are known to have everywhere good reduction.

Let Λ be the period lattice in $\mathbb{C}^2$ of the pair $\{f_1, f_2\}$:

$$\Lambda = \left\{ (2\pi i \int_\gamma f_1, 2\pi i \int_\gamma f_2) \mid \gamma \in H_1(\Gamma_\chi(N)\backslash\mathcal{H}^*, \mathbb{Z}) \right\}.$$

Set $A = \mathbb{C}^2/\Lambda$, a two-dimensional abelian variety defined over $\mathbb{Q}$. We have

$$\mathrm{End}_{\mathbb{Q}}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}(\sqrt{-d}),$$

so that A is simple over $\mathbb{Q}$, while

$$\mathrm{End}_{\mathbb{Q}(\sqrt{N})}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong M_2(\mathbb{Q})$$

so that A splits as a product of two elliptic curves (up to isogeny) over $\mathbb{Q}(\sqrt{N})$. These are the elliptic curves which we wish to compute.

Now W is defined over $\mathbb{Q}(\sqrt{N})$, and $W^2 = 1$; the splitting is achieved by separating the $+1$ and -1 eigenspaces for W. Let h_1 and h_2 be the normalized forms in $\mathbb{C}f_1 + \mathbb{C}f_2$ with W-eigenvalues -1 and $+1$ respectively; up to normalization we have $h_1 = (1 - W)f_1$ and $h_2 = (1 + W)f_1$. Then changing basis from $\{f_1, f_2\}$ to $\{h_1, h_2\}$ we find that $\Lambda = \Lambda_1 \times \Lambda_2$ where Λ_1 and Λ_2 are the (rank 2) period lattices of h_1 and h_2 in $\mathbb{C}$. Setting $A_j = \mathbb{C}/\Lambda_j$ we have $A = A_1 \times A_2$ (up to isogeny). The elliptic curves A_j are thus defined over $\mathbb{Q}(\sqrt{N})$ and are known to have everywhere good reduction.

In order to compute the curves A_j explicitly we must first identify the occurrence of a suitable pair of cusp forms f_1, f_2; then compute a large number of the Fourier coefficients (Hecke eigenvalues) a_p, a_q; and determine explicitly the cycles in integral homology which will give a $\mathbb{Z}$-basis for the lattices Λ_1, Λ_2. In practice we perform the first two steps working in the smaller space H_1^+ (fixed by conjugation), and move to the whole space H_1 to find the full period lattices before computing the periods. However, for simplicity of exposition, here we will work in the full space H_1 throughout. The periods themselves will be computed indirectly, by computing the values of certain L-series (attached to appropriate quadratic twists of h_1 and h_2) at $s = 1$.

These three stages will now be discussed in detail.

5.4. Finding the eigenforms. Having computed $H_1^\chi(N)$ using symbols as in §5.1 we restrict to the $+1$-eigenspace for conjugation and then further to the -1-eigenspace for the W involution. Then we search through primes p with $\chi(p) = +1$

for an eigenspace for T_p of dimension 1 for some rational integer eigenvalue a_p (which must satisfy $|a_p| < 2\sqrt{p}$). If some p has no rational eigenvalues we abandon this value of N. If p has a rational eigenvalue of multiplicity greater than 1 we try another prime p.

Once we have an eigenvector $\eta_1 \in H_1^\chi(N)$ with $*(\eta_1) = \eta_1$, $W(\eta_1) = -\eta_1$, $T_p(\eta_1) = a_p\eta_1$, we then compute $\eta_2 = T_q(\eta_1)$ for a prime q with $\chi(q) = -1$. We may assume that $\eta_2 \neq 0$ (otherwise we try a different q), so that $\{\eta_1, \eta_2\}$ is a basis for the 2-dimensional subspace of $H_1^\chi(N)$ corresponding to a suitable pair of eigenforms $\{f_1, f_2\}$. We thus have $T_q(\eta_2) = -k^2 d\eta_1$ where k and d are positive integers, d square-free. Also $T_p(\eta_2) = a_p\eta_2$ since T_p and T_q commute, while $W(\eta_2) = +\eta_2$ since W and T_q anti-commute. Hence we have located the occurrence of a suitable pair of newforms $\{f_1, f_2\}$ and know the imaginary quadratic field $Q(\sqrt{-d})$ in which their Fourier coefficients (or Hecke eigenvalues) lie.

5.5. Computing Fourier coefficients. We keep the notation of the previous section.

Computing a_p, $\chi(p) = +1$. The technique of [4] needs little change in this case. Let $\widehat{\eta_1}, \widehat{\eta_2}$ be dual eigenvectors with the same eigenvalues as η_1, η_2, and $\widehat{\eta_2} = \widehat{T_q}\widehat{\eta_1}$. (In practice we have a matrix for T_q, the η_j are right column eigenvectors, and the $\widehat{\eta_j}$ are left row eigenvectors, or equivalently right column eigenvectors for the transpose $\widehat{T_q}$ of T_q.) For $\chi(p) = +1$ set $\gamma(p) = \sum_{a \pmod p}\{0, a/p\}$. Let p_0 be the smallest prime p with $\chi(p) = +1$. Set

$$\widehat{\eta} = \begin{cases} \widehat{\eta_1} & \text{if } \widehat{\eta_1}\cdot\gamma(p_0) \neq 0, \\ \widehat{\eta_2} & \text{if } \widehat{\eta_1}\cdot\gamma(p_0) = 0,\ \widehat{\eta_2}\cdot\gamma(p_0) \neq 0. \end{cases}$$

(In all cases we never had $\widehat{\eta_1}\cdot\gamma(p_0) = \widehat{\eta_2}\cdot\gamma(p_0) = 0$, which is equivalent to $L(h_1, 1) = L(h_2, 1) = 0$.) We suppose that the value $\widehat{\eta_1}\cdot\gamma(p_0)$ is computed once and for all, and that we know a_{p_0} by direct computation of T_{p_0}. Then the values of a_p for all other p with $\chi(p) = +1$ are given by the following.

Lemma 5.5.1. *For all primes p with $\chi(p) = +1$,*

$$a_p = 1 + p - \frac{(1 + p_0 - a_{p_0})\gamma(p)\cdot\widehat{\eta}}{\gamma(p_0)\cdot\widehat{\eta}}.$$

Proof. We have

$$(1 + p - a_p)L(h_1, 1) = (\gamma(p)\cdot\widehat{\eta})\lambda,$$

where λ is a fixed real period of h_1, not depending on p, so $(1 + p - a_p)/(\gamma(p)\cdot\widehat{\eta})$ is independent of p and the result follows. □

Computing a_q, $\chi(q) = -1$. Recall that for $\chi(q) = -1$ we have eigenvalues of the form $a_q = b_q\sqrt{-d}$ where $b_q \in \mathbb{Z}$. For one such prime q_0 we already know b_{q_0} from the first stage. When $\chi(q) = -1$ define

$$\gamma(q) = \sum_{a \pmod q} \left\{0, \frac{1+aq_0}{qq_0}\right\} - \left\{0, \frac{q}{q_0}\right\}.$$

Lemma 5.5.2. *$\gamma(q)$ is in the integral homology.*

Proof. First suppose $q \neq q_0$. If $1+aq_0 \not\equiv 0 \pmod q$ then the fraction $(1+aq_0)/(qq_0)$ is in lowest terms, with $\chi(qq_0) = +1$, so the term $\{0, (1+aq_0)/(qq_0)\}$ is integral. Let a_0 denote the unique solution to $1 + aq_0 \equiv 0 \pmod q$. Then

$$\left\{0, \frac{1+a_0q_0}{qq_0}\right\} - \left\{0, \frac{q}{q_0}\right\} = \left\{\frac{q}{q_0}, \frac{(1+a_0q_0)/q}{q_0}\right\}$$

is integral.

If $q = q_0$ then $\{0, q/q_0\} = 0$ and $\{0, (1+aq_0)/(q_0^2)\}$ is integral for all a. □

Now the values of b_q for all q with $\chi(q) = -1$ are given by the following.

Lemma 5.5.3.

$$\frac{b_q}{b_{q_0}} = \frac{[(q-1)\gamma(p_0) - (1+p_0-a_{p_0})\gamma(q)]\cdot\widehat{\eta}}{[(q_0-1)\gamma(p_0) - (1+p_0-a_{p_0})\gamma(q_0)]\cdot\widehat{\eta}}.$$

Proof.

$$\begin{aligned} T_q\left(\left\{\frac{1}{q_0}, \infty\right\}\right) &= -\left\{\frac{q}{q_0}, \infty\right\} + \sum_{a \pmod q} \left\{\frac{1+aq_0}{qq_0}, \infty\right\} \\ &= (q-1)\{0,\infty\} - \gamma(q). \end{aligned}$$

Hence

$$a_q\left\{\frac{1}{q_0}, \infty\right\} = [(q-1)\{0,\infty\} - \gamma(q)]\cdot\widehat{\eta}.$$

Substituting $q = q_0$ and dividing gives

$$\frac{a_q}{a_{q_0}} = \frac{[(q-1)\{0,\infty\} - \gamma(q)]\cdot\widehat{\eta}}{[(q_0-1)\{0,\infty\} - \gamma(q_0)]\cdot\widehat{\eta}}$$

for all q with $\chi(q) = -1$. Since $\{0,\infty\}\cdot\widehat{\eta}$ is a constant multiple of $(\gamma(p_0)\cdot\widehat{\eta})/(1 + p_0 - a_{p_0})$, the result follows. □

Remark. If the denominator of the right-hand side of the expression for b_q/b_{q_0} is zero, we choose a new value of q_0. In practice this condition is tested in the first stage, when a suitable value for q_0 is sought.

Computing a_N. We may compute the full matrix of T_N acting on $H_1^\chi(N)$ and hence express $T_N(\eta_1)$ as a $\mathbb{Q}$-linear combination of η_1 and η_2.

Lemma 5.5.4. *Let $T_N(\eta_1) = x\eta_1 + y\eta_2$ with $x, y \in \mathbb{Q}$. Then $a_N = x + ky\sqrt{-d}$.*

Proof. The element $k\sqrt{-d}\eta_1 + \eta_2$ has eigenvalue a_p for T_p and eigenvalue $a_q = k\sqrt{-d}$ for T_q and hence corresponds to the eigenform f_1, so $T_N(k\sqrt{-d}\eta_1 + \eta_2) = a_N(k\sqrt{-d}\eta_1 + \eta_2)$. Similarly $T_N(-k\sqrt{-d}\eta_1 + \eta_2) = \overline{a_N}(-k\sqrt{-d}\eta_1 + \eta_2)$. A simple calculation now shows that $x = (a_N + \overline{a_N})/2$ and $y = (a_N - \overline{a_N})/2k\sqrt{-d}$, from which the result follows. □

In practice, computing T_N directly is very time-consuming when N is large. As an alternative we may use the following trick. We have $W(f_1) = (\overline{a_N}/\sqrt{N})f_2$, or

$$N^{-1}z^{-2}f_1(-1/Nz) = \frac{\overline{a_N}}{\sqrt{N}}f_2(z).$$

Substituting $z = i/\sqrt{N}$ gives

$$f_1(i/\sqrt{N}) = -\frac{\overline{a_N}}{\sqrt{N}}f_2(i/\sqrt{N}).$$

But also $f_2(i/\sqrt{N}) = \overline{f_1(i/\sqrt{N})}$, and hence $a_N/\sqrt{N} = -\overline{w}/w$ where $w = f_1(i/\sqrt{N})$. The latter may be computed from its Fourier expansion:

$$f_1(i/\sqrt{N}) = \sum_{n=1}^{\infty} a_n \exp(-2\pi n/\sqrt{N}).$$

Hence, finally,

$$a_N = -\sqrt{N}\frac{\sum_{n=1}^{\infty} \overline{a_n} \exp(-2\pi n/\sqrt{N})}{\sum_{n=1}^{\infty} a_n \exp(-2\pi n/\sqrt{N})}. \tag{5.5.1}$$

If we have computed sufficiently many a_n with $N \nmid n$ then we are able to compute the right-hand side of (5.5.1) sufficiently accurately to be able to determine the algebraic number $a_N = a + b\sqrt{-d}$.

For example, when $N = 509$ we have $\chi(2) = -1$ and $\chi(5) = +1$, with eigenvalues $a_2 = \sqrt{-5}$ and $a_5 = -2$. Thus $d = 5$ here. We numerically evaluate the right-hand side of (5.5.1) using a_n for $n \le 1000$, $n \ne 509$, and obtain $a_{509} = -3.000\ldots - i * 22.36067977\ldots$, from which we may deduce the exact value $a_{509} = -3 - 10\sqrt{-5}$.

5.6. Computing the period lattices. So far we have a conjugate pair of eigenforms f_1, f_2 and have computed a large supply of their Fourier coefficients a_n (we used $n \le 200$ for $N = 29$, rising to $n \le 1000$ for $N = 997$). We now compute the period lattices of the normalized forms h_1, h_2 introduced in §5.3. These are the period lattices of the elliptic curves defined over $\mathbb{Q}(\sqrt{N})$ which we seek.

Fix primes $p = p_0$ and $q = q_0$ such that, as above,

$$\chi(p) = +1, \qquad T_p(f_1) = a_p f_1, \qquad T_p(f_2) = a_p f_2,$$

and

$$\chi(q) = -1, \qquad T_q(f_1) = b_q\sqrt{-d}f_1, \qquad T_q(f_2) = -b_q\sqrt{-d}f_2,$$

where $b_q \neq 0$. Let $a_N = a + b\sqrt{-d}$, so that

$$a_N\overline{a_N} = a^2 + db^2 = N.$$

Set

$$\alpha = \frac{a+\sqrt{N}}{b\sqrt{-d}}, \qquad \alpha' = \alpha^{-1} = \frac{a-\sqrt{N}}{b\sqrt{-d}};$$

and

$$\beta = \frac{a_N}{\sqrt{N}} = \frac{a+b\sqrt{-d}}{\sqrt{N}}, \qquad \beta' = \beta^{-1} = \frac{\overline{a_N}}{\sqrt{N}} = \frac{a-b\sqrt{-d}}{\sqrt{N}}.$$

Then $W(f_1) = \beta' f_2$ and $W(f_2) = \beta f_1$.

Lemma 5.6.1. *(1)* $\beta = \dfrac{\alpha+1}{\alpha-1}$; *(2)* $\alpha = \dfrac{\beta+1}{\beta-1}$.

Proof. Both statements follow from $\alpha\beta = \alpha + \beta + 1$, which is an elementary consequence of $a^2 + db^2 = N$. □

Define

$$h_1 = \frac{1}{2}(1+\alpha)f_1 + \frac{1}{2}(1-\alpha)f_2,$$
$$h_2 = \frac{1}{2}(1+\alpha')f_1 + \frac{1}{2}(1-\alpha')f_2.$$

Lemma 5.6.2. *(1) In the Fourier expansions of h_1 and h_2 the first coefficients are both 1.*
(2) $T_p(h_j) = a_p h_j$ for $j = 1, 2$.
(3) $W(h_1) = -h_1$ and $W(h_2) = +h_2$.
(4) $T_q(h_1) = \dfrac{b_q(a+\sqrt{N})}{b}h_2$ and $T_q(h_2) = \dfrac{b_q(a-\sqrt{N})}{b}h_1$.

Proof. 1. h_1 and h_2 are both affine combinations of f_1 and f_2 which have first coefficients equal to 1.

2. Immediate since $T_p(f_j) = a_p f_j$ for $j = 1, 2$.

3.

$$\begin{aligned} W(h_1) &= \frac{1}{2}(1+\alpha)W(f_1) + \frac{1}{2}(1-\alpha)W(f_2) \\ &= \frac{1}{2}(1+\alpha)\beta' f_2 + \frac{1}{2}(1-\alpha)\beta f_1 \\ &= \frac{1}{2}(\alpha-1)f_2 - \frac{1}{2}(1+\alpha)f_1 \\ &= -h_1, \end{aligned}$$

using Lemma 5.6.1. Similarly $W(h_2) = +h_2$.

4.

$$T_q(h_1) = b_q\sqrt{-d}\left(\frac{1}{2}(1+\alpha)f_1 - \frac{1}{2}(1-\alpha)f_2\right) = b_q\sqrt{-d}\alpha h_2,$$

and similarly $T_q(h_2) = b_q\sqrt{-d}\alpha' h_1$. $\square$

It follows that h_1, h_2 are defined over $\mathbb{Q}(\sqrt{N})$; in particular they are defined over $\mathbb{R}$.

Now define eigencycles $\eta_j^{\pm} \in H_1(\Gamma_\chi(N)\backslash\mathcal{H}^*, \mathbb{Z})$ with eigenvalues as follows:

$$\begin{aligned} *(\eta_j^+) &= +\eta_j^+, \\ *(\eta_j^-) &= -\eta_j^-, \\ T_p(\eta_j^{\pm}) &= a_p\eta_j^{\pm}, \\ W(\eta_1^{\pm}) &= -\eta_1^{\pm}, \\ W(\eta_2^{\pm}) &= +\eta_2^{\pm}. \end{aligned}$$

We may also assume the normalisation $\eta_2^{\pm} = T_q(\eta_1^{\pm})$. (Note that $\eta_j^{\pm}$ has the same eigenvalues as the dual element $\widehat{\eta_j}$ used in §5.5).

Define periods as follows:

$$\begin{aligned} u_j &= 2\pi i\int_{\eta_j^+} h_j(z)dz, \\ iv_j &= 2\pi i\int_{\eta_j^-} h_j(z)dz. \end{aligned}$$

Note that u_j and v_j are real since h_1 and h_2 are defined over $\mathbb{R}$, as are the cycles $\eta_j^{\pm}$. Also if $j \neq k$, then it is easy to see that $\int_{\eta_k^{\pm}} h_j = 0$.

We now show how to obtain $\mathbb{Z}$-bases for the full period lattices of the forms h_1 and h_2; note that $\mathbb{Z}u_j + i\mathbb{Z}v_j$ will (in general) only be a sublattice of finite index in the full period lattice. For $j = 1, 2$ all integral periods of h_j are rational linear combinations of u_j and iv_j. Precisely, let $\{\gamma_j \mid j = 1, \ldots, 2g\}$ be a $\mathbb{Z}$-basis for $H_1(\Gamma_\chi(N)\backslash\mathcal{H}^*, \mathbb{Z})$; then if $\gamma = \sum c_j\gamma_j$ is an integral cycle with $c = (c_1, \ldots, c_{2g}) \in \mathbb{Z}^{2g}$, we have

$$2\pi i\int_\gamma h_j(z)dz = (c\cdot\widehat{\eta_j^+})u_j + (c\cdot\widehat{\eta_j^-})iv_j;$$

here $\widehat{\eta_j^{\pm}}$ are dual eigenvectors to $\eta_j^{\pm}$. For $j = 1, 2$ let $\{(\lambda_1^{(j)}, \mu_1^{(j)}), (\lambda_2^{(j)}, \mu_2^{(j)})\}$ be a $\mathbb{Z}$-basis for the subgroup of $\mathbb{Z}^2$ generated by the columns of the $2 \times 2g$ matrix with rows $\widehat{\eta_j^+}, \widehat{\eta_j^-}$. Then the period lattice Λ_j of h_j has $\mathbb{Z}$-basis

$$\begin{aligned} \omega_1^{(j)} &= \lambda_1^{(j)}u_j + \mu_1^{(j)}v_j i, \\ \omega_2^{(j)} &= \lambda_2^{(j)}u_j + \mu_2^{(j)}v_j i. \end{aligned}$$

In fact we may take $\mu_1^{(j)} = 0$ (so that $\omega_1^{(j)} \in \mathbb{R}$) in all cases; and if Λ_j is a rectangular lattice, then we may take $\lambda_2^{(j)} = 0$ (so that $\omega_1^{(j)}$ is pure imaginary).

Remark. The cycles $\eta_j^{\pm}$ are only defined up to a scalar multiple (by their eigenvalues), but are only used above in defining the quantities u_j and v_j. If $\eta_j^{\pm}$ are replaced by scalar multiples of themselves, thus scaling up u_j and v_j, then the dual vectors $\widehat{\eta_j^{\pm}}$ are scaled *down* by the same amount, so that the integers $\lambda_k^{(j)}$ are also scaled down; and so the periods $\omega_k^{(j)}$ are unambiguously defined by the preceding equations. In practice, we will not in fact need $\eta_j^{\pm}$ at all, but will compute the dual vectors $\widehat{\eta_j^{\pm}}$ as eigenvectors for the appropriate transposed matrices.

Hence to compute the lattices Λ_j it remains to compute the four real numbers u_j, v_j $(j = 1, 2)$. So far all the calculation has been algebraic; and in fact the periods of h_2 are algebraic multiples of those of h_1.

Lemma 5.6.3.

$$\frac{u_2}{u_1} = \frac{v_2}{v_1} = b_q \frac{a - \sqrt{N}}{b}.$$

Proof. We compute $\int_{\eta_2^+} T_q(h_1)$ in two ways. For simplicity we omit the factors of $2\pi i$. First,

$$\begin{aligned} \int_{\eta_2^+} T_q(h_1) &= \int_{\eta_2^+} b_q \frac{a + \sqrt{N}}{b} h_2 \qquad \text{by Lemma 5.6.2} \\ &= b_q(a + \sqrt{N})u_2/b. \end{aligned}$$

On the other hand,

$$\int_{\eta_2^+} T_q(h_1) = \int_{T_q(\eta_2^+)} h_1 = \int_{T_q^2(\eta_1^+)} h_1 = -b_q^2 d \int_{\eta_1^+} h_1 = -b_q^2 d u_1.$$

Comparing the two expressions gives

$$\frac{u_2}{u_1} = \frac{-b_q^2 d}{b_q(a + \sqrt{N})/b} = \frac{-b_q d(a - \sqrt{N})}{(a^2 - N)/b} = \frac{b_q(a - \sqrt{N})}{b}.$$

The calculation for v_2/v_1 is similar. For future reference we also note that

$$\frac{v_1}{v_2} = \frac{b}{b_q(a - \sqrt{N})} = \frac{b(a + \sqrt{N})}{b_q(a^2 - N)} = \frac{-(a + \sqrt{N})}{dbb_q}. \quad \square$$

We now show how to compute the periods u_1 and v_2 numerically. The computation of u_1 is simpler, since the W-eigenvalue of h_1 is -1.

Proposition 5.6.4.

$$u_1 = \frac{(1+p-a_p)L(h_1,1)}{\gamma(p)\cdot\widehat{\eta_1^+}}, \qquad \text{and} \qquad u_2 = u_1 b_q(a-\sqrt{N})/b,$$

where $\gamma(p) = \sum_{a \pmod p}\{0, a/p\}$*, expressed as a* $\mathbb{Z}$*-linear combination of the* $\mathbb{Z}$*-basis* $\{\gamma_1, \dots, \gamma_{2g}\}$*, and* $L(h_1,1)$ *is given by*

$$L(h_1,1) = 2\sum_{n=1}^{\infty}\frac{a_n}{n}\exp(-2\pi n/\sqrt{N}).$$

Proof. Identical to the method of [4, (2.8.3), (2.11.1)]. □

For h_2 we must first twist with a suitable quadratic character.

Proposition 5.6.5. *Let* l *be a prime congruent to 3 modulo 4, and* ψ *the quadratic character modulo* l*. Let* $h_2\otimes\psi$ *be the twist of* h_2 *by* ψ*. Then*
(1) $h_2\otimes\psi$ *is a cusp form of level* Nl^2 *satisfying* $W_{Nl^2}(h_2\otimes\psi) = -h_2\otimes\psi$*;*
(2)

$$L(h_2\otimes\psi) = 2\sum_{n=1}^{\infty}\frac{\psi(n)a_n}{n}\exp(-2\pi n/l\sqrt{N});$$

(3)

$$v_2 = \frac{-\sqrt{l}L(h_2\otimes\psi,1)}{\gamma(l,\psi)\cdot\widehat{\eta_2^-}}, \qquad \text{and} \qquad v_1 = -v_2(a+\sqrt{N})/dbb_q,$$

where $\gamma(l,\psi) = \sum_{a \pmod l}\psi(a)\{0, a/l\}$*.*

Proof. 1. That $h_2\otimes\psi$ is a form at level Nl^2 is standard. The W_{Nl^2}-eigenvalue may be computed by an argument similar to that used for $\Gamma_0(N)$ forms in [15]. We have

$$h_2\otimes\psi = \frac{g(\psi)}{l}\sum_{a=1}^{l-1}\psi(-a)h_2\left|\begin{pmatrix} l & a\\ 0 & l\end{pmatrix}\right.$$

where $g(\psi)$ is the Gauss sum. Hence

$$h_2\otimes\psi\left|\begin{pmatrix} 0 & -1\\ Nl^2 & 0\end{pmatrix}\right. = l^{-1}g(\psi)\sum_{a=1}^{l-1}\psi(-a)h_2\left|\begin{pmatrix} l & a\\ 0 & l\end{pmatrix}\begin{pmatrix} 0 & -1\\ Nl^2 & 0\end{pmatrix}\right..$$

Now

$$\begin{pmatrix} l & a\\ 0 & l\end{pmatrix}\begin{pmatrix} 0 & -1\\ Nl^2 & 0\end{pmatrix} = \begin{pmatrix} l & 0\\ 0 & l\end{pmatrix}\begin{pmatrix} 0 & -1\\ N & 0\end{pmatrix}\begin{pmatrix} l & b\\ -Na & c\end{pmatrix}\begin{pmatrix} l & -b\\ 0 & l\end{pmatrix}$$

where for $1 \le a \le l-1$ we choose b, c such that $Nab + lc = 1$. Note that $Nab \equiv 1 \pmod{l}$, so $\psi(-a) = \psi(-Nb)$, and that $lc \equiv 1 \pmod{N}$, so that $\chi(c) = \chi(l)$. Then

$$\begin{aligned} h_2 \otimes \psi \,|W_{Nl^2} &= l^{-1} g(\psi) \sum \psi(-a) h_2 \left| \begin{pmatrix} l & b \\ -Na & c \end{pmatrix} \begin{pmatrix} l & -b \\ 0 & l \end{pmatrix} \right. \\ &\qquad \text{(using } h_2 | W_N = h_2\text{)} \\ &= l^{-1} g(\psi) \chi(l) \sum \psi(-a) h_2 \left| \begin{pmatrix} l & -b \\ 0 & l \end{pmatrix} \right. \\ &\qquad \text{(since } \begin{pmatrix} l & b \\ -Na & c \end{pmatrix} \in \Gamma_0(N)\text{)} \\ &= l^{-1} g(\psi) \chi(l) \psi(-N) \sum \psi(b) h_2 \left| \begin{pmatrix} l & -b \\ 0 & l \end{pmatrix} \right. \\ &= \chi(l) \psi(-N) h_2 \otimes \psi. \end{aligned}$$

Hence the W_{Nl^2}-eigenvalue of $h_2 \otimes \psi$ is

$$\chi(l)\psi(-N) = \left(\frac{l}{N}\right)\left(\frac{-N}{l}\right) = \left(\frac{N}{l}\right)\left(\frac{-N}{l}\right) = \left(\frac{-1}{l}\right) = -1.$$

Parts (2) and (3) of the proposition now follow as in [4]. Note that $\gamma(l, \psi)$ is in the integral homology since

$$\begin{aligned} \gamma(l,\psi) &= \sum_{a \pmod{l}} \psi(a)\{0, a/l\} \\ &= \sum_{a \pmod{l}} \psi(a)\{1/l, a/l\}. \quad \square \end{aligned}$$

This completes the method of numerically computing generators for the period lattices Λ_1, Λ_2.

5.7. The elliptic curves. We now have, to a certain precision, $\mathbb{Z}$-bases $\{\omega_1^{(j)}, \omega_2^{(j)}\}$ for the lattices Λ_j $(j = 1, 2)$ of periods of the normalised cusp forms h_1, h_2 defined over $\mathbb{Q}(\sqrt{N})$. If we need greater precision later we merely have to compute more Hecke eigenvalues and recompute the periods from the data obtained in the previous section. If necessary we adust these $\mathbb{Z}$-bases so that each $\omega_2^{(j)}/\omega_1^{(j)}$ lies in the usual fundamental region for $SL(2, \mathbb{Z})$ in the upper half-plane.

We now use the rapidly convergent series to compute the lattice covariants $c_4^{(j)}$ and $c_6^{(j)}$. These quantities are *a priori* elements of $\mathbb{Q}(\sqrt{N})$, with $c_4^{(2)}, c_6^{(2)}$ the Galois conjugates of $c_4^{(1)}, c_6^{(1)}$, so that $c_4^{(1)} + c_4^{(2)}$, $(c_4^{(1)} - c_4^{(2)})/\sqrt{N}$, $c_6^{(1)} + c_6^{(2)}$, $(c_6^{(1)} - c_6^{(2)})/\sqrt{N}$ are rational numbers for which we have decimal approximations.

In all cases computed ($N \le 1000$) we found these four numbers to be integers; more precisely, their computed values are integral to at least 20 decimal places.

Equivalently, the computed values of $c_4^{(j)}$ and $c_6^{(j)}$ are extremely close to conjugate pairs of elements of the ring of integers of $\mathbb{Q}(\sqrt{N})$.

Let c_4 and c_6 be the exact algebraic integers obtained by rounding the approximate values computed for $c_4^{(1)}$ and $c_6^{(1)}$. Set $\Delta = (c_4^3 - c_6^2)/1728$ and $j = c_4^3/\Delta$. Then we have an elliptic curve E_1' defined over $\mathbb{Q}(\sqrt{N})$ with j-invariant j and integral covariants c_4 and c_6. In every case, j is integral and E_1' has everywhere good reduction. But also we know that the actual modular curve $E_1 = \mathbb{C}/\Lambda_1$ has everywhere good reduction and hence has integral j-invariant equal to

$$j(E_1) = \frac{1728(c_4^{(1)})^3}{(c_4^{(1)})^3 - (c_6^{(1)})^2}.$$

Hence j, the integral value obtained by numerical approximation, must be exactly equal to $j(E_1)$. Thus E_1 and E_1' both have everywhere good reduction, and also have the same j-invariant; it follows from a result of Ishii (see [13, Lemma 1.5]) that in fact $E_1 = E_1'$. Hence we have determined the curve E_1, and its conjugate E_2, exactly.

6. Results

We have carried out all the calculations described in the previous section for all 80 primes N congruent to 1 modulo 4 and less than 1000. In 15 cases we found a pair of newforms f_1, f_2 satisfying our conditions, namely for

$$N = 29, 37, 41, 109, 157, 229, 257, 337, 349, 397, 461, 509, 877, 881, 997.$$

In no case did we find more than one such pair at the same level.

In Table 1 we give, for each of these levels N,

(1) The positive integer d such that the Hecke eigenvalues lie in $\mathbb{Q}(\sqrt{-d})$.
(2) The Hecke eigenvalue a_p of f_1 for each of the first 15 primes p; when $\chi(p) = -1$ these are given in the form $b\omega$, where $w = \sqrt{-d}$ if $d \equiv 1, 2 \pmod 4$, or $w = (1 + \sqrt{-d})/2$ if $d \equiv 3 \pmod 4$.
(3) The value a_N.

In Table 2 we give the computed values for each curve E_1 found. We list the values of c_4, c_6, and the j-invariant, in the form $x + y\alpha$ where $\alpha = (1 + \sqrt{N})/2$. We also give the norm of the discriminant Δ in factorized form: this norm is not usually 1 as the curves are not usually minimal (see remarks below).

Finally, in Table 3, we give global minimal equations for the curves, where these exist. All but two are taken from [10]; we give Pinch's code in the second column (a prime here indicates the conjugate of the corresponding curve in [10]). Curves 461A and 509B are new; the equations were computed by Pinch from the c_4 and c_6 values in Table 2.

Comparing our list of curves with the table in Pinch's thesis [10], we make the following observations.

$N = 461$. This curve does not appear in [10], where there are no curves given over $\mathbb{Q}(\sqrt{461})$.

$N = 509$. Our curve is not the same as Pinch's 509A. Indeed, the latter is not isogenous to its conjugate, so could not arise via this construction. However the L-series of these two curves are congruent modulo 5 (see [11]).

$N = 733$. Pinch's 733A is again not isogenous to its conjugate; we found no curves at this level.

Our computations agree with these of Shiota at levels 29, 37, 41; Shiota computed j but not c_4 and c_6 separately.

While we always obtain integral equations for the curves (that is, c_4 and c_6 are integral) we do not always obtain a minimal equation: Δ is usually not a unit. This is in marked contrast with the situation for modular elliptic curves over $\mathbb{Q}$ attached to rational newforms for $\Gamma_0(N)$, where in all known cases the period lattice of the normalized cusp form f is that of a global minimal equation for the modular curve E_f. Indeed, in two cases ($N = 229$ and $N = 257$) there is no global minimal equation (the class number is 3 in both these cases).

Non-minimality at the primes dividing 2 and 3 in $\mathbb{Q}(\sqrt{N})$ seems to follow a pattern. Within the range of our table we have

- Minimality at primes above 2 $\iff$ $N \equiv 1 \pmod{16}$.
- Minimality at primes above 3 $\iff$ $N \equiv 1 \pmod{3}$.

It would be interesting to know whether this pattern continues, and if there is a reason for it.

We also find nonminimality at a prime dividing 5 at levels 509 and 881; but it is not clear what the pattern is here, if any.

Table 1 here

Table 2 here

Table 3 here

REFERENCES

[1] A.O.L.Atkin and W.Li. Twists of newforms and pseudo-eigenvalues of Hecke operators. *Invent. Math.* **48** (1978), 221–243.

[2] B.J.Birch and W.Kuyk (eds.). *Modular Functions of One Variable IV*, Lecture Notes in Math. vol. 476 (Springer-Verlag, 1975).

[3] W.Casselman. Abelian varieties with many endomorphisms and a conjecture of Shimura's. *Invent. Math.* **12** (1971), 225–236.

[4] J.E.Cremona. Modular elliptic curves and the Birch–Swinnerton-Dyer conjecture. (preprint, 1990).

[5] J.E.Cremona. Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields. *J. London Math. Soc.* (to appear).

[6] P.Deligne and M.Rapoport. Les schemas des modules de courbes elliptiques. In *Modular functions of one variable II*, Lecture Notes in Math. vol. 349 (Springer-Verlag,1973), pp. 143–316.

[7] S.Lang. *Introduction to modular forms.* (Springer-Verlag, 1976).

[8] Ju.I.Manin. Parabolic points and zeta-functions of modular curves. *Math. USSR-Izv.* **6** (1972), 19–64.

[9] H.Naganuma. On the coincidence of two Dirichlet series associated with cusp forms of Hecke's "Neben" type and Hilbert modular forms over a real quadratic field. *J. Math. Soc. Japan* **25** (1973), 547–55.

[10] R.G.E.Pinch. Elliptic curves over number fields. D.Phil. thesis, Oxford University (1982).

[11] R.G.E.Pinch. Elliptic curves with everywhere good reduction. (preprint).

[12] G.Shimura. *Introduction to the arithmetic theory of automorphic functions.* (Publ. Math. Soc. Japan No.11, 1971).

[13] K.Shiota. On the explicit models of Shimura's elliptic curves. *J. Math. Soc. Japan* (no.4) **38** (1986), 649–658.

[14] G.Stevens. Stickelberger elements and modular parametrizations of elliptic curves. *Invent. Math.* **948** (1989), 75–106.

[15] H.P.F.Swinnerton Dyer and B.J.Birch. Elliptic curves and modular functions. In *Modular Functions of One Variable IV*, Lecture Notes in Math. vol. 476 (Springer-Verlag, 1975).

Table 1. Hecke eigenvalues

N	d	a_2	a_3	a_5	a_7	a_{11}	a_{13}	a_{17}	a_{19}	a_{23}	a_{29}	a_N
29	5	ω	$-\omega$	-3	2	ω	-1	-2ω	0	6	$-3+2\omega$	$-3+2\omega$
37	1	2ω	-1	-2ω	3	-3	-6ω	2ω	6ω	4ω	-4ω	$-1+6\omega$
41	2	-1	2ω	2	-2ω	2ω	-4ω	0	2ω	0	-4ω	$-3+4\omega$
109	3	ω	2	-3	2	-3ω	0	2ω	-3ω	$-\omega$	-3	$-1+6\omega$
157	1	ω	-2	-4ω	-3ω	6	-5	3	0	-5ω	4ω	$-11-6\omega$
229	5	ω	1	3	0	3	0	-3	-1	-2ω	-2ω	$7+6\omega$
257	2	-1	ω	-2ω	ω	0	2	4	3ω	4	4	$-15-4\omega$
337	2	1	0	2ω	4	3ω	4	4ω	-3ω	$-\omega$	2ω	$-7+12\omega$
349	5	0	-1	2	-2ω	-2ω	2ω	3	-5	1	1	$-13-6\omega$
397	1	ω	2	-2ω	-3ω	0	0	4ω	-2	6	-3	$-19+6\omega$
461	5	ω	0	1	ω	ω	0	3	0	-6	2ω	$21+2\omega$
509	5	ω	ω	-2	ω	-2	0	7	0	6	-5	$-3-10\omega$
877	1	2ω	1	-4ω	1	-4ω	0	-2ω	-6ω	0	6	$-29-6\omega$
881	2	1	ω	4	3ω	-4	-2	4ω	0	-5ω	-2ω	$9+20\omega$
997	3	0	1	2ω	0	2ω	-1	-2ω	4	-3	4ω	$-5+18\omega$

Table 2. Elliptic curve data – computed values

N	c_4	c_6	Norm(Δ)	j
29	$32+15\alpha$	$299+140\alpha$	1	$-7688-3515\alpha$
37	$144+16\alpha$	$-1368-224\alpha$	3^{12}	4096
41	17	$103+64\alpha$	-1	$181781-49130\alpha$
109	$27+25\alpha$	$999+280\alpha$	3^{12}	$-1243-585\alpha$
157	$832+143\alpha$	$46955+8140\alpha$	3^{12}	-2197
229	$2173-235\alpha$	$-124369+15988\alpha$	3^{12}	$7334137-888615\alpha$
257	$-607-81\alpha$	$-15025-1999\alpha$	-2^{12}	$873-82\alpha$
337	$117-33\alpha$	$22599+1701\alpha$	$-2^{12}3^{12}$	$14121-1458\alpha$
349	$2112+160\alpha$	$84840+11680\alpha$	3^{12}	$1983152128-201523200\alpha$
397	$-1980-209\alpha$	$69759+7372\alpha$	3^{12}	1331
461	$3876-345\alpha$	$-333693+29700\alpha$	1	$-1595511+142155\alpha$
509	$478856-35769\alpha$	$-426923825+34954300\alpha$	5^{12}	-31541630772320810747 $+26774409257511496 75\alpha$
877	$46480+3248\alpha$	$-14405560-1006880\alpha$	3^{12}	1404928
881	$5405-321\alpha$	$-532025+32605\alpha$	$-2^{12}5^{12}$	$270553-17650\alpha$
997	$43936+2528\alpha$	$12181064+776608\alpha$	3^{24}	$32253902848+2109800448\alpha$

Table 3. Elliptic curves – minimal models

Curve	a_1	a_2	a_3	a_4	a_6
29B	α	$-2-2\alpha$	$1-\alpha$	$10+\alpha$	$-3-\alpha$
37A	0	2	1	$-19-8\alpha$	$28+11\alpha$
41C′	1	α	α	3	-2
109A′	$2-\alpha$	1	$-\alpha$	$-244-59\alpha$	$-3189-689\alpha$
157A	$-1-\alpha$	0	$1+\alpha$	$-5593-974\alpha$	$-350775-60846\alpha$
229A′	No global minimal model				
257A	No global minimal model				
337A	-1	-1	0	$-416+43\alpha$	$-4249+439\alpha$
349A′	0	2	1	$-11906+1210\alpha$	$681129-69215\alpha$
397A	-1	1	$-\alpha$	$1430031-136646\alpha$	$-486945568+46542441\alpha$
461A	α	$-1-\alpha$	α	$140-7\alpha$	$393-14\alpha$
509B	$1+\alpha$	0	$1+\alpha$	$-4051846+343985\alpha$	$4312534180-366073300\alpha$
877A′	0	1	1	-262601139278 -18354612024α	74473105793336434 -5205327618971097α
881A	-1	0	1	$-358-25\alpha$	$11329+790\alpha$
997A	0	1	-1	$-125389-8202\alpha$	$-24602589-1609311\alpha$

Department of Mathematics, University of Exeter, North Park Road, Exeter EX4 4QE, U.K.

E-mail address: cremona@exeter.ac.uk