MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 211
JULY 1995, PAGES 1235-1250

COMPUTING THE DEGREE OF THE MODULAR PARAMETRIZATION OF A MODULAR ELLIPTIC CURVE

J. E. CREMONA

ABSTRACT. The Weil–Taniyama conjecture states that every elliptic curve $E/\mathbb{Q}$ of conductor N can be parametrized by modular functions for the congruence subgroup $\Gamma_0(N)$ of the modular group $\Gamma = PSL(2, \mathbb{Z})$. Equivalently, there is a nonconstant map φ from the modular curve $X_0(N)$ to E. We present here a method of computing the degree of such a map φ for arbitrary N. Our method, which works for all subgroups of finite index in Γ and not just $\Gamma_0(N)$, is derived from a method of Zagier published in 1985; by using those ideas, together with techniques which have recently been used by the author to compute large tables of modular elliptic curves, we are able to derive an explicit and general formula which is simpler to implement than Zagier's. We discuss the results obtained, including a table of degrees for all the modular elliptic curves of conductors up to 200.

1. INTRODUCTION

The Weil–Taniyama conjecture states that every elliptic curve $E/\mathbb{Q}$ of conductor N can be parametrized by modular functions for the congruence subgroup $\Gamma_0(N)$ of the modular group $\Gamma = PSL(2, \mathbb{Z})$. Equivalently, there is a nonconstant map φ from the modular curve $X_0(N)$ to E. We present here a method of computing the degree of such a map φ for arbitrary N. Our method is derived from a method of Zagier in [5]; by using those ideas, together with techniques which have been used by the author to compute large tables of modular elliptic curves (see [2]), we are able to derive an explicit formula which is in general much simpler to implement than Zagier's, for arbitrary subgroups of finite index in Γ. To implement this formula, one needs to have explicit coset representatives for the subgroup, but it is not necessary to determine an explicit fundamental domain for its action on the upper half-plane $\mathcal{H}$. In particular, it is simple to implement for $\Gamma_0(N)$ for arbitrary N, in contrast with Zagier's formula, which is only completely explicit for N prime.

In the following section, we review the necessary background on modular parametrizations of elliptic curves. In §3 we introduce some machinery concerning coset representatives and fundamental regions, and state the main result (Theorem 3). This formula for $\deg(\varphi)$ is proved in §4. In §5 we discuss the implementation of the method for the case of $\Gamma_0(N)$, and the results of

Received by the editor February 7, 1994.
1991 *Mathematics Subject Classification*. Primary 11G05, 14H52, 14Q05; Secondary 11F11, 11F33, 11F67.

a systematic computation of the degree of the parametrization of all modular elliptic curves of conductors up to 3000, with a table of the results up to 200.

2. Modular parametrizations of elliptic curves

Let $\Gamma = PSL(2, \mathbb{Z})$ be the modular group, and Γ_0 a subgroup of Γ of finite index. Both act discretely on the upper half-plane $\mathscr{H}$ and the extended upper half-plane $\mathscr{H}^* = \mathscr{H} \cup \mathbb{Q} \cup \{\infty\}$ obtained by adjoining the cusps $\mathbb{Q} \cup \{\infty\}$, which form a single Γ-orbit. The quotient $X = X_{\Gamma_0} = \Gamma_0 \backslash \mathscr{H}^*$ can be given the structure of a Riemann surface; in the case we are most interested in, where Γ_0 is a congruence subgroup, X is also an algebraic curve defined over a number field, and is called a modular curve.

An elliptic curve E defined over $\mathbb{Q}$ is called a modular elliptic curve if there is a nonconstant map $\varphi: X \to E$ for some modular curve X. The pull-back of the unique (up to scalar multiplication) holomorphic differential on E is then of the form $2\pi i f(\tau) d\tau$, where $f(\tau)$ is a holomorphic cusp form of weight 2 for Γ_0. According to the Weil–Taniyama conjecture, this should be the case for every elliptic curve defined over $\mathbb{Q}$, with $\Gamma_0 = \Gamma_0(N)$, where N is the conductor of E. Moreover, the cusp form $f(\tau)$ should be a newform in the usual sense. [It is also conjectured that $f(\tau)$ should be normalized, with first coefficient equal to 1. In general, f will be a rational constant c times a normalized newform. In the sequel it will be irrelevant whether the "Manin constant" c is equal to 1, since we define the curve E_f below in terms of a normalized newform, and it is irrelevant whether or not this curve is minimal in the usual sense.]

We will suppose that we are given a normalized cusp form $f(\tau)$ of weight 2 for Γ_0. Since the differential $f(\tau)d\tau$ is holomorphic, the function

$$\varphi_1(\tau) = 2\pi i \int_{\infty}^{\tau} f(\zeta) d\zeta \quad (\tau \in \mathscr{H}^*)$$

is well defined (independent of the path from ∞ to τ). Also, for $\gamma \in \Gamma_0$, the function

$$\omega(\gamma) = \varphi_1(\gamma(\tau)) - \varphi_1(\tau) = 2\pi i \int_{\tau}^{\gamma(\tau)} f(\zeta) d\zeta$$

is independent of τ, and defines a function

$$\omega: \Gamma_0 \to \mathbb{C},$$

which is a homomorphism. The image Λ_f of this map will, under suitable hypotheses on f which we will assume to hold, be a lattice of rank 2 in $\mathbb{C}$, so that $E_f = \mathbb{C}/\Lambda_f$ is an elliptic curve. Hence φ_1 induces a map

$$\varphi: X = \Gamma_0 \backslash \mathscr{H}^* \to E_f = \mathbb{C}/\Lambda_f$$

via

$$\varphi(\tau \bmod \Gamma_0) = \varphi_1(\tau) \mod \Lambda_f.$$

The period map $\omega: \Gamma_0 \to \Lambda_f$ is surjective (by definition) and its kernel contains all elliptic and parabolic elements of Γ_0. We may write $\Lambda_f = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\operatorname{Im}(\omega_2/\omega_1) > 0$. Then

$$\omega(\gamma) = n_1(\gamma)\omega_1 + n_2(\gamma)\omega_2,$$

where $n_1, n_2: \Gamma_0 \to \mathbb{Z}$ are homomorphisms. It is important to observe here that these functions are explicitly and easily computable in terms of modular symbols: for the case $\Gamma_0 = \Gamma_0(N)$, see [2] for details. Alternatively, given sufficiently many Fourier coefficients of the cusp form $f(\tau)$, we may evaluate the period integrals $\varphi_1(\tau)$ to sufficient precision that (assuming that the fundamental periods ω_1 and ω_2 are also known to some precision) one can determine the values of $n_1(\gamma)$ and $n_2(\gamma)$ for all $\gamma \in \Gamma_0$. The latter approach is used in [5]. The advantage of the modular symbol approach here is that exact values are obtained directly, and that it is not necessary to compute (or even know) any Fourier coefficients of $f(\tau)$. On the other hand, it becomes computationally infeasible to carry out the modular symbol computations when the index of Γ_0 in Γ is too large, whereas the approximate approach can still be used, provided that one has an explicit equation for the curve E at hand, from which one can compute the periods and the Fourier coefficients in terms of traces of Frobenius (assuming that E is modular and defined over $\mathbb{Q}$). This method was used, for example, to compute $\deg(\varphi)$ for the curve of rank 3 with conductor 5077, in [5].

The special case we are particularly interested in is where $\Gamma_0 = \Gamma_0(N)$ and $f(\tau)$ is a normalized newform for $\Gamma_0(N)$. Then $f(\tau)$ is a Hecke eigenform with rational integer eigenvalues and therefore rational integer Fourier coefficients. The periods of $2\pi i f(\tau)$ do in this case form a lattice Λ_f, and the modular elliptic curve $E_f = \mathbb{C}/\Lambda_f$ is defined over $\mathbb{Q}$ and has conductor N.

In order to compute the degree of the map $\varphi: X \to E_f$, the idea used in [5] is to compute the Petersson norm $||f||$ in two ways. The first way involves $\deg(\varphi)$ explicitly, while the second expresses it as a sum of terms involving periods, which can be evaluated as above.

Proposition 1. *Let $f(\tau)$ be a cusp form for Γ_0 as above, and $\varphi: X \to E_f$ the associated modular parametrization. Then*

$$4\pi^2||f||^2 = \deg(\varphi)\mathrm{Vol}(E_f).$$

Proof. From the definition

$$||f||^2 = \int_X |f(\tau)|^2 du dv \quad (\text{where } \tau = u + iv)$$

we have, following [5] exactly,

$$\begin{aligned} 4\pi^2||f||^2 &= 2i\pi^2 \int_X f(\tau)d\tau \wedge \overline{f(\tau)d\tau} \\ &= \frac{i}{2}\int_X (2\pi i f(\tau)d\tau) \wedge \overline{(2\pi i f(\tau)d\tau)} \\ &= \frac{i}{2}\int_X \varphi^*(dz) \wedge \overline{\varphi^*(dz)}, \end{aligned}$$

since $\varphi^*(dz) = 2\pi i f(\tau)d\tau$, where $z = x + iy$ is the coordinate on E_f,

$$\begin{aligned} &= \frac{i}{2}\deg(\varphi)\int_{E_f} dz \wedge \overline{dz} \\ &= \deg(\varphi)\int_{E_f} dx dy \\ &= \deg(\varphi)\mathrm{Vol}(E_f), \end{aligned}$$

as required. □

Remark. In terms of the fundamental periods ω_1, ω_2 of E_f, the volume is given by

$$\mathrm{Vol}(E_f) = |\mathrm{Im}\,(\overline{\omega_1}\omega_2)|\,.$$

More generally, if ω, $\omega' \in \Lambda_f$, with $\omega = n_1(\omega)\omega_1 + n_2(\omega)\omega_2$ and $\omega' = n_1(\omega')\omega_1 + n_2(\omega')\omega_2$, then (up to sign) we have

$$\mathrm{Im}\,(\overline{\omega}\omega') = \mathrm{Vol}(E_f)\cdot\begin{vmatrix} n_1(\omega) & n_1(\omega') \\ n_2(\omega) & n_2(\omega') \end{vmatrix}.$$

3. Coset representatives and fundamental domains

Let $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ be the usual generators for Γ, so that S has order 2 and $TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ has order 3.

As fundamental domain for Γ we may take the triangular region $\mathscr{F}$ with vertices at 0, $\rho = (1+i\sqrt{3})/2$, and ∞. Since TS fixes ρ and permutes 0, ∞ and 1 cyclically, the three transforms of $\mathscr{F}$ by I, TS and $(TS)^2$ fit together around ρ to form an "ideal triangle" $\mathscr{T}$ with vertices at 0, 1 and ∞. Let $\langle\gamma\rangle$ denote the transform of $\mathscr{T}$ by γ for $\gamma \in \Gamma$. Then these triangles $\langle\gamma\rangle$ form a triangulation of the upper half-plane $\mathscr{H}$, whose vertices are precisely the cusps: the vertices of $\langle\gamma\rangle$ are the cusps $\gamma(0)$, $\gamma(1)$ and $\gamma(\infty)$. Note that

$$\langle\gamma\rangle = \langle\gamma TS\rangle = \left\langle\gamma(TS)^2\right\rangle$$

but that otherwise the triangles are distinct. The triangle $\langle\gamma\rangle$ has three (oriented) edges; in the modular symbol notation of [2], these are

$$(\gamma) = \{\gamma(0),\, \gamma(\infty)\}\,,$$
$$(\gamma TS) = \{\gamma TS(0),\, \gamma TS(\infty)\} = \{\gamma(\infty),\, \gamma(1)\}\,,$$

and

$$(\gamma(TS)^2) = \{\gamma(TS)^2(0),\, \gamma(TS)^2(\infty)\} = \{\gamma(1),\, \gamma(0)\}.$$

Here the modular symbol $\{\alpha,\, \beta\}$ denotes a geodesic path in $\mathscr{H}^*$ from α to β.

Assume, for simplicity, that Γ_0 has no nontrivial elements of finite order, i.e., no conjugates of either S or TS. (This assumption is merely for ease of exposition; in fact, it is easy to see that elliptic elements of Γ_0 contribute nothing to the formula in Theorem 2 below in any case.) Choose, once and for all, a set $\mathscr{S}$ of right coset representatives for Γ_0 in Γ, such that $\gamma \in \mathscr{S}$ implies $\gamma TS \in \mathscr{S}$; this is possible since, by hypothesis, Γ_0 contains no conjugates of TS.

Let $\mathscr{S}'$ be a subset of $\mathscr{S}$ which contains exactly one of each triple γ, γTS, $\gamma(TS)^2$, so that $\mathscr{S} = \mathscr{S}' \cup \mathscr{S}'TS \cup \mathscr{S}'(TS)^2$. Then a fundamental domain for the action of Γ_0 on $\mathscr{H}$ is given by

$$\mathscr{F}_{\Gamma_0} = \bigcup_{\gamma\in\mathscr{S}'} \langle\gamma\rangle\,.$$

In general, this set need not be connected, but this does not matter for our purposes: it can be treated as a disjoint union of triangles, whose total boundary is the sum of the oriented edges (γ) for $\gamma \in \mathcal{S}$.

The key idea in our algebraic reformulation of Zagier's method is to make use of the coset action of Γ on the set $\mathcal{S}$. We introduce notation for the actions of the generators S and T of Γ.

Action of S. For each $\gamma \in \mathcal{S}$ we set $\gamma S = s(\gamma)\sigma(\gamma)$, where $s: \mathcal{S} \to \Gamma_0$ is a function and $\sigma: \mathcal{S} \to \mathcal{S}$ is a permutation. Since S^2 is the identity, the same is true of σ, and $s(\sigma(\gamma)) = s(\gamma)^{-1}$. For brevity we will write $\gamma^* = \sigma(\gamma)$, so that $\gamma^{**} = \gamma$ for all $\gamma \in \mathcal{S}$.

Note that the triangles $\langle\gamma\rangle$ and $\langle\gamma S\rangle$ are adjacent in the triangulation of $\mathcal{H}$, since they share the common side $(\gamma) = \{\gamma(0), \gamma(\infty)\} = -(\gamma S)$. (Here the minus sign denotes reverse orientation.) However, since in general we do not have $\gamma S \in \mathcal{S}$, in the fundamental domain $\mathcal{F}_{\Gamma_0}$ for Γ_0 it is the triangles $\langle\gamma\rangle$ and $\langle\gamma^*\rangle$ which are glued together by the element $s(\gamma) \in \Gamma_0$ which takes (γ^*) to $-(\gamma)$ (the orientation is reversed).

Action of T. Similarly, for $\gamma \in \mathcal{S}$ we set $\gamma T = t(\gamma)\tau(\gamma)$ with $t(\gamma) \in \Gamma_0$ and $\tau(\gamma) \in \mathcal{S}$. The permutation τ of $\mathcal{S}$ plays a vital part in what follows. Lemma 1 will not be used later, but is included for its own interest as it explains the geometric significance of this algebraic permutation.

Lemma 1. (a) *Two elements γ and γ' of $\mathcal{S}$ are in the same τ-orbit if and only if the cusps $\gamma(\infty)$ and $\gamma'(\infty)$ are Γ_0-equivalent.*

(b) *The length of the τ-orbit of an element $\gamma \in \mathcal{S}$ is the width of the cusp $\gamma(\infty)$ of Γ_0.*

Proof. (a) γ and γ' are in the same τ-orbit if and only if $\gamma_0 = \gamma' T^j \gamma^{-1} \in \Gamma_0$ for some j, which is if and only if $\gamma_0\gamma(\infty) = \gamma'(\infty)$, since the stabilizer of ∞ in Γ is the subgroup generated by T.

(b) The length of the orbit of γ is the least $k > 0$ such that $\gamma_0 = \gamma T^k \gamma^{-1} = (\gamma T \gamma^{-1})^k \in \Gamma_0$, which is the width of the cusp $\gamma(\infty)$, since the stabilizer of $\gamma(\infty)$ in Γ is generated by $\gamma T \gamma^{-1}$. □

Thus there is a one–one correspondence between the orbits of τ on $\mathcal{S}$ and the classes of Γ_0-inequivalent cusps, with the length of each orbit being the width of the corresponding cusp.

In each τ-orbit in $\mathcal{S}$, we choose an arbitrary base point γ_1, and set $\gamma_{j+1} = \tau(\gamma_j)$ for $1 \le j \le k$, where k is the length of the orbit and $\gamma_{k+1} = \gamma_1$. Thus $\gamma_j T = t(\gamma_j)\gamma_{j+1}$, so that

$$\gamma_1 T^j = t(\gamma_1)t(\gamma_2)\cdots t(\gamma_j)\gamma_{j+1}.$$

In particular, $\gamma_1 T^k = \gamma_0\gamma_1$, where

$$\gamma_0 = t(\gamma_1)t(\gamma_2)\cdots t(\gamma_k) \in \Gamma_0.$$

Lemma 2. *There holds*

$$\sum_{j=1}^{k} \omega(t(\gamma_j)) = 0,$$

where the sum is over a complete τ-orbit on $\mathcal{S}$ and where ω is the period map of the previous section.

Proof. Since $\gamma_0 = \gamma_1 T^k \gamma_1^{-1}$ is parabolic, we have $\omega(\gamma_0) = 0$. Since ω is a homomorphism, the result follows. □

Lemma 3. *We have $s(\gamma TS) = t(\gamma)$ for all $\gamma \in \mathcal{S}$.*

Proof. We have $t(\gamma)\tau(\gamma) = \gamma T = (\gamma TS)S = s(\gamma TS)\sigma(\gamma TS)$, since $\gamma TS \in \mathcal{S}$. Hence $t(\gamma) = s(\gamma TS)$, and also $\tau(\gamma) = \sigma(\gamma TS)$. □

Write $\gamma \prec \gamma'$ if γ and γ' are in the same τ-orbit in $\mathcal{S}$, and γ precedes γ' in the fixed ordering determined by choosing a base point for each orbit. In the notation above, $\gamma \prec \gamma'$ if and only if $\gamma = \gamma_i$ and $\gamma' = \gamma_j$, where $1 \le i < j \le k$.

We can now state our main results.

Theorem 2. *Let f be a cusp form of weight 2 for Γ_0 with associated period function $\omega : \Gamma_0 \to \mathbb{C}$. Then (the square of) the Petersson norm of f is given by*

$$||f||^2 = \frac{1}{8\pi^2} \sum_{\gamma \prec \gamma'} \operatorname{Im}(\omega(t(\gamma))\overline{\omega(t(\gamma'))}).$$

Here the sum is over all ordered pairs $\gamma \prec \gamma'$ in $\mathcal{S}$ which are in the same orbit of the permutation τ of $\mathcal{S}$ induced by right multiplication by T.

Combining this result with Proposition 1 of the previous section, we immediately obtain our explicit formula for the degree of the modular parametrization φ.

Theorem 3. *With the above notation,*

$$\deg(\varphi) = \frac{1}{2\operatorname{Vol}(E_f)} \sum_{\gamma \prec \gamma'} \operatorname{Im}(\omega(t(\gamma))\overline{\omega(t(\gamma'))}) = \frac{1}{2} \sum_{\gamma \prec \gamma'} \begin{vmatrix} n_1(t(\gamma)) & n_1(t(\gamma')) \\ n_2(t(\gamma)) & n_2(t(\gamma')) \end{vmatrix}.$$

Hence, to compute $\deg(\varphi)$, we only have to compute the right coset action of T on an explicit set $\mathcal{S}$ of coset representatives for Γ_0 in Γ, and evaluate the integer-valued functions n_1 and n_2 on each of the matrices $t(\gamma)$ for $\gamma \in \mathcal{S}$. In the case of $\Gamma_0(N)$, these steps can easily be carried out within the framework described in [2], and we will give some further details in §5 below.

Remarks. 1. The formula given in Theorem 3 expresses $\deg(\varphi)$ explicitly as a sum which can be grouped as a sum of terms, one term for each cusp, by collecting together the terms for each τ-orbit. It is not at all clear what significance, if any, can be given to the individual contributions of each cusp to the total.

2. The form of our formula is identical to the one in [5]. However, we should stress that in [5], the analogue of our coset action τ is defined not algebraically, as here, but geometrically, as a permutation of the edges of a fundamental polygonal domain for Γ_0 (and dependent on the particular fundamental domain used). Then it becomes necessary to have an explicit picture of such a fundamental domain, including explicit matrices which identify the edges of the domain in pairs. This is only carried out explicitly in [5] in the case $\Gamma_0 = \Gamma_0(N)$, where N is a prime. In our formulation, the details are all algebraic rather than geometric, which makes the evaluation of the formula

more practical to implement. Also, we have the possibility of evaluating the functions n_1 and n_2 exactly using modular symbols, instead of using numerical evaluation of the periods, which reduces the computation of $\deg(\varphi)$ entirely to linear algebra and integer arithmetic.

3. There are other formulas for $\deg(\varphi)$, involving special values of the L-function attached to the symmetric square of E_f. This connection is discussed in [1] and [3]. As pointed out by an anonymous referee, this formula implies that there should be a simple relation between the degrees of modular parametrizations of quadratic twists. Also, both $\deg(\varphi)$ and the symmetric square L-value are related to so-called "congruence primes", see [4]. We do not go into these connections further here, but hope that our methods and the data which we have computed will help in these and other related investigations.

In the next section we will prove Theorem 2.

4. Derivation of the formula for $\deg(\varphi)$

Proof of Theorem 2. Starting from the definition of $||f||^2$, we compute, using our triangulation,

$$\begin{aligned}
||f||^2 &= \frac{i}{2}\int_{\mathcal{F}_{\Gamma_0}} f(\tau)\overline{f(\tau)}d\tau \wedge \overline{d\tau} \\
&= \frac{1}{4\pi}\int_{\mathcal{F}_{\Gamma_0}} d\left(\varphi_1(\tau)\overline{f(\tau)d\tau}\right) \\
&= \frac{1}{4\pi}\int_{\partial\mathcal{F}_{\Gamma_0}} \varphi_1(\tau)\overline{f(\tau)d\tau} \qquad \text{(by Stokes's Theorem)} \\
&= \frac{1}{4\pi}\sum_{\gamma\in\mathcal{S}}\int_{(\gamma)} \varphi_1(\tau)\overline{f(\tau)d\tau} \\
&= \frac{1}{8\pi}\sum_{\gamma\in\mathcal{S}}\left(\int_{(\gamma)} + \int_{(\gamma^*)}\right) \varphi_1(\tau)\overline{f(\tau)d\tau},
\end{aligned}$$

since $*:\mathcal{S}\to\mathcal{S}$ is an involution. But

$$\begin{aligned}
\int_{(\gamma^*)} \varphi_1(\tau)\overline{f(\tau)d\tau} &= \int_{(s(\gamma)^{-1}\gamma S)} \varphi_1(\tau)\overline{f(\tau)d\tau} \\
&= \int_{(\gamma S)} \varphi_1(s(\gamma)\tau)\overline{f(\tau)d\tau} \\
&= -\int_{(\gamma)} \varphi_1(s(\gamma)\tau)\overline{f(\tau)d\tau},
\end{aligned}$$

since $s(\gamma)\in\Gamma_0$, and we have used the Γ_0-invariance of $f(\tau)d\tau$. Hence,

$$\begin{aligned}
||f||^2 &= \frac{1}{8\pi}\sum_{\gamma\in\mathcal{S}}\int_{(\gamma)} [\varphi_1(\tau) - \varphi_1(s(\gamma)\tau)]\,\overline{f(\tau)d\tau} \\
&= \frac{-1}{8\pi}\sum_{\gamma\in\mathcal{S}} \omega(s(\gamma))\int_{(\gamma)} \overline{f(\tau)d\tau}.
\end{aligned}$$

Now

$$\int_{(\gamma)} f(\tau)d\tau = \int_{\gamma(0)}^{\gamma(\infty)} f(\tau)d\tau = \frac{1}{2\pi i}[\varphi_1(\gamma(\infty)) - \varphi_1(\gamma(0))],$$

so that

$$||f||^2 = \frac{-i}{16\pi^2} \sum_{\gamma \in \mathscr{S}} \omega(s(\gamma)) \overline{[\varphi_1(\gamma(\infty)) - \varphi_1(\gamma(0))]}.$$

We have now reduced the double integral to a finite sum. But

$$\begin{aligned}
\sum_\gamma \omega(s(\gamma))\overline{\varphi_1(\gamma(\infty))} &= \sum_\gamma \omega(s(\gamma^*))\overline{\varphi_1(\gamma^*(\infty))} \qquad \text{(permuting the sum)} \\
&= -\sum_\gamma \omega(s(\gamma))\overline{\varphi_1(\gamma^*(\infty))} \qquad (\text{since } s(\gamma^*) = s(\gamma)^{-1}) \\
&= -\sum_\gamma \omega(s(\gamma))\overline{\varphi_1(s(\gamma)^{-1}\gamma(0))} \qquad (\text{since } \gamma S = s(\gamma)\gamma^*) \\
&= -\sum_\gamma \omega(s(\gamma))\overline{[\varphi_1(\gamma(0)) - \omega(s(\gamma))]} \\
&= -\sum_\gamma \omega(s(\gamma))\overline{\varphi_1(\gamma(0))} + \sum_\gamma |\omega(s(\gamma))|^2.
\end{aligned}$$

Hence, since $||f||^2$ is real, we obtain

$$||f||^2 = \frac{-1}{8\pi^2} \operatorname{Im} \sum_\gamma \omega(s(\gamma))\overline{\varphi_1(\gamma(0))}.$$

Since we have chosen the set of coset representatives $\mathscr{S}$ to be closed under right multiplication by TS, we can replace γ by γTS in the previous sum, to get

$$\begin{aligned}
||f||^2 &= \frac{-1}{8\pi^2} \operatorname{Im} \sum_\gamma \omega(s(\gamma TS))\overline{\varphi_1(\gamma(\infty))} \\
&= \frac{-1}{8\pi^2} \operatorname{Im} \sum_\gamma \omega(t(\gamma))\overline{\varphi_1(\gamma(\infty))},
\end{aligned}$$

where we have also used Lemma 3. Finally, in the last expression for $||f||^2$, we divide the sum into τ-orbits; using the notation of the previous section, the contribution from one orbit is

$$\begin{aligned}
&\sum_{j=1}^{k} \omega(t(\gamma_j))\overline{\varphi_1(\gamma_j(\infty))} \\
&\quad = \sum_{j=1}^{k} \omega(t(\gamma_j))\overline{[\varphi_1(\gamma_j(\infty)) - \varphi_1(\gamma_1(\infty))]} \qquad \text{(using Lemma 2)} \\
&\quad = \sum_{j=1}^{k}\sum_{i=1}^{j-1} \omega(t(\gamma_j))\overline{[\varphi_1(\gamma_{i+1}(\infty)) - \varphi_1(\gamma_i(\infty))]} \\
&\quad = \sum_{j=1}^{k} \omega(t(\gamma_j)) \sum_{i=1}^{j-1} \overline{\varphi_1(\gamma_{i+1}(\infty)) - \varphi_1(t(\gamma_i)\gamma_{i+1}(\infty))} \\
&\quad = -\sum_{1 \le j < i \le k} \omega(t(\gamma_j))\overline{\omega(t(\gamma_i))}.
\end{aligned}$$

Summing over all orbits, we obtain the result of Theorem 2. □

5. The case of $\Gamma_0(N)$: implementation and results

In this section we discuss the case $\Gamma_0 = \Gamma_0(N)$ in greater detail. We have implemented the algorithm in this case as part of our suite of modular elliptic curves programs which were described in [2]; to date (June 1994) we have computed all modular elliptic curves of conductors up to $N = 3000$, together with the degrees of their modular parametrizations (in all but a very small number of cases). It is not practical to give complete tables of these results here, as there are approximately 9500 curves (up to isogeny) with conductor up to 3000. Instead, we give results in a selection of specific cases, and a table for $N \le 200$. A complete table of results is available electronically from the author, from which phenomena of interest (such as the growth of $\deg(\varphi)$ in terms of N, or the set of primes dividing $\deg(\varphi)$) can be observed.

Let N be an arbitrary positive integer. The index of $\Gamma_0(N)$ in Γ is given by

$$[\Gamma : \Gamma_0(N)] = N \prod_{p|N} (1 + 1/p).$$

The right coset representatives of $\Gamma_0(N)$ in Γ are in bijective correspondence with the set $P^1(N) = P^1(\mathbb{Z}/N\mathbb{Z})$ of "M-symbols" $(c : d)$, where $c, d \in \mathbb{Z}$, $\gcd(c, d) = 1$, and

$$(c : d) = (c' : d') \iff cd' \equiv c'd \pmod{N}.$$

We will also write $(c, d) \equiv (c', d')$ for this equivalence relation on $\mathbb{Z}^2$. The correspondence with right cosets is given by

$$(c : d) \leftrightarrow \Gamma_0(N) \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where $a, b \in \mathbb{Z}$ are chosen so that $ad - bc = 1$, different choices of a, b giving the same right coset.

The right coset action of Γ on $P^1(N)$ is given simply by

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

in particular, we have

$$\sigma(c : d) = (c : d)S = (d : -c) \qquad \text{and} \qquad \tau(c : d) = (c : d)T = (c : c + d).$$

Lemma 4. *The length of the τ-orbit containing $(c : d) \in P^1(N)$ is $N/\gcd(N, c^2)$.*

Proof. $\tau^k(c : d) = (c : d) \iff (c : kc + d) = (c : d) \iff cd \equiv c(kc + d) \pmod{N} \iff kc^2 \equiv 0 \pmod{N} \iff k \equiv 0 \pmod{N/\gcd(N, c^2)}$. □

In our earlier work [2], where we used M-symbols to compute modular elliptic curves, it was immaterial exactly which coset representatives were used, or in practice which pair (c, d) was used to represent the M-symbol $(c : d)$. For the application of Theorem 3, however, we must ensure that our set is closed under right multiplication by TS:

$$(c : d)TS = (c + d : -c)$$

unless $(c:d)$ is fixed by TS, which is if and only if $c^2+cd+d^2 \equiv 0 \pmod{N}$. Thus each M-symbol $(c:d)$ will be represented by a specific pair $(c, d) \in \mathbb{Z}^2$ with $\gcd(c, d) = 1$, in such a way that our set $\mathcal{S}$ of representatives contains the pairs $(c+d, -c)$ and $(-d, c+d)$ whenever it contains (c, d), unless $(c:d)$ is fixed by TS. Even when working with pairs (c, d) we will identify (c, d) and $(-c, -d)$.

Fixing these triples of pairs (c, d) corresponds to fixing the triangles $\langle\gamma\rangle$ which form a (possibly disconnected) fundamental domain for $\Gamma_0(N)$. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the pair (c, d) corresponds to the directed edge $\{\gamma(0), \gamma(\infty)\} = \{b/d, a/c\}$. The other edges of $\langle\gamma\rangle$ are $\{a/c, (a+b)/(c+d)\}$ and $\{(a+b)/(c+d), b/d\}$. For this reason we will refer to the pairs (c, d) as edges, and the triples of pairs as triangles. Right multiplication by TS corresponds geometrically to moving round to the next edge of the triangle, while right multiplication by S corresponds to moving across to the next triangle $\langle\gamma^*\rangle$ adjacent to the current one. The τ-action is given by composing these, taking $(c:d)$ (or edge $\{b/d, a/c\}$) to the symbol $(c:d)T = (c:c+d)$ with corresponding edge $\{(a+b)/(c+d), a/c\}$, up to translation by an element of $\Gamma_0(N)$. Note how in this operation the endpoint at the cusp a/c is fixed, as in Lemma 1 above.

We may therefore proceed as follows. For each orbit, start with a standard pair (c, d), chosen in an M-symbol class $(c:d)$ not yet handled. Apply T to obtain the pair $(c, c+d)$. If this pair is the standard representative for the class $(c:c+d)$, we need take no action and may continue with the orbit. But if $(c, c+d) \equiv (r, s)$, say, with $(r, s) \in \mathcal{S}$, then we must record the "glueing matrix" δ, where

$$\delta = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}^{-1} \in \Gamma_0(N),$$

and $ad - bc = ps - qr = 1$, whose period $\omega(\delta)$ will contribute to the partial sum for this orbit. When this happens, we say that the orbit has a "jump" at this point. Different choices for a, b, p and q only change δ by parabolic elements, and so do not affect the period $\omega(\delta)$. We continue until we return to the starting pair, and then move to another orbit, until all M-symbols have been used. As checks on the computation we may use Lemmas 1 and 4: the length of the orbit starting at (c, d) can be precomputed as $N/\gcd(N, c^2)$, and the number of orbits is the number of $\Gamma_0(N)$-inequivalent cusps, which is $\sum_{d|N} \varphi(\gcd(d, N/d))$. (Here φ denotes Euler's function, of course, not the modular parametrization.)

Example 1: $N = 11$. The 12 symbols form 4 triangles which we choose as follows:

$$(1, 0), (-1, 1), (0, 1); \qquad (1, 1), (-2, 1), (-1, 2);$$
$$(1, 2), (-3, 1), (-2, 3); \qquad (1, 3), (-4, 1), (-3, 4).$$

There are two τ-orbits, corresponding to the two cusps at ∞ (of width 1) and at 0 (of width 11). The first contributes nothing. The second is as follows:

$$\begin{aligned}(1,0)&\mapsto(1,1)\mapsto(1,2)\mapsto(1,3)\mapsto(1,4)\equiv(-2,3)\mapsto(-2,1)\mapsto(-2,-1)\\&\equiv(-3,4)\mapsto(-3,1)\mapsto(-3,-2)\\&\equiv(-4,1)\mapsto(-4,-3)\equiv(-1,2)\mapsto(-1,1)\mapsto(1,0).\end{aligned}$$

There are four jump matrices coming from the above sequence. From $(1,4)\equiv(-2,3)$ we obtain

$$\delta_1=\begin{pmatrix}0&-1\\1&4\end{pmatrix}\begin{pmatrix}1&-2\\-2&3\end{pmatrix}^{-1}=\begin{pmatrix}-2&-1\\11&5\end{pmatrix};$$

the others are

$$\delta_2=\begin{pmatrix}4&1\\11&3\end{pmatrix},\quad \delta_3=\begin{pmatrix}-5&-1\\11&2\end{pmatrix}\quad\text{and}\quad \delta_4=\begin{pmatrix}-3&1\\11&-4\end{pmatrix}.$$

Hence,

$$\deg(\varphi)=\frac{1}{2\mathrm{Vol}(E)}\sum_{1\le i<j\le 4}\mathrm{Im}(\omega(\delta_i)\overline{\omega(\delta_j)}).$$

Now by using modular symbols, we can compute the coefficients of $\omega(\delta_i)$ with respect to a period basis ω_1, ω_2, to obtain

$$\begin{aligned}\omega(\delta_1)&=-\omega_1; & \omega(\delta_2)&=-\omega_2;\\ \omega(\delta_3)&=\omega_1; & \omega(\delta_4)&=\omega_2.\end{aligned}$$

Hence we obtain $\deg(\varphi)=\frac{1}{2}(+1+0+(-1)+1+0+1)=1$. Of course, this answer was obvious *a priori*, since the modular curve $X_0(11)$ has genus 1, so that φ is the identity map in this case. The curve (11A1 in [2]) has coefficients $[a_1, a_2, a_3, a_4, a_6]=[0,-1,1,-10,-20]$.

Example 2: $N=26=2\cdot 13$. Here the genus is 2 and there are two newforms. Of the four cusps, only $\frac{1}{2}$ (of width 13) contributes to $\deg(\varphi)$, which is 2 in both cases. The curves are $26\mathrm{A}1=[1,0,1,-5,-8]$ and $26\mathrm{B}1=[1,-1,1,-3,3]$.

Example 3: $N=30=2\cdot 3\cdot 5$. Here the genus is 3, there are two oldforms from level 15 and a newform. The cusps $\frac{1}{2}$, $\frac{1}{5}$ and $\frac{1}{6}$ contribute respectively 1, $\frac{1}{2}$, and $\frac{1}{2}$ to $\deg(\varphi)$, which equals 2. The curve is $30\mathrm{A}1=[1,0,1,1,2]$.

Example 4: $N=210=2\cdot 3\cdot 5\cdot 7$. There are five newforms here giving five curves, A—E. There are 16 cusps, namely $\frac{1}{d}$ (of width $210/d$) for $d\mid 210$. The contributions to $\deg(\varphi)$ are as follows:

$N = 210$

d	A	B	C	D	E
1	0	0	0	0	0
2	10	12	6	2	6
3	2	27	2	0	16
5	3	−5	5/2	4	−5/2
6	14	21	19/2	1	89/2
7	10	−13	4	0	49
10	9	8	5/2	4	3/2
14	−1	3	−5/2	0	21/2
15	2	19	7/2	3	27/2
21	3	4	5/2	0	3/2
30	2	8	2	2	0
35	−6	12	0	0	−12
42	0	0	0	0	0
70	0	0	0	0	0
105	0	0	0	0	0
210	0	0	0	0	0
Total = $\deg(\varphi)$	48	96	32	16	128

The curves are A = 210A1 = [1, 0, 0, −41, −39], B = 210B1 = [1, 0, 1, −498, 4228], C = 210C1 = [1, 1, 1, 10, −13], D = 210D1 = [1, 1, 0, −3, −3] and E = 210E1 = [1, 0, 0, 210, 900].

Finally we give a complete table of all results for $N \leq 200$. For convenience, we give for each curve the code from [2] and the Antwerp Code (in parentheses), and the coefficients of the curve in standard Weierstrass form.

TABLE OF "STRONG WEIL" CURVES AND $\deg(\varphi)$ FOR $N \leq 200$

N	id	$[a_1, a_2, a_3, a_4, a_6]$	$\deg(\varphi)$
11	A1 (B)	[0, −1, 1, −10, −20]	1
14	A1 (C)	[1, 0, 1, 4, −6]	1
15	A1 (C)	[1, 1, 1, −10, −10]	1
17	A1 (C)	[1, −1, 1, −1, −14]	1
19	A1 (B)	[0, 1, 1, −9, −15]	1
20	A1 (B)	[0, 1, 0, 4, 4]	1
21	A1 (B)	[1, 0, 0, −4, −1]	1
24	A1 (B)	[0, −1, 0, −4, 4]	1
26	A1 (B)	[1, 0, 1, −5, −8]	2
26	B1 (D)	[1, −1, 1, −3, 3]	2
27	A1 (B)	[0, 0, 1, 0, −7]	1
30	A1 (A)	[1, 0, 1, 1, 2]	2
32	A1 (B)	[0, 0, 0, 4, 0]	1
33	A1 (B)	[1, 1, 0, −11, 0]	3
34	A1 (A)	[1, 0, 0, −3, 1]	2
35	A1 (B)	[0, 1, 1, 9, 1]	2
36	A1 (A)	[0, 0, 0, 0, 1]	1
37	A1 (A)	[0, 0, 1, −1, 0]	2
37	B1 (C)	[0, 1, 1, −23, −50]	2
38	A1 (D)	[1, 0, 1, 9, 90]	6
38	B1 (A)	[1, 1, 1, 0, 1]	2
39	A1 (B)	[1, 1, 0, −4, −5]	2
40	A1 (B)	[0, 0, 0, −7, −6]	2
42	A1 (A)	[1, 1, 1, −4, 5]	4
43	A1 (A)	[0, 1, 1, 0, 0]	2
44	A1 (A)	[0, 1, 0, 3, −1]	2
45	A1 (A)	[1, −1, 0, 0, −5]	2
46	A1 (A)	[1, −1, 0, −10, −12]	5
48	A1 (B)	[0, 1, 0, −4, −4]	2
49	A1 (A)	[1, −1, 0, −2, −1]	1
50	A1 (E)	[1, 0, 1, −1, −2]	2
50	B1 (A)	[1, 1, 1, −3, 1]	2
51	A1 (A)	[0, 1, 1, 1, −1]	2
52	A1 (B)	[0, 0, 0, 1, −10]	3
53	A1 (A)	[1, −1, 1, 0, 0]	2
54	A1 (E)	[1, −1, 0, 12, 8]	6
54	B1 (A)	[1, −1, 1, 1, −1]	2
55	A1 (B)	[1, −1, 0, −4, 3]	2
56	A1 (C)	[0, 0, 0, 1, 2]	2
56	B1 (A)	[0, −1, 0, 0, −4]	4
57	A1 (E)	[0, −1, 1, −2, 2]	4
57	B1 (B)	[1, 0, 1, −7, 5]	3
57	C1 (F)	[0, 1, 1, 20, −32]	12
58	A1 (A)	[1, −1, 0, −1, 1]	4
58	B1 (B)	[1, 1, 1, 5, 9]	4
61	A1 (A)	[1, 0, 0, −2, 1]	2
62	A1 (A)	[1, −1, 1, −1, 1]	2
63	A1 (A)	[1, −1, 0, 9, 0]	4
64	A1 (B)	[0, 0, 0, −4, 0]	2
65	A1 (A)	[1, 0, 0, −1, 0]	2
66	A1 (A)	[1, 0, 1, −6, 4]	4
66	B1 (E)	[1, 1, 1, −2, −1]	4
66	C1 (I)	[1, 0, 0, −45, 81]	20
67	A1 (A)	[0, 1, 1, −12, −21]	5
69	A1 (A)	[1, 0, 1, −1, −1]	2
70	A1 (A)	[1, −1, 1, 2, −3]	4
72	A1 (A)	[0, 0, 0, 6, −7]	4
73	A1 (B)	[1, −1, 0, 4, −3]	3
75	A1 (A)	[0, −1, 1, −8, −7]	6
75	B1 (E)	[1, 0, 1, −1, 23]	6
75	C1 (C)	[0, 1, 1, 2, 4]	6
76	A1 (A)	[0, −1, 0, −21, −31]	6
77	A1 (F)	[0, 0, 1, 2, 0]	4
77	B1 (D)	[0, 1, 1, −49, 600]	20
77	C1 (A)	[1, 1, 0, 4, 11]	6
78	A1 (A)	[1, 1, 0, −19, 685]	40
79	A1 (A)	[1, 1, 1, −2, 0]	2
80	A1 (F)	[0, 0, 0, −7, 6]	4
80	B1 (B)	[0, −1, 0, 4, −4]	4
82	A1 (A)	[1, 0, 1, −2, 0]	4
83	A1 (A)	[1, 1, 1, 1, 0]	2
84	A1 (C)	[0, 1, 0, 7, 0]	6

N	id	$[a_1, a_2, a_3, a_4, a_6]$	deg(φ)	N	id	$[a_1, a_2, a_3, a_4, a_6]$	deg(φ)
84	B1 (A)	[0, −1, 0, −1, −2]	6	114	C1 (G)	[1, 1, 1, −352, −2431]	60
85	A1 (A)	[1, 1, 0, −8, −13]	4	115	A1 (A)	[0, 0, 1, 7, −11]	10
88	A1 (A)	[0, 0, 0, −4, 4]	8	116	A1 (E)	[0, 0, 0, −4831, −129242]	120
89	A1 (C)	[1, 1, 1, −1, 0]	2	116	B1 (A)	[0, 1, 0, −4, 4]	8
89	B1 (A)	[1, 1, 0, 4, 5]	5	116	C1 (D)	[0, −1, 0, −4, 24]	15
90	A1 (M)	[1, −1, 0, 6, 0]	8	117	A1 (A)	[1, −1, 1, 4, 6]	8
90	B1 (A)	[1, −1, 1, −8, 11]	8	118	A1 (A)	[1, 1, 0, 1, 1]	4
90	C1 (E)	[1, −1, 1, 13, −61]	16	118	B1 (B)	[1, 1, 1, −25, 39]	12
91	A1 (A)	[0, 0, 1, 1, 0]	4	118	C1 (D)	[1, 1, 1, −4, −5]	6
91	B1 (B)	[0, 1, 1, −7, 5]	4	118	D1 (E)	[1, 1, 0, 56, −192]	38
92	A1 (A)	[0, 1, 0, 2, 1]	2	120	A1 (E)	[0, 1, 0, −15, 18]	8
92	B1 (C)	[0, 0, 0, −1, 1]	6	120	B1 (A)	[0, 1, 0, 4, 0]	8
94	A1 (A)	[1, −1, 1, 0, −1]	2	121	A1 (H)	[1, 1, 1, −30, −76]	6
96	A1 (E)	[0, 1, 0, −2, 0]	4	121	B1 (D)	[0, −1, 1, −7, 10]	4
96	B1 (A)	[0, −1, 0, −2, 0]	4	121	C1 (F)	[1, 1, 0, −2, −7]	6
98	A1 (B)	[1, 1, 0, −25, −111]	16	121	D1 (A)	[0, −1, 1, −40, −221]	24
99	A1 (A)	[1, −1, 1, −2, 0]	4	122	A1 (A)	[1, 0, 1, 2, 0]	8
99	B1 (H)	[1, −1, 1, −59, 186]	12	123	A1 (A)	[0, 1, 1, −10, 10]	20
99	C1 (F)	[1, −1, 0, −15, 8]	12	123	B1 (C)	[0, −1, 1, 1, −1]	4
99	D1 (C)	[0, 0, 1, −3, −5]	6	124	A1 (B)	[0, 1, 0, −2, 1]	6
100	A1 (A)	[0, −1, 0, −33, 62]	12	124	B1 (A)	[0, 0, 0, −17, −27]	6
101	A1 (A)	[0, 1, 1, −1, −1]	2	126	A1 (A)	[1, −1, 1, −5, −7]	8
102	A1 (E)	[1, 1, 0, −2, 0]	8	126	B1 (G)	[1, −1, 0, −36, −176]	32
102	B1 (G)	[1, 0, 0, −34, 68]	16	128	A1 (C)	[0, 1, 0, 1, 1]	4
102	C1 (A)	[1, 0, 1, −256, 1550]	24	128	B1 (F)	[0, 1, 0, 3, −5]	8
104	A1 (A)	[0, 1, 0, −16, −32]	8	128	C1 (A)	[0, −1, 0, 1, −1]	4
105	A1 (A)	[1, 0, 1, −3, 1]	4	128	D1 (G)	[0, −1, 0, 3, 5]	8
106	A1 (B)	[1, 0, 0, 1, 1]	6	129	A1 (E)	[0, −1, 1, −19, 39]	8
106	B1 (A)	[1, 1, 0, −7, 5]	8	129	B1 (B)	[1, 0, 1, −30, −29]	15
106	C1 (E)	[1, 0, 0, −283, −2351]	48	130	A1 (E)	[1, 0, 1, −33, 68]	24
106	D1 (D)	[1, 1, 0, −27, −67]	10	130	B1 (A)	[1, −1, 1, −7, −1]	8
108	A1 (A)	[0, 0, 0, 0, 4]	6	130	C1 (J)	[1, 1, 1, −841, −9737]	80
109	A1 (A)	[1, −1, 0, −8, −7]	4	131	A1 (A)	[0, −1, 1, 1, 0]	2
110	A1 (C)	[1, 1, 1, 10, −45]	20	132	A1 (A)	[0, 1, 0, 3, 0]	6
110	B1 (A)	[1, 0, 0, −1, 1]	4	132	B1 (C)	[0, −1, 0, −77, 330]	30
110	C1 (E)	[1, 0, 1, −89, 316]	28	135	A1 (A)	[0, 0, 1, −3, 4]	12
112	A1 (K)	[0, 1, 0, 0, 4]	8	135	B1 (B)	[0, 0, 1, −27, −115]	36
112	B1 (A)	[0, 0, 0, 1, −2]	4	136	A1 (A)	[0, 1, 0, −4, 0]	8
112	C1 (E)	[0, −1, 0, −8, −16]	8	136	B1 (C)	[0, −1, 0, −8, −4]	8
113	A1 (B)	[1, 1, 1, 3, −4]	6	138	A1 (E)	[1, 1, 0, −1, 1]	8
114	A1 (A)	[1, 0, 0, −8, 0]	12	138	B1 (G)	[1, 0, 1, −36, 82]	16
114	B1 (E)	[1, 1, 0, −95, −399]	20	138	C1 (A)	[1, 1, 1, 3, 3]	8

N	id	$[a_1, a_2, a_3, a_4, a_6]$	deg(φ)
139	A1 (A)	[1, 1, 0, −3, −4]	6
140	A1 (A)	[0, 1, 0, −5, −25]	12
140	B1 (C)	[0, 0, 0, 32, 212]	60
141	A1 (E)	[0, 1, 1, −12, 2]	28
141	B1 (G)	[1, 1, 1, −8, −16]	12
141	C1 (A)	[1, 0, 0, −2, 3]	6
141	D1 (I)	[0, −1, 1, −1, 0]	4
141	E1 (H)	[0, 1, 1, −26, −61]	12
142	A1 (F)	[1, −1, 1, −12, 15]	36
142	B1 (E)	[1, 1, 0, −1, −1]	4
142	C1 (A)	[1, −1, 0, −1, −3]	9
142	D1 (C)	[1, 0, 0, −8, 8]	4
142	E1 (G)	[1, −1, 0, −2626, 52244]	324
143	A1 (A)	[0, −1, 1, −1, −2]	4
144	A1 (A)	[0, 0, 0, 0, −1]	4
144	B1 (E)	[0, 0, 0, 6, 7]	8
145	A1 (A)	[1, −1, 1, −3, 2]	4
147	A1 (C)	[1, 1, 1, 48, 48]	24
147	B1 (I)	[0, 1, 1, −114, 473]	42
147	C1 (A)	[0, −1, 1, −2, −1]	6
148	A1 (A)	[0, −1, 0, −5, 1]	12
150	A1 (A)	[1, 0, 0, −3, −3]	8
150	B1 (G)	[1, 1, 0, −75, −375]	40
150	C1 (I)	[1, 1, 1, 37, 281]	48
152	A1 (A)	[0, 1, 0, −1, 3]	8
152	B1 (B)	[0, 1, 0, −8, −16]	8
153	A1 (C)	[0, 0, 1, −3, 2]	8
153	B1 (A)	[0, 0, 1, 6, 27]	16
153	C1 (E)	[1, −1, 0, −6, −1]	8
153	D1 (D)	[0, 0, 1, −27, −61]	24
154	A1 (C)	[1, −1, 0, −29, 69]	24
154	B1 (E)	[1, −1, 1, −4, −89]	24
154	C1 (A)	[1, 1, 0, −14, −28]	16
155	A1 (D)	[0, −1, 1, 10, 6]	20
155	B1 (A)	[1, 1, 1, −1, −2]	8
155	C1 (C)	[0, −1, 1, −1, 1]	4
156	A1 (E)	[0, −1, 0, −5, 6]	12
156	B1 (A)	[0, 1, 0, −13, −4]	12
158	A1 (E)	[1, −1, 1, −9, 9]	32
158	B1 (D)	[1, 1, 0, −3, 1]	8
158	C1 (H)	[1, 1, 1, −420, 3109]	48
158	D1 (B)	[1, 0, 1, −82, −92]	40
158	E1 (F)	[1, 1, 1, 1, 1]	6
160	A1 (A)	[0, 1, 0, −6, 4]	8
160	B1 (D)	[0, −1, 0, −6, −4]	8
161	A1 (B)	[1, −1, 1, −9, 8]	10
162	A1 (K)	[1, −1, 0, −6, 8]	12
162	B1 (G)	[1, −1, 1, −5, 5]	6
162	C1 (A)	[1, −1, 0, 3, −1]	6
162	D1 (E)	[1, −1, 1, 4, −1]	12
163	A1 (A)	[0, 0, 1, −2, 1]	6
166	A1 (A)	[1, 1, 0, −6, 4]	8
168	A1 (B)	[0, 1, 0, −7, −10]	8
168	B1 (E)	[0, −1, 0, −7, 52]	24
170	A1 (A)	[1, 0, 1, −8, 6]	16
170	B1 (H)	[1, 0, 1, −2554, 49452]	160
170	C1 (F)	[1, 0, 0, 399, −919]	84
170	D1 (D)	[1, 0, 1, −3, 6]	12
170	E1 (C)	[1, −1, 0, −10, −10]	20
171	A1 (D)	[1, −1, 1, −14, 20]	12
171	B1 (A)	[0, 0, 1, 6, 0]	8
171	C1 (I)	[0, 0, 1, 177, 1035]	96
171	D1 (H)	[0, 0, 1, −21, −41]	32
172	A1 (A)	[0, 1, 0, −13, 15]	12
174	A1 (I)	[1, 0, 1, −7705, 1226492]	1540
174	B1 (G)	[1, 0, 0, −1, 137]	28
174	C1 (F)	[1, 1, 1, −5, −7]	12
174	D1 (A)	[1, 0, 1, 0, −2]	10
174	E1 (E)	[1, 1, 0, −56, −192]	52
175	A1 (B)	[0, −1, 1, 2, −2]	8
175	B1 (C)	[0, −1, 1, −33, 93]	16
175	C1 (F)	[0, 1, 1, 42, −131]	40
176	A1 (C)	[0, 0, 0, −4, −4]	16
176	B1 (D)	[0, 1, 0, −5, −13]	8
176	C1 (A)	[0, −1, 0, 3, 1]	8
178	A1 (A)	[1, 0, 0, 6, −28]	32
178	B1 (C)	[1, 1, 0, −44, 80]	28
179	A1 (A)	[0, 0, 1, −1, −1]	9
180	A1 (A)	[0, 0, 0, −12, −11]	12
182	A1 (E)	[1, −1, 1, 866, 6445]	180
182	B1 (A)	[1, 0, 0, 7, −7]	12
182	C1 (J)	[1, 0, 1, −4609, 120244]	308
182	D1 (D)	[1, −1, 1, 3, −5]	36
182	E1 (I)	[1, −1, 0, −22, 884]	140

N	id	$[a_1, a_2, a_3, a_4, a_6]$	$\deg(\varphi)$
184	A1 (C)	[0, −1, 0, 0, 1]	8
184	B1 (B)	[0, −1, 0, −4, 5]	8
184	C1 (D)	[0, 0, 0, 5, 6]	12
184	D1 (A)	[0, 0, 0, −55, −157]	24
185	A1 (D)	[0, 1, 1, −156, 700]	48
185	B1 (A)	[0, −1, 1, −5, 6]	8
185	C1 (B)	[1, 0, 1, −4, −3]	6
186	A1 (D)	[1, 1, 0, −83, −369]	44
186	B1 (B)	[1, 0, 0, 15, 9]	20
186	C1 (A)	[1, 0, 1, −17, −28]	28
187	A1 (A)	[0, 1, 1, 11, 30]	16
187	B1 (C)	[0, 0, 1, 7, 1]	30
189	A1 (A)	[0, 0, 1, −3, 0]	12
189	B1 (C)	[0, 0, 1, −24, 45]	12
189	C1 (F)	[0, 0, 1, −6, 3]	12
189	D1 (B)	[0, 0, 1, −27, −7]	36
190	A1 (D)	[1, −1, 1, −48, 147]	88
190	B1 (C)	[1, 1, 0, 2, 2]	8
190	C1 (A)	[1, 0, 0, −30, −100]	24
192	A1 (Q)	[0, −1, 0, −4, −2]	8
192	B1 (A)	[0, 1, 0, −4, 2]	8
192	C1 (K)	[0, 1, 0, 3, 3]	8
192	D1 (E)	[0, −1, 0, 3, −3]	8
194	A1 (A)	[1, −1, 1, −3, −1]	14
195	A1 (A)	[1, 0, 0, −110, 435]	24
195	B1 (I)	[0, 1, 1, 0, −1]	12
195	C1 (K)	[0, 1, 1, −66, −349]	84
195	D1 (J)	[0, −1, 1, −190, 1101]	84
196	A1 (A)	[0, −1, 0, −2, 1]	6
196	B1 (C)	[0, 1, 0, −114, −127]	42
197	A1 (A)	[0, 0, 1, −5, 4]	10
198	A1 (I)	[1, −1, 0, −18, 4]	32
198	B1 (E)	[1, −1, 1, −50, −115]	32
198	C1 (M)	[1, −1, 1, −65, 209]	32
198	D1 (A)	[1, −1, 0, −87, 333]	32
198	E1 (Q)	[1, −1, 0, −405, −2187]	160
200	A1 (B)	[0, 0, 0, 125, −1250]	120
200	B1 (C)	[0, 1, 0, −3, −2]	8
200	C1 (G)	[0, 0, 0, −50, 125]	24
200	D1 (E)	[0, −1, 0, −83, −88]	40
200	E1 (A)	[0, 0, 0, 5, −10]	24

BIBLIOGRAPHY

1. J. Coates and C. G. Schmidt, *Iwasawa theory for the symmetric square of an elliptic curve*, J. Reine Angew. Math. **375** (1987), 104–156.
2. J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, 1992.
3. M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, Invent. Math. **109** (1992), 307–327.
4. H. Hida, *Congruences of cusp forms and special values of their zeta functions*, Invent. Math. **63** (1981), 225–261.
5. D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), 372–384.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF EXETER, NORTH PARK ROAD, EXETER EX4 4QE UNITED KINGDOM

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