# 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 $\Gamma=\operatorname{PSL}(2, \mathbb{Z})$. Equivalently, there is a nonconstant map $\varphi$ from the modular curve $X_{0}(N)$ to $E$. We present here a method of computing the degree of such a map $\varphi$ for arbitrary $N$. Our method, which works for all subgroups of finite index in $\Gamma$ 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 $\Gamma=\operatorname{PSL}(2, \mathbb{Z})$. Equivalently, there is a nonconstant map $\varphi$ from the modular curve $X_{0}(N)$ to $E$. We present here a method of computing the degree of such a $\operatorname{map} \varphi$ 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 $\Gamma$. 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 $\mathscr{H}$. 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 $\S 3$ we introduce some machinery concerning coset representatives and fundamental regions, and state the main result (Theorem 3). This formula for $\operatorname{deg}(\varphi)$ is proved in $\S 4$. In $\S 5$ we discuss the implementation of the method for the case of $\Gamma_{0}(N)$, and the results of

[^0]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 $\Gamma=\operatorname{PSL}(2, \mathbb{Z})$ be the modular group, and $\Gamma_{0}$ a subgroup of $\Gamma$ 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 $\Gamma$-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 $\Gamma_{0}$ 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 $\varphi: X \rightarrow E$ 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 $\Gamma_{0}$. 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 $\Gamma_{0}$. Since the differential $f(\tau) d \tau$ is holomorphic, the function

$$
\varphi_{1}(\tau)=2 \pi i \int_{\infty}^{\tau} f(\zeta) d \zeta \quad\left(\tau \in \mathscr{H}^{*}\right)
$$

is well defined (independent of the path from $\infty$ to $\tau$ ). 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 $\tau$, and defines a function

$$
\omega: \Gamma_{0} \rightarrow \mathbb{C}
$$

which is a homomorphism. The image $\Lambda_{f}$ 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 $\varphi_{1}$ induces a map

$$
\varphi: X=\Gamma_{0} \backslash \mathscr{H}^{*} \rightarrow E_{f}=\mathbb{C} / \Lambda_{f}
$$

via

$$
\varphi\left(\tau \bmod \Gamma_{0}\right)=\varphi_{1}(\tau) \bmod \Lambda_{f}
$$

The period map $\omega: \Gamma_{0} \rightarrow \Lambda_{f}$ is surjective (by definition) and its kernel contains all elliptic and parabolic elements of $\Gamma_{0}$. We may write $\Lambda_{f}=\mathbb{Z} \omega_{1}+\mathbb{Z} \omega_{2}$ with $\operatorname{Im}\left(\omega_{2} / \omega_{1}\right)>0$. Then

$$
\omega(\gamma)=n_{1}(\gamma) \omega_{1}+n_{2}(\gamma) \omega_{2},
$$

where $n_{1}, n_{2}: \Gamma_{0} \rightarrow \mathbb{Z}$ 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 $\omega_{1}$ and $\omega_{2}$ 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 $\Gamma_{0}$ in $\Gamma$ 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 $\operatorname{deg}(\varphi)$ 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 $\Lambda_{f}$, 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 $\varphi: X \rightarrow E_{f}$, the idea used in [5] is to compute the Petersson norm $\|f\|$ in two ways. The first way involves $\operatorname{deg}(\varphi)$ 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 $\Gamma_{0}$ as above, and $\varphi: X \rightarrow E_{f}$ the associated modular parametrization. Then

$$
4 \pi^{2}\|f\|^{2}=\operatorname{deg}(\varphi) \operatorname{Vol}\left(E_{f}\right)
$$

Proof. From the definition

$$
\|f\|^{2}=\int_{X}|f(\tau)|^{2} d u d v \quad(\text { where } \tau=u+i v)
$$

we have, following [5] exactly,

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

since $\varphi^{*}(d z)=2 \pi i f(\tau) d \tau$, where $z=x+i y$ is the coordinate on $E_{f}$,

$$
\begin{aligned}
& =\frac{i}{2} \operatorname{deg}(\varphi) \int_{E_{f}} d z \wedge \overline{d z} \\
& =\operatorname{deg}(\varphi) \int_{E_{f}} d x d y \\
& =\operatorname{deg}(\varphi) \operatorname{Vol}\left(E_{f}\right)
\end{aligned}
$$

as required.

Remark. In terms of the fundamental periods $\omega_{1}, \omega_{2}$ of $E_{f}$, the volume is given by

$$
\operatorname{Vol}\left(E_{f}\right)=\left|\operatorname{Im}\left(\overline{\omega_{1}} \omega_{2}\right)\right| .
$$

More generally, if $\omega, \omega^{\prime} \in \Lambda_{f}$, with $\omega=n_{1}(\omega) \omega_{1}+n_{2}(\omega) \omega_{2}$ and $\omega^{\prime}=$ $n_{1}\left(\omega^{\prime}\right) \omega_{1}+n_{2}\left(\omega^{\prime}\right) \omega_{2}$, then (up to sign) we have

$$
\operatorname{Im}\left(\bar{\omega} \omega^{\prime}\right)=\operatorname{Vol}\left(E_{f}\right) \cdot\left|\begin{array}{ll}
n_{1}(\omega) & n_{1}\left(\omega^{\prime}\right) \\
n_{2}(\omega) & n_{2}\left(\omega^{\prime}\right)
\end{array}\right|
$$

## 3. Coset representatives and fundamental domains

Let $S=\left(\begin{array}{cc}0 & -1 \\ 1 & 0\end{array}\right)$ and $T=\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ be the usual generators for $\Gamma$, so that $S$ has order 2 and $T S=\left(\begin{array}{cc}1 & -1 \\ 1 & 0\end{array}\right)$ has order 3 .

As fundamental domain for $\Gamma$ we may take the triangular region $\mathscr{F}$ with vertices at $0, \rho=(1+i \sqrt{3}) / 2$, and $\infty$. Since $T S$ fixes $\rho$ and permutes $0, \infty$ and 1 cyclically, the three transforms of $\mathscr{F}$ by $I, T S$ and $(T S)^{2}$ fit together around $\rho$ to form an "ideal triangle" $\mathscr{T}$ with vertices at 0,1 and $\infty$. Let $\langle\gamma\rangle$ denote the transform of $\mathscr{T}$ by $\gamma$ 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

$$
\langle\gamma\rangle=\langle\gamma T S\rangle=\left\langle\gamma(T S)^{2}\right\rangle
$$

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

$$
\begin{aligned}
(\gamma) & =\{\gamma(0), \gamma(\infty)\} \\
(\gamma T S) & =\{\gamma T S(0), \gamma T S(\infty)\}=\{\gamma(\infty), \gamma(1)\}
\end{aligned}
$$

and

$$
\left(\gamma(T S)^{2}\right)=\left\{\gamma(T S)^{2}(0), \gamma(T S)^{2}(\infty)\right\}=\{\gamma(1), \gamma(0)\} .
$$

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

Assume, for simplicity, that $\Gamma_{0}$ has no nontrivial elements of finite order, i.e., no conjugates of either $S$ or $T S$. (This assumption is merely for ease of exposition; in fact, it is easy to see that elliptic elements of $\Gamma_{0}$ 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 $\Gamma_{0}$ in $\Gamma$, such that $\gamma \in \mathscr{S}$ implies $\gamma T S \in \mathscr{S}$; this is possible since, by hypothesis, $\Gamma_{0}$ contains no conjugates of $T S$.

Let $\mathscr{S}^{\prime}$ be a subset of $\mathscr{P}$ which contains exactly one of each triple $\gamma, \gamma T S$, $\gamma(T S)^{2}$, so that $\mathscr{P}=\mathscr{P}^{\prime} \cup \mathscr{P}^{\prime} T S \cup \mathscr{P}^{\prime}(T S)^{2}$. Then a fundamental domain for the action of $\Gamma_{0}$ on $\mathscr{H}$ is given by

$$
\mathscr{F}_{r_{0}}=\bigcup_{\gamma^{\prime} \in \mathcal{\prime}^{\prime \prime}}\langle\gamma\rangle .
$$

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 $(\gamma)$ for $\gamma \in \mathscr{S}$.

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

Action of $S$. For each $\gamma \in \mathscr{S}$ we set $\gamma S=s(\gamma) \sigma(\gamma)$, where $s: \mathscr{S} \rightarrow \Gamma_{0}$ is a function and $\sigma: \mathscr{S} \rightarrow \mathscr{S}$ is a permutation. Since $S^{2}$ is the identity, the same is true of $\sigma$, and $s(\sigma(\gamma))=s(\gamma)^{-1}$. For brevity we will write $\gamma^{*}=\sigma(\gamma)$, so that $\gamma^{* *}=\gamma$ for all $\gamma \in \mathscr{S}$.

Note that the triangles $\langle\gamma\rangle$ and $\langle\gamma S\rangle$ are adjacent in the triangulation of $\mathscr{H}$, 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 $\gamma S \in \mathscr{S}$, in the fundamental domain $\mathscr{F}_{0}$ for $\Gamma_{0}$ it is the triangles $\langle\gamma\rangle$ and $\left\langle\gamma^{*}\right\rangle$ which are glued together by the element $s(\gamma) \in \Gamma_{0}$ which takes $\left(\gamma^{*}\right)$ to $-(\gamma)$ (the orientation is reversed).
Action of $T$. Similarly, for $\gamma \in \mathscr{S}$ we set $\gamma T=t(\gamma) \tau(\gamma)$ with $t(\gamma) \in \Gamma_{0}$ and $\tau(\gamma) \in \mathscr{S}$. The permutation $\tau$ of $\mathscr{S}$ 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 $\gamma$ and $\gamma^{\prime}$ of $\mathscr{S}$ are in the same $\tau$-orbit if and only if the cusps $\gamma(\infty)$ and $\gamma^{\prime}(\infty)$ are $\Gamma_{0}$-equivalent.
(b) The length of the $\tau$-orbit of an element $\gamma \in \mathscr{S}$ is the width of the cusp $\gamma(\infty)$ of $\Gamma_{0}$.
Proof. (a) $\gamma$ and $\gamma^{\prime}$ are in the same $\tau$-orbit if and only if $\gamma_{0}=\gamma^{\prime} T^{j} \gamma^{-1} \in \Gamma_{0}$ for some $j$, which is if and only if $\gamma_{0} \gamma(\infty)=\gamma^{\prime}(\infty)$, since the stabilizer of $\infty$ in $\Gamma$ is the subgroup generated by $T$.
(b) The length of the orbit of $\gamma$ is the least $k>0$ such that $\gamma_{0}=\gamma T^{k} \gamma^{-1}=$ $\left(\gamma T \gamma^{-1}\right)^{k} \in \Gamma_{0}$, which is the width of the cusp $\gamma(\infty)$, since the stabilizer of $\gamma(\infty)$ in $\Gamma$ is generated by $\gamma T \gamma^{-1}$.

Thus there is a one-one correspondence between the orbits of $\tau$ on $\mathscr{S}$ and the classes of $\Gamma_{0}$-inequivalent cusps, with the length of each orbit being the width of the corresponding cusp.

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

$$
\gamma_{1} T^{j}=t\left(\gamma_{1}\right) t\left(\gamma_{2}\right) \cdots t\left(\gamma_{j}\right) \gamma_{j+1}
$$

In particular, $\gamma_{1} T^{k}=\gamma_{0} \gamma_{1}$, where

$$
\gamma_{0}=t\left(\gamma_{1}\right) t\left(\gamma_{2}\right) \cdots t\left(\gamma_{k}\right) \in \Gamma_{0} .
$$

Lemma 2. There holds

$$
\sum_{j=1}^{k} \omega\left(t\left(\gamma_{j}\right)\right)=0
$$

where the sum is over a complete $\tau$-orbit on $\mathscr{S}$ and where $\omega$ is the period map of the previous section.
Proof. Since $\gamma_{0}=\gamma_{1} T^{k} \gamma_{1}^{-1}$ is parabolic, we have $\omega\left(\gamma_{0}\right)=0$. Since $\omega$ is a homomorphism, the result follows.

Lemma 3. We have $s(\gamma T S)=t(\gamma)$ for all $\gamma \in \mathscr{S}$.
Proof. We have $t(\gamma) \tau(\gamma)=\gamma T=(\gamma T S) S=s(\gamma T S) \sigma(\gamma T S)$, since $\gamma T S \in \mathscr{S}$. Hence $t(\gamma)=s(\gamma T S)$, and also $\tau(\gamma)=\sigma(\gamma T S)$.

Write $\gamma \prec \gamma^{\prime}$ if $\gamma$ and $\gamma^{\prime}$ are in the same $\tau$-orbit in $\mathscr{S}$, and $\gamma$ precedes $\gamma^{\prime}$ in the fixed ordering determined by choosing a base point for each orbit. In the notation above, $\gamma \prec \gamma^{\prime}$ if and only if $\gamma=\gamma_{i}$ and $\gamma^{\prime}=\gamma_{j}$, where $1 \leq i<j \leq k$.

We can now state our main results.
Theorem 2. Let $f$ be a cusp form of weight 2 for $\Gamma_{0}$ with associated period function $\omega: \Gamma_{0} \rightarrow \mathbb{C}$. Then (the square of) the Petersson norm of $f$ is given by

$$
\|f\|^{2}=\frac{1}{8 \pi^{2}} \sum_{\gamma<\gamma^{\prime}} \operatorname{Im}\left(\omega(t(\gamma)) \overline{\omega\left(t\left(\gamma^{\prime}\right)\right)}\right)
$$

Here the sum is over all ordered pairs $\gamma \prec \gamma^{\prime}$ in $\mathscr{S}$ which are in the same orbit of the permutation $\tau$ of $\mathscr{S}$ 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 $\varphi$.

Theorem 3. With the above notation,

$$
\operatorname{deg}(\varphi)=\frac{1}{2 \operatorname{Vol}\left(E_{f}\right)} \sum_{\gamma<\gamma^{\prime}} \operatorname{Im}\left(\omega(t(\gamma)) \overline{\omega\left(t\left(\gamma^{\prime}\right)\right)}\right)=\frac{1}{2} \sum_{\gamma<\gamma^{\prime}}\left|\begin{array}{ll}
n_{1}(t(\gamma)) & n_{1}\left(t\left(\gamma^{\prime}\right)\right) \\
n_{2}(t(\gamma)) & n_{2}\left(t\left(\gamma^{\prime}\right)\right)
\end{array}\right| .
$$

Hence, to compute $\operatorname{deg}(\varphi)$, we only have to compute the right coset action of $T$ on an explicit set $\mathscr{S}$ of coset representatives for $\Gamma_{0}$ in $\Gamma$, and evaluate the integer-valued functions $n_{1}$ and $n_{2}$ on each of the matrices $t(\gamma)$ for $\gamma \in \mathscr{S}$. 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 $\S 5$ below.

Remarks. 1. The formula given in Theorem 3 expresses $\operatorname{deg}(\varphi)$ 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 $\tau$-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 $\tau$ is defined not algebraically, as here, but geometrically, as a permutation of the edges of a fundamental polygonal domain for $\Gamma_{0}$ (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 $\operatorname{deg}(\varphi)$ entirely to linear algebra and integer arithmetic.
3. There are other formulas for $\operatorname{deg}(\varphi)$, 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 $\operatorname{deg}(\varphi)$ 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 $\operatorname{deg}(\varphi)$

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

$$
\begin{aligned}
\|f\|^{2} & =\frac{i}{2} \int_{\mathscr{F}_{T_{0}}} f(\tau) \overline{f(\tau)} d \tau \wedge \overline{d \tau} \\
& =\frac{1}{4 \pi} \int_{\mathscr{F}_{T_{0}}} d\left(\varphi_{1}(\tau) \overline{f(\tau) d \tau}\right) \\
& =\frac{1}{4 \pi} \int_{\partial \mathscr{\mathscr { F } _ { T _ { 0 } }}} \varphi_{1}(\tau) \overline{f(\tau) d \tau} \quad \text { (by Stokes's Theorem) } \\
& =\frac{1}{4 \pi} \sum_{\gamma \in \mathscr{S}} \int_{(\gamma)} \varphi_{1}(\tau) \overline{f(\tau) \overline{d \tau}} \\
& =\frac{1}{8 \pi} \sum_{\gamma \in \mathscr{\mathscr { P }}}\left(\int_{(\gamma)}+\int_{\left(\gamma^{*}\right)}\right) \varphi_{1}(\tau) \overline{f(\tau) d \tau},
\end{aligned}
$$

since ${ }^{*}: \mathscr{S} \rightarrow \mathscr{S}$ is an involution. But

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

since $s(\gamma) \in \Gamma_{0}$, and we have used the $\Gamma_{0}$-invariance of $f(\tau) d \tau$. Hence,

$$
\begin{aligned}
\|f\|^{2} & =\frac{1}{8 \pi} \sum_{\gamma \in, \mathscr{F}^{\prime}} \int_{(\gamma)}\left[\varphi_{1}(\tau)-\varphi_{1}(s(\gamma) \tau)\right] \overline{f(\tau) d \tau} \\
& =\frac{-1}{8 \pi} \sum_{\gamma \in, \mathscr{F}^{\prime}} \omega(s(\gamma)) \int_{(\gamma)} \overline{f(\tau) d \tau} .
\end{aligned}
$$

Now

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

so that

$$
\|f\|^{2}=\frac{-i}{16 \pi^{2}} \sum_{\gamma \in \mathscr{S}} \omega(s(\gamma)) \overline{\left[\varphi_{1}(\gamma(\infty))-\varphi_{1}(\gamma(0))\right]}
$$

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

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

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 $T S$, we can replace $\gamma$ by $\gamma T S$ in the previous sum, to get

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

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

$$
\begin{aligned}
\sum_{j=1}^{k} & \omega\left(t\left(\gamma_{j}\right)\right) \overline{\varphi_{1}\left(\gamma_{j}(\infty)\right)} \\
& =\sum_{j=1}^{k} \omega\left(t\left(\gamma_{j}\right)\right) \overline{\left[\varphi_{1}\left(\gamma_{j}(\infty)\right)-\varphi_{1}\left(\gamma_{1}(\infty)\right)\right]} \quad \text { (using Lemma 2) } \\
& =\sum_{j=1}^{k} \sum_{i=1}^{j-1} \omega\left(t\left(\gamma_{j}\right)\right) \overline{\left[\varphi_{1}\left(\gamma_{i+1}(\infty)\right)-\varphi_{1}\left(\gamma_{i}(\infty)\right)\right]} \\
& =\sum_{j=1}^{k} \omega\left(t\left(\gamma_{j}\right)\right) \sum_{i=1}^{j-1} \overline{\varphi_{1}\left(\gamma_{i+1}(\infty)\right)-\varphi_{1}\left(t\left(\gamma_{i}\right) \gamma_{i+1}(\infty)\right)} \\
& =-\sum_{1 \leq j<i \leq k} \omega\left(t\left(\gamma_{j}\right)\right) \overline{\omega\left(t\left(\gamma_{i}\right)\right)}
\end{aligned}
$$

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 $N \leq 200$. A complete table of results is available electronically from the author, from which phenomena of interest (such as the growth of $\operatorname{deg}(\varphi)$ in terms of $N$, or the set of primes dividing $\operatorname{deg}(\varphi))$ can be observed.

Let $N$ be an arbitrary positive integer. The index of $\Gamma_{0}(N)$ in $\Gamma$ is given by

$$
\left[\Gamma: \Gamma_{0}(N)\right]=N \prod_{p \mid N}(1+1 / p) .
$$

The right coset representatives of $\Gamma_{0}(N)$ in $\Gamma$ are in bijective correspondence with the set $P^{1}(N)=P^{1}(\mathbb{Z} / N \mathbb{Z})$ of "M-symbols" $(c: d)$, where $c, d \in \mathbb{Z}$, $\operatorname{gcd}(c, d)=1$, and

$$
(c: d)=\left(c^{\prime}: d^{\prime}\right) \Longleftrightarrow c d^{\prime} \equiv c^{\prime} d \quad(\bmod N)
$$

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

$$
(c: d) \leftrightarrow \Gamma_{0}(N)\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right)
$$

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

The right coset action of $\Gamma$ on $P^{1}(N)$ is given simply by

$$
(c: d)\left(\begin{array}{ll}
p & q \\
r & s
\end{array}\right)=(c p+d r: c q+d s)
$$

in particular, we have

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

Lemma 4. The length of the $\tau$-orbit containing $(c: d) \in P^{1}(N)$ is $N / \operatorname{gcd}\left(N, c^{2}\right)$.
Proof. $\tau^{k}(c: d)=(c: d) \Longleftrightarrow(c: k c+d)=(c: d) \Longleftrightarrow c d \equiv c(k c+d)$ $(\bmod N) \Longleftrightarrow k c^{2} \equiv 0(\bmod N) \Longleftrightarrow k \equiv 0\left(\bmod N / \operatorname{gcd}\left(N, c^{2}\right)\right)$.

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 $T S$ :

$$
(c: d) T S=(c+d:-c)
$$

unless $(c: d)$ is fixed by $T S$, which is if and only if $c^{2}+c d+d^{2} \equiv 0(\bmod N)$. Thus each M-symbol $(c: d)$ will be represented by a specific pair $(c, d) \in \mathbb{Z}^{2}$ with $\operatorname{gcd}(c, d)=1$, in such a way that our set $\mathscr{S}$ of representatives contains the pairs $(c+d,-c)$ and $(-d, c+d)$ whenever it contains $(c, d)$, unless $(c: d)$ is fixed by $T S$. 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 $\gamma=\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$, 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 $T S$ 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 $\left\langle\gamma^{*}\right\rangle$ adjacent to the current one. The $\tau$-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 $(r, s) \in \mathscr{S}$, then we must record the "glueing matrix" $\delta$, where

$$
\delta=\left(\begin{array}{ll}
a & a+b \\
c & c+d
\end{array}\right)\left(\begin{array}{ll}
p & q \\
r & s
\end{array}\right)^{-1} \in \Gamma_{0}(N),
$$

and $a d-b c=p s-q r=1$, 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 $\delta$ 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 $N / \operatorname{gcd}\left(N, c^{2}\right)$, and the number of orbits is the number of $\Gamma_{0}(N)$-inequivalent cusps, which is $\sum_{d \mid N} \varphi(\operatorname{gcd}(d, N / d))$. (Here $\varphi$ 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:

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

There are two $\tau$-orbits, corresponding to the two cusps at $\propto$ (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

$$
\delta_{1}=\left(\begin{array}{cc}
0 & -1 \\
1 & 4
\end{array}\right)\left(\begin{array}{cc}
1 & -2 \\
-2 & 3
\end{array}\right)^{-1}=\left(\begin{array}{cc}
-2 & -1 \\
11 & 5
\end{array}\right)
$$

the others are

$$
\delta_{2}=\left(\begin{array}{cc}
4 & 1 \\
11 & 3
\end{array}\right), \quad \delta_{3}=\left(\begin{array}{cc}
-5 & -1 \\
11 & 2
\end{array}\right) \quad \text { and } \quad \delta_{4}=\left(\begin{array}{cc}
-3 & 1 \\
11 & -4
\end{array}\right)
$$

Hence,

$$
\operatorname{deg}(\varphi)=\frac{1}{2 \operatorname{Vol}(E)} \sum_{1 \leq i<j \leq 4} \operatorname{Im}\left(\omega\left(\delta_{i}\right) \overline{\omega\left(\delta_{j}\right)}\right)
$$

Now by using modular symbols, we can compute the coefficients of $\omega\left(\delta_{i}\right)$ with respect to a period basis $\omega_{1}, \omega_{2}$, to obtain

$$
\begin{aligned}
\omega\left(\delta_{1}\right)=-\omega_{1} ; & \omega\left(\delta_{2}\right)=-\omega_{2} \\
\omega\left(\delta_{3}\right)=\omega_{1} ; & \omega\left(\delta_{4}\right)=\omega_{2}
\end{aligned}
$$

Hence we obtain $\operatorname{deg}(\varphi)=\frac{1}{2}(+1+0+(-1)+1+0+1)=1$. Of course, this answer was obvious a priori, since the modular curve $X_{0}(11)$ has genus 1 , so that $\varphi$ is the identity map in this case. The curve (11A1 in [2]) has coefficients $\left[a_{1}, a_{2}, a_{3}, a_{4}, a_{6}\right]=[0,-1,1,-10,-20]$.

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 $\operatorname{deg}(\varphi)$, which is 2 in both cases. The curves are $26 \mathrm{Al}=[1,0,1,-5,-8]$ and $26 \mathrm{Bl}=$ $[1,-1,1,-3,3]$.

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 $\operatorname{deg}(\varphi)$, 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 $\operatorname{deg}(\varphi)$ 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 $=\operatorname{deg}(\varphi)$ | 48 | 96 | 32 | 16 | 128 |

The curves are $\mathrm{A}=210 \mathrm{~A} 1=[1,0,0,-41,-39], \mathrm{B}=210 \mathrm{~B} 1=[1,0,1$, $-498,4228], \mathrm{C}=210 \mathrm{Cl}=[1,1,1,10,-13], \mathrm{D}=210 \mathrm{D} 1=[1,1,0$, $-3,-3]$ and $\mathrm{E}=210 \mathrm{E} 1=[1,0,0,210,900]$.

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 $\operatorname{deg}(\varphi)$ for $N \leq 200$

| $N$ | id | $\left[a_{1}, a_{2}, a_{3}, a_{4}, a_{6}\right]$ | $\operatorname{deg}(\varphi)$ |
| :---: | :---: | :---: | :---: |
| 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 |


| $N$ | id | $\left[a_{1}, a_{2}, a_{3}, a_{4}, a_{6}\right]$ | $\operatorname{deg}(\varphi)$ |
| :---: | :---: | :---: | :---: |
| 54 | B 1 (A) | $[1,-1,1,1,-1]$ | 2 |
| 55 | A 1 (B) | $[1,-1,0,-4,3]$ | 2 |
| 56 | A 1 (C) | $[0,0,0,1,2]$ | 2 |
| 56 | B 1 (A) | $[0,-1,0,0,-4]$ | 4 |
| 57 | A 1 (E) | $[0,-1,1,-2,2]$ | 4 |
| 57 | B 1 (B) | $[1,0,1,-7,5]$ | 3 |
| 57 | C 1 (F) | $[0,1,1,20,-32]$ | 12 |
| 58 | A 1 (A) | $[1,-1,0,-1,1]$ | 4 |
| 58 | B 1 (B) | $[1,1,1,5,9]$ | 4 |
| 61 | A 1 (A) | $[1,0,0,-2,1]$ | 2 |
| 62 | A 1 (A) | $[1,-1,1,-1,1]$ | 2 |
| 63 | A 1 (A) | $[1,-1,0,9,0]$ | 4 |
| 64 | A 1 (B) | $[0,0,0,-4,0]$ | 2 |
| 65 | A 1 (A) | $[1,0,0,-1,0]$ | 2 |
| 66 | A 1 (A) | $[1,0,1,-6,4]$ | 4 |
| 66 | B 1 (E) | $[1,1,1,-2,-1]$ | 4 |
| 66 | Cl (I) | $[1,0,0,-45,81]$ | 20 |
| 67 | A 1 (A) | $[0,1,1,-12,-21]$ | 5 |
| 69 | A 1 (A) | $[1,0,1,-1,-1]$ | 2 |
| 70 | A 1 (A) | $[1,-1,1,2,-3]$ | 4 |
| 72 | A 1 (A) | $[0,0,0,6,-7]$ | 4 |
| 73 | A 1 (B) | $[1,-1,0,4,-3]$ | 3 |
| 75 | A 1 (A) | $[0,-1,1,-8,-7]$ | 6 |
| 75 | B 1 (E) | $[1,0,1,-1,23]$ | 6 |
| 75 | Cl (C) | $[0,1,1,2,4]$ | 6 |
| 76 | A 1 (A) | $[0,-1,0,-21,-31]$ | 6 |
| 77 | A 1 (F) | $[0,0,1,2,0]$ | 4 |
| 77 | B 1 (D) | $[0,1,1,-49,600]$ | 20 |
| 77 | Cl (A) | $[1,1,0,4,11]$ | 6 |
| 78 | A 1 (A) | $[1,1,0,-19,685]$ | 40 |
| 79 | A 1 (A) | $[1,1,1,-2,0]$ | 2 |
| 80 | A 1 (F) | $[0,0,0,-7,6]$ | 4 |
| 80 | B 1 (B) | $[0,-1,0,4,-4]$ | 4 |
| 82 | A 1 (A) | $[1,0,1,-2,0]$ | 4 |
| 83 | A 1 (A) | $[1,1,1,1,0]$ | 2 |
| 84 | A 1 (C) | $[0,1,0,7,0]$ | 6 |


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


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

## 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), 372384.

Department of Mathematics, University of Exeter, North Park Road, Exeter EX4 4QE United Kingdom

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


[^0]:    Received by the editor February 7, 1994.
    1991 Mathematics Subject Classification. Primary 11G05, 14H52, 14Q05; Secondary 11F11, 11F33, 11F67.

