Computing Periods of Cusp Forms and Modular Elliptic Curves

John E. Cremona

CONTENTS

We present an improved method of computing the periods of a newform for Γ_0(N), which converges faster than the method used in [Cremona 1992] (and originally in [Tingley 1975]). We also present some shortcuts that speed up the process of computing all modular elliptic curves of a given conductor N. As an application of these methods, we report on the extension of the systematic computation of modular elliptic curves to all conductors up to 5077.

1. INTRODUCTION

We present an improved method of computing the periods of a newform for $\Gamma_0(N)$, which converges faster than the method used in [Cremona 1992] (and originally in [Tingley 1975]). We also present some shortcuts that speed up the process of computing all modular elliptic curves of a given conductor N. As an application of these methods, we report on the extension of the systematic computation of modular elliptic curves to all conductors up to 5077.

In Section 2, we establish a new formula for a period of a cusp form $f(z)$, using the information that $f(z)$ is an eigenform for the Fricke involution $z \mapsto -1/Nz$ as well as being a cusp form of weight 2 for $\Gamma_0(N)$. The key point is that we obtain a power series expression in $\exp(-2\pi/d\sqrt{N})$ for a small positive integer d, instead of a series in $\exp(-2\pi/cN)$ for some (other) small positive integer c, so that the convergence is greatly improved. This method has other applications, for instance to the computation of periods of cusp forms over imaginary quadratic fields; see [Cremona and Whitley 1994].

1058-6458/1997 \$0.50 per page

In Section 3, we show how in most cases we can find an elliptic curve associated to a newform $f(z)$ without having to compute the full homology space $H(N)$ (defined below). Again, this extends the methods of [Cremona 1992]. The new method is extremely quick, and so represents a major time saving for large conductors N where computation of $H(N)$ is very expensive. The disadvantage is that the curves obtained are not guaranteed to be the so-called "strong Weil" curves, but may only be isogenous to them.

Using these methods, we have been able to extend our systematic computation of modular elliptic curves from the limit of $N = 1000$ as in [Cremona 1992], to $N = 5077$. (The reason for stopping at 5077 instead of (say) 5000 was simply that we wished to verify that there was no curve of rank 3 with conductor below the known example of conductor 5077.) In the final section we report briefly on the results obtained.

2. COMPUTING THE PERIODS OF A CUSP FORM

We will follow the notation of [Cremona 1992], most of which is standard. We fix a positive integer N and let $\Gamma_0(N)$ denote the usual congruence subgroup of level N. Let f be a cusp form of weight 2 for $\Gamma_0(N)$, so that f is holomorphic on the upper half-plane $\mathcal{H}$ and also on the extended upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$, and the differential $\omega_f = 2\pi i f(z)\,dz$ is $\Gamma_0(N)$-invariant.

We denote by $I_f(\alpha,\beta)$ the integral $I_f(\alpha,\beta) = \int_\alpha^\beta \omega_f$, and set $I_f(\alpha) = I_f(\alpha,\infty)$. Let $M \in \Gamma_0(N)$. Since f is holomorphic, the period integral

$$I_f(\alpha, M(\alpha))$$

is independent of the basepoint α, and can be expressed as $I_f(\alpha) - I_f(M(\alpha))$. We will denote this period of f by $P_f(M)$. (The map $M \mapsto P_f(M)$ is in fact a group homomorphism from $\Gamma_0(N)$ to $\mathbb{C}$, but we will not use this fact here.)

For the application to modular elliptic curves, we will be interested in forms that are "rational newforms" in the sense of [Cremona 1992]. Such forms are eigenforms for the Hecke algebra with rational eigenvalues. In order to compute the modular elliptic curve attached to such a form f, we need to compute the set Λ_f of periods of the differential ω_f:

$$\Lambda_f = \{P_f(M) \mid M \in \Gamma_0(N)\}.$$

For rational newforms f, the set Λ_f is a rank 2 lattice in $\mathbb{C}$, and the elliptic curve attached to f is $E_f = \mathbb{C}/\Lambda_f$, which is defined over $\mathbb{Q}$ and has integral invariants c_4, c_6. Finding the coefficients of an equation for E_f is straightforward provided that we have computed two generating periods ω_1 and ω_2 for Λ_f to sufficient precision. We cannot say easily in advance how much precision will be required, as this can vary considerably with the newform, even at the same level N. We will compute the invariants c_4 and c_6 of the curve E_f as floating point approximations, so the number of decimal places we need in order to be able to recognise them as integers depends on the number of digits in c_4 and c_6.

The modular symbol method (described in detail in [Cremona 1992]) provides us with two matrices M_j such that $\omega_j = P_f(M_j)$ for $j = 1, 2$. Hence to compute the periods we need to choose suitable base points α, and evaluate integrals of the form $I_f(\alpha)$. For the remainder of this section, however, it will not be necessary to assume that f is a newform, only that ω_f is $\Gamma_0(N)$-invariant, and later that f is an eigenform for the Fricke involution.

Let $z_0 = x_0 + iy_0 \in \mathcal{H}$ so that $y_0 > 0$. Using the Fourier expansion $f(z) = \sum_{n=1}^\infty a_n e^{2\pi i n z}$ we can integrate term-by-term over a vertical path from z_0 to ∞, obtaining the basic formula

$$I_f(z_0) = -\sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n x_0} e^{-2\pi n y_0}; \tag{2.1}$$

see [Cremona 1992, Proposition 2.10.1]. We can sum this series to get an approximation to $I_f(z_0)$, provided that we have sufficiently many Fourier coefficients a_n. For a newform, these coefficients are computed using modular symbols to obtain the a_p for prime p and multiplicative relations for general a_n: see [Cremona 1992] for details. The important point to notice is that this series is a power series in $e^{-2\pi y_0}$ (with bounded coefficients since $|a_n| < n$ for all n), so will converge best when y_0 is large (or at least not too small).

Suppose we are given a matrix $M = \left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \in \Gamma_0(N)$, where $a, b, c, d \in \mathbb{Z}$, and we wish to compute the associated period $P_f(M) = I_f(\alpha) - I_f(M(\alpha))$ of f. How should we choose α? If α has large imaginary part, $M(\alpha)$ will tend to have a small imaginary part; we would like to maximise both of these simultaneously. The solution used in [Cremona 1992], and before that by Tingley [1975] for the original computations of modular elliptic curves, is to choose

$$\alpha = \frac{-d+i}{cN}, \qquad \text{so that} \qquad M(\alpha) = \frac{a+i}{cN}.$$

Thus both α and $M(\alpha)$ have imaginary part equal to $(cN)^{-1}$. (Note that, by replacing M by $-M$ if necessary, we may assume that $c > 0$; we are not interested in M with $c = 0$ since these are parabolic, and hence have zero period.) Substituting these values of z_0 into (2.1) we obtain the series

$$P_f(M) = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-2\pi n/cN} \left(e^{2\pi i a n/cN} - e^{-2\pi i d n/cN}\right), \tag{2.2}$$

as in [Cremona 1992, Proposition 2.10.1]. This series converges adequately quickly for small N, but when N increases we require too many terms in order to obtain the periods to sufficient precision. (Not only does it take longer to sum the series when we use more terms, but more significantly, computing the coefficients a_n by modular symbols becomes more expensive as n increases.)

In [Cremona 1992], an indirect approach to the computation of the periods ω_j was presented, involving the computation of $L(f \otimes \chi, 1)$ for suitable quadratic characters χ. This involves summing series similar to (2.2) but involving $e^{-2\pi/l\sqrt{N}}$ for certain primes l instead of $e^{-2\pi/cN}$ (see the next section). Clearly these series will converge much faster (unless $l > c\sqrt{N}$, which rarely happens for large N). However, the drawback of this method is that it only applies when N is not a perfect square: when N is square we can only find either the real or the imaginary period of f, but not both. This is frustrating, since in a systematic computation it means that the square levels take far more than their fair share of the computation time, as we have to use the series (2.2) to compute the periods, which in turn require the computation of very large numbers of a_p. Originally we intended to extend the twisting trick to square levels N by using quadratic characters of conductor not coprime to N, but we never worked out the details. Instead we have been able to use the Fricke involution (which was already responsible for the replacement of N by $\sqrt{N}$ in the series for $L(f \otimes \chi, 1)$) to compute the periods $P_f(M)$ using better converging series than (2.2).

Let $W = W_N$ denote, as usual, the transformation $z \mapsto -1/Nz$ of $\mathcal{H}^*$. This induces an involution on the space of cusp forms of weight 2 for $\Gamma_0(N)$. Assume that the cusp form f is an eigenform for W, so that it satisfies the functional equation

$$f(z) = \varepsilon\, (f \mid W)(z) = \varepsilon \frac{1}{Nz^2} f\left(\frac{-1}{Nz}\right),$$

where $\varepsilon = \pm 1$ is *minus* the sign in the functional equation of the L-series $L(f, s)$.

By changing variables in the integrals, we see that

$$I_f(W(\alpha), W(\beta)) = I_{f|W}(\alpha, \beta) = \varepsilon I_f(\alpha, \beta).$$

In particular, if $\beta = W(\alpha)$ we obtain

$$I_f(\alpha, W(\alpha)) = -\varepsilon I_f(\alpha, W(\alpha)),$$

so that when $\varepsilon = +1$ we have $I_f(\alpha, W(\alpha)) = 0$ for all α.

Assume we are in this case ($\varepsilon = +1$). Then in any period integral we may replace an endpoint α with $W(\alpha)$ without affecting the value of the integral. In particular,

$$P_f(M) = I_f(\alpha, M(\alpha)) = I_f(W(\alpha), M(\alpha)).$$

Setting $\alpha = di/(\sqrt{N} - cNi)$ we find that

$$M(\alpha) = \frac{b}{d} + \frac{i}{d\sqrt{N}} \quad \text{and} \quad W(\alpha) = \frac{c}{d} + \frac{i}{d\sqrt{N}},$$

with the same imaginary part; now both imaginary parts are $1/d\sqrt{N}$. (Again, we may assume that $d > 0$ by replacing M by $-M$ if necessary.) Hence

$$\begin{aligned} P_f(M) &= I_f(W(\alpha)) - I_f(M(\alpha)) \\ &= I_f\Big(\frac{c}{d} + \frac{i}{d\sqrt{N}}\Big) - I_f\Big(\frac{b}{d} + \frac{i}{d\sqrt{N}}\Big), \end{aligned}$$

where both integrals converge relatively well.

When $\varepsilon = -1$, we can obtain a slightly more complicated result that is just as good in practice. Combining both cases gives the main result of this section.

Proposition 2.1. *Let f be a cusp form of weight 2 for $\Gamma_0(N)$ such that $f \mid W = \varepsilon f$ with $\varepsilon = \pm 1$. Then, for all*

$$M = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N),$$

the period $P_f(M)$ is given by

$$P_f(M) = (1-\varepsilon) I_f(i/\sqrt{N}) + \varepsilon I_f(W(\alpha)) - I_f(M(\alpha)), \tag{2.3}$$

where $\alpha \in \mathcal{H}$ is arbitrary. Taking

$$\alpha = M^{-1}\Big(\frac{b}{d} + \frac{i}{d\sqrt{N}}\Big),$$

so that

$$W(\alpha) = \frac{c}{d} + \frac{i}{d\sqrt{N}},$$

we have

$$\begin{aligned} P_f(M) &= (1-\varepsilon) I_f(i/\sqrt{N}) \\ &\qquad + \varepsilon I_f\left(\frac{c}{d} + \frac{i}{d\sqrt{N}}\right) - I_f\left(\frac{b}{d} + \frac{i}{d\sqrt{N}}\right) \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n}\Big((\varepsilon - 1)e^{-2\pi n/\sqrt{N}} \\ &\qquad + e^{-2\pi n/d\sqrt{N}}\big(e^{2\pi i n b/d} - \varepsilon e^{2\pi i n c/d}\big)\Big). \end{aligned}$$

Proof. Using $W(i/\sqrt{N}) = i/\sqrt{N}$ we simply compute:

$$\begin{aligned} &I_f(\alpha, M(\alpha)) \\ &\quad = I_f(\alpha, i/\sqrt{N}) + I_f(i/\sqrt{N}, W(\alpha)) \\ &\qquad\qquad + I_f(W(\alpha), M(\alpha)) \\ &\quad = \varepsilon I_f(W(\alpha), i/\sqrt{N}) + I_f(i/\sqrt{N}, W(\alpha)) \\ &\qquad\qquad + I_f(W(\alpha), M(\alpha)) \\ &\quad = (1-\varepsilon)(I_f(i/\sqrt{N}) - I_f(W(\alpha))) + I_f(W(\alpha)) \\ &\qquad\qquad - I_f(M(\alpha)) \\ &\quad = (1-\varepsilon) I_f(i/\sqrt{N}) + \varepsilon I_f(W(\alpha)) - I_f(M(\alpha)). \end{aligned}$$

The final formula now follows from (2.1) using the value of α defined before. $\square$

Note that the term $(1-\varepsilon) I_f(i/\sqrt{N})$ that appears in (2.3) is equal to $-L(f, 1)$, by [Cremona 1992, Proposition 2.11.1]. Hence this term is zero unless the analytic rank of f is zero.

3. FINDING MODULAR ELLIPTIC CURVES QUICKLY

To find all modular elliptic curves of a given conductor N, one proceeds in two phases. In the first phase one computes rational newforms f for $\Gamma_0(N)$, and in the second phase one finds the period lattice Λ_f of f, as defined in the previous section. Then the final step, of determining an equation for the modular elliptic curve E_f attached to f from its period lattice, is straightforward and quick, using the well-known rapidly convergent series for the invariants c_4 and c_6 of E_f. These are known to be rational (since E_f is defined over $\mathbb{Q}$). Moreover, work of Edixhoven [1991] on the Manin constant implies that these computed values of c_4 and c_6 are *integral*, which is of course crucial if we are to recognise them from floating point approximations. Given the integers c_4 and c_6, it is then easy to find a standard Weierstrass equation for the curve E_f.

In this section we will describe an approach to the second phase that is much faster in practice than the one presented in [Cremona 1992], though yielding slightly less information. The idea is essentially this: we need to compute both the real and the imaginary periods of f in order to determine E_f; the real period may be obtained with little extra effort during the first phase; while computing the exact imaginary period then takes considerable extra time, it is easy to compute an integer multiple of the imaginary period, and then one can (by trial and error) determine which multiple of the imaginary period this is.

In order to explain this idea, it is necessary to recall some aspects of the modular symbol method we described in detail in the book [Cremona 1992]. Using this method we compute the homology space $H(N) = H_1(X_0(N), \mathbb{Z})$, finding an explicit basis in terms of modular symbols, and computing the matrices of various Hecke operators on $H(N)$ with respect to this basis. The dimension of $H(N)$ is $2g$ where g is the genus of $X_0(N)$, which increases approximately linearly with N. For the first phase, however, we may work in $H^+(N)$, the g-dimensional subspace of $H(N)$ fixed by the involution induced by complex conjugation. This space (rather, the real g-dimensional vector space $H(N)\otimes_{\mathbb{Q}}\mathbb{R}$) is dual to the space of cusp forms of weight 2 for $\Gamma_0(N)$ with real coefficients. Thus, using linear algebra, one can determine the one-dimensional eigenspaces in $H(N)$ for the algebra of Hecke operators, which correspond by duality to rational newforms for $\Gamma_0(N)$.

Working in $H^+(N)$ is faster than working in $H(N)$ as it has half the dimension. Hence it is of interest to see exactly how much information we can obtain here. At the end of the first phase, we will know how many rational newforms there are, and hence how many modular elliptic curves of conductor N there are, up to isogeny. For each newform f, we can (by computing the Hecke action on $H^+(N)$) determine a large number of coefficients a_n of its Fourier expansion. We can also determine the sign of the functional equation of the associated L-series $L(f,s)$, and whether the L-series vanishes at $s = 1$. This tells us partial information about the analytic rank of the associated curve E_f: we know its parity and whether or not it is zero. We can also compute an approximation to the value $L(f,1)$ (when it is non-zero), and a real period $\Omega(f)$, which is 1 or 2 times the least real period $\Omega_0(f)$ (though we do not know at this stage whether $\Omega(f)/\Omega_0(f) = 1$ or 2). In other words, we can compute the projection of the period lattice Λ_f onto the real axis. Of course, this is insufficient information from which to construct the curve E_f: we still need the imaginary period.

In the original implementation described in [Cremona 1992], this extra information was obtained by starting afresh, working in the full $2g$-dimensional space $H(N)$. In $H(N)$ we find, for each rational newform f, the two-dimensional eigenspace associated to f, which is split into two one-dimensional eigenspaces by the conjugation involution. Once we have this two-dimensional eigenspace, it is a simple matter of linear algebra to determine elements $\gamma_1, \gamma_2 \in H(N)$ such that the periods

$$\omega_i = I_f(\gamma_i)$$

are a $\mathbb{Z}$-basis for the period lattice Λ_f. (Here, for $\gamma \in H(N)$, we denote by $I_f(\gamma)$ the integral of ω_f along γ.) Then we may compute these generating periods, again approximately, using the methods of the previous section. Finally, from ω_1 and ω_2 we can compute approximations to the c_4 and c_6 invariants of the elliptic curve E_f.

For large N (say over 3000), we have found this second phase to be very costly in computation time and space required: not only does it take longer to compute an explicit basis for $H(N)$ than for $H^+(N)$ (there are approximately twice as many modular symbol generators with twice as many relations between them), but also the linear algebra has to then work with matrices of double the dimension, which takes at least four times as long. Hence we have been led to develop an indirect approach to determining the imaginary period of each rational newform f, where we quickly compute an integer multiple of the imaginary period and then guess which multiple it is. This new approach is extremely fast, but does have one critical disadvantage: we can (in most cases) determine a period lattice Λ'_f that is a sublattice of finite index in the full period lattice Λ_f, and such that $\mathbb{C}/\Lambda'_f$ is an elliptic curve E'_f of conductor N with $L(E'_f, s) = L(f, s)$, but we do not know that $\Lambda'_f = \Lambda_f$, so that E'_f might only be isogenous to the curve E_f.

First we recall briefly the indirect method for computing periods described in [Cremona 1992]. It relies on the fact that the values

$$\sqrt{l} L(f \otimes \chi, 1)$$

for quadratic characters χ (with conductor l coprime to N) are, on the one hand, easy to compute to high precision (given enough Fourier coefficients of the newform f); and on the other hand, they are integral multiples of the basic periods of f. In our original approach we used modular symbols in $H(N)$ to determine these multipliers exactly and explicitly, so that two computations of $L(f \otimes \chi, 1)$ for suitable characters χ were enough to determine the period lattice.

There exist positive real numbers x and y such that, for each cycle γ in $H(N, \mathbb{Z})$, we have

$$I_f(\gamma) = m^+(\gamma)x + m^-(\gamma)yi.$$

Here $\gamma \mapsto m^{\pm}(\gamma)$ are homomorphisms $\Gamma_0(N) \to \mathbb{Z}$, which may be computed easily in terms of modular symbols, provided that we have an explicit representation of the space $H(N)$ to hand. The cycle γ will be represented by an integer vector of length $2g$ giving its coordinates with respect to a specific basis of $H(N)$; attached to f we will have determined two integer vectors $v^{\pm}$ (eigenvectors of explicit Hecke matrices), such that

$$m^{\pm} = v^{\pm} \cdot \gamma.$$

If we only know the space $H^+(N)$ explicitly, then we can compute $m^+(\gamma)$ in this way, and hence determine the real part of each period $I_f(\gamma)$, but not the imaginary part.

There are two possibilities for the period lattice Λ_f: either $\Lambda_f = \langle 2x,\, x + yi \rangle$, in which case we say the lattice is of Type 1, or $\Lambda_f = \langle x, yi \rangle$, when it is of Type 2. In the notation used earlier, $\Omega(f) = 2x$ in both cases while the least real period $\Omega_0(f) = \Omega(f)/t$ if the type is t.

The direct method of computing the lattice Λ_f is to compute $I_f(\gamma)$ numerically for a cycle γ such that $m^{\pm}(\gamma)$ are both non-zero, using the formula of the previous section. Here, γ will be expressed as a linear combination of paths of the form $\alpha \to M(\alpha)$ for various $M \in \Gamma_0(N)$. This is the only method we can use when N is a perfect square; otherwise we may alternatively obtain the periods indirectly, using special values of twisted L-series $L(f \otimes \chi,\, s)$.

For each odd prime l not dividing the level N, let χ be the quadratic character modulo l. Then there is an integral period

$$P(l, f) = \sqrt{l^*} L(f \otimes \chi,\, 1) = I_f(\gamma_l),$$

where $l^* = \pm l \equiv 1 \pmod 4$ and

$$\gamma_l = \sum_{a \pmod l} \chi(a)\{0, a/l\}.$$

Here the modular symbol $\{\alpha, \beta\}$ denotes the image in the homology of $X_0(N)$ of a geodesic path from α to β in the upper half-plane.

If $l \equiv 1 \pmod 4$ then $m^-(\gamma_l) = 0$, since $\gamma_l \in H^+(N)$, and now the integer $m^+(l, f) = m^+(\gamma_l)$ satisfies $P(l, f) = m^+(l, f)x$. Secondly, when $l \equiv -1 \pmod 4$ we have $m^+(\gamma_l) = 0$, since $\gamma_l \in H^-(N)$, and the integer $m^-(l, f) = m^-(\gamma_l)$ satisfies

$$P(l, f) = m^-(l, f)yi.$$

Hence to compute x and y, and so determine the period lattice, we simply have to find primes $l^{\pm} \equiv \pm 1 \pmod 4$ such that the integers $m^{\pm} = m^{\pm}(\gamma_{l^{\pm}})$ are non-zero, and set $x = P(l^+, f)/m^+$ and $yi = P(l^-, f)/m^-$. For the multipliers to be non-zero it is necessary (though not sufficient) that $\chi(-N)$ be equal to the eigenvalue of the Fricke involution W_N (denoted ε in section 2), since otherwise the sign of the functional equation of $L(f \otimes \chi,\, s)$ is -1 and the value $L(f \otimes \chi, 1)$ is trivially zero. This is what makes this method fail when N is a perfect square, since then $\chi(-N) = \chi(-1)$ cannot have the correct sign for both real and imaginary periods.

For each quadratic character χ such that $\chi(-N)$ equals ε, the value of $L(f \otimes \chi, 1)$ is computed using the following series [Cremona 1992]:

$$L(f\otimes\chi, 1) = 2\sum_{n=1}^{\infty} \frac{\chi(n)a_n}{n} \exp(-2\pi n/l\sqrt{N}). \quad (3.1)$$

As explained above, the integers $m^{\pm}$ may be obtained algebraically from modular symbol calculations in $H(N)$. The result of this algebraic computation thus consists of the following data for each rational newform f: primes $l^{\pm}$ congruent respectively to ± 1 modulo 4; nonzero integers $m^{\pm}$; and the type (1 or 2) of the lattice. (The type is defined at the top of the preceding column.) To compute the period lattice from this data set of five integers, we compute the periods $P(l^{\pm}, f)$ using (3.1), divide by $m^{\pm}$ respectively to obtain x and y, and take Λ_f to be the lattice $\langle 2x, x+yi\rangle$ (if type 1) or $\langle x, yi\rangle$ (if type 2). In practice we can store these five integers with the Hecke eigenvalues from which we can obtain the Fourier coefficients, and recompute the periods when we need them. In particular, if at the first attempt we are unable to compute the integer invariants c_4, c_6 of the curve E_f to sufficient precision to recognise them, then we will return to $H^+(N)$ in order to compute more Hecke eigenvalues, and then recompute the periods to greater precision without having to recompute $H(N)$.

However, the data l^+ and m^+ can be computed earlier in the first $H^+(N)$ phase, since they only depend on the real projection of the period lattice, so we can already compute the real period x from the data we have from the first phase. Moreover, it is easy to find a suitable prime l^- once we know the Hecke eigenvalues of f, by numerically computing $P(l, f)$ for several primes $l \equiv -1 \pmod 4$ until we find a value which is clearly non-zero.

Thus the only purpose of the time-consuming second phase of the computation, working in $H(N)$, is to determine the integer factor m^- and the type of the lattice. Our new method, which we have used systematically for larger levels ($N > 3000$), is simply to guess the value of m^- by trying each positive integer m in turn. For each $m \geq 1$ we set $yi = P(l^-, f)/m$ and test the two possible lattices (one of each type). If either lattice has approximate integer invariants c_4 and c_6, and the rounded integral values are valid invariants of an elliptic curve over $\mathbb{Q}$, and the resulting curve has conductor N, then we store for later use the successful value m^- of m, and the type, and consider the curve E'_f we have found as a possible candidate for the actual modular elliptic curve E_f.

As we pointed out above, the curves E_f and E'_f are certainly isogenous; they even have the same real period. In many cases, the curve E'_f has no rational isogenies; in such a case we can conclude that $E_f = E'_f$ with no ambiguity. In any case, we can compute the isogeny class of curves isogenous to E'_f via rational isogenies, and the only loss is that we do not always know exactly which curve in the class is the "strong Weil curve" E_f. A further disadvantage is that we cannot compute the degree of the modular parametrisation of E_f, as this requires knowledge of $H(N)$: see [Cremona 1995].

The huge advantage of this method is that in only a few extra seconds computation time, as soon as we have a rational newform, we can (almost always) write down an associated curve E'_f; before this was implemented, it could take many hours of computation time to determine $H(N)$, find the eigenvectors corresponding to f, and hence determine the factor m^- and the lattice type, before we could compute E_f.

We will give an example of this method (with $N = 11$) below.

We now discuss some variants of the method just described.

1. We may use same trick to find l^+ and m^+ if we have not computed them earlier. Then we are obtaining the period lattice and equation of the curve using only: the Fourier coefficients of f (i.e., the coefficients of the L-series of the curve); the sign of the functional equation; and the conductor N. No modular symbol information at all is needed in this case. For an example of this, see the case $N = 11$ below; we have carried this out for other examples too, but at present we do not normally need to use it, as in our implementation we always compute the real period directly.

One may also guess the sign of the functional equation if all one has is the L-series [Cohen 1993, p. 406].

2. Let l_1 and l_2 be two primes congruent to -1 (mod 4), for which $-N$ has the correct quadratic character, so that $P(l_1, f)$ and $P(l_2, f)$ are both not trivially zero. We may compute both the periods $P(l_j, f)$; assume that these are nonzero (or use different primes l_j). We know that there exist nonzero integers m_j such that $P(l_j, f) = m_j y i$ for $j = 1, 2$. Therefore

$$\frac{P(l_2, f)}{P(l_1, f)} = \frac{m_2}{m_1},$$

and we may compute a floating point approximation to this rational number. In practice (provided we have many Fourier coefficients, and the primes l_j are fairly small) we will be able to recognise this rational number using continued fractions. Its denominator is a factor of the unknown integer m_1. If we do this for several different values of l_2 (with the same l_1) then the least common multiple of the denominators may give us a nontrivial factor of m_1, and then in our search for the exact value we may restrict to multiples of this factor. This is useful in practice.

3. Another possibility, which we have not implemented, is to compute $H^-(N)$ in order to determine m^- exactly, as we do m^+ from $H^+(N)$. This would be about as much work as the original computation of $H^+(N)$ (in fact, it would be easier to find the eigenvector corresponding to each newform, since we already know its eigenvalues), and certainly less work than computing the larger space $H(N)$. The result would be that we would have computed exactly all the data we need, in a shorter time than would be required for computing $H(N)$, except for the type of the lattice. If we do not know the type, we can try both types to see which results in a curve with integral coefficients. If both types succeed (as does happen), we will only know the curve E_f up to a 2-isogeny. This final ambiguity can in fact be eliminated, at least in principle, since the lattice has type 1 if and only if $m^+(\gamma) \equiv m^-(\gamma) \pmod 2$ for all $\gamma \in H(N)$, and the parities of these numbers may be determined while working in $H^+(N)$ and $H^-(N)$ respectively.

4. The formulas of Section 2 enable us to compute the period $P_f(M)$ quickly for each $M \in \Gamma_0(N)$. Another variant would then be to choose matrices $M \in \Gamma_0(N)$ at random (with small entry d for greater precision) until some value of $P_f(M)$ had non-zero imaginary part. This imaginary part would be an integer multiple of the quantity denoted y above, and as before we could guess y by repeated division and testing. Again, we could also determine divisors of the multiplier, by comparing the imaginary parts of $P_f(M)$ for several different matrices M.

This last variant works equally well when N is a square, as we compute periods directly. Taken to the extreme, it amounts to computing *random* periods $P_f(M)$ in the period lattice Λ_f, until one has a sublattice Λ'_f of Λ_f of (unknown) finite index, and then searching for a superlattice Λ of Λ'_f for which the curve $\mathbb{C}/\Lambda$ has integral invariants and conductor N. See below for examples of this.

Example: N = 11

There is a single newform f for $\Gamma_0(11)$, with Fourier coefficients given by the following table.

n	1	2	3	4	5	6	7	8
$a(n)$	1	-2	-1	2	1	2	-2	0
n	9	10	11	12	13	14	15	16
$a(n)$	-2	-2	1	-2	4	4	-1	-4

Modular symbol calculations in $H^+(11)$ show that $L(f,1)/\Omega(f) = 1/5$. We compute

$$L(f,1) = 2\sum_{n=1}^{\infty} \frac{a(n)}{n} t^n,$$

where $t = \exp(-2\pi/\sqrt{11}) = 0.15\ldots$. Using the first 16 terms that we have already gives this to 13 decimal places: $L(f,1) = 0.2538418608559\ldots$; thus $\Omega(f) = 5L(f,1) = 1.269209304279\ldots$.

Next, modular symbol calculations in $H(11)$ reveal that the period lattice is of type 1, say

$$\langle \omega_1, \omega_2 \rangle = \langle 2x,\, x + yi \rangle\,.$$

Hence $\Omega(f) = \Omega_0(f) = 2x$, so $x = 5L(f,1)/2 = 0.634604652139\ldots$. For the imaginary period, we find that $y = P(3,f)/2i = \sqrt{3}L(f \otimes 3, 1)/2$. Summing the series for $L(f \otimes 3, 1)$ to 16 terms gives only 4 decimal places: $L(f \otimes 3, 1) = 1.6845\ldots$. This is less accurate than $L(f,1)$, since it is a power series in $\exp(-2\pi/3\sqrt{11}) = 0.53\ldots$, compared with $0.15\ldots$. Hence $y = 1.4588\ldots$, so that $\omega_2 = x + yi = 0.634604652139\ldots + 1.4588\ldots i$. If we use these approximate values for the period lattice generators we find the approximate values $c_4 = 495.99$ and $c_6 = 20008.09$, which round to the integer values $c_4 = 496$ and $c_6 = 20008$. These exact values of c_4 and c_6 are the invariants of an elliptic curve of conductor 11, which is therefore the modular curve E_f:

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

This is the first curve in our tables, with code 11A1 (or code 11B in [Birch and Kuyk 1975]).

We now illustrate the shortcut method presented above, where we guess the imaginary period and lattice type without computing $H(11)$. Having computed $P(3,f) = 2.9176\ldots i \neq 0$, we consider the lattices $\langle x, yi \rangle$ and $\langle 2x,\, x + yi \rangle$, where $2x = 1.2692\ldots$ (from above) and $yi = P(3,f)/m^-$, for $m^- = 1, 2, 3, \ldots$. With $m^- = 1$ we do not find integral invariants, but for $m^- = 2$ and lattice type 1 we find the curve $E_f = [0, -1, 1, -10, -20]$ given above.

Using the first variant of the method, where we do not even know x, we can take $l^+ = 5$ since $P(5,f) = 6.346\ldots \neq 0$. The correct value of m^+ here is 10; if we do not know this, but try $m^+ = 1, 2, 3\ldots$ in a double loop with m^-, the first valid lattice we come across is with $(m^+, m^-) = (2,2)$ and type 1, which leads to the curve $E' = [0, -1, 1, 0, 0]$ of conductor 11; this is 5-isogenous to the "correct" curve E_f, which comes from

$$(m^+, m^-) = (10, 2)$$

and type 1.

We may also consider the ratios $P(l,f)/P(3,f)$ for other primes $l \equiv 3 \pmod 4$; we restrict to those l satisfying

$$\left(\frac{-11}{l}\right) = \left(\frac{l}{11}\right) = +1,$$

since otherwise $P(l,f)$ is trivially 0 (since the sign of the functional equation for the corresponding $L(f \otimes \chi,\, s)$ is then -1). We find the following table of values (rounded: they are only computed approximately):

l	3	23	31	47	59	67	71
$\frac{P(l,f)}{P(3,f)}$	1	1	1	0	1	9	1
l	103	163	179	191	199	223	251
$\frac{P(l,f)}{P(3,f)}$	0	4	25	1	4	1	1

The zero values for $l = 47$ and $l = 103$ indicate that the corresponding twists of the newform f have positive even analytic rank (the corresponding twists of the curve E_f do indeed have rank 2). As all these values are integral here (*a priori* they are only known to be rational) we do not find any nontrivial divisor of m^- (which we know in fact equals 2). The fact that all the integers are perfect squares is an amusing observation, but has a simple explanation in terms of the numbers appearing in the Birch–Swinnerton-Dyer conjecture for the twists of E_f.

Finally, there is one other curve E'' isogenous to E_f in addition to E' (found above). If the period lattice of $E_f = [0, -1, 1, -10, -20]$ is $\langle 2x, yi \rangle$

with $x = 0.6346\ldots$ and $y = 1.4588\ldots$, then $E' = [0,-1,1,0,0]$ has period lattice $\langle 10x,\, 5x+yi\rangle$, and $E'' = [0,-1,1,-7820,263580]$ has lattice

$$\langle x/5,\, 2x/5+yi\rangle\,.$$

These curves are linked by 5-isogenies $E \leftrightarrow E'$ and $E \leftrightarrow E''$.

Lastly, we give examples of the method that works for all N, including squares.

Example: N = 36

At level 36 there is a single newform f. We compute $P_f((\begin{smallmatrix}-7 & 1\\ -36 & 5\end{smallmatrix})) = 0$ (approximately) and

$$P_f((\begin{smallmatrix}29 & 2\\ 72 & 5\end{smallmatrix})) = x + yi$$

with

$$x = 2.103273157988181392\ldots,$$
$$y = 1.2143253239437908058\ldots.$$

The lattice $\langle 2x,\, x+yi\rangle$ leads to the correct curve $y^2 = x^3+1$ of conductor 36.

Example: N = 4900

At level 4900 there are 23 newforms; let f be the first of these, with $a_2 = 1$, $a_3 = -1$, $a_5 = -1$, $a_7 = -1$, $a_{11} = -3$, $a_{13} = -2$, $a_{17} = -3$, and $a_{19} = -1$. We compute the period $P_f(M)$ of f for various matrices $M = (\begin{smallmatrix}a & b\\ cN & d\end{smallmatrix}) \in \Gamma_0(4900)$; we find each one to be (approximately) a $\mathbb{Z}$-linear combination $n_x x + n_y yi$ of x and yi where $x = 0.350453337706059\ldots$ and $y = 0.368564884916029\ldots$, as given in the following table. For brevity, we only give b/d and the coefficients n_x and n_y, which we emphasize are only obtained approximately.

b/d	n_x	n_y
1/3	5	0
1/9	1	4
2/9	1	4
4/9	7	0

b/d	n_x	n_y
1/11	2	4
2/11	2	4
3/11	1	0
4/11	9	1

From this we test the lattice $\langle x, yi\rangle$. It gives $c_4 = 137200$, $c_6 = 9604000$, and hence the curve $y^2 = x^3 - x^2 - 2858x - 10163$ of conductor 4900.

4. CURVES OF CONDUCTORS UP TO 5077

We have carried out the computations described above for all levels N up to 5077. For each N we found the rational newforms, and computed many Hecke eigenvalues for each; in the worst case we needed all a_p for $p < 30000$. For each form we computed a period lattice, and hence found a corresponding curve of conductor N. At present (February 1996), we have found the full period lattice and hence E_f only for $N \le 3200$; for $3200 < N \le 5077$ we have only used the method of section 3 to find a suitable curve, which we only know to be isogenous to E_f. For each curve, we verified by 2-descent (in most cases, including all cases of rank 2) that the rank was equal to the analytic rank, and by finding the Mordell-Weil group of each curve (again, in most cases) we were able to compute the value predicted by the Birch–Swinnerton-Dyer conjecture for the order of the Tate–Shafarevich group.

We summarise the results obtained in Table 1, where for brevity we only give the numbers of newforms found, subdivided by rank. The first examples of each rank are: $N = 11$ for rank 0; $N = 37$ for rank 1; $N = 389$ for rank 2; and $N = 5077$ for rank 3.

Range of N	Total	$r=0$	$r=1$	$r=2$	$r=3$
1–1000	2463	1321	1124	18	0
1001–2000	3391	1575	1737	79	0
2001–3000	3661	1663	1852	146	0
3001–4000	3836	1664	2006	166	0
4001–5000	3948	1685	2087	176	0
5001–5077	284	121	148	14	1
1–5077	17583	8029	8954	599	1

TABLE 1. Summary of rational newforms for $\Gamma_0(N)$, $N \le 5077$.

ELECTRONIC AVAILABILITY

For conductors $N > 1000$, tables of the curves and related data may be obtained from the author from ftp://euclid.ex.ac.uk/pub/cremona/data. At present the data available is not quite as extensive as that published in [Cremona 1992] for conductors up to 1000; more complete data is in preparation, and a fuller report will be published when it is available.

REFERENCES

[Birch and Kuyk 1975] B. J. Birch and W. Kuyk (editors), *Modular functions of one variable IV* (Antwerp, 1972), Lecture Notes in Math. **476**, Springer, Berlin, 1975.

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math., Springer-Verlag, Berlin, 1993.

[Cremona 1992] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992.

[Cremona 1995] J. E. Cremona, "Computing the degree of the modular parametrization of a modular elliptic curve", *Math. Comp.* **64** (1995), 1235–1250.

[Cremona and Whitley 1994] J. E. Cremona and E. Whitley, "Periods of cusp forms and elliptic curves over imaginary quadratic fields", *Math. Comp.* **62** (1994), 407–429.

[Edixhoven 1991] B. Edixhoven, "On the Manin constants of modular elliptic curves", pp. 25–39 in *Arithmetic algebraic geometry* (Texel, 1989), edited by G. van der Geer et al., Progr. Math. **89**, Birkhäuser, Boston, MA, 1991.

[Tingley 1975] D. J. Tingley, *Elliptic curves uniformised by modular functions*, Ph.D. thesis, Oxford U., 1975.

John E. Cremona, Department of Mathematics, University of Exeter, North Park Road, Exeter EX4 4QE, United Kingdom (cremona@maths.exeter.ac.uk)

Received June 17, 1996; accepted in revised form December 15, 1996