

## PERIODS OF CUSP FORMS AND ELLIPTIC CURVES OVER IMAGINARY QUADRATIC FIELDS

J. E. CREMONA AND E. WHITLEY

**ABSTRACT.** In this paper we explore the arithmetic correspondence between, on the one hand, (isogeny classes of) elliptic curves  $E$  defined over an imaginary quadratic field  $K$  of class number one, and on the other hand, rational newforms  $F$  of weight two for the congruence subgroups  $\Gamma_0(n)$ , where  $n$  is an ideal in the ring of integers  $R$  of  $K$ . This continues work of the first author and forms part of the Ph.D. thesis of the second author. In each case we compute numerically the value of the  $L$ -series  $L(F, s)$  at  $s = 1$  and compare with the value of  $L(E, 1)$  which is predicted by the Birch–Swinnerton-Dyer conjecture, finding agreement to several decimal places. In particular, we find that  $L(F, 1) = 0$  whenever  $E(K)$  has a point of infinite order. Several examples are given in detail from the extensive tables computed by the authors.

### 1. INTRODUCTION

In [5, 6, 7], a systematic study was started of a Weil–Taniyama-type correspondence between elliptic curves  $E$  defined over an imaginary quadratic field  $K$  and certain automorphic forms  $F$  over  $K$ . This followed on from work of Mennicke and others (see [15], for example). The forms  $F$ , which will be described in §2 below, were computed by an extension to  $K$  of the modular symbol method, which is well known in the rational case and described fully in [8]. So far, the only fields treated fully are the nine fields  $K$  of class number one, namely the Euclidean fields  $\mathbb{Q}(\sqrt{-m})$  for  $m = 1, 2, 3, 7, 11$  (see [6]), and the non-Euclidean fields of class number one ( $m = 19, 43, 67, 163$ ) (see [23]). Work is in progress to extend the methods to fields of higher class number.

In essence, the results of [5, 6, 23] were as follows. There was observed to be a correspondence between

- (1) isogeny classes of elliptic curves  $E$  defined over  $K$  of conductor  $n$ , where  $n$  is a nonzero ideal of the ring of integers  $R$  of  $K$ ;
- (2) cuspidal automorphic forms of weight 2 for the congruence subgroup  $\Gamma_0(n)$  of  $GL(2, R)$ , which are newforms with rational integer Hecke eigenvalues.

For each such corresponding pair  $(E, F)$ , the conductor  $n$  of the curve  $E$  equals the level  $n$  of  $F$ . Also, the Hasse–Weil  $L$ -function  $L(E, s)$  of  $E$  and

---

Received by the editor January 17, 1992.

1991 *Mathematics Subject Classification*. Primary 11F67, 11G40; Secondary 11G05, 14H52, 14Q05.

© 1994 American Mathematical Society  
0025-5718/94 \$1.00 + \$.25 per page

the  $L$ -function  $L(F, s)$  attached to  $F$  (essentially the Mellin transform of  $F$ , see §2), which both have Euler product expansions of the same type, also agree in at least the first 50 Euler factors. Explicitly, for small primes  $p$  of  $K$  not dividing  $n$ , the trace of Frobenius  $a_p$  of  $E$  at  $p$  and the eigenvalue of the Hecke operator  $T_p$  also agree.

*Remark.* In fact, certain curves and forms must be excluded from this correspondence. On the one hand, if  $E$  has complex multiplication by an order in  $K$  itself, then  $L(E, s)$  is related to an Eisenstein series over  $K$  rather than a cusp form, as observed in [21 and 11]. On the other hand, the first author in [9] found examples of forms  $F$  of type (2) which are (possibly up to quadratic twist) lifted from cusp forms over  $\mathbb{Q}$  and which do not correspond to elliptic curves over  $K$  in this way. Instead, they correspond to certain two-dimensional modular abelian varieties over  $\mathbb{Q}$  which are simple over  $K$ . Examples of this phenomenon are given in [9]. For the five Euclidean fields they all lie beyond the range of the tables in [6], but one example over  $\mathbb{Q}(\sqrt{-43})$  will be seen below.

In this paper we explore the arithmetic correspondence between these pairs  $E$  and  $F$  in greater depth, particularly in relation to the Birch–Swinnerton-Dyer conjecture. It should be stressed that there is no known method of constructing an elliptic curve from the forms  $F$  we are considering, in marked contrast with the situation over  $\mathbb{Q}$ , where Shimura’s construction of modular elliptic curves  $E_f$  attached to newforms for  $\Gamma_0(N)$  is well known. (The exception to this is when  $F$  is the lift, possibly twisted by a quadratic character, of a cusp form of weight 2 for  $\Gamma_0(N)$  over  $\mathbb{Q}$ ; then  $E$  is a twist of the modular elliptic curve  $E_f$ , viewed as a curve defined over  $K$ .) The cusp forms  $F$  are essentially real analytic harmonic 1-forms on a 3-dimensional hyperbolic manifold (with no complex structure), and have a single real period  $\Omega(F)$ . We describe how to compute  $\Omega(F)$  numerically in §2.8. Also, by an analogue of the Manin-Drinfeld Theorem, the quantity  $L(F, 1)$  is a rational multiple of  $\Omega(F)$ , and the ratio  $L(F, 1)/\Omega(F)$  may be computed exactly using modular symbols over  $K$ . In particular, we may determine easily whether  $L(F, 1)$  is zero.

On the other hand, the value of  $L(E, 1)$  is predicted by the Birch–Swinnerton-Dyer conjectures as follows:

(1) We have the equivalence

$$(1.1) \quad L(E, 1) = 0 \iff \text{rank}(E(K)) > 0.$$

(2) Moreover, if  $E(K)$  is finite, then

$$(1.2) \quad L(E, 1) = \frac{2}{\sqrt{|D|}} \frac{\Omega(E) \prod c_p |\text{III}|}{|E(K)|^2}.$$

Here,  $D$  is the discriminant of  $K$ ,  $\text{III}$  is the Tate–Shafarevich group of  $E$  over  $K$ ,  $c_p$  is the local index  $[E(K_p) : E^0(K_p)]$ , and  $\Omega(E)$  is the “complex period” of  $E$ :

$$\Omega(E) = \int_{E(\mathbb{C})} \omega \wedge \overline{\omega},$$

where  $\omega$  is the Néron differential on  $E$ . (Explicitly, if the period lattice  $\Lambda$  of  $E$  has  $\mathbb{Z}$ -basis  $\lambda_1, \lambda_2$ , then  $\Omega(E) = |\text{Im}(\overline{\lambda_1} \lambda_2)|$ , the area of a fundamental parallelogram for  $\Lambda$ .) We will call  $\Omega(E)$  the *area* of  $E$ . To simplify formulae, set  $\Omega^*(E) = 2\Omega(E)/\sqrt{|D|}$ .

As far as (1.1) is concerned, we check in each case where  $L(F, 1) = 0$  that  $E(K)$  is infinite, by finding a point of infinite order on  $E(K)$ . We have not proved that  $E(K)$  has rank 0 in the cases where  $L(F, 1) \neq 0$ , however.

We verify (1.2) in two ways: first, we compute  $\Omega^*(E)$  and  $\Omega(F)$  numerically and check that they are equal to within the accuracy of the computation, in all cases. Secondly, when  $L(F, 1) \neq 0$ , we compare the nonzero rational numbers  $L(F, 1)/\Omega(F)$  and  $\prod c_p/|E(K)|^2$ . Specifically, we compute the nonzero rational number

$$S = \frac{L(F, 1)}{\Omega(F)} \bigg/ \frac{\prod c_p}{|E(K)|^2},$$

which, if  $L(F, s) = L(E, s)$  and the conjectural equation (1.2) holds for  $E$ , should equal the order of the Tate–Shafarevich group  $\text{III}$ . We find that  $S = 1$  in most cases, with  $S = 4, 9$ , or  $16$  occasionally: see §4 for examples. These values are consistent with the theorem of Cassels [3], that  $|\text{III}|$  is a perfect square, if finite. We have not computed  $|\text{III}|$ , or even the 2-primary part via 2-descent, for any of the curves yet. Thus, in all cases we find that  $L(F, 1)$  is equal to the value of  $L(E, 1)$  predicted by the Birch–Swinnerton-Dyer conjecture, provided that  $\text{III}$  has order  $S$ .

We should remark that  $L(E, s)$ , and hence the left-hand side of (1.2), is invariant under isogeny; so is the right-hand side of (1.2) by a theorem of Cassels [3]. However, the individual factors on the right of (1.2) are not isogeny invariant. In order to take this into account, we compute for each curve  $E$  the curves isogenous to  $E$ . For each curve in the isogeny class we compute the ratio  $\prod c_p/|E(K)|^2$  and the area  $\Omega(E)$ . In each class we found one or more curves for which (a)  $\Omega^*(E) = \Omega(F)$ ; and, when  $L(F, 1) \neq 0$ , also (b)  $\prod c_p/|E(K)|^2 = L(F, 1)/\Omega(F)$ , possibly up to a square factor  $S$ .

This somewhat ad hoc approach seemed unavoidable, as we could see no way of determining a priori which of the curves in the isogeny class was ‘most closely’ related to the form  $F$ . This uncertainty does not arise in studying modular curves over  $\mathbb{Q}$  (as in [8]), of course, since there one can single out the ‘strong Weil curve’ in the isogeny class as the one whose period lattice consists precisely of the  $X_0(N)$ -periods of the associated cusp form  $f$  for  $\Gamma_0(N)$ .

A recent result of Stevens [19] shows that every isogeny class of curves over  $\mathbb{Q}$  has a unique ‘minimal’ curve with period lattice minimal amongst all the curves in the class. The evidence suggests, and Stevens conjectures, that this minimal curve can be characterized as the curve attached to the  $\Gamma_1(N)$ -period lattice of the associated cusp form, rather than the  $\Gamma_0(N)$  lattice. These results do not appear to generalize to number fields other than  $\mathbb{Q}$ : some of the isogeny classes of curves which we compute here have no unique minimal element.

It is hoped to consider the ‘positive rank’ case (where  $L(F, 1) = 0$ ) in more detail in the future. First of all, this would involve computing  $L'(F, 1)$ , and higher derivatives if necessary. A method similar to the one used in [2 and 8] might be possible here. Secondly, one would need to compute a basis for the points of infinite order on the curves, and their heights. This should be more straightforward, using our existing implementation of Silverman’s algorithm [18] to compute the heights.

We are also extending the whole investigation to fields with class number greater than one.

The work described here forms part of the University of Exeter Ph.D. thesis of the second author, under the supervision of the first author.

## 2. PERIODS OF CUSP FORMS

**2.1. Cusp forms of weight two for  $\Gamma_0(\mathfrak{n})$ .** Automorphic forms for general global fields are discussed in [22 and 16]; for the case of an imaginary quadratic field, see [10, 5, or 13]. Here we are only concerned with cusp forms of weight two for  $\Gamma_0(\mathfrak{n})$ , where  $\mathfrak{n}$  is a nonzero ideal in the ring of integers  $R$  of an imaginary quadratic field  $K$  of class number one and discriminant  $D$ . The theory of these forms, Hecke operators, oldforms and newforms is entirely analogous to the classical ‘Atkin–Lehner’ theory over  $\mathbb{Q}$ . For a complete discussion of the general case, see [16]; here we quote a summary of the facts we will need.

Let  $\mathcal{H}_3$  be the hyperbolic three-space

$$\mathcal{H}_3 = \{(z, t) \mid z \in \mathbb{C}, t \in \mathbb{R}, t > 0\},$$

with the usual hyperbolic structure and action of  $GL(2, \mathbb{C})$ . We set

$$\beta = \left(-\frac{dz}{t}, \frac{dt}{t}, \frac{d\bar{z}}{t}\right),$$

a basis for the left-invariant differential forms on  $\mathcal{H}_3$ .

A cusp form of weight two for  $\Gamma_0(\mathfrak{n})$  is a vector-valued function  $F: \mathcal{H}_3 \rightarrow \mathbb{C}^3$  such that

- (1)  $F \cdot \beta$  is a  $\Gamma_0(\mathfrak{n})$ -invariant harmonic differential one-form on  $\mathcal{H}_3$ ;
- (2)  $\int_{R \setminus \mathbb{C}} (F|\sigma)(z, t) dz = 0$  for all  $\sigma \in SL(2, R)$ .

Such functions have Fourier expansions of the following form:

$$(2.1) \quad F = (F_0, F_1, F_2) = \sum_{0 \neq \alpha \in R} c(\alpha) t^2 \mathbf{K} \left( \frac{4\pi|\alpha|t}{\sqrt{|D|}} \right) \psi \left( \frac{\alpha z}{\sqrt{D}} \right),$$

where

$$\psi(z) = \exp(2\pi i(z + \bar{z}))$$

for  $z \in \mathbb{C}$ , and

$$\mathbf{K}(t) = \left(-\frac{i}{2}K_1(t), K_0(t), \frac{i}{2}K_1(t)\right)$$

for  $t \in \mathbb{R}$ ,  $t > 0$ . Here,  $K_0$  and  $K_1$  are  $K$ -Bessel functions.

The space of such functions will be denoted  $S(\mathfrak{n})$ , and is finite-dimensional for each  $\mathfrak{n}$ . As in the classical theory, there is a commutative algebra of Hecke operators acting on  $S(\mathfrak{n})$ . For primes  $\pi$  of  $R$  not dividing the level  $\mathfrak{n}$  we have an operator  $T_\pi$  which takes the form with coefficients  $c(\alpha)$  to one with coefficients  $c'(\alpha)$ , where

$$c'(\alpha) = N(\pi)c(\alpha\pi) + c(\alpha/\pi),$$

and  $c(\alpha) = 0$  if  $\alpha \notin R$ .

For each prime  $\pi$  dividing  $\mathfrak{n}$  there is also an ‘Atkin–Lehner’ operator  $W_\pi$  which is an involution. The product of the  $W_\pi$  involutions is the ‘Fricke involution’  $W_\mathfrak{n}$ , induced by the action of the matrix  $\begin{pmatrix} 0 & -1 \\ \nu & 0 \end{pmatrix}$ , where  $\nu$  is a generator of the ideal  $\mathfrak{n}$ .

**2.2. Newforms.** A *newform* in  $S(n)$  is an eigenform for all the Hecke operators  $T_\pi$  for  $\pi$  not dividing  $n$ , which is not induced from a form in  $S(m)$  for any level  $m$  properly dividing  $n$ . Newforms can be normalized so that  $c(1) = 1$ , and then the Fourier coefficients  $c(\alpha)$  are all determined from the Hecke eigenvalues as follows: for all primes  $\pi$  not dividing  $n$ ,  $T_\pi F = c(\pi)F$ ; for primes  $\pi$  dividing  $n$ , we have  $W_\pi F = \epsilon_\pi F$  with  $\epsilon_\pi = \pm 1$ , and

$$c(\pi) = \begin{cases} 0 & \text{if } \pi^2 \mid n, \\ -\epsilon_\pi & \text{if } \pi \mid n \text{ but } \pi^2 \nmid n. \end{cases}$$

For prime powers, we have the recursive relation, for  $r \geq 1$ ,

$$c(\pi^{r+1}) = \begin{cases} c(\pi)c(\pi^r) - N(\pi)c(\pi^{r-1}), & \pi \nmid n, \\ c(\pi)c(\pi^r), & \pi \mid n, \end{cases}$$

and for composite  $\alpha$  the function  $c(\alpha)$  is multiplicative. For the present application, we will be interested in ‘rational’ newforms whose Fourier coefficients are rational integers.

**2.3. Cusp forms and homology.** In [5 and 6], a method based on modular symbols was presented for computing the space  $S(n)$  for ideals  $n$  of small norm, in the case where  $K$  is Euclidean. This was extended to non-Euclidean fields of class number one by the second author in her thesis [23]. The method relies on an isomorphism (duality) between  $S(n)$  and the homology space  $V(n) = H_1(\Gamma_0(n) \backslash \mathcal{H}_3^*, \mathbb{C})$ ; the isomorphism respects the Hecke action on both spaces, so that  $S(n)$  and  $V(n)$  are isomorphic as modules for the Hecke algebra. In practice, one finds newforms in  $S(n)$  by computing the action of enough Hecke operators on  $V(n)$ , and finding one-dimensional eigenspaces with rational eigenvalues.

**2.4. Plusforms.** In addition to the Hecke operators on  $S(n)$  described above, there is also an involution  $J$  induced by the action on  $\mathcal{H}_3$  of the matrix  $\begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}$ , where  $\varepsilon$  generates the unit group  $R^*$  of  $R$ . [In the two fields where  $\varepsilon \neq -1$  it is perhaps not obvious that  $J$  is an involution; but  $J^2$  is induced by the action of  $\begin{pmatrix} \varepsilon^2 & 0 \\ 0 & 1 \end{pmatrix}$ , which is equal modulo scalar matrices to  $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} \in \Gamma_0(n)$ .]

The effect of  $J$  on Fourier coefficients is  $c(\alpha) \rightarrow c(\varepsilon\alpha)$ ; this involution commutes with the Hecke operators, and splits  $S(n)$  into two eigenspaces,

$$S(n) = S^+(n) \oplus S^-(n).$$

Newforms in  $S^+(n)$  were called ‘plusforms’ in [5], and their Fourier coefficients satisfy the additional condition  $c(\varepsilon\alpha) = c(\alpha)$  for all  $\alpha \in R$ . It is plusforms which appear to correspond directly to elliptic curves, and we will restrict to plusforms with rational Fourier coefficients from now on. (No information is lost in making this restriction, since ‘minusforms’ in  $S^-(n)$  may be twisted into plusforms at a possibly larger level, as explained in [5 and 6]; see also §2.8 below, where we also use quadratic twists.) An alternative viewpoint is that the forms in  $S^+(n)$  are invariant under the larger group

$$\Gamma_0^+(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, R) \mid c \in n \right\}.$$

Note that, for a plusform  $F$ , the Fourier coefficient  $c(\alpha)$  depends only on the ideal  $(\alpha)$  generated by  $\alpha$ , and so we may write  $c(a)$ , where  $a$  is an ideal

of  $R$ . Then we may attach to  $F$  the formal Dirichlet series

$$(2.2) \quad L(F, s) = \sum c(\mathfrak{m})N(\mathfrak{m})^{-s},$$

where  $\mathfrak{m}$  runs over the nonzero ideals of  $R$ , and  $N(\mathfrak{m}) = |R/\mathfrak{m}|$  denotes the ideal norm. The multiplicative property of the Fourier coefficients  $c(\alpha)$  immediately implies that  $L(F, s)$  has an Euler product expansion:

$$L(F, s) = \prod_{\mathfrak{p}} (1 - c(\mathfrak{p})N(\mathfrak{p})^{-s} + \chi(\mathfrak{p})N(\mathfrak{p})^{1-2s})^{-1},$$

where

$$\chi(\mathfrak{p}) = \begin{cases} 0 & \text{if } \mathfrak{p} \mid \mathfrak{n}, \\ 1 & \text{if } \mathfrak{p} \nmid \mathfrak{n}. \end{cases}$$

As in the classical case, we have the estimate  $|c(\mathfrak{p})| \leq 2N(\mathfrak{p})^{1/2}$ , from which it follows that the series  $L(F, s)$  converges for  $\operatorname{Re}(s) > 3/2$ ; in the next section we show, moreover, that the Mellin transform of  $F$  provides an analytic continuation of  $L(F, s)$  which satisfies a functional equation.

**2.5. Mellin transforms of cusp forms.** Let  $F \in S(\mathfrak{n})$ . We form the Mellin transform of  $F$  by multiplying by  $t^{2s-2}$  and integrating along the imaginary axis to obtain a function of the complex variable  $s$ :

$$(2.3) \quad \Lambda(F, s) = a_K \int_0^\infty t^{2s-2} F \cdot \beta.$$

Here the normalizing constant  $a_K$  depends only on the field  $K$ , and not on the form  $F$  or its level:

$$a_K = \frac{(4\pi)^2}{w|D|},$$

where  $w = |R^*|$ . The rapid decay of  $F(0, t)$  as  $t \rightarrow \infty$  ensures that  $\Lambda(F, s)$  is an entire function of  $s$ . In particular, we have the special value

$$(2.4) \quad \Lambda(F, 1) = a_K \int_0^\infty F \cdot \beta.$$

We will usually only consider  $\Lambda(F, s)$  for  $F \in S^+(\mathfrak{n})$ , since it is easy to see that  $\Lambda(F, s) = 0$  identically for  $F \in S^-(\mathfrak{n})$ .

**Proposition 2.1.** *Let  $F$  be a newform in  $S^+(\mathfrak{n})$ . Then*

(1) *For  $\operatorname{Re}(s) > 3/2$  we have*

$$(2.5) \quad \Lambda(F, s) = (2\pi)^{2-2s} |D|^{s-1} \Gamma(s)^2 L(F, s).$$

(2)  *$\Lambda(F, s)$  satisfies the functional equation*

$$(2.6) \quad \Lambda(F, s) = \pm N(\mathfrak{n})^{1-s} \Lambda(F, 2-s).$$

*Proof.* (1) If  $\operatorname{Re}(s) > 3/2$ , then we may substitute the Fourier series (2.1) into (2.3) and integrate term by term. Notice that since we are integrating along a

vertical path with the  $z$ -coordinate constant, we may ignore the  $dz$  and  $d\bar{z}$  components of the differential  $F \cdot \beta$ . We obtain

$$\begin{aligned}\Lambda(F, s) &= a_K \int_0^\infty t^{2s-2} F_1(0, t) \frac{dt}{t} \\ &= a_K \int_0^\infty t^{2s-2} \sum_{0 \neq \alpha \in R} c(\alpha) t^2 K_0 \left( \frac{4\pi|\alpha|t}{\sqrt{|D|}} \right) \frac{dt}{t} \\ &= a_K \sum c(\alpha) \int_0^\infty t^{2s-1} K_0 \left( \frac{4\pi|\alpha|t}{\sqrt{|D|}} \right) dt.\end{aligned}$$

Now  $\int_0^\infty t^k K_0(t) dt = 2^{k-1} \Gamma(\frac{k+1}{2})^2$ , so after a change of variable we have

$$\begin{aligned}\Lambda(F, s) &= a_K \sum_{\alpha} c(\alpha) (4\pi)^{-2s} |D|^s |\alpha|^{-2s} 2^{2s-2} \Gamma(s)^2 \\ &= w^{-1} (2\pi)^{2-2s} |D|^{s-1} \Gamma(s)^2 \sum_{\alpha} c(\alpha) N(\alpha)^{-s} \\ &= (2\pi)^{2-2s} |D|^{s-1} \Gamma(s)^2 L(F, s).\end{aligned}$$

(2) We use the fact that newforms in  $S(\mathfrak{n})$  are eigenforms for the Fricke involution  $W_{\mathfrak{n}}$ . Suppose that  $W_{\mathfrak{n}}F = \epsilon F$  with  $\epsilon = \pm 1$ . Now

$$(W_{\mathfrak{n}}F)(0, t) = F\left(0, \frac{1}{|\nu|t}\right) \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix};$$

hence,

$$(2.7) \quad F_1\left(0, \frac{1}{|\nu|t}\right) = -\epsilon F_1(0, t).$$

Multiply by  $t^{2s-1}dt$  and integrate from 0 to  $\infty$ ; the right-hand side gives  $-\epsilon\Lambda(F, s)$ , while the left-hand side, after a change of variable from  $t$  to  $1/(|\nu|t)$ , becomes  $N(\mathfrak{n})^{1-s}\Lambda(F, 2-s)$ . This gives the result.  $\square$

In view of (2.5), we may abuse notation to write  $L(F, 1) = \Lambda(F, 1)$ , although of course the series for  $L(F, s)$  does not converge at  $s = 1$ .

**2.6. Numerical computation of  $\Lambda(F, 1)$ .** In order to compute  $\Lambda(F, 1)$  numerically, we may use the well-known trick of splitting the range of integration at the fixed point of the  $W_{\mathfrak{n}}$  involution, namely  $(z, t) = (0, 1/\sqrt{|\nu|})$ . We obtain the following formula.

**Proposition 2.2.** *Let  $F$  be a newform in  $S^+(\mathfrak{n})$  with Fourier coefficients  $c(\alpha)$ , and suppose that  $W_{\mathfrak{n}}F = \epsilon F$ . If  $\epsilon = +1$ , then  $\Lambda(F, 1) = 0$ ; if  $\epsilon = -1$ , then*

$$(2.8) \quad \Lambda(F, 1) = \frac{8\pi}{\sqrt{|\nu D|}} \sum_{(\alpha)} \frac{c(\alpha)}{|\alpha|} K_1\left(\frac{4\pi|\alpha|}{\sqrt{|\nu D|}}\right),$$

where the sum is over all nonzero  $\alpha \in R$  modulo units.

*Proof.* In (2.3) we split the range of integration at  $t = 1/\sqrt{|\nu|}$ , and change variable from  $t$  to  $1/(|\nu|t)$  in the integral from 0 to  $1/\sqrt{|\nu|}$ , to obtain

$$\Lambda(F, 1) = a_K(1 - \epsilon) \int_{1/\sqrt{|\nu|}}^\infty F_1(0, t) \frac{dt}{t}.$$

Assume  $\epsilon = -1$ ; otherwise,  $\Lambda(F, 1) = 0$ . Replacing  $F_1$  by its Fourier expansion, we obtain

$$\Lambda(F, 1) = 2a_K \int_{1/\sqrt{|\nu|}}^{\infty} \sum_{\alpha} c(\alpha) t^2 K_0 \left( \frac{4\pi|\alpha|t}{\sqrt{|D|}} \right) \frac{dt}{t}.$$

Now we use the standard integral

$$\int x K_0(x) dx = -x K_1(x)$$

and integrate term by term to obtain

$$\begin{aligned} \Lambda(F, 1) &= 2a_K \sum_{\alpha} c(\alpha) \int_{1/\sqrt{|\nu|}}^{\infty} t^2 K_0 \left( \frac{4\pi|\alpha|t}{\sqrt{|D|}} \right) \frac{dt}{t} \\ &= 2w^{-1} \sum_{\alpha} \frac{c(\alpha)}{|\alpha|^2} \int_{\frac{4\pi|\alpha|}{\sqrt{|\nu D|}}}^{\infty} u K_0(u) du \\ &= 2w^{-1} \sum_{\alpha} \frac{c(\alpha)}{|\alpha|^2} \frac{4\pi|\alpha|}{\sqrt{|\nu D|}} K_1 \left( \frac{4\pi|\alpha|}{\sqrt{|\nu D|}} \right) \\ &= \frac{8\pi}{\sqrt{|\nu D|}} \sum_{(\alpha)} \frac{c(\alpha)}{|\alpha|} K_1 \left( \frac{4\pi|\alpha|}{\sqrt{|\nu D|}} \right). \end{aligned}$$

Since  $K_1(t)$  tends to zero very rapidly as  $t \rightarrow \infty$ , this series converges quickly.  $\square$

**2.7 Modular symbols.** Let  $\Gamma$  be a subgroup of finite index in  $SL(2, R)$ , such as  $\Gamma_0(n)$ . Let  $A$  and  $B$  be points in  $\mathcal{H}_3^* = \mathcal{H}_3 \cup K \cup \{\infty\}$  which are equivalent under the action of  $\Gamma$ , so that  $B = \gamma(A)$  for some  $\gamma \in \Gamma$ . Any smooth path from  $A$  to  $B$  in  $\mathcal{H}_3^*$  projects to a closed path in the quotient space  $X_{\Gamma} = \Gamma \backslash \mathcal{H}_3^*$ , and hence determines a homology class in  $H_1(X_{\Gamma}, \mathbb{Z})$  which depends only on  $A$  and  $B$  and not on the path chosen, because  $\mathcal{H}_3^*$  is simply connected. (In fact the class depends only on  $\gamma$ : see (5) in the lemma below.) We denote this homology class by the ‘modular symbol’  $\{A, B\}_{\Gamma}$ , or simply  $\{A, B\}$  if the group  $\Gamma$  is clear from the context. The symbol  $\{A, B\}_{\Gamma}$  gives a functional  $S(\Gamma) \rightarrow \mathbb{C}$  via  $F \mapsto a_K \int_A^B F \cdot \beta$ , since by harmonicity the integral is independent of the path from  $A$  to  $B$ . We may thus extend the definition of the symbol  $\{A, B\}$  to points  $A, B \in \mathcal{H}_3^*$  not necessarily  $\Gamma$ -equivalent by identifying  $\{A, B\}$  with the functional  $F \mapsto a_K \int_A^B F \cdot \beta$ ; now, in general, we have  $\{A, B\} \in H_1(X_{\Gamma}, \mathbb{C})$ . A generalization of the Manin-Drinfeld Theorem (see [13]) says that when  $A, B$  are  $K$ -rational cusps (i.e.,  $A, B \in K \cup \infty$ ) and  $\Gamma$  is a congruence subgroup, then  $\{A, B\} \in H_1(X_{\Gamma}, \mathbb{Q})$ , the homology with rational coefficients. In particular,  $\{0, \infty\} \in H_1(X_{\Gamma}, \mathbb{Q})$ . The following simple facts are now immediate.

**Lemma.** *We have*

- (1)  $\{A, A\} = 0$ ;
- (2)  $\{A, B\} + \{B, A\} = 0$ ;
- (3)  $\{A, B\} + \{B, C\} + \{C, A\} = 0$ ;



- (4)  $\{\gamma A, \gamma B\}_\Gamma = \{A, B\}_\Gamma$  for all  $\gamma \in \Gamma$ ;
- (5)  $\{A, \gamma A\}_\Gamma = \{B, \gamma B\}_\Gamma$  for all  $\gamma \in \Gamma$ ;
- (6)  $\{A, \gamma A\}_\Gamma \in H_1(X_\Gamma, \mathbb{Z})$  for all  $\gamma \in \Gamma$ .

It follows that the map  $\gamma \mapsto \{A, \gamma A\}_\Gamma$  is a surjective group homomorphism  $\Gamma \rightarrow H_1(X_\Gamma, \mathbb{Z})$ , which is independent of  $A \in \mathcal{H}_3^*$ .

**2.8. The periods of a cusp form.** Let  $F$  be a newform in  $S(n)$ , and write  $X_0(n)$  for  $X_{\Gamma_0(n)}$  in the case  $\Gamma = \Gamma_0(n)$ . Then  $F$  induces a map

$$I_F: H_1(X_0(n), \mathbb{C}) \rightarrow \mathbb{C}$$

via

$$\{A, B\} \mapsto a_K \int_A^B F \cdot \beta,$$

which is surjective (see [13]) and hence has a kernel of codimension 1. The restriction of  $I_F$  to  $H_1(X_0(n), \mathbb{Z})$  has an image which is a nontrivial, discrete subgroup of  $\mathbb{R}$ , hence has the form  $\Omega(F)\mathbb{Z}$ , for some unique positive real number  $\Omega(F)$ . This  $\Omega(F)$  is the *real period* of  $F$ .

We now derive a formula for the numerical computation of  $\Omega(F)$ . We will in fact give two methods: a direct method, and an indirect (but usually more accurate) method, involving  $\Lambda(F, 1)$ , when this is nonzero, or  $\Lambda(F \otimes \chi, 1)$  for a suitable quadratic character  $\chi$ , when  $\Lambda(F, 1) = 0$ .

*Direct method.* To each rational newform  $F \in S_2(n)$  there is an associated one-dimensional eigenspace  $V_F$  of  $V_{\mathbb{Q}}(n) = H_1(X_0(n), \mathbb{Q})$ , given explicitly in terms of modular symbols. Hence we may determine  $\gamma \in \Gamma_0(n)$  such that the symbol  $\{A, \gamma(A)\}$  generates  $V_F \cap H_1(X_0(n), \mathbb{Z})$ . In practice, the generator may be given as a linear combination of such elementary symbols, but for simplicity we ignore this. Then  $\Omega(F) = I_F(\{A, \gamma(A)\})$ .

**Proposition 2.3.** *Let  $F$  be a newform in  $S^+(n)$ , and let  $\gamma = \begin{pmatrix} a & b \\ \nu c & d \end{pmatrix} \in \Gamma_0(n)$  be such that  $\Omega(F) = I_F(\{A, \gamma(A)\})$ ; then  $\Omega(F)$  is given by*

$$(2.9) \quad \Omega(F) = \frac{4\pi}{|\nu c| \sqrt{|D|}} \sum_{(\alpha)} \frac{c(\alpha)}{|\alpha|} K_1 \left( \frac{4\pi|\alpha|}{|\nu c| \sqrt{|D|}} \right) \left( \tilde{\psi} \left( \frac{-\alpha d}{\nu c \sqrt{D}} \right) - \tilde{\psi} \left( \frac{\alpha a}{\nu c \sqrt{D}} \right) \right),$$

where the sum is over nonzero  $\alpha \in R$  modulo units, and  $\tilde{\psi}(z) = \sum_{\varepsilon \in R^*} \psi(\varepsilon z)$ .

*Proof.* Since  $\{A, \gamma(A)\} = \{A, \infty\} - \{\gamma(A), \infty\}$ , we first consider paths of the form  $\{A, \infty\}$  for  $A = (z_0, t_0) \in \mathcal{H}_3$ . Set  $I_F(A) = I_F(\{A, \infty\})$ . Then

$$\begin{aligned} I_F(A) &= a_K \int_A^\infty F \cdot \beta = a_K \int_{t_0}^\infty F_1(z_0, t) \frac{dt}{t} \\ &= a_K \int_{t_0}^\infty \sum_{\alpha} c(\alpha) t K_0 \left( \frac{4\pi|\alpha|t}{\sqrt{|D|}} \right) \psi \left( \frac{\alpha z_0}{\sqrt{D}} \right) dt \\ &= a_K \sum_{\alpha} c(\alpha) \psi \left( \frac{\alpha z_0}{\sqrt{D}} \right) \int_{t_0}^\infty t K_0 \left( \frac{4\pi|\alpha|t}{\sqrt{|D|}} \right) dt. \end{aligned}$$

Using  $\int tK_0(t)dt = -tK_1(t)$  again, we obtain

$$\begin{aligned} I_F(A) &= a_K \frac{\sqrt{|D|}}{4\pi} \sum_{\alpha} \frac{c(\alpha)}{|\alpha|} \psi\left(\frac{\alpha z_0}{\sqrt{D}}\right) t_0 K_1\left(\frac{4\pi|\alpha|t_0}{\sqrt{|D|}}\right) \\ &= \frac{4\pi t_0}{w\sqrt{|D|}} \sum_{\alpha} \frac{c(\alpha)}{|\alpha|} \psi\left(\frac{\alpha z_0}{\sqrt{D}}\right) K_1\left(\frac{4\pi|\alpha|t_0}{\sqrt{|D|}}\right). \end{aligned}$$

Since  $F$  is a plusform, we may simplify the sum to

$$(2.10) \quad I_F(A) = \frac{4\pi t_0}{\sqrt{|D|}} \sum_{(\alpha)} \frac{c(\alpha)}{|\alpha|} \tilde{\psi}\left(\frac{\alpha z_0}{\sqrt{D}}\right) K_1\left(\frac{4\pi|\alpha|t_0}{\sqrt{|D|}}\right),$$

the sum being taken over all nonzero  $\alpha \in R$  modulo units.

As in (2.8), this sum converges fairly quickly, and to aid convergence, we seek to choose  $A$  so that  $t_0$  is as large as possible. Write  $\gamma = \begin{pmatrix} a & b \\ \nu c & d \end{pmatrix}$ . Then it is best to take

$$A = \left( \frac{-d}{\nu c}, \frac{1}{|\nu c|} \right), \quad \gamma(A) = \left( \frac{a}{\nu c}, \frac{1}{|\nu c|} \right),$$

and the value of  $t_0$  in both cases is  $1/|\nu c|$ ; in practice, we will try to choose  $\gamma$  so that  $|c|$  is as small as possible. Substituting into (2.10), we find, finally, that

$$\begin{aligned} \Omega(F) &= I_F(\{A, \gamma(A)\}) = I_F(\{A, \infty\}) - I_F(\{\gamma(A), \infty\}) \\ &= \frac{4\pi}{|\nu c|\sqrt{|D|}} \sum_{(\alpha)} \frac{c(\alpha)}{|\alpha|} K_1\left(\frac{4\pi|\alpha|}{|\nu c|\sqrt{|D|}}\right) \left( \tilde{\psi}\left(\frac{-\alpha d}{\nu c\sqrt{D}}\right) - \tilde{\psi}\left(\frac{\alpha a}{\nu c\sqrt{D}}\right) \right). \quad \square \end{aligned}$$

Comparing (2.8) with (2.9), we see that the coefficient of  $|\alpha|$  in the  $K_1$ -term is greater in (2.8) by a factor of at least  $\sqrt{|\nu|} = N(\mathfrak{n})^{1/4}$ ; hence, in practice, we can compute  $\Lambda(F, 1)$  using (2.8) more accurately (given a fixed number of Fourier coefficients  $c(\alpha)$ ) than  $\Omega(F)$  using (2.9). This is the idea behind the second method of computing  $\Omega(F)$ . Similar tricks were used in [8].

*Indirect method.* If  $\Lambda(F, 1) \neq 0$ , then we may compute  $\Omega(F)$  indirectly by computing  $\Lambda(F, 1)$  via (2.8) and dividing by the ratio  $\Lambda(F, 1)/\Omega(F)$ .

From (2.4) we have  $\Lambda(F, 1) = I_F(\{0, \infty\})$ . Let  $\pi$  be any prime not dividing the level  $\mathfrak{n}$ , so that the newform  $F$  is an eigenform for the Hecke operator  $T_\pi$  with eigenvalue  $c(\pi)$ . Integrating the equation  $T_\pi F = c(\pi)F$  from 0 to  $\infty$  gives

$$c(\pi)I_F(\{0, \infty\}) = I_{T_\pi F}(\{0, \infty\}) = I_F(T_\pi(\{0, \infty\})).$$

Now by definition of  $T_\pi$  we have

$$\begin{aligned} T_\pi(\{0, \infty\}) &= \sum_{\alpha \pmod{\pi}} \left\{ \frac{\alpha}{\pi}, \infty \right\} + \{0, \infty\} \\ &= (N(\pi) + 1)\{0, \infty\} - \sum_{\alpha \pmod{\pi}} \left\{ 0, \frac{\alpha}{\pi} \right\}. \end{aligned}$$

Hence,

$$(2.11) \quad (1 + N(\pi) - c(\pi))I_F(\{0, \infty\}) = \sum_{\alpha \pmod{\pi}} I_F(\{0, \alpha/\pi\}).$$

Now each cycle  $\{0, \alpha/\pi\}$  is in  $H_1(X_0(n), \mathbb{Z})$ , since  $\pi \nmid n$ . Thus, the right-hand side of (2.11) has the form  $n(\pi)\Omega(F)$  with  $n(\pi) \in \mathbb{Z}$ , and we have the result

$$(2.12) \quad \frac{\Lambda(F, 1)}{\Omega(F)} = \frac{n(\pi)}{1 + N(\pi) - c(\pi)}.$$

In practice, it is easy to compute the integer  $n(\pi)$  using modular symbols, by expressing each path  $\{0, \alpha/\pi\}$  in terms of a basis for  $H_1(X_0(n), \mathbb{Z})$  and projecting onto the  $F$ -isotypic eigenspace. For the Euclidean fields this is done using the continued fraction convergents of  $\alpha/\pi$ . In the non-Euclidean cases, a ‘pseudo-Euclidean’ algorithm was presented in [23]; this can be used to determine generalized continued fraction convergents to the same effect.

*Remarks.* 1. From (2.11) it follows that  $\{0, \infty\} \in H_1(X_0(n), \mathbb{Q})$ , and from (2.12) that  $\Lambda(F, 1)/\Omega(F)$  is rational for all rational newforms  $F$ . This fact was first proved for these forms in [13].

2. We may also use (2.12) as a quick way of computing many eigenvalues  $c(\pi)$  of the newform  $F$ , once one such value and the value of  $\Lambda(F, 1)/\Omega(F)$  are known (at least if  $\Lambda(F, 1) \neq 0$ ), since the right-hand side of (2.12) is independent of the prime  $\pi$ . An identical method was used in [8]. If  $\Lambda(F, 1) = 0$ , then a variation on this method can be devised, again similar to the methods of [8].

Thus, to compute the period  $\Omega(F)$ , we first compute the integer  $n(\pi)$  for one prime  $\pi$  not dividing  $n$ , using modular symbols. If  $n(\pi) \neq 0$ , then we compute  $\Lambda(F, 1)$  via (2.8) and set

$$(2.13) \quad \Omega(F) = \Lambda(F, 1) \frac{(1 + N(\pi) - c(\pi))}{n(\pi)}.$$

In §4 we give examples of this method, listing the values of  $\Lambda(F, 1)$  and  $\Omega(F)$  to 8 decimal places, as well as the exact rational value of  $\Lambda(F, 1)/\Omega(F)$  computed using (2.12).

If, on the other hand,  $n(\pi) = 0$ , then  $\Lambda(F, 1) = 0$  and this approach fails. We may use the direct method (2.9), though in practice the number of coefficients  $c(\alpha)$  we need in order to obtain an accuracy of even three or four decimal places is rather large, and computing very many Hecke eigenvalues is time-consuming. Alternatively, we may use the trick of twisting by a quadratic character, as also used (over the rationals) by the first author in [8]. We now describe this method.

Let  $\mathfrak{l} = (\lambda)$  be a prime ideal of the ring of integers  $R$  not dividing  $2n$ , and let  $\chi$  be the quadratic character modulo  $\mathfrak{l}$ . In [6] we described the twisting operator  $R_\chi$  associated with  $\chi$ ; here we denote  $F|R_\chi$  by  $F \otimes \chi$  and summarize the facts which we need. If  $F$  is a newform in  $S(n) = S(\nu)$  and  $\mathfrak{l} = (\lambda)$  and  $\chi$  are as above, then

- (1)  $F \otimes \chi$  is a newform in  $S(n\mathfrak{l}^2)$ ;
- (2) the Fourier coefficients of  $F \otimes \chi$  are  $\chi(\alpha)c(\alpha)$ ;
- (3) if  $F \in S^\sigma(n)$ , then  $F \otimes \chi \in S^\tau(n\mathfrak{l}^2)$ , where  $\tau = \chi(\varepsilon_0)\sigma$ ; in particular, if  $F$  is a plusform and  $\chi(\varepsilon_0) = +1$ , then  $F \otimes \chi$  is also a plusform (here,  $\varepsilon_0$  is a fundamental unit);
- (4) if  $W_\nu F = \epsilon F$ , then  $W_{\nu\lambda^2}(F \otimes \chi) = \chi(-\nu)\epsilon(F \otimes \chi)$ ;

(5) there holds

$$(2.14) \quad \Lambda(F \otimes \chi, 1) = \frac{a_K}{|\lambda|} \int_{\gamma(\lambda)} F \cdot \beta,$$

where

$$\gamma(\lambda) = \sum_{\alpha \pmod{\lambda}} \chi(-\alpha) \{0, \alpha/\lambda\}.$$

The latter two facts are proved in an entirely analogous way to the corresponding results for cusp forms over  $\mathbb{Q}$ .

In (2.14), the “twisting cycle”  $\gamma(\lambda)$  is in the integral homology, since  $\lambda$  is coprime to  $n$ ; hence we may express the integral  $a_K \int_{\gamma(\lambda)} F \cdot \beta$  as an integral multiple of the period  $\Omega(F)$ . This integer  $n(\lambda)$  may be computed using modular symbols by expressing  $\gamma(\lambda)$  in terms of a basis for the integral homology and projecting onto the  $F$ -isotypic eigenspace. Then we obtain the equation

$$\Lambda(F \otimes \chi, 1) = \frac{n(\lambda)}{|\lambda|} \Omega(F).$$

We must choose  $\lambda$ , depending on the form  $F$  as well as the level  $n$ , to have the properties

- (1)  $\chi(\epsilon_0) = +1$  (so that  $F \otimes \chi$  is also a plusform);
- (2)  $\chi(\nu)\epsilon = -1$ , where  $\epsilon$  is the  $W_n$ -eigenvalue of  $F$  as above;
- (3)  $n(\lambda) \neq 0$  (so that  $\Lambda(F \otimes \chi, 1) \neq 0$ ).

The second of these conditions, which is necessary for the third, ensures that the value  $L(F \otimes \chi, 1)$  may be computed by the method described earlier (equation (2.8)). Taking into account the level  $n^2$  and coefficients  $\chi(\alpha)c(\alpha)$  of  $F \otimes \chi$ , we obtain the following result.

**Proposition 2.4.** *Let  $F$  be a newform in  $S^+(n)$  and  $\mathfrak{l} = (\lambda)$  a prime not dividing  $2n$ , satisfying conditions (1)–(3) above. Then*

(1)

$$(2.15) \quad \Lambda(F \otimes \chi, 1) = \frac{8\pi}{\sqrt{|\nu\lambda^2 D|}} \sum_{(\alpha)} \frac{\chi(\alpha)c(\alpha)}{|\alpha|} K_1 \left( \frac{4\pi|\alpha|}{\sqrt{|\nu\lambda^2 D|}} \right);$$

(2) *We have*

$$(2.16) \quad \Omega(F) = \frac{|\lambda|}{n(\lambda)} \Lambda(F \otimes \chi, 1).$$

We have used this method to compute  $\Omega(F)$  whenever  $\Lambda(F, 1) = 0$ . In §4 we give examples of this method, giving in each case the twisting prime  $\lambda$ , the value of  $\Lambda(F \otimes \chi, 1)$  to about eight decimal places, and the nonzero rational number  $|\lambda|\Lambda(F \otimes \chi, 1)/\Omega(F)$ .

There is still one situation in which this method fails: when the level  $n$  is a square, so that  $\nu$  is a square (up to a unit); then we will always have  $\chi(\nu) = +1$  and so condition (2) above will not be attainable when  $\epsilon = +1$ . This only occurred once in the range of our computations, at level (16) over  $\mathbb{Q}(\sqrt{-2})$ . However, in this case the awkward form was already a twist of a second form at the same level for which  $\Lambda(F, 1) \neq 0$ , and the periods of the two forms were easily seen to be equal. Hence, we were never forced to resort

to the less accurate direct method of computing the period  $\Omega(F)$ , although we did in fact compute the periods this way as well in many cases as a check on the calculations.

*Remark.* We need an efficient way of approximating the sum of series of the form (2.8) or (2.11), where the coefficients  $c(\alpha)$  are determined recursively in terms of the  $c(\pi)$  for prime  $\pi$ , when we have the first several values of  $c(\pi)$ . The method we use here is a straightforward generalization to the unique factorization domain  $R$  of the recursive method used in [8], and originally in [1].

### 3. ELLIPTIC CURVES OVER $K$

In this section we describe the elliptic curve computations which were carried out. In each case we first find one elliptic curve  $E$  of conductor  $n$ , defined over  $K$ , for each newform  $F$  for  $\Gamma_0(n)$ . If we have two or more newforms at the same level, we must of course find one curve for each, matching curves with newforms by comparing  $L$ -series. The procedures used to find the curves are described in §3.0. The next step (§3.1) is to find all elliptic curves isogenous to  $E$  over  $K$ . Then for each curve we compute (§§3.2–3.4)

- the order of the torsion subgroup,  $E(K)_{\text{tors}}$ ;
- the periods and area  $\Omega(E)$ ;
- the local factors  $c_p$ .

In addition, for those curves  $E$  for which the corresponding form  $F$  has  $L(F, 1) = 0$ , we look for points of infinite order on  $E(K)$ . In fact, we also know the sign  $\epsilon$  of the functional equation of  $L(F, s)$  as in (2.6), and we expect this to match the parity of the rank of  $E$ . In most cases we have either  $\epsilon = +1$  and  $L(F, 1) \neq 0$ , or  $\epsilon = -1$  and  $L(F, 1) = 0$ , and expect the rank to be 0 or 1, respectively. For two forms over  $\mathbb{Q}(\sqrt{-19})$  we found  $\epsilon = +1$  and  $L(F, 1) = 0$  and expect the corresponding curves to have rank 2; in these cases we do find two independent points of infinite order, and in one case (where the curve is defined over  $\mathbb{Q}$ ) we can confirm that the curve does indeed have rank 2. See §3.5 for details of this example.

The algorithms are described below in some detail, except for Tate's algorithm, which is so well known as to need no extra comment. Some of the algorithms are very similar to those used by the first author in his investigations of modular elliptic curves over  $\mathbb{Q}$ , while in other cases there are new features involved in working over a number field. It is hoped that the ideas we have developed here will be useful in other investigations of elliptic curves over number fields.

**3.0. Finding the curves.** Given a newform  $F$  for  $\Gamma_0(n)$  with rational Hecke eigenvalues  $a_p$ , we wish to find a curve  $E$  of conductor  $n$  whose  $L$ -series  $L(E, s)$  is equal to  $L(F, s)$ , at least up to the first several Euler factors.

Note that every elliptic curve over  $K$  has a global minimal model, since  $K$  has class number 1. Such a model has the standard Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with the coefficients  $a_i$  in the ring of integers  $R$ . Let  $1, \omega$  be the standard  $\mathbb{Z}$ -basis for  $R$ . We may also normalize the equation so that  $a_1, a_2$ , and  $a_3$  are reduced modulo 2, 3, and 2, respectively:  $a_1, a_3 = u + v\omega$  with  $u, v \in \{0, 1\}$ , and  $a_2 = u + v\omega$  with  $u, v \in \{-1, 0, 1\}$ . It is easy to see from the

standard transformation formulae for elliptic curves that the resulting equation for  $E$  is unique in all those fields for which  $R^* = \{+1, -1\}$ ; over  $\mathbb{Q}(\sqrt{-1})$  we get two such equations, and over  $\mathbb{Q}(\sqrt{-3})$  we get three. In the latter cases we choose one of the equations arbitrarily. Such equations will be called *reduced*.

As a first step we ran a blanket search over all reduced equations with  $a_4$  and  $a_6$  in some bounded region, keeping only those curves whose conductors (found using Tate's algorithm) were within the appropriate bound for the field  $K$ . This produced curves of most of the conductors desired. No other curves were found, except for those with complex multiplication in  $K$ , which do not correspond to cusp forms, as remarked in the introduction.

For the remaining conductors a more targeted search was carried out. (This is the same method as the first author used in [7] to find those curves listed as missing in [6].) As well as knowing the conductor of the curve for which we are looking, we also know how many points the curve has modulo  $p$  for several small primes  $p$ , since this number is determined by the traces of Frobenius  $a_p$  which are equal to the known Hecke eigenvalues for the form  $F$ . This gives us a restricted set of values modulo  $p$  for the coefficients of the curve. By using several such auxiliary primes, we can determine the possible coefficients of  $E$  modulo their product  $m = \prod p$ , and hence eventually the coefficients themselves, once  $m$  is large enough that  $a_4$  and  $a_6$  are reduced modulo  $m$ . The primes  $p$  are chosen so that the number of possible equations modulo  $p$  is as small as possible, to speed up the search; if too many primes are needed, then the combinatorial explosion means that the running time becomes prohibitive.

In all but one case we were able to find a curve  $E$  corresponding to the newform  $F$ . This exceptional case is of some interest.

Over  $K = \mathbb{Q}(\sqrt{-43})$  there is a newform  $F$  at level (1), in the 'minus' space  $S^-(1)$ . This form is in fact the base-change lift of a cusp form  $f$  of weight 2 for  $\Gamma_0(43^2)$  over  $\mathbb{Q}$  with coefficients in  $\mathbb{Q}(\sqrt{6})$ , which has 'extra twist' by  $\mathbb{Q}(\sqrt{-43})$  in the sense of [9]. Attached to  $f$  is a two-dimensional abelian variety  $A$  which is simple over  $\mathbb{Q}$ , whose endomorphism algebra over  $\mathbb{Q}(\sqrt{-43})$  is isomorphic to the quaternion algebra  $(\frac{6, -43}{\mathbb{Q}})$ . Since 6 is not a norm from  $\mathbb{Q}(\sqrt{-43})$  to  $\mathbb{Q}$ , this algebra is not split, and hence  $A$  remains simple over  $\mathbb{Q}(\sqrt{-43})$ . If  $\chi$  is a quadratic character of  $R$  with conductor  $q$ , then the twist  $F \otimes \chi$  will be a newform at level  $q^2$  of eigenvalue  $-\chi(-1)$ . In particular, when  $\chi$  is the quadratic character modulo  $q = (\omega)$ , where  $\omega = (1 + \sqrt{-43})/2$ , we obtain a plusform  $F \otimes \chi$  for  $\Gamma_0(q^2) = \Gamma_0(\omega - 11)$  which has no corresponding elliptic curve. This newform (and its conjugate at level  $\bar{\omega}^2$ ) were found in [23].

In all other cases we found an elliptic curve  $E$  of conductor  $n$  whose first 50 traces of Frobenius  $a_p$  agreed with the Hecke eigenvalues of the newform  $F$  for  $\Gamma_0(n)$ , for each of the rational newforms in the range of our investigation over all nine fields.

**3.1. Isogenies.** Given an elliptic curve  $E$  over the field  $K$ , we now wish to find all curves isogenous to  $E$  over  $K$ . We may use Vélú's formulae [20] to find an  $l$ -isogenous curve if we have the coordinates of the points of a subgroup of  $E$  of order  $l$  defined over  $K$ . Finding such coordinates by algebraic means is troublesome, except when the subgroup is pointwise defined over  $K$ , and instead we resort to a floating-point method similar to the one used by the first author in compiling tables of elliptic curves over the rationals.

First we find the period lattice  $\Lambda = [\omega_1, \omega_2]$  of  $E$ ; see §3.3 below for how we do this. For each prime  $l$  that we wish to consider, we list the points  $z \in \mathbb{C}/\Lambda$  of each of the  $l+1$  subgroups of order  $l$ . We then evaluate numerically the Weierstrass functions  $\wp(z)$  and  $\wp'(z)$  to obtain complex floating-point approximations to the  $x$ - and  $y$ -coordinates of the  $l$ -division points. Substituting into Vélú's formulae, we obtain the coefficients of all  $l+1$  curves over  $\mathbb{C}$  which are  $l$ -isogenous to  $E$  over  $\mathbb{C}$ . If these coefficients are close to integers (in  $R$ ), we round them and check that the resulting curve over  $K$  has the right conductor  $n$ . It is possible that the isogenous curve might be defined over  $K$  but with non-integral coefficients; however, it is easy to see from the  $l$ -division equation and Vélú's formulae that at worst we would have  $l^i a_i \in R$  for  $i \in \{1, 2, 3, 4, 6\}$ . Hence, we also try rounding these scaled coefficients.

The resulting program finds  $l$ -isogenous curves very quickly for any given prime  $l$ . We ran it for all primes  $l \leq 13$ , applying it recursively to each new curve found until we had a set of curves closed under  $l$ -isogeny for these values of  $l$ . In the semistable case ( $n$  square-free) this is guaranteed to be a complete isogeny class, since no  $l$ -isogenies can exist for primes  $l > 13$ . To see this, we combine Serre's result [17] that at least one of a pair of semistable  $l$ -isogenous curves must have a point of order  $l$  defined over  $K$ , and Kamienny's result [12] that an elliptic curve over an (arbitrary) quadratic field can have a point of prime order  $l$  only for  $l \leq 13$ .

It is possible that we might have missed higher-degree isogenies in the non-semistable cases.

**3.2. Torsion.** To determine the torsion subgroup of an elliptic curve defined over a number field, we may use the Lutz–Nagell Theorem. The situation is slightly more complicated than over  $\mathbb{Q}$ , on account of the ramified primes: first we have to find a model for the curve in which all torsion points are integral.

**Proposition 3.1.** *Let  $E$  be an elliptic curve defined over a quadratic or cubic number field  $K$  with ring of integers  $R$ , given by an equation*

$$(*) \quad y^2 = x^3 + ax^2 + bx + c,$$

where  $a, b, c \in R$ . If  $P = (x_0, y_0) \in E(K)$  has finite order, then

(1) If  $a = 0$ , or if 3 is unramified in  $K$ , then  $x_0, y_0 \in R$ ;

(2) If 3 is ramified in  $K$ , then  $3^2 x_0, 3^3 y_0 \in R$ , and even  $(\sqrt{-3})^2 x_0, (\sqrt{-3})^3 y_0 \in R$  in the case  $K = \mathbb{Q}(\sqrt{-3})$ .

*Proof.* We use the form of the Lutz–Nagell-type results given in Lang's book [14, Chapter III]. By Theorem 2.1 (op. cit.), if  $P$  has order  $n$  and is not integral, then  $n$  must be a prime power, say  $n = p^m$ , and the denominator of  $x_0$  divides the ideal  $\prod_{p|p} p^{f_p}$ , where  $0 \leq r_p \leq e_p/2$ , and even  $0 \leq r_p \leq e_p/4$  if the coefficient  $a$  of  $x^2$  is zero. Here,  $e_p$  is the ramification degree of  $p$ . In a cubic or quadratic field this forces  $r_p$  to be zero, and  $x_0$  integral, in the case  $a = 0$ . If  $a \neq 0$  and  $p$  is unramified, the same holds.

If  $a \neq 0$ , we can always complete the cube after scaling the equation  $(*)$  as follows: set  $Y = 3^3 y$ ,  $X = 3^2 x + 3a$ ,  $B = 81b - 27a^2$ , and  $C = 729c + 54a^3 - 243ab$ . Then  $(X, Y)$  satisfies the equation

$$(**) \quad Y^2 = X^3 + BX + C,$$

and so  $X(P)$  and  $Y(P)$  are integral as above. Thus  $3^2x_0$  and  $3^3y_0$  are also integral, and  $P$  must have order a power of 3. In the case  $K = \mathbb{Q}(\sqrt{-3})$  we may achieve the same effect with the scaling transformation  $Y = (\sqrt{-3})^3y$ ,  $X = (\sqrt{-3})^2x - a$ ,  $B = 9b - 3a^2$ , and  $C = -27c - 2a^3 + 9ab$ .  $\square$

In practice then, before searching for torsion points, we complete the square in a Weierstrass equation (if necessary) to obtain an equation of the form (\*); when  $K = \mathbb{Q}(\sqrt{-3})$  (the only one of our fields in which 3 is ramified), we carry out a further scaling and complete the cube as above, to obtain an equation of the form (\*\*). We now have a model for our curve in which all torsion points are integral.

Finally, we apply the standard trick to bound the  $y$ -coordinate of torsion points (see [14, Theorem 1.4]): if  $P$  is torsion, then  $P$  and  $2P$  are both integral, and then either  $y(P) = 0$  (and  $P$  has order 2) or  $y(P)^2$  divides the discriminant  $\Delta$ , where  $\Delta = a^2b^2 - 4a^3c + 18abc - 4b^3 - 27c^2$ . This gives us a finite number of values of  $y$  to check; for each, we attempt to solve the cubic for  $x \in R$ , to obtain all torsion points on  $E$ .

Note that we are actually determining all points  $P$  such that both  $P$  and  $2P$  are integral (in the possibly scaled model for  $E$ ), which includes all torsion points, but may also include points of infinite order. To determine whether a given integral point has finite or infinite order, we simply compute multiples  $mP$  successively until either  $mP = 0$ , in which case  $P$  has order  $m$ , or  $mP$  is not integral, in which case  $P$  has infinite order. If we find points of infinite order at this stage, we keep a note of them for later use (see §3.5).

**3.3. Periods.** Let  $E$  be an elliptic curve defined over the complex numbers  $\mathbb{C}$ , given by a Weierstrass equation. Let  $\lambda_1, \lambda_2$  be a  $\mathbb{Z}$ -basis for the period lattice  $\Lambda$ . We wish to compute the periods  $\lambda_i$ , as well as the quantity

$$\Omega(E) = |\operatorname{Im}(\overline{\lambda_1}\lambda_2)|.$$

We do this using Gauss' arithmetic-geometric mean. Write the equation for  $E$  in the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

where the roots  $e_i$  are found as complex floating-point approximations (using Cardano's formula, say). Then the periods are given by

$$\lambda_1 = \frac{\pi}{\operatorname{agm}(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})}, \quad \lambda_2 = \frac{\pi i}{\operatorname{agm}(\sqrt{e_3 - e_1}, \sqrt{e_2 - e_1})}.$$

Notice that we are here computing the agm of pairs of complex numbers. This is a multivalued function: at each stage of the agm algorithm we must make a choice of complex square root. It appears from work of Cox [4] that while a different set of choices does lead to a different value for the agm, the periods we obtain this way will nevertheless be a  $\mathbb{Z}$ -basis for the full period lattice  $\Lambda$ . We have found this to be the case in practice, where we always choose a square root in the right half-plane. The computation of  $\lambda_1$  and  $\lambda_2$  by this method is very fast, as the agm algorithm converges extremely quickly, even in its complex form. As a check on the values obtained, in each case we recomputed the covariants  $c_4 (= 12g_2)$  and  $c_6 (= 216g_3)$  of each curve from  $\lambda_1$  and  $\lambda_2$ , using



the standard formulae

$$c_4 = \left(\frac{2\pi}{\lambda_2}\right)^4 \left(1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1 - q^n}\right), \quad c_6 = \left(\frac{2\pi}{\lambda_2}\right)^6 \left(1 - 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1 - q^n}\right),$$

where  $q = \exp(2\pi i \lambda_1 / \lambda_2)$ . In every case we obtained the correct values (known exactly from the coefficients of the minimal Weierstrass equation) to within computational accuracy.

**3.4. Local factors.** We have implemented Tate's algorithm for elliptic curves over imaginary quadratic fields, in order to compute conductors and minimal equations. The local factors  $c_p$  for all bad primes  $p$  are obtained at the same time.

**3.5. Points of infinite order.** For each curve  $E$  we ran a search program looking for  $K$ -rational points of infinite order on  $E$ . Writing such a point (essentially uniquely) as  $(x, y) = (a/c^2, b/c^3)$  with  $a, b, c \in R$ , and  $\gcd(a, c) = \gcd(b, c) = 1$ , we search through  $c$  (modulo units) and through  $a$  coprime to  $c$ . Given  $a$  and  $c$ , we attempt to solve the appropriate quadratic equation for  $b \in R$ . To speed up this procedure, for each denominator  $c$  we precompute for about 10 auxiliary primes  $p$  the residue classes modulo  $p$  to which  $a$  must belong if the equation for  $b$  is to be soluble modulo  $p$ . Each candidate value of  $a$  can then first be checked to see if it is admissible modulo each auxiliary prime before the more time-consuming step of attempting to solve for  $b$ . This improvement to a naive search resulted in a major time saving in some cases, though for most of the curves on which we expected to find points of infinite order, such a point was found very quickly anyway. (In some cases we had already found such a point during the search for torsion points.)

For those curves  $E$  which are defined over  $\mathbb{Q}$ , we could alternatively just look for  $\mathbb{Q}$ -rational points on both  $E$  and its twist  $E^{(d)}$ , where  $K = \mathbb{Q}(\sqrt{d})$ . In these cases we computed the rank of  $E(K)$  from the elementary result

$$\text{rank}(E(K)) = \text{rank}(E(\mathbb{Q})) + \text{rank}(E^{(d)}(\mathbb{Q})),$$

using our 2-descent program to compute ranks of curves over  $\mathbb{Q}$ . We have not yet implemented a program to compute ranks of general curves over quadratic fields.

For example, take the curve

$$E: \quad y^2 + y = x^3 - x^2 - 2x + 2$$

of conductor  $(3\sqrt{-19})$  over  $K = \mathbb{Q}(\sqrt{-19})$ , which is defined over  $\mathbb{Q}$ . The conductor of  $E$  over  $\mathbb{Q}$  is (57), and  $\text{rank}(E(\mathbb{Q})) = 1$  with generator  $(2, 1)$ . The  $(-19)$ -twist is

$$E^{(-19)}: \quad y^2 + y = x^3 + x^2 - 842x - 10633,$$

which has conductor  $(1083) = (3)(19)^2$ , and rank 1 also. Hence,  $\text{rank}(E(K)) = 2$ , and we have independent points  $(2, 1)$  and  $(1 + 4\omega, 15 - 12\omega)$  on  $E(K)$ . Furthermore, the corresponding form  $F$  at level  $(3\sqrt{-19})$  over  $K$  has the properties that  $L(F, 1) = 0$ , and the sign of the functional equation of  $L(F, s)$  is  $+1$ , so that the order of  $L(F, s)$  at  $s = 1$  is even and at least 2.

## 4. EXAMPLES AND RESULTS

In this final section, we illustrate the methods described above with a series of examples, showing the various different situations which can arise for the nine fields under consideration. Complete tables giving all the results of our computations formed part of [23], but are not included here for reasons of space; they may be obtained from the first author via electronic mail.

We do not give here the Hecke eigenvalues of the newforms; these (for the first 15 primes in each field) can be found in [6] for the Euclidean fields, and in [23] for the non-Euclidean fields. In the following examples we have attempted to obtain eight decimal places accuracy, computing up to 500 Hecke eigenvalues; however in some cases (particularly over the fields  $\mathbb{Q}(\sqrt{-43})$  and  $\mathbb{Q}(\sqrt{-67})$ ) we had to be content with less accuracy.

First we give a table showing, for each field  $K = \mathbb{Q}(\sqrt{-d})$ , the range of levels  $n$  covered and the number of rational newforms  $F$  found. The bounds on the norm  $N(n)$  are taken from [6 and 23]. Here we only count one of each pair of conjugate levels  $n, \bar{n}$ .

$d$	1	2	3	7	11	19	43	67	163
Bound on $N(n)$	500	300	500	300	200	500	230	265	100
Number of forms $F$	39	36	27	17	17	55	7	6	0

Note that no rational newforms were found over  $\mathbb{Q}(\sqrt{-163})$  at the levels considered. It has not yet been possible, for practical implementation reasons, to run the program on higher levels such as (11) or  $(\sqrt{-163})$  over this field, where we would have expected to find rational newforms lifted from  $\mathbb{Q}$ , corresponding to elliptic curves defined over  $\mathbb{Q}$  of conductors 11 and 163, respectively.

**Example 1.** Field:  $K = \mathbb{Q}(\sqrt{-2})$ . Level:  $n = (13 + 8\theta) = (1 - \theta)^2(3 + \theta)$ , where  $\theta = \sqrt{-2}$ . There are two rational newforms in  $S^+(13 + 8\theta)$ , which is two-dimensional.

(a) For the first newform we compute  $\Lambda(F, 1)/\Omega(F) = 1/3$ , using (2.12), and  $\Lambda(F, 1) \simeq 0.58775231$  to eight decimal places, using (2.8) with 50 primes; hence,  $\Omega(F) \simeq 1.76325694$ . We found an isogeny class of three curves of conductor  $(13 + 8\theta)$  corresponding to  $F$  (in the sense that the first 50  $a_p$  for the curves agree with those of  $F$ ):

	$a_1$	$a_2$	$a_3$	$a_4$	$a_6$	$ T $	$c_p$	$\prod c_p/ T ^2$	$\Omega^*$
$A$	0	$-1 + \theta$	1	$1 - \theta$	$\theta$	3	1, 1	1/9	5.28977075
$B$	0	$-1 + \theta$	1	$11 - 11\theta$	$-27 + 3\theta$	3	3, 1	1/3	1.76325692
$C$	0	$-1 + \theta$	1	$-9 + 39\theta$	$-210 - 39\theta$	1	1, 1	1	0.58775231

Here,  $T = E(K)_{\text{tors}}$ . The curves are linked by 3-isogenies:

$$A \xleftrightarrow{3} B \xleftrightarrow{3} C.$$

In each case we have

$$\Omega^* \prod c_p/|T|^2 \simeq 0.58775231 \simeq \Lambda(F, 1)$$

to eight decimal places; moreover, for curve  $B$  we also have exact equality of the ratios  $\prod c_p/|T|^2 = \Lambda(F, 1)/\Omega(F) = 1/3$  and  $\Omega^*(B) \simeq \Omega(F)$  to eight decimal places. Thus, we may say that curve  $B$  is the ‘strong’ curve in the class.

(b) For the second newform at this level,  $\Lambda(F, 1)/\Omega(F) = 1$  with  $\Lambda(F, 1) = \Omega(F) \simeq 2.82769670$  (again using 50 primes). The isogeny class consists of a single curve:

	$a_1$	$a_2$	$a_3$	$a_4$	$a_6$	$ T $	$c_p$	$\prod c_p/ T ^2$	$\Omega^*$
$D$	0	$1 - \theta$	1	$2 - 2\theta$	1	1	1, 1	1	2.82769659

giving agreement as before.

**Example 2.** Field:  $K = \mathbb{Q}(\sqrt{-1})$ . Level:  $n = (13 + 8i)$  (a prime), where  $i = \sqrt{-1}$ . The unique rational newform  $F$  in  $S^+(13 + 8i)$ , which is one-dimensional, has  $\Lambda(F, 1) = 0$ , with the sign of the functional equation being  $-1$ . Using the twisting prime  $\lambda = 3$ , we have  $\Lambda(F \otimes \chi, 1)|\lambda|/\Omega(F) = 2$ , and compute  $\Lambda(F \otimes \chi, 1) \simeq 5.87129440$ , using (2.15) with 300 primes. Hence,  $\Omega(F) \simeq 8.80694160$ . The unique curve we found of conductor  $(13 + 8i)$  is as follows:

	$a_1$	$a_2$	$a_3$	$a_4$	$a_6$	$ T $	$c_p$	$\prod c_p/ T ^2$	$\Omega^*$
$A$	0	$1 - i$	$i$	$-i$	0	1	1	1	8.80694161

Again, we observe that  $\Omega^*(D) \simeq \Omega(F)$  to eight decimal places. In this case we expect the curve to have rank 1, and the rank is certainly positive since the point  $(0, 0)$  has infinite order.

**Example 3.** Field:  $K = \mathbb{Q}(\sqrt{-19})$ . Level:  $n = (2\omega) = (2)(\omega)$ , where  $\omega = (1 + \sqrt{-19})/2$ . The unique rational newform  $F$  in  $S^+(2\omega)$ , which is 1-dimensional, has  $\Lambda(F, 1)/\Omega(F) = 2/3$ , and we compute  $\Lambda(F, 1) \simeq 0.95601768$  (using 50 primes), so that  $\Omega(F) \simeq 1.43402652$ . We found an isogeny class of three curves of conductor  $(2\omega)$  which correspond to  $F$ :

	$a_1$	$a_2$	$a_3$	$a_4$	$a_6$	$ T $	$c_p$	$\prod c_p/ T ^2$	$\Omega^*$
$A$	$\omega$	$1 - \omega$	1	$-1$	0	3	1, 2	2/9	4.30207956
$B$	$\omega$	$1 - \omega$	1	$9 - 5\omega$	$-24 - 2\omega$	3	3, 2	2/3	1.43402652
$C$	$\omega$	$1 - \omega$	1	$-31 - 15\omega$	$-60 - 54\omega$	1	1, 2	2	0.47800884

The curves are linked by 3-isogenies:

$$A \xleftrightarrow{3} B \xleftrightarrow{3} C.$$

For each curve we have  $\Omega^*(E) \prod c_p/|T|^2 \simeq 0.95601768$ , in agreement with  $\Lambda(F, 1)$ ; curve  $B$  is ‘strong’ with  $\prod c_p/|T|^2 = \Lambda(F, 1)/\Omega(F) = 2/3$ , and  $\Omega^*(B) \simeq \Omega(F)$  to eight decimal places.

**Example 4.** Field:  $K = \mathbb{Q}(\sqrt{-3})$ . Level:  $n = (19) = (3 + 2\rho)(2 + 3\rho)$ , where  $\rho = (1 + \sqrt{-3})/2$ . The unique rational newform  $F$  in  $S^+(19)$ , which is 1-dimensional, has  $\Lambda(F, 1) = 0$ ; the sign of the functional equation is  $-1$ .

Using  $\lambda = 3 + \rho$ , we compute  $\Lambda(F \otimes \chi, 1)|\lambda|/\Omega(F) = 2$ , and  $\Lambda(F \otimes \chi, 1) \simeq 5.39169497$  (using 300 primes), so that  $\Omega(F) \simeq 9.72001634$ . We found an isogeny class of five curves of conductor (19) which correspond to  $F$ , linked by three-isogenies:

$$\begin{array}{ccccc} & & A & & \\ & & \updownarrow 3 & & \\ D & \xleftrightarrow{3} & B & \xleftrightarrow{3} & E \\ & & \updownarrow 3 & & \\ & & C & & \end{array}$$

	$a_1$	$a_2$	$a_3$	$a_4$	$a_6$	$ T $	$c_p$	$\prod c_p/ T ^2$	$\Omega^*$
$A$	0	$-\rho$	1	$-1 + \rho$	0	3	1, 1	1/9	9.72001634
$B$	0	$-\rho$	1	$9 - 9\rho$	-15	9	3, 3	1/9	3.24000545
$C$	0	$-\rho$	1	$769 - 769\rho$	-8470	3	1, 1	1/9	1.08000182
$D$	0	$-\rho$	1	$-31 - 99\rho$	$74 - 498\rho$	3	1, 9	1	1.08000182
$E$	0	$-\rho$	1	$99 + 31\rho$	$-424 + 498\rho$	3	9, 1	1	1.08000182

Here we can only compare periods, and note that  $\Omega^*(A) \simeq \Omega(F)$  to eight decimal places, so that  $A$  is the ‘strong’ curve. The point  $(1, 0)$  has infinite order on curve  $A$ , which we expect to have rank 1.

**Example 5.** Field:  $K = \mathbb{Q}(\sqrt{-1})$ . Level:  $n = (6 + 6i) = (1 + i)^3(3)$ . The unique rational newform  $F$  in  $S^+(6 + 6i)$ , which is 1-dimensional, has  $\Lambda(F, 1)/\Omega(F) = 1/8$ ; the sign of the functional equation is  $+1$ . We compute  $\Lambda(F, 1) \simeq 0.45441838$ , so that  $\Omega(F) \simeq 3.63534702$ . We found an isogeny class of six curves of conductor  $(6 + 6i)$  which correspond to  $F$ , linked by two-isogenies:

$$\begin{array}{ccccccc} A & \xleftrightarrow{2} & B & \xleftrightarrow{2} & C & \xleftrightarrow{2} & E \\ & & \updownarrow 2 & & \updownarrow 2 & & \\ & & D & & F & & \end{array}$$

	$a_1$	$a_2$	$a_3$	$a_4$	$a_6$	$ T $	$c_p$	$\prod c_p/ T ^2$	$\Omega^*$
$A$	0	1	0	1	0	8	4, 1	1/16	7.27069404
$B$	$1 + i$	$-i$	$1 + i$	$1 - i$	$-i$	8	2, 2	1/16	7.27069404
$C$	$1 + i$	$-i$	$1 + i$	$6 - i$	$4i$	8	2, 4	1/8	3.63534702
$D$	$1 + i$	$-i$	$1 + i$	$16 - i$	$-28i$	4	2, 1	1/8	3.63534702
$E$	$1 + i$	$-i$	$1 + i$	$-4 - i$	$22i$	8	2, 8	1/4	1.81767351
$F$	$1 + i$	$-i$	$1 + i$	$96 - i$	$346i$	4	2, 2	1/4	1.81767351

For all curves we have  $\Omega^* \prod c_p/|T|^2 \simeq 0.45441838 \simeq \Lambda(F, 1)$  to eight decimal places; however, there are now *two* curves in the class,  $C$  and  $D$ , which might be considered as ‘strong’, with  $\Omega^*(C) = \Omega^*(D) \simeq \Omega(F)$  and  $\prod c_p/|T|^2 = \Lambda(F, 1)/\Omega(F) = 1/8$ .

**Example 6.** Field:  $K = \mathbb{Q}(\sqrt{-19})$ . Level:  $n = (3 - 6\omega) = (3)(\sqrt{-19})$ , where  $\omega = (1 + \sqrt{-19})/2$ . The space  $S^+(2\omega)$  is 5-dimensional, with a two-dimensional space of oldforms from level  $(\sqrt{-19})$  and three newforms. One of these shows a new phenomenon which can occur. We have  $\Lambda(F, 1)/\Omega(F) = 16/5$ , and we compute (using 200 primes)  $\Lambda(F, 1) \simeq 1.99511543$ , so that  $\Omega(F) \simeq 0.62347357$ . We found an isogeny class of two 5-isogenous curves of conductor  $(3 - 6\omega)$  which correspond to  $F$  (these curves are defined over  $\mathbb{Q}$  with conductor (57) over  $\mathbb{Q}$ ):

	$a_1$	$a_2$	$a_3$	$a_4$	$a_6$	$ T $	$c_p$	$\prod c_p/ T ^2$	$\Omega^*$
$A$	0	1	1	20	-32	5	10, 2	4/5	0.62347357
$B$	0	1	1	-4390	-113432	1	2, 2	4	0.12469471

For each curve we have  $\Omega^* \prod c_p/|T|^2 \simeq 0.49877886$ , which is  $1/4$  the value of  $\Lambda(F, 1)$ ; also no curve has  $\prod c_p/|T|^2 = 16/5 = \Lambda(F, 1)/\Omega(F)$ , though  $\Omega^*(A) \simeq \Omega(F)$ . Hence, if we were to postulate that both curves had a non-trivial Tate-Shafarevich group  $\text{III}$  of order 4, then the Birch-Swinnerton-Dyer conjecture would predict that

$$L(A, 1) = \Omega^*(A)|\text{III}| \prod c_p/|T|^2 \simeq 4 * 0.49877886 \simeq 1.99511542 \simeq \Lambda(F, 1),$$

and we would also have (for curve  $A$ )

$$|\text{III}| \prod c_p/|T|^2 = 16/5 = \Lambda(F, 1)/\Omega(F),$$

as well as  $\Omega^*(A) \simeq \Omega(F)$ , so that  $A$  would be the ‘strong’ curve. It would be interesting to carry out a 2-descent on these curves to support this hypothetical value of  $|\text{III}|$ .

It is also interesting to notice that of the other two newforms at this level, one has the properties that  $\Lambda(F, 1) = 0$  with the sign of the functional equation being  $+1$ , and the corresponding curve has rank 2 (see §3.5). This phenomenon, where a curve of rank 2 appears at the same level as one with nontrivial  $\text{III}$ , occurred twice in the first author’s computations over the rationals in [8], with conductors 571 and 681.

**Example 7.** Field:  $K = \mathbb{Q}(\sqrt{-43})$ . Level:  $n = (13 + \omega)$  (a prime), where  $\omega = (1 + \sqrt{-43})/2$ . The unique rational newform  $F$  in  $S^+(13 + \omega)$ , which is one-dimensional, has  $\Lambda(F, 1) = 0$ , with the sign of the functional equation being  $-1$ . Using the twisting prime  $\lambda = 2 - \omega$ , we have  $\Lambda(F \otimes \chi, 1)|\lambda|/\Omega(F) = 2$ , and compute  $\Lambda(F \otimes \chi, 1) \simeq 1.22122769$ , using (2.15) with 400 primes. Hence,  $\Omega(F) \simeq 2.20159953$ . The unique curve we found of conductor  $(13 + \omega)$  is as follows:

	$a_1$	$a_2$	$a_3$	$a_4$	$a_6$	$ T $	$c_p$	$\prod c_p/ T ^2$	$\Omega^*$
$A$	0	$-\omega$	$1 + \omega$	-2	$1 - \omega$	1	1	1	2.20155358

Again, we observe that  $\Omega^*(A)$  and  $\Omega(F)$  are approximately equal. In this case we expect the curve to have rank 1, and the rank is certainly positive since the point  $(-1, -2)$  has infinite order.

**Example 8.** Field:  $K = \mathbb{Q}(\sqrt{-67})$ . Level:  $n = (3\omega) = (3)(\omega)$ , where  $\omega = (1 + \sqrt{-67})/2$ . The unique rational newform  $F$  in  $S^+(3\omega)$ , which is 7-dimensional, has  $\Lambda(F, 1) = 0$ , with the sign of the functional equation being  $-1$ . Using the twisting prime  $\lambda = 1 - \omega$ , we have  $\Lambda(F \otimes \chi, 1)|\lambda|/\Omega(F) = 8$ , and compute  $\Lambda(F \otimes \chi, 1) \simeq 1.03780493$ , using (2.15) with 400 primes. Hence,  $\Omega(F) \simeq 0.53487242$ . The unique curve we found of conductor  $(3\omega)$  is as follows:

	$a_1$	$a_2$	$a_3$	$a_4$	$a_6$	$ T $	$c_p$	$\prod c_p/ T ^2$	$\Omega^*$
$A$	$\omega$	$1 + \omega$	$\omega$	$-1 - 3\omega$	$16 - 5\omega$	1	5, 4	20	0.53058984

Again, we observe that  $\Omega^*(A)$  and  $\Omega(F)$  are approximately equal. In this case we expect the curve to have rank 1, and the rank is certainly positive since the point  $(-\omega, -4)$  has infinite order.

*Final remarks.* As seen in Example 5, we did not always find a unique ‘strong’ curve in each isogeny class. Also, we may look at a class of curves defined over  $\mathbb{Q}$ , such as those of conductor (11) over  $\mathbb{Q}$ , and see how they behave in the various quadratic fields. We find that over all nine fields the class still contains just the three curves (linked by 5-isogenies) with Antwerp codes 11A, 11B, 11C. Of these, the ‘strong Weil curve’ over  $\mathbb{Q}$  is 11B. Over the eight quadratic fields  $\mathbb{Q}(\sqrt{-d})$ , excluding  $\mathbb{Q}(\sqrt{-163})$ , we find that for  $d = 1, 3, 11$ , and  $67$  the rank is 0 and 11B is the strong curve, while for  $d = 2, 7, 19$ , and  $43$  the rank is 1 and 11A is the strong curve. We have no explanation for this ‘coincidence’.

#### BIBLIOGRAPHY

1. J. P. Buhler and B. H. Gross, *Arithmetic on curves with complex multiplication*. II, *Invent. Math.* **79** (1985), 11–29.
2. J. P. Buhler, B. H. Gross, and D. B. Zagier, *On the conjecture of Birch and Swinnerton Dyer for an elliptic curve of rank 3*, *Math. Comp.* **44** (1985), 473–481.
3. J. W. S. Cassels, *Arithmetic on curves of genus 1 (IV). Proof of the Hauptvermutung*, *J. Reine Angew. Math.* **211** (1962), 95–112.
4. D. Cox, *The arithmetic-geometric mean of Gauss*, *Enseign. Math.* **30** (1984), 270–330.
5. J. E. Cremona, *Modular symbols*, D.Phil. thesis, Oxford, 1981.
6. ———, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, *Compositio Math.* **51** (1984), 275–323.
7. ———, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields (Addendum and Errata)*, *Compositio Math.* **63** (1987), 271–272.
8. ———, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, 1992.
9. ———, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, *J. London Math. Soc.* (2) **45** (1992), 404–416.
10. S. Friedberg, *On the imaginary quadratic Doi-Naganuma lifting of modular forms of arbitrary level*, *Nagoya Math. J.* **92** (1983).
11. P. Gérardin, J. P. Labesse, *Base change problem for  $GL(2)$* , *Automorphic Forms, Representations and L-functions*, Proc. Sympos. Pure Math., vol. 33 (Part 2), Amer. Math. Soc., Providence, RI, 1979, pp. 115–133.
12. S. Kamienny, *Torsion points on elliptic curves*, *Bull. Amer. Math. Soc.* (N. S.) **23** (1990), 371–373.
13. P. F. Kurčanov, *Cohomology of discrete groups and Dirichlet series connected with Jacquet-Langlands cusp forms*, *Math. USSR Izv.* **12** (1978), 543–555.
14. S. Lang, *Elliptic curves and Diophantine analysis*, Springer-Verlag, Berlin and New York, 1978.
15. J. Elstrodt, F. Grunewald, and J. Mennicke, *On the group  $PSL_2(\mathbb{Z}[i])$* , *J. Arith.* 1980, LMS Lecture Notes, vol. 56, Cambridge Univ. Press, 1981.
16. T. Miyake, *On automorphic forms for  $GL(2)$  and Hecke operators*, *Ann. of Math.* **94** (1971), 174–189.
17. J.-P. Serre, *Propriétés galoisiennes des points d’ordre finis des courbes elliptiques*, *Invent. Math.* **15** (1972), 259–331.
18. J. H. Silverman, *Computing heights on elliptic curves*, *Math. Comp.* **51** (1988), 339–358.
19. G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, *Invent. Math.* **98** (1989), 75–106.
20. J. Vêlu, *Isogénies entre courbes elliptiques*, *C. R. Acad. Sci. Paris* **273** (1971), 238–241.

21. A. Weil, *Zeta functions and Mellin transforms*, Colloquium on Algebraic geometry, Bombay, 1968.
22. ———, *Dirichlet series and automorphic forms*, Lecture Notes in Math., vol. 189, Springer-Verlag, Berlin and New York, 1971.
23. E. Whitley, *Modular symbols and elliptic curves over imaginary quadratic number fields*, Ph.D. thesis, Exeter University, 1990.

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

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