ABELIAN VARIETIES WITH EXTRA TWIST, CUSP FORMS, AND ELLIPTIC CURVES OVER IMAGINARY QUADRATIC FIELDS

J. E. CREMONA

ABSTRACT

This paper concerns certain two-dimensional abelian varieties A which are $\mathbb{Q}$-simple factors of $J_0(N)$ and have extra twist by the character associated to a quadratic number field k. Results of Ribet [22] and Momose [21] are used to give a simple necessary and sufficient condition for A to split over k. The L-series of A over k is the square of the Mellin transform of a cusp form of weight 2 over k with rational integer coefficients which, if A does not split over k, is thus *not* the L-series of any elliptic curve defined over k. This answers negatively a question raised by the author [5] and others [8, 15] in relation to a Weil–Taniyama conjecture for imaginary quadratic number fields.

All examples coming from $J_0(N)$ with $N \leqslant 300$ are given explicitly. The complex multiplication case is also considered in more detail: if A has CM by an imaginary quadratic order $\mathcal{O}$, it is shown that $\mathcal{O}$ must have class number 1 or 2. An explicit construction is given for these (finitely many) cases.

1. *Introduction*

In this paper we consider certain abelian varieties defined over $\mathbb{Q}$ which arise as simple factors of the Jacobian variety $J_0(N)$ of the modular curve $X_0(N)$. These abelian varieties with 'extra twist' were investigated fully by Ribet [22] and Momose [21]. Here we shall be interested in the case where the variety A is two-dimensional and the extra twist is given by the character attached to a quadratic field k; the L-series of A then turns out to be the Mellin transform $L(F, s)$ of a cuspidal automorphic form F of weight 2 over k, with rational integer coefficients. Such cusp forms, for imaginary quadratic k, have been studied by the author in [4, 5], and others [8, 15], seeking a Weil–Taniyama-type correspondence between cusp forms of weight 2 and elliptic curves over k. Our main result (Theorem 5) is that if A remains simple over k then $L(F, s)$ is *not* the L-series of an elliptic curve defined over k. We give explicit examples of this phenomenon in Section 3; these provide counterexamples to the conjecture, stated in [4, 5], that such an elliptic curve would always exist. The possibility of such counterexamples was raised in [8, p. 267], but no examples were given there.

In order to decide whether A splits over k, we derive a simple necessary and sufficient condition (Corollary to Theorem 1) from the results of [21, 22], in which the structure of the endomorphism algebra of A is determined (Theorem 1).

These exceptional forms F over k, whose Mellin transforms are not L-series of elliptic curves over k, are lifts of forms over $\mathbb{Q}$; this lifting of forms is described in Section 4. On the other hand, if a lifted form F is associated with the curve E then for each quadratic character ε of $\mathrm{Gal}(\bar{k}/k)$ the twist $F \otimes \varepsilon$ of F by ε is associated with the corresponding twisted curve, and $F \otimes \varepsilon$ will not be a lift unless ε is invariant under $\mathrm{Gal}(k/\mathbb{Q})$. So we can restate the question posed in [8, problems 2 and 2′] as follows.

Received 23 July 1990.

1991 *Mathematics Subject Classification* 11F.

Let F be a cuspidal automorphic newform for $\Gamma_0(\mathbf{a})$, with $\mathbf{a}$ an ideal of the imaginary quadratic field k, with rational integer coefficients. Is there *either* an elliptic curve E over k with $L(F,s) = L(E/k,s)$, *or* a quadratic character ε of $\mathrm{Gal}(\bar{k}/k)$ such that $F \otimes \varepsilon$ is the lift of a form f over $\mathbb{Q}$?

In the latter case, $L(F \otimes \varepsilon, s) = L(A,s)$ for some 2-dimensional abelian variety A over $\mathbb{Q}$, which is the quotient of some $J_0(N)$. But in the former case, the problem of constructing the curve E from the form geometrically remains unsolved.

In Section 2 we describe the two-dimensional abelian varieties A with extra twist, and their endomorphism algebras, and give the condition for A to split over the twisting field k. We discuss the case where A also has complex multiplication by an imaginary quadratic field K, and show that K must have class number 1 or 2, so that only finitely many such K occur. In Section 3 we give all examples which come from $X_0(N)$ for $N \leqslant 300$, and give explicitly the construction of examples with complex multiplication. In Section 4 we discuss the application to cuspidal automorphic forms over k.

Thanks are due to Gross and Ribet for encouragement and useful suggestions, and to the referee of a previous version of this paper who made several simplifications, especially in the proof of Theorem 2. The computations described in Section 3 were carried out at the Kiewit Computation Centre at Dartmouth College, partly with programs written in PASCAL (to compute the homology and Hecke eigenvalues) and partly with the MACSYMA symbolic manipulation package (to manipulate the period matrices and perform calculations with multiple precision complex numbers and algebraic integers).

Notation

$\mathrm{End}(A)$	The ring of endomorphisms of the abelian variety A
$\mathrm{End}_M(A)$	The ring of endomorphisms of A defined over the field M
$\mathrm{End}^0(A)$	$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$
$\mathrm{End}^0_M(A)$	$\mathrm{End}_M(A) \otimes_{\mathbb{Z}} \mathbb{Q}$
$\left(\frac{a,b}{F}\right)$	The quaternion algebra of dimension 4 over the field F, with basis 1, i, j and k satisfying $i^2 = a, j^2 = b$, and $k = ij = -ji$

2. *Cusp forms of weight* 2 *with extra twists*

For a positive integer N, let $S_2(N)$ denote the space of cusp forms of weight 2 for the group $\Gamma_0(N)$. Suppose that $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ is a newform in $S_2(N)$ with the following properties:

(1) $K_f = \mathbb{Q}(a_1, a_2, a_3, \ldots)$ is the real quadratic field $\mathbb{Q}(\sqrt{d})$, d squarefree;

(2) there exists a quadratic Dirichlet character χ such that for all primes p not dividing N,

$$a_p^\sigma = \chi(p) a_p,$$

where σ is the non-trivial automorphism of $K_f/\mathbb{Q}$.

The conjugate form f^σ with coefficients a_n^σ is then also a newform in $S_2(N)$. Let $k = \mathbb{Q}(\sqrt{r})$ be the quadratic field associated with χ, where $|r|$ is the conductor of χ, and N is divisible by r^2. The pair (σ, χ) is a 'twist of f' in the sense of [21], and f has an 'extra twist' in the sense of [22].

Let A be the 2-dimensional abelian variety over $\mathbb{Q}$ attached to f. Then $\operatorname{End}^0_{\mathbb{Q}}(A) \cong K_f$ by [**28**, Theorem 7.14]. The full endomorphism algebra of A may be determined from the more general results of [**22**, Theorem 5.1; **21**, Theorem 4.1]; in our case we have the following result.

THEOREM 1. *Let $f \in S_2(N)$ be a newform satisfying conditions* (1) *and* (2) *above, and A the associated abelian variety. Assume that f does not have complex multiplication. Then*

$$\operatorname{End}^0(A) = \operatorname{End}^0_k(A) \cong \left(\frac{d, r}{\mathbb{Q}}\right).$$

Note that if f does not have complex multiplication then the character χ in condition (2) is uniquely determined.

Explicitly, $\operatorname{End}^0(A)$ is generated as a K_f-vector space by the identity 1_A and a twisting endomorphism η_χ coming from the twisting character χ, first defined by Shimura in [**27**, §4]. In the complex representation of $\operatorname{End}^0(A)$, acting on the tangent space at the origin identified with the $\mathbb{C}$-span of f and f^σ, this twist η_χ has matrix

$$\begin{pmatrix} 0 & \sqrt{r} \\ \sqrt{r} & 0 \end{pmatrix},$$

and

$$\operatorname{End}^0(A) \cong \left\{ \begin{pmatrix} \alpha & \beta\sqrt{r} \\ \beta^\sigma \sqrt{r} & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in K_f \right\}.$$

COROLLARY. (We use the notation and hypotheses of Theorem 1.) *A splits over k into a product of two elliptic curves if and only if d is a norm from k to $\mathbb{Q}$; or, equivalently, if and only if r is a norm from K_f to $\mathbb{Q}$.*

Proof. These conditions are equivalent to the quaternion algebra $\left(\frac{d, r}{\mathbb{Q}}\right)$ being split over $\mathbb{Q}$ by [**18**, Theorem 2.7], which in turn is equivalent to A splitting over k, by Theorem 1.

THEOREM 2. *With the notation and hypothesis of Theorem* 1, *suppose that k is real* (*so $r > 0$*). *Then A does split over k, whether or not f has complex multiplication.*

Proof. Since $\operatorname{End}^0_k(A)$ contains $D = K_f + K_f \cdot \eta_\chi$ which is a 4-dimensional central simple algebra over $\mathbb{Q}$ consisting of endomorphisms defined over $\mathbb{R}$; and D has a 2-dimensional rational representation on the subspace of $H_1(A, \mathbb{Q})$ fixed by complex conjugation, it follows that $D \cong M_2(\mathbb{Q})$. So $\operatorname{End}^0_k(A)$ is not a division algebra, and A splits over k.

REMARK. More generally, if A is an abelian variety of dimension g defined over $\mathbb{R}$, and $\operatorname{End}^0_{\mathbb{R}}(A)$ contains a central simple algebra D of dimension g^2 over $\mathbb{Q}$, then A splits (by the same proof).

THEOREM 3. *Let the hypotheses be as in Theorem* 1. *If some prime p divides N but p^2 does not divide N, then A splits over k.*

Proof. This follows from [**23**] (Theorem 3 and the remark following).

PROPOSITION 1. *With notation and hypothesis as in Theorem 1, if A is isogenous to a product $C_1 \times C_2$ of elliptic curves, then C_1 and C_2 are isogenous.*

Proof. If not, then we would have

$$\mathrm{End}^0(A) = \mathrm{End}^0(C_1 \times C_2) \cong \mathrm{End}^0(C_1) \oplus \mathrm{End}^0(C_2).$$

Since each $\mathrm{End}^0(C_i)$ is isomorphic either to $\mathbb{Q}$ or to an imaginary quadratic field, this would imply that $\mathrm{End}^0(A)$ was a commutative algebra, contradicting the fact that $\mathrm{End}^0(A)$ contains a non-commutative subalgebra.

The complex multiplication case

For the rest of this section, we shall suppose that in addition to properties (1) and (2) the form f has complex multiplication by the imaginary quadratic field $K = \mathbb{Q}(\sqrt{R})$, with associated character ψ of conductor $|R|$. Then f has a total of four twists: (ι, ε), (ι, ψ), (σ, χ), and $(\sigma, \chi\psi)$ (in the notation of **[21]**) where $\{\iota, \sigma\} = \mathrm{Gal}(K_f/\mathbb{Q})$. Since ψ is imaginary we may choose notation so that χ is imaginary and $\chi\psi$ real. The field $k_1 = \mathbb{Q}(\sqrt{(Rr)})$ associated with $\chi\psi$ is thus real quadratic, and by Theorem 2, A splits over k_1.

As is well known **[26]**, A is isogenous to a product of two copies of an elliptic curve E with complex multiplication by K, and $\mathrm{End}^0(A) \cong M_2(K)$, an 8-dimensional algebra over $\mathbb{Q}$. Each of the twists χ, ψ and $\chi\psi$ gives rise to an endomorphism of A as before (η_χ, η_ψ, and $\eta_{\chi\psi}$ respectively), defined over the corresponding quadratic field. Using the same representation as above these endomorphisms have matrices

$$\begin{pmatrix} 0 & \sqrt{r} \\ \sqrt{r} & 0 \end{pmatrix}, \quad \begin{pmatrix} \sqrt{R} & 0 \\ 0 & \sqrt{R} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & \sqrt{(Rr)} \\ \sqrt{(Rr)} & 0 \end{pmatrix}$$

respectively. We can thus determine the structure of $\mathrm{End}^0_M(A)$ for each of the relevant fields M, as in Table 1.

TABLE 1. *Structure of* $\mathrm{End}(A)$ *in the complex multiplication case*

Field of definition M	Structure of $\mathrm{End}^0_M(A)$	Basis over $\mathbb{Q}(\sqrt{d})$
$\mathbb{Q}$	$\mathbb{Q}(\sqrt{d})$	1
$\mathbb{Q}(\sqrt{(Rr)})$	$\left(\dfrac{d, Rr}{\mathbb{Q}}\right) \cong M_2(\mathbb{Q})$	$1, \eta_{\chi\psi}$
$\mathbb{Q}(\sqrt{r})$	$\left(\dfrac{r, d}{\mathbb{Q}}\right)$	$1, \eta_\chi$
$\mathbb{Q}(\sqrt{R})$	$\mathbb{Q}(\sqrt{d}, \sqrt{R})$	$1, \eta_\psi$
$\mathbb{Q}(\sqrt{r}, \sqrt{R})$	$\left(\dfrac{r, d}{\mathbb{Q}(\sqrt{R})}\right) \cong M_2(\mathbb{Q}(\sqrt{R}))$	$1, \eta_\chi, \eta_\psi, \eta_{\chi\psi}$

In particular, we see that all endomorphisms of A are generated by Hecke operators and twists, and are defined over the biquadratic field $\mathbb{Q}(\sqrt{r}, \sqrt{R})$.

THEOREM 4. *The field $K = \mathbb{Q}(\sqrt{R})$ has class number 1 or 2. In the latter case, its Hilbert class field H is $K(\sqrt{(Rr)}) = \mathbb{Q}(\sqrt{r}, \sqrt{R})$ and A does not split over $k = \mathbb{Q}(\sqrt{r})$. Over $\mathbb{Q}(\sqrt{(Rr)})$, A is isogenous to a product of two copies of an elliptic curve E with complex multiplication by an order $\mathcal{O}$ in K of class number 1 or 2.*

TABLE 2. *Imaginary quadratic orders with class number* 2

R_0	$h(K)$	$[\mathcal{O}_K:\mathcal{O}]$	r_0
-5	2	1	-1
-6	2	1	-3
-10	2	1	-2
-13	2	1	-1
-15	2	1	-3
-22	2	1	-11
-35	2	1	-7
-37	2	1	-1
-51	2	1	-3
-58	2	1	-2
-91	2	1	-7
-115	2	1	-23
-123	2	1	-3
-187	2	1	-11
-235	2	1	-47
-267	2	1	-3
-403	2	1	-31
-427	2	1	-7
-1	1	3	-3
-1	1	4	-2
-1	1	5	-5
-2	1	2	-1
-3	1	4	-1
-3	1	5	-15
-3	1	7	-7
-7	1	4	-1
-11	1	3	-3
-15	2	2	-3

Proof. As observed above, by Theorem 2, A splits over $\mathbb{Q}(\sqrt{(Rr)})$ as a product $E\times E$ (up to isogeny) where $\mathrm{End}^0(E)\cong K$. Then E is defined over $\mathbb{Q}(\sqrt{(Rr)})$ and so in particular $j(E)\in\mathbb{Q}(\sqrt{(Rr)})$. *Let* $\mathcal{O}=\mathrm{End}(E)$, an order in K. Then

$$H=K(j(\mathcal{O}_K))\subseteq K(j(\mathcal{O}))=K(j(E))\subseteq K(\sqrt{(Rr)})$$

by [**19**, Chapter 10, Theorems 1 and 6]. Thus either $H=K$ or $H=K(\sqrt{(Rr)})$, as required.

Lastly, if A splits over $\mathbb{Q}(\sqrt{r})$ we have similarly $H\subseteq K(\sqrt{r})$. Since $K(\sqrt{r})\cap K(\sqrt{Rr})=K$ this gives $H=K$.

COROLLARY. *Only finitely many fields K arise as complex multiplication fields in this way.*

Proof. There are only finitely many fields with class number 1 or 2: see [**29**] or [**2**].

Starting with a quadratic complex multiplication field K with class number 1 or 2, one can determine whether or not there is an example of an abelian variety A as in the Theorem, and if so, construct it. For simplicity, we consider only the case where $\mathcal{O}$ is the maximal order $\mathcal{O}_K$ of K.

If A, E are as in Theorem 4, then E is a $\mathbb{Q}$-curve in the sense of [**14**, §11] since it is isogenous to its conjugate by Proposition 1. Such curves do not exist for

$R = -5$, -13, or -37 by [14, (11.3)] but do exist for the other 15 fields with class number 2. The corresponding level N is then R^2 if R is odd and $4R^2$ if R is even. The construction of such examples is given in the next section.

For reference, we give in Table 2 the 28 imaginary quadratic orders $\mathcal{O}$ of class number 2. In the table, R_0 and r_0 are the squarefree parts of R and r respectively.

3. *Examples*

There are twelve 2-dimensional abelian varieties A which are $\mathbb{Q}$-simple factors of the 'new' part of $J_0(N)$ for $N \leqslant 300$, and which have an extra twist by an imaginary quadratic field k, to which the previous results apply. Of these, two have complex multiplication (by $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-15})$) and two (one with complex multiplication and one without) fail to split over the twisting field k. We summarise the facts for each in Tables 3 and 4. In Table 3,

TABLE 3

#	N	K_f	a_2	a_3	a_5	a_7	a_{11}	k
1	$63 = 3^2\cdot 7$	$\mathbb{Q}(\sqrt{3})$	$\sqrt{3}$	$+$	$-2\sqrt{3}$	$-$	$2\sqrt{3}$	$\mathbb{Q}(\sqrt{-3})$
2	$81 = 3^4$	$\mathbb{Q}(\sqrt{3})$	$-\sqrt{3}$	$-$	$\sqrt{3}$	2	$2\sqrt{3}$	$\mathbb{Q}(\sqrt{-3})$
3	$98 = 2\cdot 7^2$	$\mathbb{Q}(\sqrt{2})$	$-$	$-\sqrt{2}$	$2\sqrt{2}$	$+$	-2	$\mathbb{Q}(\sqrt{-7})$
4	$117 = 3^2\cdot 13$	$\mathbb{Q}(\sqrt{3})$	$-\sqrt{3}$	$+$	0	2	$2\sqrt{3}$	$\mathbb{Q}(\sqrt{-3})$
5	$160 = 2^5\cdot 5$	$\mathbb{Q}(\sqrt{2})$	$+$	$-2\sqrt{2}$	$-$	$2\sqrt{2}$	$4\sqrt{2}$	$\mathbb{Q}(\sqrt{-1})$
6	$189 = 3^3\cdot 7$	$\mathbb{Q}(\sqrt{3})$	$-\sqrt{3}$	$+$	$-\sqrt{3}$	$-$	$\sqrt{3}$	$\mathbb{Q}(\sqrt{-3})$
7	$189 = 3^3\cdot 7$	$\mathbb{Q}(\sqrt{7})$	$-\sqrt{7}$	$-$	$\sqrt{7}$	$+$	$\sqrt{7}$	$\mathbb{Q}(\sqrt{-3})$
8	$196 = 2^2\cdot 7^2$	$\mathbb{Q}(\sqrt{2})$	$-$	$-2\sqrt{2}$	$\sqrt{2}$	$+$	4	$\mathbb{Q}(\sqrt{-7})$
9	$225 = 3^2\cdot 5^2$	$\mathbb{Q}(\sqrt{5})$	$-\sqrt{5}$	$+$	$-$	0	0	$\mathbb{Q}(\sqrt{-3})$
10	$243 = 3^5$	$\mathbb{Q}(\sqrt{3})$	$\sqrt{3}$	$-$	$2\sqrt{3}$	-1	$-2\sqrt{3}$	$\mathbb{Q}(\sqrt{-3})$
11	$243 = 3^5$	$\mathbb{Q}(\sqrt{6})$	$\sqrt{6}$	$-$	$-\sqrt{6}$	2	$\sqrt{6}$	$\mathbb{Q}(\sqrt{-3})$
12	$256 = 2^8$	$\mathbb{Q}(\sqrt{2})$	$-$	$2\sqrt{2}$	0	0	$-2\sqrt{2}$	$\mathbb{Q}(\sqrt{-1})$

TABLE 4

#	N	Split?	CM?	a_1	a_2	a_3	a_4	a_6	Conductor
1	63	yes	no	1	-1	$-\omega$	$5\omega-3$	$1-4\omega$	$(21) = \mathfrak{p}_3^2\mathfrak{p}_7\mathfrak{p}_7'$
2	81	yes	no	-1	-1	ω	$-\omega$	ω	$(27) = \mathfrak{p}_3^6$
3	98	yes	no	-1	$\alpha-2$	$-\alpha$	$\alpha-10$	$-\alpha-8$	$(14) = \mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_7^2$
4	117	yes	no	-1	-1	$1-\omega$	$-4-8\omega$	-11ω	$(39) = \mathfrak{p}_3^2\mathfrak{p}_{13}\mathfrak{p}_{13}'$
5	160	yes	no	0	$i-1$	0	$3+6i$	$5-i$	$(40) = \mathfrak{p}_2^6\mathfrak{p}_5\mathfrak{p}_5'$
6	189	yes	no	-1	-1	$1-\omega$	$-7-2\omega$	$-6-2\omega$	$(63) = \mathfrak{p}_3^4\mathfrak{p}_7\mathfrak{p}_7'$
7	189	yes	no	-1	-1	$-\omega$	$12+16\omega$	$31-28\omega$	$(63) = \mathfrak{p}_3^4\mathfrak{p}_7\mathfrak{p}_7'$
8	196	yes	no	0	$1-\alpha$	0	-4	$2+\alpha$	$(28) = \mathfrak{p}_2^2\mathfrak{p}_{22}'\mathfrak{p}_7^2$
9	225	no	$\mathbb{Q}(\sqrt{-15})$						
10	243	yes	no	-1	-1	$-\omega$	$-6-5\omega$	$-3-7\omega$	$(81) = \mathfrak{p}_3^8$
11	243	no	no						
12	256	yes	$\mathbb{Q}(\sqrt{-2})$	0	$1+i$	0	$-i$	$1-i$	$(64) = \mathfrak{p}_2^{12}$

N is the level;

a_p (for $p = 2, 3, 5, 7, 11$) denotes the T_p-eigenvalue of f if p does not divide N; an entry of '$+$' or '$-$' denotes an eigenvalue of the W_p involution if p divides N;

K_f is the field generated by the coefficients of f;

k is the imaginary quadratic field with character χ, conductor $|r|$, such that r^2 divides N and (σ, χ) is a twist of f.

In Table 4, two columns indicate whether or not A splits over k, and whether or not A has complex multiplication. In the latter case, the complex multiplication field K is given.

Lastly, when A splits over k as a product (up to isogeny) of two elliptic curves, the coefficients a_1, a_2, a_3, a_4 and a_6 (in $\mathcal{O}_k$) of a minimal equation

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

of one of the curves is given, with the conductor of this curve over k. The other curve is the conjugate of this one. We have set $i = \sqrt{-1}, \omega = (1+\sqrt{-3})/2$, and $\alpha = (1+\sqrt{-7})/2$. The ambiguity of the notation $a_2, a_3, \ldots$ is traditional.

Some of the information in these tables (excluding the coefficients and conductors of the curves) may be obtained from existing tables of newforms for $\Gamma_0(N)$ and their eigenvalues. In [3, Table 5] one can determine the values of N for which there is a 2-dimensional $\mathbb{Q}$-simple factor of $J_0(N)$, but there is no information about which quadratic fields are involved and the eigenvalues are not listed, so that it is impossible to tell which have extra twists. More information about the eigenvalues (specifically, numerical approximations to their values for $p \leqslant 11$) can be found in [32] (unpublished). We repeated these calculations, using the modular symbols method described in detail in [7], in order to obtain the exact algebraic eigenvalues a_p, and thus determine which forms have an extra twist. For these forms, in the cases where A splits over k, the eigenvalues a_p for $p < 500$ were computed using methods similar to those in [7] (suitably modified since the a_p are not all rational integers). These were then used to compute numerical approximations to the periods of A and of a curve $E = \pi(A)$, for some suitably chosen endomorphism $\pi \in \mathrm{End}_k(A)$. Here we again use modular symbols to obtain explicit generators for the integral homology $H_1(X_0(N), \mathbb{Z})$, as in [7].

From the periods of E the usual quantities c_4 and c_6 were computed and found to be integers, within computational accuracy (at least 10 decimal places). Minimal equations of the curves were then found by applying Tate's algorithm [31].

For example, for $N = 63$ the computed values were

$$c_4 = 45.00000000000004 - 107.9999999999998\sqrt{-3}$$

and

$$c_6 = 1160.999999999994 + 1133.999999999998\sqrt{-3},$$

and the curve given in Table 4 has $c_4 = 45-108\sqrt{-3}$ and $c_6 = 1161+1134\sqrt{-3}$. The curve with equation

$$y^2 = x^3-27c_4x-54c_6$$

has minimal model

$$y^2+xy-\omega y = x^3-x^2+(5\omega-3)x+(1-4\omega)$$

which has c_4 and c_6 as above, discriminant $\Delta = -3^3(2-\sqrt{-3})^3(2+\sqrt{-3})\omega$ and conductor $(21) = (\sqrt{-3})^2(2-\sqrt{-3})(2+\sqrt{-3})$. Here $\omega = (1+\sqrt{-3})/2$.

In the complex multiplication case ($N = 256$) the equation of E is correct: there are only four curves over $\mathbb{Q}(i)$ with good reduction outside 2 and complex multiplication by $\mathbb{Z}[\sqrt{-2}]$, namely III_1 to III_4 in [30]. The one given is III_1. The equations are also exact in the cases $N = 81$ and $N = 243$ which were computed independently by Koike [17]. There, a different method was used to determine exact equations in these cases, obtaining curves isomorphic to the ones given here. It may be possible to apply that method to the remaining seven cases, but this has not yet been done. For more remarks on examples with complex multiplication, see below.

$N = 63, 98$. The curves here fill gaps in the tables of [**4**, **5**], as does the $(4-5\omega)$-twist of the former, which has conductor $(14+7\omega) = \mathfrak{p}_7^2\mathfrak{p}_7'$. (The other 'missing curves' in [**5**] are listed in [**6**].)

$N = 225$. Here there is complex multiplication by $\mathbb{Q}(\sqrt{-15})$ which has class number 2 with Hilbert class field $\mathbb{Q}(\sqrt{5}, \sqrt{-3})$. The abelian variety A is isogenous to $\mathbb{C}/\mathcal{O}$ with $\mathcal{O}$ the ring of integers in $\mathbb{Q}(\sqrt{-15})$, and $\mathbb{Q}(j(\mathcal{O})) = \mathbb{Q}(\sqrt{5})$. In fact, $j(\mathcal{O}) = -138\,510 + 85995\varepsilon = (3\sqrt{5}(4-\sqrt{5}))^3\varepsilon^{-2}$, where $\varepsilon = (1+\sqrt{5})/2$ is the fundamental unit in $\mathbb{Q}(\sqrt{5})$.

$N = 256$. Here there is complex multiplication by $\mathbb{Z}[\sqrt{-2}]$ which has class number 1. The variety A splits over both $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{2})$ (but not over $\mathbb{Q}$, of course) as follows. Let E be the curve defined over $\mathbb{Q}$ with equation [**7**, 256A1]

$$y^2 = x^3 + x^2 - 3x + 1;$$

E has conductor $N = 256 = 2^8$ over $\mathbb{Q}$, and conductor $(1+i)^{12} = (64)$ over $\mathbb{Q}(i)$. Then A is isogenous over $\mathbb{Q}(i)$ to $E^{(1+i)} \times E^{(1-i)}$, where $E^{(1+i)}$ and $E^{(1-i)}$ denote the $(1+i)$- and $(1-i)$-twists of E respectively; moreover, these twisted curves are 2-isogenous. Over $\mathbb{Q}(\sqrt{2})$, the variety A splits as $E^{(\varepsilon)} \times E^{(\varepsilon^\sigma)}$, where $\varepsilon = 1+\sqrt{2}$. Again, these curves are conjugate and 2-isogenous. All the elliptic curves here have j-invariant $20^3 = 8000$, and have complex multiplication by $\mathbb{Z}[\sqrt{-2}]$, the full ring of integers of $\mathbb{Q}(\sqrt{-2})$.

Construction of examples with complex multiplication

Let K be an imaginary quadratic field with class number 2, discriminant $-D$, and ring of integers $\mathcal{O}$. Let H be the Hilbert class field of K (which is biquadratic over $\mathbb{Q}$), $H^+ = \mathbb{Q}(j(\mathcal{O}))$ the real subfield of H, and k the third quadratic subfield of H. Assume that $D \neq 20$, 52, or 148 (see the remark at the end of Section 2). Let $\mathfrak{c} = (\sqrt{-D})$ if D is odd, or $(2\sqrt{-D})$ if D is even. Let χ_1 be a canonical Hecke character of K with conductor $\mathfrak{c}$ (as in [**25**]) and ϕ the non-trivial ideal class character of K; then $\chi_2 = \chi_1\phi$ is another canonical Hecke character, and χ_1 and χ_2 have values in H. (If D is odd then χ_1 and χ_2 are the only such characters, while if D is even there is another pair: see [**25**].) Set $\chi = \chi_1 \circ N_{H/K}$ $(= \chi_2 \circ N_{H/K})$, a Hecke character of H with values in K. Then we have $L(\chi, s) = L(\chi_1, s)L(\chi_2, s)$. Attached to χ is an elliptic curve E defined over H^+ such that [**14**, (10.3.1)] $L(E/H^+, s) = L(\chi, s)$.

Let $A = R_{H^+/\mathbb{Q}}(E)$ be the 2-dimensional abelian variety obtained by restricting scalars from H^+ to $\mathbb{Q}$; then over H we have $A \cong E \times E^\sigma$, where $\langle\sigma\rangle = \mathrm{Gal}(H^+/\mathbb{Q})$. Since $L(A/\mathbb{Q}, s) = L(E/H^+, s)$ we have

$$L(A/\mathbb{Q}, s) = L(E/H^+, s) = L(\chi, s) = L(\chi_1, s)L(\chi_2, s).$$

For $j = 1, 2$ let

$$f_j(z) = \sum_{\mathfrak{a}} \chi_j(\mathfrak{a})e^{2\pi i N(\mathfrak{a})z} = \sum_{n-1}^{\infty} a_n^{(j)} e^{2\pi i n z}$$

(the first sum being over all non-zero ideals $\mathfrak{a}$ of K). By [**26**, Lemma 3], each $f_j(z)$ is a cusp form of weight 2 for $\Gamma_0(N)$, where $N = D\cdot N(\mathfrak{c}) = D^2$ or $4D^2$, which is a common eigenform of all Hecke operators. The coefficients $a_n^{(j)}$ lie in H^+, and $\sigma(a_n^{(1)}) = a_n^{(2)}$. Thus we can attach an abelian variety A_0 to f_1 and f_2 as in Section 2, which is isogenous over $\mathbb{Q}$ to A by [9, Kor. 2], since their L-series are equal:

$$L(A_0/\mathbb{Q}, s) = L(f_1, s)\,L(f_2, s) = L(\chi_1, s)\,L(\chi_2, s) = L(A/\mathbb{Q}, s).$$

The situation is then exactly as in Theorem 4.

4. *Application to the Weil–Taniyama conjecture over imaginary quadratic fields*

For the notion of a 'cusp form of weight 2' for an imaginary quadratic field k we refer to [**33**, **34**, **20**, **4**, **10**, **11**, **1**]. In [**4**, **5**] an algorithm was presented for computing the dimension of the space $S_2(\mathbf{a})$ of cusp forms of weight 2 for $\Gamma_0(\mathbf{a})$, with $\mathbf{a}$ a non-zero integral ideal of k, in the cases where k is Euclidean: that is, $k = \mathbb{Q}(\sqrt{r})$ with $r = -3$, -4, -7, -8 or -11. This followed on from work of Mennicke and Grunewald in [**15**], where the special case of $\mathbf{a}$ a split prime was studied over the fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-3})$. The first few Fourier coefficients of these forms were computed, for $\mathbf{a}$ with small norm. Also in [**4**, **5**], tables of elliptic curves defined over k with small conductor were compiled (by a computer search procedure), and it was observed that there was a remarkable coincidence between

(1) the set of newforms F of weight 2 for $\Gamma_0(\mathbf{a})$ with rational integer coefficients; and

(2) the set of isogeny classes of elliptic curves E defined over k with conductor $\mathbf{a}$.

In this correspondence, the Mellin transform $L(F, s)$ of the newform F agrees with the L-series $L(E/k, s)$ of the curve E at the first 15 primes of k. Two questions thus arise.

QUESTION 1. If F is a newform of weight 2 for $\Gamma_0(\mathbf{a})$ with rational integer coefficients, for $\mathbf{a}$ a non-zero integral ideal of k, is its Mellin transform $L(F, s)$ the L-series of an elliptic curve defined over k with conductor $\mathbf{a}$?

QUESTION 2. If E is an elliptic curve defined over k with conductor $\mathbf{a}$, is the L-series of E the Mellin transform of a newform for $\Gamma_0(\mathbf{a})$?

As observed in [**8**, **5**, **4**, **34**], the answer to Question 2 as it stands is negative, for if E has complex multiplication by an order in k itself, then E is associated with an Eisenstein series and not a cusp form. (This can only happen when the class number of k is 1.) This leads to a modification.

QUESTION 2′. If E is an elliptic curve defined over k with conductor $\mathbf{a}$ which does not have complex multiplication by an order in k, is the L-series of E the Mellin transform of a newform for $\Gamma_0(\mathbf{a})$?

An affirmative answer to Question 2′ would follow from the conjectural analytic continuation and functional equation satisfied by $L(E, s)$ and its character twists, by the results of [**16**].

We now show that the answer to Question 1 is also negative, as predicted in [**8**], by providing explicit counterexamples from 2-dimensional abelian varieties with extra twists.

THEOREM 5. *Let A be a 2-dimensional abelian variety associated with a newform f in $S_2(N)$ with extra twist by the imaginary quadratic field k, as in Theorem 1. Suppose that* $\mathrm{End}_k^0(A)$ *is a division algebra, so that A remains simple over k. Then the lift F of f from $\mathbb{Q}$ to k is a cusp form of weight 2 over k with rational integer coefficients whose Mellin transform $L(F, s)$ is not the L-series of an elliptic curve defined over k; instead, we have $L(F, s) = L(A/\mathbb{Q}, s)$.*

COROLLARY. *Cusp forms F exist as in Theorem 5 for $k = \mathbb{Q}(\sqrt{r})$ for $r = -2$, -3, -7, -11, -23, -31, and -47.*

Proof. This is immediate from Theorem 4 and the examples of Section 3.

As discussed in the introduction, a suitable modification to Question 1 would be the following.

QUESTION 1′. If F is a newform of weight 2 for $\Gamma_0(\mathbf{a})$ with rational integer coefficients, for a non-zero integral ideal $\mathbf{a}$ of k, is there *either* an elliptic curve E defined over k with $L(F, s) = L(E/k, s)$, *or* a quadratic character ε of $\mathrm{Gal}(\bar{k}/k)$ such that $F \otimes \varepsilon$ is the lift of a form f over $\mathbb{Q}$?

Before proving Theorem 5, we summarize some facts about lifting forms from $\mathbb{Q}$ to an imaginary quadratic field k with discriminant $-D$. In the literature this lifting is described either in terms of automorphic representations (see [**16**, **13**]) or in the more classical language of automorphic forms (see [**10**, **11**, **1**]). We restrict to the special case of the lift of a holomorphic cusp form of weight 2 for $\Gamma_0(N)$ to k (see [**13**, Theorem 2; **10**]).

(1) Every cusp form f of weight 2 for $\Gamma_0(N)$ lifts to a form of weight 2 for $\Gamma_0(\mathbf{a})$, where $\mathbf{a}$ is an ideal of k divisible by the primes of k which divide ND.

(2) A cusp form F of weight 2 for $\Gamma_0(\mathbf{a})$ is the lift of a form f on some $\Gamma_0(N)$ if and only if $c(\alpha) = c(\bar{\alpha})$ for all the Fourier coefficients $c(\alpha)$ $(\alpha \in \mathcal{O}_k)$ of F.

(3) The lift of a cusp form f is again a cusp form except when f has complex multiplication by k (that is, when $f \otimes \chi = f$ for the quadratic character χ attached to $k/\mathbb{Q}$).

(4) If F is the lift of the newform f, then f is also the lift of $f \otimes \chi$ (and of no other newform over $\mathbb{Q}$).

The lift can be described simply in terms of Fourier coefficients, at least when k has class number 1 (see [**10**]). Let $f(z) = \sum_{n=1}^{\infty} a_n \exp(2\pi i n z)$ be a cusp form of weight 2 for $\Gamma_0(N)$ which is a newform and hence an eigenform for all Hecke operators T_p for p not dividing N, so that $a_1 = 1$ and $f | T_p = a_p f$ for p not dividing N. Then the lift F has Fourier coefficients determined by the $c(\pi)$ for prime π, which are given by the formulae:

$$c(\pi) = \begin{cases} c(\bar{\pi}) = a_p & \text{if } \chi(p) = +1 \quad \text{and so } (p) = (\pi)(\bar{\pi}) \text{ splits in } \mathcal{O}_k; \\ a_p^2 - 2p & \text{if } \chi(p) = -1 \quad \text{and so } (p) = (\pi) \text{ remains prime in } \mathcal{O}_k: \\ a_p & \text{if } \chi(p) = 0 \quad \text{and so } (p) = (\pi)^2 \text{ ramifies in } \mathcal{O}_k. \end{cases}$$

In terms of L-series we have

$$L(F,s)=\sum_{(\alpha)} c(\alpha)\,N(\alpha)^{-s}=L(f,s)\,L(f\otimes\chi,s),$$

where $L(f,s)=\sum a_n n^{-s}$ and $L(f\otimes\chi,s)=\sum\chi(n)\,a_n n^{-s}$. The Mellin transform of F is $Z(F,s)$, given by

$$Z(F,s)=D^{s-1}(2\pi)^{-2s}\Gamma(s)^2 L(F,s)$$

for $\mathrm{Re}(s)>3/2$, which is an entire function of s with functional equation

$$Z(F,s)=\pm N(\mathbf{a})^{1-s}Z(F,2-s).$$

Question 2′ then asks, for E an elliptic curve over k with conductor $\mathbf{a}$ and no complex multiplication in k, whether $L(E,s)=L(F,s)$ for a newform F in $S_2(\mathbf{a})$. Question 1 asks whether, given such an F, there is a curve E over k with $L(E,s)=L(F,s)$.

If $f(z)$ is a newform in $S_2(N)$ has integer coefficients then the formulae given above show that the lift f also has integer coefficients. Associated to f in this case is the modular elliptic curve E_f, defined over $\mathbb{Q}$, whose period lattice is the lattice of periods of the differential $2\pi if(z)dz$, and $L(E_f,s)=L(f,s)$ (see [**12**, Section 4]). If E_f^χ denotes the twist of E_f by χ then we have $E_f^\chi=E_{f\otimes\chi}$; the curves E_f and E_f^χ are isomorphic over k, and

$$L(E_f/k,s)=L(E_f,s)\,L(E_f^\chi,s)=L(F,s).$$

Thus $L(F,s)$ is the L-series of E_f, viewed as a curve over k.

More generally, the coefficients $c(\alpha)$ of F will be rational integers provided only that $a_p\in\mathbb{Z}$ whenever $\chi(p)=+1$ and $a_p^2\in\mathbb{Z}$ whenever $\chi(p)=-1$. This will also occur whenever the coefficients of $f(z)$ lie in a (necessarily real) quadratic field $\mathbb{Q}(\sqrt{d})$, and f is the χ-twist of its conjugate. This is precisely the situation of Section 2 above.

Proof of Theorem 5. Let $f_1=f$ and $f_2=f^\sigma=f\otimes\chi$, where σ and χ are as above. Let F be the lift from $\mathbb{Q}$ to k of f; then F has rational integer Fourier coefficients $c(\alpha)$. For it suffices to prove that $c(\pi)\in\mathbb{Z}$ for prime $\pi\in\mathcal{O}_k$: let p be the rational prime below π, and a_p the pth Fourier coefficient of f. By the extra twist hypothesis, we have $a_p^\sigma=\chi(p)a_p$. If $\chi(p)=0$ or $+1$ then $a_p^\sigma=a_p$, so $c(\pi)=a_p\in\mathbb{Z}$; on the other hand, if $\chi(p)=-1$ then $a_p^\sigma=-a_p$, so $a_p^2\in\mathbb{Z}$, and hence $c(\pi)=a_p^2-2p\in\mathbb{Z}$ as required.

The L-series of the two-dimensional abelian variety A determined by f is

$$L(A/\mathbb{Q},s)=L(f_1,s)\,L(f_2,s)=L(f,s)\,L(f\otimes\chi,s)=L(F,s).$$

Hence $L(F,s)$ is the L-series of a 2-dimensional abelian variety defined over $\mathbb{Q}$. We also have $L(A/k,s)=L(F,s)^2$.

If A splits over k, say $A=E_1\times E_2$ (up to isogeny) with E_1 and E_2 defined over k, then we have

$$L(A/k,s)=L(E_1/k,s)\,L(E_2/k,s)=L(E_1/k,s)^2$$

since E_1 and E_2 are isogenous by Proposition 1. Hence $L(E_1/k,s)=L(F,s)=L(E_2/k,s)$ and $L(F,s)$ is indeed the L-series of an elliptic curve defined over k.

But if A remains simple over k then there is no elliptic curve E defined over k with $L(E/k,s)=L(F,s)$. For then we would have

$$L(A/k,s)=L(F,s)^2=L(E/k,s)^2=L(E\times E/k,s),$$

and so A would be isogenous to $E\times E$ over k by the isogeny theorem [**9**, Kor. 2].

REMARKS. 1. In searching for more non-split examples with no complex multiplication, one must restrict to values of N not exactly divisible by any prime, by Theorem 3. This condition is not sufficient, as the cases $N = 81$, 196 and 243 show. At present there is no way of systematically producing such examples. To quote Ribet [23]: 'It would be of interest to give an *a priori* construction of forms with extra twisting. If the level N is divisible by a high power of a prime, these forms seem to be more the rule than the exception'.

2. In the examples constructed at the end of Section 3, with complex multiplication by a field k of class number 2, notice that $L(F,s) = L(E/H^+,s)$ so that the Mellin transform of F *is* the L-series of an elliptic curve: one defined not over k, but over the *real* quadratic field H^+.

3. If k is real quadratic, or any number field with a real embedding, then the phenomenon of Theorem 5 cannot occur, by Theorem 2.

References

1. T. ASAI, 'On the Doi–Naganuma lifting associated with imaginary quadratic fields', *Nagoya Math. J.* 71 (1978) 149–167.
2. A. BAKER, 'Imaginary quadratic fields with class number 2', *Ann. of Math.* 94 (1971) 139–152.
3. B. J. BIRCH and W. KUYK (eds.), *Modular functions of one variable* IV, Lecture Notes in Mathematics 476 (Springer, Berlin, 1975).
4. J. E. CREMONA, 'Modular symbols', D.Phil. Thesis, Oxford 1981.
5. J. E. CREMONA, 'Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields', *Compositio Math.* 51 (1984) 275–323.
6. J. E. CREMONA, 'Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields' (Addendum and Errata), *Compositio Math.* 63 (1987) 271–272.
7. J. E. CREMONA, *Algorithms for modular elliptic curves* (University Press, Cambridge, 1992).
8. J. ELSTRODT, F. GRUNEWALD and J. MENNICKE, 'On the group $\mathrm{PSL}_2(\mathbb{Z}[i])$', *Journées arithmétiques* 1980, London Mathematical Society Lecture Notes 56 (University Press, Cambridge, 1981).
9. G. FALTINGS, 'Endlichkeitsätze für abelsche Varietäten über Zahlkörpen', *Invent. Math.* 73 (1983) 349–366.
10. S. FRIEDBERG, 'On Maass wave forms and the imaginary quadratic Doi–Naganuma lifting', *Math. Ann.* 263 (1983) 483–508.
11. S. FRIEDBERG, 'On the imaginary quadratic Doi–Naganuma lifting of modular forms of arbitrary level', *Nagoya Math. J.* 92 (1983).
12. S. GELBART, 'Elliptic curves and automorphic representations', *Adv. in Math.* 21 (1976) 235–292.
13. P. GÉRARDIN and J. P. LABESSE, 'Base change problem for GL(2)', *Automorphic forms, representations and L-functions*, Proceedings of Symposia in Pure Mathematics 33:2 (American Mathematical Society, Providence, 1979) 115–133.
14. B. H. GROSS, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics 776 (Springer, Berlin, 1980).
15. F. GRUNEWALD, H. HELLING and J. MENNICKE, 'SL_2 over complex quadratic number fields I', *Algebra i Logica* 17 (1978) 512–580.
16. H. JACQUET, *Automorphic Forms on* GL(2) II, Lecture Notes in Mathematics 278 (Springer, Berlin, 1972).
17. M. KOIKE, 'On certain abelian varieties obtained from newforms of weight 2 on $\Gamma_0(3^4)$ and $\Gamma_0(3^5)$', *Nagoya Math. J.* 62 (1976) 29–39.
18. T. Y. LAM, *The algebraic theory of quadratic forms* (Benjamin, New York, 1973).
19. S. LANG, *Elliptic functions* (Addison–Wesley, Reading, Mass., 1973).
20. T. MIYAKE, 'On automorphic forms for GL(2) and Hecke operators', *Ann. of Math.* 94 (1971) 174–189.
21. F. MOMOSE, 'On the l-adic representations attached to modular forms', *J. Fac. Sci. Univ. Tokyo* 28 (1981) 89–109.
22. K. A. RIBET, 'Twists of modular forms and endomorphisms of abelian varieties', *Math. Ann.* 253 (1980) 43–62.
23. K. A. RIBET, 'Endomorphism algebras of abelian varieties attached to newforms of weight 2', *Séminaire de théorie des nombres* 1979–80 (Birkhäuser, Boston, Mass., 1980).
24. K. A. RIBET, 'Galois representations attached to eigenfunctions with nebentypus', *Modular functions of one variable* V, Lecture Notes in Mathematics 601 (Springer, Berlin, 1976).

25. D. Rohrlich, 'On the L-functions of canonical Hecke characters of imaginary quadratic fields', *Duke Math. J.* 47 (1980) 547–557.

26. G. Shimura, 'On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields', *Nagoya Math. J.* 43 (1971) 199–208.

27. G. Shimura, 'On the factors of the Jacobian variety of a modular function field', *J. Math. Soc. Japan* 25 (1973) 523–544.

28. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan 11 (Tokyo–Princeton, 1971).

29. H. M. Stark, 'A complete determination of the complex quadratic fields with class number one', *Michigan Math. J.* 14 (1967) 1–27.

30. R. J. Stroeker, 'Elliptic curves defined over imaginary quadratic fields', Doctoral Thesis, Amsterdam 1975.

31. J. Tate, 'Algorithm for determining the singular fiber in an elliptic pencil', *Modular functions of one variable* IV, Lecture Notes in Mathematics 476 (Springer, Berlin, 1975).

32. D. J. Tingley, 'Elliptic curves uniformized by modular functions', D.Phil. Thesis, Oxford 1975.

33. A. Weil, 'Zeta functions and Mellin transforms', *Colloquium on algebraic geometry* (Bombay, 1968).

34. A. Weil, *Dirichlet series and automorphic forms*, Lecture Notes in Mathematics 189 (Springer, Berlin, 1971).

Department of Mathematics
University of Exeter
North Park Road
Exeter EX4 4QE