J. Math. Soc. Japan
Vol. 58, No. 4 (2006) pp. 927–948

Non-elliptic Shimura curves of genus one

Dedicated to Pilar Bayer on her 60th birthday

By Josep González and Victor Rotger

(Received Jul. 22, 2005)

Abstract. We present explicit models for non-elliptic genus one Shimura curves $X_0(D,N)$ with $\Gamma_0(N)$-level structure arising from an indefinite quaternion algebra of reduced discriminant D, and Atkin-Lehner quotients of them. In addition, we discuss and extend Jordan's work [**10**, Ch. III] on points with complex multiplication on Shimura curves.

1. Introduction.

Let D be the reduced discriminant of an indefinite quaternion algebra B over $\boldsymbol{Q}$ and let $N \geq 1$ be a positive integer coprime to D. Let $X_0(D,N)/\boldsymbol{Q}$ be the Shimura curve over $\boldsymbol{Q}$ of discriminant D and level N attached to an Eichler order of level N in B. When $D = 1$ these are the classical modular curves $X_0(N)$ which have been extensively studied. Throughout this article, let us assume $D \neq 1$.

It follows from the genus formula for $X_0(D,N)$ that only for (D,N) with values in the table below, the genus of $X_0(D,N)$ is 1.

(D,N)	(14, 1)	(15, 1)	(21, 1)	(33, 1)	(34, 1)
(46, 1)	(6, 5)	(6, 7)	(6, 13)	(10, 3)	(10, 7)

Shimura curves $X_0(D,N)$ of genus 1.

By a result of Shimura, $X_0(D,N)(\boldsymbol{R}) = \varnothing$ and hence these curves are not elliptic curves over $\boldsymbol{Q}$.

For trivial level structure $N = 1$, equations for all these curves have already been given (cf. [**7**], [**10**], [**11**], [**12**]) except for $D = 34$. In some of these cases (especially for $D > 10$), the method employed to construct an equation for these curves led to large ad hoc computations and messy diophantine equations (cf. for instance [**10**], pp. 57–68 for the curve $X_0(33,1)$). These computations turn out to be even less feasible to handle when one attempts to apply the same ideas to the discriminant $D = 34$.

In Section 2 we present a simple procedure to provide equations for curves of genus one provided certain initial data is at our disposal. In Section 3 we apply these methods to write down explicit equations for all the above mentioned curves $X_0(D,N)$ of genus 1. Since the genus of $X_0(D,N)$ is never 0 nor 2 when $N > 1$, the present work together with [**9**], [**10**] and [**12**] completes the full list of curves $X_0(D,N)$ of genus $g \leq 2$. In

2000 *Mathematics Subject Classification.* Primary 11G18; Secondary 14G35.

Key Words and Phrases. Shimura curve, curve of genus one, elliptic curve, complex multiplication points.

Both authors are supported in part by DGICYT Grant BFM2003-06768-C02-02.

particular, we prove that Kurihara's conjectured equation [**13**] for $X_0(34,1)$ is correct.

Moreover, in Section 4 we show how our procedure allows us also to compute equations for the seventeen Atkin-Lehner quotients of $X_0(D,1)$ of genus 1 which are non-elliptic over $\boldsymbol{Q}$. Our methods also apply to Atkin-Lehner quotients of Shimura curves $X_0(D,N)$ with nontrivial level structure N, but we do not include these computations here for the sake of brevity.

As in [**9**], [**10**], [**12**] we make a crucial use of the diophantine properties of Shimura curves: their points of complex multiplication and the class fields generated by them, the group of Atkin-Lehner involutions acting on $X_0(D,N)$ and their fixed points, and Cerednik-Drinfeld's description of the special fibres of $X_0(D,N)$ at primes $p \mid D$ of bad reduction.

However, our approach differs from the previous works in that we take advantage of an explicit description which goes back to Cassels of the $\boldsymbol{Q}$-soluble $\boldsymbol{Q}$-equivalence classes of an elliptic curve over $\boldsymbol{Q}$, and has been made explicit by Cremona and Stoll [**6**], [**25**].

In [**10**, Ch. III] Jordan proves fundamental statements on complex multiplication points on Shimura curves with trivial level structure attached to maximal orders of imaginary quadratic fields. Since in this note we work in the more general setting of $\Gamma_0(N)$-*level structure* and points with complex multiplication by *non maximal* imaginary quadratic orders (which arise in a natural way for instance as fixed points of some Atkin-Lehner involutions), we extend these statements to this more general context in the *appendix* to this note.

Most of Jordan's arguments in [**10**, Ch. III] extend in a straightforward way, except for the local behavior at primes dividing both the level N and the conductor f of the quadratic order. Indeed, primes $p \mid (N,f)$ deserve a closer analysis, as the approach given in [**10**, Ch. III] does not apply immediately to these (cf. specially Lemma 5.10). Due to this and the fact that Jordan's Ph. D. Thesis [**10**] is unpublished and not easily available, we present these results in the appendix to this article, including proofs of all them in full generality.

In the last years there have been interesting explicit and computational approaches to Shimura curves. As recent contributions let us mention the works of Baba-Granath [**1**], Bayer [**2**] and Elkies [**7**], [**8**]. Some of our results may be regarded as progress towards the open problems posed in [**7**].

It is a pleasure to thank Anatoli Segura for a careful reading of previous drafts of this article and valuable comments on it.

2. Explicit models for genus one double coverings of $\boldsymbol{P^1}$.

Let C be a (projective, nonsingular) curve of genus one over a field K of characteristic different from 2. Let us denote by $\mathscr{I}(C)$ the set of involutions acting on C over a separable closure $\overline{K}$ of K, i.e.,

$$\mathscr{I}(C) := \left\{ v \in \mathrm{Aut}_{\overline{K}}(C) : v^2 = \mathrm{id} \right\}.$$

For $i = 0, 1$, set

$$\mathscr{I}_i(C) := \{ v \in \mathscr{I}(C) : C/\langle v \rangle \text{ has genus } i \}.$$

We recall that $\mathscr{I}_1(C)$ is a group isomorphic to $(\boldsymbol{Z}/2\boldsymbol{Z})^2$, whose elements commute with all involutions of C. For a given $v \in \mathscr{I}(C)$, set $\mathscr{F}_v = \{P \in C(\overline{K}) : v(P) = P\}$ and let K_v denote the field extension of K obtained by adjoining the coordinates of all $P \in \mathscr{F}_v$. For $v \in \mathscr{I}(C)$, $v \neq \mathrm{id}$, it is well known that $\mathscr{F}_v \neq \varnothing$ if and only if $v \in \mathscr{I}_0(C)$ and in this case $|\mathscr{F}_v| = 4$. Moreover, for any two different involutions $u, v \in \mathscr{I}_0$ we have $\mathscr{F}_v \cap \mathscr{F}_u = \varnothing$, and u, v commute if and only if $u \cdot v \in \mathscr{I}_1(C)$.

The following result is well known.

LEMMA 2.1. *The following conditions are equivalent*:

(i) *There exists an involution* $w \in \mathrm{Aut}_K(C)$ *such that* $C/\langle w\rangle \overset{K}{\simeq} \boldsymbol{P}^1_K$.
(ii) *There exists* $P \in C(\overline{K})$ *such that* $[K(P) : K] \leq 2$.
(iii) *There exist* $x, y \in K(C)$ *and a polynomial* $f[X] \in K[X]$ *of degree* 3 *or* 4 *such that* $y^2 = f(x)$ *and* $K(C) = K(x, y)$.

Assuming (ii), we quickly describe these equivalences. For a point P as in (ii) take $\sigma \in \mathrm{Gal}(\overline{K}/K)$ such that the divisor $D = (P) + ({}^\sigma P)$ is defined over K. By Riemann-Roch's Theorem, there exists a nonconstant function $x \in K(C)$ such that $\operatorname{div} x \geq -D$. Since the field extension $K(C)/K(x)$ has degree 2, the nontrivial involution of $K(C)$ over $K(x)$ acts on $H^0(C, \Omega^1)$ as multiplication by -1. The functions x and $y = dx/\omega$, where ω is a nonzero regular differential of C defined over K, satisfy the conditions stated in (iii) and w acts on $K(C)$ by sending (x, y) to $(x, -y)$ and P to ${}^\sigma P$. The polynomial $f(X)$ has degree 3 or 4 depending on whether $P \in C(K)$ or not. Finally, for an involution w as in (i), any $P \in C(\overline{K})$ which projects to a point in $C/\langle w\rangle(\boldsymbol{Q})$ satisfies (ii).

Attached to an equation as in (iii) of the above lemma, there are two invariants I and J defined by:

$$I = 12a_4a_0 - 3a_3a_1 + a_2^2 \quad \text{and} \quad J = 72a_4a_2a_0 + 9a_3a_2a_1 - 27a_4a_1^2 - 27a_3^2a_0 - 2a_2^3,$$

where $f(x) = \sum_{i=0}^4 a_i x^i$ (cf. [**6**]). With this notation, the elliptic curve E/K given by the equation

$$v^2 = u^3 - 27Iu - 27J$$

is isomorphic over K to the Jacobian $\mathrm{Jac}(C)$ of C.

From now on, we also assume that $\mathrm{char}(K) \neq 2, 3$. For a curve C/K of genus one satisfying the conditions of Lemma 2.1, let $\pi : C \to C/\langle w\rangle \simeq \boldsymbol{P}^1_K$ denote the natural projection. The aim of this section is to present two methods in order to find an equation describing C/K.

2.1. First method.

In this subsection we describe an approach in order to find an equation for C/K, provided one knows (or can compute) the following *initial data*:

(i_1) An element $d \in K^* \setminus K^{*2}$ such that $\pi(C(K(\sqrt{d}))) \cap C/\langle w\rangle(K) \neq \varnothing$.
(i_2) An equation $y^2 = x^3 + Ax + B$, $A, B \in K$ for the elliptic curve $E := \mathrm{Jac}\, C/K$,
(i_3) The field K_w.

For any two polynomials $f_1(x)$, $f_2(x) \in K[x]$ of degree 3 or 4 without double roots, we say that the equations $eq_1 : y^2 = f_1(x)$ and $eq_2 : y^2 = f_2(x)$ are equivalent over K if there exist

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL(2,K) \quad \text{and} \quad \lambda \in K^*$$

such that

$$f_2(x) = \lambda^2 f_1\left(\frac{\alpha x + \beta}{\gamma x + \delta}\right)(\gamma x + \delta)^4.$$

Let C_i be the curve given by the equation eq_i, $i \leq 2$. If eq_1 and eq_2 are equivalent over K, then $C_1 \overset{K}{\simeq} C_2$ and the splitting fields of f_1 and f_2 are equal. However, the converse is not true.

It is known that for a given elliptic curve E over K, there is a one-to-one correspondence between the set $E(K)/2E(K)$ and the set of K-equivalence classes of equations $y^2 = f(x)$, $\deg(f) = 3$ or 4, such that the corresponding curves given by these ones are isomorphic to E over K (cf. [**6**]).

Let C/K be a non-elliptic curve of genus one satisfying the conditions of Lemma 2.1. Assume further that we know the initial data $(i_1), (i_2), (i_3)$.

Since C admits an equation of the form $y^2 = df(x)$, where $f \in K[x]$ is monic of degree 4 and the action of w is given by $(x, y) \mapsto (x, -y)$, we propose the following strategy in order to determine f.

Consider the twisted elliptic curve $E_d : y^2 = x^3 + Ad^2x + Bd^3$ of E and determine a set $\mathscr{S} = \{\infty, P_1 = (x_1, y_1), \ldots, P_r = (x_r, y_r)\} \subseteq E_d(K)$ of representative elements of $E_d(K)/2E_d(K)$. The equations $y^2 = f_i(x)$, $0 \leq i \leq r$, where

$$f_i(x) = \begin{cases} x^3 + Ad^2x + Bd^3 & \text{if } i = 0, \\ x^4 - 6x_ix^2 + 8y_ix - 3x_i^2 - 4Ad^2 & \text{if } 1 \leq i \leq r, \end{cases}$$

exhaust all K-equivalence classes of equations attached to E_d (cf. [**25**, Proposition 2.2]). Therefore, C must be isomorphic over K to a curve given by one of the equations $y^2 = df_i(x)$ for $1 \leq i \leq r$, since the equation obtained from ∞, $y^2 = df_0(x)$, corresponds to an elliptic curve over K.

Any diophantine information about C at our disposal may serve to pick the correct equation for our curve. This may be for instance the case if the field K_w agrees with exactly one of the splitting fields of the polynomials f_i. As we show in Sections 3 and 4, this approach always succeeds for all Shimura curves and Shimura curve quotients of genus one that we deal with. Of course, in general there is no reason to expect that the initial data $(i_1), (i_2), (i_3)$ suffices to determine C.

2.2. Second method.

Let C/K be a curve of genus one as in Lemma 2.1. In order to describe a second method to provide an explicit model for C under additional assumptions, we need the following result.

PROPOSITION 2.2. *Let C/K be a curve of genus one together with $w, u \in \mathscr{I}_0(C)$ defined over K such that $C/\langle w\rangle \simeq \boldsymbol{P}^1_K$ and that $u \cdot w \in \mathscr{I}_1(C)$.*

Let $L = K(\sqrt{d})$ be a quadratic extension of K and $\sigma \in \mathrm{Gal}(L/K)$, $\sigma \neq 1$, such that there exists a point $P \in C(L)\backslash C(K)$ with $w(P) = {}^\sigma P$. We have that

(1) *If $P \in \mathscr{F}_u$, there exist $x, y \in K(C)$ such that $K(C) = K(x, y)$, $w(x, y) = (x, -y)$, $u(x, y) = (-x, y)$ and*

$$y^2 = d(x^4 + bx^2 + c), \quad b, c \in K.$$

Moreover, $Y^2 = d(X^3 + bX^2 + cX)$ is an equation for $C/\langle u \cdot w\rangle$.

(2) *If $P \notin \mathscr{F}_u$, there exist $x, y \in K(C)$ such that $K(C) = K(x, y)$, $w(x, y) = (x, -y)$, $u(x, y) = (\varepsilon/x, \varepsilon y/x^2)$ for some $\varepsilon \in K^*$ and*

$$y^2 = d(x^4 + bx^3 + cx^2 + b\varepsilon x + \varepsilon^2), \quad b, c \in K.$$

Moreover, $Y^2 = d(X^2 - 4\varepsilon)(X^2 + bX + c - 2\varepsilon)$ is an equation for $C/\langle u \cdot w\rangle$.

PROOF. Let us first assume that $P \in \mathscr{F}_u$. Then $\mathscr{F}_u = \{P, {}^\sigma P, Q, Q'\}$ for some points Q, $Q' \in C(\overline{K})$ such that the divisor $D = (Q) + (Q') - (P) - ({}^\sigma P)$ is a K-rational divisor invariant under w. Thus, there exist $x, y \in K(C)$ such that $K(C) = K(x, y)$,

$$\operatorname{div} x = D \quad \text{and} \quad y^2 = af(x),$$

where $a \in K^*$ and $f(X) \in K[X]$ is a monic polynomial of degree 4 without double roots. Since the value of the function $(y/x^2)^2$ at P and ${}^\sigma P$ is a, it follows that $a = da_0^2$ for a certain $a_0 \in K^*$. Switching y by $a_0 y$, we can assume that $y^2 = df(x)$. Since D is also invariant under u, it follows that u maps x to either x or $-x$. Since $u \in \mathscr{I}_0$ and $u \neq w$, we deduce that u acts on C by mapping (x, y) to $(-x, y)$ and that f is an even polynomial. The function field of $C/\langle u \cdot w\rangle$ is generated by the functions $X = x^2$ and $Y = xy$, which clearly satisfy the equation claimed in our statement.

Assume now that $P \notin \mathscr{F}_u$. As before, the divisor $D = (u(P)) + (u({}^\sigma P)) - (P) - ({}^\sigma P)$ is rational over K and invariant under w. Since $w(P) = {}^\sigma P$ and $u \cdot w$ has not fixed points, it follows that $u(P) \neq {}^\sigma P$. Therefore, there exist $x, y \in K(C)$ such that

$$K(C) = K(x, y), \quad w(x, y) = (x, -y), \quad \operatorname{div} x = D \quad \text{and} \quad y^2 = df(x),$$

where $f(X) \in K[X]$ is a monic polynomial of degree 4. Since $u(D) = -D$, u maps x to ε/x and y to $\varepsilon y/x^2$ for some $\varepsilon \in K^*$. Thus $f(X) = X^4 + bX^3 + cX^2 + \varepsilon bX + \varepsilon^2$ for some $b, c \in K$ and the function field of $C/\langle u \cdot w\rangle$ is generated by the functions $X = x + \varepsilon/x$ and $Y = y(1 - \varepsilon/x^2)$, which again satisfy the equation claimed in our statement. □

REMARK 2.3. Under the assumptions of Proposition 2.2, there exists (in both cases) a point $P \in \mathrm{Jac}(C)[2](K)$ such that $\mathrm{Jac}(C)/\langle P\rangle = \mathrm{Jac}(C/\langle u \cdot w\rangle)$. In particular, it holds that $|\operatorname{Aut}_K(C) \cap \mathscr{I}_1|$ divides $|\mathrm{Jac}(C)[2](K)|$. If K is a number field, this implies that both Jacobians have the same conductor over K.

Remark 2.4. Assume that $C(K)=\varnothing$. In case (1), $C/\langle u\cdot w\rangle$ is an elliptic curve over K. In case (2), if in addition there exists a point $P\in\mathscr{F}_u$ such that $\pi(P)\in \boldsymbol{P}^1_K$, then C admits a model as in (1) for a suitable choice of d; otherwise, $\varepsilon\notin K^2$, $K(\sqrt{\varepsilon})$ is a subfield of $K(\mathscr{F}_u)$ and $C/\langle u\cdot w\rangle$ might not be an elliptic curve over K.

In the particular case that C belongs to case (1) of Proposition 2.2, the following result describes an easier and better procedure to find an equation for C, provided one knows the initial data (i_1), (i_2) as above and

(i_4) An equation $V^2=U^3+A'U+B'$, $A',B'\in K$, for the elliptic curve $C/\langle u\cdot w\rangle$.

Proposition 2.5. *Let C/K be as in* (1) *of Proposition* 2.2. *Assume that $V^2=U^3+A'U+B'$, $A',B'\in K$, is an affine equation over K for the elliptic curve $C'=C/\langle u\cdot w\rangle$. Then,*

$$y^2=dx^4+3u_0x^2+\big(A'+3u_0^2\big)/d$$

is an equation for C, where $u_0\in K$ is the root of the polynomial $U^3+A'U+B'$ such that $C'/\langle(u_0,0)\rangle$ is isomorphic to $\operatorname{Jac}C$ *over K.*

Proof. By Proposition 2.2, $Y^2=d(X^3+bX^2+cX)$ is an equation for C'/K and it is isomorphic over K to the elliptic curve

$$V^2=\left(U-\frac{bd}{3}\right)\left(U^2+\frac{bd}{3}U-d^2\frac{2b^2-9c}{9}\right)=U^3-\frac{d^2(b^2-3c)}{3}U+\frac{bd^3(2b^2-9c)}{27}.$$

Computing the I and J invariants attached to the equation $y^2=d(x^4+bx^2+c)$, it can be checked that the quotient curve $C'/\langle(bd/3,0)\rangle$ is isomorphic over K to the elliptic curve $v^2=u^3-27Iu-27J$, which is isomorphic over K to $\operatorname{Jac}C/K$.

Since the K-equivalence class of the equation $y^2=dx^4+3u_0x^2+(A'+3u_0^2)/d$ does not depend on the chosen equation

$$V^2=U^3+A'U+B'=(U-u_0)\big(U^2+u_0U+(A'+u_0^2)\big)$$

for C'/K, we can assume the following equalities

$$\frac{db}{3}=u_0,\quad -d^2\frac{2b^2-9c}{9}=A'+u_0^2.$$

It follows that $db=3u_0$ and $dc=(A'+3u_0^2)/d$. □

3. Genus one Shimura curves.

Let $D=p_1\cdots p_{2r}$, $r>0$, be the product of an even number of distinct prime numbers and let $N\geq 1$, $(D,N)=1$ be an integer. Let $X_0(D,N)/\boldsymbol{Q}$ be the canonical model over $\boldsymbol{Q}$ of the Shimura curve of discriminant D and level N. Let $W_{D,N}=\{\omega_m : m\mid D\cdot N,(m,D\cdot N/m)=1\}\simeq(\boldsymbol{Z}/2\boldsymbol{Z})^{\sharp\{p\mid D\cdot N\}}$ be the group of

Atkin-Lehner involutions on $X_0(D,N)$. All these involutions are defined over $\boldsymbol{Q}$ and we let $\pi_m : X_0(D,N) \to X_0(D,N)/\langle \omega_m \rangle$ the natural projection (cf. the Appendix for more details). We shall also let $K_m = K_{w_m}$ denote the field extension over K obtained by adjoining the coordinates of the fixed points of w_m.

The aim of this section is to provide equations for these curves when their genera are 1. Note that these are never elliptic curves over $\boldsymbol{Q}$ because they fail to have real points (cf. [**23**]).

LEMMA 3.1. *The Shimura curve $X_0(D,N)$ has genus one exactly for the following values of (D,N): $(14,1)$, $(15,1)$, $(21,1)$, $(33,1)$, $(34,1)$, $(46,1)$, $(6,5)$, $(6,7)$, $(6,13)$, $(10,3)$, $(10,7)$.*

PROOF. It readily follows from a close inspection to the genus formula for $X_0(D,N)$ given in Proposition 5.2. □

In order to apply the methods indicated in the previous section, let us mention what are the key ingredients we use about (genus one) Shimura curves:

- The determination of the isogeny class of the elliptic curve $\mathrm{Jac}(X_0(D,N))$ over $\boldsymbol{Q}$ can be carried out from Ribet's isogeny theorem (cf. Theorem 5.4). In all cases of Lemma 3.1, it turns out that $\mathrm{Jac}(X_0(D,N))$ lies in the single isogeny class of conductor $D \cdot N$.
- When the genera of $X_0(D,N)$ and $X_0(D,N)/\langle \omega_m \rangle$ are 1, their Jacobians are isogenous over $\boldsymbol{Q}$ and their $\boldsymbol{Q}$-isomorphism classes are determined by the computation of the Kodaira symbols of the reduction of both curves at primes $p \mid D$ by using Cerednik-Drinfeld's Theory ([**3**, Section 1.7], [**11**], [**12**]), combined with Table 1 of [**5**]. David Kohel's *Brandt modules* package implemented in Magma [**14**] is very practical to determine Cerednik-Drinfeld's dual graphs of $X_0(D,N)$ at primes $p \mid D$.
- For all curves in Lemma 3.1, there exists an imaginary quadratic field $K = \boldsymbol{Q}(\sqrt{d})$ of class number 1 and a point $P \in X_0(D,N)(K)$ such that $\pi_{D\cdot N}(P) \in X_0(D,N)/\langle \omega_{D\cdot N} \rangle(\boldsymbol{Q})$. The explicit computation of d follows from Corollary 5.14. In particular, it turns out that

$$X_0(D,N)/\langle \omega_{D\cdot N} \rangle \simeq \boldsymbol{P}^1_{\boldsymbol{Q}}$$

  for all these curves, since their genera are always 0.
- For every $m | D \cdot N$, the number field K_m can be determined by using Proposition 5.7, Theorem 5.12 and Remark 5.11. These numbers fields are displayed in the next Lemma.

LEMMA 3.2. *The set of Atkin-Lehner involutions $\omega_m \in \mathscr{I}_0(X_0(D,N))$ for the Shimura curves of Lemma* 3.1 *just as the field of definition of their fixed points are collected in the following tables*:

$(14,1),\{\omega_{14},\omega_2\}$	$(15,1),\{\omega_{15},\omega_3\}$	$(21,1),\{\omega_{21},\omega_3\}$
$K_{14}=\boldsymbol{Q}(\sqrt{-1\pm\sqrt{-7}})$	$K_{15}=\boldsymbol{Q}(\sqrt{-3})$	$K_{21}=\boldsymbol{Q}(\sqrt{-3},\sqrt{-7})$
$K_2=\boldsymbol{Q}(\sqrt{-1},\sqrt{-2})$	$K_3=\boldsymbol{Q}(\sqrt{-3})$	$K_7=\boldsymbol{Q}(\sqrt{-7})$

$(33,1),\{\omega_{33},\omega_3\}$	$(34,1),\{\omega_{34},\omega_{17}\}$	$(46,1),\{\omega_{46},\omega_2\}$
$K_{33}=\boldsymbol{Q}(\sqrt{-3},\sqrt{-11})$	$K_{34}=\boldsymbol{Q}(\sqrt{3\pm2\sqrt{-2}})$	$K_{46}=\boldsymbol{Q}(\sqrt{-3\pm\sqrt{-23}})$
$K_3=\boldsymbol{Q}(\sqrt{-3})$	$K_{17}=\boldsymbol{Q}(\sqrt{-1\pm4\sqrt{-1}})$	$K_2=\boldsymbol{Q}(\sqrt{-1},\sqrt{-2})$

$(6,5),\{\omega_{30},\omega_2,\omega_6,\omega_{10}\}$	$(6,7),\{\omega_{42},\omega_3,\omega_6,\omega_{21}\}$	$(6,13),\{\omega_{78},\omega_2,\omega_3,\omega_{13}\}$
$K_{30}=\boldsymbol{Q}(\sqrt{-3},\sqrt{5})$	$K_{42}=\boldsymbol{Q}(\sqrt{-2},\sqrt{-3})$	$K_{78}=\boldsymbol{Q}(\sqrt{-3},\sqrt{13})$
$K_2=\boldsymbol{Q}(\sqrt{-1})$	$K_3=\boldsymbol{Q}(\sqrt{-3})$	$K_2=\boldsymbol{Q}(\sqrt{-1})$
$K_6=\boldsymbol{Q}(\sqrt{2},\sqrt{-3})$	$K_6=\boldsymbol{Q}(\sqrt{2},\sqrt{-3})$	$K_3=\boldsymbol{Q}(\sqrt{-3})$
$K_{10}=\boldsymbol{Q}(\sqrt{-2},\sqrt{5})$	$K_{21}=\boldsymbol{Q}(\sqrt{3},\sqrt{-3})$	$K_{13}=\boldsymbol{Q}(\sqrt{13},\sqrt{-1})$

$(10,3),\{\omega_{30},\omega_2,\omega_3,\omega_5\}$	$(10,7),\{\omega_{70},\omega_5,\omega_{10},\omega_{35}\}$
$K_{30}=\boldsymbol{Q}(\sqrt{-6},\sqrt{10})$	$K_{70}=\boldsymbol{Q}(\sqrt{-14},\sqrt{10})$
$K_2=\boldsymbol{Q}(\sqrt{-2})$	$K_5=\boldsymbol{Q}(\sqrt{-1},\sqrt{5})$
$K_3=\boldsymbol{Q}(\sqrt{-3})$	$K_{10}=\boldsymbol{Q}(\sqrt{-2},\sqrt{5})$
$K_5=\boldsymbol{Q}(\sqrt{-1},\sqrt{5})$	$K_{35}=\boldsymbol{Q}(\sqrt{5},\sqrt{-7})$

Remark 3.3. When $K_2=\boldsymbol{Q}(\sqrt{-1},\sqrt{-2})$, two fixed points of ω_2 are rational over $\boldsymbol{Q}(\sqrt{-1})$ while the coordinates of the other two lie in $\boldsymbol{Q}(\sqrt{-2})$. In the remaining cases, the Galois closure of the field of definition of every $P\in\mathscr{F}_{\omega_m}$ is equal to K_m. The notation $\boldsymbol{Q}(\sqrt{a\pm\sqrt{b}})$ means that the field of definition of each $P\in\mathscr{F}_{\omega_m}$ is either $\boldsymbol{Q}(\sqrt{a+\sqrt{b}})$ or $\boldsymbol{Q}(\sqrt{a-\sqrt{b}})$.

Theorem 3.4. *Equations for the eleven Shimura curves of genus one and the action of their Atkin-Lehner involutions are collected in the following tables*:

(D,N)	$y^2=\quad f(x)$
$(14,1)$	$y^2=-x^4+13x^2-128$
$(15,1)$	$y^2=-3x^4-82x^2-27$
$(21,1)$	$y^2=-7x^4+94x^2-343$
$(33,1)$	$y^2=-3x^4-10x^2-243$
$(34,1)$	$y^2=-3x^4+26x^3-53x^2-26x-3$
$(46,1)$	$y^2=-x^4+45x^2-512$
$(6,5)$	$y^2=-x^4+61x^2-1024$
$(6,7)$	$y^2=-3x^4-34x^2-2187$
$(6,13)$	$y^2=-x^4-115x^2-4096$
$(10,3)$	$y^2=-2x^4-11x^2-32$
$(10,7)$	$y^2=-27x^4-40x^3+6x^2+40x-27$

Table 1. Equations for Shimura curves of genus one.

The involution $\omega_{D\cdot N}$ maps (x,y) to $(x,-y)$. The action of the remaining Atkin-Lehner involutions in $\mathscr{I}_0(X_0(D,N))$ which together with $\omega_{D\cdot N}$ generate $W_{D,N}$ are:

14	15	21	33	34	46
$\omega_2(x,y)$	$\omega_3(x,y)$	$\omega_7(x,y)$	$\omega_3(x,y)$	$\omega_{17}(x,y)$	$\omega_2(x,y)$
$(-x,y)$	$(-x,y)$	$(-x,y)$	$(-x,y)$	$(-1/x,-y/x^2)$	$(-x,y)$

$(6,5)$	$(6,7)$	$(6,13)$	$(10,3)$	$(10,7)$
$\omega_2(x,y)$	$\omega_3(x,y)$	$\omega_2(x,y)$	$\omega_2(x,y)$	$\omega_{15}(x,y)$
$(-x,y)$	$(-x,y)$	$(-x,y)$	$(-x,y)$	$\left(\frac{-1}{x},\frac{-y}{x^2}\right)$
$\omega_6(x,y)$	$\omega_6(x,y)$	$\omega_3(x,y)$	$\omega_3(x,y)$	$\omega_{10}(x,y)$
$\left(\frac{32}{x},\frac{32y}{x^2}\right)$	$\left(\frac{-27}{x},\frac{-27y}{x^2}\right)$	$\left(\frac{64}{x},\frac{64y}{x^2}\right)$	$\left(\frac{4}{x},\frac{4y}{x^2}\right)$	$\left(\frac{2x-1}{x-2},\frac{5y}{(x-2)^2}\right)$

PROOF. For $X_0(D,N)$ as in Lemma 3.1, set $w=\omega_{D\cdot N}$ and let $d<0$ be an integer such that there exists $P\in X_0(D,N)(\boldsymbol{Q}(\sqrt{d}))$, $\pi_{DN}(P)\in X_0(D,N)/\langle w\rangle(\boldsymbol{Q})$.

Assume first that $N=1$. Then, there exists a single Atkin-Lehner involution $u\neq w$, $u\in\mathscr{I}_0(X_0(D,1))$. Next table collects Cremona's labels for the elliptic curves $\mathrm{Jac}(X_0(D,1))$ and $\mathrm{Jac}(X_0(D,1)/\langle u\cdot w\rangle)$ together with some possible values for d:

D	d	$\mathrm{Jac}(X_0(D,1))$	$\mathrm{Jac}(X_0(D,1)/\langle u\cdot w\rangle)$
14	$-1,-2$	$A2$	$A1$
15	-3	$A1$	$A2$
21	-7	$A2$	$A6$
33	-3	$A1$	$A4$
34	-3	$A3$	$A4$
46	$-1,-2$	$A2$	$A1$

Comparing the above table with the fields K_m of Lemma 3.2, we obtain that $X_0(D,1)$ for $D=14$, 15, 21, 33 and 46 correspond to case (1) of Proposition 2.2. Corresponding equations as collected in Table 1 are automatically obtained by applying Proposition 2.5.[1]

Let us now consider separately the exceptional case $C=X_0(34,1)$, to which we apply the first method outlined in Section 2.1. As it follows from the table above, C can be described by an affine equation of the form

$$y^2=-3f(x),$$

for some monic polynomial $f(x)\in\boldsymbol{Q}[x]$ of degree 4. Moreover, its Jacobian is the elliptic curve $34A_3$ given by the equation

$$E: y^2=x^3-\frac{4945}{3}x-\frac{695374}{27}.$$

[1]Note that equations for these five curves were already obtained in [**10**], [**11**] and [**12**]. Some of the models proposed there are different but correspond to equations which are equivalent over $\boldsymbol{Q}$ to ours.

Consider the twisted curve of C:

$$C_{-3} : y^2 = f(x),$$

which is isomorphic over $\boldsymbol{Q}$ to the elliptic curve $306B3$:

$$E_{-3} : y^2 = x^3 - 14835x + 695374.$$

By means of [**14**] we obtain that $E_{-3}(\boldsymbol{Q}) = \langle P_1, P_2 \rangle \simeq \boldsymbol{Z}/6\boldsymbol{Z} \times \boldsymbol{Z}$, where $P_1 = (143, 1224)$, $P_2 = (63, 104)$ and $\mathrm{ord}(P_1) = 6$. Thus, since $|E_{-3}(\boldsymbol{Q})/2E_{-3}(\boldsymbol{Q})| = 4$, the $\boldsymbol{Q}$-equivalence class of $y^2 = f(x)$ must agree with one of the following three $\boldsymbol{Q}$-equivalence classes attached to E_{-3}:

case	$P \in E_{-3}(\boldsymbol{Q})/2E_{-3}(\boldsymbol{Q})$	$y^2 =$ $f(x)$
(i)	$3P_1 = (71, 0)$	$y^2 = x^4 - 426x^2 + 44217$
(ii)	$P_2 = (63, 104)$	$y^2 = x^4 - 378x^2 + 832x + 47433$
(iii)	$3P_1 + P_2 = (35, -468)$	$y^2 = x^4 - 210x^2 - 3744x + 5565$

Since (ii) is the single case such that the splitting field of the polynomial $f(x)$ is K_w, we conclude that for $f(x)$ as in (ii), $y^2 = -3f(x)$ is an equation for $X_0(34, 1)$. The map $(x, y) \mapsto (6x - 13, 12y)$ transforms it into the model proposed in Table 1.

Let us consider now the cases for which $N > 1$. In all of them, the conductor of $\mathrm{Jac}(X_0(D, N))$ is $D \cdot N$ and, moreover, $\mathrm{Jac}(X_0(D, N))[2](\boldsymbol{Q}) \simeq (\boldsymbol{Z}/2\boldsymbol{Z})^2$ since $(\boldsymbol{Z}/2\boldsymbol{Z})^3$ is a subgroup of $\mathrm{Aut}_{\boldsymbol{Q}}(X_0(D, N))$.

For $(D, N) = (6, 5)$, $(6, 7)$, $(6, 13)$ and $(10, 3)$ there exists an Atkin-Lehner involution ω_m such that $K_m = \boldsymbol{Q}(\sqrt{d})$ and $m \neq D \cdot N$. More precisely, these are

(D, N)	m	d	$\mathrm{Jac}(X_0(D, N))$	$\mathrm{Jac}(X_0(D, N)/\langle \omega_{D \cdot N/m} \rangle)$
$(6, 5)$	2	-1	$30A6$	$30A3$
$(6, 7)$	3	-3	$42A3$	$42A6$
$(6, 13)$	2	-1	$78A2$	$78A1$
$(10, 3)$	2	-2	$30A2$	$30A1$

Equations as claimed in Table 1 are immediately obtained by applying again Proposition 2.5.

As for $(D, N) = (10, 7)$ we proceed similarly as we did for $(34, 1)$. We have that $E := \mathrm{Jac}(X_0(10, 7))$ is the elliptic curve $70A_2$, because this is the single isomorphism class of conductor 70 with all its 2-torsion points rational over $\boldsymbol{Q}$ and we take the following equation $y^2 = x^3 - 283x - 1482$ for E. In this case, we can take $d = -3$ and we have $E_{-3} : y^2 = x^3 - 2547x + 40014$, which is the elliptic curve $630E2$. In addition, $E_{-3}(\boldsymbol{Q}) = \langle P_1, P_2, P_3 \rangle \simeq (\boldsymbol{Z}/2\boldsymbol{Z})^2 \times \boldsymbol{Z}$, where $P_1 = (18, 0)$, $P_2 = (39, 0)$ and $P_3 = (-17, 280)$. Hence we must check the following seven $\boldsymbol{Q}$-equivalence classes of equations attached to E_{-3}:

case	$P \in E_{-3}(\boldsymbol{Q})/2E_{-3}(\boldsymbol{Q})$	$y^2 = \quad f(x)$
(i)	$P_1 = (18, 0)$	$y^2 = x^4 - 108x^2 + 9216$
(ii)	$P_2 = (39, 0)$	$y^2 = x^4 - 234x^2 + 5625$
(iii)	$P_1 + P_2 = (-57, 0)$	$y^2 = x^4 + 342x^2 + 441$
(iv)	$P_3 = (-17, 280)$	$y^2 = x^4 + 102x^2 + 2240x + 9321$
(v)	$P_1 + P_3 = (63, 360)$	$y^2 = x^4 - 378x^2 + 2880x - 1719$
(vi)	$P_2 + P_3 = (3, -180)$	$y^2 = x^4 - 18x^2 - 1440x + 10161$
(vii)	$P_1 + P_2 + P_3 = (123, -1260)$	$y^2 = x^4 - 738x^2 - 10080x - 35199$

Only for case (iv) the splitting field of $f(x)$ agrees with K_{70} given in Lemma 3.1. Thus, $y^2 = -3(x^4 + 102x^2 + 2240x + 9321)$ is an equation for $X_0(10, 7)$. The transformation $(x, y) \mapsto ((11x + 1)/(-x + 1), 36y/(-x + 1)^2)$ yields the model collected in Table 1.

Finally, for each of the equations in Table 1, we can compute all their involutions over $\boldsymbol{Q}$ which commute with $\omega_{D.N}$. The explicit expression of the Atkin-Lehner involutions acting on each of these models is determined by comparing these computations with the fields K_m as in Lemma 3.2. □

REMARK 3.5. Kurihara conjectured in [**13**] the following equation for $X_0(34, 1)$:

$$\begin{cases} z^2 + 44u^2 - 68u + 27 = 0, \\ w^2 - (u^2 + 1) = 0. \end{cases}$$

It is checked that the map

$$(u, w, z) = \left(-\frac{2x}{x^2 - 1}, -\frac{1 + x^2}{x^2 - 1}, \frac{9y}{x^2 - 1} \right)$$

transforms it into

$$-3y^2 = x^4 + 136/27x^3 + 122/27x^2 - 136/27x + 1.$$

In turn, the transformation $(x, y) \mapsto \left(\frac{-5x+3}{3x+5}, \frac{68y}{9(3x+5)^2}\right)$ shows that Kurihara's conjectured curve coincides with ours collected in Table 1. See [**4**] for an application of the explicit knowledge of an equation for $X_0(34, 1)$.

4. Genus one Atkin-Lehner quotients of Shimura curves.

Let $D = p_1 \cdots p_{2r}$, $r > 0$, be the product of an even number of distinct prime numbers and let $X_D = X_0(D, 1)$. For a positive divisor $m \mid D$, $m > 1$, let us denote by $X_D^{(m)}$ the Atkin-Lehner quotient $X_D/\langle \omega_m \rangle$. Note that despite $X_D(\boldsymbol{R}) = \varnothing$, it might (and does in several cases) happen that $X_D^{(m)}(\boldsymbol{Q}) \neq \varnothing$.

The complete list of values of (D, m) for which $X_D^{(m)}$ has genus one, together with Weierstrass models for those $X_D^{(m)}$ which are elliptic curves over $\boldsymbol{Q}$, can be found in

[**18**][2]. In this section we provide explicit equations for the remaining genus one curves, that is, those that fail to have rational points over $\boldsymbol{Q}$.

LEMMA 4.1 ([**18**]). *The curve $X_D^{(m)}$ is a non-elliptic curve of genus one over $\boldsymbol{Q}$ exactly for the following values of (D,m): $(39,13)$, $(55,5)$, $(62,2)$, $(69,3)$, $(77,11)$, $(85,17)$, $(94,2)$, $(178,89)$, $(210,30)$, $(210,42)$, $(210,70)$, $(210,105)$, $(330,3)$, $(330,22)$, $(330,33)$, $(330,165)$, $(462,154)$.*

Let us mention which are the main tools we use in order to apply the methods exposed in Section 2:

- Similarly as in Section 3, the isogeny class of the Jacobian of $X_D^{(m)}$ can be determined by combining Theorem 5.4 with Table 3 of [**5**]. The isomorphism class is obtained by comparing Table 1 of [**5**] with the Kodaira symbols of the special fibres at primes $p \mid D$, which can be computed by means of Cerednik-Drinfeld's Theory.
- For any $m' \mid D$, the Atkin-Lehner involution $\omega_{m'}$ on X_D induces an involution on $X_D^{(m)}$ that we shall denote $\tilde{\omega}_{m'}$. Then $\mathscr{F}_{\tilde{\omega}_{m'}} = \pi_m(\mathscr{F}_{\omega_{m'}}) \cup \pi_m(\mathscr{F}_{\omega_m \cdot \omega_{m'}})$. In all cases of Lemma 4.1 it turns out that $\mathscr{F}_{\tilde{\omega}_D} = \pi_m(\mathscr{F}_{\omega_D})$. The number field generated by the coordinates of the fixed points of $\tilde{\omega}_{m'}$ on $X_D^{(m)}$ can be computed by means of Proposition 5.7, Corollary 5.14 and Remark 5.11.
- For all curves $X_D^{(m)}$ in Lemma 4.1, $X_D^{(m)}/\langle\tilde{\omega}_D\rangle = X_D/\langle\omega_m,\omega_D\rangle \simeq \boldsymbol{P}^1_{\boldsymbol{Q}}$. This can be deduced from the following two general results: Firstly, the set of fixed points of ω_D is nonempty (cf. Proposition 5.6 and 5.7) and thus $X_D^{(m)}/\langle\tilde{\omega}_D\rangle$ has genus 0. Secondly, $X_D/\langle\omega_D\rangle$ has points everywhere locally by [**21**, Theorem 3.1]. By the Hasse principle this implies that $X_D^{(m)}/\langle\tilde{\omega}_D\rangle \simeq \boldsymbol{P}^1_{\boldsymbol{Q}}$.
- There always exists an imaginary quadratic field $K = \boldsymbol{Q}(\sqrt{d})$ such that $h(K) = 1$ and $\pi(X_D(K)) \cap (X_D^{(m)}/\langle\tilde{\omega}_D\rangle(\boldsymbol{Q})) \neq \varnothing$, where now we let $\pi : X_D \to X_D^{(m)}/\langle\tilde{\omega}_D\rangle$ denote the natural projection of degree 4. The computation of d follows from Corollary 5.14.

THEOREM 4.2. *Equations for the Atkin-Lehner quotients $X_D^{(m)}$ listed in Lemma 4.1 together with Cremona's label for their Jacobians are collected in Table 2 where $\tilde{\omega}_D$ acts as $(x,y) \mapsto (x,-y)$.*

PROOF. The equations in Table 2 are obtained by applying the first procedure described in Section 2. For every pair (D,m) we take as d the leading coefficient of the polynomial $f(x)$ in Table 2. In all these cases there is a single element in $E_d(\boldsymbol{Q})/2E_d(\boldsymbol{Q})$ such that the splitting field of its attached equivalent class agrees with the field $K_{\tilde{\omega}_D}$. We summarize the computations in Table 3.

---

[2] In Table 2 of [**18**], we claimed that the genus one curves $X_D^{(m)}$ for $(D,m) = (35,7)$, $(51,3)$ and $(115,23)$ fail to have rational points over the local fields $\boldsymbol{Q}_5$, $\boldsymbol{Q}_{17}$ and $\boldsymbol{Q}_5$, respectively. This is wrong: these curves admit rational points everywhere locally. In fact, both three curves are elliptic curves over $\boldsymbol{Q}$, since in each case $h(\boldsymbol{Q}(\sqrt{-D})) = 2$ and there exists a point $P \in \mathrm{CM}\big(\boldsymbol{Z}[\frac{1+\sqrt{-D}}{2}]\big)$ on X_D that projects onto a rational point on $X_D^{(m)}$. Namely, these three elliptic curves are, in Cremona notation, $35A1$, $51A2$ and $115A1$. Finally, let us also note in passing that Table 3 of [**18**] should read $(26,\omega_{26})$ instead of $(26,\omega_{13})$.

(D,m)	$y^2 = \quad f(x)$	$\mathrm{Jac}\left(X_D^{(m)}\right)$
$(39,13)$	$y^2 = -7x^4 - 24x^3 - 34x^2 + 24x - 7$	$39A1$
$(55,5)$	$y^2 = -3x^4 - 2x^3 - 9x^2 + 2x - 3$	$55A1$
$(62,2)$	$y^2 = -x^4 - 8x^3 - 78x^2 + 248x - 961$	$62A3$
$(69,3)$	$y^2 = -3(x^4 - 156x^2 + 6912)$	$69A2$
$(77,11)$	$y^2 = -11x^4 - 19x^2 - 16$	$77C2$
$(85,17)$	$y^2 = -3x^4 + 10x^3 - x^2 - 10x - 3$	$85A1$
$(94,2)$	$y^2 = -x^4 + 9x^2 - 32$	$94A2$
$(178,89)$	$y^2 = -12x^4 + 4x^3 - 19x^2 - 4x - 12$	$178B1$
$(210,30)$	$y^2 = -43x^4 - 686x^3 - 2915x^2 - 1372x - 172$	$210E5$
$(210,42)$	$y^2 = -43x^4 + 600x^3 - 986x^2 - 600x - 43$	$210A6$
$(210,70)$	$y^2 = -43x^4 + 256x^3 - 130x^2 - 768x - 387$	$210C3$
$(210,105)$	$y^2 = -43x^4 + 2x^3 + 505x^2 + 12x - 1548$	$210B6$
$(330,3)$	$y^2 = -3x^4 - 22x^3 - 125x^2 - 66x - 27$	$330B3$
$(330,22)$	$y^2 = -3x^4 + 1358x^2 - 177147$	$330C3$
$(330,33)$	$y^2 = -3x^4 + 2846x^2 - 2381643$	$330D2$
$(330,165)$	$y^2 = -3x^4 + 614x^2 - 19683$	$330A2$
$(462,154)$	$y^2 = -x^4 - 283x^2 - 16384$	$462B2$

Table 2. Equations for non-elliptic Atkin-Lehner quotients of genus one.

(D,m)	(A,B)	P
$(39,13)$	$(-217/3, -5510/27)$	$(-11/3, 288)$
$(55,5)$	$(-67, 126)$	$(-17, 44)$
$(62,2)$	$(-491, -154)$	$(-9, 62)$
$(69,3)$	$(-2235, 40534)$	$(26, 0)$
$(77,11)$	$(-2473/3, 227050/27)$	$(-418/3, 0)$
$(85,17)$	$(-409/3, -16454/27)$	$(23, 20)$
$(94,2)$	$(-155, -714)$	$(6, 0)$
$(178,89)$	$(-2137/3, 170170/27)$	$(-37, -128)$
$(210,30)$	$(-5762401/3, -27665272798/27)$	$(102257/3, 102900)$
$(210,42)$	$(-129649/3, -90882286/27)$	$(46301/3, 1646400)$
$(210,70)$	$(-50401/3, -22628702/27)$	$(9493/3, -4800)$
$(210,105)$	$(-1053721/3, -2163135238/27)$	$(43433/3, -43904)$
$(330,3)$	$(-12241/3, -2249422/27)$	$(-129, -2200)$
$(330,22)$	$(-513841/3, -733647278/27)$	$(679, 0)$
$(330,33)$	$(-5864929/3, -22155907934/27)$	$(1423, 0)$
$(330,165)$	$(-67849/3, -33554486/27)$	$(307, 0)$
$(462,154)$	$(-276697/3, 288510010/27)$	$(-566/3, 0)$

Table 3.

Here, $E = \mathrm{Jac}\left(X_D^{(m)}\right) : y^2 = x^3 + Ax + B$ and $P \in E_d(\boldsymbol{Q})$ lies in the class of $E_d(\boldsymbol{Q})/2E_d(\boldsymbol{Q})$ which provides the single $\boldsymbol{Q}$-equivalence class $dy^2 = f(x)$ isomorphic to E_d such that the splitting field of f is $K_{\tilde{\omega}_D}$. □

Remark 4.3. For all these curves, there is at the least one involution $u \in \mathscr{I}_0$ defined over $\boldsymbol{Q}$ commuting with w (though in some cases u does not arise from any Atkin-Lehner involution on $X_0(D,1)$). The equations obtained from the point P in Table 3 have been replaced in Table 2 by equivalent equations as in (1) or (2) of Proposition 2.2 depending on whether there exists an involution u with a fixed point that projects onto a rational point on $X_D^{(m)}/\langle\tilde{\omega}_D\rangle$ or not.

Remark 4.4. Kurihara conjecured in [**13**] equations for the genus three curves X_{39}, X_{55}, X_{62}, X_{69} and X_{94}. For $(D,m) = (39,13), (55,5), (62,2), (69,3), (94,2)$, our theorem above proves that Kurihara's conjectural equations for these genus one quotients are correct.

5. Appendix: Shimura curves and their points of complex multiplication.

Let B be an indefinite division quaternion algebra of discriminant $D = p_1 \cdots p_{2r}$, $D \geq 1$. For any integer $N \geq 1$ coprime to D, Shimura introduced a projective smooth algebraic curve $X_0(D,N)/\boldsymbol{Q}$ which can be described as follows.

Let $\mathscr{O}_{D,N}$ be an Eichler order of level N in B. Let $\mathrm{n} : B \to \boldsymbol{Q}$ denote the reduced norm on B and let B_+^* be the subgroup of elements of B^* of positive reduced norm. Let $\mathscr{O}_{D,N}^1 = \{\gamma \in \mathscr{O}_{D,N} : \mathrm{n}(\gamma) = 1\}$, which we regard as a discrete subgroup of $SL_2(\boldsymbol{R})$ through a fixed isomorphism $\Psi : B \otimes \boldsymbol{R} \simeq \mathrm{M}_2(\boldsymbol{R})$. Let $\mathscr{H}$ denote Poincaré's upper half-plane. Then

$$\mathscr{O}_{D,N}^1 \backslash \mathscr{H}$$

is a Riemann surface which is compact unless $D = 1$. We let $\Phi : \mathscr{H} \to \mathscr{O}_{D,N}^1 \backslash \mathscr{H}$ denote the natural uniformization map.

The following fundamental result is due to Shimura.

Theorem 5.1 ([**22**, Main Theorem I], [**24**, Theorem 2.5]). *Let $D = p_1 \cdots p_{2r} \geq 1$ be a square-free integer and let N be a positive integer coprime to D. There is a projective algebraic curve $X_0(D,N)/\boldsymbol{Q}$ such that there exists an open immersion of Riemann surfaces*

$$\mathscr{O}_{D,N}^1 \backslash \mathscr{H} \hookrightarrow X_0(D,N)(\boldsymbol{C}).$$

When $D > 1$, this is a biregular isomorphism.

In the theorem, $X_0(D,N)/\boldsymbol{Q}$ denotes Shimura's canonical model over $\boldsymbol{Q}$ as in [**22**, Section 3]. When $D = 1$, $X_0(N) := X_0(1,N)$ stands for the classical elliptic modular curve.

Proposition 5.2 ([**15**, p. 280, 301]). *For $D \neq 1$, the genus of $X_0(D,N)$ is*

$$g = 1 + \frac{DN}{12} \cdot \prod_{p|D} \left(1 - \frac{1}{p}\right) \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right) - \frac{e_3}{3} - \frac{e_4}{4},$$

where for $k = 3, 4$:

$$e_k = \prod_{p|D}\left(1 - \left(\frac{-k}{p}\right)\right) \cdot \prod_{p\|N}\left(1 + \left(\frac{-k}{p}\right)\right) \prod_{p^2|N} \nu_p(k), \quad \nu_p(k) = \begin{cases} 2 & \text{if } \left(\frac{-k}{p}\right) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Here $(\frac{\cdot}{\cdot})$ *stands for the Kronecker quadratic symbol.*

PROPOSITION 5.3 ([**23**, Proposition 4.4]). *Let* $D > 1$, $N \geq 1$, $(D, N) = 1$. *Then*

$$X_0(D, N)(\boldsymbol{R}) = \varnothing.$$

A fortiori, curves $X_0(D, N)$ fail to have rational points over $\boldsymbol{Q}$ when $D > 1$.

Assume for the rest of this appendix that N is square-free. As a natural subgroup of the group of automorphisms of $X_0(D, N)$ over $\boldsymbol{Q}$ there is the Atkin-Lehner group of involutions

$$W(D, N) = \text{Normalizer}_{B_+^*}(\mathscr{O}_{D,N}^1)/(\boldsymbol{Q}^* \cdot \mathscr{O}_{D,N}^1).$$

Its elements can be labelled as $W(D, N) = \{\omega_m(D, N) : m \mid D \cdot N, m > 0\}$, where $\omega_m(D, N) \in \mathscr{O}_{D,N}$ can be taken to be any generator of the only two-sided ideal of reduced norm m of $\mathscr{O}_{D,N}$. When no confusion on the choices of D and N can arise, we will simply denote $\omega_m = \omega_m(D, N)$. The Atkin-Lehner group is abelian, $W(D, N) \simeq (\boldsymbol{Z}/2\boldsymbol{Z})^{\sharp p|DN}$ and $\omega_m \cdot \omega_n = \omega_{m \cdot n/(m,n)^2}$ for any pair of divisors $n, m \mid DN$.

Let $J_0(D, N)/\boldsymbol{Q}$ denote the Jacobian variety of $X_0(D, N)$. In particular, $J_0(N) = J_0(1, N)$ stands for the Jacobian variety of $X_0(N)$. By the universal property of $J_0(D, N)$, we can regard $W(D, N)$ as a subgroup of $\text{Aut}_{\boldsymbol{Q}}(J_0(D, N))$.

For any integer $M \geq 1$ and a positive divisor $d \mid M$, let $J_0(M)^{d-\text{new}}/\boldsymbol{Q}$ denote the optimal quotient variety of $J_0(M)$ which is d-new with respect to the action of the Hecke algebra in the sense of [**3**, Section 1.7] and [**17**]. The action of the group $W(1, M)$ on $J_0(M)$ restricts to a well-defined action on $J_0(M)^{d-\text{new}}$.

THEOREM 5.4 ([**16**], [**3**, Sections 1.3–1.8]). *There exists an isogeny defined over* $\boldsymbol{Q}$

$$\psi : J_0(D \cdot N)^{D-\text{new}} \longrightarrow J_0(D, N)$$

such that, for each $\omega_m(D, N) \in W(D, N)$, *we have*

$$\psi^*(\omega_m(D, N)) = (-1)^{\sharp\{p|(D,m)\}}\omega_m(1, D \cdot N) \in \text{Aut}_{\boldsymbol{Q}}(J_0(D \cdot N)).$$

Note that when the genus $g(X_0(D, N)) = 1$ and $D > 1$, $X_0(D, N)$ is a non-elliptic genus one curve, which becomes isomorphic over $\bar{\boldsymbol{Q}}$ to the elliptic curve $J_0(D, N)$. The above result shows that in this case the conductor of $J_0(D, N)$ is $D \cdot N_0$ for some positive divisor $N_0 \mid N$. It turns out that for all these cases (cf. Lemma 3.1) $\dim J_0(D \cdot N)^{\text{new}} = 1$ and thus $\text{cond}(J_0(D, N)) = D \cdot N$.

5.1. CM-points and their fields of definition.

Let K be an imaginary quadratic field and let $R \subset K$ be an order of K. Following Eichler, we say that an embedding $q : R \hookrightarrow \mathscr{O}_{D,N}$ is *optimal* if $q(K) \cap \mathscr{O}_{D,N} = q(R)$. Via $\Psi \circ q$, $R \setminus \{0\}$ embeds in $GL_2^+(\boldsymbol{R}) = \{A \in GL_2(\boldsymbol{R}) : \det(A) > 0\}$ and there is a single point $x_q \in \mathscr{H}$ which is fixed by the action of $R \setminus \{0\}$ on $\mathscr{H}$. We say that q is *normalized* if for any $a \in K^*$, $\Psi \circ q(a) \cdot \left(\begin{smallmatrix} x_q \\ 1 \end{smallmatrix}\right) = a \cdot \left(\begin{smallmatrix} x_q \\ 1 \end{smallmatrix}\right)$.

Definition 5.5. The set $\mathrm{CM}(R)$ of complex multiplication (CM) points by R on $X_0(D,N)$ is the set $\{\Phi(x_q) \in X_0(D,N)(\boldsymbol{C})\}$, where $q : R \hookrightarrow \mathscr{O}_{D,N}$ is any normalized optimal embedding of R into $\mathscr{O}_{D,N}$.

As it follows from the definition, a point $x \in \mathscr{H}$ has complex multiplication by R if and only if the stabilizer

$$\mathrm{Stab}_{\mathscr{O}_{D,N}^+}(x) := \left\{\alpha \in \mathscr{O}_{D,N} \cap B_+^* : \Psi(\alpha) \cdot x = x\right\}$$

is $R \setminus \{0\}$. Indeed, if we let $\Phi(x_q) \in \mathrm{CM}(R)$ for some optimal embedding $q : R \hookrightarrow \mathscr{O}_{D,N}$, we have $\mathrm{Stab}_{\mathscr{O}_{D,N}^+}(x_q) = q(R) \setminus \{0\}$. Otherwise, if $x \in \mathscr{H}$ is not a CM-point, then $\mathrm{Stab}_{\mathscr{O}_{D,N}^+}(x) = \boldsymbol{Z} \setminus \{0\}$.

From now on, we fix the following notation.

- p denotes an integer prime.
- $K = \boldsymbol{Q}(\sqrt{-s})$ is a quadratic imaginary field.
- R is an order in K.
- f is the conductor of R.
- $\left(\frac{K}{p}\right)$ is the Kronecker symbol.
- $\left(\frac{R}{p}\right) = \begin{cases} \left(\frac{K}{p}\right) & \text{if } p \nmid f \\ 1 & \text{if } p \mid f \end{cases}$ is the Eichler symbol.
- $\mathrm{I}(R)$ is the group of fractional invertible ideals of R.
- $\mathfrak{a}, \mathfrak{b}, \ldots$ are elements in $\mathrm{I}(R)$.
- $\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a}) = |R/\mathfrak{a}|$.
- H_R is the ring class field of R, that is, the abelian extension of K unramified outside c such that $\mathrm{Gal}(H_R/K) \simeq \mathrm{Pic}(R)$.
- $h(R) = [H_R : K]$.
- $\sigma_{\mathfrak{a}}$ is the element in $\mathrm{Gal}(H_R/K)$ attached to $\mathfrak{a}$ by the Artin symbol.

Attached to the quadratic order R, the discriminant D and the level N, let us define

$$D(R) = \prod_{p \mid D, \left(\frac{R}{p}\right) = -1} p, \quad N(R) = \prod_{p \mid N, \left(\frac{R}{p}\right) = 1} p, \quad N^*(R) = \prod_{p \mid N, p \nmid f, \left(\frac{R}{p}\right) = 1} p,$$

and $W(R) = \{\omega_m \in W : m \mid D(R)N(R)\}$. Note that

$$\gcd(D(R)N^*(R), \mathrm{disc}(R)) = 1 \quad \text{and} \quad \gcd(D(R)N(R), \mathrm{disc}(R)) = \gcd(N, f).$$

PROPOSITION 5.6 ([**15**, Section 1], [**10**], [**3**, Lemma 2.5]). *The set* $\mathrm{CM}(R)$ *is nonempty if and only if* $\frac{DN}{D(R)N^*(R)}$ *divides* $\mathrm{disc}(R)$. *Moreover, in this case we have that* $W(R) \times \mathrm{Gal}(H_R/K)$ *acts freely and transitively on* $\mathrm{CM}(R)$, *and thus*

$$\sharp\mathrm{CM}(R) = 2^{\sharp\{p|D(R)N(R)\}} \cdot h(R).$$

Let $E(R, \mathscr{O}_{D,N})$ denote the set of normalized optimal embeddings $q : R \hookrightarrow \mathscr{O}_{D,N}$. The unit group $\mathscr{O}^1_{D,N}$ acts on $E(R, \mathscr{O}_{D,N})$ by conjugation and there is a one-to-one correspondence between $\mathscr{O}^1_{D,N}\backslash E(R, \mathscr{O}_{D,N})$ and $\mathrm{CM}(R)$. Proposition 5.6 above follows from this correspondence and Eichler's theory on optimal embeddings.

For any prime p, let $E_p(R, \mathscr{O}_{D,N}) := \{q : R \otimes \boldsymbol{Z}_p \hookrightarrow \mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p\}$ be the set of local optimal embeddings[3] at p. The coset $(\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p)^*\backslash E_p(R, \mathscr{O}_{D,N})$ has cardinality 1 or 2, and it is 2 if and only if $p \mid D(R) \cdot N(R)$. For any such prime p, there is a natural *orientation* map

$$o_p : \mathscr{O}^1_{D,N}\backslash E(R, \mathscr{O}_{D,N}) \longrightarrow (\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p)^*\backslash E_p(R, \mathscr{O}_{D,N}) = \{\pm 1\}.$$

Proposition 5.6 can be refined to claim that for any $v \in \{\pm 1\}^{\sharp\{p|D(R)N(R)\}}$, the cardinality of the fibre at v of $\prod_{p|D(R)N(R)} o_p$ is $h(R)$. We say that two points $P, P' \in \mathrm{CM}(R)$ lie in the same *branch* if the corresponding normalized optimal embeddings $q, q' \in E(R, \mathscr{O}_{D,N})$ are locally equivalent, that is, have the same orientation at all $p \mid D(R)N(R)$. The set $\mathrm{CM}(R)$ is the disjoint union of $2^{\sharp\{p|D(R)N(R)\}}$ branches, consisting of $h(R)$ points each (cf. [**15**, Section 1]).

More precisely, Galois elements $\sigma \in \mathrm{Gal}(H_R/K)$ preserve all local orientations of points in $\mathrm{CM}(R)$. For $p \mid D(R)N(R)$, Atkin-Lehner involutions ω_p switch the local orientation at p and preserve the remaining ones ([**3**, Lemmas 2.4 and 2.5]).

Fixed points of Atkin-Lehner involutions acting on Shimura curves are points of complex multiplication, sometimes by a non-maximal quadratic order:

PROPOSITION 5.7 ([**15**, Section 1]). *Let* $m \mid D \cdot N$, $m > 0$. *The set of fixed points of the Atkin-Lehner involution* ω_m *acting on* $X_0(D, N)$ *is*

$$\mathscr{F}_{\omega_m} = \begin{cases} \mathrm{CM}\big(\boldsymbol{Z}[\sqrt{-1}]\big) \cup \mathrm{CM}\big(\boldsymbol{Z}[\sqrt{-2}]\big) & \text{if } m = 2 \\ \mathrm{CM}\big(\boldsymbol{Z}[\sqrt{-m}]\big) \cup \mathrm{CM}\big(\boldsymbol{Z}\big[\frac{1+\sqrt{-m}}{2}\big]\big) & \text{if } m \equiv 3 \bmod 4 \\ \mathrm{CM}\big(\boldsymbol{Z}[\sqrt{-m}]\big) & \text{otherwise.} \end{cases}$$

For the rest of this section, let $R \subset K = \boldsymbol{Q}(\sqrt{-s})$, $s > 0$, be an imaginary quadratic order such that $\mathrm{CM}(R) \neq \varnothing$.

THEOREM 5.8 ([**22**, Main Theorem II], [**24**]). *Let* $P \in \mathrm{CM}(R)$ *and* $\boldsymbol{Q}(P)$ *be the*

[3]There is not a natural notion of *normalized* embeddings into $\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p$. Note also that the coset $\mathscr{O}^1_{D,N}\backslash E(R, \mathscr{O}_{D,N})$ is in one-to-one correspondence with the set of (non necessarily normalized) optimal embeddings $q : R \hookrightarrow \mathscr{O}_{D,N}$ up to conjugation by $\mathscr{O}^*_{D,N}$.

number field generated by the coordinates of P on $X_0(D,N)$. Then

(1) $H_R = K \cdot \boldsymbol{Q}(P)$.
(2) (*Shimura's reciprocity law*) *Let $q : R \hookrightarrow \mathscr{O}_{D,N}$ be a normalized optimal embedding such that $P = \Phi(x_q)$ and let $\mathfrak{a} \in \mathrm{I}(R)$. There exists $\beta \in \mathscr{O}_{D,N}$, $\mathrm{n}(\beta) > 0$, such that $q(\mathfrak{a})\mathscr{O}_{D,N} = \beta\mathscr{O}_{D,N}$ and for any such β we have*

$$P^{\sigma_{\mathfrak{a}}} = \Phi\big(\beta^{-1} x_q\big).$$

By part (1) of the above Theorem, we know that H_R is an extension of $Q(P)$ of degree at most 2. The determination of this subfield of H_R is the main result of this section, which is contained in Theorem 5.12. In order to obtain this, we need some previous lemmas.

Lemma 5.9. *Let $m \mid D \cdot N$ and $P \in \mathrm{CM}(R)$. Then $\omega_m(P) = P^\sigma$ for some $\sigma \in \mathrm{Gal}(H_R/K)$ if and only if $m \mid \frac{DN}{D(R)N(R)}$. If this is the case, $\sigma = \sigma_{\mathfrak{b}}$ for the ideal $\mathfrak{b} \in \mathrm{I}(R)$ such that $\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{b}) = m$.*

Proof. If $p \mid D(R)N(R)$ then ω_p switches the local orientation of P at p, whereas any $\sigma \in \mathrm{Gal}(H_R/K)$ preserves it and hence $\omega_p(P) \notin \mathrm{Gal}(H_R/K) \cdot P$.

Let $p \mid \frac{DN}{D(R)N(R)}$. By Proposition 5.6, p is a ramified prime of R which does not divide the conductor f and thus there exists $\mathfrak{p} \in \mathrm{I}(R)$ such that $\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{p}) = p$. Let $\beta \in \mathscr{O}_{D,N}$, $\mathrm{n}(\beta) > 0$, be such that $q(\mathfrak{p})\mathscr{O}_{D,N} = \beta\mathscr{O}_{D,N}$. Since $\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{p}) = p$ we have $\mathrm{n}(\beta) = p$.

Let $P = \Phi(x_q)$ for some optimal embedding $q : R \hookrightarrow \mathscr{O}_{D,N}$. By Theorem 5.8, we have $P^{\sigma_{\mathfrak{p}}} = \Phi(\beta^{-1}x_q)$. Let us show that $\omega_p(P) = \Phi(\beta x_q) = \Phi(\beta^{-1}x_q)$ as well. In order to prove this, it follows from the definition and properties of the Atkin-Lehner group that it suffices to show that $\mathscr{O}_{D,N} \cdot \beta$ is a two-sided ideal.

For $p \mid \frac{D}{D(R)}$ this is immediate, as there exists a unique ideal of norm p in $\mathscr{O}_{D,N}$, which is two-sided. Assume now that $p \mid \frac{N}{N(R)}$. The question is local and for all primes $\ell \neq p$, $\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_\ell \cdot \beta = \mathscr{O}_{D,N} \otimes \boldsymbol{Z}_\ell$. Locally at p, the Eichler order $\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p$ can be described as $\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p = \left\{ \left(\begin{smallmatrix} a & b \\ cp & d \end{smallmatrix}\right) : a,b,c,d \in \boldsymbol{Z}_p \right\}$. Since $\mathfrak{p}^2 = (p)$ it follows that $\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p \cdot \beta^2 = p \cdot \mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p$ and it is elementary to check that $\beta \in (\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p)^* \cdot \left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right)$ and hence normalizes $\mathscr{O}_{D,N}$. □

We next describe the action of complex conjugation on points of complex multiplication on $X_0(D,N)$. This shall serve us in the next section to exhibit rational points on the quotient curves $X_0(D,N)/\langle\omega_m\rangle$.

Lemma 5.10. *Let $P \mapsto \bar{P}$ denote the complex conjugation on $X_0(D,N)(\bar{\boldsymbol{Q}})$. Then*

(1) $\overline{\mathrm{CM}(R)} = \mathrm{CM}(R)$.
(2) *For every $P \in \mathrm{CM}(R)$ there exist $m \mid D(R)N(R)$ and $\mathfrak{a} \in \mathrm{I}(R)$ such that*

$$\bar{P} = \omega_m(P^{\sigma_{\mathfrak{a}}}).$$

Moreover, the integer m and the class $[\mathfrak{a}] \in \mathrm{Pic}(R)/\mathrm{Pic}(R)^2$ do not depend on P. More precisely, $m = D(R)N^*(R)$, $\mathfrak{a}$ satisfies

$$B_D \simeq \left(\frac{-s, D(R)N^*(R)N_{K/\boldsymbol{Q}}(\mathfrak{a})}{\boldsymbol{Q}}\right),$$

and for all $\mathfrak{b} \in [\mathfrak{a}]$ *there exists* $Q \in \mathrm{Gal}(H_R/K) \cdot P$ *such that* $\bar{Q} = \omega_m(Q^{\sigma_\mathfrak{b}})$.

Proof. Let $P = \Phi(x_q)$ for some normalized optimal embedding $q : R \hookrightarrow \mathscr{O}_{D,N}$. Let $\epsilon \in \mathscr{O}_{D,N}$ be of reduced norm $\mathrm{n}(\epsilon) = -1$. By [**23**], [**15**], $\bar{P} = \Phi(\epsilon \bar{x}_q)$.

(1) We have $\bar{P} = \Phi(\epsilon \bar{x}_q) = \Phi(x_{q \cdot \epsilon^{-1}})$. The embedding $a \mapsto \epsilon q(\bar{a})\epsilon^{-1}$ is a normalized optimal embedding of R into $\mathscr{O}_{D,N}$ and hence $\bar{P}$ is also a point of complex multiplication by R.

(2) Let $P \in \mathrm{CM}(R)$. By Proposition 5.6, $\bar{P} = \omega_{m_P}(P^{\sigma_{\mathfrak{a}_P}})$ for some $m_P \mid D(R)N(R)$ and $\mathfrak{a}_P \in \mathrm{I}(R)$. For a fixed P, the integer m_P and the class of the ideal $\mathfrak{a}_P$ in $\mathrm{Pic}(R)$ are unique, but may depend on P.

Let $Q \in \mathrm{CM}(R)$ be any other point with complex multiplication by R. By Proposition 5.6, $Q = \omega_d(P^{\sigma_\mathfrak{b}})$ for some $d \mid D(R)N(R)$ and $\mathfrak{b} \in \mathrm{I}(R)$. Thus $\bar{Q} = \omega_d(\overline{P^{\sigma_\mathfrak{b}}}) = \omega_d(\bar{P})^{\sigma_\mathfrak{b}^{-1}} = \omega_d(\omega_{m_P}(P^{\sigma_{\mathfrak{a}_P}}))^{\sigma_\mathfrak{b}^{-1}} = \omega_{m_P}(Q^{\sigma_{\mathfrak{a}_\mathfrak{b}^{-2}}})$. Hence, $m_P = m_Q$ and $[\mathfrak{a}_P] = [\mathfrak{a}_Q]$ in $\mathrm{Pic}(R)/\mathrm{Pic}(R)^2$ for any two points $P, Q \in \mathrm{CM}(R)$.

Let $m = m_P$ and $\mathfrak{a} = \mathfrak{a}_P$. Changing, if necessary, $\mathfrak{a}$ by an ideal in the same class in $\mathrm{Pic}(R)$, we can assume that $q(\mathfrak{a}^{-1}) \subset \mathscr{O}_{D,N}$ and $(\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a}^{-1}), DN) = 1$. For this choice, let $\beta \in \mathscr{O}_{D,N}$ be such that $q(\mathfrak{a}^{-1})\mathscr{O}_{D,N} = \beta\mathscr{O}_{D,N}$. Let $i = q(\sqrt{-s}) \in \mathscr{O}_{D,N}$. We first show the following

Claim. *There exists* $j \in \mathscr{O}_{D,N}$ *such that* $j^2 = m\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a}^{-1})$, $ij = -ji$.

We have that $\bar{P} = \omega_m(P^{\sigma_\mathfrak{a}})$. Since $\bar{P} = \Phi(\epsilon \bar{x}_q)$, by Theorem 5.8

$$\Phi(\epsilon \bar{x}_q) = \Phi(\gamma\beta x_q)$$

for some $\gamma \in \mathscr{O}_{D,N}$, $\mathrm{n}(\gamma) = m$. Thus $\alpha\epsilon\bar{x}_q = \gamma\beta x_q$ for some $\alpha \in \mathscr{O}^1_{D,N}$. If we write $\eta = \alpha\epsilon$, this reads

$$\eta\bar{x}_q = \gamma\beta x_q, \text{ with } \mathrm{n}(\eta) = -1.$$

Let $j = \eta^{-1}\gamma\beta \in \mathscr{O}_{D,N}$. As it is checked, $j(\mathscr{H}) = \bar{\mathscr{H}}$ and $j(\bar{\mathscr{H}}) = \mathscr{H}$; with $j(\bar{x}_q) = x_q$ and $j(\bar{x}_q) = x_q$. Hence j has no fixed points on $\mathscr{H} \cup \bar{\mathscr{H}}$ whereas j^2 fixes x_q and $\bar{x}_q$. By [**23**, Proposition 1.2] we obtain that $j^2 \in \boldsymbol{Q}^*$. Since $\mathrm{n}(j) = -m\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a}^{-1}) \in \boldsymbol{Z}$, $j^2 = m\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a}^{-1})$.

Moreover, the single fixed point of $jqj^{-1} : R \hookrightarrow \mathscr{O}_{D,N}$ on $\mathscr{H}$ is $j(\bar{x}_q) = x_q$. Hence, either $jq(\sqrt{-s})j^{-1} = q(\sqrt{-s})$ or $-q(\sqrt{-s})$. In the first case, it implies that $j \in q(K)$ and this can not be possible, since $\mathrm{n}(j) < 0$. Hence, $ij = -ji$. This proves our claim.

Let us now show that $m = D(R)N^*(R)$. By the discussion following Proposition 5.6, it suffices to show that for $p \mid D(R)N(R)$, we have $o_p(P) = -o_p(\bar{P})$ if and only if $p \mid D(R)N^*(R)$. In other words, for $p \mid D(R)N(R)$, there exists $\alpha \in (\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p)^*$ such that $\bar{q} = \alpha q \alpha^{-1}$ if and only if $p \mid (N, f)$.

Let $p \mid D(R)$. Then $B \otimes \boldsymbol{Q}_p = q(K \otimes \boldsymbol{Q}_p) \oplus q(K \otimes \boldsymbol{Q}_p) \cdot \pi$, where $\pi^2 = p$ and

$a \cdot \pi = \pi \cdot \bar{a}$ for any $a \in K$. For any $\alpha \in B_p$, we have $\alpha q(\sqrt{-s})\alpha^{-1} = -q(\sqrt{-s})$ if and only if $\alpha \in q(K \otimes \boldsymbol{Q}_p) \cdot \pi$, but none of these elements is an integral unit. Thus $o_p(P) = -o_p(\bar{P})$.

Let $p \mid N(R) = N^*(R) \cdot (N, f)$. Then $B_p \simeq \mathrm{M}_2(\boldsymbol{Q}_p)$ and we may assume that $\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p = \left\{ \left(\begin{smallmatrix} a & b \\ pc & d \end{smallmatrix}\right) : a, b, c, d \in \boldsymbol{Z}_p \right\} \subset \mathrm{M}_2(\boldsymbol{Q}_p)$. Assume now that $p \mid N^*(R)$. Then $q : K \otimes \boldsymbol{Q}_p \simeq \boldsymbol{Q}_p \times \boldsymbol{Q}_p \to \mathrm{M}_2(\boldsymbol{Q}_p)$, $(a, d) \mapsto \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$. Since $\bar{q}(a, d) = q(d, a)$, we have $\alpha q \alpha^{-1} = \bar{q}$ if and only if $\alpha = \left(\begin{smallmatrix} 0 & b \\ pc & 0 \end{smallmatrix}\right)$. None of these elements are units of $\mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p$, hence $o_p(P) = -o_p(\bar{P})$.

On the other hand, if $p \mid (N, f)$ we have (unless $p \neq 2$ and $s \equiv 3 \bmod 4$) $R \otimes \boldsymbol{Z}_p \simeq \boldsymbol{Z}_p + p^k \boldsymbol{Z}_p \sqrt{-s}$, where $p^k \parallel f$, $k \geq 1$. We can write $q : R \otimes \boldsymbol{Z}_p \to \mathscr{O}_{D,N} \otimes \boldsymbol{Z}_p$, $q(p^k\sqrt{-s}) \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -p^{2k}s & 0 \end{smallmatrix}\right)$. Since $\left(\begin{smallmatrix} 0 & -1 \\ p^{2k}s & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -p^{2k}s & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)^{-1}$, we deduce that $o_p(P) = o_p(\bar{P})$.

Similarly, if $p = 2 \mid (N, f)$ and $s \equiv 3 \bmod 4$, we have $R \otimes \boldsymbol{Z}_2 \simeq \boldsymbol{Z}_2 + 2^{k-1}\boldsymbol{Z}_2\sqrt{-s}$, where $2^k \parallel f$, $k \geq 1$, and $q(2^{k-1}\sqrt{-s}) \mapsto \left(\begin{smallmatrix} 2^{k-1} & -2^{k-2}(s+1) \\ 2^k & -2^{k-1} \end{smallmatrix}\right)$. As before, conjugating by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ we obtain that $o_p(P) = o_p(\bar{P})$. Summing up, we have shown that $m = D(R)N^*(R)$.

For the ideal $\mathfrak{a}$, we have $B_D = \boldsymbol{Q}(i, j) = \left(\frac{-s, m\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a}^{-1})}{\boldsymbol{Q}}\right) \simeq \left(\frac{-s, m\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a})}{\boldsymbol{Q}}\right)$.

Finally, let $\tau = \sigma_{\mathfrak{a}} \cdot \sigma_0^{-2}$ with $\sigma_0 \in \mathrm{Gal}(H_R/K)$. Then, $\bar{Q} = \omega_m(Q^\tau)$, where $Q = P^{\sigma_0}$. □

REMARK 5.11. If $\mathfrak{a} \in \mathrm{I}(R)$ satisfies $B_D \simeq \left(\frac{-s, m\,\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a})}{\boldsymbol{Q}}\right)$, then any other ideal in the class of $[\mathfrak{a}] \in \mathrm{Pic}(R)/\mathrm{Pic}(R)^2$ also satisfies this isomorphism. In general, the converse is not true, but if H_R is the Hilbert class field of K, then $[\mathfrak{a}] \in \mathrm{Pic}(R)/\mathrm{Pic}(R)^2$ is uniquely determined. Indeed, the isomorphism $\left(\frac{-s, m\,\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a})}{\boldsymbol{Q}}\right) \simeq \left(\frac{-s, m\,\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{b})}{\boldsymbol{Q}}\right)$ implies that $\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a} \cdot \mathfrak{b}^{-1}) = \mathrm{Norm}_{K/\boldsymbol{Q}}(\alpha)$ for some $\alpha \in K^*$. Then the value $\mathrm{Norm}_{K/\boldsymbol{Q}}(\alpha)$ (mod $\mathrm{disc}(R)$) is represented by a quadratic form of the principal genus of discriminant $\mathrm{disc}(R)$ and by genus theory $[\mathfrak{a}] = [\mathfrak{b}]$.

As a consequence of Theorem 5.8 and Lemma 5.10, we obtain the following result.

THEOREM 5.12. *Let $P \in \mathrm{CM}(R)$. We have that*

(1) *If $D(R)N^*(R) \neq 1$ then $\boldsymbol{Q}(P) = H_R$.*
(2) *If $D(R)N^*(R) = 1$ then $[H_R : \boldsymbol{Q}(P)] = 2$ and $\boldsymbol{Q}(P) \subset H_R$ is the subfield fixed by $\sigma = c \cdot \sigma_{\mathfrak{a}} \in \mathrm{Gal}(H_R/\boldsymbol{Q})$ for some $\mathfrak{a} \in \mathrm{I}(R)$ such that $B_D \simeq \left(\frac{-s, \mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a})}{\boldsymbol{Q}}\right)$, where c denotes the complex conjugation.*

PROOF. Let $P \in \mathrm{CM}(R)$. By Lemma 5.10 (2),

$$\mathrm{Gal}(H_R/\boldsymbol{Q}) \cdot P = \big(\mathrm{Gal}(H_R/K) \cdot P\big) \cup \big(\mathrm{Gal}(H_R/K) \cdot \omega_{D(R)N^*(R)}(P)\big).$$

Assume first that $D(R)N^*(R) \neq 1$. Then

$$\big(\mathrm{Gal}(H_R/K) \cdot P\big) \cap \big(\mathrm{Gal}(H_R/K) \cdot \omega_{D(R)N^*(R)}(P)\big) = \varnothing$$

because the action of $W(R) \times \mathrm{Pic}(R)$ on $\mathrm{CM}(R)$ is free by Proposition 5.6. Hence $\sharp\,\mathrm{Gal}(H_R/\boldsymbol{Q}) \cdot P = 2h(R) = [H_R : \boldsymbol{Q}]$. Since $K(P) \subseteq H_R$ by Theorem 5.8, it follows that $\boldsymbol{Q}(P) = H_R$.

Assume now that $D(R)N^*(R) = 1$. By Lemma 5.10 (2), $\sharp\,\mathrm{Gal}(H_R/\boldsymbol{Q}) \cdot P = h(R)$ and $\boldsymbol{Q}(P) \subset H_R$ must be a subfield of index 2 of H_R. Again, by Lemma 5.10 (2), $\boldsymbol{Q}(P)$ is the subfield of H_R fixed by $c \cdot \sigma_{\mathfrak{a}} \in \mathrm{Gal}(H_R/\boldsymbol{Q})$ for some $\mathfrak{a} \in \mathrm{I}(R)$ such that $B_D \simeq \left(\frac{-s,\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a})}{\boldsymbol{Q}}\right)$. □

Corollary 5.13. *Assume that either $h(R) = 1$ or $h(R) = 2$ and $D(R)N^*(R) = 1$. Then $X_0(D,N)(K) \neq \varnothing$.*

Let $m | D \cdot N$ and let $\pi_m : X_0(D,N) \to X_0(D,N)/\langle \omega_m \rangle$ denote the natural projection map. We say that a point $Q \in X_0(D,N)/\langle \omega_m \rangle(\bar{\boldsymbol{Q}})$ is a CM point if $\pi_m^{-1}(Q)$ is a pair of CM points on $X_0(D,N)$.

Corollary 5.14. *Let $P \in \mathrm{CM}(R) \subset X_0(D,N)(\bar{\boldsymbol{Q}})$ and $Q = \pi_m(P)$ for some $m \mid DN$. Set $m_r = \gcd\left(m, \frac{DN}{D(R)N(R)}\right) = \gcd(m, \mathrm{disc}(R)/\gcd(N,f))$ and let $\mathfrak{b}$ be the invertible ideal of R such that $\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{b}) = m_r$.*

(1) *Assume $D(R)N^*(R) \neq 1$. Then $\boldsymbol{Q}(Q)$ is*

$$\begin{cases} H_R^{\sigma_{\mathfrak{b}}} & \text{if } m/m_r = 1, \\ H_R^{\sigma_{\mathfrak{b}\mathfrak{a}} \cdot c} \text{ for some } \mathfrak{a} \text{ such that } B_D \simeq \left(\frac{-s,\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a})}{\boldsymbol{Q}}\right) & \text{if } m/m_r = D(R)N^*(R), \\ H_R & \text{otherwise.} \end{cases}$$

(2) *Assume $D(R)N^*(R) = 1$. Then*

$$\boldsymbol{Q}(Q) = \begin{cases} H_R^{\langle c \cdot \sigma_{\mathfrak{a}}, \sigma_{\mathfrak{b}} \rangle} & \text{if } m/m_r = 1, \\ H_R^{c \cdot \sigma_{\mathfrak{a}}} & \text{otherwise,} \end{cases}$$

for some $\mathfrak{a} \in \mathrm{Pic}(R)$ such that $B_D \simeq \left(\frac{-s,\mathrm{N}_{K/\boldsymbol{Q}}(\mathfrak{a})}{\boldsymbol{Q}}\right)$.

References

[1] S. Baba and H. Granath, Genus 2 curves with quaternionic multiplication, Preprint 2005.

[2] P. Bayer, Uniformization of certain Shimura curves, Differential Galois Theory, Banach Center Publications, **58**, Polish Academy of Sciences, 2002.

[3] M. Bertolini and H. Darmon, Heegner points on Mumford-Tate curves, Invent. Math., **126** (1996), 413–456.

[4] N. Bruin, V. Flynn, J. Gonzàlez and V. Rotger, On finiteness conjectures for endomorphism algebras of abelian surfaces, to appear in Math. Proc. Camb. Phil. Soc.

[5] J. E. Cremona, Elliptic curve data, 21 June, 2004. http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html.

[6] J. E. Cremona, Classical invariants and 2-descent on elliptic curves, J. Symbolic Comput., **31** (2001), 71–87.

[7] N. Elkies, Shimura curve computations, Lect. Notes Comp. Sci., **1423** (1998), 1–49.

[8] N. Elkies, Shimura curves for level-3 subgroups of the (2,3,7) triangle group, and some other examples, available at http://arxiv.org/math.NT/0409020.
[9] J. González and V. Rotger, Equations of Shimura curves of genus two, Int. Math. Res. Not., **14** (2004), 661–674.
[10] B. W. Jordan, On the Diophantine arithmetic of Shimura curves, Harvard Ph. D. Thesis, 1981.
[11] B. W. Jordan and R. Livné, Local diophantine properties of Shimura curves, Math. Ann., **270** (1985), 235–248.
[12] A. Kurihara, On some examples of equations defining Shimura curves and the Mumford uniformization, J. Fac. Sci. Univ. Tokyo, Sec. IA, **25** (1979), 277–301.
[13] A. Kurihara, On p-adic Poincaré series and Shimura curves, Intern. J. Math., **5** (1994), 747–763.
[14] The Magma Computational Algebra System. Available at http://magma.maths.usyd.edu.au/magma/
[15] A. P. Ogg, Real points on Shimura curves, Arithmetic and geometry, Progr. Math., **35**, Birkhäuser Boston, Boston, MA, 1983, 277–307.
[16] K. A. Ribet, Sur les varietés abéliennes à multiplications réelles, C. R. Acad. Sci. Paris, **291** (1980), 121–123.
[17] D. P. Roberts, Shimura curves analogous to $X_0(N)$, Harvard Ph. D. Thesis, 1989.
[18] V. Rotger, On the group of automorphisms of Shimura curves and applications, Compos. Math., **132** (2002), 229–241.
[19] V. Rotger, Modular Shimura varieties and forgetful maps, Trans. Amer. Math. Soc., **356** (2004), 1535–1550.
[20] V. Rotger, Shimura curves embedded in Igusa's threefold, Modular curves and abelian varieties, (eds. J. Cremona, J.-C. Lario, J. Quer and K. Ribet), Progr. Math., **224**, Birkhäuser, 2004, 263–273.
[21] V. Rotger, A. Skorobogatov and A. Yafaev, Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over $\boldsymbol{Q}$, Moscow Math. J., **5:2** (2005), 463–476.
[22] G. Shimura, Construction of class fields and zeta functions of algebraic curves, Ann. Math., **85** (1967), 58–159.
[23] G. Shimura, On the real points of an arithmetic quotient of a bounded symmetric domain, Math. Ann., **215** (1975), 135–164.
[24] G. Shimura, On canonical models of arithmetic quotients of bounded symmetric domains, Ann. Math., **91** (1970), 144–222.
[25] M. Stoll and J. E. Cremona, Minimal models for 2-coverings of elliptic curves, LMS J. Comput. Math., **5** (2002), 220–243.
[26] M. F. Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Math., **800**, Springer, 1980.

Josep González

Universitat Politècnica de Catalunya
Departament de Matemàtica Aplicada IV (EPSEVG)
Av. Victor Balaguer s/n
08800 Vilanova i la Geltrú
Spain
E-mail: josepg@ma4.upc.edu

Victor Rotger

Universitat Politècnica de Catalunya
Departament de Matemàtica Aplicada IV (EPSEVG)
Av. Victor Balaguer s/n
08800 Vilanova i la Geltrú
Spain
E-mail: vrotger@ma4.upc.edu