Compositio Mathematica **132:** 229–241, 2002.

On the Group of Automorphisms of Shimura Curves and Applications

VICTOR ROTGER*
Departament d'Àlgebra i Geometria, Universitat de Barcelona, Gran Via, 585, E-08007, Barcelona, Spain. e-mail: vrotger@mat.ub.es

(Received: 4 October 2000; accepted: 3 May 2001)

Abstract. Let V_D be the Shimura curve over $\mathbb{Q}$ attached to the indefinite rational quaternion algebra of discriminant D. In this note we investigate the group of automorphisms of V_D and prove that, in many cases, it is the Atkin–Lehner group. Moreover, we determine the family of bielliptic Shimura curves (over $\bar{\mathbb{Q}}$ and over $\mathbb{Q}$) and we use it to study the set of rational points on V_D over quadratic fields. Finally, we obtain explicit equations of elliptic Atkin–Lehner quotients of V_D.

Mathematics Subject Classifications (2000). 11G18, 14G35.

Key words: Shimura curves, automorphisms, rational points.

Introduction

Let B be an indefinite rational quaternion algebra and choose a maximal order $\mathcal{O} \subset B$ of integers. Let $D = p_1 \cdot \ldots \cdot p_{2r}$, p_i prime numbers, be the discriminant of B. We can view $\Gamma = \{\gamma \in \mathcal{O}, n(\gamma) = 1\}$ as an arithmetic subgroup of $\mathbf{SL}_2(\mathbb{R})$ through an identification $\Psi : B \otimes \mathbb{R} \cong M_2(\mathbb{R})$ and consider the Riemann surface $\Gamma\backslash\mathcal{H}$, where $\mathcal{H}$ denotes the upper-half plane of Poincaré. Shimura ([30]) showed that this is the set of complex points of an algebraic curve $V_D/\mathbb{Q}$ over $\mathbb{Q}$ which parametrizes **Abelian** surfaces with quaternionic multiplication by $\mathcal{O}$.

The classical modular case arises when we consider the split quaternion algebra $B = M_2(\mathbb{Q})$ of discriminant $D = 1$. In this case, $V_1 = \mathbf{A}^1_{\mathbb{Q}}$ is the j-line that classifies elliptic curves or, by squaring, **Abelian** surfaces with multiplication by $M_2(\mathbb{Z})$. Throughout, we will limit ourselves to *nonsplit* quaternion algebras, that is, $D \neq 1$. In this case, Γ has no parabolic elements and $\Gamma\backslash\mathcal{H}$ is already compact so there are no cusps and the automorphic forms on V_D do not admit Fourier expansions. In this regard, see [22].

As in the modular case, the elements of the Atkin–Lehner group $W = \{w_m : m \mid D\} \cong C_2^{2r}$, where C_2 is the cyclic group of order two, act as rational involutions on the Shimura curve V_D and there is a natural inclusion $W \subseteq \mathrm{Aut}_{\mathbb{Q}}(V_D)$ (see,

*Partially supported by a grant FPI from Ministerio de Educación y Ciencia, by DGCYT PB97-0893 and DGCYT PB96-0166.

e.g., [12, 25]). The aim of the present study is to examine the full group of automorphisms $\mathrm{Aut}(V_D \otimes \mathbb{C})$ of these curves. In the first section we describe its group structure and the field of definition of its elements and we prove that $\mathrm{Aut}(V_D \otimes \mathbb{C}) = W$ in many cases. In [24], Ogg studied the group of automorphisms of the modular curves $X_0(N)$ for square-free levels N and there, the action of $\mathrm{Aut}(X_0(N))$ on the set of cusps played a fundamental role. When $D > 1$, the difficulty lies precisely in the absence of cusps on V_D.

In Section 2, the family of Shimura curves V_D that admit bielliptic involutions is determined. The hyperelliptic problem was already settled by Michon and Ogg independently in [21, 23, 25] and the family of bielliptic modular curves $X_0(N)$ was given in [4]. Since $\mathrm{Aut}(X_0(N))$ is largely understood ([24, 17]), the main point in [4] was to count the number of fixed points of the non-Atkin–Lehner involutions that appear when $4 \mid N$ or $9 \mid N$. In our case, this difficulty does not arise but, on the other hand, the automorphism groups of the Shimura curves V_D are much less known.

In the last section, we derive some arithmetical consequences from the above results concerning the set of rational points on V_D over quadratic fields. Recall that by a fundamental theorem of Shimura, there are no real points on Shimura curves and therefore quadratic imaginary fields are the simplest fields over which these curves may have rational points. Our main theorem in this section completely solves a question posed and studied by Kamienny in [16]: which Shimura curves V_D of genus $g \geqslant 2$ admit infinitely many quadratic points? This question is motivated by Faltings' theorem on Mordell's conjecture and the answer is based upon ideas of Abramovich, Harris and Silverman (see [1] and [11]).

Finally, we use the Čerednik–Drinfeld theory to compute equations of elliptic Atkin–Lehner quotients of Shimura curves. Table III in Section 3 gives a Weierstrass equation of *all* elliptic curves of the form $V_D/\langle w \rangle$ where $w \in \mathrm{Aut}(V_D)$ is any $\mathbb{Q}$-bielliptic involution on the curve. Some examples were already given in [29].

The main tools used in this paper come from the reduction of Shimura curves at both good and bad places. Drinfeld constructed a projective model M_D over $\mathbb{Z}$ of the Shimura curve V_D which extends the moduli interpretation given by Shimura to Abelian schemes over arbitrary bases ([6, 7, 10]). Morita showed that M_D has good reduction at any prime $p \nmid D$ and Shimura ([30]) determined the zeta function of the special fibre of M_D at p. Moreover, the Čerednik–Drinfeld theory ([6, 8, 10, 14]) provides a good account of the behaviour of the reduction of $M_D \pmod p$ when $p \mid D$.

NOTATIONS. We will denote by $\beta \mapsto \bar{\beta}$ the conjugation map on B. The reduced trace and reduced norm on B will be denoted respectively by $\mathrm{tr}(\beta) = \beta + \bar{\beta}$ and $\mathrm{n}(\beta) = \beta \cdot \bar{\beta}$.

1. The Group of Automorphisms of Shimura Curves

Throughout, V_D will denote the canonical model over $\mathbb{Q}$ of the Shimura curve of discriminant $D = p_1 \cdot \ldots \cdot p_{2r} \neq 1$ (cf. [30]). It is a proper smooth scheme over $\mathbb{Q}$ of

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

dimension 1. Let $\mathrm{Aut}_{\mathbb{Q}}(V_D)$ be the group of $\mathbb{Q}$-automorphisms of V_D that sits inside the full group of automorphisms $\mathrm{Aut}_{\mathbb{C}}(V_D \otimes \mathbb{C})$ of the complex algebraic curve $V_D \otimes \mathbb{C}$.

PROPOSITION 1. *If $g(V_D) \geqslant 2$, then*

(1) *All automorphisms of $V_D \otimes \mathbb{C}$ are defined over $\mathbb{Q}$. That is:* $\mathrm{Aut}_{\mathbb{C}}(V_D \otimes \mathbb{C}) = \mathrm{Aut}_{\mathbb{Q}}(V_D)$.
(2) $\mathrm{Aut}_{\mathbb{Q}}(V_D) \cong C_2^s$, $s \geqslant 2r$.

Proof. In [27], Ribet proved that all the endomorphisms of an Abelian variety A/K with semistable reduction over a number field K are defined over an unramified extension of K. The Jacobian variety $J_D/\mathbb{Q}$ of V_D has good reduction at primes $p \nmid D$ and, from [15], we know that the identity's connected component of the reduction mod p, $p \mid D$, of the Néron model of J_D is a torus. Hence, J_D has semistable reduction over $\mathbb{Q}$ and all its endomorphisms are rational because $\mathbb{Q}$ has no nontrivial unramified extensions.

Since, by Hurwitz theorem, $\mathrm{Aut}_{\mathbb{C}}(V_D \otimes \mathbb{C})$ is a finite group, any automorphism of $V_D \otimes \mathbb{C}$ is defined over $\bar{\mathbb{Q}}$. Moreover, the natural map $\mathrm{Aut}_{\bar{\mathbb{Q}}}(V_D \otimes \bar{\mathbb{Q}}) \to \mathrm{Aut}_{\bar{\mathbb{Q}}}(J_D \otimes \bar{\mathbb{Q}})$ is injective and $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-equivariant and therefore, we conclude from above that all automorphisms of $V_D \otimes \mathbb{C}$ are rational.

For the second part, let $X_0(D)/\mathbb{Q}$ be the modular curve of level D and consider the new part $J_0(D)^{\mathrm{new}}/\mathbb{Q}$ of its Jacobian variety $J_0(D)$. It is well known ([27]) that $\mathrm{End}^0_{\mathbb{Q}}(J_0(D)^{\mathrm{new}}) \cong \mathbb{T} \otimes \mathbb{Q} \cong \prod_{i=1}^t K_i$, where $\mathbb{T}$ denotes the Hecke algebra of level D and K_i are totally real number fields. Ribet's isogeny theorem ([28]) states the existence of an isogeny $\varphi : J_D \longrightarrow J_0(D)^{\mathrm{new}}$ between J_D and $J_0(D)^{\mathrm{new}}$. This isogeny is Hecke invariant (but sign-interchanging for the Atkin–Lehner action) and defined over $\mathbb{Q}$. Hence, the ring of endomorphisms $\mathrm{End}_{\mathbb{Q}}(J_D)$ is an order in $\prod_{i=1}^t K_i$. An automorphism of the curve V_D induces an automorphism of finite order on J_D. Moreover, the group of integral units in $\prod_{i=1}^t K_i$ is isomorphic to C_2^t. So $\mathrm{Aut}_{\mathbb{Q}}(V_D) \cong C_2^s$ with $2r \leqslant s \leqslant t$, the first inequality holding just because $W \subseteq \mathrm{Aut}_{\mathbb{Q}}(V_D)$. □

We conclude that any automorphism of V_D acts as a rational involution on it. In view of the above proposition, we will simply denote the group $\mathrm{Aut}_{\mathbb{C}}(V_D \otimes \mathbb{C}) = \mathrm{Aut}_{\mathbb{Q}}(V_D)$ by $\mathrm{Aut}(V_D)$. Naturally we ask whether the Atkin–Lehner group is the full group of automorphisms of the curve, provided that $g(V_D) \geqslant 2$. This is the case for modular curves $X_0(N)$ of square free level N, $N \neq 37$ ([17, 24]).

Recall that an elliptic point on the curve V_D is a branched point of the natural projection $\mathcal{H} \to \Gamma\backslash\mathcal{H} = V_D(\mathbb{C})$. The stabilizers of those elliptic points in $\Gamma/\{\pm 1\}$ are of order 2 or 3. 2-elliptic points (resp. 3-elliptic points) correspond to Γ-conjugacy classes of embeddings of the quadratic order $\mathbb{Z}[i]$, $i^2 = -1$ (resp. $\mathbb{Z}[\rho]$, $\rho^3 = 1$) in the quaternion order $\mathcal{O}$. Their cardinality is given by

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

$$e_2 = \prod_{\ell|D}\left(1 - \left(\frac{-4}{\ell}\right)\right), \qquad e_3 = \prod_{\ell|D}\left(1 - \left(\frac{-3}{\ell}\right)\right),$$

where $(\frac{\cdot}{\cdot})$ denotes the Kronecker symbol.

THEOREM 2. *Let V_D be the Shimura curve of discriminant D. If it has no elliptic points, then* $\mathrm{Aut}(V_D) = W$.

Proof. If there are no elliptic points on $V_D(\mathbb{C})$, then the natural projection $\mathcal{H} \to \Gamma\backslash\mathcal{H} = V_D(\mathbb{C})$ is the universal cover of the Riemann surface $V_D(\mathbb{C})$ so $\mathrm{Aut}(V_D) \cong \mathrm{Norm}_{\mathbf{PGL}_2^+(\mathbb{R})}(\Gamma)/\Gamma$. Here the superindex $+$ denotes matrices with positive determinant. It is known that $W \cong \mathrm{Norm}_{B^\times}(\Gamma)/\mathbb{Q}^\times\Gamma \cong C_2^{2r}$ ([21, 25]). We observe now that the $\mathbb{Q}$-vector space spanned by Γ is $\langle\Gamma\rangle_{\mathbb{Q}} = B$. Indeed, since the reduced norm n is indefinite on the space of *pure quaternions* $B_0 = \{b \in B, \mathrm{tr}(b) = 0\}$, we can find linearly independent elements $\omega_1, \omega_2, \omega_3 \in B_0$ such that $\mathbb{Z}[\omega_i] \subset B$ is a real quadratic order in B. Then, by solving the corresponding Pell equations, we find units $\gamma_i \in \mathbb{Z}[\omega_i] \cap \Gamma$, $\gamma_i \neq \pm 1$, such that $\{1, \gamma_1, \gamma_2, \gamma_3\}$ is a $\mathbb{Q}$-basis of B.

Hence, any $\alpha \in \mathrm{Norm}_{\mathbf{GL}_2^+(\mathbb{R})}(\Gamma)$ will actually normalize $B^\times$. By the Skolem–Noether theorem, α induces an inner automorphism of B so that $\alpha \in \mathbb{R}^\times\mathrm{Norm}_{B^\times}(\Gamma)$. This shows that $\mathrm{Aut}(V_D) = W$.

Remark. In proving the above theorem, we have also shown that the Atkin–Lehner group W of an arbitrary Shimura curve V_D is exactly the subgroup of automorphisms that lift to a Möbius transformation on $\mathcal{H}$ through the natural uniformization $\mathcal{H} \to V_D(\mathbb{C}) = \Gamma\backslash\mathcal{H}$.

The proof remains valid for Eichler orders of square-free level N and therefore, it generalizes an analogous result of Lehner and Newman for discriminant $D = 1$ ([20]).

The next theorem is similar in spirit to Theorem 2 and requires a previous lemma due to Ogg.

LEMMA 3 ([24]). *Let K be a field and $\mu(K)$ its group of roots of unity. Let $p = \max(1, \mathrm{char}\, K)$ the characteristic exponent of K. Let C be an irreducible curve defined over K and $P \in C(K)$ a regular point on it. Let G be a finite group of K-automorphisms acting on C and fixing the point P. Then there is a homomorphism $f\colon G \to \mu(K)$ whose kernel is a p-group.*

THEOREM 4. *Let $D = 2p$, $3p$; p a prime number. If $g(V_D) \geqslant 2$, then* $\mathrm{Aut}(V_D) = W \cong C_2 \times C_2$.

Proof. Suppose first that $D = 2p$ with $p \equiv 3 \pmod 4$. In this case, the fixed points on V_D of the Atkin–Lehner involution w_2 are *Heegner points* (see, e.g., [2] for a general account). Their coordinates on Shimura's canonical model V_D generate certain class fields. More precisely, if the genus $g(V_D)$ is even, then w_2 exactly fixes two points P, P' with complex multiplication by the quadratic order $\mathbb{Z}[i]$ and hence

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

([32]) P, $P' \in V_D(\mathbb{Q}(i))$. If $g(V_D)$ is odd, then, besides P and P', w_2 fixes two more points Q, $Q' \in V_D(\mathbb{Q}(\sqrt{-2}))$ which have CM by $\mathbb{Z}[\sqrt{-2}]$. As we have seen, $\mathrm{Aut}(V_D)$ is an Abelian group so it acts on the set of fixed points of w_2 on V_D. Since all automorphisms are rational, they must keep the field of rationality of these points so that $\mathrm{Aut}(V_D)$ actually acts on $\{P, P'\}$. It follows from the previous lemma that the order of the stabilizer of P or P' in $\mathrm{Aut}(V_D)$ is at most 2. Hence, $\#\mathrm{Aut}(V_D) \leqslant 4$ and $\mathrm{Aut}(V_D) = W$.

Suppose now that $D = 2p$, $p \equiv 1 \pmod 4$ or $D = 3p$, $p \equiv 1 \pmod 3$. By the theory of Čerednik and Drinfeld, the special fibre $M_D \otimes \mathbb{F}_p$ of the reduction mod p of the integral model M_D of our Shimura curve consists of two rational irreducible components Z, Z' defined over $\mathbb{F}_{p^2}$. The complete local rings of the intersection points of Z and Z' over the maximal unramified extension $\mathbb{Z}_p^{\mathrm{unr}}$ of $\mathbb{Z}_p$ are isomorphic to $\mathbb{Z}_p^{\mathrm{unr}}[x, y]/(xy - p^\ell)$ for some *length* $\ell \geqslant 1$. The reduction mod p of the Atkin–Lehner involution w_p switches Z and Z', fixing the double points of intersection. Among these double points, there is exactly one, say $\tilde{Q}$, which has *length* 2, as it follows from [18]. Thus $\mathrm{Aut}(V_D)$ acting on $M_D \otimes \mathbb{F}_p$ must fix $\tilde{Q}$. Recalling now that $\mathrm{Aut}(V_D) \cong C_2^s$, we again apply Ogg's lemma to the curve $Z/\mathbb{F}_{p^2}$ ($p \neq 2$) and the point $\tilde{Q}$ to obtain that $\#\mathrm{Aut}(V_D) \leqslant 4$. Therefore, $\mathrm{Aut}(V_D) = W$.

In the remaining case, namely when $D = 3p$, $p \equiv -1 \pmod 3$, we observe the curious phenomenon that $\ell = 109$ is a prime of good reduction for the Shimura curve V_D that yields

$$\#M_D \otimes \mathbb{F}_{109}(\mathbb{F}_{109}) \not\equiv 0 \pmod 4$$

except for the two exceptional cases $D = 3 \times 89$ and $D = 3 \times 137$. In any case, we check that $\#M_{3\times 89} \otimes \mathbb{F}_{67}(\mathbb{F}_{67}) = 94$ and $\#M_{3\times 137} \otimes \mathbb{F}_{103}(\mathbb{F}_{103}) = 98$. This is carried out by using the explicit formula for the number of rational points over finite fields of the reduction of Shimura curves at good places given by Jordan and Livné in [14]. From this we proceed as above: since all automorphisms of V_D are defined over $\mathbb{Q}$, their reduction mod ℓ must preserve the $\mathbb{F}_\ell$-rational points on $M_D \otimes \mathbb{F}_\ell$ and we apply Ogg's lemma to the regular curve $M_D \otimes \mathbb{F}_\ell$ to conclude that $\mathrm{Aut}(V_D) = W$. □

Remark. The first argument can be adapted for more general discriminants in an obvious way. For instance, if $D = p\delta$ where p is a prime integer, $p \equiv 3 \pmod 8$, and $(\frac{-p}{\ell}) = -1$ for any $\ell \mid \delta$, then we again obtain that $\mathrm{Aut}(V_D) = W$ because the Hilbert class field of $\mathbb{Q}(\sqrt{-p})$ is strictly contained in the ring class field of conductor 2 and, by genus theory, $h(-p)$ is odd.

EXAMPLE. Shimura curve quotient $V_{291}^+ = V_{291}/W$ has genus 2 and therefore, it is hyperelliptic. However, the hyperelliptic involution on V_{291}^+ is exceptional: it does not lift to a Möbius transformation on $\mathcal{H}$ through $\pi\colon \mathcal{H} \to V_{291}^+(\mathbb{C}) = \Gamma \cdot W \backslash \mathcal{H}$, while all automorphisms of V_{291} are of Atkin–Lehner type by Theorem 4. This is caused by the fact that π is not the universal cover of V_{291}^+.

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

2. Bielliptic Shimura Curves

Recall that an algebraic curve C of genus $g \geqslant 2$ is (geometrically) bielliptic if it admits a degree 2 map $\varphi\colon C \to E$ onto a curve E of genus 1. We will ignore fields of rationality until the next section. Alternatively, C is bielliptic iff there is an involutive automorphism acting on it with $2g-2$ fixed points. We present now some facts about bielliptic curves C such that, like Shimura curves, $\mathrm{Aut}(C) \cong C_2^s$.

LEMMA 5. *Let C/K, $\mathrm{char}\, K \neq 2$, be a bielliptic curve of genus g with $\mathrm{Aut}(C) \cong C_2^s$ for some $s \geqslant 1$. For any $w \in \mathrm{Aut}(C)$, let $n(w)$ denote the number of fixed points of w on C. Let v be a bielliptic involution on C and for any $w \in \mathrm{Aut}(C)$, $w \neq 1$ or v, denote $w' = v \cdot w$.*

(1) *If g is even, then $n(w) = 2$ and $n(w') = 6$, or vice versa. If g is odd, then $\{n(w), n(w')\} = \{0,0\}, \{0,8\}$ or $\{4,4\}$ as nonordered pairs.*
(2) *If g is even, then $s \leqslant 3$. If g is odd, then $s \leqslant 4$.*
(3) *If $g \geqslant 6$, then the bielliptic involution v is unique.*

Proof. The first part follows from Hurwitz's theorem applied to the map $C \to C/\langle v, w\rangle$, while 2. and 3. are simple corollaries of that. □

Remark. Observe that if D is odd, then $g(V_D)$ is always odd, as we check from Eichler's formula for the genus (see, e.g., [25]).

Obviously, the main source for possible bielliptic involutions on the curves V_D is the Atkin–Lehner group. From Eichler's formula for $n(w)$, $w \in W$ (see [25]), it is a routine exercise to check whether V_D has bielliptic involutions of the Atkin–Lehner type. An alternative way to compute $n(w)$ is to read *backwards* the last column of Table 5 in [3]. This is because Ribet's isogeny $\varphi\colon J_D \to J_0(D)^{\mathrm{new}}$ switches the sign of the Atkin–Lehner action. But, first, we should focus on possible extra involutions and also bound the bielliptic discriminants D. Following Ogg's method in [23], we give such an upper bound in the next

PROPOSITION 6. *If $D > 547$, V_D is not bielliptic.*

Proof. Suppose that the curve V_D is bielliptic: there is a degree 2 map $\varphi\colon V_D \to E$ onto a curve E of genus 1. By Proposition 1.2, both φ and E are defined over $\mathbb{Q}$ although E may not be an elliptic curve over $\mathbb{Q}$ since it may fail to have rational points (see Section 3 for examples). Choose a prime of good reduction $\ell \nmid D$ of V_D, let K_ℓ be the quadratic unramified extension of $\mathbb{Q}_\ell$ and let R_ℓ denote its ring of integers. As follows from [14], $V_D(K_\ell) \neq \emptyset$ and, hence, E is an elliptic curve over K_ℓ. Moreover, due to Ribet's isogeny theorem, E also has good reduction over ℓ. By the universal property of the Néron model of E over R_ℓ, φ extends to the minimal smooth model $M_D \otimes R_\ell$ of V_D and we can reduce the bielliptic structure mod ℓ to obtain a $2:1$ map $\tilde{\varphi}\colon M_D \otimes \mathbb{F}_{\ell^2} \to \tilde{E}$. From Weil's estimate,

$$N_{\ell^2} = \#M_D \otimes \mathbb{F}_{\ell^2}(\mathbb{F}_{\ell^2}) \leqslant 2 \cdot \#\tilde{E}(\mathbb{F}_{\ell^2}) \leqslant 2(\ell+1)^2.$$

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

Besides, we obtain from [14] that

$$\frac{(\ell-1)}{12}\prod_{p|D}(p-1) \leqslant N_{\ell^2}$$

so N_{ℓ^2} grows as D tends to infinity. Applying these inequalities for $\ell = 2, 3, 5, 7$ and 11, we conclude that, if $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \nmid D$, then $D \leqslant 546$. But, if $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \mid D$, then $s \geqslant 5$ and therefore, V_D cannot be bielliptic (Lemma 5.2). □

We are now able to prove the following theorem.

THEOREM 7. *There are exactly 32 values of D for which V_D is bielliptic. In each case, the bielliptic involutions are of Atkin–Lehner type. These values, together with the genus $g = g(V_D)$ and the bielliptic involutions are given in Table I.*

Proof. Since we need only consider discriminants $D \leqslant 546$, we can first use any programming package to build up the list of Atkin–Lehner bielliptic involutions on Shimura curves V_D. These computations yield Table I below. In order to ensure that no extra bielliptic involutions arise, we observe that the above results (and in particular Theorem 4) imply that any bielliptic involution on V_D, for most of the discriminants $D \leqslant 546$, must be of Atkin–Lehner type. There are exactly three cases, namely $D = 55$, $D = 85$ and $D = 145$, for which none of the previous results and their obvious generalizations seem to apply.

Ad hoc arguments can be worked out for them. Firstly, the Jacobian varieties of the curves V_{55} and V_{85} have just one $\mathbb{Q}$-isogeny class of sub-Abelian varieties of dimension 1, so there can be at most one bielliptic involution on these curves. But w_5 (resp. w_{17}) is already a bielliptic involution on V_{55} (resp. V_{85}).

More interesting is the curve V_{145} of genus 9. It is not bielliptic by any Atkin–Lehner involution although $J_{145} \sim_{\mathbb{Q}} E \times S \times A_3 \times A_3'$, where each factor has dimension 1, 2, 3 and 3, respectively. We check that $n(w_5) = n(w_{29}) = 0$ and $n(w_{145}) = 8$,

Table 1. Bielliptic Shimura curves

D	g	w_m	D	g	w_m	D	g	w_m
26	2	w_2, w_{13}	82	3	w_{82}	210	5	$w_{30}, w_{42},$
35	3	w_7	85	5	w_{17}			$w_{70}, w_{105},$
38	2	w_2, w_{19}	94	3	w_2			w_{210}
39	3	w_{13}	106	4	w_{53}, w_{106}	215	15	w_{215}
51	3	w_3	115	6	w_{23}	314	14	w_{314}
55	3	w_5	118	4	w_{59}, w_{118}	330	5	w_3, w_{22}
57	3	w_{57}	122	6	w_{122}			$w_{33}, w_{165},$
58	2	w_2, w_{58}	129	7	w_{129}			w_{330}
62	3	w_2	143	12	w_{143}	390	9	w_{390}
65	5	w_{65}	166	6	w_{166}	462	9	w_{154}
69	3	w_3	178	7	w_{89}	510	9	w_{510}
77	5	w_{11}, w_{77}	202	8	w_{101}	546	13	w_{546}

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

so if there was a bielliptic involution v on V_{145} then $n(w'_{145}) = 0$, by lemma 5.1. It follows from Lefschetz's fixed point formula (see [5]) that the rational traces of these three involutions on the Jacobian J_{145} would be $\mathrm{tr}(w_5) = \mathrm{tr}(w_{29}) = \mathrm{tr}(w'_{145}) = 2$. Moreover, involutions on J_{145} must be of the form $\{\pm 1_E\} \times \{\pm 1_S\} \times \{\pm 1_{A_3}\} \times \{\pm 1_{A'_3}\}$, up to conjugation by φ, thus $\mathrm{tr} = 2$ can only be attained by two different involutions. Therefore, v cannot exist and V_{145} is not bielliptic.

It can be showed that actually $\mathrm{Aut}(V_{145}) = W$: from the decomposition of J_{145} we know that $W \cong C_2^2 \subseteq \mathrm{Aut}(V_{145}) \subseteq C_2^4$. Since V_{145} is neither hyperelliptic ([25]) nor bielliptic (as we have just seen), it follows that the involutions

$$\{-1_E\} \times \{-1_S\} \times \{-1_{A_3}\} \times \{-1_{A'_3}\}$$

and

$$\{+1_E\} \times \{-1_S\} \times \{-1_{A_3}\} \times \{-1_{A'_3}\}$$

cannot be induced from $\mathrm{Aut}(V_{145})$. Thus it is a subgroup of index at least 4 in C_2^4 and $\mathrm{Aut}(V_{145}) = W$. □

3. Infinitely Many Quadratic Points on Shimura Curves

In [31], Shimura proved that $V_D(\mathbb{R}) = \emptyset$ and in particular there are no $\mathbb{Q}$-rational points on Shimura curves V_D. Jordan and Livné ([14]) gave explicit criteria for deciding whether the curves V_D do have rational points over the p-adic fields $\mathbb{Q}_p$ for any finite prime p.

Much less is known about rational points over global fields. Jordan [13] proved that for a fixed quadratic imaginary field K, with class number $h_K \neq 1$, there are only finitely many discriminants D for which K splits the quaternion algebra B of discriminant D and $V_D(K) \neq \emptyset$. In this section we solve a question that is to an extent reciprocal: which Shimura curves V_D, $g(V_D) \geqslant 2$, have infinitely many quadratic points over $\mathbb{Q}$?

That is,

$$\#V_D(\mathbb{Q}, 2) = \#\{P \in V_D(\bar{\mathbb{Q}}), [\mathbb{Q}(P) : \mathbb{Q}] \leqslant 2\} = +\infty.$$

We will say that an algebraic curve C/K of genus $g \geqslant 2$ is *hyperelliptic* over K (respectively *bielliptic* over K) if there is an involution $v \in \mathrm{Aut}_K(C)$ such that the quotient curve $C/\langle v \rangle$ is K-isomorphic to $\mathbb{P}^1_K$ (resp. an elliptic curve E/K). Notice that in both cases $C/\langle v \rangle(K) \neq \emptyset$ while it perfectly well happen that $C(K) = \emptyset$.

The following theorem of Abramovich and Harris shows that the question above is closely related to the diophantine problem of determining the family of hyperelliptic and bielliptic Shimura curves over $\mathbb{Q}$.

THEOREM 8 ([1]). *Let C be an algebraic curve of genus greater than or equal to 2, defined over a number field K. Then $C(K, 2) = \#\infty$ if and only if C is either hyperelliptic over K or bielliptic over K mapping to an elliptic curve E of* $\mathrm{rank}_K(E) \geqslant 1$.

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

Ogg ([25, 26]) gave the list of hyperelliptic Shimura curves over $\mathbb{Q}$. In what follows, we will determine which bielliptic Shimura curves from Table I are bielliptic over $\mathbb{Q}$.

We first observe that the map $V_D \to V_D/\langle w\rangle$ is always defined over $\mathbb{Q}$ since we showed that $\mathrm{Aut}_{\mathbb{C}}(V_D \otimes \mathbb{C}) = \mathrm{Aut}_{\mathbb{Q}}(V_D)$ (Proposition 1). In order to check whether $V_D/\langle w\rangle(\mathbb{Q}) \neq \emptyset$ for each pair (D,w) in Table I, we can disregard those in which $V_D/\langle w\rangle$ fails to have rational points over some completion $\mathbb{Q}_v$ of $\mathbb{Q}$. This is done by using the precise results in that direction given by Jordan and Livné in [14] and Ogg in [25] and [26]; the conclusions are compiled in Table II. Let us say that a field L is *deficient* for an algebraic curve C defined over a subfield $K \subset L$ if $C(L) = \emptyset$.

On the genus 1 Atkin–Lehner quotients $V_D/\langle w_m\rangle$ that do have rational points over all completions of $\mathbb{Q}$, we can try to construct a $\mathbb{Q}$-rational point by means of the theory of complex multiplication. That is, a Heegner point $P \in V_D(K)$ with CM by a quadratic imaginary order R, $R \otimes \mathbb{Q} = K$, $h(R) = 1$, will project onto a $\mathbb{Q}$-rational point on $V_D/\langle w_m\rangle$ if and only if $w_m(P) = \bar{P}$, where $\bar{P}$ is the complex conjugate of P on $V_D(K)$. From [12], 3.1.4, we deduce that $w_m(P) = \bar{P}$ if m is the product of the primes $p \mid D$ that are inert in K.

Performing the necessary computations, it follows that among those pairs (D, w) that $V_D/\langle w\rangle(\mathbb{Q}_v) \neq \emptyset$ for every completion $\mathbb{Q}_v$ of $\mathbb{Q}$, it is always possible to produce a $\mathbb{Q}$-rational point on $V_D/\langle w\rangle$ by the above means, except for two interesting cases: (V_{26}, w_2) and (V_{58}, w_2).

Since $\mathrm{g}(V_{26}) = \mathrm{g}(V_{58}) = 2$, we may apply a result of Kuhn ([19]) to deduce that there are also rational points on the quotients $V_{26}/\langle w_2\rangle$ and $V_{58}/\langle w_2\rangle$. Therefore, the Hasse–Minkowsky principle is never violated for the Atkin–Lehner quotients from Table I and those pairs $V_D/\langle w_m\rangle$ that do not appear in Table II are bielliptic curves over $\mathbb{Q}$. There are only eighteen values of D for which V_D admits a bielliptic involution over $\mathbb{Q}$.

It still remains to compute the Mordell–Weil rank of the elliptic curves $V_D/\langle w\rangle$ over $\mathbb{Q}$. Using Cremona's tables ([9]), switching the sign of the Atkin–Lehner action as explained above, we can determine the $\mathbb{Q}$-isogeny class of these elliptic curves.

Table II. Deficient completions L of $\mathbb{Q}$ for $V_D/\langle w_m\rangle$

D	w_m	L	D	w_m	L	D	w_m	L
35	w_7	$\mathbb{Q}_5$	115	w_{23}	$\mathbb{Q}_5$	330	w_3	$\mathbb{R},\mathbb{Q}_2$
39	w_{13}	$\mathbb{R},\mathbb{Q}_3$	178	w_{89}	$\mathbb{R},\mathbb{Q}_2$			$\mathbb{Q}_5,\mathbb{Q}_{11}$
51	w_3	$\mathbb{Q}_{17}$	210	w_{30}	$\mathbb{R},\mathbb{Q}_3$	330	w_{22}	$\mathbb{R},\mathbb{Q}_2,\mathbb{Q}_3$
55	w_5	$\mathbb{R},\mathbb{Q}_{11}$	210	w_{42}	$\mathbb{R},\mathbb{Q}_2,\mathbb{Q}_3$			$\mathbb{Q}_5,\mathbb{Q}_{11}$
62	w_2	$\mathbb{R},\mathbb{Q}_{31}$			$\mathbb{Q}_5,\mathbb{Q}_7$	330	w_{33}	$\mathbb{R},\mathbb{Q}_2$
69	w_3	$\mathbb{R},\mathbb{Q}_{23}$	210	w_{70}	$\mathbb{R},\mathbb{Q}_2$			$\mathbb{Q}_3,\mathbb{Q}_5$
77	w_{11}	$\mathbb{R},\mathbb{Q}_7$			$\mathbb{Q}_3,\mathbb{Q}_5$	330	w_{165}	$\mathbb{Q}_2,\mathbb{Q}_3$
85	w_{17}	$\mathbb{Q}_5$	210	w_{105}	$\mathbb{R},\mathbb{Q}_2$			$\mathbb{Q}_5,\mathbb{Q}_{11}$
94	w_2	$\mathbb{R},\mathbb{Q}_{47}$			$\mathbb{Q}_7$	462	w_{154}	$\mathbb{R},\mathbb{Q}_{11}$

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

This is enough to compute their Mordell–Weil rank but we can use a beautiful idea of Roberts ([29]) to compute the $\mathbb{Q}$-isomorphism class and, hence, a Weierstrass equation for them as follows: Cremona's tables give the Kodaira symbols of the reduction of elliptic curves E at the primes $p \mid \mathrm{cond}(E)$. This is done by using Tate's algorithm which makes use of a Weierstrass equation of the curve. This is not available in our case, but we can instead use the Čerednik–Drinfeld theory to compute the Kodaira symbols for the reduction mod p, $p \mid D$, of $V_D/\langle w \rangle$ and contrast them with Cremona's tables. This procedure uniquely determines the $\mathbb{Q}$-isomorphism class of the curves.

EXAMPLE. Curve V_{210} has genus 5 and is bielliptic by the Atkin–Lehner involution w_{210}. After Eichler's theory on optimal embeddings (see, e.g., [25]), the quadratic order $\mathbb{Z}[\sqrt{-43}]$ embeds in the quaternion algebra B of discriminant 210. Such an embedding produces a point $P \in V_{210}(\mathbb{Q}(\sqrt{-43}))$. From the above, it follows that $w_{210}(P) = \bar{P}$. Therefore, $V_{210}/\langle w_{210} \rangle(\mathbb{Q}) \neq \emptyset$ and we obtain that (V_{210}, w_{210}) is a bielliptic pair over $\mathbb{Q}$. A glance at Cremona's Table 3 in [9], pp. 249–250, shows that the elliptic curve $V_{210}/\langle w_{210} \rangle$ falls in the $\mathbb{Q}$-isogeny class $210D$ because it is the only one that corresponds to a newform $f \in H^0(\Omega^1, J_{210})$ such that $w_{210}^*(f) = f$ (recall that the sign for the Atkin–Lehner action is opposite to the classical modular case!). Therefore, from Cremona's Table 4, $\mathrm{rank}_{\mathbb{Q}}(V_{210}/\langle w_{210} \rangle) = 1$.

In order to determine a Weierstrass equation for $V_{210}/\langle w_{210} \rangle$ we may compute the Kodaira symbols of its reduction mod p, $p \mid 210$. It suffices to study the reduction at $p = 3$. The Čerednik–Drinfeld theory asserts that $M_{210} \otimes \mathbb{F}_3$ is reduced and its irreducible components are all rational and defined over $\mathbb{F}_9$. Moreover, $M_{210} \otimes \mathbb{Z}_3$ is a (minimal) regular model over $\mathbb{Z}_3$. This is because over the quadratic unramified integral extension R_3 of Z_3, $M_{210} \otimes R_3$ is a Mumford curve uniformized by a (torsion-free) Schottky group, as one checks from Čerednik–Drinfeld's explicit description of this group and the congruences $5 \equiv -1 \pmod 3$ and $7 \equiv -1 \pmod 4$.

In a way, Čerednik–Drinfeld's description of the reduction of Shimura curves at $p \mid D$ is not so different from Deligne–Rappoport's for the modular curves $X_0(N)$ at $p \parallel N$ because $M_{p\delta} \otimes \mathbb{F}_p$ is again the union of two copies of the Shimura curve – also called the Gross curve – $M_\delta \otimes \mathbb{F}_p$, defined in terms of a *definite* quaternion algebra.

Let $h(\delta, v)$ denote the class number of an (arbitrary) Eichler order of level v in the quaternion algebra of discriminant δ. The dual graph $\mathcal{G}$ of $M_{210} \otimes \mathbb{F}_3$ has as vertices the irreducible components of $M_{210} \otimes \mathbb{F}_3$. There are

$$2h\left(\frac{210}{3}, 1\right) = 2h(70, 1) = 4$$

of them. Two vertices v, $\tilde{v}$ in $\mathcal{G}$ are joined by as many edges as there are intersection points between the corresponding components Z, $\tilde{Z}$ in $M_{210} \otimes \mathbb{F}_3$. In our case, there are $h(\frac{210}{3}, 3) = 8$ edges in $\mathcal{G}$, that is, 8 double points in $M_{210} \otimes \mathbb{F}_3$.

We may label the 4 vertices v_1, v_1', v_2, v_2' so that $w_3(v_i) = v_i'$, where w_3 still denotes the involution w_3 now acting on $\mathcal{G}$. There are no edges joining v_1 and v_2, and the same holds for v_1' and v_2'. The total number of edges joining v_1 with v_1' and v_2 with

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

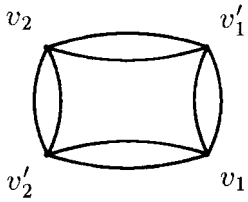

Figure 1. Dual graph of $M_{210} \otimes \mathbb{F}_3$.

Table III. Shimura curves V_D, $g(V_D) \geqslant 2$, with $\#V_D(\mathbb{Q}, 2) = +\infty$

D	w_m	$V_D/\langle w_m \rangle$	D	w_m	$V_D/\langle w_m \rangle$	D	w_m	$V_D/\langle w_m \rangle$
26	w_{13}	$\mathbb{P}^1_{\mathbb{Q}}$	77	w_{77}	$77A_1$	143	w_{143}	$143A_1$
35	w_{35}	$\mathbb{P}^1_{\mathbb{Q}}$	82	w_{82}	$82A_1$	146	w_{146}	$\mathbb{P}^1_{\mathbb{Q}}$
38	w_{38}	$\mathbb{P}^1_{\mathbb{Q}}$	86	w_{86}	$\mathbb{P}^1_{\mathbb{Q}}$	159	w_{159}	$\mathbb{P}^1_{\mathbb{Q}}$
39	w_{39}	$\mathbb{P}^1_{\mathbb{Q}}$	87	w_{87}	$\mathbb{P}^1_{\mathbb{Q}}$	166	w_{166}	$166A_1$
51	w_{51}	$\mathbb{P}^1_{\mathbb{Q}}$	94	w_{94}	$\mathbb{P}^1_{\mathbb{Q}}$	194	w_{194}	$\mathbb{P}^1_{\mathbb{Q}}$
55	w_{55}	$\mathbb{P}^1_{\mathbb{Q}}$	95	w_{95}	$\mathbb{P}^1_{\mathbb{Q}}$	206	w_{206}	$\mathbb{P}^1_{\mathbb{Q}}$
57	w_{57}	$57A_1$	106	w_{106}	$106B_1$	210	w_{210}	$210D_2$
58	w_{29}	$\mathbb{P}^1_{\mathbb{Q}}$	111	w_{111}	$\mathbb{P}^1_{\mathbb{Q}}$	215	w_{215}	$215A_1$
	w_{58}	$58A_1$	118	w_{118}	$118A_1$	314	w_{314}	$314A_1$
62	w_{62}	$\mathbb{P}^1_{\mathbb{Q}}$	119	w_{119}	$\mathbb{P}^1_{\mathbb{Q}}$	330	w_{330}	$330E_2$
65	w_{65}	$65A_1$	122	w_{122}	$122A_1$	390	w_{390}	$390A_2$
69	w_{69}	$\mathbb{P}^1_{\mathbb{Q}}$	129	w_{129}	$129A_1$	510	w_{510}	$510D_2$
74	w_{74}	$\mathbb{P}^1_{\mathbb{Q}}$	134	w_{134}	$\mathbb{P}^1_{\mathbb{Q}}$	546	w_{546}	$546C_2$

v_2' is 4, as Kurihara ([18]) deduced from trace formulae of Brandt matrices. Since there must also be $p + 1 = 4$ edges at the star of any vertex, it turns out that the dual graph $\mathcal{G}$ must be as Figure 1.

Since $3 \mid 210$, $w_{210}(\{v_1, v_2\}) = \{v_1', v_2'\}$ and therefore, $\mathcal{G}/\langle w_{210} \rangle$ is a graph with two vertices joined by two edges, which corresponds to the Kodaira symbol I_2. The only elliptic curve in the $\mathbb{Q}$-isogeny class $210D$ whose reduction type at $p = 3$ is I_2 is $210D2$. Hence, a Weierstrass equation for $V_{210}/\langle w_{210} \rangle$ is $y^2 + xy = x^3 + x^2 - 23x + 33$.

Performing similar computations, we obtain the list of bielliptic Shimura curves (V_D, w) over $\mathbb{Q}$ such that the genus 1 Atkin–Lehner quotient $V_D/\langle w \rangle$ is an elliptic curve with infinitely many rational points. With this procedure, we also give a Weierstrass equation for the elliptic curves $V_D/\langle w \rangle$. Together with the hyperelliptic Shimura curves over $\mathbb{Q}$ given by Ogg, we obtain the family of Shimura curves of genus $g(V_D) \geqslant 2$ with infinitely many quadratic points. Summing up, we obtain the following theorem:

THEOREM 9. *There are only finitely many D for which V_D has infinitely many quadratic points over $\mathbb{Q}$. These curves, together with their rational or elliptic quotients, are listed in Table III above.*

https://doi.org/10.1023/A:1015858710606 Published online by Cambridge University Press

Acknowledgements

I am indebted to Prof. Pilar Bayer for her help and encouragement throughout this study. I also express my gratitude to Prof. Gerald E. Welters for some helpful conversations, to Prof. Jordi Quer for providing me with his algorithm on the decomposition of the Jacobian varieties of modular curves, and to the referee for some useful remarks. Finally, I thank the Tata Institute of Fundamental Research and Mehta Research Institute for their warm hospitality during the fall of 1999.

References

1. Abramovich, D. and Harris, J.: Abelian varieties and curves in $W_d(C)$, *Compositio Math.* **78** (1991), 227–238.
2. Alsina, M.: Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura, Univ. Barcelona PhD. Thesis, 1999.
3. Birch, B. and Kuyk, W.: (eds.), *Modular Functions of One Variable IV*, Lecture Notes in Math. 476, Springer, New York, 1975.
4. Bars, F.: Bielliptic modular curves, *J. Number Theory* **76** (1999), 154–165.
5. Birkenhake, C. and Lange, H.: *Complex Abelian Varieties*, Springer-Verlag, Berlin, 1992.
6. Boutot, J. F. and Carayol, H.: Uniformisation *p*-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld, *Astérisque* **196–197** (1991), 45–158.
7. Buzzard, K.: Integral models of certain Shimura curves, *Duke Math. J.* **87** (1996), 591–612.
8. Čerednik, I. V.: Uniformization of algebraic curves by discrete arithmetic subgroups of $\mathbf{PGL}_2(k_w)$ with compact quotients (in Russian), *Mat. Sb.* **100** (1976), *Math. USSR Sb.* **29** (1976), 55–78.
9. Cremona, J. E.: *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1992.
10. Drinfeld, V. G.: Coverings of *p*-adic symmetric regions (in Russian), *Funktsion Anal. i Prilozn.* **10** (1976), 29–40. Transl. in *Funct. Anal. Appl.* **10** (1976), 107–115.
11. Harris, J. and Silverman, J. H.: Bielliptic curves and symmetric products, *Proc. Amer. Math. Soc.* **112** (1991), 347–356.
12. Jordan, B. W.: On the diophantine arithmetic of Shimura curves, Harvard PhD. Thesis, 1981.
13. Jordan, B. W.: Points on Shimura curves rational over number fields, *J. Reine Angew. Math.* **371** (1986), 92–114.
14. Jordan, B. W. and Livné, R.: Local diophantine properties of Shimura curves, *Math. Ann.* **270** (1985), 235–248.
15. Jordan, B. W. and Livné, R.: On the Néron model of jacobians of Shimura curves, *Compositio Math.* **60** (1986), 227–236.
16. Kamienny, S.: Points on Shimura curves over fields of even degree, *Math. Ann.* **286** (1990), 731–734.
17. Kenku, M. A. and Momose, F.: Automorphisms groups of the modular curves $X_0(N)$, *Compositio Math.* **65** (1988), 51–80.
18. Kurihara, A.: On some examples of equations defining Shimura curves and the Mumford uniformization, *J. Fac. Sci. Univ. Tokyo, Sec. IA* **25** (1979), 277–301.
19. Kuhn, R. M.: Curves of genus 2 with split jacobian, *Trans. Amer. Math. Soc.* **307** (1988), 41–49.
20. Lehner, J. and Newman, M.: Weierstrass points of $\Gamma_0(N)$, *Ann. Math.* **79** (1964), 360–368.

21. Michon, J. F. Courbes de Shimura hyperelliptiques, *Bull. Soc. Math. France* **109** (1981), 217–225.
22. Mori, A.: Power series expansions of modular forms at CM points, *Rend. Sem. Mat. Univ. Pol. Torino* **53** (1995), 361–374.
23. Ogg, A. P.: Hyperelliptic modular curves, *Bull. Soc. Math. France* **102** (1974), 449–462.
24. Ogg, A. P.: Über die Automorphismengruppe von $X_0(N)$, *Math. Ann.* **228** (1977), 279–292.
25. Ogg, A. P.: Real Points on Shimura Curves, *Birkhaüser PM* **35** (1983), 277–307.
26. Ogg, A. P.: Mauvaise réduction des courbes de Shimura, In: *Progr. Math.* 59, Birkhäuser, Basel, 1983/4, pp. 199–217.
27. Ribet, K. A.: Endomorphisms of semi-stable abelian varieties over number fields, *Ann. Math.* **101** (1975), 555–562.
28. Ribet, K. A.: Sur les varietés abéliennes à multiplications réelles, *C.R. Acad. Sc. Paris* **291** (1980), 121–123.
29. Roberts, D.P.: *Shimura curves analogous to* $X_0(N)$, Harvard PhD. Thesis, 1989.
30. Shimura, G.: Construction of class fields and zeta functions of algebraic curves, *Ann. Math.* **85** (1967), 58–15.
31. Shimura, G.: On the real points of an arithmetic quotient of a bounded symmetric domain, *Math. Ann.* **215** (1975), 135–164.
32. Shimura, G. and Taniyama, Y.: Complex multiplication of abelian varieties and its applications to number theory, *Publ. Math. Soc. Japan* **6** (1961).