ACTA ARITHMETICA
164.4 (2014)

An effective bound of p for algebraic points on Shimura curves of $\varGamma_0(p)$-type

by

Keisuke Arai (Tokyo)

1. Introduction. Let B be an indefinite quaternion division algebra over $\mathbb{Q}$ with discriminant d. Fix a maximal order $\mathcal{O}$ of B. A *QM-abelian surface by* $\mathcal{O}$ over a field F is a pair (A, i) where A is an abelian variety over F of dimension 2, and $i : \mathcal{O} \hookrightarrow \mathrm{End}_F(A)$ is an injective ring homomorphism (sending 1 to id) (cf. [6, p. 591]). Here $\mathrm{End}_F(A)$ is the ring of endomorphisms of A defined over F. We assume that A has a left $\mathcal{O}$-action. We will sometimes omit "by $\mathcal{O}$" and simply write "a QM-abelian surface" if there is no risk of confusion. Let M^B be the coarse moduli scheme over $\mathbb{Q}$ parameterizing isomorphism classes of QM-abelian surfaces by $\mathcal{O}$ (cf. [9, p. 93]). Then M^B is a proper smooth curve over $\mathbb{Q}$, called a *Shimura curve*. Throughout this article, let p be a prime number not dividing d. Let $M_0^B(p)$ be the coarse moduli scheme over $\mathbb{Q}$ parameterizing isomorphism classes of triples (A, i, V), where (A, i) is a QM-abelian surface by $\mathcal{O}$ and V is a left $\mathcal{O}$-submodule of $A[p]$ of $\mathbb{F}_p$-dimension 2. Here $A[p]$ is the kernel of multiplication by p in A. Then $M_0^B(p)$ is a proper smooth curve over $\mathbb{Q}$, which we call a *Shimura curve of $\varGamma_0(p)$-type*. We have a natural map

$$\pi^B(p) : M_0^B(p) \to M^B$$

over $\mathbb{Q}$ defined by $(A, i, V) \mapsto (A, i)$.

In previous articles, we showed that for number fields in a certain large class, there are at most elliptic points on $M_0^B(p)$ if p is large enough. In this article, we prove that in fact there are no elliptic points, and obtain an effective bound for such p. The main result is:

Theorem 1.1. *Let k be a finite Galois extension of $\mathbb{Q}$ which does not contain the Hilbert class field of any imaginary quadratic field. Assume*

2010 *Mathematics Subject Classification*: Primary 11G18, 14G05; Secondary 11G10, 11G15.
Key words and phrases: effective bound, rational points, Shimura curves, QM-abelian surfaces.

DOI: 10.4064/aa164-4-2

that there is a prime number q which splits completely in k and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$. Then there is an effectively computable constant $C_0(k)$ depending on k and independent of B such that $M_0^B(p)(k) = \emptyset$ if $p > \max\{4q, C_0(k)\}$, $p \neq 13$.

We can identify $M_0^B(p)(\mathbb{C})$ with a quotient of the upper half-plane, and we use the notion of elliptic points in this context, assuming that k is a subfield of $\mathbb{C}$. The Shimura curve $M_0^B(p)$ is an analogue of the modular curve $X_0(p)$. Points on $X_0(p)$ rational over $\mathbb{Q}$ and quadratic fields are studied in [11], [12] (see [1] for related topics). We can also define a proper smooth curve $M_0^B(p)$ over $\mathbb{Q}$ for $B = \mathrm{M}_2(\mathbb{Q})$ that is isomorphic to $X_0(p)$. But Theorem 1.1 does not apply in this setting because $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$ for any prime q.

In §2–4, we review a part of [3]. In §5–6, we classify the characters associated to QM-abelian surfaces, and show that there are no k-rational points on $M_0^B(p)$ if p ($> 4q$, $\neq 13$) does not belong to an exceptional finite set $\mathcal{N}_1^{\mathrm{new}}(k)$. In §7, we give an upper bound of $\mathcal{N}_1^{\mathrm{new}}(k)$ by the method of [7]. In §8, we give an example of the estimate of p.

Remark 1.2. $M^B(\mathbb{R}) = \emptyset$ (see [13, Theorem 0]), and so $M_0^B(p)(\mathbb{R}) = \emptyset$.

Notation. For a field F, let $\mathrm{char}\, F$ denote the characteristic, $\overline{F}$ an algebraic closure, F^{sep} (resp. F^{ab}) the separable closure (resp. the maximal abelian extension) inside $\overline{F}$, and let $\mathrm{G}_F := \mathrm{Gal}(F^{\mathrm{sep}}/F)$ and $\mathrm{G}_F^{\mathrm{ab}} := \mathrm{Gal}(F^{\mathrm{ab}}/F)$. For a prime number p and a field F with $\mathrm{char}\, F \neq p$, let $\theta_p : \mathrm{G}_F \to \mathbb{F}_p^{\times}$ denote the mod p cyclotomic character.

Let $|\cdot|$ denote the usual complex absolute value on $\mathbb{C}$. For a number field k, let $n_k := [k : \mathbb{Q}]$; fix an inclusion $k \hookrightarrow \mathbb{C}$ and take the algebraic closure $\overline{k}$ inside $\mathbb{C}$; let $\mathcal{O}_k$ denote the ring of integers; let $\mathrm{N}(\mathfrak{q}) := \sharp(\mathcal{O}_k/\mathfrak{q})$ for a prime $\mathfrak{q}$ of k; let d_k denote the absolute value of the discriminant; Cl_k the ideal class group; h_k the class number; r_k the rank of the unit group $\mathcal{O}_k^{\times}$; R_k the regulator; k_v the completion of k at v, where v is a place (or a prime) of k; and $\mathsf{Ram}(k)$ the set of prime numbers which are ramified in k.

2. Galois representations associated to QM-abelian surfaces. We briefly review [3, §2] in order to consider the Galois representations associated to a QM-abelian surface. Let F be a field with $\mathrm{char}\, F \neq p$. Let (A, i) be a QM-abelian surface by $\mathcal{O}$ over F. The action of G_F on $A[p](F^{\mathrm{sep}}) \cong \mathbb{F}_p^4$ determines a representation $\overline{\rho} : \mathrm{G}_F \to \mathrm{GL}_4(\mathbb{F}_p)$. By a suitable choice of basis, $\overline{\rho}$ factors as

$$\overline{\rho} : \mathrm{G}_F \to \left\{ \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix} \,\middle|\, \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \right\} \subseteq \mathrm{GL}_4(\mathbb{F}_p).$$

Let

$$\overline{\rho}_{A,p} : \mathrm{G}_F \to \mathrm{GL}_2(\mathbb{F}_p) \tag{2.1}$$

denote the Galois representation induced from $\overline{\rho}$ by "$\left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right)$", so that

$$\overline{\rho}_{A,p}(\sigma) = \begin{pmatrix} s(\sigma) & t(\sigma) \\ u(\sigma) & v(\sigma) \end{pmatrix} \text{ for any } \sigma \in \mathrm{G}_F \quad \text{if} \quad \overline{\rho}(\sigma) = \begin{pmatrix} s(\sigma)I_2 & t(\sigma)I_2 \\ u(\sigma)I_2 & v(\sigma)I_2 \end{pmatrix}.$$

Suppose $A[p](F^{\mathrm{sep}})$ has a left $\mathcal{O}$-submodule V which has dimension 2 over $\mathbb{F}_p$ and is stable under the action of G_F. Then we may assume that

$$\overline{\rho}_{A,p}(\mathrm{G}_F) \subseteq \left\{ \begin{pmatrix} s & t \\ 0 & v \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_p).$$

Let

$$\lambda : \mathrm{G}_F \to \mathbb{F}_p^\times \tag{2.2}$$

denote the character induced from $\overline{\rho}_{A,p}$ by "s", so that $\overline{\rho}_{A,p}(\sigma) = \left(\begin{smallmatrix} \lambda(\sigma) & * \\ 0 & * \end{smallmatrix}\right)$ for any $\sigma \in \mathrm{G}_F$. Note that G_F acts on V by λ (i.e. $\overline{\rho}(\sigma)(v) = \lambda(\sigma)v$ for any $\sigma \in \mathrm{G}_F$, $v \in V$).

3. Automorphism groups. We give a brief summary of [3, §3] concerning the automorphism groups of a QM-abelian surface. Let (A, i) be a QM-abelian surface by $\mathcal{O}$ over a field F. Let $\mathrm{End}(A)$ (resp. $\mathrm{Aut}(A)$) denote the ring of endomorphisms (resp. the group of automorphisms) of A defined over $\overline{F}$. Define

$$\begin{aligned} \mathrm{End}_{\mathcal{O}}(A) &:= \{f \in \mathrm{End}(A) \mid f \circ i(g) = i(g) \circ f \text{ for any } g \in \mathcal{O}\}, \\ \mathrm{Aut}_{\mathcal{O}}(A) &:= \mathrm{Aut}(A) \cap \mathrm{End}_{\mathcal{O}}(A). \end{aligned}$$

If $\mathrm{char}\, F = 0$, then $\mathrm{Aut}_{\mathcal{O}}(A) \cong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$.

Let (A, i, V) be a triple, where (A, i) is a QM-abelian surface by $\mathcal{O}$ over F and V is a left $\mathcal{O}$-submodule of $A[p](\overline{F})$ of $\mathbb{F}_p$-dimension 2. Define a subgroup $\mathrm{Aut}_{\mathcal{O}}(A, V)$ of $\mathrm{Aut}_{\mathcal{O}}(A)$ by

$$\mathrm{Aut}_{\mathcal{O}}(A, V) := \{f \in \mathrm{Aut}_{\mathcal{O}}(A) \mid f(V) = V\}.$$

Assume $\mathrm{char}\, F = 0$. Then $\mathrm{Aut}_{\mathcal{O}}(A, V) \cong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$. Note that $\mathrm{Aut}_{\mathcal{O}}(A) \cong \mathbb{Z}/2\mathbb{Z}$ (resp. $\mathrm{Aut}_{\mathcal{O}}(A, V) \cong \mathbb{Z}/2\mathbb{Z}$) if and only if $\mathrm{Aut}_{\mathcal{O}}(A) = \{\pm 1\}$ (resp. $\mathrm{Aut}_{\mathcal{O}}(A, V) = \{\pm 1\}$).

4. Fields of definition. From now on, let k be a number field. We recall from [3, §4] some facts about the field of definition of a point of $M_0^B(p)(k)$. Fix a point

$$x \in M_0^B(p)(k).$$

Let $x' \in M^B(k)$ be the image of x by the map $\pi^B(p) : M_0^B(p) \to M^B$. Then x' is represented by a QM-abelian surface (say (A_x, i_x)) over $\overline{k}$, and x is represented by a triple (A_x, i_x, V_x) where V_x is a left $\mathcal{O}$-submodule of $A[p](\overline{k})$ of $\mathbb{F}_p$-dimension 2. For a finite extension M of k, we say that *we can take* (A_x, i_x, V_x) *to be defined over* M if there is a QM-abelian surface (A, i) over M and a G_M-stable left $\mathcal{O}$-submodule V of $A[p](\overline{k})$ with $\dim_{\mathbb{F}_p} V = 2$ such that there is an isomorphism between $(A, i) \otimes_M \overline{k}$ and (A_x, i_x) under which V corresponds to V_x. Let

$$\mathrm{Aut}(x) := \mathrm{Aut}_{\mathcal{O}}(A_x, V_x) \quad \text{and} \quad \mathrm{Aut}(x') := \mathrm{Aut}_{\mathcal{O}}(A_x).$$

Then $\mathrm{Aut}(x)$ is a subgroup of $\mathrm{Aut}(x')$. Note that x is an elliptic point of order 2 (resp. 3) if and only if $\mathrm{Aut}(x) \cong \mathbb{Z}/4\mathbb{Z}$ (resp. $\mathrm{Aut}(x) \cong \mathbb{Z}/6\mathbb{Z}$). Since x is a k-rational point, ${}^{\sigma}x = x$ for any $\sigma \in \mathrm{G}_k$. Then for any $\sigma \in \mathrm{G}_k$, there is an isomorphism

$$\phi_\sigma : {}^{\sigma}(A_x, i_x, V_x) \to (A_x, i_x, V_x),$$

which we fix once for all. For $\sigma, \tau \in \mathrm{G}_k$, let

$$c_x(\sigma, \tau) := \phi_\sigma \circ {}^{\sigma}\phi_\tau \circ \phi_{\sigma\tau}^{-1} \in \mathrm{Aut}(x).$$

Then c_x is a 2-cocycle, and it defines the cohomology class $[c_x]$ in $H^2(\mathrm{G}_k, \mathrm{Aut}(x))$. Here, the action of G_k on $\mathrm{Aut}(x)$ is defined in a natural manner (cf. [3, §4]). For a place v of k, let $[c_x]_v \in H^2(\mathrm{G}_{k_v}, \mathrm{Aut}(x))$ denote the restriction of $[c_x]$ to G_{k_v}.

Proposition 4.1 ([3, Proposition 4.2]).

(1) *Suppose* $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$. *Further, assume* $\mathrm{Aut}(x) \neq \{\pm 1\}$ *or* $\mathrm{Aut}(x') \not\cong \mathbb{Z}/4\mathbb{Z}$. *Then we can take* (A_x, i_x, V_x) *to be defined over* k.
(2) *Assume* $\mathrm{Aut}(x) = \{\pm 1\}$. *Then there is a quadratic extension* K *of* k *such that we can take* (A_x, i_x, V_x) *to be defined over* K.

Lemma 4.2 ([3, Lemma 4.3]). *Let* K *be a quadratic extension of* k. *Assume* $\mathrm{Aut}(x) = \{\pm 1\}$. *Then the following conditions are equivalent:*

(1) *We can take* (A_x, i_x, V_x) *to be defined over* K.
(2) *For any place* v *of* k *satisfying* $[c_x]_v \neq 0$, *the tensor product* $K \otimes_k k_v$ *is a field.*

5. Classification of characters. We keep the notation from Section 4. Throughout this section, we assume $\mathrm{Aut}(x) = \{\pm 1\}$. Let K be a quadratic extension of k which satisfies the equivalent conditions in Lemma 4.2. Then x is represented by a triple (A, i, V), where (A, i) is a QM-abelian surface over K and V is a left $\mathcal{O}$-submodule of $A[p](\overline{k})$ of $\mathbb{F}_p$-dimension 2 which is stable under the action of G_K. Let $\lambda : \mathrm{G}_K \to \mathbb{F}_p^\times$ be the character associated to V in (2.2). Let $\lambda^{\mathrm{ab}} : \mathrm{G}_K^{\mathrm{ab}} \to \mathbb{F}_p^\times$ be the natural map induced from λ. Let

$$\varphi := \lambda^{\mathrm{ab}} \circ \mathrm{tr}_{K/k} : \mathrm{G}_k \to \mathrm{G}_K^{\mathrm{ab}} \to \mathbb{F}_p^\times, \tag{5.1}$$

where $\mathrm{tr}_{K/k} : \mathrm{G}_k \to \mathrm{G}_K^{\mathrm{ab}}$ is the transfer map. Then φ^{12} is unramified at every prime of k not dividing p (see [3, Corollary 5.2]), and so φ^{12} corresponds to a character of the ideal group $\mathfrak{I}_k(p)$ consisting of fractional ideals of k prime to p. By abuse of notation, let φ^{12} also denote the corresponding character of $\mathfrak{I}_k(p)$.

Let us now introduce several sets in a manner similar to [3, §5]. Let $\mathcal{M}^{\mathrm{new}}(k)$ be the set of prime numbers which split completely in k. Note that a prime number in the set $\mathcal{M}$ of [3] does not divide $6h_k$. Let $\mathcal{N}^{\mathrm{new}}(k)$ be the set of primes of k which divide some prime number in $\mathcal{M}^{\mathrm{new}}(k)$. Fix a finite subset $\emptyset \neq \mathcal{S}^{\mathrm{new}}(k) \subseteq \mathcal{N}^{\mathrm{new}}(k)$ which generates Cl_k. For each prime $\mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k)$, fix an element $\alpha_{\mathfrak{q}} \in \mathcal{O}_k \setminus \{0\}$ satisfying

$$\mathfrak{q}^{h_k} = \alpha_{\mathfrak{q}} \mathcal{O}_k. \tag{5.2}$$

For an integer $n \geq 1$, let

$$\mathcal{FR}(n) := \{\beta \in \mathbb{C} \mid \beta^2 + a\beta + n = 0 \text{ for some } a \in \mathbb{Z} \text{ with } |a| \leq 2\sqrt{n}\}.$$

For any element $\beta \in \mathcal{FR}(n)$, we have $|\beta| = \sqrt{n}$. From now to the end of this section, assume that k is Galois over $\mathbb{Q}$. Define

$$\mathcal{E}(k) := \Big\{\varepsilon_0 = \sum_{\sigma \in \mathrm{Gal}(k/\mathbb{Q})} a_\sigma \sigma \in \mathbb{Z}[\mathrm{Gal}(k/\mathbb{Q})] \;\Big|\; a_\sigma \in \{0, 8, 12, 16, 24\}\Big\},$$

$$\begin{aligned}
\mathcal{M}_1^{\mathrm{new}}(k) &:= \{(\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \mid \mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k),\ \varepsilon_0 \in \mathcal{E}(k),\ \beta_{\mathfrak{q}} \in \mathcal{FR}(\mathrm{N}(\mathfrak{q}))\},\\
\mathcal{M}_2^{\mathrm{new}}(k) &:= \{\mathrm{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}(\alpha_{\mathfrak{q}}^{\varepsilon_0} - \beta_{\mathfrak{q}}^{24h_k}) \in \mathbb{Z} \mid (\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \in \mathcal{M}_1^{\mathrm{new}}(k)\} \setminus \{0\},\\
\mathcal{N}_0^{\mathrm{new}}(k) &:= \{\text{prime divisors of some of the integers in } \mathcal{M}_2^{\mathrm{new}}(k)\},\\
\mathcal{T}^{\mathrm{new}}(k) &:= \{\text{prime numbers divisible by some prime in } \mathcal{S}^{\mathrm{new}}(k)\} \cup \{2, 3\},\\
\mathcal{N}_1^{\mathrm{new}}(k) &:= \mathcal{N}_0^{\mathrm{new}}(k) \cup \mathcal{T}^{\mathrm{new}}(k) \cup \mathsf{Ram}(k).
\end{aligned}$$

Note that all the sets $\mathcal{FR}(n)$, $\mathcal{E}(k)$, $\mathcal{M}_1^{\mathrm{new}}(k)$, $\mathcal{M}_2^{\mathrm{new}}(k)$, $\mathcal{N}_0^{\mathrm{new}}(k)$, $\mathcal{T}^{\mathrm{new}}(k)$ and $\mathcal{N}_1^{\mathrm{new}}(k)$ are finite. We have the following classification of φ:

THEOREM 5.1 (cf. [3, Theorem 5.6]). *If $p \notin \mathcal{N}_1^{\mathrm{new}}(k)$, then the character $\varphi : \mathrm{G}_k \to \mathbb{F}_p^\times$ is of one of the following types:*

TYPE 2: $\varphi^{12} = \theta_p^{12}$ *and* $p \equiv 3 \bmod 4$.

TYPE 3: *There is an imaginary quadratic field L such that:*

(a) *The Hilbert class field H_L of L is contained in k.*

(b) *There is a prime $\mathfrak{p}_L$ of L lying over p such that*

$$\varphi^{12}(\mathfrak{a}) \equiv \delta^{24} \bmod \mathfrak{p}_L$$

for any fractional ideal $\mathfrak{a}$ of k prime to p. Here, δ is any element of L such that $\mathrm{Norm}_{k/L}(\mathfrak{a}) = \delta \mathcal{O}_L$.

Proof. It suffices to modify the proof of [3, Theorem 5.6] slightly. By replacing K if necessary, we may assume that every prime $\mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k)$ is ramified in K/k (see Lemma 4.2). Suppose $p \notin \mathcal{T}^{\mathrm{new}}(k) \cup \mathsf{Ram}(k)$. Take any prime $\mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k)$. Let q be the residual characteristic of $\mathfrak{q}$, and let $\mathfrak{q}_K$ be the unique prime of K above $\mathfrak{q}$. Then $p \neq q$. *Without assuming* $q \geq 5$, we know that the abelian surface $A \otimes_K K_{\mathfrak{q}_K}$ over $K_{\mathfrak{q}_K}$ has good reduction over a totally ramified finite extension $M(\mathfrak{q})/K_{\mathfrak{q}_K}$ (see [9, Proposition 3.2]). Choose a prime $\mathfrak{p}$ of k above p. Then $\lambda^{12}(\mathfrak{q}_K) \equiv \beta_{\mathfrak{q}}^{12} \bmod \mathfrak{p}_2$, where $\beta_{\mathfrak{q}}$ is an element of $\mathcal{FR}(q)$ and $\mathfrak{p}_2$, which depends on $\mathfrak{p}$, is a prime of $\mathbb{Q}(\beta_{\mathfrak{q}} \,|\, \mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k))$ above p. We find an element $\varepsilon \in \mathcal{E}(k)$ which satisfies the condition (ii) in [3, Lemma 5.4(2)] and $\varphi^{12}(\gamma\mathcal{O}_k) \equiv \gamma^{\varepsilon} \bmod \mathfrak{p}$ for any $\gamma \in k^{\times}$ prime to p. Suppose $p \notin \mathcal{N}_1^{\mathrm{new}}(k)$. Then for any prime $\mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k)$, we have $\alpha_{\mathfrak{q}}^{\varepsilon} = \beta_{\mathfrak{q}}^{24h_k}$. Choose a prime $\mathfrak{q}_0 \in \mathcal{S}^{\mathrm{new}}(k)$. Applying [3, Lemma 5.5] to $\mathfrak{q}_0$, we see that ε is of type 2 or 3 in the sense of [3].

First, assume that ε is of type 2. For any prime $\mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k)$, we have $\beta_{\mathfrak{q}}^{24h_k} = q^{12h_k}$. We prove $\beta_{\mathfrak{q}}^{24} = q^{12}$ *without assuming* $q \nmid 6h_k$. Write $\beta = \beta_{\mathfrak{q}}$ for simplicity. Let $\overline{\beta}$ be the complex conjugate of β. Since $\beta^{24h_k} = \overline{\beta}^{24h_k}$, we have $\overline{\beta} = \zeta\beta$ for some $\zeta \in \mathbb{C}$ with $\zeta^{24h_k} = 1$. Since

$$\mathbb{Q}(\beta) = \mathbb{Q}(\overline{\beta}) = \mathbb{Q}(\zeta\beta) = \mathbb{Q}(\beta, \zeta) \supseteq \mathbb{Q}(\zeta) \quad \text{and} \quad [\mathbb{Q}(\beta) : \mathbb{Q}] = 2,$$

we have $\zeta^4 = 1$ or $\zeta^6 = 1$. Then $\zeta^{12} = 1$. This implies $\overline{\beta}^{12} = \zeta^{12}\beta^{12} = \beta^{12}$, and so $\beta^{12} \in \mathbb{Q}$. Since $|\beta| = \sqrt{q}$, we have $\beta^{12} = \pm q^6$. Therefore $\beta^{24} = q^{12}$.

Note that the case $\beta^{12} = -q^6$ really occurs (e.g. $q = 2$ and $\beta = 1+\sqrt{-1}$). Then

$$\varphi^{12}(\mathrm{Frob}_{\mathfrak{q}}) = \varphi^{12}(\mathfrak{q}) = \lambda^{24}(\mathfrak{q}_K) \equiv \beta_{\mathfrak{q}}^{24} = q^{12} = \mathrm{N}(\mathfrak{q})^{12} \equiv \theta_p(\mathrm{Frob}_{\mathfrak{q}})^{12} \bmod p,$$

where $\mathrm{Frob}_{\mathfrak{q}} \in \mathrm{G}_k$ is any (arithmetic) Frobenius element at $\mathfrak{q}$. Combining this with $\varphi^{12}(\gamma\mathcal{O}_k) \equiv \mathrm{Norm}_{k/\mathbb{Q}}(\gamma)^{12} \bmod p$ for any $\gamma \in k^{\times}$ prime to p, we conclude that $\varphi^{12} = \theta_p^{12}$.

Next, assume that ε is of type 3 (for $\mathfrak{q}_0$). Then by the same argument as in the proof of [3, Theorem 5.6] we obtain the desired result. ∎

As for λ, we have:

LEMMA 5.2 (cf. [4, Lemma 5.11]). *Suppose that* $p \geq 11$, $p \neq 13$ *and* $p \notin \mathcal{N}_1^{\mathrm{new}}(k)$. *Further, assume that the following conditions hold:*

(a) *Every prime* $\mathfrak{p}$ *of* k *above* p *is inert in* K/k.
(b) *Every prime* $\mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k)$ *is ramified in* K/k.

If φ *is of type* 2, *then we have the following assertions:*

(i) *The character* $\lambda^{12}\theta_p^{-6} : \mathrm{G}_K \to \mathbb{F}_p^{\times}$ *is unramified everywhere.*
(ii) *The map* $\mathrm{Cl}_K \to \mathbb{F}_p^{\times}$ *induced from* $\lambda^{12}\theta_p^{-6}$ *is trivial on* $C_{K/k} := \mathrm{Im}(\mathrm{Cl}_k \to \mathrm{Cl}_K)$, *where* $\mathrm{Cl}_k \to \mathrm{Cl}_K$ *is the map defined by* $[\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_K]$.

Proof. (i) The proof is the same as that of [4, Lemma 5.11(i)].

(ii) We slightly modify the argument in the proof of [4, Lemma 5.11(ii)]. Take any prime $\mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k)$. Let q be the residual characteristic of $\mathfrak{q}$, and let $\mathfrak{q}_K$ be the unique prime of K above $\mathfrak{q}$. Then $\lambda^{12}(\mathfrak{q}_K) \equiv \beta^{12}$ modulo a prime of $\mathbb{Q}(\beta)$ above p, where $\beta \in \mathcal{FR}(q)$ is an element satisfying $\beta^{24h_k} = q^{12h_k}$. Then we have seen in the proof of Theorem 5.1 that $\beta^{24} = q^{12}$. Note that we may not have $\beta = \pm\sqrt{-q}$. Therefore, $\lambda^{12}(\mathfrak{q}\mathcal{O}_K) = \lambda^{12}(\mathfrak{q}_K^2) = \lambda^{24}(\mathfrak{q}_K) \equiv \beta^{24} = q^{12} \equiv \theta_p^{12}(\mathfrak{q}_K) = \theta_p^6(\mathfrak{q}\mathcal{O}_K) \bmod p$, as required. ∎

We have the following lemma with the same proof as in [2–4]:

Lemma 5.3 (cf. [2, Lemma 5.6], [3, Lemma 5.12], [4, 3]). *Suppose that $p \geq 11$, $p \neq 13$, $p \notin \mathcal{N}_1^{\mathrm{new}}(k)$, and that φ is of type 2. Let $q \in \mathcal{M}^{\mathrm{new}}(k)$ be a prime number satisfying $q < p/4$. Then $\left(\frac{q}{p}\right) = -1$ and $q^{(p-1)/2} \equiv -1 \bmod p$. Furthermore, $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$.*

6. Irreducibility of $\overline{\rho}_{A,p}$ and algebraic points on $M_0^B(p)$. Let (A, i) be a QM-abelian surface by $\mathcal{O}$ over k. Assume that the representation

$$\overline{\rho}_{A,p} : \mathrm{G}_k \to \mathrm{GL}_2(\mathbb{F}_p)$$

in (2.1) is reducible. Then there is a 1-dimensional subrepresentation of $\overline{\rho}_{A,p}$, and let ν be its associated character. In this case, there is a left $\mathcal{O}$-submodule V of $A[p](\overline{k})$ satisfying $\dim_{\mathbb{F}_p} V = 2$ on which G_k acts by ν, and so the triple (A, i, V) determines a point $x \in M_0^B(p)(k)$. Take any quadratic extension K of k. Then we have the characters $\lambda : \mathrm{G}_K \to \mathbb{F}_p^\times$ and $\varphi : \mathrm{G}_k \to \mathbb{F}_p^\times$ associated to the triple $(A \otimes_k K, i, V)$. Note that $\varphi = \nu^2$ by the construction of φ.

From now to the end of this section, assume that k is Galois over $\mathbb{Q}$, that k does not contain the Hilbert class field of any imaginary quadratic field, and that there is a prime number $q \in \mathcal{M}^{\mathrm{new}}(k)$ satisfying

$$B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q})).$$

Fix such a q. Then we have the following irreducibility result for $\overline{\rho}_{A,p}$:

Theorem 6.1 (cf. [2, Theorem 6.5]). *If $p > 4q$, $p \neq 13$ and $p \notin \mathcal{N}_1^{\mathrm{new}}(k)$, then the representation $\overline{\rho}_{A,p} : \mathrm{G}_k \to \mathrm{GL}_2(\mathbb{F}_p)$ is irreducible.*

Proof. Assume that $\overline{\rho}_{A,p}$ is reducible. Then the associated character φ is of type 2 in Theorem 5.1, because k does not contain the Hilbert class field of any imaginary quadratic field. By Lemma 5.3, we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$. This contradicts the assumption. ∎

We have the following theorem concerning the algebraic points on $M_0^B(p)$:

Theorem 6.2 (cf. [2, Theorem 1.3]). *If $p > 4q$, $p \neq 13$ and $p \notin \mathcal{N}_1^{\mathrm{new}}(k)$, then $M_0^B(p)(k) = \emptyset$.*

Proof. Suppose $p > 4q$, $p \neq 13$ and $p \notin \mathcal{N}_1^{\mathrm{new}}(k)$. Assume that there is a point $x \in M_0^B(p)(k)$.

(1) Suppose $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$.

(1-i) Assume $\mathrm{Aut}(x) \neq \{\pm 1\}$ or $\mathrm{Aut}(x') \not\cong \mathbb{Z}/4\mathbb{Z}$. Then x is represented by a triple (A, i, V) defined over k by Proposition 4.1(1), and the representation $\overline{\rho}_{A,p}$ is reducible. This contradicts Theorem 6.1.

(1-ii) Assume otherwise (i.e. $\mathrm{Aut}(x) = \{\pm 1\}$ and $\mathrm{Aut}(x') \cong \mathbb{Z}/4\mathbb{Z}$). Then x is represented by a triple (A, i, V) defined over a quadratic extension of k by Proposition 4.1(2), and we have a character $\varphi : \mathrm{G}_k \to \mathbb{F}_p^\times$ as in (5.1). By Theorem 5.1 and Lemma 5.3, we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$, which is a contradiction.

(2) Suppose $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$.

(2-i) Assume $\mathrm{Aut}(x) = \{\pm 1\}$. Then by the same argument as in (1-ii), we have a contradiction.

(2-ii) Assume otherwise. Then x is an elliptic point of order 2 or 3. Let $\mathbb{Q}(x)$ be the number field generated over $\mathbb{Q}$ by the coordinates of x on $M_0^B(p)$. Then $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ by [8, Theorem 5.12], and so $k \supseteq \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. This contradicts the assumption because $\mathbb{Q}(\sqrt{-1})$ (resp. $\mathbb{Q}(\sqrt{-3})$) is the Hilbert class field of itself. ■

7. An estimate of $\mathcal{N}_1^{\mathrm{new}}(k)$. We give an upper bound of the set $\mathcal{N}_1^{\mathrm{new}}(k)$ by the method of [7]. The following theorem and proposition are key ingredients of the estimate:

THEOREM 7.1 ([10, Theorem 1.1]). *There is an absolute, effectively computable constant $A_1 > 1$ such that for every finite extension k_1 of $\mathbb{Q}$, every finite Galois extension k_2 of k_1 and every conjugacy class C of* $\mathrm{Gal}(k_2/k_1)$, *there is a prime $\mathfrak{q}$ of k_1 which is unramified in k_2, for which* $\mathrm{Fr}_{\mathfrak{q}} = C$ *and* $\mathrm{N}(\mathfrak{q})$ *is a prime number satisfying* $\mathrm{N}(\mathfrak{q}) \leq 2d_{k_2}^{A_1}$. *Here,* $\mathrm{Fr}_{\mathfrak{q}}$ *is the* (*arithmetic*) *Frobenius conjugacy class at $\mathfrak{q}$ in* $\mathrm{Gal}(k_2/k_1)$.

PROPOSITION 7.2 ([7, Proposition 4.2]). *Assume that k is Galois over $\mathbb{Q}$. Let A_1 be the constant in Theorem* 7.1. *Then we can take $\mathcal{S}^{\mathrm{new}}(k)$ so that every prime $\mathfrak{q} \in \mathcal{S}^{\mathrm{new}}(k)$ satisfies* $\mathrm{N}(\mathfrak{q}) \leq 2d_k^{A_1 h_k}$.

For a place v of k and an element $\alpha \in k$, define $\|\alpha\|_v$ as follows:

- If v is finite, let $\mathfrak{q}$ be the prime of k corresponding to v, and let $\|\alpha\|_v := \mathrm{N}(\mathfrak{q})^{-\mathrm{ord}_{\mathfrak{q}}(\alpha)}$ where $\mathrm{ord}_{\mathfrak{q}}(\alpha)$ is the order of α at $\mathfrak{q}$. Here, we let $\|\alpha\|_v := 0$ if $\alpha = 0$.
- If v is real, let $\tau : k \hookrightarrow \mathbb{R}$ be the embedding corresponding to v, and let $\|\alpha\|_v := |\tau(\alpha)|$.
- If v is complex, let $\tau : k \hookrightarrow \mathbb{C}$ be one of the embeddings corresponding to v, and let $\|\alpha\|_v := |\tau(\alpha)|^2$.

For an element $\alpha \in k$, let $\mathrm{H}(\alpha)$ denote the absolute height of α defined by

$$\mathrm{H}(\alpha) := \Big(\prod_{v} \max\{1, \|\alpha\|_v\}\Big)^{1/n_k},$$

where v runs through all places of k. We know that there is a positive constant δ_k, depending on k, such that for every non-zero element $\alpha \in k$ that is not a root of unity, $\log \mathrm{H}(\alpha) \geq \delta_k/n_k$ (cf. [5, p. 70]). We can take $\delta_k = \log 2/(r_k+1)$ for $n_k = 1, 2$. Both

$$\delta_k = \frac{1}{53 n_k \log 6 n_k} \quad \text{and} \quad \delta_k = \frac{1}{1201}\left(\frac{\log\log n_k}{\log n_k}\right)^3$$

are appropriate choices for $n_k \geq 3$. Fix such a constant δ_k. Let

$$C_1(k) := r_k^{1+r_k}\delta_k^{1-r_k}/2.$$

Lemma 7.3. *Let $\mathfrak{q}$ be a prime of k. Then there is an element $\alpha'_{\mathfrak{q}} \in \mathcal{O}_k \setminus \{0\}$ which satisfies*

$$\mathfrak{q}^{h_k} = \alpha'_{\mathfrak{q}}\mathcal{O}_k \quad \textit{and} \quad \mathrm{H}(\alpha'_{\mathfrak{q}}) \leq |\mathrm{Norm}_{k/\mathbb{Q}}(\alpha'_{\mathfrak{q}})|^{1/n_k} \exp(C_1(k)R_k).$$

Proof. Take an element $\gamma \in \mathcal{O}_k \setminus \{0\}$ which satisfies $\mathfrak{q}^{h_k} = \gamma\mathcal{O}_k$. Then, by [7, Lemme 3] (or [5, Lemma 2]), there is an element $u \in \mathcal{O}_k^\times$ satisfying

$$\mathrm{H}(u\gamma) \leq |\mathrm{Norm}_{k/\mathbb{Q}}(\gamma)|^{1/n_k} \exp(C_1(k)R_k).$$

If we let $\alpha'_{\mathfrak{q}} = u\gamma$, then $\mathfrak{q}^{h_k} = \alpha'_{\mathfrak{q}}\mathcal{O}_k$ and

$$\begin{aligned}\mathrm{H}(\alpha'_{\mathfrak{q}}) &\leq |\mathrm{Norm}_{k/\mathbb{Q}}(u^{-1}\alpha'_{\mathfrak{q}})|^{1/n_k} \exp(C_1(k)R_k)\\ &= |\mathrm{Norm}_{k/\mathbb{Q}}(\alpha'_{\mathfrak{q}})|^{1/n_k} \exp(C_1(k)R_k).\end{aligned}$$

The last equality holds because $\mathrm{Norm}_{k/\mathbb{Q}}(u^{-1}) \in \mathbb{Z}^\times = \{\pm 1\}$. ∎

Let $C_2(k) := \exp(24 n_k C_1(k) R_k)$. Until the end of this section, assume that k is Galois over $\mathbb{Q}$.

Lemma 7.4. *Under the situation of Lemma 7.3, we have*

$$|(\alpha'_{\mathfrak{q}})^{\varepsilon}| \leq \mathrm{N}(\mathfrak{q})^{24 h_k} C_2(k)$$

for any $\varepsilon \in \mathcal{E}(k)$.

Proof. Let $\varepsilon = \sum_{\sigma \in \mathrm{Gal}(k/\mathbb{Q})} a_\sigma \sigma$. Then

$$\begin{aligned}&|(\alpha'_{\mathfrak{q}})^{\varepsilon}|\\ &= \Big|\prod_{\sigma \in \mathrm{Gal}(k/\mathbb{Q})} (\alpha'_{\mathfrak{q}})^{a_\sigma \sigma}\Big| \leq \Big(\prod_{\sigma \in \mathrm{Gal}(k/\mathbb{Q})} \max\{1, |(\alpha'_{\mathfrak{q}})^{\sigma}|\}\Big)^{24} = \prod_{v \mid \infty} \max\{1, \|\alpha'_{\mathfrak{q}}\|_v\}^{24}\\ &= \mathrm{H}(\alpha'_{\mathfrak{q}})^{24 n_k} \leq |\mathrm{Norm}_{k/\mathbb{Q}}(\alpha'_{\mathfrak{q}})|^{24} \exp(24 n_k C_1(k) R_k) = \mathrm{N}(\mathfrak{q})^{24 h_k} C_2(k).\end{aligned}$$

Note that the third equality holds because $\alpha'_{\mathfrak{q}} \in \mathcal{O}_k$. ∎

For $a > 0$, let $C(k, a) := (a^{24 h_k} C_2(k) + a^{12 h_k})^{2 n_k}$.

Lemma 7.5. *Under the situation of Lemma* 7.3, *we have*

$$|\mathrm{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}((\alpha'_{\mathfrak{q}})^{\varepsilon}-\beta_{\mathfrak{q}}^{24h_k})|\le C(k,\mathrm{N}(\mathfrak{q}))$$

for any $\varepsilon\in\mathcal{E}(k)$ *and* $\beta_{\mathfrak{q}}\in\mathcal{FR}(\mathrm{N}(\mathfrak{q}))$.

Proof. For any $\tau\in\mathrm{Gal}(k(\beta_{\mathfrak{q}})/\mathbb{Q})$, we have

$$|((\alpha'_{\mathfrak{q}})^{\varepsilon}-\beta_{\mathfrak{q}}^{24h_k})^{\tau}|\le|(\alpha'_{\mathfrak{q}})^{\varepsilon\tau}|+|\beta_{\mathfrak{q}}^{24h_k\tau}|\le\mathrm{N}(\mathfrak{q})^{24h_k}C_2(k)+\mathrm{N}(\mathfrak{q})^{12h_k}.$$

Then

$$\begin{aligned}|\mathrm{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}((\alpha'_{\mathfrak{q}})^{\varepsilon}-\beta_{\mathfrak{q}}^{24h_k})|&=\prod_{\tau\in\mathrm{Gal}(k(\beta_{\mathfrak{q}})/\mathbb{Q})}|((\alpha'_{\mathfrak{q}})^{\varepsilon}-\beta_{\mathfrak{q}}^{24h_k})^{\tau}|\\&\le(\mathrm{N}(\mathfrak{q})^{24h_k}C_2(k)+\mathrm{N}(\mathfrak{q})^{12h_k})^{2n_k}=C(k,\mathrm{N}(\mathfrak{q})).\ \blacksquare\end{aligned}$$

Until the end of this section, assume that $\mathcal{S}^{\mathrm{new}}(k)$ satisfies the condition in Proposition 7.2, and take $\alpha_{\mathfrak{q}}$ in (5.2) to be the $\alpha'_{\mathfrak{q}}$ in Lemma 7.3 for any $\mathfrak{q}\in\mathcal{S}^{\mathrm{new}}(k)$.

Lemma 7.6. *For any* $m\in\mathcal{M}_2^{\mathrm{new}}(k)$, *we have* $|m|\le C(k,2d_k^{A_1h_k})$.

Proof. We have $m=\mathrm{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}(\alpha_{\mathfrak{q}}^{\varepsilon}-\beta_{\mathfrak{q}}^{24h_k})$ for some $\mathfrak{q}\in\mathcal{S}^{\mathrm{new}}(k)$, $\varepsilon\in\mathcal{E}(k)$ and $\beta_{\mathfrak{q}}\in\mathcal{FR}(\mathrm{N}(\mathfrak{q}))$. Then we obtain $|m|\le C(k,\mathrm{N}(\mathfrak{q}))\le C(k,2d_k^{A_1h_k})$ by Proposition 7.2 and Lemma 7.5. ■

Finally we obtain an upper bound of $\mathcal{N}_1^{\mathrm{new}}(k)$ as follows:

Theorem 7.7. *For any* $l\in\mathcal{N}_1^{\mathrm{new}}(k)$, *we have* $l\le C(k,2d_k^{A_1h_k})$.

Proof. Let $l\in\mathcal{N}_1^{\mathrm{new}}(k)$. If $l\in\mathcal{N}_0^{\mathrm{new}}(k)$, then $l\le C(k,2d_k^{A_1h_k})$ by Lemma 7.6. If $l\in\mathcal{T}^{\mathrm{new}}(k)$, then $l\le\max\{3,2d_k^{A_1h_k}\}$. If $l\in\mathsf{Ram}(k)$, then $l\le d_k$. Since $A_1>1$, we conclude that $l\le C(k,2d_k^{A_1h_k})$. ■

Now Theorem 1.1 follows from Theorems 6.2 and 7.7. Note that we can take $C_0(k)=C(k,2d_k^{A_1h_k})$.

8. An example. We give an example of the estimate of p as follows:

Proposition 8.1. *Let* $k=\mathbb{Q}(\sqrt{-5})$. *Assume that there is a prime number* $q\in\mathcal{M}^{\mathrm{new}}(k)$ *satisfying* $B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-q})\not\cong\mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$. *Then we have* $M_0^B(p)(k)=\emptyset$ *if* $p>\max\{4q,(3^{48}+3^{24})^4\}$.

Proof. We have $n_k=2$, $h_k=2$, $r_k=0$, $C_1(k)=0$, $C_2(k)=1$ and

$$\mathcal{M}^{\mathrm{new}}(k)=\{l:\text{prime number}\mid l\equiv1,3,7,9\bmod 20\}.$$

Let $\mathfrak{q}=(3,1+\sqrt{-5})\subseteq\mathcal{O}_k$. Note that we do not assume $\mathfrak{q}\,|\,q$ here. Then $\mathrm{N}(\mathfrak{q})=3$ and we can take $\mathcal{S}^{\mathrm{new}}(k)=\{\mathfrak{q}\}$. We have $\mathfrak{q}^2=(2-\sqrt{-5})$. Let $\alpha_{\mathfrak{q}}=\alpha'_{\mathfrak{q}}=2-\sqrt{-5}$. Then $\mathrm{H}(\alpha_{\mathfrak{q}})=3$ and $\mathrm{Norm}_{k/\mathbb{Q}}(\alpha_{\mathfrak{q}})=9$. By Lemma 7.5,

$$|\mathrm{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}((\alpha'_{\mathfrak{q}})^{\varepsilon}-\beta_{\mathfrak{q}}^{24h_k})|\le C(k,3)=(3^{48}+3^{24})^4$$

for any $\varepsilon \in \mathcal{E}(k)$ and $\beta_{\mathfrak{q}} \in \mathcal{FR}(3)$. Then $\max \mathcal{M}_2^{\mathrm{new}}(k) \leq (3^{48} + 3^{24})^4$ and $\max \mathcal{N}_0^{\mathrm{new}}(k) \leq (3^{48} + 3^{24})^4$. Since $\mathcal{T}^{\mathrm{new}}(k) = \{2, 3\}$ and $\mathsf{Ram}(k) = \{2, 5\}$, we conclude that $\max \mathcal{N}_1^{\mathrm{new}}(k) \leq (3^{48} + 3^{24})^4$. Applying Theorem 6.2, we obtain the desired result. ∎

Acknowledgments. The author would like to thank the anonymous referee for helpful comments.

References

[1] K. Arai, *Galois images and modular curves*, in: Proceedings of the Symposium on Algebraic Number Theory and Related Topics, RIMS Kôkyûroku Bessatsu B32, Res. Inst. Math. Sci. (RIMS), Kyoto, 2012, 145–161.

[2] K. Arai, *Algebraic points on Shimura curves of $\Gamma_0(p)$-type (II)*, arXiv:1205.3596v2 (2012).

[3] K. Arai and F. Momose, *Algebraic points on Shimura curves of $\Gamma_0(p)$-type*, J. Reine Angew. Math. 690 (2014), 179–202.

[4] K. Arai and F. Momose, *Errata to "Algebraic points on Shimura curves of $\Gamma_0(p)$-type"*, J. Reine Angew. Math. 690 (2014), 203–205.

[5] Y. Bugeaud and K. Győry, *Bounds for the solutions of unit equations*, Acta Arith. 74 (1996), 67–80.

[6] K. Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. 87 (1997), 591–612.

[7] A. David, *Caractère d'isogénie et critères d'irréductibilité*, arXiv:1103.3892v2 (2012).

[8] J. González and V. Rotger, *Non-elliptic Shimura curves of genus one*, J. Math. Soc. Japan 58 (2006), 927–948.

[9] B. Jordan, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. 371 (1986), 92–114.

[10] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. 54 (1979), 271–296.

[11] B. Mazur, *Rational isogenies of prime degree* (with an appendix by D. Goldfeld), Invent. Math. 44 (1978), 129–162.

[12] F. Momose, *Isogenies of prime degree over number fields*, Compos. Math. 97 (1995), 329–348.

[13] G. Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. 215 (1975), 135–164.

Keisuke Arai
Department of Mathematics
School of Engineering
Tokyo Denki University
5 Senju Asahi-cho
Adachi-ku, Tokyo 120-8551, Japan
E-mail: araik@mail.dendai.ac.jp

Received on 24.1.2013
and in revised form on 2.4.2014 (7327)