RIMS Kôkyûroku Bessatsu
B44 (2013), 185–196

On the Rasmussen-Tamagawa conjecture for QM-abelian surfaces

By

Keisuke ARAI*

Abstract

In a previous article, we proved the Rasmussen-Tamagawa conjecture for QM-abelian surfaces over almost all imaginary quadratic fields. In this article, we generalize the previous work to QM-abelian surfaces over number fields of higher degree. We also give several explicit examples.

§ 1. Introduction

For a number field K and a prime number p, let $\overline{K}$ denote an algebraic closure of K, and let $\widetilde{K}_p$ denote the maximal pro-p extension of $K(\boldsymbol{\mu}_p)$ in $\overline{K}$ which is unramified away from p, where $\boldsymbol{\mu}_p$ is the group of p-th roots of unity in $\overline{K}$. For a number field K, an integer $g \geq 0$ and a prime number p, let $\mathscr{A}(K, g, p)$ denote the set of K-isomorphism classes of abelian varieties A over K, of dimension g, which satisfy

$$K(A[p^\infty]) \subseteq \widetilde{K}_p, \tag{1.1}$$

where $K(A[p^\infty])$ is the subfield of $\overline{K}$ generated over K by the p-power torsion of A. It follows from [16, Theorem 1, p.493] that an abelian variety A over K has good reduction at any prime of K not dividing p if its class belongs to $\mathscr{A}(K, g, p)$, because the extension $K(A[p^\infty])/K(\boldsymbol{\mu}_p)$ is unramified away from p. So we can conclude that $\mathscr{A}(K, g, p)$ is a finite set ([18, 1. Theorem, p.309], cf. [7, Satz 6, p.363]). For fixed K and g, define the set

$$\mathscr{A}(K, g) := \{([A], p) \mid p : \text{prime number}, [A] \in \mathscr{A}(K, g, p)\}.$$

We have the following conjecture concerning finiteness for abelian varieties, which is called the Rasmussen-Tamagawa conjecture ([13, p.2391]):

Received March 31, 2012. Revised November 22, 2012 and December 12, 2012.
2000 Mathematics Subject Classification(s): 11F80, 11G10.
Key Words: QM-abelian surfaces, Galois representations.
*School of Engineering, Tokyo Denki University, Tokyo 120-8551, Japan.
e-mail: araik@mail.dendai.ac.jp

Conjecture 1.1 ([15, Conjecture 1, p.1224])**.**
Let K be a number field, and let $g \geq 0$ be an integer. Then the set $\mathscr{A}(K, g)$ is finite.

For elliptic curves, we have the following result related to Conjecture 1.1 (owing to [10, Theorem 7.1, p.153] and [11, Theorem B, p.330]):

Theorem 1.2 ([15, Theorem 2, p.1224 and Theorem 4, p.1227])**.**
Let K be $\mathbb{Q}$ or a quadratic field which is not an imaginary quadratic field of class number one. Then the set $\mathscr{A}(K, 1)$ is finite.

We are interested in higher dimensional cases, in particular, in the case of QM-abelian surfaces, which are analogous to elliptic curves. Let B be an indefinite quaternion division algebra over $\mathbb{Q}$. Let

$$d = \mathrm{disc}(B)$$

be the discriminant of B. Then $d > 1$ and d is the product of an even number of distinct prime numbers. Choose and fix a maximal order $\mathcal{O}$ of B. If a prime number p does not divide d, fix an isomorphism

$$\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{M}_2(\mathbb{Z}_p)$$

of $\mathbb{Z}_p$-algebras. Now we recall the definition of QM-abelian surfaces.

Definition 1.3 (cf. [6, p.591])**.**
Let S be a scheme over $\mathbb{Q}$. A QM-abelian surface by $\mathcal{O}$ over S is a pair (A, i) where A is an abelian surface over S (i.e. A is an abelian scheme over S of relative dimension 2), and $i : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$ is an injective ring homomorphism (sending 1 to id). Here $\mathrm{End}_S(A)$ is the ring of endomorphisms of A defined over S. 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 fear of confusion.

For a number field K and a prime number p, let $\mathscr{A}(K, 2, p)_B$ be the set of K-isomorphism classes of abelian varieties A over K in $\mathscr{A}(K, 2, p)$ such that there is an injective ring homomorphism $\mathcal{O} \hookrightarrow \mathrm{End}_K(A)$ (sending 1 to id). Let us also define the set

$$\mathscr{A}(K, 2)_B := \{([A], p) \mid p : \text{prime number}, [A] \in \mathscr{A}(K, 2, p)_B\}.$$

Let h_K denote the class number of K. Conjecture 1.1 for QM-abelian surfaces has been partly confirmed.

Theorem 1.4 ([4, Theorem 9.3], cf. [5])**.**
Let K be an imaginary quadratic field with $h_K \geq 2$. Then the set $\mathscr{A}(K, 2)_B$ is finite.

The main result of this article is the following theorem, which is a generalization of Theorem 1.4 to number fields of higher degree.

Theorem 1.5.

Let K be a finite Galois extension of $\mathbb{Q}$ which does not contain the Hilbert class field of any imaginary quadratic field. Assume that there is a prime number q which splits completely in K and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$. Then the set $\mathscr{A}(K,2)_B$ is finite.

In the next section, we prove Theorem 1.5. In §4, we give examples of the main result after recalling needed facts in §3.

Remark.

(1) The condition (1.1) is equivalent to the following assertion (see [15, Lemma 3, p.1225] or [13, Definition 4.1, p.2390]):
The abelian variety A has good reduction outside p, and the group $A[p](\overline{K})$ consisting of p-torsion points of A has a filtration of G_K-modules $\{0\} = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_{2g-1} \subseteq V_{2g} = A[p](\overline{K})$ such that V_i has dimension i for each $1 \leq i \leq 2g$, where G_K is the absolute Galois group of K. Furthermore, for each $1 \leq i \leq 2g$, there is an integer $a_i \in \mathbb{Z}$ such that G_K acts on V_i/V_{i-1} by $gv = \theta_p(g)^{a_i} v$, where $g \in \mathrm{G}_K$, $v \in V_i/V_{i-1}$, and θ_p is the mod p cyclotomic character.

(2) Conjecture 1.1 is equivalent to the following assertion:
There exists a constant $C_{\mathrm{RT}}(K,g) > 0$ depending on K and g such that we have $\mathscr{A}(K,g,p) = \emptyset$ for any prime number $p > C_{\mathrm{RT}}(K,g)$.

(3) The set $\mathscr{A}(K,2,p)_B$ (resp. $\mathscr{A}(K,2)_B$) is a subset of $\mathscr{A}(K,2,p)$ (resp. $\mathscr{A}(K,2)$). If one of the following two conditions is satisfied, we know that the sets $\mathscr{A}(K,2,p)_B$, $\mathscr{A}(K,2)_B$ are empty for a trivial reason: there are no QM-abelian surfaces by $\mathcal{O}$ over K ([17, Theorem 0, p.136], [8, Theorem (1.1), p.93]).
(i) K has a real place.
(ii) $B \otimes_{\mathbb{Q}} K \ncong \mathrm{M}_2(K)$.

(4) Let $\mathcal{QM}$ be the set of isomorphism classes of indefinite quaternion division algebras over $\mathbb{Q}$. Define the set

$$\mathscr{A}(K,2)_{\mathcal{QM}} := \bigcup_{B \in \mathcal{QM}} \mathscr{A}(K,2)_B$$

which is a subset of $\mathscr{A}(K,2)$. We then have the following corollary to Theorem 1.4 (see [4, Corollary 9.5]):
Let K be an imaginary quadratic field with $h_K \geq 2$. Then the set $\mathscr{A}(K,2)_{\mathcal{QM}}$ is finite.

(5) Conjecture 1.1 is solved for any K and g when restricted to semi-stable abelian varieties ([13, Corollary 4.5, p.2392]) or abelian varieties with abelian Galois representations ([14, Theorem 1.2]). See also [2, §6] for a summary.

Notation

For a field k, let $\overline{k}$ denote an algebraic closure of k, let k^{sep} denote the separable closure of k inside $\overline{k}$, and let $\mathrm{G}_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

For an integer $n \geq 1$ and a commutative group (or a commutative group scheme) G, let $G[n]$ denote the kernel of multiplication by n in G.

For a prime number p and an abelian variety A over a field k, let $T_pA := \varprojlim A[p^n](\overline{k})$ be the p-adic Tate module of A, where the inverse limit is taken with respect to multiplication by $p : A[p^{n+1}](\overline{k}) \longrightarrow A[p^n](\overline{k})$.

For a number field K, let $\mathcal{O}_K$ denote the ring of integers of K, let K_v denote the completion of K at v where v is a place (or a prime) of K, and let $\mathbf{Ram}(K)$ denote the set of prime numbers which are ramified in K.

Acknowledgments. The author would like to thank the organizers Noriyuki Suwa, Atsushi Shiho and Kanetomo Sato for giving him an opportunity to talk at the conference. He would also like to thank Noriyuki Suwa and the referee for helpful comments.

§ 2. Galois representations

A QM-abelian surface has a Galois representation which looks like that of an elliptic curve as explained below (cf. [12]). Let k be a field of characteristic 0, and let (A, i) be a QM-abelian surface by $\mathcal{O}$ over k, where $\mathcal{O}$ is a fixed maximal order of B which is an indefinite quaternion division algebra over $\mathbb{Q}$. We consider the Galois representations associated to (A, i). Take a prime number p not dividing $d = \mathrm{disc}(B)$. We then have isomorphisms of $\mathbb{Z}_p$-modules:

$$\mathbb{Z}_p^4 \cong T_pA \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{M}_2(\mathbb{Z}_p).$$

The middle is also an isomorphism of left $\mathcal{O}$-modules; the last is also an isomorphism of $\mathbb{Z}_p$-algebras (which was fixed in §1). We sometimes identify these $\mathbb{Z}_p$-modules. Take a $\mathbb{Z}_p$-basis

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ e_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ e_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

of $\mathrm{M}_2(\mathbb{Z}_p)$. Then the image of the natural map

$$\mathrm{M}_2(\mathbb{Z}_p) \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \mathrm{End}(T_pA) \cong \mathrm{M}_4(\mathbb{Z}_p)$$

lies in $\left\{ \begin{pmatrix} aI_2 & bI_2 \\ cI_2 & dI_2 \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}_p \right\}$, where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The G_k-action on T_pA induces a representation

$$\rho_{A/k,p} : \mathrm{G}_k \longrightarrow \mathrm{Aut}_{\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_pA) \subseteq \mathrm{Aut}(T_pA) \cong \mathrm{GL}_4(\mathbb{Z}_p),$$

where $\mathrm{Aut}_{\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_pA)$ is the group of automorphisms of T_pA commuting with the action of $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p$. The above observation implies

$$\mathrm{Aut}_{\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_pA)=\left\{\begin{pmatrix}X & 0\\ 0 & X\end{pmatrix}\,\middle|\, X\in \mathrm{GL}_2(\mathbb{Z}_p)\right\}\subseteq \mathrm{GL}_4(\mathbb{Z}_p).$$

Then the representation $\rho_{A/k,p}$ factors as

$$\rho_{A/k,p}:\mathrm{G}_k\longrightarrow\left\{\begin{pmatrix}X & 0\\ 0 & X\end{pmatrix}\,\middle|\, X\in \mathrm{GL}_2(\mathbb{Z}_p)\right\}\subseteq \mathrm{GL}_4(\mathbb{Z}_p).$$

Let

$$\rho_{(A,i)/k,p}:\mathrm{G}_k\longrightarrow \mathrm{GL}_2(\mathbb{Z}_p)$$

denote the Galois representation determined by "X", so that we have $\rho_{(A,i)/k,p}(\sigma)=X(\sigma)$ if $\rho_{A/k,p}(\sigma)=\begin{pmatrix}X(\sigma) & 0\\ 0 & X(\sigma)\end{pmatrix}$ for $\sigma\in\mathrm{G}_k$. Let

$$\overline{\rho}_{A/k,p}:\mathrm{G}_k\longrightarrow\mathrm{GL}_4(\mathbb{F}_p)\qquad(\text{resp.}\quad \overline{\rho}_{(A,i)/k,p}:\mathrm{G}_k\longrightarrow\mathrm{GL}_2(\mathbb{F}_p))$$

denote the reduction of $\rho_{A/k,p}$ (resp. $\rho_{(A,i)/k,p}$) modulo p. Note that this construction of $\overline{\rho}_{(A,i)/k,p}$ is slightly different from that in [4, §2], but the resulting representations are the same.

We have the following criterion for Conjecture 1.1 for QM-abelian surfaces.

Lemma 2.1.

Assume that there is a constant $C(B,K)$ depending on B and a number field K such that $\overline{\rho}_{(A,i)/K,p}$ is irreducible for any prime number $p>C(B,K)$ and any QM-abelian surface (A,i) by $\mathcal{O}$ over K. Then the set $\mathscr{A}(K,2)_B$ is finite.

Proof.

Take an element $([A],p)\in\mathscr{A}(K,2)_B$. Since $[A]\in\mathscr{A}(K,2,p)$, we know that $\overline{\rho}_{A/K,p}$ is conjugate to $\begin{pmatrix}*&*&*&*\\0&*&*&*\\0&0&*&*\\0&0&0&*\end{pmatrix}$. By the definition of $\mathscr{A}(K,2)_B$, there is an embedding $i:\mathcal{O}\hookrightarrow\mathrm{End}_K(A)$. Then (A,i) is a QM-abelian surface by $\mathcal{O}$ over K. We have seen that there is a map $X:\mathrm{G}_K\longrightarrow\mathrm{GL}_2(\mathbb{F}_p)$ such that $\overline{\rho}_{A/K,p}(\sigma)=\begin{pmatrix}X(\sigma) & 0\\ 0 & X(\sigma)\end{pmatrix}$ for any $\sigma\in\mathrm{G}_K$. Then there is a matrix $M=\begin{pmatrix}M_1 & M_2\\ M_3 & M_4\end{pmatrix}\in\mathrm{GL}_4(\mathbb{F}_p)$ (where M_1,M_2,M_3,M_4

are 2×2 matrices) such that $M^{-1}\begin{pmatrix} X(\sigma) & 0 \\ 0 & X(\sigma) \end{pmatrix} M \in \left\{ \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \right\}$ for any $\sigma \in \mathrm{G}_K$.

We claim the following.

(C): There is a matrix $H \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $H^{-1}X(\sigma)H \in \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ for any $\sigma \in \mathrm{G}_K$.

Let $M_1 = (\boldsymbol{a}_1\ \boldsymbol{a}_2)$, $M_3 = (\boldsymbol{c}_1\ \boldsymbol{c}_2)$ and $M^{-1}\begin{pmatrix} X(\sigma) & 0 \\ 0 & X(\sigma) \end{pmatrix} M = \begin{pmatrix} s(\sigma) & t(\sigma) & * & * \\ 0 & u(\sigma) & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix}$. Then $X(\sigma)\boldsymbol{a}_1 = s(\sigma)\boldsymbol{a}_1$, $X(\sigma)\boldsymbol{a}_2 = t(\sigma)\boldsymbol{a}_1 + u(\sigma)\boldsymbol{a}_2$, $X(\sigma)\boldsymbol{c}_1 = s(\sigma)\boldsymbol{c}_1$, and $X(\sigma)\boldsymbol{c}_2 = t(\sigma)\boldsymbol{c}_1 + u(\sigma)\boldsymbol{c}_2$ for any $\sigma \in \mathrm{G}_K$. If $\boldsymbol{a}_1 \neq \boldsymbol{0}$, take a vector $\boldsymbol{b} \in \mathbb{F}_p^2$ not contained in the linear subspace $\mathbb{F}_p\boldsymbol{a}_1$ and put $H = (\boldsymbol{a}_1\ \boldsymbol{b})$. Then (C) holds. If $\boldsymbol{a}_1 = \boldsymbol{0}$ and $\boldsymbol{a}_2 \neq \boldsymbol{0}$, then $X(\sigma)\boldsymbol{a}_2 = u(\sigma)\boldsymbol{a}_2$, and so (C) holds. If $\boldsymbol{a}_1 = \boldsymbol{a}_2 = \boldsymbol{0}$, then $\boldsymbol{c}_1 \neq \boldsymbol{0}$ or $\boldsymbol{c}_2 \neq \boldsymbol{0}$ because the matrix $M = \begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix}$ is invertible. Then (C) follows.

In this case $\overline{\rho}_{(A,i)/K,p}$ is reducible, and so $p \leq C(B,K)$. Therefore $\sharp\mathscr{A}(K,2)_B < \infty$. □

Theorem 1.5 is a consequence of the following theorem (Theorem 2.2) together with Lemma 2.1. Before stating this theorem, we need some preparation. For a number field K, let $\mathcal{M}$ be the set of prime numbers q such that q splits completely in K and q does not divide $6h_K$. Let $\mathcal{N}$ be the set of primes $\mathfrak{q}$ of K such that $\mathfrak{q}$ divides some prime number $q \in \mathcal{M}$. Take a finite subset $\emptyset \neq \mathcal{S} \subseteq \mathcal{N}$ such that $\mathcal{S}$ generates the ideal class group of K. For each prime $\mathfrak{q} \in \mathcal{S}$, fix an element $\alpha_{\mathfrak{q}} \in \mathcal{O}_K \setminus \{0\}$ satisfying $\mathfrak{q}^{h_K} = \alpha_{\mathfrak{q}}\mathcal{O}_K$. For a prime number q, put

$$\mathcal{FR}(q) := \left\{ \beta \in \mathbb{C} \;\middle|\; \beta^2 + a\beta + q = 0 \text{ for some integer } a \in \mathbb{Z} \text{ with } |a| \leq 2\sqrt{q} \right\}.$$

For $\mathfrak{q} \in \mathcal{S}$, put $\mathrm{N}(\mathfrak{q}) = \sharp(\mathcal{O}_K/\mathfrak{q})$. Then $\mathrm{N}(\mathfrak{q})$ is a prime number. For a finite Galois extension K of $\mathbb{Q}$, define the sets (cf. [3], [4])
$\mathcal{M}_1'(K) :=$

$$\left\{ (\mathfrak{q}, \varepsilon_0', \beta_{\mathfrak{q}}) \;\middle|\; \mathfrak{q} \in \mathcal{S},\ \varepsilon_0' = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} a_\sigma' \sigma \text{ with } a_\sigma' \in \{0,4,6,8,12\},\ \beta_{\mathfrak{q}} \in \mathcal{FR}(\mathrm{N}(\mathfrak{q})) \right\}$$

(where ε_0' is an element of the group ring $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$),

$\mathcal{M}_2'(K) := \left\{ \mathrm{Norm}_{K(\beta_\mathfrak{q})/\mathbb{Q}}(\alpha_\mathfrak{q}^{\varepsilon_0'} - \beta_\mathfrak{q}^{12h_K}) \in \mathbb{Z} \,\middle|\, (\mathfrak{q}, \varepsilon_0', \beta_\mathfrak{q}) \in \mathcal{M}_1'(K) \right\} \setminus \{0\}$,
$\mathcal{N}_0'(K) := \{\, l : \text{prime number} \mid l \text{ divides some integer } m \in \mathcal{M}_2'(K) \,\}$,
$\mathcal{T}(K) := \{\, l' : \text{prime number} \mid l' \text{ is divisible by some prime } \mathfrak{q}' \in \mathcal{S} \,\} \cup \{2, 3\}$,
and
$\mathcal{N}_1'(K) := \mathcal{N}_0'(K) \cup \mathcal{T}(K) \cup \mathbf{Ram}(K)$.
Note that all the sets, $\mathcal{FR}(q), \mathcal{M}_1'(K)$, $\mathcal{M}_2'(K)$, $\mathcal{N}_0'(K)$, $\mathcal{T}(K)$, and $\mathcal{N}_1'(K)$, are finite.

Theorem 2.2 ([3, Theorem 6.5])**.**
Let K be a finite Galois extension of $\mathbb{Q}$ which does not contain the Hilbert class field of any imaginary quadratic field. Assume that there is a prime number q which splits completely in K and satisfies $B \otimes_\mathbb{Q} \mathbb{Q}(\sqrt{-q}) \ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$. Let $p > 4q$ be a prime number which also satisfies $p \nmid d$ and $p \notin \mathcal{N}_1'(k)$. Then the representation

$$\overline{\rho}_{(A,i)/K,p} : \mathrm{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

is irreducible for any QM-abelian surface (A, i) by $\mathcal{O}$ over K.

§ 3. Points on Shimura curves

Let M^B be the coarse moduli scheme over $\mathbb{Q}$, parameterizing isomorphism classes of QM-abelian surfaces by $\mathcal{O}$. Then M^B is a proper smooth curve over $\mathbb{Q}$, called a Shimura curve. The notation M^B is permissible, although we should write $M^\mathcal{O}$ instead of M^B because, even if we replace $\mathcal{O}$ by another maximal order $\mathcal{O}'$, we have a natural isomorphism $M^\mathcal{O} \cong M^{\mathcal{O}'}$ since $\mathcal{O}$ and $\mathcal{O}'$ are conjugate in B. We discuss points on M^B, and the consequences of this section will be used to provide examples of Theorem 1.5 (see Proposition 4.1 in §4). For real points on M^B, we know the following.

Theorem 3.1 ([17, Theorem 0, p.136])**.**
We have $M^B(\mathbb{R}) = \emptyset$.

The genus of the Shimura curve M^B is 0 if and only if $d \in \{6, 10, 22\}$ ([1, Lemma 3.1, p.168]). The defining equations of such curves are

$$\begin{cases} d = 6 \ : \ x^2 + y^2 + 3 = 0, \\ d = 10 \ : \ x^2 + y^2 + 2 = 0, \\ d = 22 \ : \ x^2 + y^2 + 11 = 0 \end{cases} \tag{3.1}$$

(see [9, Theorem 1-1, p.279]). In these cases, for a field k of characteristic 0, the condition $M^B(k) \neq \emptyset$ implies that the base change $M^B \otimes_\mathbb{Q} k$ is isomorphic to the projective line $\mathbb{P}^1_k$, and so $\sharp M^B(k) = \infty$.

Theorem 3.2 ([8, Theorem (1.1), p.93])**.**
Let k be a field of characteristic 0. A point of $M^B(k)$ can be represented by a QM-abelian surface by $\mathcal{O}$ over k if and only if $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$.

Remark.
For a field k of characteristic 0, note that if $\sharp M^B(k) = \infty$ and $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$, then there are infinitely many $\overline{k}$-isomorphism classes of QM-abelian surfaces (A, i) by $\mathcal{O}$ over k.

Next we quote a recent result concerning algebraic points on Shimura curves of $\Gamma_0(p)$-type, which is related to Theorem 2.2 (but there is no implication from or to that theorem). For a prime number p 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 $A[p]$ with $\mathbb{F}_p$-dimension 2. Then $M_0^B(p)$ is a proper smooth curve over $\mathbb{Q}$, which we call a Shimura curve of $\Gamma_0(p)$-type. We have a natural map $M_0^B(p) \longrightarrow M^B$ over $\mathbb{Q}$ defined by $(A, i, V) \longmapsto (A, i)$. So, Theorem 3.1 implies $M_0^B(p)(\mathbb{R}) = \emptyset$ for any p. For a finite Galois extension K of $\mathbb{Q}$, define the finite sets
$\mathcal{M}_1(K) :=$

$$\left\{ (\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \;\middle|\; \mathfrak{q} \in \mathcal{S},\ \varepsilon_0 = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} a_\sigma \sigma \text{ with } a_\sigma \in \{0, 8, 12, 16, 24\},\ \beta_{\mathfrak{q}} \in \mathcal{FR}(\mathrm{N}(\mathfrak{q})) \right\}$$

(where ε_0 is an element of the group ring $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$),
$\mathcal{M}_2(K) := \left\{ \mathrm{Norm}_{K(\beta_{\mathfrak{q}})/\mathbb{Q}}(\alpha_{\mathfrak{q}}^{\varepsilon_0} - \beta_{\mathfrak{q}}^{24h_K}) \in \mathbb{Z} \;\middle|\; (\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \in \mathcal{M}_1(K) \right\} \setminus \{0\}$,
$\mathcal{N}_0(K) := \{\, l : \text{prime number} \mid l \text{ divides some integer } m \in \mathcal{M}_2(K) \,\}$,
and
$\mathcal{N}_1(K) := \mathcal{N}_0(K) \cup \mathcal{T}(K) \cup \mathbf{Ram}(K)$.
The following theorem is proved by a method similar to the proof of Theorem 2.2 (cf. [11]).

Theorem 3.3 ([3, Theorem 1.4])**.**
Let K be a finite Galois extension of $\mathbb{Q}$ which does not contain the Hilbert class field of any imaginary quadratic field. Assume that there is a prime number q which splits completely in K and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$. Let $p > 4q$ be a prime number which also satisfies $p \neq 13$, $p \nmid d$ and $p \notin \mathcal{N}_1(K) \cup \mathcal{N}_1'(K)$.
(1) If $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$, then $M_0^B(p)(K) = \emptyset$.
(2) If $B \otimes_{\mathbb{Q}} K \ncong \mathrm{M}_2(K)$, then $M_0^B(p)(K) \subseteq \{$elliptic points of order 2 or 3$\}$.

Here an elliptic point of order 2 (resp. 3) is a point whose corresponding triple (A, i, V) (over $\overline{K}$) satisfies $\mathrm{Aut}_{\mathcal{O}}(A, V) \cong \mathbb{Z}/4\mathbb{Z}$ (resp. $\mathbb{Z}/6\mathbb{Z}$), where $\mathrm{Aut}_{\mathcal{O}}(A, V)$ is the

group of automorphisms of A defined over $\overline{K}$ commuting with the action of $\mathcal{O}$ and stabilizing V.

§ 4. Examples

We give several explicit examples of Theorem 1.5 in the following proposition.

Proposition 4.1.
Let $d \in \{6, 10, 22\}$ and $K \in \{\mathbb{Q}(\sqrt{3}, \sqrt{-5}), \mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_{17})\}$. Assume $(d, K) \neq (22, \mathbb{Q}(\zeta_5))$. Then there are infinitely many $\overline{K}$-isomorphism classes of QM-abelian surfaces (A, i) by $\mathcal{O}$ over K, and the set $\mathscr{A}(K, 2)_B$ is finite.

To prove Proposition 4.1, we need the following four lemmas.

Lemma 4.2.
Let K be $\mathbb{Q}(\sqrt{3}, \sqrt{-5})$ (resp. $\mathbb{Q}(\zeta_5)$, resp. $\mathbb{Q}(\zeta_{17})$). Then a prime number q splits completely in K if and only if $q \equiv 1, 23, 47, 49 \bmod 60$ (resp. $q \equiv 1 \bmod 5$, resp. $q \equiv 1 \bmod 17$).

Proof.
A prime number q splits in $\mathbb{Q}(\sqrt{3})$ (resp. $\mathbb{Q}(\sqrt{-5})$) if and only if $q \equiv \pm 1 \bmod 12$ (resp. $q \equiv 1, 3, 7, 9 \bmod 20$). Then the assertion for $\mathbb{Q}(\sqrt{3}, \sqrt{-5})$ follows. The rest of the assertions are trivial.

□

Lemma 4.3.
Let d be 6 (resp. 10, resp. 22). For a prime number q, we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$ if and only if $q \equiv 2, 5, 7, 11, 17, 23 \bmod 24$
(resp. $q \equiv 1, 7, 9, 11, 19, 21, 23, 29, 31, 39 \bmod 40$,
resp. $q \equiv 2, 7, 13, 15, 17, 19, 21, 23, 29, 31, 35, 39, 41, 43, 47, 51, 57, 61, 63, 65, 71, 73, 79, 83, 85, 87$ mod88).

Proof.
For a quadratic field L, we have $B \otimes_{\mathbb{Q}} L \ncong \mathrm{M}_2(L)$ if and only if there is a prime divisor of d which splits in L. The prime number 2 (resp. 3, resp. 5, resp. 11) splits in $\mathbb{Q}(\sqrt{-q})$ if and only if $q \equiv -1 \bmod 8$ (resp. $q \equiv -1 \bmod 3$, resp. $q \equiv \pm 1 \bmod 5$, resp. $q \equiv 2, 6, 7, 8, 10 \bmod 11$). Then we have done.

□

Lemma 4.4.
Let $d \in \{6, 10, 22\}$ and $K \in \{\mathbb{Q}(\sqrt{3}, \sqrt{-5}), \mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_{17})\}$. Assume $(d, K) \neq (22, \mathbb{Q}(\zeta_5))$. Then $\sharp M^B(K) = \infty$.

Proof.

It suffices to show $M^B(K) \neq \emptyset$. Looking at (3.1), it is enough to show $M^B(K_v) \neq \emptyset$ for any place v of K, owing to the Hasse principle. If v is infinite, it is trivial since $K_v = \mathbb{C}$. For $d = 6$ (resp. $d = 10$, resp. $d = 22$) and a prime number p, we have $M^B(\mathbb{Q}_p) = \emptyset$ if and only if $p = 3$ (resp. $p = 2$, resp. $p = 11$). (To show $M^B(\mathbb{Q}_p) \neq \emptyset$, if $p \neq 2$, consider the equations in (3.1) modulo p and use Hensel's lemma; if $p = 2$, find explicit solutions of the equations $(\sqrt{-7})^2 + 2^2 + 3 = 0$ with $\sqrt{-7} \in \mathbb{Q}_2$ and $(\sqrt{-15})^2 + 2^2 + 11 = 0$ with $\sqrt{-15} \in \mathbb{Q}_2$. To show $M^B(\mathbb{Q}_p) = \emptyset$, we use the fact that the equation $x^2 + y^2 + p = 0$ has a solution in $\mathbb{Q}_p$ if and only if $p \equiv 1 \bmod 4$.) For any quadratic extension L of $\mathbb{Q}_p$, we have $M^B(L) \neq \emptyset$. So, for $d = 6$ (resp. $d = 10$, resp. $d = 22$), it suffices to show that K_v contains a quadratic extension of $\mathbb{Q}_3$ (resp. $\mathbb{Q}_2$, resp. $\mathbb{Q}_{11}$) for any place v of K above 3 (resp. 2, resp. 11).

For a prime number p, let $e_p(K)$ (resp. $f_p(K)$, resp. $g_p(K)$) be the ramification index of p in $K/\mathbb{Q}$ (resp. the degree of the residual field extension above p in $K/\mathbb{Q}$, resp. the number of primes of K above p). For

$K = \mathbb{Q}(\sqrt{3}, \sqrt{-5})$ (resp. $\mathbb{Q}(\zeta_5)$, resp. $\mathbb{Q}(\zeta_{17})$), we have

$(e_3(K), f_3(K), g_3(K)) = (2, 1, 2)$ (resp. $(1, 4, 1)$, resp. $(1, 16, 1)$),

$(e_2(K), f_2(K), g_2(K)) = (2, 1, 2)$ (resp. $(1, 4, 1)$, resp. $(1, 8, 2)$),

$(e_{11}(K), f_{11}(K), g_{11}(K)) = (1, 2, 2)$ (resp. $(\mathbf{1}, \mathbf{1}, \mathbf{4})$, resp. $(1, 16, 1)$).

Then K_v contains a quadratic extension of $\mathbb{Q}_3$ (resp. $\mathbb{Q}_2$, resp. $\mathbb{Q}_{11}$) for any place v of K above 3 (resp. 2, resp. 11) unless $K = \mathbb{Q}(\zeta_5)$ and $v|11$. Note that if $K = \mathbb{Q}(\zeta_5)$ and $v|11$, then $K_v = \mathbb{Q}_{11}$. For the proof of the next lemma, we add

$(e_5(K), f_5(K), g_5(K)) = (2, 2, 1)$ (resp. $(4, 1, 1)$, resp. $(1, 16, 1)$).

□

Lemma 4.5.

Let $d \in \{6, 10, 22\}$ *and* $K \in \{\mathbb{Q}(\sqrt{3}, \sqrt{-5}), \mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_{17})\}$. *Assume* $(d, K) \neq (22, \mathbb{Q}(\zeta_5))$. *Then* $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$.

Proof.

It suffices to show $B \otimes_{\mathbb{Q}} K_v \cong \mathrm{M}_2(K_v)$ for any place v of K. It is trivial if v is infinite, or if v is finite and does not divide d. By the computation in the proof of Lemma 4.4, no prime divisor of d splits completely in K unless $(d, K) = (22, \mathbb{Q}(\zeta_5))$. So, if $(d, K) \neq (22, \mathbb{Q}(\zeta_5))$, and if v is finite and divides d, then K_v contains a quadratic extension of $\mathbb{Q}_{p(v)}$, where $p(v)$ is the residual characteristic of v. In such a case, $B \otimes_{\mathbb{Q}} K_v \cong \mathrm{M}_2(K_v)$.

□

(Proof of Proposition 4.1)

The only imaginary quadratic subfields of $\mathbb{Q}(\sqrt{3}, \sqrt{-5})$ are $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{-15})$, which are not of class number one. Since the extension $\mathbb{Q}(\sqrt{3}, \sqrt{-5})/\mathbb{Q}(\sqrt{-5})$ (resp.

$\mathbb{Q}(\sqrt{3},\sqrt{-5})/\mathbb{Q}(\sqrt{-15})$) is ramified over the primes above 3 (resp. 2), the field $\mathbb{Q}(\sqrt{3},\sqrt{-5})$ is not the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$ (resp. $\mathbb{Q}(\sqrt{-15})$). The only quadratic subfield of $\mathbb{Q}(\zeta_5)$ (resp. $\mathbb{Q}(\zeta_{17})$) is $\mathbb{Q}(\sqrt{5})$ (resp. $\mathbb{Q}(\sqrt{17})$). So, none of $\mathbb{Q}(\sqrt{3},\sqrt{-5}), \mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_{17})$ contains the Hilbert class field of any imaginary quadratic field. By Lemmas 4.2 and 4.3, there is a prime number q which splits completely in K and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$. Then Lemma 2.1 and Theorem 2.2 imply $\sharp\mathscr{A}(K,2)_B < \infty$. By the remark in §3, together with Lemmas 4.4 and 4.5, there are infinitely many $\overline{K}$-isomorphism classes of QM-abelian surfaces (A,i) by $\mathcal{O}$ over K.

References

[1] K. Arai, On the Galois images associated to QM-abelian surfaces, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, RIMS Kôkyûroku Bessatsu, **B4** (2007), 165–187.

[2] K. Arai, Galois images and modular curves, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, RIMS Kôkyûroku Bessatsu, **B32**, (2012), 145–161.

[3] K. Arai, Algebraic points on Shimura curves of $\Gamma_0(p)$-type II, preprint, available at the web page (http://arxiv.org/pdf/1205.3596v2.pdf).

[4] K. Arai and F. Momose, Algebraic points on Shimura curves of $\Gamma_0(p)$-type, J. Reine Angew. Math., published online (ahead of print).

[5] K. Arai and F. Momose, Errata to Algebraic points on Shimura curves of $\Gamma_0(p)$-type, J. Reine Angew. Math., published online (ahead of print).

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

[7] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math., **73** (1983), 349–366.

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

[9] A. Kurihara, On some examples of equations defining Shimura curves and the Mumford uniformization, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **25** (1979), 277–300.

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

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

[12] M. Ohta, On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **21** (1974), 299–308.

[13] Y. Ozeki, Non-existence of certain Galois representations with a uniform tame inertia weight, Int. Math. Res. Not. **2011** (2011), 2377–2395.

[14] Y. Ozeki, Non-existence of certain CM abelian varieties with prime power torsion, Tohoku Math. J., **65** (2013), 357–371.

[15] C. Rasmussen and A. Tamagawa, A finiteness conjecture on abelian varieties with constrained prime power torsion, Math. Res. Lett., **15** (2008), 1223–1231.

[16] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math., **88** (1968), 492–517.

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

[18] Y. G. Zarhin, A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction, Invent. Math., **79** (1985), 309–321.