ACTA ARITHMETICA
172.3 (2016)

Non-existence of points rational over number fields on Shimura curves

by

KEISUKE ARAI (Tokyo)

1. Introduction. Let B be an indefinite quaternion division algebra over $\mathbb{Q}$, and $d(B)$ its discriminant. Fix a maximal order $\mathcal{O}$ of B. A *QM-abelian surface with multiplication by* $\mathcal{O}$ over a field F is a pair (A, i) where A is a 2-dimensional abelian variety over F, and $i : \mathcal{O} \hookrightarrow \mathrm{End}_F(A)$ is an injective ring homomorphism satisfying $i(1) = \mathrm{id}$ (cf. [1, 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. Let M^B be the Shimura curve over $\mathbb{Q}$ associated to B, which parameterizes the isomorphism classes of QM-abelian surfaces with multiplication by $\mathcal{O}$ (cf. [2, p. 93]). We know that M^B is a proper smooth curve over $\mathbb{Q}$, and that its isomorphism type over $\mathbb{Q}$ depends only on $d(B)$, but not on the particular choice of B and $\mathcal{O}$.

For an imaginary quadratic field k, the set $M^B(k)$ of k-rational points on M^B is empty under a certain assumption ([2, Theorem 6.3], [4, Theorem 1.1]). We extend this result to the case where k is a number field of higher degree. The method of proof is based on the strategy in [2], and the key is to control the field of definition of the QM-abelian surface corresponding to a k-rational point on M^B. We also give counterexamples to the Hasse principle on M^B over number fields. We will discuss the relevance to the Manin obstruction (cf. [6]) in a forthcoming article.

For a prime number q, let $\mathcal{B}(q)$ be the set of the isomorphism classes of indefinite quaternion division algebras B over $\mathbb{Q}$ such that

$$\begin{cases} B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q})) & \text{if } q \neq 2, \\ B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1})) & \\ \quad \text{and } B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-2}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-2})) & \text{if } q = 2. \end{cases}$$

2010 *Mathematics Subject Classification*: Primary 11G18, 14G05; Secondary 11G10, 11G15.
Key words and phrases: rational points, Shimura curves, QM-abelian surfaces, Hasse principle.
Received 2 February 2015; revised 15 October 2015.
Published online 20 January 2016.

DOI: 10.4064/aa8071-10-2015

For positive integers N and e, let

$$\mathcal{C}(N,e) := \{\alpha^e + \overline{\alpha}^e \in \mathbb{Z} \mid \alpha \in \mathbb{C} \text{ is a root of } T^2 + sT + N \text{ for some } s \in \mathbb{Z},\ s^2 \le 4N\},$$

$$\mathcal{D}(N,e) := \{a, a \pm N^{e/2}, a \pm 2N^{e/2}, a^2 - 3N^e \in \mathbb{R} \mid a \in \mathcal{C}(N,e)\}.$$

Here, $\overline{\alpha}$ is the complex conjugate of α. If e is even, then $\mathcal{D}(N,e) \subseteq \mathbb{Z}$. For a subset $\mathcal{D} \subseteq \mathbb{Z}$, let

$$\mathcal{P}(\mathcal{D}) := \big\{\text{prime divisors of some of the integers in } \mathcal{D} \setminus \{0\}\big\}.$$

For a number field k and a prime $\mathfrak{q}$ of k of residue characteristic q, define:

- $\kappa(\mathfrak{q})$: the residue field of $\mathfrak{q}$,
- $\mathrm{N}_{\mathfrak{q}}$: the cardinality of $\kappa(\mathfrak{q})$,
- $e_{\mathfrak{q}}$: the ramification index of $\mathfrak{q}$ in $k/\mathbb{Q}$,
- $f_{\mathfrak{q}}$: the degree of the extension $\kappa(\mathfrak{q})/\mathbb{F}_q$,
- $\mathcal{S}(k,\mathfrak{q})$: the set of the isomorphism classes of indefinite quaternion division algebras B over $\mathbb{Q}$ such that any prime divisor of $d(B)$ belongs to

$$\begin{cases} \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, e_{\mathfrak{q}})) \cup \{q\} & \text{if } B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k) \text{ and } e_{\mathfrak{q}} \text{ is even},\\ \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2e_{\mathfrak{q}})) \cup \{q\} & \text{if } B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k). \end{cases}$$

Note that $\mathcal{S}(k,\mathfrak{q})$ is a finite set. The main result of this article is:

THEOREM 1.1. *Let k be a number field of even degree, and q a prime number such that*

- *there is a unique prime $\mathfrak{q}$ of k above q,*
- *$f_{\mathfrak{q}}$ is odd (and so $e_{\mathfrak{q}}$ is even), and*
- *$B \in \mathcal{B}(q) \setminus \mathcal{S}(k,\mathfrak{q})$.*

Then $M^B(k) = \emptyset$.

REMARK 1.2. (1) By [5, Theorem 0], we have $M^B(\mathbb{R}) = \emptyset$.

(2) If k is of odd degree, then k has a real place, and so $M^B(k) = \emptyset$.

2. Canonical isogeny characters. In this section, we review canonical isogeny characters associated to QM-abelian surfaces, which were introduced in [2, §4]. Let K be a number field, $\overline{K}$ an algebraic closure of K, $\mathrm{G}_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K, $\mathcal{O}_K$ the ring of integers of K, (A,i) a QM-abelian surface with multiplication by $\mathcal{O}$ over K, and p a prime divisor of $d(B)$. The p-torsion subgroup $A[p](\overline{K})$ of A has exactly one nonzero proper left $\mathcal{O}$-submodule, which we shall denote by C_p. It has order p^2, and is stable under the action of G_K. Let $\mathfrak{P}_{\mathcal{O}} \subseteq \mathcal{O}$ be the unique left ideal of reduced norm $p\mathbb{Z}$. In fact, $\mathfrak{P}_{\mathcal{O}}$ is a two-sided ideal of $\mathcal{O}$. Then C_p is free of rank 1 over $\mathcal{O}/\mathfrak{P}_{\mathcal{O}}$. Fix an isomorphism $\mathcal{O}/\mathfrak{P}_{\mathcal{O}} \cong \mathbb{F}_{p^2}$. The action of G_K

on C_p yields a character

$$\varrho_p : \mathrm{G}_K \to \mathrm{Aut}_{\mathcal{O}}(C_p) \cong \mathbb{F}_{p^2}^\times.$$

Here, $\mathrm{Aut}_{\mathcal{O}}(C_p)$ is the group of $\mathcal{O}$-linear automorphisms of C_p. The character ϱ_p depends on the choice of the isomorphism $\mathcal{O}/\mathfrak{P}_{\mathcal{O}} \cong \mathbb{F}_{p^2}$, but the pair $\{\varrho_p, (\varrho_p)^p\}$ is independent of this choice. Either of the characters $\varrho_p, (\varrho_p)^p$ is called a *canonical isogeny character* at p. We have an induced character

$$\varrho_p^{\mathrm{ab}} : \mathrm{G}_K^{\mathrm{ab}} \to \mathbb{F}_{p^2}^\times,$$

where $\mathrm{G}_K^{\mathrm{ab}}$ is the Galois group of the maximal abelian extension K^{ab}/K.

For a prime $\mathfrak{L}$ of K, let $\mathcal{O}_{K,\mathfrak{L}}$ be the completion of $\mathcal{O}_K$ at $\mathfrak{L}$, and let

$$r_p(\mathfrak{L}) : \mathcal{O}_{K,\mathfrak{L}}^\times \xrightarrow{\omega_{\mathfrak{L}}} \mathrm{G}_K^{\mathrm{ab}} \xrightarrow{\varrho_p^{\mathrm{ab}}} \mathbb{F}_{p^2}^\times.$$

Here, $\omega_{\mathfrak{L}}$ is the Artin map.

Proposition 2.1 ([2, Proposition 4.7(2)]). *If $\mathfrak{L} \nmid p$, then $r_p(\mathfrak{L})^{12} = 1$.*

Fix a prime $\mathfrak{P}$ of K above p. Then we have an isomorphism $\kappa(\mathfrak{P}) \cong \mathbb{F}_{p^{f_{\mathfrak{P}}}}$ of finite fields. Let $t_{\mathfrak{P}} := \gcd(2, f_{\mathfrak{P}}) \in \{1,2\}$.

Proposition 2.2 ([2, Proposition 4.8]).

(1) *There is a unique element $c_{\mathfrak{P}} \in \mathbb{Z}/(p^{t_{\mathfrak{P}}} - 1)\mathbb{Z}$ satisfying $r_p(\mathfrak{P})(u) = \mathrm{Norm}_{\kappa(\mathfrak{P})/\mathbb{F}_{p^{t_{\mathfrak{P}}}}}(\widetilde{u})^{-c_{\mathfrak{P}}}$ for any $u \in \mathcal{O}_{K,\mathfrak{P}}^\times$. Here, $\widetilde{u} \in \kappa(\mathfrak{P})^\times$ is the reduction of u modulo $\mathfrak{P}$.*

(2) $2c_{\mathfrak{P}}/t_{\mathfrak{P}} \equiv e_{\mathfrak{P}} \bmod (p-1)$.

Corollary 2.3. *For any prime number $l \neq p$, we have $r_p(\mathfrak{P})(l^{-1})^2 \equiv l^{e_{\mathfrak{P}} f_{\mathfrak{P}}} \bmod p$.*

Proof. $r_p(\mathfrak{P})(l^{-1})^2 = (\mathrm{Norm}_{\kappa(\mathfrak{P})/\mathbb{F}_{p^{t_{\mathfrak{P}}}}}(l^{-1})^{-c_{\mathfrak{P}}})^2 = \mathrm{Norm}_{\mathbb{F}_{p^{f_{\mathfrak{P}}}}/\mathbb{F}_{p^{t_{\mathfrak{P}}}}}(l)^{2c_{\mathfrak{P}}}$ $\equiv l^{2c_{\mathfrak{P}} f_{\mathfrak{P}}/t_{\mathfrak{P}}} = l^{e_{\mathfrak{P}} f_{\mathfrak{P}}} \bmod p$. ∎

For a prime number l, the action of G_K on the l-adic Tate module $T_l A$ yields a representation

$$R_l : \mathrm{G}_K \to \mathrm{Aut}_{\mathcal{O}}(T_l A) \cong \mathcal{O}_l^\times \subseteq B_l^\times,$$

where $\mathrm{Aut}_{\mathcal{O}}(T_l A)$ is the group of $\mathcal{O}$-linear automorphisms of $T_l A$, and $\mathcal{O}_l = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_l$, $B_l = B \otimes_{\mathbb{Q}} \mathbb{Q}_l$. Let $\mathrm{Nrd}_{B_l/\mathbb{Q}_l}$ be the reduced norm on B_l. Let $\mathfrak{M}$ be a prime of K, and $F_{\mathfrak{M}} \in \mathrm{G}_K$ a Frobenius element at $\mathfrak{M}$. For each $e \geq 1$, there is an integer $a(F_{\mathfrak{M}}^e)$ satisfying

$$\mathrm{Nrd}_{B_l/\mathbb{Q}_l}(T - R_l(F_{\mathfrak{M}}^e)) = T^2 - a(F_{\mathfrak{M}}^e)T + (\mathrm{N}_{\mathfrak{M}})^e \in \mathbb{Z}[T]$$

for any l prime to $\mathfrak{M}$.

Proposition 2.4 ([2, Proposition 5.3]).

(1) $a(F_{\mathfrak{M}}^e)^2 \leq 4(\mathrm{N}_{\mathfrak{M}})^e$ *for any positive integer e.*

(2) *Assume* $\mathfrak{M} \nmid p$. *Then*

$$a(F_{\mathfrak{M}}^e) \equiv \varrho_p(F_{\mathfrak{M}}^e) + (\mathrm{N}_{\mathfrak{M}})^e \varrho_p(F_{\mathfrak{M}}^e)^{-1} \bmod p$$

for any positive integer e.

Let $\alpha_{\mathfrak{M}}, \overline{\alpha}_{\mathfrak{M}} \in \mathbb{C}$ be the roots of $T^2 - a(F_{\mathfrak{M}})T + \mathrm{N}_{\mathfrak{M}}$. Then $\alpha_{\mathfrak{M}} + \overline{\alpha}_{\mathfrak{M}} = a(F_{\mathfrak{M}})$ and $\alpha_{\mathfrak{M}}\overline{\alpha}_{\mathfrak{M}} = \mathrm{N}_{\mathfrak{M}}$. We see that the roots of $T^2 - a(F_{\mathfrak{M}}^e)T + (\mathrm{N}_{\mathfrak{M}})^e$ are $\alpha_{\mathfrak{M}}^e, \overline{\alpha}_{\mathfrak{M}}^e$. Then $\alpha_{\mathfrak{M}}^e + \overline{\alpha}_{\mathfrak{M}}^e = a(F_{\mathfrak{M}}^e)$. We have the following corollary to Proposition 2.4(1):

Corollary 2.5. $a(F_{\mathfrak{M}}^e) \in \mathcal{C}(\mathrm{N}_{\mathfrak{M}}, e)$ *for any positive integer* e.

For later use, we give the following lemma:

Lemma 2.6. *Let* m *be the residue characteristic of* $\mathfrak{M}$. *Then the following conditions are equivalent:*

(i) $m \mid a(F_{\mathfrak{M}})$.
(ii) $m \mid a(F_{\mathfrak{M}}^e)$ *for a positive integer* e.
(iii) $m \mid a(F_{\mathfrak{M}}^e)$ *for any positive integer* e.

Proof. For each $e \geq 1$, there is a polynomial $P_e(S,T) \in \mathbb{Z}[S,T]$ such that $(S+T)^e = S^e + T^e + STP_e(S+T, ST)$. Then $a(F_{\mathfrak{M}})^e = a(F_{\mathfrak{M}}^e) + \mathrm{N}_{\mathfrak{M}} P_e(a(F_{\mathfrak{M}}), \mathrm{N}_{\mathfrak{M}})$. Since $m \mid \mathrm{N}_{\mathfrak{M}}$, we have $m \mid a(F_{\mathfrak{M}})$ if and only if $m \mid a(F_{\mathfrak{M}}^e)$. ∎

3. Proof of the main result. Now we prove Theorem 1.1. Suppose that the assumptions of Theorem 1.1 hold. Assume that there is a point $x \in M^B(k)$. When $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$, let K_0 be a quadratic extension of k satisfying $B \otimes_{\mathbb{Q}} K_0 \cong \mathrm{M}_2(K_0)$. Let

$$K := \begin{cases} k & \text{if } B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k), \\ K_0 & \text{if } B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k). \end{cases}$$

Note that the degree $[K:\mathbb{Q}]$ is even. Then x is represented by a QM-abelian surface (A,i) with multiplication by $\mathcal{O}$ over K (see [2, Theorem 1.1]). Recall that $\mathfrak{q}$ denotes the unique prime of k above q. Since $B \notin \mathcal{S}(k, \mathfrak{q})$, there is a prime divisor p of $d(B)$ such that $p \neq q$ and p does not belong to

$$\begin{cases} \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, e_{\mathfrak{q}})) & \text{if } B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k), \\ \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2e_{\mathfrak{q}})) & \text{if } B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k). \end{cases}$$

Fix such a p, and let $\varrho_p : \mathrm{G}_K \to \mathbb{F}_{p^2}^{\times}$ be a canonical isogeny character at p associated to (A,i).

By Proposition 2.1, the character ϱ_p^{12} is unramified outside p. Hence it can be identified with a character $\mathfrak{I}_K(p) \to \mathbb{F}_{p^2}^{\times}$, where $\mathfrak{I}_K(p)$ is the group of fractional ideals of K prime to p. When $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$, we may assume that $\mathfrak{q}$ is ramified in K/k by replacing K_0 if necessary. In any case, let $\mathfrak{Q}$

be the unique prime of K above $\mathfrak{q}$. Note that $\mathfrak{Q}$ is the unique prime of K above q, and so $q\mathcal{O}_K = \mathfrak{Q}^{e_{\mathfrak{Q}}}$ and $(\mathrm{N}_{\mathfrak{Q}})^{e_{\mathfrak{Q}}} = (q^{f_{\mathfrak{Q}}})^{e_{\mathfrak{Q}}} = q^{[K:\mathbb{Q}]}$. Then by Corollary 2.3, we have

$$\begin{aligned}\varrho_p^{12}(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) &= \varrho_p^{12}(\mathfrak{Q}^{e_{\mathfrak{Q}}}) = \varrho_p^{12}(q\mathcal{O}_K) = \varrho_p^{12}(1,\ldots,1,q,\ldots,q,\ldots)\\ &= \varrho_p^{12}(q^{-1},\ldots,q^{-1},1,\ldots,1,\ldots) = \prod_{\mathfrak{P}\mid p} r_p(\mathfrak{P})^{12}(q^{-1}) \equiv \prod_{\mathfrak{P}\mid p} q^{6e_{\mathfrak{P}}f_{\mathfrak{P}}}\\ &= q^{6[K:\mathbb{Q}]} \bmod p.\end{aligned}$$

Here, $(1,\ldots,1,q,\ldots,q,\ldots)$ (resp. $(q^{-1},\ldots,q^{-1},1,\ldots,1,\ldots)$) is the idèle of K where the components above p are 1 and the others are q (resp. where the components above p are q^{-1} and the others are 1), and $\mathfrak{P}$ runs through the primes of K above p. On the other hand,

$$a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \equiv \varrho_p(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) + (\mathrm{N}_{\mathfrak{Q}})^{e_{\mathfrak{Q}}}\varrho_p(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}})^{-1} = \varrho_p(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) + q^{[K:\mathbb{Q}]}\varrho_p(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}})^{-1} \bmod p$$

by Proposition 2.4(2). Let $\varepsilon := q^{-[K:\mathbb{Q}]/2}\varrho_p(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \in \mathbb{F}_{p^2}^\times$. Then

$$\varepsilon^{12} = 1 \quad\text{and}\quad a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \equiv (\varepsilon+\varepsilon^{-1})q^{[K:\mathbb{Q}]/2} \bmod p.$$

Therefore

$$a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \equiv 0, \pm q^{[K:\mathbb{Q}]/2}, \pm 2q^{[K:\mathbb{Q}]/2} \bmod p \quad\text{or}\quad a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}})^2 \equiv 3q^{[K:\mathbb{Q}]} \bmod p.$$

By Corollary 2.5, we have $a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \in \mathcal{C}(\mathrm{N}_{\mathfrak{Q}}, e_{\mathfrak{Q}})$. Moreover,

$$\mathrm{N}_{\mathfrak{Q}} = \mathrm{N}_{\mathfrak{q}} \quad\text{and}\quad e_{\mathfrak{Q}} = \begin{cases} e_{\mathfrak{q}} & \text{if } B\otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k),\\ 2e_{\mathfrak{q}} & \text{if } B\otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k).\end{cases}$$

Then

$$a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}), a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \pm q^{[K:\mathbb{Q}]/2}, a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \pm 2q^{[K:\mathbb{Q}]/2}, a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}})^2 - 3q^{[K:\mathbb{Q}]} \in \mathcal{D}(\mathrm{N}_{\mathfrak{Q}}, e_{\mathfrak{Q}}).$$

Since $p \notin \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, e_{\mathfrak{Q}}))$, we have

(1) $a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) = 0, \pm q^{[K:\mathbb{Q}]/2}, \pm 2q^{[K:\mathbb{Q}]/2}$, or
(2) $a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}})^2 = 3q^{[K:\mathbb{Q}]}$.

Case (1). In this case, we have $q \mid a(F_{\mathfrak{Q}}^{e_{\mathfrak{Q}}})$. Then $q \mid a(F_{\mathfrak{Q}})$ by Lemma 2.6. Since $f_{\mathfrak{Q}}$ $(= f_{\mathfrak{q}})$ is odd, we obtain $B\otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$ or ($q = 2$ and $B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-1}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1}))$) (see [2, Theorem 2.1, Propositions 2.3 and 5.1(1)]). This contradicts $B \in \mathcal{B}(q)$.

Case (2). In this case, $q = 3$ and $[K:\mathbb{Q}]$ is odd, a contradiction.

Therefore we conclude $M^B(k) = \emptyset$. ∎

4. Counterexamples to the Hasse principle. We have computed the sets $\mathcal{C}(N,e), \mathcal{D}(N,e), \mathcal{P}(\mathcal{D}(N,e))$ in several cases as seen in Table 1. Then we obtain the following counterexamples to the Hasse principle on M^B over number fields:

Table 1. Examples of $\mathcal{P}(\mathcal{D}(N,e))$

(N,e)	$\mathcal{C}(N,e)$	$\mathcal{D}(N,e)$	$\mathcal{P}(\mathcal{D}(N,e))$
$(2,2)$	$0, -3, -4$	$0, \pm1, \pm2, -3, \pm4, -5, -6, -7, -8, -12$	$2, 3, 5, 7$
$(2,4)$	$1, \pm8$	$0, 1, -3, \pm4, 5, -7, \pm8, 9, \pm12, \pm16, -47$	$2, 3, 5, 7, 47$
$(2,6)$	$0, 9, -16$	$0, 1, -7, \pm8, 9, \pm16, 17, -24, 25, -32, 64, -111, -192$	$2, 3, 5, 7, 17, 37$
$(2,8)$	$-31, 32$	$0, 1, -15, 16, -31, 32, -47, 48, -63, 64, 193, 256$	$2, 3, 5, 7, 31, 47, 193$
$(2,10)$	$0, 57, -64$	$0, -7, 25, \pm32, 57, \pm64, 89, -96, 121, -128, 177, 1024, -3072$	$2, 3, 5, 7, 11, 19, 59, 89$
$(2,12)$	$-47, \pm128$	$0, 17, -47, \pm64, 81, -111, \pm128, -175, \pm192, \pm256, 4096, -10079$	$2, 3, 5, 7, 17, 37, 47, 10079$
$(2,14)$	$0, -87, -256$	$0, 41, -87, \pm128, 169, -215, \pm256, -343, -384, -512, 16384, -41583, -49152$	$2, 3, 5, 7, 13, 29, 41, 43, 83, 167$
$(2,16)$	$449, 512$	$0, -63, 193, 256, 449, 512, 705, 768, 961, 1024, 4993, 65536$	$2, 3, 5, 7, 31, 47, 193, 449, 4993$
$(3,2)$	$-2, 3, -5, -6$	$0, 1, -2, \pm3, 4, -5, \pm6, -8, \pm9, -11, -12, -18, -23$	$2, 3, 5, 11, 23$
$(3,4)$	$7, -9, -14, 18$	$0, -2, 4, -5, 7, \pm9, -11, -14, 16, \pm18, -23, 25, \pm27, -32, 36, -47, 81, -162, -194$	$2, 3, 5, 7, 11, 23, 47, 97$
$(3,6)$	$10, 46, -54$	$0, -8, 10, -17, 19, -27, 37, -44, 46, -54, 64, -71, 73, -81, 100, -108, 729, -2087$	$2, 3, 5, 11, 17, 19, 23, 37, 71, 73, 2087$
$(3,8)$	$34, -81, -113, 162$	$0, -32, 34, -47, 49, \pm81, -113, 115, -128, \pm162, -194, 196, \pm243, -275, 324, 6561, -6914, -13122, -18527$	$2, 3, 5, 7, 11, 17, 23, 47, 97, 113, 191, 3457$
$(3,10)$	$243, 475, -482, -486$	$0, 4, -11, 232, -239, \pm243, 475, -482, \pm486, 718, -725, \pm729, 961, -968, -972, 48478, 55177, 59049, -118098$	$2, 3, 5, 11, 19, 23, 29, 31, 239, 241, 359, 2399, 24239$
$(3,12)$	$658, -1358, 1458$	$0, -71, 100, -629, 658, 729, -800, -1358, 1387, 1458, -2087, 2116, 2187, -2816, 2916, 249841, 531441, -1161359$	$2, 3, 5, 7, 11, 17, 19, 23, 37, 47, 71, 73, 97, 433, 577, 1009, 1151, 2087$
$(3,14)$	$2187, 2515, 3022, -4374$	$0, 328, 835, -1352, -1859, \pm2187, 2515, 3022, \pm4374, 4702, 5209, \pm6561, 6889, 7396, -8748, 4782969, -5216423, -8023682, -9565938$	$2, 3, 5, 11, 13, 23, 41, 43, 83, 167, 337, 503, 673, 1511, 2351, 5209, 24023$
$(3,16)$	$-353, -6561, -11966, 13122$	$0, -353, 1156, -5405, 6208, \pm6561, -6914, -11966, 12769, \pm13122, -13475, -18527, \pm19683, -25088, 26244, 14044993, 43046721, -86093442, -129015554$	$2, 3, 5, 7, 11, 17, 23, 31, 47, 97, 113, 191, 193, 353, 383, 2113, 3457, 30529, 36671$

PROPOSITION 4.1.

(1) *Assume* $d(B) = 39$, *and let* $k = \mathbb{Q}(\sqrt{2}, \sqrt{-13})$ *or* $\mathbb{Q}(\sqrt{-2}, \sqrt{-13})$. *Then* $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$, $M^B(k) = \emptyset$ *and* $M^B(k_v) \neq \emptyset$ *for any place* v *of* k. *Here,* k_v *is the completion of* k *at* v.

(2) *Let* L *be the subfield of* $\mathbb{Q}(\zeta_9)$ *satisfying* $[L : \mathbb{Q}] = 3$, *where* ζ_9 *is a primitive* 9*th root of unity. Assume* $(d(B), k) = (62, L(\sqrt{-39}))$ *or* $(86, L(\sqrt{-15}))$. *Then* $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$, $M^B(k) = \emptyset$ *and* $M^B(k_v) \neq \emptyset$ *for any place* v *of* k.

Proof. (1) The prime number 3 (resp. 13) is inert (resp. ramified) in $\mathbb{Q}(\sqrt{-13})$. Thus $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-13}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-13}))$, and so $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$.

Applying Theorem 1.1 with $q = 2$, we obtain $M^B(k) = \emptyset$. In fact, $(e_{\mathfrak{q}}, f_{\mathfrak{q}}) = (4, 1)$ where $\mathfrak{q}$ is the unique prime of k above $q = 2$, and the prime divisor 13 of $d(B)$ does not belong to $\mathcal{P}(\mathcal{D}(2, 4)) \cup \{2\}$ (see Table 1). Since 3 (resp. 13) splits in $\mathbb{Q}(\sqrt{-2})$ (resp. $\mathbb{Q}(\sqrt{-1})$), we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-2}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-2}))$ (resp. $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1}))$).

By [2, p. 94], we have $M^B(\mathbb{Q}(\sqrt{-13})_w) \neq \emptyset$ for any place w of $\mathbb{Q}(\sqrt{-13})$ (cf. [3]). Therefore $M^B(k_v) \neq \emptyset$ for any place v of k.

(2) Assume $(d(B), k) = (62, L(\sqrt{-39}))$ (resp. $(86, L(\sqrt{-15}))$). First, we prove $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$. The prime number 2 splits in k as a product of two distinct primes with inertial degree 3. Then we let v be the place corresponding to one of these primes. By [7, Chapitre II, Théorème 1.3], we have $B \otimes_{\mathbb{Q}} k_v \not\cong \mathrm{M}_2(k_v)$. Therefore $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$.

Applying Theorem 1.1 with $q = 3$, we obtain $M^B(k) = \emptyset$. In fact, $(e_{\mathfrak{q}}, f_{\mathfrak{q}}) = (6, 1)$ where $\mathfrak{q}$ is the unique prime of k above $q = 3$, and the prime divisor 31 (resp. 43) of $d(B)$ does not belong to $\mathcal{P}(\mathcal{D}(3, 12)) \cup \{3\}$. Since 31 (resp. 43) splits in $\mathbb{Q}(\sqrt{-3})$, we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-3}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-3}))$.

By [4, Table 1], we have $M^B(\mathbb{Q}(\sqrt{-39})_w) \neq \emptyset$ (resp. $M^B(\mathbb{Q}(\sqrt{-15})_w) \neq \emptyset$) for any place w of $\mathbb{Q}(\sqrt{-39})$ (resp. $\mathbb{Q}(\sqrt{-15})$). Therefore $M^B(k_v) \neq \emptyset$ for any place v of k. ∎

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

References

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

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

[3] B. Jordan and R. Livné, *Local Diophantine properties of Shimura curves*, Math. Ann. 270 (1985), 235–248.

[4] V. Rotger and C. de Vera-Piquero, *Galois representations over fields of moduli and rational points on Shimura curves*, Canad. J. Math. 66 (2014), 1167–1200.

[5] G. Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. 215 (1975), 135–164.
[6] A. Skorobogatov, *Shimura coverings of Shimura curves and the Manin obstruction*, Math. Res. Lett. 12 (2005), 779–788.
[7] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math. 800, Springer, Berlin, 1980.

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