Nagoya Math. J., **230** (2018), 144–159
DOI 10.1017/nmj.2017.6

RATIONAL POINTS ON SHIMURA CURVES AND THE MANIN OBSTRUCTION

KEISUKE ARAI

Abstract. In a previous article, we proved that Shimura curves have no points rational over number fields under a certain assumption. In this article, we give another criterion of the nonexistence of rational points on Shimura curves and obtain new counterexamples to the Hasse principle for Shimura curves. We also prove that such counterexamples obtained from the above results are accounted for by the Manin obstruction.

§1. Introduction

Let B be an indefinite quaternion division algebra over $\mathbb{Q}$, and $d(B)$ its discriminant. Choose and fix a maximal order $\mathcal{O}$ of B, which is unique up to conjugation. A *QM-abelian surface* by $\mathcal{O}$ over a field K is a pair (A, i), where A is a two-dimensional abelian variety over K and $i : \mathcal{O} \hookrightarrow \mathrm{End}_K(A)$ is an injective ring homomorphism sending 1 to id (cf. [4, p. 591]). Here, $\mathrm{End}_K(A)$ is the ring of endomorphisms of A defined over K. We assume that $\mathcal{O}$ acts on A from the left. Let M^B be the Shimura curve over $\mathbb{Q}$ associated to B, which parameterizes the isomorphism classes of QM-abelian surfaces by $\mathcal{O}$ (cf. [7, p. 93]). Then M^B is a proper smooth curve over $\mathbb{Q}$. Note that its isomorphism class over $\mathbb{Q}$ depends only on $d(B)$.

We study rational points on M^B. By [9, Theorem 0], we have $M^B(\mathbb{R}) = \emptyset$. Let k be a number field. If k has a real place, then $M^B(k) = \emptyset$. We have a natural question: If k has no real place and if $d(B)$ is large enough, does $M^B(k)$ become small? In some cases, $M^B(k)$ is expected to become empty when $d(B)$ grows; in other cases, it might consist of only CM points (in the sense of [6, Definition 5.5]). In this context, Jordan obtained a criterion of the emptiness of $M^B(k)$ when k is imaginary quadratic and $B \otimes_{\mathbb{Q}} k \cong$

Received November 20, 2015. Revised November 22, 2016. Accepted March 2, 2017.
2010 Mathematics subject classification. Primary 11G18, 14G05; Secondary 11G10, 11G15.
This work was supported by JSPS KAKENHI Grant Numbers JP25800025, JP16K17578 and Research Institute for Science and Technology of Tokyo Denki University Grant Number Q16K-06/Japan.

$\mathrm{M}_2(k)$ (see [7, Theorems 6.3 and 6.6]). In the situation of [7, Theorem 6.3], Skorobogatov proved that counterexamples to the Hasse principle for M^B is accounted for by the Manin obstruction in the sense of [10, Section 5.2] (see [11, Theorem 3.1]). Rotger and de Vera-Piquero expanded these results to the case where $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ by using projective Galois representations (see [8, Theorem 1.1]). Note that a point of $M^B(k)$ is represented by a QM-abelian surface by $\mathcal{O}$ over k if and only if $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ (see [7, Theorem 1.1]). So one cannot use the geometry over k to study rational points on M^B over k when $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$. The author gave a criterion of the emptiness of $M^B(k)$ with no restriction on the degree $[k : \mathbb{Q}]$ in a form of expanding the above results, without relevance to the Manin obstruction (see [2, Theorem 1.1]). In this article, we give another criterion of the emptiness of $M^B(k)$ and obtain new counterexamples to the Hasse principle for M^B. We also prove that such counterexamples obtained from these results are accounted for by the Manin obstruction. As for [7, Theorem 6.6], the author expanded the result to the case where $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ by imposing a certain congruent condition on a prime divisor of $d(B)$ (see [1]).

There is an attempt to produce a family of counterexamples to the Hasse principle for Shimura curves. Skorobogatov–Yafaev and Clark obtained some results in this direction (see [12] and [5, Theorems 1, 2 and 3], respectively). The results of this article enable us to produce an explicit infinite family of such counterexamples which are accounted for by the Manin obstruction.

§2. Main results

To state the main results, we give several notations.

- k: a number field;
- $\overline{k}$: an algebraic closure of k;
- $\mathcal{O}_k$: the integer ring of k;
- $\mathbb{A}_k$: the adèle ring of k;
- Cl_k: the ideal class group of k;
- h'_k: the largest order of the elements in Cl_k;
- Ω_k: the set of places of k;
- k_v: the completion of k at $v \in \Omega_k$;
- $\mathrm{Br}(k_v)$: the Brauer group of k_v;
- $\mathrm{Br}(M^B) = H^2_{\text{ét}}(M^B, \mathbb{G}_m)$: the Brauer group of M^B;
- $\mathcal{K}_1(k, B)$: the set of quadratic extensions K of k (contained in $\overline{k}$) such that $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$;

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

- $\mathcal{K}_2(k, B)$: the set of quadratic extensions K of k (contained in $\overline{k}$) such that for any prime divisor p of $d(B)$, any prime $\mathfrak{p}$ of k above p is ramified in K/k.

Note that $\mathcal{K}_2(k, B)$ is contained in $\mathcal{K}_1(k, B)$ (cf. Proof of Lemma 2.2). For positive integers N and e, let

- $\mathcal{C}(N, e) := \{\beta^e + \overline{\beta}^e \in \mathbb{Z} \mid \beta, \overline{\beta} \in \mathbb{C}$ are the roots of $T^2 + sT + N = 0$ for some $s \in \mathbb{Z}, s^2 \leqslant 4N\}$;
- $\mathcal{D}(N, e) := \{a, a \pm N^{e/2}, a \pm 2N^{e/2}, a^2 - 3N^e \in \mathbb{R} \mid a \in \mathcal{C}(N, e)\}$.

If e is even, then $\mathcal{D}(N, e) \subseteq \mathbb{Z}$. For a subset $\mathcal{D} \subseteq \mathbb{Z}$, let

- $\mathcal{P}(\mathcal{D})$: the set of prime divisors of some of the nonzero integers in $\mathcal{D}$.

For a later use, we give:

LEMMA 2.1. *If e is even, then $\mathcal{P}(\mathcal{D}(N, e))$ contains $2, 3$ and every prime divisor of N.*

Proof. Assume that e is even. Let $\beta, \overline{\beta}$ be the roots of $T^2 + N = 0$. Then $\beta^2 = \overline{\beta}^2 = -N$ and $\beta^e = \overline{\beta}^e = (-N)^{e/2}$. Hence $\mathcal{C}(N, e)$ and $\mathcal{D}(N, e)$ contain $\beta^e + \overline{\beta}^e = 2(-N)^{e/2}$. Therefore $\mathcal{P}(\mathcal{D}(N, e))$ contains 2 and every prime divisor of N.

In the following, we prove $3 \in \mathcal{P}(\mathcal{D}(N, e))$.

[Case $3 \mid N$]. It has already been proved.

[Case $3 \nmid N$]. Let $a := 2(-N)^{e/2}$. Then $a \in \mathcal{C}(N, e)$ and $a \not\equiv 0 \bmod 3$.

(i) Case $a \equiv 1 \bmod 3$. First, assume $N^{e/2} \equiv 1 \bmod 3$. Then $a - N^{e/2}, a + 2N^{e/2} \equiv 0 \bmod 3$. Since $\mathcal{D}(N, e)$ contains two distinct elements $a - N^{e/2}, a + 2N^{e/2}$, we have $3 \in \mathcal{P}(\mathcal{D}(N, e))$. Next, assume $N^{e/2} \equiv 2 \bmod 3$. Then $a + N^{e/2}, a - 2N^{e/2} \equiv 0 \bmod 3$. Since $a + N^{e/2}, a - 2N^{e/2} \in \mathcal{D}(N, e)$, we have $3 \in \mathcal{P}(\mathcal{D}(N, e))$.

(ii) Case $a \equiv 2 \bmod 3$. If $N^{e/2} \equiv 1 \bmod 3$, then $a + N^{e/2}, a - 2N^{e/2} \equiv 0 \bmod 3$ and $a + N^{e/2}, a - 2N^{e/2} \in \mathcal{D}(N, e)$. If $N^{e/2} \equiv 2 \bmod 3$, then $a - N^{e/2}, a + 2N^{e/2} \equiv 0 \bmod 3$ and $a - N^{e/2}, a + 2N^{e/2} \in \mathcal{D}(N, e)$. □

For a prime number q and a prime $\mathfrak{q}$ of k above q, let

- $k_{\mathfrak{q}}$: the completion of k at $\mathfrak{q}$;
- $\kappa(\mathfrak{q})$: the residue field of $\mathfrak{q}$;
- $\mathrm{N}_{\mathfrak{q}}$: the cardinality of $\kappa(\mathfrak{q})$;

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

- $e_{\mathfrak{q}}$: the ramification index of $\mathfrak{q}$ in $k/\mathbb{Q}$;
- $f_{\mathfrak{q}}$: the degree of the extension $\kappa(\mathfrak{q})/\mathbb{F}_q$;
- $\mathcal{B}(q)$: the set of the isomorphism classes of indefinite quaternion division algebras B over $\mathbb{Q}$ such that

$$\begin{cases} B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q})) & \text{if } q \neq 2, \\ B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1}) \ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1})) \text{ and} & \\ \quad B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-2}) \ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-2})) & \text{if } q = 2; \end{cases}$$

- $\mathcal{S}(k, \mathfrak{q})$: the set of the isomorphism classes of indefinite quaternion division algebras B over $\mathbb{Q}$ such that every prime divisor of $d(B)$ belongs to

$$\begin{cases} \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, e_{\mathfrak{q}})) & \text{if } B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k) \text{ and } e_{\mathfrak{q}} \text{ is even}, \\ \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2e_{\mathfrak{q}})) & \text{if } B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k); \end{cases}$$

- $\mathcal{K}(k, \mathfrak{q})$: the set of quadratic extensions K of k (contained in $\overline{k}$) such that $\mathfrak{q}$ is ramified in K/k.

Note that $\mathcal{S}(k, \mathfrak{q})$ is a finite set, while $\mathcal{K}_2(k, B) \cap \mathcal{K}(k, \mathfrak{q})$ is an infinite set (cf. [3, Remark 4.4]). We have the following criterion of $B \in \mathcal{B}(q)$.

LEMMA 2.2.

(1) *Assume $q \neq 2$. Then $B \in \mathcal{B}(q)$ if and only if there is a prime divisor of $d(B)$ which splits in $\mathbb{Q}(\sqrt{-q})$.*
(2) *We have $B \in \mathcal{B}(2)$ if and only if there are prime divisors p_1, p_2 of $d(B)$ satisfying $p_1 \equiv 1 \bmod 4$ and $p_2 \equiv 1, 3 \bmod 8$. Here, the case where $p_1 = p_2$ is allowed.*

Proof. By the Hasse principle, we have $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ if and only if $B \otimes_{\mathbb{Q}} k_v \cong \mathrm{M}_2(k_v)$ for any $v \in \Omega_k$ (see [13, Propriété I in p. 74]). Let l be a prime number and D_l the quaternion division algebra over $\mathbb{Q}_l$. If L is a quadratic extension of $\mathbb{Q}_l$, then $D_l \otimes_{\mathbb{Q}_l} L \cong \mathrm{M}_2(L)$ (see [13, Théorème 1.3 in Chapitre II]). Therefore (1) follows.

We see that l splits in $\mathbb{Q}(\sqrt{-1})$ (resp. $\mathbb{Q}(\sqrt{-2})$) if and only if $l \equiv 1 \bmod 4$ (resp. $l \equiv 1, 3 \bmod 8$). Then (2) follows. □

Note that $\mathcal{B}(q)$ is an infinite set for any q. Since M^B is proper over $\mathbb{Q}$, we have $M^B(\mathbb{A}_k) = \prod_{v \in \Omega_k} M^B(k_v)$. Define a pairing

$$(\ ,\ ) : \mathrm{Br}(M^B) \times M^B(\mathbb{A}_k) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

by $(c, \{x_v\}_{v\in\Omega_k}) = \sum_{v\in\Omega_k} \mathrm{inv}_v(x_v^* c)$. Here, $\mathrm{inv}_v : \mathrm{Br}(k_v) \longrightarrow \mathbb{Q}/\mathbb{Z}$ is the local invariant at v, and $x_v^* : \mathrm{Br}(M^B) \longrightarrow \mathrm{Br}(k_v)$ is the map associated to $x_v : \mathrm{Spec}(k_v) \longrightarrow M^B$. In this sum, we have $\mathrm{inv}_v(x_v^* c) = 0$ for all but finitely many $v \in \Omega_k$. Let $M^B(\mathbb{A}_k)^{\mathrm{Br}}$ be the right kernel of this pairing. Then $M^B(k) \subseteq M^B(\mathbb{A}_k)^{\mathrm{Br}} \subseteq M^B(\mathbb{A}_k)$ (see [10, Section 5.2]). The main results of this article are:

THEOREM 2.3. *Assume that $k/\mathbb{Q}$ has even degree. Let q be 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);*
- *$B \in \mathcal{B}(q) \setminus \mathcal{S}(k, \mathfrak{q})$.*

Then $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$.

THEOREM 2.4. *Let p, q be distinct prime numbers, and let $\mathfrak{q}$ be a prime of k above q. Assume that*

- *$f_{\mathfrak{p}}$ is odd for any prime $\mathfrak{p}$ of k above p;*
- *$f_{\mathfrak{q}}$ is odd;*
- *$B \in \mathcal{B}(q)$;*
- *$p \mid d(B)$;*
- *$p \notin \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2h'_k))$.*

Then $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$.

REMARK 2.5.

(1) If $k/\mathbb{Q}$ has odd degree, then k has a real place, and so $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = M^B(\mathbb{A}_k) = \emptyset$.
(2) In [2], we proved only $M^B(k) = \emptyset$ in the setting of Theorem 2.3.
(3) Theorem 2.3 for imaginary quadratic fields was proved in [7, Theorem 6.3], [8, Theorem 1.1], [11, Theorem 3.1].

From these theorems, we obtain the following counterexamples to the Hasse principle for Shimura curves, which are accounted for by the Manin obstruction. Especially, we obtain an infinite family of such counterexamples.

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

PROPOSITION 2.6.

(1) *Let $n \in \mathbb{Z}$ be an odd integer. Assume that n is square free and that $(d(B), k) = (39, \mathbb{Q}(\sqrt{2n}, \sqrt{-13}))$. Then $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$, $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ and $M^B(\mathbb{A}_k) \neq \emptyset$.*

(2) *Assume $(d(B), k) = (39, \mathbb{Q}(\sqrt{3}, \sqrt{-13}))$ or $(39, \mathbb{Q}(\sqrt{17}, \sqrt{-13}))$. Then $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$, $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ and $M^B(\mathbb{A}_k) \neq \emptyset$.*

(3) *Let L be the subfield of $\mathbb{Q}(\zeta_9)$ satisfying $[L : \mathbb{Q}] = 3$, where ζ_9 is a primitive 9th root of unity. Assume $(d(B), k) = (62, L(\sqrt{-39}))$ or $(86, L(\sqrt{-15}))$. Then $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$, $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ and $M^B(\mathbb{A}_k) \neq \emptyset$.*

(4) *Assume $(d(B), k) = (122, \mathbb{Q}(\sqrt{-39}, \sqrt{-183}))$. Then $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$, $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ and $M^B(\mathbb{A}_k) \neq \emptyset$.*

In Sections 3–4, we review the classification of characters associated to QM-abelian surfaces, which plays a key role in the proof. In Section 5 (resp. Section 6), we prove Theorem 2.4 (resp. Theorem 2.3). In Section 7, we deduce Proposition 2.6(1)(3) (resp. Proposition 2.6(2)(4)) from Theorem 2.3 (resp. Theorem 2.4). Note that we cannot apply Theorem 2.3 to $k = \mathbb{Q}(\sqrt{3}, \sqrt{-13})$, $\mathbb{Q}(\sqrt{17}, \sqrt{-13})$ or $\mathbb{Q}(\sqrt{-39}, \sqrt{-183})$, because no prime number q is totally ramified in these fields.

§3. Canonical isogeny characters

We review canonical isogeny characters associated to QM-abelian surfaces, which were introduced in [7, Section 4]. Let K be a field of characteristic 0 possessing an algebraic closure $\overline{K}$, (A, i) a QM-abelian surface 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. Then C_p has order p^2, and is called the *canonical torsion subgroup* of (A, i) of reduced order p; it is stable under the action of the Galois group $\mathrm{G}_K = \mathrm{Gal}(\overline{K}/K)$. 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

$$\varrho_p = \varrho_{(A,i,p)} : \mathrm{G}_K \longrightarrow \mathrm{Aut}_{\mathcal{O}}(C_p) \cong \mathbb{F}_{p^2}^{\times},$$

where $\mathrm{Aut}_{\mathcal{O}}(C_p)$ 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

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

the pair $\{\varrho_p, (\varrho_p)^p\}$ does not depend on this choice. Either of the characters $\varrho_p, (\varrho_p)^p$ is called a *canonical isogeny character* at p.

Let $\widehat{\mathbb{Z}}$ be the profinite completion of $\mathbb{Z}$, and let

$$D_p := \{a \in \mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} \mid a \equiv 1 \bmod \mathfrak{P}_{\mathcal{O}}\}.$$

Let M_p^B be the Shimura curve over $\mathbb{Q}$ associated to D_p. Then it parameterizes the isomorphism classes of triples (A, i, c), where (A, i) is a QM-abelian surface by $\mathcal{O}$ and c is a generator of its canonical torsion subgroup C_p as an $\mathcal{O}$-module. Note that the curve M_p^B over $\mathbb{Q}$ is not geometrically connected if $p \neq 2$ (see [11, p. 780] for details). The map $(A, i, c) \longmapsto (A, i)$ defines a covering $M_p^B \longrightarrow M^B$ (over $\mathbb{Q}$) whose automorphism group $\mathrm{Aut}(M_p^B/M^B)$ is isomorphic to

$$\mathbb{F}_{p^2}^{\times}/\{\pm 1\} \cong \begin{cases} \mathbb{Z}/\dfrac{p^2-1}{2}\mathbb{Z} & \text{if } p \neq 2, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } p = 2. \end{cases}$$

If $p \geqslant 5$, then $\mathbb{F}_{p^2}^{\times}/\{\pm 1\}$ has a unique subgroup $C(6)$ which is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. The quotient of M_p^B by $C(6)$ defines an unramified subcovering

$$f_p^B : Y_p^B \longrightarrow M^B,$$

which is an M^B-torsor under the constant group scheme $(\mathbb{F}_{p^2}^{\times})^{12} \cong \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$ (see [11, Corollary 1.2]). Let $x \in M^B(K)$. Then the action of G_K on the fiber of f_p^B at x yields a character

$$\phi_x : \mathrm{G}_K \longrightarrow (\mathbb{F}_{p^2}^{\times})^{12}.$$

LEMMA 3.1. [11, Lemma 2.1] *Assume $p \geqslant 5$. If x is represented by a QM-abelian surface (A, i) by $\mathcal{O}$ over K, then $\varrho_{(A,i,p)}^{12} = \phi_x$.*

§4. Classification of characters

We review the classification of characters associated to QM-abelian surfaces over local fields of characteristic 0. Let m be a prime number, M a finite extension of $\mathbb{Q}_m$, and $\mathfrak{M}$ (resp. $\kappa(M)$) the maximal ideal (resp. the residue field) of M. For a QM-abelian surface (A, i) by $\mathcal{O}$ over M, fix a canonical isogeny character $\varrho_p = \varrho_{(A,i,p)} : \mathrm{G}_M \longrightarrow \mathbb{F}_{p^2}^{\times}$, where p is a prime divisor of $d(B)$. Let $\mathrm{G}_M^{\mathrm{ab}}$ be the Galois group of the maximal abelian

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

extension M^{ab}/M. Then we have an induced character $\varrho_p^{\mathrm{ab}} : \mathrm{G}_M^{\mathrm{ab}} \longrightarrow \mathbb{F}_{p^2}^{\times}$. Let $\omega_M : \mathcal{O}_M^{\times} \longrightarrow \mathrm{G}_M^{\mathrm{ab}}$ be the Artin map, and let

$$r_{(A,i,p)} := \varrho_p^{\mathrm{ab}} \circ \omega_M : \mathcal{O}_M^{\times} \longrightarrow \mathbb{F}_{p^2}^{\times}.$$

In this local setting, we have:

PROPOSITION 4.1. [7, Proposition 4.7(2)] *If $m \neq p$, then $r_{(A,i,p)}^{12} = 1$.*

Let e_M (resp. f_M) be the ramification index of $M/\mathbb{Q}_m$ (resp. the degree of the residue field extension $\kappa(M)/\mathbb{F}_m$). Let $\mathrm{N}_M := m^{f_M}$, $t_M := \gcd(2, f_M) \in \{1, 2\}$.

PROPOSITION 4.2. [7, Proposition 4.8] *Assume $m = p$. Then there is a unique element $c \in \mathbb{Z}/(p^{t_M} - 1)\mathbb{Z}$ satisfying*

$$r_{(A,i,p)}(u) = \mathrm{Norm}_{\kappa(M)/\mathbb{F}_{p^{t_M}}}(\widetilde{u})^{-c}$$

for any $u \in \mathcal{O}_M^{\times}$, where $\widetilde{u} \in \kappa(M)^{\times}$ is the reduction of u modulo $\mathfrak{M}$. Furthermore, we have

$$\frac{2c}{t_M} \equiv e_M \bmod (p-1).$$

Let l be a prime number, $T_l A$ the l-adic Tate module of A, and $\mathrm{Aut}_{\mathcal{O}}(T_l A)$ the group of $\mathbb{Z}_l$-linear automorphisms of $T_l A$ commuting with the action of $\mathcal{O}$. Let $\mathcal{O}_l := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_l$, $B_l := B \otimes_{\mathbb{Q}} \mathbb{Q}_l$, and fix an isomorphism $\mathrm{Aut}_{\mathcal{O}}(T_l A) \cong \mathcal{O}_l^{\times}$. Let

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

be the representation determined by the action of G_M on $T_l A$. Let $\mathrm{Trd}_{B_l/\mathbb{Q}_l}$ (resp. $\mathrm{Nrd}_{B_l/\mathbb{Q}_l}$) be the reduced trace (resp. the reduced norm) on B_l, and $\mathrm{Fr} \in \mathrm{G}_M$ a Frobenius element. For each positive integer e, let $a_l(\mathrm{Fr}^e) := \mathrm{Trd}_{B_l/\mathbb{Q}_l}(R_l(\mathrm{Fr}^e))$. If $l \neq m$, then $a_l(\mathrm{Fr}^e) \in \mathbb{Z}$ and it does not depend on l. We shall denote it by $a(\mathrm{Fr}^e)$. Then

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

if $l \neq m$.

PROPOSITION 4.3. [7, Proposition 5.3]

(1) $a(\mathrm{Fr}^e) \in \mathcal{C}(\mathrm{N}_M, e)$ *for any $e \geqslant 1$.*
(2) *If $m \neq p$, then*

$$a(\mathrm{Fr}^e) \equiv \varrho_p(\mathrm{Fr}^e) + (\mathrm{N}_M)^e \varrho_p(\mathrm{Fr}^e)^{-1} \bmod p$$

for any $e \geqslant 1$.

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

§5. Proof of Theorem 2.4

Suppose that the assumptions of Theorem 2.4 hold. Since $p \notin \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2h'_k))$, we have $p \geqslant 5$ and $p \neq q$ (see Lemma 2.1). If $M^B(\mathbb{A}_k) = \emptyset$, then $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$. So, in the following, assume $M^B(\mathbb{A}_k) \neq \emptyset$. Then for any $v \in \Omega_k$, there is a point $x_v \in M^B(k_v)$. Note that k has no real place in this case. We have a family of characters

$$\{\phi_{x_v} : \mathrm{G}_{k_v} \longrightarrow (\mathbb{F}_{p^2}^{\times})^{12}\}_{v \in \Omega_k}$$

associated to the covering $f_p^B : Y_p^B \longrightarrow M^B$.

Assume that there is a global character $\Phi : \mathrm{G}_k \longrightarrow (\mathbb{F}_{p^2}^{\times})^{12}$ such that $\Phi|_{\mathrm{G}_{k_v}} = \phi_{x_v}$ for any $v \in \Omega_k$. If $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$, fix $K_0 \in \mathcal{K}_2(k, B) \cap \mathcal{K}(k, \mathfrak{q})$. Let

$$K := \begin{cases} k & \text{if } B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k), \\ K_0 & \text{if } B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k). \end{cases}$$

Then $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$ because $K_0 \in \mathcal{K}_2(k, B) \subseteq \mathcal{K}_1(k, B)$. Let $\mathfrak{M}$ be a prime of K, $\mathfrak{m}$ the prime of k below $\mathfrak{M}$, and $v(\mathfrak{m})$ the place of k corresponding to $\mathfrak{m}$. Since $B \otimes_{\mathbb{Q}} K_{\mathfrak{M}} \cong \mathrm{M}_2(K_{\mathfrak{M}})$, the point $x_{v(\mathfrak{m})}$ is represented by a QM-abelian surface $(A_{\mathfrak{M}}, i_{\mathfrak{M}})$ by $\mathcal{O}$ over $K_{\mathfrak{M}}$ (see [7, Theorem 1.1]). Then $\Phi|_{\mathrm{G}_{K_{\mathfrak{M}}}} = \phi_{x_{v(\mathfrak{m})}}|_{\mathrm{G}_{K_{\mathfrak{M}}}} = \varrho^{12}_{(A_{\mathfrak{M}}, i_{\mathfrak{M}}, p)}$ by Lemma 3.1. Since $K_0 \in \mathcal{K}(k, \mathfrak{q})$, there is a unique prime $\mathfrak{Q}$ of K above $\mathfrak{q}$. We also have

$$f_{\mathfrak{Q}} = f_{\mathfrak{q}}, \quad \mathrm{N}_{\mathfrak{Q}} = \mathrm{N}_{\mathfrak{q}} \quad \text{and} \quad \mathfrak{q}\mathcal{O}_K = \begin{cases} \mathfrak{q} = \mathfrak{Q} & \text{if } B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k), \\ \mathfrak{Q}^2 & \text{if } B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k). \end{cases}$$

Let $\mathrm{Fr}_{\mathfrak{Q}} \in \mathrm{G}_{K_{\mathfrak{Q}}} (\subseteq \mathrm{G}_K)$ be a Frobenius element. Fix an element $\alpha \in \mathcal{O}_k$ satisfying

$$\mathfrak{q}^{h'_k} = \alpha \mathcal{O}_k.$$

We see that the character $\Phi|_{\mathrm{G}_K}$ is unramified away from p. In fact, its restriction to $\mathrm{G}_{K_{\mathfrak{M}}}$ is $\varrho^{12}_{(A_{\mathfrak{M}}, i_{\mathfrak{M}}, p)}$, which is unramified if $\mathfrak{M} \nmid p$ (see Proposition 4.1). Then $\Phi|_{\mathrm{G}_K}$ is identified with a character $\mathfrak{I}_K(p) \longrightarrow (\mathbb{F}_{p^2}^{\times})^{12}$, where $\mathfrak{I}_K(p)$ is the group of fractional ideals of K prime to p.

For $\mathfrak{M} = \mathfrak{Q}$, we claim $\varrho^{12}_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) \equiv \mathrm{Norm}_{k/\mathbb{Q}}(\alpha)^{12} \bmod p$.

[Case $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$]. In this case, $[K : k] = 2$ and $\mathfrak{q}\mathcal{O}_K = \mathfrak{Q}^2$. Then

$$\begin{aligned} \varrho^{12}_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) &= \Phi|_{\mathrm{G}_{K_{\mathfrak{Q}}}}(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) = \Phi|_{\mathrm{G}_K}(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) = \Phi|_{\mathrm{G}_K}(\mathfrak{Q}^{2h'_k}) \\ &= \Phi|_{\mathrm{G}_K}(\mathfrak{q}^{h'_k}\mathcal{O}_K) = \Phi|_{\mathrm{G}_K}(\alpha\mathcal{O}_K) = \Phi|_{\mathrm{G}_K}((1)_\infty, (1)_p, (\alpha)^{\infty, p}) \end{aligned}$$

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

$$= \Phi|_{\mathrm{G}_K}((\alpha^{-1})_\infty, (\alpha^{-1})_p, (1)^{\infty,p}) = \Phi|_{\mathrm{G}_K}((\alpha^{-1})_p, (1)^p)$$
$$= \prod_{\mathfrak{P}|p} r^{12}_{(A_\mathfrak{P}, i_\mathfrak{P}, p)}(\alpha^{-1}).$$

Here, ∞ is the infinite place of $\mathbb{Q}$, $((1)_\infty, (1)_p, (\alpha)^{\infty,p})$ (resp. $((\alpha^{-1})_\infty, (\alpha^{-1})_p, (1)^{\infty,p})$, resp. $((\alpha^{-1})_p, (1)^p)$) is the element of $\mathbb{A}_K^\times$ where the components above ∞, p are 1 and the others α (resp. where the components above ∞, p are α^{-1} and the others 1, resp. where the components above p are α^{-1} and the others 1), and $\mathfrak{P}$ runs through the primes of K above p. Note that the components above ∞ have no contribution since K has no real place. Since $K_0 \in \mathcal{K}_2(k, B)$, we have $f_\mathfrak{P} = f_\mathfrak{p}$ where $\mathfrak{p}$ is the prime of k below $\mathfrak{P}$. By the assumption, $f_\mathfrak{p}$ is odd. Then $t_{K_\mathfrak{P}} = 1$ for any $\mathfrak{P}$. By Proposition 4.2, we have

$$r^{12}_{(A_\mathfrak{P}, i_\mathfrak{P}, p)}(\alpha^{-1}) = \mathrm{Norm}_{\kappa(\mathfrak{P})/\mathbb{F}_p}(\alpha \bmod \mathfrak{P})^{6e_\mathfrak{P}},$$

and so

$$\varrho^{12}_{(A_\mathfrak{Q}, i_\mathfrak{Q}, p)}(\mathrm{Fr}_\mathfrak{Q}^{2h'_k}) = \prod_{\mathfrak{P}|p} \mathrm{Norm}_{\kappa(\mathfrak{P})/\mathbb{F}_p}(\alpha \bmod \mathfrak{P})^{6e_\mathfrak{P}} \equiv \mathrm{Norm}_{K/\mathbb{Q}}(\alpha)^6$$
$$= \mathrm{Norm}_{k/\mathbb{Q}}(\alpha)^{12} \bmod p.$$

[Case $B \otimes_\mathbb{Q} k \cong \mathrm{M}_2(k)$]. In this case, $K = k$ and $\mathfrak{Q} = \mathfrak{q}$. Then

$$\varrho^{12}_{(A_\mathfrak{Q}, i_\mathfrak{Q}, p)}(\mathrm{Fr}_\mathfrak{Q}^{2h'_k}) = \Phi|_{\mathrm{G}_K}(\mathfrak{Q}^{2h'_k}) = \Phi|_{\mathrm{G}_K}(\alpha^2 \mathcal{O}_K) = \prod_{\mathfrak{P}|p} r^{24}_{(A_\mathfrak{P}, i_\mathfrak{P}, p)}(\alpha^{-1})$$
$$= \prod_{\mathfrak{P}|p} \mathrm{Norm}_{\kappa(\mathfrak{P})/\mathbb{F}_p}(\alpha \bmod \mathfrak{P})^{12e_\mathfrak{P}} \equiv \mathrm{Norm}_{K/\mathbb{Q}}(\alpha)^{12}$$
$$= \mathrm{Norm}_{k/\mathbb{Q}}(\alpha)^{12} \bmod p,$$

as claimed. Here, $\mathfrak{P}$ runs through the primes of $K = k$ above p.

Since $\mathfrak{q}^{h'_k} = \alpha \mathcal{O}_k$, we have $\mathrm{N}_\mathfrak{q}^{h'_k} = |\mathrm{Norm}_{k/\mathbb{Q}}(\alpha)|$ and $\mathrm{N}_\mathfrak{q}^{12h'_k} = \mathrm{Norm}_{k/\mathbb{Q}}(\alpha)^{12}$. Then

$$\varrho^{12}_{(A_\mathfrak{Q}, i_\mathfrak{Q}, p)}(\mathrm{Fr}_\mathfrak{Q}^{2h'_k}) \equiv \mathrm{N}_\mathfrak{q}^{12h'_k} = q^{12h'_k f_\mathfrak{q}} \bmod p.$$

On the other hand, we have

$$a(\mathrm{Fr}_\mathfrak{Q}^{2h'_k}) \equiv \varrho_{(A_\mathfrak{Q}, i_\mathfrak{Q}, p)}(\mathrm{Fr}_\mathfrak{Q}^{2h'_k}) + \mathrm{N}_\mathfrak{Q}^{2h'_k} \varrho_{(A_\mathfrak{Q}, i_\mathfrak{Q}, p)}(\mathrm{Fr}_\mathfrak{Q}^{2h'_k})^{-1}$$
$$= \varrho_{(A_\mathfrak{Q}, i_\mathfrak{Q}, p)}(\mathrm{Fr}_\mathfrak{Q}^{2h'_k}) + q^{2h'_k f_\mathfrak{Q}} \varrho_{(A_\mathfrak{Q}, i_\mathfrak{Q}, p)}(\mathrm{Fr}_\mathfrak{Q}^{2h'_k})^{-1} \bmod p$$

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

by Proposition 4.3(2), where $a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k})$ is the integer associated to $(A_{\mathfrak{Q}}, i_{\mathfrak{Q}})$ as in the last section. Let $\varepsilon := q^{-h'_k f_{\mathfrak{Q}}} \varrho_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) \in \mathbb{F}_{p^2}^{\times}$. Recall that $f_{\mathfrak{Q}} = f_{\mathfrak{q}}$. Then

$$\varepsilon^{12} = 1 \quad \text{and} \quad a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) \equiv (\varepsilon + \varepsilon^{-1}) q^{h'_k f_{\mathfrak{q}}} \bmod p.$$

Therefore

$$a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) \equiv 0, \quad \pm q^{h'_k f_{\mathfrak{q}}}, \quad \pm 2q^{h'_k f_{\mathfrak{q}}} \bmod p \quad \text{or} \quad a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k})^2 \equiv 3q^{2h'_k f_{\mathfrak{q}}} \bmod p.$$

By Proposition 4.3(1), we have $a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) \in \mathcal{C}(\mathrm{N}_{\mathfrak{Q}}, 2h'_k) = \mathcal{C}(q^{f_{\mathfrak{q}}}, 2h'_k)$. Then

$$\begin{aligned} &a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}), a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) \pm q^{h'_k f_{\mathfrak{q}}}, a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) \pm 2q^{h'_k f_{\mathfrak{q}}}, a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k})^2 - 3q^{2h'_k f_{\mathfrak{q}}} \\ &\quad \in \mathcal{D}(q^{f_{\mathfrak{q}}}, 2h'_k) = \mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2h'_k). \end{aligned}$$

Since $p \notin \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2h'_k))$, we have

(1) $a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) = 0, \pm q^{h'_k f_{\mathfrak{q}}}, \pm 2q^{h'_k f_{\mathfrak{q}}}$; or
(2) $a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k})^2 = 3q^{2h'_k f_{\mathfrak{q}}}$.

[Case (1)]. In this case, q divides $a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k})$. Then by [2, Lemma 2.6], q divides $a(\mathrm{Fr}_{\mathfrak{Q}})$. We have $f_{\mathfrak{Q}} = f_{\mathfrak{q}}$, which is odd by the assumption. Then we obtain $B \notin \mathcal{B}(q)$ (see [7, Theorem 2.1, Propositions 2.3 and 5.1(1)]). This is a contradiction.

[Case (2)]. Since $a(\mathrm{Fr}_{\mathfrak{Q}}^{2h'_k}) \in \mathbb{Z}$, this case cannot happen.

Then we have proved that the family $\{\phi_{x_v}\}_{v \in \Omega_k}$ does not come from a global character $\Phi : \mathrm{G}_k \longrightarrow (\mathbb{F}_{p^2}^{\times})^{12}$. This means that the subset $M^B(\mathbb{A}_k)^{f_p^B}$ of $M^B(\mathbb{A}_k)$ associated to f_p^B (see [10, Definition 5.3.1]) is empty. Then by [10, Theorem 6.1.2], we conclude $M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$. □

§6. Proof of Theorem 2.3

Suppose that the assumptions of Theorem 2.3 hold. Assume $M^B(\mathbb{A}_k) \neq \emptyset$. Then for any $v \in \Omega_k$, there is a point $x_v \in M^B(k_v)$. Since $B \notin \mathcal{S}(k, \mathfrak{q})$, there is a prime divisor p of $d(B)$ such that

$$p \notin \begin{cases} \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, e_{\mathfrak{q}})) & \text{if } B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k), \\ \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2e_{\mathfrak{q}})) & \text{if } B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k). \end{cases}$$

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

Fix such p. Then $p \geqslant 5$, $p \neq q$ and we have a family of characters

$$\{\phi_{x_v} : \mathrm{G}_{k_v} \longrightarrow (\mathbb{F}_{p^2}^{\times})^{12}\}_{v \in \Omega_k}$$

associated to f_p^B.

Assume that there is a global character $\Phi : \mathrm{G}_k \longrightarrow (\mathbb{F}_{p^2}^{\times})^{12}$ such that $\Phi|_{\mathrm{G}_{k_v}} = \phi_{x_v}$ for any $v \in \Omega_k$. If $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$, fix $K_0 \in \mathcal{K}_1(k, B) \cap \mathcal{K}(k, \mathfrak{q})$. Let $K, \mathfrak{M}, \mathfrak{m}, v(\mathfrak{m}), (A_{\mathfrak{M}}, i_{\mathfrak{M}})$ be the same as in the last section. Note that $[K : \mathbb{Q}]$ is even since $k/\mathbb{Q}$ has even degree. Then $\Phi|_{\mathrm{G}_{K_{\mathfrak{M}}}} = \phi_{x_{v(\mathfrak{m})}}|_{\mathrm{G}_{K_{\mathfrak{M}}}} = \varrho^{12}_{(A_{\mathfrak{M}}, i_{\mathfrak{M}}, p)}$. Let $\mathfrak{Q}$ be the unique prime of K above $\mathfrak{q}$, and let $\mathrm{Fr}_{\mathfrak{Q}} \in \mathrm{G}_{K_{\mathfrak{Q}}} (\subseteq \mathrm{G}_K)$ be a Frobenius element. Note that $\mathfrak{Q}$ is the unique prime of K above q. Then $q\mathcal{O}_K = \mathfrak{Q}^{e_{\mathfrak{Q}}}$ and $\mathrm{N}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}} = q^{[K:\mathbb{Q}]}$.

For $\mathfrak{M} = \mathfrak{Q}$, we prove $\varrho^{12}_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \equiv q^{6[K:\mathbb{Q}]} \bmod p$. The character $\Phi|_{\mathrm{G}_K}$ is unramified away from p, and it is identified with a character $\mathfrak{I}_K(p) \longrightarrow (\mathbb{F}_{p^2}^{\times})^{12}$. Then

$$\begin{aligned}
\varrho^{12}_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) &= \Phi|_{\mathrm{G}_{K_{\mathfrak{Q}}}}(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) = \Phi|_{\mathrm{G}_K}(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) = \Phi|_{\mathrm{G}_K}(\mathfrak{Q}^{e_{\mathfrak{Q}}}) = \Phi|_{\mathrm{G}_K}(q\mathcal{O}_K) \\
&= \Phi|_{\mathrm{G}_K}((1)_\infty, (1)_p, (q)^{\infty,p}) = \Phi|_{\mathrm{G}_K}((q^{-1})_\infty, (q^{-1})_p, (1)^{\infty,p}) \\
&= \Phi|_{\mathrm{G}_K}((q^{-1})_p, (1)^p) = \prod_{\mathfrak{P}|p} r^{12}_{(A_{\mathfrak{P}}, i_{\mathfrak{P}}, p)}(q^{-1}) \equiv \prod_{\mathfrak{P}|p} q^{6e_{\mathfrak{P}} f_{\mathfrak{P}}} = q^{6[K:\mathbb{Q}]} \bmod p.
\end{aligned}$$

Here, $((1)_\infty, (1)_p, (q)^{\infty,p}), ((q^{-1})_\infty, (q^{-1})_p, (1)^{\infty,p}), ((q^{-1})_p, (1)^p) \in \mathbb{A}_K^{\times}$ are defined in the same way as in the last section, $\mathfrak{P}$ runs through the primes of K above p, and the congruence follows from Proposition 4.2 (or [2, Corollary 2.3]).

In the following, we repeat the argument in [2, Section 3] and deduce a contradiction. We have

$$\begin{aligned}
a(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) &\equiv \varrho_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) + \mathrm{N}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}} \varrho_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}})^{-1} \\
&= \varrho_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) + q^{[K:\mathbb{Q}]} \varrho_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}})^{-1} \bmod p
\end{aligned}$$

by Proposition 4.3(2). Let $\varepsilon := q^{-[K:\mathbb{Q}]/2} \varrho_{(A_{\mathfrak{Q}}, i_{\mathfrak{Q}}, p)}(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \in \mathbb{F}_{p^2}^{\times}$. Then

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

Therefore

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

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

By Proposition 4.3(1), we have $a(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \in \mathcal{C}(\mathrm{N}_{\mathfrak{Q}}, e_{\mathfrak{Q}})$. Moreover, we have

$$f_{\mathfrak{Q}} = f_{\mathfrak{q}}, \quad \mathrm{N}_{\mathfrak{Q}} = \mathrm{N}_{\mathfrak{q}} \quad \text{and} \quad e_{\mathfrak{Q}} = \begin{cases} e_{\mathfrak{q}} & \text{if } B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k), \\ 2e_{\mathfrak{q}} & \text{if } B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k). \end{cases}$$

Then

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

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

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

[Case (1)]. In this case, q divides $a(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}})$ and $a(\mathrm{Fr}_{\mathfrak{Q}})$. Since $f_{\mathfrak{Q}}$ is odd, we have $B \notin \mathcal{B}(q)$. This is a contradiction.

[Case (2)]. Since $[K:\mathbb{Q}]$ is even and $a(\mathrm{Fr}_{\mathfrak{Q}}^{e_{\mathfrak{Q}}}) \in \mathbb{Z}$, this case cannot happen.

Then we have proved that the family $\{\phi_{x_v}\}_{v \in \Omega_k}$ does not come from $\Phi : \mathrm{G}_k \longrightarrow (\mathbb{F}_{p^2}^{\times})^{12}$. Therefore $M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$. □

§7. Counterexamples to the Hasse principle

Jordan obtained the following counterexamples to the Hasse principle, and Skorobogatov proved that it is accounted for by the Manin obstruction.

Proposition 7.1. ([7, Example 6.4] and [11, Section 4.1]) *If* $(d(B), k) = (39, \mathbb{Q}(\sqrt{-13}))$, *then* $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ *and* $M^B(\mathbb{A}_k) \neq \emptyset$.

Especially, the existence of adelic points help us produce counterexamples to the Hasse principle for $d(B) = 39$ and number fields containing $\mathbb{Q}(\sqrt{-13})$. In Lemma 7.2 below, we restrict our attention to the special case and study the assumptions of Theorem 2.4.

For a prime number $q \neq 2$, let $(\frac{\cdot}{q}) \in \{0, 1, -1\}$ be the Legendre symbol. For a nonzero integer $N \in \mathbb{Z}$, let $(N)'$ be the square free part of N. Precisely, if $N = ab^2$ where $a, b \in \mathbb{Z}$, a is square free and $\gcd(a, b) = 1$, then $(N)' = a$. For a finite Galois extension k of $\mathbb{Q}$ and a prime number l, let $e_l(k)$ (resp. $f_l(k)$, resp. $g_l(k)$) be the ramification index of l in $k/\mathbb{Q}$ (resp. the degree of the residue field extension above l in $k/\mathbb{Q}$, resp. the number of primes of k above l).

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

LEMMA 7.2.

(1) *Assume* $d(B)=39$. *Then:*

(i) $B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-13})\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-13}))$.
(ii) $B\in\mathcal{B}(q)$ *if and only if* $q\equiv 2 \bmod 3$ *or* $q\equiv 1,3,4,9,10,12 \bmod 13$.

(2) *Let* l *be a prime number, and assume* $(d(B),k)=(39,\mathbb{Q}(\sqrt{l},\sqrt{-13}))$. *Let* p,q *be distinct prime numbers, and let* $\mathfrak{q}$ *be a prime of* k *above* q. *Then the conditions* $p\mid d(B)$ *and* $p\notin\mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}},2h'_k))$ *imply* $p=13$. *In this case, we have:*

(i) $f_{\mathfrak{p}}$ *is odd for any prime* $\mathfrak{p}$ *of* k *above* p *if and only if* $l\equiv 0,1,3,4,9,10,12 \bmod 13$.
(ii) $f_{\mathfrak{q}}$ *is odd if and only if*

$$\begin{cases} \text{(a)} & q\equiv 1,7,9,11,13,15,17,19,25,29,31,47,49 \bmod 52, \\ & \left(\dfrac{l}{q}\right)\in\{0,1\} \text{ and } \left(\dfrac{(-13l)'}{q}\right)\in\{0,1\} \text{ when } q\neq 2, \\ \text{(b)} & l\equiv 1,2,3 \bmod 8 \text{ when } q=2. \end{cases}$$

Proof. (1) (i) The prime number 3 (resp. 13) is inert (resp. ramified) in $\mathbb{Q}(\sqrt{-13})$. Then $B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-13})\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-13}))$ (cf. Proof of Lemma 2.2).

(ii) By taking $p_1=13$ and $p_2=3$ in Lemma 2.2(2), we have $B\in\mathcal{B}(2)$. We see that 3 (resp. 13) splits in $\mathbb{Q}(\sqrt{-q})$ if and only if $q\equiv 2 \bmod 3$ (resp. $q\equiv 1,3,4,9,10,12 \bmod 13$). Then the assertion follows from Lemma 2.2(1).

(2) (i) Since $p=13$ is ramified in $\mathbb{Q}(\sqrt{-13})$, we have $e_p(k)=2$ or 4. Since a prime number except 2 is not totally ramified in a biquadratic field, we have $e_p(k)=2$. Then the following conditions are equivalent.

- $f_{\mathfrak{p}}$ is odd for any prime $\mathfrak{p}$ of k above p.
- $f_p(k)=1$.
- $(e_p(k),f_p(k),g_p(k))=(2,1,2)$.
- 13 splits in $\mathbb{Q}(\sqrt{l})$ or $l=13$.
- $l\equiv 0,1,3,4,9,10,12 \bmod 13$.

(ii) The following conditions are equivalent.

- $f_{\mathfrak{q}}$ is odd.
- $f_q(k)=1$.
- q is not inert in $\mathbb{Q}(\sqrt{-13})$, $\mathbb{Q}(\sqrt{l})$ or $\mathbb{Q}(\sqrt{(-13l)'})$.

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press

- $\begin{cases} \text{(a)} & \left(\frac{-13}{q}\right), \left(\frac{l}{q}\right), \left(\frac{(-13l)'}{q}\right) \in \{0,1\} \text{ when } q \neq 2, \\ \text{(b)} & l \not\equiv 5, 7 \bmod 8 \text{ when } q = 2. \end{cases}$
- $\begin{cases} \text{(a)} & q \equiv 1, 7, 9, 11, 13, 15, 17, 19, 25, 29, 31, 47, 49 \bmod 52, \\ & \left(\frac{l}{q}\right) \in \{0,1\} \text{ and } \left(\frac{(-13l)'}{q}\right) \in \{0,1\} \text{ when } q \neq 2, \\ \text{(b)} & l \equiv 1, 2, 3 \bmod 8 \text{ when } q = 2. \end{cases}$ □

Lemma 7.2 and a similar study combined with Proposition 7.1, [8, Table 1] help us prove Proposition 2.6 as follows.

(1) By Lemma 7.2(1)(i), we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-13}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-13}))$. Then $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$. Let $q = 2$. Then $(e_q(k), f_q(k), g_q(k)) = (4, 1, 1)$. Let $\mathfrak{q}$ be the unique prime of k above q. Then $\mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, e_{\mathfrak{q}})) = \mathcal{P}(\mathcal{D}(2, 4)) = \{2, 3, 5, 7, 47\}$ (see [2, Table 1]). By Lemma 7.2(1)(ii), we have $B \in \mathcal{B}(q)$. Let $p = 13$. Then $p \mid d(B)$ and $p \notin \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, e_{\mathfrak{q}}))$. Hence $B \notin \mathcal{S}(k, \mathfrak{q})$. Applying Theorem 2.3, we obtain $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$. By Proposition 7.1, we have $M^B(\mathbb{A}_{\mathbb{Q}(\sqrt{-13})}) \neq \emptyset$. Therefore $M^B(\mathbb{A}_k) \neq \emptyset$.

(2) Since $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-13}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-13}))$, we have $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$. Assume $k = \mathbb{Q}(\sqrt{3}, \sqrt{-13})$ (resp. $k = \mathbb{Q}(\sqrt{17}, \sqrt{-13})$). Then $Cl_k \cong \mathbb{Z}/4\mathbb{Z}$ (resp. $Cl_k \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) and $h'_k = 4$. These are due to the mathematics software system Sage. In any case, let $(p, q) = (13, 2)$. Then by Lemma 7.2, we have $B \in \mathcal{B}(q)$ and $f_p(k), f_q(k)$ are odd. In fact, $(e_p(k), f_p(k), g_p(k)) = (e_q(k), f_q(k), g_q(k)) = (2, 1, 2)$. Let $\mathfrak{q}$ be a prime of k above q. Then $\mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2h'_k)) = \mathcal{P}(\mathcal{D}(2, 8)) = \{2, 3, 5, 7, 31, 47, 193\}$ does not contain $p = 13$. By Theorem 2.4, we have $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$. Since $M^B(\mathbb{A}_{\mathbb{Q}(\sqrt{-13})}) \neq \emptyset$, we have $M^B(\mathbb{A}_k) \neq \emptyset$.

(3) The assertion follows from Theorem 2.3 with $q = 3$. See [2, Proof of Proposition 4.1(2)].

(4) We have $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ since 2 splits completely in k. In this case, $Cl_k \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $h'_k = 8$. Let $(p, q) = (61, 3)$. Then $(e_p(k), f_p(k), g_p(k)) = (e_q(k), f_q(k), g_q(k)) = (2, 1, 2)$. Since 61 splits in $\mathbb{Q}(\sqrt{-3})$, we have $B \in \mathcal{B}(q)$ (see Lemma 2.2(1)). Then $\mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2h'_k)) = \mathcal{P}(\mathcal{D}(3, 16)) = \{2, 3, 5, 7, 11, 17, 23, 31, 47, 97, 113, 191, 193, 353, 383, 2113, 3457, 30529, 36671\}$ does not contain $p = 61$. Applying Theorem 2.4, we have $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$. By [8, Table 1], we have $M^B(\mathbb{A}_{\mathbb{Q}(\sqrt{-183})}) \neq \emptyset$. Therefore $M^B(\mathbb{A}_k) \neq \emptyset$. □

Acknowledgments. The author would like to thank the anonymous referee for helpful comments, which have contributed to improving the article.

References

[1] K. Arai, *Points on Shimura curves rational over imaginary quadratic fields in the non-split case*. Preprint, http://arxiv.org/pdf/1411.1162.pdf, 2014.

[2] K. Arai, *Non-existence of points rational over number fields on Shimura curves*, Acta Arith. **172** (2016), 243–250.

[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. Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. **87**(3) (1997), 591–612.

[5] P. Clark, *On the Hasse principle for Shimura curves*, Israel J. Math. **171** (2009), 349–365.

[6] J. González and V. Rotger, *Non-elliptic Shimura curves of genus one*, J. Math. Soc. Japan **58**(4) (2006), 927–948.

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

[8] 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.

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

[10] A. Skorobogatov, *Torsors and Rational Points*, Cambridge Tracts in Mathematics **144**, Cambridge University Press, Cambridge, 2001.

[11] A. Skorobogatov, *Shimura coverings of Shimura curves and the Manin obstruction*, Math. Res. Lett. **12**(5–6) (2005), 779–788.

[12] A. Skorobogatov and A. Yafaev, *Descent on certain Shimura curves*, Israel J. Math. **140** (2004), 319–332.

[13] M.-F. Vignéras, *Arithmétique des algèbres de quaternions (French) [Arithmetic of quaternion algebras]*, Lecture Notes in Mathematics **800**, Springer, Berlin, 1980, vii+169 pp. ISBN: 3-540-09983-2.

Department of Mathematics
School of Science and Technology for Future Life
Tokyo Denki University
5 Senju Asahi-cho
Adachi-ku
Tokyo 120-8551
Japan

araik@mail.dendai.ac.jp

https://doi.org/10.1017/nmj.2017.6 Published online by Cambridge University Press