RIMS Kôkyûroku Bessatsu
B72 (2018), 197–207

A survey of rational points on Shimura curves

By

Keisuke Arai*

Abstract

In this survey, we summarize known results and the author's works concerning rational points on Shimura curves.

§ 1. Introduction

For a prime number p, let $Y_0(p)$ be the coarse moduli scheme over $\mathbb{Q}$ classifying (E, C) where E is an elliptic curve and C is a cyclic subgroup of E of order p. Let $X_0(p)$ be the smooth compactification of $Y_0(p)$. Then $Y_0(p)$ is an affine smooth curve over $\mathbb{Q}$, while $X_0(p)$ is a proper smooth curve over $\mathbb{Q}$. These curves are called *modular curves*. See [11, Chapter II, §1] or [12, §2].

For rational points on $Y_0(p)$ and $X_0(p)$, we have the following theorem.

Theorem 1.1 ([13, Theorem 7.1]). *If $p > 163$, then $Y_0(p)(\mathbb{Q}) = \emptyset$. Equivalently, if $p > 163$, then $X_0(p)(\mathbb{Q})$ consists of only cusps.*

This theorem was expanded to quadratic fields.

Theorem 1.2 ([15, Theorem B]). *Let k be a quadratic field which is not an imaginary quadratic field of class number one. Then there is a constant $C(k)$ depending on k such that if $p > C(k)$, then $Y_0(p)(k) = \emptyset$ (equivalently, $X_0(p)(k)$ consists of only cusps).*

Received March 31, 2016. Revised October 7, 2016.
2010 Mathematics Subject Classification(s): Primary 11G18, 14G05; Secondary 11G10, 11G15.
Key Words: *rational points, Shimura curves, QM-abelian surfaces.*
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.
*Department of Mathematics, School of Science and Technology for Future Life, Tokyo Denki University, Tokyo 120-8551, Japan.
e-mail: araik@mail.dendai.ac.jp

In Theorems 1.1 and 1.2, the number of cusps is two. If we regard p as the level of $Y_0(p)$ and $X_0(p)$, then the above theorems can be interpreted as follows: If the level of a modular curve is sufficiently large, then the set of rational points over a number field on the modular curve is small.

From now to the end of this article, let k be a number field. We propose a basic problem concerning k-rational points on a certain moduli of abelian varieties or its compactification.

Problem 1.3. *Let X be a certain moduli of abelian varieties with a level structure* (*e.g.* $X = Y_0(p)$) *or its compactification* (*e.g.* $X = X_0(p)$). *If the level of X grows, does the set $X(k)$ become small?*

In Problem 1.3, the meaning of "$X(k)$ is small" depends on the case. In some cases, it means that $X(k) = \emptyset$ or that $X(k)$ consists of only cusps. In another case, for example, we have the following open problem (see [2, Question 2.1] or [17, p.187–188]): If p is sufficiently large (depending on k), does $Y_0(p)(k)$ (resp. $X_0(p)(k)$) consist of at most CM points (resp. at most cusps and CM points)? Here, a CM point means a point which corresponds to an elliptic curve with complex multiplication.

§ 2. Results on Shimura curves

In the following, we discuss the case where X in Problem 1.3 is a Shimura curve over $\mathbb{Q}$, and give partial solutions to this problem. Let B be an indefinite quaternion division algebra over $\mathbb{Q}$, and let $d(B)$ be the product of prime numbers p such that $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \not\cong \mathrm{M}_2(\mathbb{Q}_p)$. Then $d(B)$ is called the *discriminant* of B. Note that $B \mapsto d(B)$ induces a bijection between the set of the isomorphism classes of indefinite quaternion division algebras over $\mathbb{Q}$, and the set of $d \in \mathbb{Z}$ such that $d > 1$ and d is the product of an even number of distinct prime numbers (see [18, Theorem 3.5]). Choose a maximal order $\mathcal{O}$ of B, which we fix. Note that $\mathcal{O}$ is not unique, but it is unique up to conjugation (see [1, Theorem 1.59], [14, Theorem 5.2.12] or [18, Theorem 3.10]). A *QM-abelian surface* by $\mathcal{O}$ over a field F is a pair (A, i), where A is a two-dimensional abelian variety over F and $i\colon \mathcal{O} \hookrightarrow \mathrm{End}_F(A)$ is an injective ring homomorphism satisfying $i(1) = id$. Here, $\mathrm{End}_F(A)$ is the ring of endomorphisms of A defined over F. Note that a QM-abelian surface is sometimes called a *false elliptic curve* (see [7, §1]). Let M^B be the coarse moduli scheme over $\mathbb{Q}$ classifying QM-abelian surfaces by $\mathcal{O}$. Then M^B is a proper smooth curve over $\mathbb{Q}$, which is called the *Shimura curve* associated to B. Note that M^B has no cusps. Note also that the isomorphism class of M^B does not depend on the choice of $\mathcal{O}$. See [8, p.93] or [9, p.235]. We regard $d(B)$ as the level of M^B.

There are no $\mathbb{R}$-rational points on M^B as follows.

Theorem 2.1 ([19, Theorem 0]). $M^B(\mathbb{R}) = \emptyset$.

Example 2.2. If $d(B) = 6$, then M^B is defined by the equation $x^2 + y^2 + 3 = 0$ (see [10, Theorem 1-1]).

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

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

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

- $\kappa(\mathfrak{q})$: the residue field of $\mathfrak{q}$,
- $l_{\mathfrak{q}}$: the characteristic of $\kappa(\mathfrak{q})$,
- $\mathrm{N}_{\mathfrak{q}}$: 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 $\kappa(\mathfrak{q})/\mathbb{F}_{l_{\mathfrak{q}}}$.

We have the following theorem concerning non-existence of k-rational points on M^B.

Theorem 2.3 ([3, Theorem 1.1]). *Assume that*

- $[k : \mathbb{Q}]$ *is even,*
- $\mathfrak{q}$ *is a prime of* k *of residue characteristic* q*,*
- $\mathfrak{q}$ *is the unique prime of* k *above* q*,*
- $f_{\mathfrak{q}}$ *is odd,*
- $B \in \mathcal{B}(q)$.

Then there is a finite set $P_1(k, \mathfrak{q})$ *of prime numbers depending on* k *and* $\mathfrak{q}$ *satisfying: If there is a prime divisor* p *of* $d(B)$ *which is not in* $P_1(k, \mathfrak{q})$*, then* $M^B(k) = \emptyset$.

Remark.

1. Roughly speaking, the condition that "there is a prime divisor p of $d(B)$ which is not in $P_1(k, \mathfrak{q})$" is equivalent to that $d(B)$ is sufficiently large, because $d(B)$ is square free. Then Theorem 2.3 can be interpreted as follows: Under some assumptions, we have $M^B(k) = \emptyset$ if $d(B)$ is sufficiently large. So, this theorem gives a partial solution to Problem 1.3.

2. For an imaginary quadratic field k, Theorem 2.3 was proved in [8, Theorem 6.3] (in the case where $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$) and [16, Theorem 1.1] (under mild extra assumptions).

3. If $[k:\mathbb{Q}]$ is odd, then there is an embedding $k \hookrightarrow \mathbb{R}$, and so $M^B(k) = \emptyset$ by Theorem 2.1.

In Theorem 2.3, the uniqueness of $\mathfrak{q}$ seems strong. In the following theorem, we do not assume the uniqueness of $\mathfrak{q}$, though we impose an additional condition on a prime divisor p of $d(B)$.

Theorem 2.4 ([4, Theorem 2.4]). *Assume that*

- $[k:\mathbb{Q}]$ *is even,*
- $\mathfrak{q}$ *is a prime of* k *of residue characteristic* q*,*
- $f_{\mathfrak{q}}$ *is odd,*
- $B \in \mathcal{B}(q)$.

Then there is a finite set $P_2(k, \mathfrak{q})$ *of prime numbers depending on* k *and* $\mathfrak{q}$ *satisfying: If there is a prime divisor* p *of* $d(B)$ *such that* $p \notin P_2(k, \mathfrak{q})$ *and* $f_{\mathfrak{p}}$ *is odd for any prime* $\mathfrak{p}$ *of* k *above* p*, then* $M^B(k) = \emptyset$.

Definitions of the exceptional sets $P_1(k, \mathfrak{q})$, $P_2(k, \mathfrak{q})$ will be given in §3. Let h_k be the class number of k. From now to the end of this section, assume that k is an imaginary quadratic field of $h_k > 1$ unless otherwise specified. Then as seen in the following theorem, we need no auxiliary prime $\mathfrak{q}$ as in Theorems 2.3 and 2.4.

Theorem 2.5 ([8, Theorem 6.6]). *There is a finite set* $P(k)$ *of prime numbers depending on* k *satisfying: If* $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ *and if there is a prime divisor* p *of* $d(B)$ *which is not in* $P(k)$*, then* $M^B(k) = \emptyset$.

Remark.

1. Theorem 2.5 can be interpreted as follows: If $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ and if $d(B)$ is sufficiently large, then $M^B(k) = \emptyset$. So, this theorem gives a partial solution to Problem 1.3.

2. If $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ and if k is an imaginary quadratic field of $h_k = 1$, then $M^B(k) \neq \emptyset$ (see [8, Proposition 6.5]).

We have the following theorem in the case where $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$.

Theorem 2.6 ([5]). *There is a finite set $P'(k)$ of prime numbers depending on k satisfying: If $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$ and if there is a prime divisor p of $d(B)$ such that*

(i) *$p \notin P'(k)$, and*

(ii) *if p splits in k, then $p \equiv 1 \bmod 4$,*

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

Definitions of the exceptional sets $P(k)$, $P'(k)$ will be given in §3.

Remark. In Theorem 2.6, the assumption (ii) is technical, and might be unnecessary. If we can drop it, then the following assertion is true: If $d(B)$ is sufficiently large, then $M^B(k) = \emptyset$.

§ 3. Definitions of the exceptional sets and numerical examples

In this section, we give a definition of the exceptional set $P_1(k, \mathfrak{q})$ (resp. $P_2(k, \mathfrak{q})$, resp. $P(k)$, resp. $P'(k)$) of prime numbers in Theorem 2.3 (resp. Theorem 2.4, resp. Theorem 2.5, resp. Theorem 2.6) explicitly. We also give numerical examples of Theorems 2.3 and 2.4. Let

- Cl_k: the ideal class group of k,
- h'_k: the largest order of the elements in Cl_k.

Then h'_k divides h_k. For positive integers N and e, let

$$\mathcal{C}(N,e) :=$$

$$\left\{ \beta^e + \overline{\beta}^e \in \mathbb{Z} \;\middle|\; \beta, \overline{\beta} \in \mathbb{C} \text{ are the roots of } T^2 + sT + N = 0 \text{ for some } s \in \mathbb{Z},\ s^2 \leq 4N \right\},$$

$$\mathcal{D}(N,e) := \left\{ a, a \pm N^{\frac{e}{2}}, a \pm 2N^{\frac{e}{2}}, a^2 - 3N^e \in \mathbb{R} \;\middle|\; a \in \mathcal{C}(N,e) \right\}.$$

Note that any element $a \in \mathcal{C}(N,e)$ satisfies $|a| \leq 2N^{\frac{e}{2}}$. For a subset $\mathcal{D} \subseteq \mathbb{Z}$, let

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

If e is even, then $\mathcal{D}(N,e)$ is a subset of $\mathbb{Z}$, and the set $\mathcal{P}(\mathcal{D}(N,e))$ contains $2, 3$ and every prime divisor of N. We define the finite sets

$$\widetilde{P}_1(k,\mathfrak{q}) := \begin{cases} \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, e_{\mathfrak{q}})) & \text{if } B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k) \text{ and } e_{\mathfrak{q}} \text{ is even,} \\ \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2e_{\mathfrak{q}})) & \text{if } B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k), \end{cases}$$

$$\widetilde{P}_2(k,\mathfrak{q}) := \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2h'_k)).$$

In Theorems 2.3 and 2.4, $P_1(k,\mathfrak{q}) = \widetilde{P}_1(k,\mathfrak{q})$ and $P_2(k,\mathfrak{q}) = \widetilde{P}_2(k,\mathfrak{q})$ are appropriate choices, respectively.

For a finite Galois extension k of $\mathbb{Q}$ and a prime number l, let e_l (resp. f_l, resp. g_l) 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). Note that $e_l f_l g_l = [k:\mathbb{Q}]$. We have the following examples of Theorems 2.3 and 2.4, which will be reconsidered in §5 in the context of the Hasse principle and the Manin obstruction.

Example 3.1. Assume $d(B) = 39$, $k = \mathbb{Q}(\sqrt{2}, \sqrt{-13})$. Let $(p,q) = (13,2)$. Then $(e_p, f_p, g_p) = (2,2,1)$ and $(e_q, f_q, g_q) = (4,1,1)$. 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. $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1}))$). Then $B \in \mathcal{B}(q)$. Since $(e_3, f_3, g_3) = (1,2,2)$ and $(e_{13}, f_{13}, g_{13}) = (2,2,1)$, we have $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ (see [22, Chapitre II, Théorème 1.3]). Let $\mathfrak{q}$ be the unique prime of k above $q = 2$. Then $e_{\mathfrak{q}} = 4$, $f_{\mathfrak{q}} = 1$, $\mathrm{N}_{\mathfrak{q}} = 2$, and $\widetilde{P}_1(k,\mathfrak{q}) = \mathcal{P}(\mathcal{D}(2,4)) = \{2,3,5,7,47\} \not\ni p$ (see [3, Table 1]). Applying Theorem 2.3, we obtain $M^B(k) = \emptyset$.

Example 3.2. Assume $d(B) = 122$, $k = \mathbb{Q}(\sqrt{-39}, \sqrt{-183})$. Let $(p,q) = (61,3)$. Then $(e_p, f_p, g_p) = (e_q, f_q, g_q) = (2,1,2)$. Since 61 splits in $\mathbb{Q}(\sqrt{-3})$, we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-3}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-3}))$ and $B \in \mathcal{B}(q)$. Let $\mathfrak{q}$ be any prime of k above $q = 3$. Then $f_{\mathfrak{q}} = 1$, $\mathrm{N}_{\mathfrak{q}} = 3$. Since $Cl_k \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we have $h'_k = 8$ and $\widetilde{P}_2(k,\mathfrak{q}) = \mathcal{P}(\mathcal{D}(3,16)) = \{2,3,5,7,11,17,23,31,47,97,113,191,193,353,383,2113,3457,30529, 36671\} \not\ni p$. Applying Theorem 2.4, we obtain $M^B(k) = \emptyset$.

Remark.

1. If $k = \mathbb{Q}(\sqrt{-39}, \sqrt{-183})$, then no prime number is totally ramified in k. So, in the situation of Example 3.2, no prime $\mathfrak{q}$ of k satisfies the assumptions of Theorem 2.3. Then we cannot obtain Example 3.2 from Theorem 2.3.

2. If $k = \mathbb{Q}(\sqrt{2}, \sqrt{-13})$, then $f_3 = f_{13} = 2$. So, in the situation of Example 3.1, there is no prime divisor p of $d(B) = 39$ satisfying the assumptions of Theorem 2.4. Then we cannot obtain Example 3.1 from Theorem 2.4.

From now to the end of this section, assume that k is an imaginary quadratic field of $h_k > 1$. Let $\mathcal{S}_0$ be the set of non-principal primes of k which split in $k/\mathbb{Q}$. Then $\mathcal{S}_0 \neq \emptyset$ since $h_k > 1$. For each prime $\mathfrak{q}$ of k, fix an element $\beta_{\mathfrak{q},J} \in \mathcal{O}_k$ (resp. $\beta_{\mathfrak{q}} \in \mathcal{O}_k$) satisfying $\mathfrak{q}^{h_k} = \beta_{\mathfrak{q},J}\mathcal{O}_k$ (resp. $\mathfrak{q}^{h'_k} = \beta_{\mathfrak{q}}\mathcal{O}_k$). Let c_k be the least positive integer such that Cl_k is generated by primes $\mathfrak{q}$ of k satisfying $f_{\mathfrak{q}} = 1$ and $\mathrm{N}_{\mathfrak{q}} < c_k$. Let

- $\mathcal{A}_{1,\mathfrak{q},J}(k) := \left\{ a - \mathrm{Tr}_{k/\mathbb{Q}}(\beta_{\mathfrak{q},J}^{12}) \in \mathbb{Z} \;\middle|\; a \in \mathbb{Z},\ |a| \le 2\mathrm{N}_{\mathfrak{q}}^{6h_k} \right\}$,

- $\mathcal{A}_{2,\mathfrak{q},J}(k) := \{\, a - \mathrm{N}_{\mathfrak{q}}^{4h_k}\mathrm{Tr}_{k/\mathbb{Q}}(\beta_{\mathfrak{q},J}^4) \in \mathbb{Z} \mid a \in \mathbb{Z},\ |a| \leq 2\mathrm{N}_{\mathfrak{q}}^{6h_k} \,\}$,
- $\mathcal{A}_{3,J}(k)$: the set of integers of the forms $\mathrm{Norm}_{\mathbb{Q}(\zeta_{3h_k})/\mathbb{Q}}(a^2 - q(\theta + \theta^{-1} + 2))$ and $\mathrm{Norm}_{\mathbb{Q}(\zeta_{3h_k})/\mathbb{Q}}(a^2 + q(\theta + \theta^{-1} - 2))$, where $\theta^{3h_k} = 1$, q is a prime number less than c_k, and $a \in \mathbb{Z}$, $|a| \leq 2\sqrt{q}$,
- $\mathcal{N}_{4,J}(k)$: the set of prime numbers $p > 2$ satisfying $\left(\frac{q}{p}\right) = -1$ for all prime numbers q such that $3 < q < \frac{p}{4}$ and q is not inert in k.

Here, ζ_{3h_k} is a primitive $3h_k$-th root of unity. The subscript "J" denotes the initial of Jordan. Note that $\mathcal{A}_{1,\mathfrak{q},J}(k)$ and $\mathcal{A}_{2,\mathfrak{q},J}(k)$ are independent of the choice of $\beta_{\mathfrak{q},J}$, because $\mathcal{O}_k^\times = \{\, \pm 1 \,\}$. Let $\mathbf{Ram}(k)$ be the set of prime numbers which are ramified in k. We define

$$\widetilde{P}(k) := \mathbf{Ram}(k) \cup \{\, p \mid p \leq 7 \,\} \cup \left(\bigcap_{\mathfrak{q} \in \mathcal{S}_0} \mathcal{P}(\mathcal{A}_{1,\mathfrak{q},J}(k)) \right) \cup \left(\bigcap_{\mathfrak{q} \in \mathcal{S}_0} \mathcal{P}(\mathcal{A}_{2,\mathfrak{q},J}(k)) \right)$$
$$\cup \mathcal{P}(\mathcal{A}_{3,J}(k)) \cup \mathcal{N}_{4,J}(k).$$

Let

- $\mathcal{A}_{1,\mathfrak{q}}(k) := \{\, a - \mathrm{Tr}_{k/\mathbb{Q}}(\beta_{\mathfrak{q}}^{24}) \in \mathbb{Z} \mid a \in \mathcal{C}(\mathrm{N}_{\mathfrak{q}}, 24h'_k) \,\}$,
- $\mathcal{A}_{2,\mathfrak{q}}(k) := \left\{\, a - \mathrm{N}_{\mathfrak{q}}^{8h'_k}\mathrm{Tr}_{k/\mathbb{Q}}(\beta_{\mathfrak{q}}^{8}) \in \mathbb{Z} \,\middle|\, a \in \mathcal{C}(\mathrm{N}_{\mathfrak{q}}, 24h'_k) \,\right\}$,
- $\mathcal{A}_{3,\mathcal{S}}(k) := \left\{\, a - 2\mathrm{N}_{\mathfrak{q}}^{12h'_k} \in \mathbb{Z} \,\middle|\, \mathfrak{q} \in \mathcal{S},\ a \in \mathcal{C}(\mathrm{N}_{\mathfrak{q}}, 24h'_k) \,\right\}$, where $\mathcal{S}$ is a non-empty finite subset of $\mathcal{S}_0$ generating Cl_k,
- $\mathcal{N}(k)$: the set of integers $N \in \mathbb{Z}$ such that
  - (i) N is the discriminant of a quadratic field, and
  - (ii) for any prime number $2 < q < \frac{|N|}{4}$, if q splits in k, then q does not split in $\mathbb{Q}(\sqrt{N})$,
- $\mathcal{N}^{prime}(k)$: the set of prime numbers in $\mathcal{N}(k)$.

Note that $\mathcal{A}_{1,\mathfrak{q}}(k)$ and $\mathcal{A}_{2,\mathfrak{q}}(k)$ are independent of the choice of $\beta_{\mathfrak{q}}$. We define

$$\widetilde{P}'(k) := \mathbf{Ram}(k) \cup \{\, p \mid p \leq 23 \,\} \cup \left(\bigcap_{\mathfrak{q} \in \mathcal{S}_0} \mathcal{P}(\mathcal{A}_{1,\mathfrak{q}}(k)) \right) \cup \left(\bigcap_{\mathfrak{q} \in \mathcal{S}_0} \mathcal{P}(\mathcal{A}_{2,\mathfrak{q}}(k)) \right)$$
$$\cup \left(\bigcap_{\mathcal{S} \subseteq \mathcal{S}_0} \left(\mathcal{P}(\mathcal{A}_{3,\mathcal{S}}(k)) \cup \{\, l_{\mathfrak{q}} \mid \mathfrak{q} \in \mathcal{S} \,\} \right) \right) \cup \mathcal{N}^{prime}(k),$$

where $\mathcal{S}$ runs through non-empty finite subsets of $\mathcal{S}_0$ generating Cl_k. Note that $\widetilde{P}'(k)$ is defined by modifying $\widetilde{P}(k)$. By [13, Theorem A], the sets $\mathcal{N}_{4,J}(k)$ and $\mathcal{N}(k)$ are finite, and their upper bounds can be effectively estimated except at most one element. Then the sets $\widetilde{P}(k)$ and $\widetilde{P}'(k)$ are finite. In Theorems 2.5 and 2.6, $P(k) = \widetilde{P}(k)$ and $P'(k) = \widetilde{P}'(k)$ are appropriate choices, respectively.

§ 4. Difficulty of the case where $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$

In this section, we explain the difficulty of the case where $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$, and the way to overcome it. For a rational point on M^B, there is sometimes a gap between the field of moduli and the field of definition as follows.

Theorem 4.1 ([8, Theorem 1.1]). *Let F be a field of characteristic 0. Then a point $x \in M^B(F)$ is represented by a QM-abelian surface by $\mathcal{O}$ over F if and only if $B \otimes_{\mathbb{Q}} F \cong \mathrm{M}_2(F)$.*

So, when $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$, a point $x \in M^B(k)$ is *not* represented by a QM-abelian surface by $\mathcal{O}$ over k. This is the reason why the case where $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$ is difficult. We can overcome the difficulty by improving Jordan's method of studying canonical isogeny characters.

First, we explain Jordan's method in the case where $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$. Suppose that there is a point $x \in M^B(k)$. Then x is represented by a QM-abelian surface (A, i) by $\mathcal{O}$ over k. Let p be a prime divisor of $d(B)$, and let T_pA be the p-adic Tate module of A. Then T_pA has a structure of a free $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$-module of rank one. Let $\overline{k}$ be an algebraic closure of k, and let $\mathrm{G}_k = \mathrm{Gal}(\overline{k}/k)$ be the absolute Galois group of k. The action of G_k on T_pA yields a representation

$$R_p \colon \mathrm{G}_k \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T_pA) \cong (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{\times},$$

where $\mathrm{Aut}_{\mathcal{O}}(T_pA)$ is the group of $\mathbb{Z}_p$-linear automorphisms of T_pA commuting with the action of $\mathcal{O}$. Let $\overline{R}_p := R_p \bmod p$. Then by conjugating if necessary, we have

$$\overline{R}_p \colon \mathrm{G}_k \longrightarrow \left\{ \begin{pmatrix} a & * \\ 0 & a^p \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2}) \right\}.$$

From the $(1, 1)$ entry, we obtain a character

$$\varrho_p \colon \mathrm{G}_k \longrightarrow \mathbb{F}_{p^2}^{\times}.$$

This is called a *canonical isogeny character* at p, which was introduced in [8, §4]. In Theorems 2.3, 2.4 and 2.5, we use the classification of ϱ_p to conclude that p is in an exceptional finite set.

Next, we explain how to modify Jordan's method in the case where $B\otimes_{\mathbb{Q}}k \not\cong \mathrm{M}_2(k)$. Suppose that there is a point $x \in M^B(k)$. Let K be a quadratic extension of k such that $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$, equivalently, if a prime $\mathfrak{l}$ of k satisfies $B \otimes_{\mathbb{Q}} k_{\mathfrak{l}} \not\cong \mathrm{M}_2(k_{\mathfrak{l}})$, then it does not split in K (see [1, Proposition 1.14]). Here, $k_{\mathfrak{l}}$ is the completion of k at $\mathfrak{l}$. We can always take such K (see [6, Remark 4.4]). Then x is represented by a QM-abelian surface (A, i) by $\mathcal{O}$ over K. Let p be a prime divisor of $d(B)$. Then by the same argument as above, we obtain a representation

$$R_{p,K} \colon \mathrm{G}_K \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T_pA) \cong (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$$

and a character

$$\varrho_{p,K} \colon \mathrm{G}_K \longrightarrow \mathbb{F}_{p^2}^\times.$$

To prove Theorems 2.3 and 2.4, it suffices to take a good choice of K. To prove Theorem 2.6, we use the composition

$$\varphi_{p,K} \colon \mathrm{G}_k \xrightarrow{\mathrm{tr}_{K/k}} \mathrm{G}_K^{\mathrm{ab}} \xrightarrow{\varrho_{p,K}^{\mathrm{ab}}} \mathbb{F}_{p^2}^\times,$$

where $\mathrm{tr}_{K/k}$ is the transfer map, $\mathrm{G}_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$, K^{ab} is the maximal abelian extension of K in $\overline{K}$, and $\varrho_{p,K}^{\mathrm{ab}}$ is the natural map induced from $\varrho_{p,K}$. Then we classify $\varphi_{p,K}$, and conclude that p is in $\widetilde{P}'(k)$. Here, $\varphi_{p,K}$ depends on K, but $\varphi_{p,K}^4$ does not. This is a key to the proof.

Remark. In [16], a different approach is taken when $B\otimes_{\mathbb{Q}}k \not\cong \mathrm{M}_2(k)$. In this case, we do not have a representation $R_p \colon \mathrm{G}_k \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T_pA) \cong (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$, but instead a projective representation $\mathrm{G}_k \longrightarrow (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times/\{\pm 1\}$ is defined and studied.

§ 5. Relevance to the Manin obstruction

In this section, we introduce the concept of the Manin obstruction, and give an example concerning Shimura curves. Let $\mathbb{A}_k$ be the adèle ring of k, and let Ω_k be the set of places of k. For $v \in \Omega_k$, let k_v be the completion of k at v. Since M^B is proper over $\mathbb{Q}$, we have $M^B(\mathbb{A}_k) = \prod_{v\in\Omega_k} M^B(k_v)$. Let $\mathrm{Br}(k_v)$ (resp. $\mathrm{Br}(M^B) = H^2_{\text{ét}}(M^B, \mathbb{G}_m)$) be the Brauer group of k_v (resp. M^B). Let

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

be the pairing defined by $(c, \{x_v\}_{v\in\Omega_k}) = \sum_{v\in\Omega_k} \mathrm{inv}_v(x_v^* c)$. Here, $\mathrm{inv}_v \colon \mathrm{Br}(k_v) \longrightarrow \mathbb{Q}/\mathbb{Z}$ is the local invariant at v, and $x_v^* \colon \mathrm{Br}(M^B) \longrightarrow \mathrm{Br}(k_v)$ is the map associated to

$x_v\colon \mathrm{Spec}(k_v) \longrightarrow M^B$. Note that in the above 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, i.e.,

$$M^B(\mathbb{A}_k)^{\mathrm{Br}} := \left\{ \{x_v\}_{v\in\Omega_k} \in M^B(\mathbb{A}_k) \;\middle|\; (c, \{x_v\}_{v\in\Omega_k}) = 0 \text{ for any } c \in \mathrm{Br}(M^B) \right\}.$$

Then

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

When $M^B(k) = \emptyset$ and $M^B(\mathbb{A}_k) \neq \emptyset$, M^B is called a *counterexample to the Hasse principle* over k. Such a counterexample is said to be accounted for by the *Manin obstruction* if $M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ (see [20, §5.2]).

Theorem 5.1 ([4, Theorems 2.3 and 2.4])**.** *In Theorems* 2.3 *and* 2.4*, we can replace "*$M^B(k) = \emptyset$*" with "*$M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$*". Moreover, we can take* $P_1(k, \mathfrak{q}) = \widetilde{P}_1(k, \mathfrak{q})$ *and* $P_2(k, \mathfrak{q}) = \widetilde{P}_2(k, \mathfrak{q})$*.*

Remark. In the situation of Theorem 2.3, $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ for an imaginary quadratic field k was proved in [21, Theorem 3.1] (in the case where $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$) and [16, Theorem 1.1] (under mild extra assumptions).

Example 5.2. In the situations of Examples 3.1 and 3.2, we have $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ and $M^B(\mathbb{A}_k) \neq \emptyset$ (see [3, Proposition 4.1], [4, Proposition 2.6]). So, in these cases, M^B is a counterexample to the Hasse principle over k, and it is accounted for by the Manin obstruction.

Remark. In the situations of Theorems 2.5 and 2.6, we expect $M^B(k) = M^B(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$, but there is no such result so far.

Acknowledgements

The author would like to thank the organizers Hiroki Sumida-Takahashi, Yasuo Ohno and Takahiro Tsushima for giving him an opportunity to talk at the conference. He would also like to thank the anonymous referee for helpful comments.

References

[1] Alsina, M. and Bayer, P., Quaternion orders, quadratic forms, and Shimura curves, *CRM Monograph Series*, 22. American Mathematical Society, Providence, RI, 2004.

[2] Arai, K., Galois images and modular curves, *Algebraic number theory and related topics 2010*, 145–161, *RIMS Kôkyûroku Bessatsu*, **B32**, Res. Inst. Math. Sci. (RIMS), Kyoto, 2012.

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

[4] Arai, K., Rational points on Shimura curves and the Manin obstruction, *Nagoya Math. J.*, **230** (2018), 144–159.

[5] Arai, K., Points on Shimura curves rational over imaginary quadratic fields in the non-split case, *preprint*, available at the web page (https://arxiv.org/pdf/1411.1162v1).

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

[7] Buzzard, K., Integral models of certain Shimura curves, *Duke Math. J.*, **87** (1997), no. 3, 591–612.

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

[9] Jordan, B. and Livné, R., Local Diophantine properties of Shimura curves, *Math. Ann.*, **270** (1985), no. 2, 235–248.

[10] Kurihara, A, On some examples of equations defining Shimura curves and the Mumford uniformization, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **25** (1979), no. 3, 277–300.

[11] Mazur, B., Modular curves and the Eisenstein ideal, *I.H.E.S. Publ. Math.*, No. **47** (1977), 33–186.

[12] Mazur, B., Rational points on modular curves, *Modular functions of one variable V, Lecture Notes in Math.*, Vol. 601, Springer, Berlin (1977), 107–148.

[13] Mazur, B., Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.*, **44** (1978), no. 2, 129–162.

[14] Miyake, T., Modular forms. Translated from the 1976 Japanese original by Yoshitaka Maeda. Reprint of the first 1989 English edition. *Springer Monographs in Mathematics*. Springer-Verlag, Berlin, 2006.

[15] Momose, F., Isogenies of prime degree over number fields, *Compositio Math.*, **97** (1995), no. 3, 329–348.

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

[17] Serre, J.-P., Représentations l-adiques, *Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976)*, 177–193. Japan Soc. Promotion Sci., Tokyo, 1977.

[18] Shimizu, H., Hokei kansu. I–III. (Japanese) [Automorphic functions. I–III] Second edition. *Iwanami Shoten Kiso Sūgaku [Iwanami Lectures on Fundamental Mathematics], 8. Daisū [Algebra]*, vii. Iwanami Shoten, Tokyo, 1984.

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

[20] Skorobogatov, A., Torsors and rational points, *Cambridge Tracts in Mathematics*, 144, Cambridge University Press, Cambridge, 2001.

[21] Skorobogatov, A., Shimura coverings of Shimura curves and the Manin obstruction, *Math. Res. Lett.*, **12** (2005), no. 5-6, 779–788.

[22] Vignéras, M.-F., Arithmétique des algèbres de quaternions. (French) [Arithmetic of quaternion algebras]. *Lecture Notes in Mathematics*, 800. Springer, Berlin, 1980.