

Algebraic points on Shimura curves of $\Gamma_0(p)$ -type (IV)

By

Keisuke ARAI*

Abstract

In previous articles, we proved that there are no points rational over a fixed number field on the Shimura curve of $\Gamma_0(p)$ -type for every sufficiently large prime number p under a mild assumption. In this article, (1) we generalize the previous result to an infinite family of number fields, and (2) give examples not satisfying the mild assumption as mentioned above.

§ 1. Introduction

Let B be an indefinite quaternion division algebra over \mathbb{Q} , let $d(B)$ be its discriminant, and let M^B be the Shimura curve over \mathbb{Q} associated to B . For a prime number p not dividing $d(B)$, let $M_0^B(p)$ be the Shimura curve of $\Gamma_0(p)$ -type over \mathbb{Q} associated to B . Then there is a natural finite morphism

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

over \mathbb{Q} (see [4, §1]). We see $M^B(\mathbb{R}) = \emptyset$ and $M_0^B(p)(\mathbb{R}) = \emptyset$ by [6, Theorem 0]. Let k be a number field. In previous articles [2], [3], [4], we proved that the set $M_0^B(p)(k)$ of k -rational points is empty for every sufficiently large prime number p under a mild assumption (see §2). In this article, we generalize the previous result to an infinite family of number fields in Theorem 1.1 below. In §3, we prove Theorem 1.1 by a method of classical algebraic number theory. In §4, we give examples not satisfying the mild assumption as mentioned above.

Before stating the main result, we give some notation and convention. A prime \mathfrak{q} of k is of *odd degree* if the residue field of \mathfrak{q} is an extension of \mathbb{F}_q of odd degree, where q is the residue characteristic of \mathfrak{q} . Throughout this article, we assume that all number fields are contained in \mathbb{C} . For simplicity, we say that

Received March 28, 2014. Revised September 30, 2014.

2010 Mathematics Subject Classification(s): 11G18, 14G05.

Key Words: rational points, Shimura curves.

*School of Science and Technology for Future Life, Tokyo Denki University, Tokyo 120-8551, Japan.
e-mail: araik@mail.dendai.ac.jp

- k satisfies NCH if k does not contain the Hilbert class field of any imaginary quadratic field,
- a prime \mathfrak{q} of k satisfies $\text{OD}(B)$ if \mathfrak{q} is of odd degree and its residue characteristic q satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong M_2(\mathbb{Q}(\sqrt{-q}))$, and
- k satisfies $\text{EOD}(B)$ if there is a prime of k satisfying $\text{OD}(B)$.

Here, note that NCH (resp. OD, resp. E) is an abbreviation of “not contain Hilbert” (resp. “odd degree,” resp. “exist”). Let $\mathcal{P}_{\text{OD}(B)}(k)$ be the set of primes of k satisfying $\text{OD}(B)$. We have $\mathcal{P}_{\text{OD}(B)}(k) \neq \emptyset$ if and only if k satisfies $\text{EOD}(B)$. The main result of this article is:

Theorem 1.1. *Suppose that k is Galois over \mathbb{Q} and satisfies NCH, $\text{EOD}(B)$. Let $n \geq 1$ be an integer. Then there are infinitely many extensions k' of k of $[k' : k] = 2^n$ and constants $C(B, k')$ depending on B, k' such that $M_0^B(p)(k') = \emptyset$ for any prime number $p > C(B, k')$.*

In Theorem 1.1, the assumption is important, and the essential part of the proof is to find infinitely many quadratic extensions of k satisfying NCH, $\text{EOD}(B)$.

§ 2. Result for a fixed number field

We review a result in [3]. Let $\mathcal{M}^{\text{new}}(k)$ be the set of prime numbers which split completely in k . Let $\mathcal{N}^{\text{new}}(k)$ be the set of primes of k which divide some prime number in $\mathcal{M}^{\text{new}}(k)$. Fix a finite subset $\emptyset \neq \mathcal{S}^{\text{new}}(k) \subseteq \mathcal{N}^{\text{new}}(k)$ which generates the ideal class group of k . Let h_k (resp. \mathcal{O}_k) be the class number of k (resp. the ring of integers of k). For each prime $\mathfrak{q} \in \mathcal{S}^{\text{new}}(k)$, fix an element $\alpha_{\mathfrak{q}} \in \mathcal{O}_k \setminus \{0\}$ satisfying $\mathfrak{q}^{h_k} = \alpha_{\mathfrak{q}} \mathcal{O}_k$. Let $\mathbf{Ram}(k)$ be the set of prime numbers which are ramified in k . For a prime \mathfrak{q} of k , let $N(\mathfrak{q}) := \sharp(\mathcal{O}_k/\mathfrak{q})$. For an integer $n \geq 1$, let

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

From now to the end of this article, suppose that k is Galois over \mathbb{Q} . Let

$$\begin{aligned} \mathcal{E}(k) &:= \left\{ \varepsilon_0 = \sum_{\sigma \in \text{Gal}(k/\mathbb{Q})} a_{\sigma} \sigma \in \mathbb{Z}[\text{Gal}(k/\mathbb{Q})] \mid a_{\sigma} \in \{0, 8, 12, 16, 24\} \right\}, \\ \mathcal{M}_1^{\text{new}}(k) &:= \{ (\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \mid \mathfrak{q} \in \mathcal{S}^{\text{new}}(k), \varepsilon_0 \in \mathcal{E}(k), \beta_{\mathfrak{q}} \in \mathcal{FR}(N(\mathfrak{q})) \}, \\ \mathcal{M}_2^{\text{new}}(k) &:= \{ \text{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}(\alpha_{\mathfrak{q}}^{\varepsilon_0} - \beta_{\mathfrak{q}}^{24h_k}) \in \mathbb{Z} \mid (\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \in \mathcal{M}_1^{\text{new}}(k) \} \setminus \{0\}, \\ \mathcal{N}_0^{\text{new}}(k) &:= \{ \text{prime divisors of some of the integers in } \mathcal{M}_2^{\text{new}}(k) \}, \\ \mathcal{T}^{\text{new}}(k) &:= \{ \text{prime numbers divisible by some prime in } \mathcal{S}^{\text{new}}(k) \} \cup \{2, 3\}, \\ \mathcal{N}_1^{\text{new}}(k) &:= \mathcal{N}_0^{\text{new}}(k) \cup \mathcal{T}^{\text{new}}(k) \cup \mathbf{Ram}(k). \end{aligned}$$

Note that the set $\mathcal{N}_1^{\text{new}}(k)$ is finite. In this setting, we obtained:

Theorem 2.1 ([3]). *Suppose that k satisfies NCH, EOD(B). Let p be a prime number satisfying $p > \min_{\mathfrak{q} \in \mathcal{P}_{\text{OD}}(B)(k)} 4N(\mathfrak{q})$, $p \nmid 13d(B)$, $p \notin \mathcal{N}_1^{\text{new}}(k)$.*

- (1) *If $B \otimes_{\mathbb{Q}} k \cong M_2(k)$, then $M_0^B(p)(k) = \emptyset$.*
- (2) *If $B \otimes_{\mathbb{Q}} k \not\cong M_2(k)$, then $M_0^B(p)(k) \subseteq \{\text{elliptic points of order 2 or 3}\}$.*

Note that an upper bound of $\mathcal{N}_1^{\text{new}}(k)$ is estimated in [1]. We can easily eliminate elliptic points of $M_0^B(p)(k)$ with the aid of the classification of their fields of moduli as follows:

Proposition 2.2. *Let K be a subfield of \mathbb{C} . If $M_0^B(p)(K)$ has an elliptic point of order 2 (resp. 3), then K contains $\mathbb{Q}(\sqrt{-1})$ (resp. $\mathbb{Q}(\sqrt{-3})$).*

Proof. Let $x \in M_0^B(p)(K)$ be an elliptic point of order 2 (resp. 3). Then x is a CM point by $\mathbb{Z}[\sqrt{-1}]$ (resp. $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$) in the sense of [5, Definition 5.5]. Let $\mathbb{Q}(x)$ be the number field generated over \mathbb{Q} by the coordinates of x on $M_0^B(p)$. Since $M_0^B(p)(\mathbb{Q}) = \emptyset$, we have $\mathbb{Q}(x) \neq \mathbb{Q}$. Then $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{-1})$ (resp. $\mathbb{Q}(\sqrt{-3})$) by [5, Theorem 5.12]. \square

A number field satisfying NCH contains neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-3})$. Therefore:

Theorem 2.3. *Suppose that k satisfies NCH, EOD(B). Then $M_0^B(p)(k) = \emptyset$ for any prime number p satisfying $p > \min_{\mathfrak{q} \in \mathcal{P}_{\text{OD}}(B)(k)} 4N(\mathfrak{q})$, $p \nmid 13d(B)$, $p \notin \mathcal{N}_1^{\text{new}}(k)$.*

§ 3. Proof of Theorem 1.1

Recall that k is a finite Galois extension of \mathbb{Q} . The key to proving Theorem 1.1 is:

Proposition 3.1. *Suppose that k satisfies NCH. Let \mathfrak{q} be a prime of k of odd degree.*

- (1) *There are infinitely many quadratic extensions k' of k such that*
 - (i) *k' is Galois over \mathbb{Q} ,*
 - (ii) *k' satisfies NCH, and*
 - (iii) *there is a prime \mathfrak{q}' of k' of odd degree which divides \mathfrak{q} .*
- (2) *Let $n \geq 1$ be an integer. Then there are infinitely many extensions k' of k of $[k' : k] = 2^n$ such that*
 - (i) *k' is Galois over \mathbb{Q} ,*

- (ii) k' satisfies NCH, and
- (iii) there is a prime \mathfrak{q}' of k' of odd degree which divides \mathfrak{q} .

Corollary 3.2. *Suppose that k satisfies NCH, EOD(B). Let $n \geq 1$ be an integer. Then there are infinitely many extensions k' of k of $[k' : k] = 2^n$ such that*

- (i) k' is Galois over \mathbb{Q} , and
- (ii) k' satisfies NCH, EOD(B).

Proof. Let $\mathfrak{q} \in \mathcal{P}_{\text{OD}(B)}(k)$. Applying Proposition 3.1 (2) to k, \mathfrak{q} , we obtain the result. \square

Theorem 1.1 is a consequence of Theorem 2.3 and Corollary 3.2. More precisely:

Theorem 3.3. *Suppose that k satisfies NCH, EOD(B). Let $n \geq 1$ be an integer. Then there are infinitely many extensions k' of k of $[k' : k] = 2^n$ such that*

- (i) k' is Galois over \mathbb{Q} ,
- (ii) k' satisfies NCH, EOD(B), and
- (iii) $M_0^B(p)(k') = \emptyset$ for any prime number p satisfying $p > \min_{\mathfrak{q}' \in \mathcal{P}_{\text{OD}(B)}(k')} 4N(\mathfrak{q}')$, $p \nmid 13d(B)$, $p \notin \mathcal{N}_1^{\text{new}}(k')$.

The rest of this section is devoted to proving Proposition 3.1. For a prime \mathfrak{q} of k and a finite Galois extension k' of k , let $e_{\mathfrak{q}}(k'/k)$ be the ramification index of \mathfrak{q} in k'/k . From now to the end of this section, suppose that the assumption in Proposition 3.1 holds. Let q be the residue characteristic of \mathfrak{q} . For a non-zero integer $N \in \mathbb{Z}$, consider the following conditions:

- (C1) N is square free.
- (C2) $\left(\frac{N}{q}\right) = 1$ if $q \neq 2$; $N \equiv 1 \pmod{8}$ if $q = 2$.
- (C3) $q \mid N$ if $q \neq 2$; $N \equiv 2, 3 \pmod{4}$ if $q = 2$.

Here, $\left(\frac{N}{q}\right) \in \{0, 1, -1\}$ is the Legendre symbol. For an integer $N \in \mathbb{Z} \setminus \{0\}$ satisfying (C1), let

$$W_N := \mathbb{Q}(\sqrt{N}).$$

Note that if two distinct integers $N_1, N_2 \in \mathbb{Z} \setminus \{0\}$ satisfy (C1), then $W_{N_1} \neq W_{N_2}$.

Lemma 3.4. *Let $N \in \mathbb{Z} \setminus \{0\}$ be an integer satisfying (C1).*

- (1) (i) *We have (C2) if and only if q splits in W_N .*

(ii) We have (C3) if and only if q is ramified in W_N .

(2) Let \mathfrak{q}' be a prime of the composite field kW_N above \mathfrak{q} .

(i) If (C2) holds, then \mathfrak{q}' is of odd degree.

(ii) If (C3) holds and if $2 \nmid e_q(k/\mathbb{Q})$, then \mathfrak{q}' is of odd degree.

Proof. (1) Easy.

(2) If $kW_N = k$, then the assertion is trivial. Assume otherwise i.e. $kW_N \neq k$.

(i) The prime \mathfrak{q} splits in kW_N since q splits in W_N . Therefore \mathfrak{q}' is of odd degree.

(ii) By (1) (ii), we have $e_q(W_N/\mathbb{Q}) = 2$. Since $2 \nmid e_q(k/\mathbb{Q})$, we have $e_q(kW_N/k) = 2$.

Therefore \mathfrak{q}' is of odd degree. \square

Let $\mathcal{V}_{1;2}$ (resp. $\mathcal{V}_{1;2,3}$) be the set of integers $N \in \mathbb{Z} \setminus \{0\}$ satisfying (C1) and (C2) (resp. (C1) and ((C2) or (C3))). Then $\mathcal{V}_{1;2} \subseteq \mathcal{V}_{1;2,3}$.

Lemma 3.5. *We have $\#\mathcal{V}_{1;2} = \infty$ and $\#\mathcal{V}_{1;2,3} = \infty$.*

Proof. It suffices to prove $\#\mathcal{V}_{1;2} = \infty$. This follows from the Dirichlet prime number theorem. \square

Let

$$\mathcal{V} := \begin{cases} \mathcal{V}_{1;2} & \text{if } 2 \mid e_q(k/\mathbb{Q}), \\ \mathcal{V}_{1;2,3} & \text{if } 2 \nmid e_q(k/\mathbb{Q}). \end{cases}$$

Then $\#\mathcal{V} = \infty$. Let

$$\mathcal{V}_0 := \{ N \in \mathcal{V} \mid kW_N \text{ satisfies NCH} \}.$$

Lemma 3.6.

(1) We have $\#\mathcal{V}_0 = \infty$.

(2) We have $\#\{ kW_N \mid N \in \mathcal{V}_0 \text{ and } kW_N \neq k \} = \infty$.

Proof. (1) For any $N \in \mathcal{V} \setminus \mathcal{V}_0$, there is an imaginary quadratic field J_N such that kW_N contains the Hilbert class field H_N of J_N . Since $H_N \not\subseteq k$, we have $k \subsetneq kH_N \subseteq kW_N$. Then $kH_N = kW_N$ and $[kW_N : k] = 2$ because $[W_N : \mathbb{Q}] = 2$. Therefore $h_{J_N} = [H_N : J_N] = \frac{1}{2}[H_N : \mathbb{Q}] \leq \frac{1}{2}[kH_N : \mathbb{Q}] = \frac{1}{2}[kW_N : \mathbb{Q}] = [k : \mathbb{Q}]$. There are only finitely many such imaginary quadratic fields J_N , because their class numbers are bounded above. We also have $kH_N = kW_N \supseteq W_N$. Now, assume $\#\mathcal{V}_0 < \infty$. Then $\#(\mathcal{V} \setminus \mathcal{V}_0) = \infty$. This implies that finitely many number fields contain infinitely many quadratic fields, which is a contradiction.

(2) The assertion follows from (1). \square

Proof of Proposition 3.1. (1) The assertion follows from Lemmas 3.4 (2) and 3.6 (2).

(2) By applying (1) successively, we obtain the result. \square

§ 4. Examples not satisfying the assumption

In this section, we give examples of number fields not satisfying the assumption of Theorem 3.3.

Lemma 4.1. *Let p, q be prime numbers. Assume $p \equiv -1 \pmod{8}$.*

(1) *The following conditions are equivalent:*

- (i) q splits in $\mathbb{Q}(\sqrt{-p})$.
- (ii) ($q \neq 2$ and $\left(\frac{-p}{q}\right) = 1$) or $q = 2$.
- (iii) $\left(\frac{q}{p}\right) = 1$.

(2) *The following conditions are equivalent:*

- (i) q is ramified in $\mathbb{Q}(\sqrt{-p})$.
- (ii) $q = p$.
- (iii) $\left(\frac{q}{p}\right) = 0$.

(3) *The following conditions are equivalent:*

- (i) q is inert in $\mathbb{Q}(\sqrt{-p})$.
- (ii) $\left(\frac{q}{p}\right) = -1$.

Proof. (1) Since $p \equiv -1 \pmod{8}$, the prime number 2 splits in $\mathbb{Q}(\sqrt{-p})$ and we have $\left(\frac{2}{p}\right) = 1$. Suppose $q \neq 2$. Then $\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) (-1)^{\frac{(p-1)(q-1)}{4}} = \left(\frac{q}{p}\right)$. Here, the last equality holds because $p \equiv -1 \pmod{4}$. Then the assertion holds.

(2) The discriminant of $\mathbb{Q}(\sqrt{-p})$ is $-p$, as required.

(3) The assertion follows from (1) and (2). \square

Let p_1, p_2 be distinct prime numbers satisfying

$$p_1 \equiv -1 \pmod{8}, \quad p_2 \equiv -1 \pmod{8},$$

and let

$$k_{p_1, p_2} := \mathbb{Q}(\sqrt{-p_1}, \sqrt{-p_2}).$$

Fix a prime number q . Let e_q (resp. f_q , resp. g_q) be the ramification index of q in $k_{p_1, p_2}/\mathbb{Q}$ (resp. the degree of the residue field extension above q in $k_{p_1, p_2}/\mathbb{Q}$, resp. the number of primes of k_{p_1, p_2} above q).

Lemma 4.2.

(1) *The following conditions are equivalent:*

- (i) f_q is odd.
- (ii) $f_q = 1$.
- (iii) $(e_q, f_q, g_q) = (1, 1, 4)$ or $(2, 1, 2)$.

(2) *The following conditions are equivalent:*

- (i) $(e_q, f_q, g_q) = (1, 1, 4)$.
- (ii) q splits in both $\mathbb{Q}(\sqrt{-p_1})$ and $\mathbb{Q}(\sqrt{-p_2})$.
- (iii) $\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_2}\right) = 1$.

(3) *The following conditions are equivalent:*

- (i) $(e_q, f_q, g_q) = (2, 1, 2)$.
- (ii) (q is ramified in $\mathbb{Q}(\sqrt{-p_1})$ and splits in $\mathbb{Q}(\sqrt{-p_2})$) or (q splits in $\mathbb{Q}(\sqrt{-p_1})$ and is ramified in $\mathbb{Q}(\sqrt{-p_2})$).
- (iii) $\left(\left(\frac{q}{p_1}\right) = 0 \text{ and } \left(\frac{q}{p_2}\right) = 1\right)$ or $\left(\left(\frac{q}{p_1}\right) = 1 \text{ and } \left(\frac{q}{p_2}\right) = 0\right)$.

Proof. (1) If $(e_q, f_q, g_q) = (4, 1, 1)$, then q is ramified in both $\mathbb{Q}(\sqrt{-p_1})$ and $\mathbb{Q}(\sqrt{-p_2})$. By Lemma 4.1 (2), we have $q = p_1 = p_2$. This is a contradiction. Therefore $(e_q, f_q, g_q) \neq (4, 1, 1)$, and the assertion holds.

(2), (3) The assertion follows from Lemma 4.1 (1), (2). \square

Lemma 4.3. *If $d(B) = p_1 p_2$, then the following conditions are equivalent:*

- (i) $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong M_2(\mathbb{Q}(\sqrt{-q}))$.
- (ii) At least one of p_1, p_2 splits in $\mathbb{Q}(\sqrt{-q})$.
- (iii) $\left(\frac{-q}{p_1}\right) = 1$ or $\left(\frac{-q}{p_2}\right) = 1$.

$$(iv) \left(\frac{q}{p_1}\right) = -1 \text{ or } \left(\frac{q}{p_2}\right) = -1.$$

Proof. For $i = 1, 2$, we have $\left(\frac{-1}{p_i}\right) = -1$ since $p_i \equiv -1 \pmod{4}$. Then (iii) and (iv) are equivalent. The rest is obvious (cf. Lemma 3.4 (1) (i)). \square

Concerning EOD(B), we have:

Proposition 4.4. *If $d(B) = p_1 p_2$, then k_{p_1, p_2} does not satisfy EOD(B).*

Proof. The assertion follows from Lemmas 4.2 and 4.3. \square

As for NCH, we have:

Proposition 4.5. *The following conditions are equivalent:*

- (i) k_{p_1, p_2} does not satisfy NCH.
- (ii) $h_{\mathbb{Q}(\sqrt{-p_1})} = 1$ or $h_{\mathbb{Q}(\sqrt{-p_2})} = 1$.
- (iii) $p_1 = 7$ or $p_2 = 7$.

Proof. [(i) \implies (ii)] Let $H(i)$ be the Hilbert class field of $\mathbb{Q}(\sqrt{-p_i})$ for $i = 1, 2$. By the assumption, we have $k_{p_1, p_2} \supseteq H(1)$ or $H(2)$. We may assume $k_{p_1, p_2} \supseteq H(1)$. Suppose $h_{\mathbb{Q}(\sqrt{-p_1})} \neq 1$. Then $H(1) \not\supseteq \mathbb{Q}(\sqrt{-p_1})$, and so $k_{p_1, p_2} = H(1)$. Let \mathfrak{p}_2 be a prime of $\mathbb{Q}(\sqrt{-p_1})$ above p_2 . Since p_2 is unramified in $\mathbb{Q}(\sqrt{-p_1})/\mathbb{Q}$, the prime \mathfrak{p}_2 is ramified in $k_{p_1, p_2}/\mathbb{Q}(\sqrt{-p_1})$. This contradicts $k_{p_1, p_2} = H(1)$. Therefore $h_{\mathbb{Q}(\sqrt{-p_1})} = 1$.

[(ii) \implies (i)] Clear.

[(ii) \iff (iii)] All the imaginary quadratic fields of class number one are $\mathbb{Q}(\sqrt{-N})$, where $N \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Then the assertion holds. \square

Acknowledgements

The author would like to thank the organizers Tadashi Ochiai, Takeshi Tsuji and Iwao Kimura for giving him an opportunity to talk at the conference.

References

- [1] Arai, K., An effective bound of p for algebraic points on Shimura curves of $\Gamma_0(p)$ -type, *Acta Arith.* **164** (2014), 343–353.
- [2] Arai, K., Algebraic points on Shimura curves of $\Gamma_0(p)$ -type (II), *Manuscripta Math.*, published online.

- [3] Arai, K., Algebraic points on Shimura curves of $\Gamma_0(p)$ -type (III), *preprint*, available at the web page (<http://arxiv.org/pdf/1303.5270v1.pdf>).
- [4] Arai, K. and Momose, F., Algebraic points on Shimura curves of $\Gamma_0(p)$ -type, *J. Reine Angew. Math.* **690** (2014), 179–202.
- [5] González, J. and Rotger, V., Non-elliptic Shimura curves of genus one, *J. Math. Soc. Japan* **58** (2006), no. 4, 927–948.
- [6] Shimura, G., On the real points of an arithmetic quotient of a bounded symmetric domain, *Math. Ann.* **215** (1975), 135–164.