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

Keisuke Arai

Received: 23 June 2015 / Accepted: 16 December 2015 / Published online: 23 February 2016
© Springer Science+Business Media New York 2016

Abstract In previous works, we proved that under a certain assumption, the set of rational points over a number field on the Shimura curve of $\Gamma_0(p)$-type consists of at most elliptic points for every sufficiently large prime number $p$. In this article, we relax the assumption of the previous result and prove the non-existence of elliptic points under a mild extra assumption.

Keywords Rational points · Shimura curves · QM-abelian surfaces · Galois representations

Mathematics Subject Classification 11G18 · 14G05

1 Introduction

Let $p$ be a prime number, and let $Y_0(p)$ be the affine modular curve over $\mathbb{Q}$ classifying the isomorphism classes of $(E, C)$, where $E$ is an elliptic curve and $C$ is a (cyclic) subgroup of $E$ of order $p$ (cf. [8]). Let $X_0(p)$ be the smooth compactification of $Y_0(p)$. Then by [11, Theorem 7.1], we have $X_0(p)(\mathbb{Q}) = \{ \text{cusps} \}$ if $p > 163$. This result was expanded to quadratic fields in [12, Theorem B].

Let $B$ be an indefinite quaternion division algebra over $\mathbb{Q}$ of discriminant $d$. In the following, we assume $p \nmid d$. Fix a maximal order $\mathcal{O}$ of $B$. Let $M^B$ (resp. $M_0^B(p)$) be the Shimura curve (resp. the Shimura curve of $\Gamma_0(p)$-type) over $\mathbb{Q}$ associated to $B$ (cf. [5,9]). Then $M^B$ classifies the isomorphism classes of QM-abelian surfaces $(A, i)$ by...
$O$, where $A$ is a two-dimensional abelian variety and $i$ is an embedding of $O$ into the endomorphism ring of $A$. Here, we assume that $A$ has a left $O$-action. Also, $M^B_0(p)$ classifies the isomorphism classes of $(A, i, V)$, where $(A, i)$ is a QM-abelian surface by $O$ and $V$ is a left $O$-submodule of $A[p] = \ker([p] : A \to A)$ of $\mathbb{F}_p$-dimension 2. Note that there is a natural map

$$\pi^B(p) : M^B_0(p) \to M^B$$

defined over $\mathbb{Q}$ given by $(A, i, V) \mapsto (A, i)$.

We can view $M^B_0(p)$ as an analogue of $X_0(p)$. The set of rational points over a number field $k$ on $M^B_0(p)$ is expected to become small if $p$ increases. In previous works [3,5], we proved that under a certain assumption, $M^B_0(p)(k)$ consists of at most elliptic points (in the sense of [14, §1.5]) if $p$ is sufficiently large. In this article, (1) we relax the assumption of the previous result (see Theorem 5.4) and (2) prove the non-existence of elliptic points under a mild extra assumption (see Theorem 1.1). Note that Theorem 5.4 will be applied in [4] to give an infinite family $\{k\}'$ of number fields such that $M^B_0(p)(k)' = \emptyset$ if $p$ is sufficiently large (depending on $B$ and $k'$).

We say that a prime of a number field is of odd degree if the cardinality of the residue field is an odd power of the residue characteristic. The main result of this article is:

**Theorem 1.1** Let $k$ be a finite Galois extension of $\mathbb{Q}$ which does not contain the Hilbert class field of any imaginary quadratic field. Assume that there is a prime $q$ of $k$ such that $q$ is of odd degree, the residue characteristic $q$ of $q$ is unramified in $k$, and $B \otimes_\mathbb{Q} \mathbb{Q}(\sqrt{-q}) \cong M_2(\mathbb{Q}(\sqrt{-q}))$. Then there is a constant $C(B, k, q)$ depending on $B, k, q$ such that $M^B_0(p)(k) = \emptyset$ if $p > C(B, k, q)$.

We prove Theorem 1.1 in §6. The idea of the proof is to extend $k$ so that it satisfies $B \otimes_\mathbb{Q} k \cong M_2(k)$ (cf. Theorem 5.4). This seems somewhat strange because the set of rational points tends to grow if $k$ becomes larger.

**Remark 1.2** By [15, Theorem 0], we have $M^B(\mathbb{R}) = \emptyset$. Since there is a map $\pi^B(p) : M^B_0(p) \to M^B$ defined over $\mathbb{Q}$, we have $M^B_0(p)(\mathbb{R}) = \emptyset$ for any $p$.

**Notations**

- $F$: a field,
- $\text{char } F$: the characteristic of $F$,
- $\overline{F}$: an algebraic closure of $F$,
- $F^{\text{sep}}$: the separable closure of $F$ inside $\overline{F}$,
- $F^{\text{ab}}$: the maximal abelian extension of $F$ inside $\overline{F}$,
- $G_F = \text{Gal}(F^{\text{sep}}/F)$,
- $G_F^{\text{ab}} = \text{Gal}(F^{\text{ab}}/F)$,
- $\theta_p : G_F \to \mathbb{F}_p^\times$: the mod $p$ cyclotomic character, where $\text{char } F \neq p$,
- $k$: a number field,
- $\mathcal{O}_k$: the integer ring of $k$,
- $\kappa(q)$: the residue field of $q$, where $q$ is a prime of $k$,
• $N(q)$: the cardinality of $\kappa(q)$,
• $Cl_k$: the ideal class group of $k$,
• $h_k$: the class number of $k$,
• $\overline{u}$: the complex conjugate of $u \in \mathbb{C}$,
• fix an inclusion $k \hookrightarrow \mathbb{C}$ and take the algebraic closure $\overline{k}$ inside $\mathbb{C}$,
• $k_v$: the completion of $k$ at $v$, where $v$ is a place (or a prime) of $k$,
• $\text{Ram}(k)$: the set of prime numbers which are ramified in $k$.

2 Basics of QM-abelian surfaces

We briefly review [5, §2–3] in order to consider the automorphism groups and the Galois representations associated to QM-abelian surfaces. Let $(A, i)$ be a QM-abelian surface by $O$ over $F$ (i.e., $A$ is a two-dimensional abelian variety over $F$ and $i$ is an embedding of $O$ into the endomorphism ring $\text{End}_F(A)$ of $A$ over $F$). Let $\text{End}_O(A)$ (resp. $\text{Aut}_O(A)$) be the endomorphism ring (resp. the automorphism group) of $A$ over $F$, and let

$$\text{End}_O(A) := \{ f \in \text{End}(A) | f \circ i(g) = i(g) \circ f \text{ for any } g \in O \},$$
$$\text{Aut}_O(A) := \text{Aut}(A) \cap \text{End}_O(A).$$

If $\text{char } F = 0$, then $\text{Aut}_O(A) \cong \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z},$ or $\mathbb{Z}/6\mathbb{Z}$.

Assume $\text{char } F \neq p$. Then the action of $G_F$ on $A[p](F^{\text{sep}}) \cong \mathbb{F}_p^d$ determines a Galois representation $\overline{\rho} : G_F \rightarrow \text{GL}_4(\mathbb{F}_p)$. By a suitable choice of basis, $\overline{\rho}$ factors as

$$\overline{\rho} : G_F \rightarrow \left\{ \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix} \Bigg| \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \text{GL}_2(\mathbb{F}_p) \right\} \subseteq \text{GL}_4(\mathbb{F}_p),$$

where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Let

$$\overline{\rho}_{A,p} : G_F \rightarrow \text{GL}_2(\mathbb{F}_p)$$

be the Galois representation induced from $\overline{\rho}$ by $\begin{pmatrix} s & t \\ u & v \end{pmatrix}$, so that $\overline{\rho}_{A,p}(\sigma) = \begin{pmatrix} s(\sigma) & t(\sigma) \\ u(\sigma) & v(\sigma) \end{pmatrix}$ for any $\sigma \in G_F$ if $\overline{\rho}(\sigma) = \begin{pmatrix} s(\sigma)I_2 & t(\sigma)I_2 \\ u(\sigma)I_2 & v(\sigma)I_2 \end{pmatrix}$.

Let $V$ be a left $O$-submodule of $A[p](F^{\text{sep}})$ of $\mathbb{F}_p$-dimension 2. Define a subgroup $\text{Aut}_O(A, V)$ of $\text{Aut}_O(A)$ by

$$\text{Aut}_O(A, V) := \{ f \in \text{Aut}_O(A) | f(V) = V \}.$$

If $\text{char } F = 0$, then $\text{Aut}_O(A, V) \cong \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z},$ or $\mathbb{Z}/6\mathbb{Z}$. Note that we have $\text{Aut}_O(A) \cong \mathbb{Z}/2\mathbb{Z}$ (resp. $\text{Aut}_O(A, V) \cong \mathbb{Z}/2\mathbb{Z}$) if and only if $\text{Aut}_O(A) = \{ \pm 1 \}$ (resp. $\text{Aut}_O(A, V) = \{ \pm 1 \}$).
Suppose that $V$ is stable under the action of $G_F$. Then there is a unique character
\[ \lambda : G_F \longrightarrow \mathbb{F}_p^\times \]
such that $\overline{\rho}(\sigma)(v) = \lambda(\sigma)v$ for any $\sigma \in G_F$, $v \in V$. By conjugating if necessary, we have $\overline{\rho}_{A,p}(\sigma) = \left( \begin{array}{cc} \lambda(\sigma) & * \\ 0 & * \end{array} \right)$ for any $\sigma \in G_F$.

3 Fields of definition

We recall from [5, §4] some facts about the field of definition of a point of $M^B_0(p)(k)$. Fix a point
\[ x \in M^B_0(p)(k). \]
Let $x' \in M^B(k)$ be the image of $x$ by the map $\pi^B(p) : M^B_0(p) \longrightarrow M^B$. Then $x'$ is represented by a QM-abelian surface (say $(A_x, i_x)$) by $\mathcal{O}$ over $\overline{k}$, and $x$ is represented by a triple $(A_x, i_x, V_x)$ where $V_x$ is a left $\mathcal{O}$-submodule of $A[p](\overline{k})$ of dim $\mathbb{F}_p V_x = 2$.

For any $\sigma \in G_k$, we have an isomorphism between $(A_x, i_x)$ and $(\sigma(A_x), i_x)$ so that $V$ corresponds to $V_x$ under this isomorphism. Let
\[ \text{Aut}(x) := \text{Aut}_\mathcal{O}(A_x, V_x), \quad \text{Aut}(x') := \text{Aut}_\mathcal{O}(A_x). \]

Then Aut$(x)$ is a subgroup of Aut$(x')$. Note that $x$ is an elliptic point of order 2 (resp. order 3) if and only if Aut$(x)$ $\cong \mathbb{Z}/4\mathbb{Z}$ (resp. Aut$(x)$ $\cong \mathbb{Z}/6\mathbb{Z}$). Since $x$ is a $k$-rational point, we have $\sigma x = x$ for any $\sigma \in G_k$. Then for any $\sigma \in G_k$, there is an isomorphism
\[ \phi_\sigma : \sigma(A_x, i_x, V_x) \longrightarrow (A_x, i_x, V_x), \]
which we fix once for all. For $\sigma, \tau \in G_k$, let
\[ c_x(\sigma, \tau) := \phi_\sigma \circ \sigma \circ \phi^{-1}_\tau \in \text{Aut}(x). \]

Then $c_x$ is a 2-cocycle and defines the cohomology class $[c_x] \in H^2(G_k, \text{Aut}(x))$. Here, the action of $G_k$ on Aut$(x)$ is defined in a natural manner (cf. [5, §4]). For a place $v$ of $k$, let $[c_x]_v \in H^2(G_{k_v}, \text{Aut}(x))$ be the restriction of $[c_x]$ to $G_{k_v}$.

**Proposition 3.1** [5, Proposition 4.2]

1. Suppose $B \otimes \mathbb{Q} k \cong M_2(k)$. Further, assume Aut$(x) \neq \{ \pm 1 \}$ or Aut$(x') \neq \mathbb{Z}/4\mathbb{Z}$. Then we can take $(A_x, i_x, V_x)$ to be defined over $k$.

2. Assume Aut$(x) = \{ \pm 1 \}$. Then there is a quadratic extension $K$ of $k$ such that we can take $(A_x, i_x, V_x)$ to be defined over $K$.
Lemma 3.2 [5, Lemma 4.3] Let $K$ be a quadratic extension of $k$. Assume $\text{Aut}(x) = \{ \pm 1 \}$. Then the following conditions are equivalent:

1. We can take $(A_x, i_x, V_x)$ to be defined over $K$.
2. For any place $v$ of $k$ satisfying $[c_x]_v \neq 0$, the tensor product $K \otimes_k k_v$ is a field.

4 Classification of characters

We keep the notations from §3. Throughout this section, we assume $\text{Aut}(x) = \{ \pm 1 \}$. Let $K$ be a quadratic extension of $k$ which satisfies the equivalent conditions in Lemma 3.2. Then $x$ is represented by a triple $(A, i, V)$, where $(A, i)$ is a QM-abelian surface by $\mathcal{O}$ over $K$ and $V$ is a left $\mathcal{O}$-submodule of $A[p](\bar{k})$ of $\dim_{\mathbb{F}_p} V = 2$ which is stable under the action of $G_K$. Let

$$\lambda : G_K \rightarrow \mathbb{F}_p^\times$$

be the character associated to $V$ in (2) and $\lambda^{ab} : G_K^{ab} \rightarrow \mathbb{F}_p^\times$ be the natural map induced by $\lambda$. Let $\text{tr}_{K/k} : G_k \rightarrow G_K^{ab}$ be the transfer map, and let

$$\varphi := \lambda^{ab} \circ \text{tr}_{K/k} : G_k \rightarrow \mathbb{F}_p^\times.$$  \hspace{1cm} (3)

Then by [5, Lemma 5.1] (resp. [5, Corollary 5.2]), the character $\lambda^{12}$ (resp. $\varphi^{12}$) is unramified outside $p$, and so it is identified with a character of the ideal group $\mathfrak{I}_K(p)$ (resp. $\mathfrak{I}_k(p)$) consisting of non-zero fractional ideals of $K$ (resp. $k$) prime to $p$. Also, $\theta_p : G_K \rightarrow \mathbb{F}_p^\times$ (resp. $\theta_p : G_k \rightarrow \mathbb{F}_p^\times$) is identified with a character of $\mathfrak{I}_K(p)$ (resp. $\mathfrak{I}_k(p)$).

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 $q \in \mathcal{M}^\text{new}(k)$. Fix a finite subset $\emptyset \neq \mathcal{S}^\text{new}(k) \subseteq \mathcal{N}^\text{new}(k)$ which generates $\mathcal{C}_k$. For each prime $q \in \mathcal{S}^\text{new}(k)$, fix an element $\alpha_q \in \mathcal{O}_k \setminus \{ 0 \}$ satisfying $q^{hk} = \alpha_q \mathcal{O}_k$. For an integer $n \geq 1$, let

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

For any element $\beta \in \mathcal{F}_n(n)$, we have $|\beta| = \sqrt{n}$. From now until the end of this article, we suppose that $k$ is Galois over $\mathbb{Q}$. Let

$$\mathcal{E}(k) := \left\{ \varepsilon_0 = \sum_{\sigma \in \text{Gal}(k/\mathbb{Q})} a_\sigma \sigma \in \mathbb{Z}[\text{Gal}(k/\mathbb{Q})] \mid a_\sigma \in \{ 0, 8, 12, 16, 24 \} \right\},$$

$$\mathcal{M}^\text{new}(k) := \left\{ (q, \varepsilon_0, \beta_q) \mid q \in \mathcal{S}^\text{new}(k), \varepsilon_0 \in \mathcal{E}(k), \beta_q \in \mathcal{F}_n(N(q)) \right\},$$

$$\mathcal{M}_2^\text{new}(k) := \left\{ \text{Norm}_{k(\beta_q)/\mathbb{Q}}(a_q^{\varepsilon_0} - \beta_q^{24h^r}) \in \mathbb{Z} \mid (q, \varepsilon_0, \beta_q) \in \mathcal{M}_1^\text{new}(k) \right\} \setminus \{ 0 \},$$

$$\mathcal{N}_0^\text{new}(k) := \{ \text{prime divisors of some of the integers in } \mathcal{M}_2^\text{new}(k) \},$$

$$\mathcal{T}^\text{new}(k) := \{ \text{prime numbers divisible by some prime in } \mathcal{S}^\text{new}(k) \} \cup \{ 2, 3 \},$$

$$\mathcal{N}_1^\text{new}(k) := \mathcal{N}_0^\text{new}(k) \cup \mathcal{T}^\text{new}(k) \cup \mathcal{R}(k).$$
Note that all the sets $\mathcal{F}(n), E(k), M_1^{\text{new}}(k), M_2^{\text{new}}(k), M_0^{\text{new}}(k), T^{\text{new}}(k),$ and $N_1^{\text{new}}(k)$ are finite. In [2], an upper bound of $N_1^{\text{new}}(k)$ is given. We have the following classification of $\varphi$:

**Theorem 4.1** [2, Theorem 5.1] If $p \notin N_1^{\text{new}}(k)$, then the possible character $\varphi : G_k \rightarrow \mathbb{F}_p^\times$ is of one of the following types:

Type 2. $\varphi^{12} = \theta_p^{12}$ and $p \equiv 3 \mod 4$.

Type 3. There is an imaginary quadratic field $L$ satisfying the following conditions:

(a) The Hilbert class field $H_L$ of $L$ is contained in $k$.

(b) There is a prime $p_L$ of $L$ above $p$ such that $\varphi^{12}(a) \equiv \delta_p^2 \mod p_L$ for any fractional ideal $a \neq (0)$ of $k$ prime to $p$. Here, $\delta_p \in L^\times$ is any element satisfying $\text{Norm}_{k/L}(a) = \delta_p \mathcal{O}_L$.

**Lemma 4.2** [2, Lemma 5.2] Suppose $p \geq 11$, $p \neq 13$, and $p \notin N_1^{\text{new}}(k)$. Further, assume that the following conditions hold:

(a) Every prime of $k$ above $p$ is inert in $K/k$.

(b) Every prime of $k$ in $\mathcal{S}^{\text{new}}(k)$ is ramified in $K/k$.

If $\varphi$ is of type 2, then

(i) the character $\lambda^{12} \phi^{-6} : G_K \rightarrow \mathbb{F}_p^\times$ is unramified everywhere; and

(ii) the map $\text{Cl}_K \rightarrow \mathbb{F}_p^\times$ induced by $\lambda^{12} \phi^{-6}$ is trivial on $C_{K/k} := \text{Im}(\text{Cl}_k \rightarrow \text{Cl}_K)$, where $C_{cl} \rightarrow C_{K}$ is the map defined by $[\alpha] \mapsto [aO_K]$.

From now until the end of this section, we suppose that $p \geq 11$, $p \neq 13$, $p \notin N_1^{\text{new}}(k)$, and that $\varphi$ is of type 2. Let $q \neq p$ be a prime number, and fix a prime $q$ of $k$ above $p$. By [5, Lemma 5.3], the character $\varphi^{12}$ does not depend on the choice of $K$. Then, by replacing $K$ if necessary, we may assume that the conditions (a) and (b) in Lemma 4.2 hold and that $\varphi$ is ramified in $K/k$ (cf. [5, Remark 4.4]). Let $Q_K$ be the unique prime of $K$ above $q$. The abelian surface $A \otimes_k Q_K$ has good reduction over a totally ramified finite extension $M/Q_K$ (see [9, Proposition 3.2]). Let $\tilde{A}$ be the special fiber of the Néron model of $A \otimes_k M$ and $\tilde{i} : \tilde{O} \hookrightarrow \text{End}_{k(q)}(\tilde{A})$ be the map induced by $i$. Then $(\tilde{A}, \tilde{i})$ is a QM-abelian surface by $O$ over $k(q)$. Let $\text{Frob}_M$ be a Frobenius element in $G_M(\subseteq G_{k/q})$. By [9, p. 97], there is an element $a \in \mathbb{Z}$ such that $|a| \leq 2\sqrt{|q|}$ and $\det(T - \overline{\beta}_{A,p}(\text{Frob}_M)) \equiv T^2 - aT + N(q) \mod p$. Let $\beta, \overline{\beta} \in \mathbb{C}$ be the roots of $T^2 - aT + N(q) = 0$. Then $\beta, \overline{\beta} \in \mathcal{F}(N(q))$ and $(T - \lambda(\text{Frob}_M))(T - *) \equiv (T - \beta)(T - \overline{\beta}) \mod p$. Fix a prime $p_0$ of $\mathbb{Q}^\text{cycl}(q)$ above $p$. Then $\lambda(\text{Frob}_M) \equiv \beta \mod p_0$. By replacing $\overline{\beta}$ with $\beta$ if necessary, we may assume $\lambda(\text{Frob}_M) \equiv \beta \mod p_0$. Note that $\beta$ is an eigenvalue of the Frobenius endomorphism of $\tilde{A}$ relative to $k(q)$. Since $\det(\overline{\beta}_{A,p}) = \theta_p$ (cf. [13, Proposition 1.1(2)]), we have $(\lambda^{-1} \theta_p)(\text{Frob}_M) \equiv \overline{\beta} \mod p_0$. Let
\[ \psi := \lambda \theta_p^{-\frac{p+1}{2}} : G_K \rightarrow \mathbb{F}_p^\times. \]

Then \( \psi^{12} = \lambda^{12} \theta_p^{-3(p+1)} = \lambda^{12} \theta_p^{-6}. \)

**Lemma 4.3** (1) \( \psi(F(\text{Frob}_M))^6 = 1. \)
(2) \( \psi(F(\text{Frob}_M))^2 + \psi(F(\text{Frob}_M))^{-2} = -1 \) or 2.
(3) \( \beta^2 + \overline{\beta}^2 \equiv -N(q)^{\frac{p+1}{2}} \) or \( 2N(q)^{\frac{p+1}{2}} \mod p. \)

**Proof** (1) By Lemma 4.2(ii), we have \( 1 = \lambda^{12}(q \mathcal{O}_K)\theta_p^{-6}(q \mathcal{O}_K) = \psi^{12}(q \mathcal{O}_K) = \psi^{24}(q_K) = \psi^{24}(\text{Frob}_M) = (\psi(\text{Frob}_M)^3)^8. \) Note that the fourth equality holds because the extension \( M/K_{\mathcal{O}_K} \) is totally ramified. Then the order of \( \psi(\text{Frob}_M)^3 \) divides gcd\( (8, p - 1) \) because \( (\psi(\text{Frob}_M)^3)^{p-1} = 1. \) Since \( p \equiv 3 \mod 4, \) we have gcd\( (8, p - 1) = 2. \) Therefore \( \psi(\text{Frob}_M)^6 = 1. \)

(2) This follows immediately from (1).

(3) We have \( \beta \equiv \lambda(\text{Frob}_M) = (\psi \theta_p^{\frac{p+1}{2}})(\text{Frob}_M) \mod p_0 \) and \( \overline{\beta} \equiv (\lambda^{-1} \theta_p)(\text{Frob}_M) = (\psi^{-1} \theta_p^{\frac{p+1}{2}})(\text{Frob}_M) \mod p_0. \) Then \( \beta^2 + \overline{\beta}^2 \equiv \psi(\text{Frob}_M)^2 \theta_p(\text{Frob}_M)^{\frac{p+1}{2}} + \psi(\text{Frob}_M)^{-2} \theta_p(\text{Frob}_M)^{-\frac{p+1}{2}} = \theta_p(\text{Frob}_M)^{\frac{p+1}{2}} (\psi(\text{Frob}_M)^2 + \psi(\text{Frob}_M)^{-2}) \equiv -N(q)^{\frac{p+1}{2}} \) or \( 2N(q)^{\frac{p+1}{2}} \mod p. \)

We repeat the argument in [3, §3] when \( q \) is of odd degree as follows:

**Lemma 4.4** Suppose that \( q \) is of odd degree and that \( N(q) < \frac{p}{4}. \) Then

(1) \( N(q)^{\frac{p-1}{2}} \equiv -1 \mod p; \)
(2) \( \beta + \overline{\beta} \equiv 3N(q) \text{ or } 0 \mod p; \)
(3) \( q = 3 \) and \( |\beta + \overline{\beta}| = \sqrt{3N(q)}, \) or \( \beta + \overline{\beta} = 0; \) and
(4) \( B \otimes \mathbb{Q}(\sqrt{-q}) \cong M_2(\mathbb{Q}(\sqrt{-q})). \)

**Proof** (1) Assume \( N(q)^{\frac{p-1}{2}} \equiv 1 \mod p. \) Then Lemma 4.3(3) implies \( \beta^2 + \overline{\beta}^2 \equiv -N(q) \) or \( 2N(q) \mod p. \) Since \( \beta \in \mathcal{F}(N(q)), \) we have \( \beta \overline{\beta} = N(q) \) and \( |\beta + \overline{\beta}| \leq 2 \sqrt{N(q)}. \) Then \( \beta + \overline{\beta} \equiv N(q) \) or \( 4N(q) \mod p. \) We also have \( |(\beta + \overline{\beta})^2 - N(q)| \leq 3N(q) < p \) and \( |(\beta + \overline{\beta})^2 - 4N(q)| \leq 4N(q) < p. \) Then \( (\beta + \overline{\beta})^2 = N(q) \) or \( 4N(q). \) Since \( q \) is of odd degree, this contradicts \( \beta + \overline{\beta} \in \mathbb{Z}. \) Therefore \( N(q)^{\frac{p-1}{2}} \equiv -1 \mod p. \)

(2) By (1) and Lemma 4.3(3), we have \( \beta^2 + \overline{\beta}^2 \equiv N(q) \) or \( -2N(q) \mod p. \) Therefore \( \beta + \overline{\beta} \equiv 3N(q) \) or \( 0 \mod p. \)

(3) We have \( (\beta + \overline{\beta})^2 \leq 4N(q). \) First, assume \( (\beta + \overline{\beta})^2 \equiv 3N(q) \mod p. \) Then \( (\beta + \overline{\beta})^2 = 3N(q) \) since \( |(\beta + \overline{\beta})^2 - 3N(q)| \leq 3N(q) < p. \) Therefore \( q = 3 \) and \( |\beta + \overline{\beta}| = \sqrt{3N(q)}. \) Next, assume \( (\beta + \overline{\beta})^2 \equiv 0 \mod p. \) Then \( (\beta + \overline{\beta})^2 = 0 \) since \( (\beta + \overline{\beta})^2 \leq 4N(q) < p. \) Therefore \( \beta + \overline{\beta} = 0. \)

(4) The number \( \beta \) is an eigenvalue of the Frobenius endomorphism of \( \tilde{A} \) relative to \( \kappa(q), \) where \( q \) is of odd degree. Then by (3) and [9, Theorem 2.1(2)(4) and Proposition 2.3], we conclude \( \text{End}_{\kappa(q)}(\tilde{A}) \otimes \mathbb{Z} \cong M_2(\mathbb{Q}(\sqrt{-q})) \cong B \otimes \mathbb{Q}(\sqrt{-q}). \)

\( \square \)
5 Irreducibility of $\overline{\rho}_{A,p}$ and algebraic points on $M_0^B(p)$

Let $(A, i)$ be a QM-abelian surface by $O$ over $k$. Assume that the representation $\overline{\rho}_{A,p} : G_k \rightarrow \text{GL}_2(\mathbb{F}_p)$ in (1) is reducible. Then there is a one-dimensional subrepresentation of $\overline{\rho}_{A,p}$. Let

$$\nu : G_k \rightarrow \mathbb{F}_p^\times$$

be its associated character. Then by [5, Lemma 6.1], $\nu^{12}$ is unramified outside $p$, and so it is identified with a character of $\mathbb{J}_k(p)$. In this case, note that there is a left $O$-submodule $V$ of $A[p](\overline{k})$ of $\text{dim}_{\mathbb{F}_p} V = 2$ on which $G_k$ acts by $\nu$, and so the triple $(A, i, V)$ determines a point $x \in M_0^B(p)(k)$. We have the following classification of $\nu$:

**Theorem 5.1** If $p \notin N_1^{\text{new}}(k)$, then the possible character $\nu$ is of one of the following types:

Type 2'. $\nu^{24} = \theta_p^{12}$ and $p \equiv 3 \mod 4$.

Type 3. There is an imaginary quadratic field $L$ satisfying the following conditions:

(a) The Hilbert class field $H_L$ of $L$ is contained in $k$.

(b) There is a prime $p_L$ of $L$ above $p$ such that $\nu^{12}(a) \equiv \delta_a^{12} \mod p_L$ for any fractional ideal $a \neq (0)$ of $k$ prime to $p$. Here, $\delta_a \in L^\times$ is any element satisfying $\text{Norm}_{k/L}(a) = \delta_a^qG_L$.

**Proof** We repeat the argument in [5] with some modifications. Assume $p \notin T^{\text{new}}(k) \cup \text{Ram}(k)$. Then $p \geq 5$ and $p$ is unramified in $k$. Let $q \in S^{\text{new}}(k)$, and let $q$ be its residue characteristic. Then $p \neq q$, and $q$ splits completely in $k$. There is a totally ramified finite extension $M(q)$ of $k_q$ such that $A \otimes_k M(q)$ has good reduction, and let $\tilde{A}$ be the special fiber of its Néron model. Then $\tilde{A}$ is defined over $k(q) = \mathbb{F}_q$. Let $\text{Frob}_{M(q)} \in G_{M(q)}(\subseteq G_{k_q} \subseteq G_k)$ be a Frobenius element. Then $\nu^{12}(q) = \nu(\text{Frob}_{M(q)})^{12}$. There is an element $\beta_q \in \mathcal{F}_R(q)$ and a prime $p_q$ of $\mathbb{Q}(\beta_q)$ above $p$ such that $\nu(\text{Frob}_{M(q)}) \equiv \beta_q \mod p_q$. Here, $\beta_q$ is an eigenvalue of the Frobenius endomorphism of $A$ relative to $\mathbb{F}_q$.

Choose a prime $p$ of $k$ above $p$, and fix a prime $p_1$ of $k(\beta_q | q \in S^{\text{new}}(k))$ above $p$. Let $p_2$ be the prime of $\mathbb{Q}(\beta_q | q \in S^{\text{new}}(k))$ below $p_1$. By replacing each $\beta_q$ with $\overline{\beta}_q$ if necessary, we may assume $\nu(\text{Frob}_{M(q)}) \equiv \beta_q \mod p_2$ for any $q \in S^{\text{new}}(k)$. Then $\nu^{12}(q) \equiv \beta_q^{12} \mod p_2$. By [5, Lemma 6.2(1)] and [6, 4], there is an element $\gamma' = \sum_{\sigma \in \text{Gal}(k/Q)} a'_\sigma \in \mathbb{Z}[\text{Gal}(k/Q)]$ with $a'_\sigma \in \{0, 4, 6, 8, 12\}$ such that

(i) $\nu^{12}(\gamma'Q_k) \equiv \gamma' \mod p$ for any $\gamma \in k^\times$ prime to $p$;

(ii) if $p \equiv 2 \mod 3$ (resp. $p \equiv 3 \mod 4$), then $a'_\sigma \in \{0, 6, 12\}$ (resp. $a'_\sigma \in \{4, 8, 12\}$) for any $\sigma \in \text{Gal}(k/Q)$; and

(iii) $\nu^{12}|_{\nu^{-1}} = \theta_p^{a'_{\sigma^{-1}}}$ for any $\sigma \in \text{Gal}(k/Q)$.

In particular, $\alpha'_{q'} \equiv \nu^{12}(\alpha_qQ_k) = \nu^{12}(q^{hk}) \equiv \beta_q^{12h_k} \mod p_1$ for any $q \in S^{\text{new}}(k)$. Then $\alpha'_{q'}^{24} \equiv \beta_q^{24h_k} \mod p_1$, $p_1 \mid \text{Norm}_{k(q)}(\alpha'_{q'} - \beta_q^{12h_k})$ and $p \mid \text{Ram}(k(q))$. 

\(\natural\) Springer
Norm_{k(\beta_q)/Q}(\alpha_q^{2\epsilon'} - \beta_q^{24\text{hk}}). Further, assume \( p \not\in N_{0}^{\text{new}}(k) \). Then Norm_{k(\beta_q)/Q}(\alpha_q^{2\epsilon'} - \beta_q^{24\text{hk}}) = 0 and \( \alpha_q^{2\epsilon'} = \beta_q^{24\text{hk}}. \)

We claim \( \alpha_q^{\epsilon'} = \beta_q^{12\text{hk}} \) (for any \( q \in S_{\text{new}}(k) \)). If \( \alpha_q^{\epsilon'} = -\beta_q^{12\text{hk}} \), then \( p \) divides Norm_{k(\beta_q)/Q}(\alpha_q^{\epsilon'} - \beta_q^{12\text{hk}}) = Norm_{k(\beta_q)/Q}(-2\beta_q^{12\text{hk}}). \) Since \( \beta_q \in \mathcal{F}(q) \), \( Q(\beta_q) \) is an imaginary quadratic field. Then \( \text{Norm}_{Q(\beta_q)/Q}(\beta_q) = q \) and \( \text{Norm}_{k(\beta_q)/Q}(-2\beta_q^{12\text{hk}}) = \text{Norm}_{k(\beta_q)/Q}(-2)(\text{Norm}_{Q(\beta_q)/Q}(\text{Norm}_{k(\beta_q)/Q}(\beta_q)))^{12\text{hk}} = \frac{2^{(k(\beta_q):Q)}}{\text{Norm}_{Q(\beta_q)/Q}(\beta_q)^{12\text{hk}(k(\beta_q):Q(\beta_q))}} \).

This implies \( p = 2 \) or \( q \), which is a contradiction. Therefore \( \alpha_q^{\epsilon'} = \beta_q^{12\text{hk}} \), as claimed.

Fix a prime \( q_0 \in S_{\text{new}}(k) \). Then by [5, Lemma 6.3] for \( q_0 \), \( \epsilon' \) is of one of the following types:

Type 2. \( \epsilon' = \sum_{\sigma \in \text{Gal}(k/Q)} 6\sigma \) and \( p \equiv 3 \mod 4 \).

Type 3. \( k \) contains \( Q(\beta_{q_0}) \), and \( \epsilon' = \sum_{\sigma \in \text{Gal}(k/Q(\beta_{q_0}))} 12\sigma \) or \( \sum_{\sigma \not\in \text{Gal}(k/Q(\beta_{q_0}))} 12\sigma \).

First, assume that \( \epsilon' \) is of type 2. Then \( \beta_q^{12\text{hk}} = \alpha_q^{\epsilon'} = \text{Norm}_{k/Q}(\alpha_q)^6 \in \{ t \in Q \mid t > 0 \} \) for any \( q \in S_{\text{new}}(k) \). Since \( |\beta_q^{12\text{hk}}| = q^{6\text{hk}} \), we have \( \beta_q^{12\text{hk}} = q^{6\text{hk}}. \)

Here, we claim \( \beta_q^{24} = q^{12}. \) For simplicity, write \( \beta = \beta_q. \) Since \( \beta^{12\text{hk}} = \beta^{12\text{hk}}, \) there is an element \( \zeta \in C \) such that \( \zeta^{12\text{hk}} = 1 \) and \( \zeta = \beta \). Then \( \zeta^4 = 1 \) or \( \zeta^6 = 1, \) because \( Q(\beta) = Q(\beta') = Q(\zeta) \supseteq Q(\xi) \) and \( [Q(\beta) : Q] = 2. \) Hence \( \zeta^{12} = 1, \) and so \( \beta^{12} = \beta^{12}. \) Therefore \( \beta^{24} = q^{12}, \) as claimed. We then have \( v^{24}(q) = \beta^{24} = q^{12} = \theta_p(q^{12}) \mod p. \)

Therefore we conclude \( v^{24} = \theta_p^{12}, \) because \( v^{24}(\gamma O_L) = \gamma^{2\epsilon'} = \text{Norm}_{k/Q}(\gamma)^{12} = \theta_p(\gamma O_L^{12}) \mod p \) for any \( \gamma \in k^\times \) prime to \( p. \)

Next, assume that \( \epsilon' \) is of type 3 (for \( q_0 \)). Let \( L = Q(\beta_{q_0}) \). Then \( L \) is an imaginary quadratic field. Applying [5, Lemma 6.3] to each \( q \in S_{\text{new}}(k) \), we have \( k \supseteq Q(\beta_{q_0}), \) and \( \epsilon' = \sum_{\sigma \in \text{Gal}(k/Q(\beta_{q_0}))} 12\sigma \) or \( \sum_{\sigma \not\in \text{Gal}(k/Q(\beta_{q_0}))} 12\sigma \). Then \( Q(\beta_q) = L = Q(\beta_{q_0}), \) which is independent of \( q \in S_{\text{new}}(k) \). In this case, note that \( p_2 \) is a prime of \( L = Q(\beta_q) \mid q \in S_{\text{new}}(k) \).

[Case \( \epsilon' = \sum_{\sigma \in \text{Gal}(k/L)} 12\sigma \).] We have \( \text{Norm}_{k/L}(q)^{12\text{hk}} = \text{Norm}_{k/L}(\alpha_q)^{12}O_L = \alpha_q^{\epsilon'}O_L = \beta_q^{12\text{hk}}O_L = (\beta_qO_L)^{12\text{hk}} \) for any \( q \in S_{\text{new}}(k) \). Then \( \text{Norm}_{k/L}(q) = \beta_qO_L \), which is a principal ideal. Then the image of the ideal group of \( k \) by \( \text{Norm}_{k/L} \) is contained in the principal ideal group of \( L \). Therefore \( k \supseteq H_L. \) For any \( q \in S_{\text{new}}(k) \), we have \( v^{12}(q) = \beta_q^{12} \mod p_2 \) and \( \text{Norm}_{k/L}(q) = \beta_qO_L. \) Also, \( v^{12}(\gamma O_L) = \gamma^{\epsilon'} = \text{Norm}_{k/L}(\gamma)^{12} \mod p \) for any \( \gamma \in k^\times \) prime to \( p. \) Since \( k = k(\beta_q \mid q \in S_{\text{new}}(k)), \) we have \( p = p_1 \mid p_2. \) Then \( v^{12}(a) = \delta_a^{12} \mod p_2 \) for any fractional ideal \( a \not\equiv (0) \) of \( k \) prime to \( p, \) where \( \delta_a \in L^\times \) is an element such that \( \text{Norm}_{k/L}(a) = \delta_aO_L. \) But \( \delta_a \) is uniquely determined by a because \( \delta_aO_L^2 = 2, 4, \) or 6. Then the assertion holds by taking \( p_L = p_2. \)

[Case \( \epsilon' = \sum_{\sigma \not\in \text{Gal}(k/L)} 12\sigma \).] We have \( \text{Norm}_{k/Q}(q)^{12\text{hk}}\text{Norm}_{k/L}(q)^{-12\text{hk}} = \text{Norm}_{k/Q}(\alpha_q)^{12}\text{Norm}_{k/L}(\alpha_q)^{-12}O_L = \alpha_q^{\epsilon'}O_L = \beta_q^{12\text{hk}}O_L = (\beta_qO_L)^{12\text{hk}} \) and \( \text{Norm}_{k/Q}(q)\text{Norm}_{k/L}(q)^{-1} = \beta_qO_L \) for any \( q \in S_{\text{new}}(k). \) Applying the non-trivial element \( c \in \text{Gal}(L/Q), \) we have \( \text{Norm}_{k/L}(c) = \overline{\beta}_qO_L, \) which is a principal ideal.

\( \square \) Springer
Then \( k \supseteq H_L \). Since \( \nu^{12}(q) \equiv \beta q^{12} \mod p_2 \), we have \( \nu^{12}(q) \equiv \bar{\beta} q^{12} \mod p_2^5 \). Also, \( \nu^{12}(\gamma \mathcal{O}_k) \equiv \gamma^e = \text{Norm}_{k/Q}(\gamma)^{12}\text{Norm}_{L/k}(\gamma)^{-12} \mod p_2 \) for any \( \gamma \in k^\times \) prime to \( p \). Applying \( c \), we have \( \nu^{12}(\gamma \mathcal{O}_k) \equiv \text{Norm}_{L/k}(\gamma)^{12} \mod p_2^5 \). Then \( \nu^{12}(\alpha) \equiv \delta q^{12} \mod p_2^5 \) for any fractional ideal \( \mathfrak{a} \neq (0) \) of \( \mathfrak{a}^\perp \) prime to \( p \), where \( \delta \in L^\times \) is an element such that \( \text{Norm}_{L/k}(\alpha) = \delta \alpha \mathcal{O}_L \). Then the assertion holds by taking \( p_L = p_2^5 \). \( \square \)

Suppose that \( p \notin \mathcal{N}_1^\text{new}(k) \) and that \( \nu \) is of type 2' in Theorem 5.1. Let \( q \neq p \) be a prime number, and fix a prime \( q \) of \( k \) above \( q \). Then \( A \otimes_k k_q \) has good reduction over a totally ramified finite extension \( M' / k_q \). Let \( \text{Frob}_{M'} \in G_{M'}(\subseteq G_k) \) be a Frobenius element. There is an element \( \beta \in \mathcal{F}(\mathcal{N}(q)) \) and a prime \( p_0 \) of \( \mathcal{Q}(\beta) \) above \( p \) such that \( \nu(\text{Frob}_{M'}) \equiv \beta \mod p_0 \). In this situation, we have the following lemma:

**Lemma 5.2** Suppose that \( q \) is of odd degree and that \( N(q) < \frac{p}{4} \). Then

1. \( \beta^2 + \beta^2 \equiv -N(q)\frac{p+1}{2} \) or \( 2N(q)\frac{p+1}{2} \mod p \);
2. \( N(q)\frac{p-1}{2} \equiv -1 \mod p \);
3. \( (\beta + \beta^2) \equiv 3N(q) \) or \( 0 \mod p \);
4. \( q = 3 \) and \( |\beta + \beta^2| = \sqrt{3N(q)} \), or \( \beta + \beta^2 = 0 \); and
5. \( B \otimes_{\mathcal{Q}} (\mathcal{Q}(\sqrt{-q}) \cong M_2(\mathcal{Q}(\sqrt{-q})) \).

**Proof** (1) Let \( \psi' : \nu^{24} = v^{24}\theta_p^{-6(p+1)} = v^{24}\theta_p^{-12} = 1 \), because \( v \) is of type 2'. Since \( p \equiv 3 \mod 4 \), we have \( \psi'^6 = 1 \). Then for each \( \sigma \in G_k \), we have \( \psi'(\sigma)^2 + \psi'(\sigma)^{-2} = -1 \) or 2. Since \( \nu(\text{Frob}_{M'}) \equiv \beta \mod p_0 \) and \( (\nu^{-1}\theta_p)(\text{Frob}_{M'}) \equiv \beta \mod p_0 \), we conclude \( \beta^2 + \beta^2 \equiv \psi'(\text{Frob}_{M'})^2 \theta_p \) \( (\text{Frob}_{M'})^{\frac{p+1}{2}} + \psi'(\text{Frob}_{M'})^{-2}\theta_p (\text{Frob}_{M'})^{\frac{p-1}{2}} = \theta_p (\text{Frob}_{M'})^{\frac{p+1}{2}} (\psi'(\text{Frob}_{M'})^2 + \psi'(\text{Frob}_{M'})^{-2}) \equiv -N(q)\frac{p+1}{2} \) or \( 2N(q)\frac{p+1}{2} \mod p \).

(2), (3), (4) We can prove the assertions by the same argument as in the proof of Lemma 4.4.

(5) Let \( \tilde{A} \) be the special fiber of the Néron model of \( A \otimes_k M' \). Then \( \tilde{A} \) is defined over \( \kappa(q) \) where \( q \) is of odd degree, and has an action of \( \mathcal{O} \). By (4) and [9, Theorem 2.1(2)(4) and Proposition 2.3], we conclude \( \text{End}_{\kappa(q)}(\tilde{A}) \otimes_{\mathcal{Z}} \mathcal{Q} \cong M_2(\mathcal{Q}(\sqrt{-q})) \cong B \otimes_{\mathcal{Q}} (\mathcal{Q}(\sqrt{-q})) \).

We have the following irreducibility theorem for \( \overline{\rho}_{A,p} \):

**Theorem 5.3** Assume that

- \( k \) does not contain the Hilbert class field of any imaginary quadratic field,
- \( p \notin \mathcal{N}_1^\text{new}(k) \), and
- there is a prime \( q \) of \( k \) of odd degree such that \( N(q) < \frac{p}{4} \) and the residue characteristic \( q \) of \( q \) satisfies \( B \otimes_{\mathcal{Q}} (\mathcal{Q}(\sqrt{-q}) \cong M_2(\mathcal{Q}(\sqrt{-q})) \).

Then the representation \( \overline{\rho}_{A,p} : G_k \longrightarrow \text{GL}_2(\mathbb{F}_p) \) is irreducible.

**Proof** Suppose that \( \overline{\rho}_{A,p} \) is reducible. Then the associated character \( \nu \) of type 2', because \( k \) does not contain the Hilbert class field of any imaginary quadratic field. By Lemma 5.2(5), we have \( B \otimes_{\mathcal{Q}} (\mathcal{Q}(\sqrt{-q}) \cong M_2(\mathcal{Q}(\sqrt{-q})) \). This is a contradiction. \( \square \)
For $k$-rational points on $M^B_0(p)$, we have:

**Theorem 5.4** Suppose that the assumption in Theorem 5.3 holds. Further, assume $p \neq 13$.

1. If $B \otimes \mathbb{Q} k \cong M_2(k)$, then $M^B_0(p)(k) = \emptyset$.
2. If $B \otimes \mathbb{Q} k \not\cong M_2(k)$, then $M^B_0(p)(k) \subseteq \{\text{elliptic points of order 2 or 3}\}$.

**Proof** Take a point $x \in M^B_0(p)(k)$.

(1) (1-i) Assume $\text{Aut}(x) \neq \{\pm 1\}$ or $\text{Aut}(x') \not\cong \mathbb{Z}/4\mathbb{Z}$. Then $x$ is represented by a triple $(A, i, V)$ defined over $k$ by Proposition 3.1(1), and the representation $\bar{\rho}_{A, p}$ is reducible. This contradicts Theorem 5.3.

(1-ii) Assume $\text{Aut}(x) = \{\pm 1\}$ and $\text{Aut}(x') \cong \mathbb{Z}/4\mathbb{Z}$. Then $x$ is represented by a triple $(A, i, V)$ defined over a quadratic extension of $k$ by Proposition 3.1(2), and we have a character $\varphi : G_k \longrightarrow \mathbb{F}_p^\times$ as in (3). By Theorem 4.1, $\varphi$ is of type 2. Then by Lemma 4.4(4), we have $B \otimes \mathbb{Q} (\sqrt{-q}) \cong M_2(\mathbb{Q}(\sqrt{-q}))$. This is a contradiction.

(2) Assume that $x$ is not an elliptic point of order 2 or 3. Then $\text{Aut}(x) = \{\pm 1\}$, and by Proposition 3.1(2), $x$ is represented by $(A, i, V)$ defined over a quadratic extension of $k$. By the same argument as in (1-ii), we have a contradiction. \qed

**6 Elimination of elliptic points**

In this section, we deduce Theorem 1.1 from Theorem 5.4(1).

**Proposition 6.1** Suppose that $k$ does not contain the Hilbert class field of any imaginary quadratic field. Assume that there is a prime $q$ of $k$ such that $q$ is of odd degree, the residue characteristic $q$ of $q$ is unramified in $k$, and $B \otimes \mathbb{Q} (\sqrt{-q}) \not\cong M_2(\mathbb{Q}(\sqrt{-q}))$.

Then there is a finite Galois extension $W$ of $\mathbb{Q}$ satisfying the following conditions:

(i) The composite field $kW$ does not contain the Hilbert class field of any imaginary quadratic field.

(ii) There is a prime $q'$ of $kW$ of odd degree with residue characteristic $q$.

(iii) $B \otimes \mathbb{Q} (kW) \cong M_2(kW)$.

We prove Proposition 6.1 at the end of this section.

**Theorem 6.2** In the situation of Proposition 6.1, further assume $p > 4N(q')$, $p \neq 13$, and $p \notin \mathcal{N}_{1}^{\text{new}}(kW)$. Then $M^B_0(p)(k) = M^B_0(p)(kW) = \emptyset$.

**Proof** Applying Theorem 5.4(1) to $kW$, we obtain the result. \qed

Theorem 1.1 follows immediately from Theorem 6.2. From now until the end of this section, we suppose that the assumptions in Proposition 6.1 hold. Fix a prime $q$ of $k$ as in Proposition 6.1. Let $\mathcal{U}$ be the set of non-zero integers $N \in \mathbb{Z}$ such that

- $N$ is square free,
- $d | N$, and
Let $N \in \mathbb{Z}$. For an integer $N \in \mathbb{Z}$, let $W_N := \mathbb{Q}(\sqrt{N})$.

**Lemma 6.3** Let $N \in \mathcal{U}$. Then

1. $B \otimes_{\mathbb{Q}} W_N \cong M_2(W_N)$;
2. $[kW_N : k] = 2$, and the prime $q$ is ramified in $kW_N$; and
3. the unique prime $q'$ of $kW_N$ above $q$ is of odd degree.

**Proof** (1) The isomorphism holds because any prime divisor of $d$ is ramified in $W_N$.

(2) The prime number $q$ is ramified in $W_N$ and is unramified in $k$. Therefore the assertion holds.

(3) By (2) we have $N(q') = N(q)$, which is an odd power of $q$. 

Then Proposition 6.1 is a consequence of the following lemma:

**Lemma 6.4** There is an integer $N \in \mathcal{U}$ such that $kW_N$ does not contain the Hilbert class field of any imaginary quadratic field.

**Proof** Assume to the contrary that for any $N \in \mathcal{U}$, there is an imaginary quadratic field $J_N$ such that $kW_N$ contains the Hilbert class field $H_N$ of $J_N$. Since $H_N \not\subset k$, we have $k \subset kH_N \subset kW_N$. Then $kH_N = kW_N$ because $[kW_N : k] = 2$. Therefore $h_{J_N} = [H_N : J_N] = \frac{1}{2}[H_N : \mathbb{Q}] = \frac{1}{2}[kH_N : \mathbb{Q}] = [k : \mathbb{Q}]$. Then there are only finitely many such imaginary quadratic fields $J_N$. We also have $kH_N = kW_N \supset W_N$. Since $\mathcal{U} = \infty$, this implies that finitely many number fields contain infinitely many subfields, which is a contradiction.

**Remark 6.5** There is an alternate way to eliminate elliptic points. See [2] for details.

### 7 An example

We give an example of Theorem 1.1 (or Theorem 6.2) as follows:

**Proposition 7.1** Suppose $k = \mathbb{Q}(\zeta_{31})$ and $d \in \{6, 22\}$. Then

1. $B \otimes_{\mathbb{Q}} k \not\cong M_2(k)$;
2. $\#M^B(k) = \infty$;
3. $kW_{-d}$ does not contain the Hilbert class field of any imaginary quadratic field;
4. if $p > 128$ and $p \notin \mathcal{N}_{1}^{\text{new}}(kW_{-d})$, then $M_0^B(p)(k) = M_0^B(p)(kW_{-d}) = \emptyset$.

**Proof** For a prime number $l$, let $e_l$ (resp. $f_l$, resp. $g_l$, resp. $v_l$) be the ramification index of $l$ in $k$ (resp. the degree of the residue field extension above $l$ in $k/\mathbb{Q}$, resp. the number of primes of $k$ above $l$, resp. a place of $k$ above $l$).

(1) We observe that $(e_2, f_2, g_2) = (1, 5, 6)$. Since $[k_{v_2} : \mathbb{Q}] = e_2f_2 = 5$ is odd, we have $B \otimes_{\mathbb{Q}} k_{v_2} \cong M_2(k_{v_2})$. Therefore $B \otimes_{\mathbb{Q}} k \not\cong M_2(k)$. 

\@ Springer
The curve $M^B$ is defined by the equation $x^2 + y^2 + 3z^2 = 0$ (resp. $x^2 + y^2 + 11z^2 = 0$) in homogeneous coordinates if $d = 6$ (resp. $d = 22$) (see [10, Theorem 1-1]). We have $M^B(\mathbb{Q}) \neq \emptyset$ if and only if $l \neq 3$ (resp. $l \neq 11$) (cf. [1, Proof of Lemma 4.4]). We observe that $(e_3, f_3, g_3) = (1, 30, 1)$ (resp. $(e_{11}, f_{11}, g_{11}) = (1, 30, 1)$). Since $[k_{v_3} : \mathbb{Q}] = 30$ (resp. $[k_{v_{11}} : \mathbb{Q}] = 30$) is even, we have $M^B(k_{v_3}) \neq \emptyset$ (resp. $M^B(k_{v_{11}}) \neq \emptyset$). Then $M^B(k_v) \neq \emptyset$ for every place $v$ of $k$.

By the Hasse–Minkowski theorem (cf. [7, Theorem 5.3.3]), we have $M^B(k) \neq \emptyset$. Since the genus of $M^B$ is 0, we conclude $\sharp M^B(k) = \infty$.

Let $H(N)$ be the Hilbert class field of $\mathbb{Q}(\sqrt{N})$ for any negative $N \in \mathbb{Z}$.

[Case $d = 6$.] All the imaginary quadratic subfields of $kW_{-6}$ are $\mathbb{Q}(\sqrt{-6})$ and $\mathbb{Q}(\sqrt{-31})$, whose class numbers are 2 and 3, respectively. First, assume $kW_{-6} \not\subseteq H(-6)$. Then $H(-6) = \mathbb{Q}(\sqrt{-6}, \sqrt{-31})$, because we have $[H(-6) : \mathbb{Q}] = h_Q(\sqrt{-6}, \mathbb{Q}) = 4$ and $\text{Gal}(kW_{-6}/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. But in the extension $\mathbb{Q}(\sqrt{-6}, \sqrt{-31})/\mathbb{Q}(\sqrt{-6})$, the primes of $\mathbb{Q}(\sqrt{-6})$ above 31 are ramified. This is a contradiction. Next, assume $kW_{-6} \supseteq H(-31)$. Fix a prime $\mathcal{P}$ of $kW_{-6}$ above 31, and let $p_H$ (resp. $p$) be the prime of $H(-31)$ (resp. $\mathbb{Q}(\sqrt{-31})$) below $\mathcal{P}$. Then $e(\mathcal{P}/p_H) = 15$ because $e(\mathcal{P}/31) = 30$, $e(p/31) = 2$, and $e(p_H/p) = 1$, where $e(\cdot/\cdot)$ is the ramification index. Since $H(-31) = \mathbb{Q}(\sqrt{-31})$, we have $[kW_{-6} : H(-31)] = 10$. This contradicts $e(\mathcal{P}/p_H) = 15$.

[Case $d = 22$.] All the imaginary quadratic subfields of $kW_{-22}$ are $\mathbb{Q}(\sqrt{-22})$ and $\mathbb{Q}(\sqrt{-31})$, whose class numbers are 2 and 3, respectively. First, assume $kW_{-22} \not\subseteq H(-22)$. Then $H(-22) = \mathbb{Q}(\sqrt{-22}, \sqrt{-31})$. But this is a contradiction, because the primes of $\mathbb{Q}(\sqrt{-22})$ above 31 are ramified in $\mathbb{Q}(\sqrt{-22}, \sqrt{-31})$. Next, assume $kW_{-22} \supseteq H(-31)$. Fix a prime $\mathcal{P}$ of $kW_{-22}$ above 31, and let $p_H$ be the prime of $H(-31)$ below $\mathcal{P}$. Then $e(\mathcal{P}/p_H) = 15$ and $[kW_{-22} : H(-31)] = 10$. This is a contradiction.

Since $B \otimes \mathbb{Q} W_{-d} \cong M_2(W_{-d})$, we have $B \otimes \mathbb{Q} (kW_{-d}) \cong M_2(kW_{-d})$. The least $N(q')$ for primes $q'$ of $kW_{-d}$ of odd degree, whose residue characteristic $q$ is unramified in $k$ and satisfies $B \otimes \mathbb{Q} (\sqrt{-q}) \not\cong M_2(\mathbb{Q}(\sqrt{-q}))$, is $2^5 = 32$ (cf. [1, Lemma 4.3]). Then the assertion follows from Theorem 5.4(1).

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

References

1. Arai, K.: On the Rasmussen-Tamagawa conjecture for QM-abelian surfaces. RIMS Kōkyūroku Bessatsu B44, 185–196 (2013)

2. Arai, K.: An effective bound of $p$ for algebraic points on Shimura curves of $\Gamma_0(p)$-type. Acta Arith. 164, 343–353 (2014)

3. Arai, K.: Algebraic points on Shimura curves of $\Gamma_0(p)$-type (II). Manuscr. Math. 149, 63–70 (2016)

4. Arai, K.: Algebraic points on Shimura curves of $\Gamma_0(p)$-type (IV). RIMS Kōkyūroku Bessatsu (to appear)

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

6. Arai, K., Momose, F.: Errata to: Algebraic points on Shimura curves of $\Gamma_0(p)$-type. J. Reine Angew. Math. 690, 203–205 (2014)
7. Cohen, H.: Number Theory. Vol. I. Tools and Diophantine Equations. Graduate Texts in Mathematics, vol. 239. Springer, New York (2007)
8. Deligne, P., Rapoport, M.: Les schémas de modules de courbes elliptiques. Modular Functions of One Variable II. Lecture Notes in Mathematics, vol. 349. Springer, Berlin (1973)
9. Jordan, B.: Points on Shimura curves rational over number fields. J. Reine Angew. Math. 371, 92–114 (1986)
10. Kurihara, A.: On some examples of equations defining Shimura curves and the Mumford uniformization. J. Fac. Sci. Univ. Tokyo Sect. IA 25(3), 277–300 (1979)
11. Mazur, B.: Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. 44(2), 129–162 (1978)
12. Momose, F.: Isogenies of prime degree over number fields. Compos. Math. 97(3), 329–348 (1995)
13. Ohta, M.: On $l$-adic representations of Galois groups obtained from certain two-dimensional abelian varieties. J. Fac. Sci. Univ. Tokyo Sect. IA 21, 299–308 (1974)
14. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Kanô Memorial Lectures, No. 1. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten and Princeton University Press, Tokyo and Princeton (1971)
15. Shimura, G.: On the real points of an arithmetic quotient of a bounded symmetric domain. Math. Ann. 215, 135–164 (1975)