RIMS Kôkyûroku Bessatsu
B32 (2012), 145–161

Galois images and modular curves

By

Keisuke Arai*

To the memory of Professor Fumiyuki Momose

Abstract

This is a survey paper about Galois images, points on modular curves and Shimura curves, together with an application. The main topics are as follows. (1) The images of the Galois representations associated to elliptic curves and QM-abelian surfaces. (2) Rational points, points over quadratic fields on modular curves and Shimura curves. (3) Application to a finiteness conjecture on abelian varieties with constrained prime power torsion.

Contents

§ 1. Galois images associated to elliptic curves

Let k be a field of characteristic 0, and let $\mathrm{G}_k = \mathrm{Gal}(\overline{k}/k)$ be the absolute Galois group of k where $\overline{k}$ is an algebraic closure of k. Let p be a prime. For an elliptic curve

Received March 31, 2011. Revised October 15, 2011.
2000 Mathematics Subject Classification(s): 11F80, 11G18, 14G05
Key Words: *Galois representations, modular curves, rational points*
*School of Engineering, Tokyo Denki University, Tokyo 120-8551, Japan.
e-mail: araik@mail.dendai.ac.jp

E over k, let T_pE denote the p-adic Tate module of E (for precise definition, look at the last of this section), and let

$$\rho_{E/k,p} : \mathrm{G}_k \longrightarrow \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p)$$

be the p-adic Galois representation determined by the action of G_k on T_pE. By a "number field" we mean a finite extension of the rational number field $\mathbb{Q}$.

For an elliptic curve E over a number field K, it is very important to understand the Galois representation $\rho_{E/K,p}$ since it reflects arithmetic and geometric properties of E. The following theorem asserts that the representation $\rho_{E/K,p}$ has a large image if E has no CM (complex multiplication: the precise definition is given in §5). This seems to be a starting point of studying the images of Galois representations.

Theorem 1.1 ([43, IV-11 Theorem], [44, p.299 Théorème 3])**.**
Let K be a number field, and let E be an elliptic curve over K. Suppose that E has no CM. Then the following assertions hold.
(1) For any prime p, the image $\rho_{E/K,p}(\mathrm{G}_K)$ is open in $\mathrm{GL}_2(\mathbb{Z}_p)$ i.e. there exists an integer $n \geq 1$ depending on K, E and p such that $\rho_{E/K,p}(\mathrm{G}_K) \supseteq 1 + p^n \mathrm{M}_2(\mathbb{Z}_p)$.
(2) For all but finitely many primes p, we have $\rho_{E/K,p}(\mathrm{G}_K) = \mathrm{GL}_2(\mathbb{Z}_p)$.

Remark.
In Theorem 1.1 (2), the upper bound of primes p satisfying $\rho_{E/K,p}(\mathrm{G}_K) \neq \mathrm{GL}_2(\mathbb{Z}_p)$ is effectively estimated in terms of K and E ([18, p.487 Main Theorem 1]).

Remark.
In the situation of Theorem 1.1, suppose that E has CM. Then the image $\rho_{E/K,p}(\mathrm{G}_K)$ contains an abelian subgroup of index 1 or 2 (cf. [48, p.106 Theorem 2.2 (b)]). In particular $\rho_{E/K,p}(\mathrm{G}_K)$ is not open in $\mathrm{GL}_2(\mathbb{Z}_p)$.

We have the following question concerning the uniform surjectivity of $\rho_{E/K,p}$.

Question 1.2 ([45, p.187 (Question) 6.5])**.**
For a number field K, does there exist a constant $C_{\mathrm{Serre}}(K) > 0$ satisfying the following?
"For any prime $p > C_{\mathrm{Serre}}(K)$ and for any elliptic curve E over K without CM, we have $\rho_{E/K,p}(\mathrm{G}_K) = \mathrm{GL}_2(\mathbb{Z}_p)$."

We know a weak answer to the question i.e. the image $\rho_{E/K,p}(\mathrm{G}_K)$ has a uniform lower bound.

Theorem 1.3 ([2, p.24 Theorem 1.2], cf. [9, Theorem 1.1])**.**
Let K be a number field, and let p be a prime. Then there exists an integer $n \geq 1$ depending on K and p satisfying the following.
"For any elliptic curve E over K without CM, we have $\rho_{E/K,p}(\mathrm{G}_K) \supseteq 1 + p^n \mathrm{M}_2(\mathbb{Z}_p)$."

Remark.

In Theorem 1.3, the integer n is effectively estimated if the invariant $j(E)$ is not contained in an exceptional finite set ([2, p.24 Theorem 1.3]).

Notice that Theorem 1.3 is generalized to the following situation: not fixing K, but bounding the degree of K.

Theorem 1.4 (Corollary of [10, Theorem 1.1])**.**

Let $g \geq 1$ be an integer, and let p be a prime. Then there exists an integer $n \geq 1$ depending on g and p satisfying the following.
"For any number field K with $[K : \mathbb{Q}] \leq g$ and for any elliptic curve E over K without CM, we have $\rho_{E/K,p}(\mathrm{G}_K) \supseteq 1 + p^n \mathrm{M}_2(\mathbb{Z}_p)$."

We can switch Question 1.2 concerning the images of p-adic representations to the question below concerning the images of mod p representations via the following lemma.

Lemma 1.5 ([43, IV-23 Lemma 3])**.**

Let $p \geq 5$ be a prime, and let H be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. Then H contains $\mathrm{SL}_2(\mathbb{Z}_p)$ if and only if H mod p contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let

$$\overline{\rho}_{E/k,p} : \mathrm{G}_k \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

denote the reduction of $\rho_{E/k,p}$ modulo p.

Question 1.6.

For a number field K, does there exist a constant $C(K) > 0$ satisfying the following? "For any prime $p > C(K)$ and for any elliptic curve E over K without CM, we have $\overline{\rho}_{E/K,p}(\mathrm{G}_K) = \mathrm{GL}_2(\mathbb{F}_p)$."

For an integer $N \geq 1$ and a commutative group (or a commutative group scheme) A, let $A[N]$ denote the kernel of multiplication by N in A. For a field k, let $\overline{k}$ denote an algebraic closure of k. For a scheme S and an abelian scheme A over S, let $\mathrm{End}_S(A)$ denote the ring of endomorphisms of A defined over S. If $S = \mathrm{Spec}\,(k)$ for a field k and if k'/k is a field extension, simply put $\mathrm{End}_{k'}(A) := \mathrm{End}_{\mathrm{Spec}\,(k')}(A \times_{\mathrm{Spec}\,(k)} \mathrm{Spec}\,(k'))$ and $\mathrm{End}(A) := \mathrm{End}_{\overline{k}}(A)$. For a prime p and an abelian variety A over a field k, let $T_pA := \varprojlim A[p^n](\overline{k})$ be the p-adic Tate module of A, where the inverse limit is taken with respect to multiplication by $p : A[p^{n+1}](\overline{k}) \longrightarrow A[p^n](\overline{k})$. For a number field K, let h_K denote the class number of K.

The author is very sorry for the death of Professor Fumiyuki Momose, who has made a major contribution to the study of Galois images, modular curves and modular forms.

Acknowledgements. The author would like to thank the organizers Masanari Kida, Noriyuki Suwa and Shinichi Kobayashi for giving him an opportunity to talk at the conference. He would also like to thank the anonymous referee for helpful comments.

§ 2. Points on modular curves corresponding to maximal subgroups

We divide Question 1.6 into four parts corresponding to the maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$. For each prime p, a maximal subgroup G of $\mathrm{GL}_2(\mathbb{F}_p)$ with $\det G = \mathbb{F}_p^\times$ is conjugate to one of the following subgroups ([27, p.115–116]).

- Borel subgroup :
  $\mathbf{B} = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$.
- Normalizer of a split Cartan subgroup :
  $\mathbf{N}_+ = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\}$.
- Normalizer of a non-split Cartan subgroup (when $p \geq 3$) :
  $\mathbf{N}_- = \left\{ \begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}, \begin{pmatrix} x & y \\ -\lambda y & -x \end{pmatrix} \;\middle|\; (x,y) \in \mathbb{F}_p \times \mathbb{F}_p \setminus \{(0,0)\} \right\}$, where $\lambda \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$ is a fixed element.
- Exceptional subgroup (when $p \geq 5$ and $p \equiv \pm 3 \bmod 8$) :
  $\mathbf{Ex}$ = the inverse image of a subgroup (of $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$) which is isomorphic to S_4 by the natural surjection $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $X_*(p)$ be the modular curve corresponding to $* = \mathbf{B}, \mathbf{N}_+, \mathbf{N}_-, \mathbf{Ex}$ ([27, p.116 Table], cf. [12]). Each of $X_*(p)$ is a proper smooth curve over $\mathbb{Q}$. We give moduli interpretations of $X_{\mathbf{B}}(p)$ and $X_{\mathbf{N}_+}(p)$ below.

Let $N \geq 1$ be an integer. Let $Y_0(N)$ be the coarse moduli scheme over $\mathbb{Q}$ parameterizing isomorphism classes of pairs (E, A) where E is an elliptic curve and A is a cyclic subgroup of E of order N. For a number filed K, a pair (E, A) as above over K (i.e. E is an elliptic curve over K, and A is a cyclic subgroup of $E(\overline{K})$ of order N which is stable under the action of the Galois group G_K; in other words A is K-rational) determines a K-rational point on $Y_0(N)$. Conversely, a K-rational point on $Y_0(N)$ corresponds to the $\overline{K}$-isomorphism class of a pair (E, A), where E is an elliptic curve over K and A is a cyclic subgroup of $E(\overline{K})$ of order N which is stable under the action of G_K. Let $X_0(N)$ be the smooth compactification of $Y_0(N)$ which is also defined over $\mathbb{Q}$. For a prime $N = p$, we have a natural identification $X_{\mathbf{B}}(p) = X_0(p)$. For a later use, let w_N denote the involution on $X_0(N)$ defined over $\mathbb{Q}$ determined by $(E, A) \longmapsto (E/A, E[N]/A)$.

For a prime p, let $Y_{\mathrm{split}}(p)$ be the coarse moduli scheme over $\mathbb{Q}$ parameterizing isomorphism classes of triples $(E, \{A, B\})$ where E is an elliptic curve and $\{A, B\}$ is an unordered pair of cyclic subgroups of E of order p with $A \cap B = 0$. For a number filed K, a triple $(E, \{A, B\})$ as above over K (i.e. E is an elliptic curve over K, and $\{A, B\}$ is an unordered pair of cyclic subgroups of $E(\overline{K})$ of order p with $A \cap B = 0$ which $(= \{A, B\})$ is stable under the action of G_K) determines a K-rational point on $Y_{\mathrm{split}}(p)$. Conversely, a K-rational point on $Y_{\mathrm{split}}(p)$ corresponds to the $\overline{K}$-isomorphism class of a triple $(E, \{A, B\})$, where E is an elliptic curve over K and $\{A, B\}$ is an unordered pair of cyclic subgroups of $E(\overline{K})$ of order p with $A \cap B = 0$ which $(= \{A, B\})$ is stable under the action of G_K. Let $X_{\mathrm{split}}(p)$ be the smooth compactification of $Y_{\mathrm{split}}(p)$ which is also defined over $\mathbb{Q}$. We have a natural identification $X_{\mathbf{N}_+}(p) = X_{\mathrm{split}}(p)$. A point on a modular curve is called a CM point if it corresponds to an elliptic curve with CM.

Then Question 1.6 is divided into four parts.

Question 2.1 (Question $*$)**.**

For a number field K, does there exist a constant $C_*(K) > 0$ satisfying the following?

"For any prime $p > C_*(K)$, we have $X_*(p)(K) \subseteq \{\text{cusps, CM points}\}$."

Then, owing to the following lemma, the answer to Question 1.6 is affirmative if and only if the answers to Questions $\mathbf{B}, \mathbf{N}_+, \mathbf{N}_-, \mathbf{Ex}$ are all affirmative.

Lemma 2.2.

For a number field K, there exists a constant $C_{cyc}(K) > 0$ satisfying the following. "For any prime $p > C_{cyc}(K)$ and for any elliptic curve E over K, we have $\det \rho_{E/K,p}(\mathrm{G}_K) = \mathbb{Z}_p^\times$ (and so $\det \overline{\rho}_{E/K,p}(\mathrm{G}_K) = \mathbb{F}_p^\times$)."

Proof.

Since $\det \rho_{E/K,p}$ is the p-adic cyclotomic character ([43, IV-5]), we can choose $C_{\mathrm{cyc}}(K)$ to be the largest prime that divides the discriminant of K (and $C_{\mathrm{cyc}}(\mathbb{Q})$ to be 1).

□

We have the following partial answers to these questions. Theorem 2.3 below was shown by combining several (algebraic, geometric and analytic) methods, which have been widely used to study rational points on various modular curves.

Theorem 2.3 ([28, p.129 Theorem 1])**.**

We have $X_{\mathbf{B}}(p)(\mathbb{Q}) = \{cusps\}$ for any prime $p > 163$. Equivalently, for any prime $p > 163$ and for any elliptic curve E over $\mathbb{Q}$, the representation $\overline{\rho}_{E/\mathbb{Q},p}$ is irreducible.

Theorem 2.3 was generalized to almost all quadratic fields.

Theorem 2.4 ([33, p.330 Theorem B])**.**
Let K be a quadratic field which is not an imaginary quadratic field of class number one. Then there exists a constant $C_{\mathbf{B}}(K) > 0$ satisfying the following two equivalent conditions.
(1) For any prime $p > C_{\mathbf{B}}(K)$, we have $X_{\mathbf{B}}(p)(K) = \{cusps\}$.
(2) For any prime $p > C_{\mathbf{B}}(K)$ and for any elliptic curve E over K, the representation $\overline{\rho}_{E/K,p}$ is irreducible.

Remark.
In Theorem 2.4, the set of primes p with $X_{\mathbf{B}}(p)(K) \neq \{\text{cusps}\}$ is effectively estimated except at most one prime. If such a prime exists, it is concerned with a Siegel zero of the L-functions of quadratic characters (cf. [28, p.160 Theorem A]).

Remark.
We know by [28, p.131 Theorem 4] (cf. [44, p.306 Proposition 21]) that for any prime $p \geq 11$ and for any semi-stable elliptic curve E over $\mathbb{Q}$, the representation $\overline{\rho}_{E/\mathbb{Q},p}$ is irreducible (and furthermore surjective). This result is generalized to semi-stable elliptic curves over certain number fields ([23, p.246 Théorème], [24, p.615 Théorème 1, Théorème 2], cf. [11]).

For a prime p, let $J_0(p)$ be the Jacobian variety of $X_0(p)$, which is an abelian variety over $\mathbb{Q}$. By abuse of notation let w_p denote also the involution on $J_0(p)$ defined over $\mathbb{Q}$ induced by $w_p : X_0(p) \longrightarrow X_0(p)$. Consider the quotient $J_0^-(p)$ of $J_0(p)$ defined by $J_0^-(p) := J_0(p)/(1 + w_p)J_0(p)$, which is also an abelian variety over $\mathbb{Q}$. For rational points on $X_{\mathbf{N}_+}(p)$, we know the following.

Theorem 2.5 ([31, p.116 Theorem (0.1)])**.**
Let p be a prime satisfying ($p = 11$ or $p \geq 17$) and $p \neq 37$. Suppose $\sharp J_0^-(p)(\mathbb{Q}) < \infty$. Then $X_{\mathbf{N}_+}(p)(\mathbb{Q}) \subseteq \{cusps,\ CM\ points\}$.

Remark.
Theorem 2.5 seems to be the first result that distinguishes CM points among non-cuspidal rational points. In fact, the formal immersion method was used in a part of the proof of Theorem 2.3: we deduce a contradiction by assuming the existence of a non-cuspidal rational point on $X_{\mathbf{B}}(p)$. But a priori the modular curve $X_{\mathbf{N}_+}(p)$ has a non-cuspidal rational point (which is a CM point), so the above method is not applicable.

Remark.
The genus of the modular curve $X_0(p)$ is positive if and only if $p = 11$ or $p \geq 17$. In Theorem 2.5, $p = 37$ is excluded since the group $\mathrm{Aut}(X_0(37))$ of automorphisms of

$X_0(37)$ defined over $\overline{\mathbb{Q}}$ is large i.e. $\mathrm{Aut}(X_0(37)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (cf. [29, p.27], [36, p.279 Satz 1]). Notice that each automorphism in $\mathrm{Aut}(X_0(37))$ is defined over $\mathbb{Q}$.

Later the assertion in Theorem 2.5 was shown to hold even if $p = 37$.

Theorem 2.6 ([16, p.288 Theorem 3.2] or [34, p.160 Theorem 0.1])**.**
We have $X_{\mathbf{N}_+}(37)(\mathbb{Q}) \subseteq \{$*cusps, CM points*$\}$.

Now we know the existence of the constant $C_{\mathbf{N}_+}(\mathbb{Q})$. The following theorem was shown by a new method using a modular unit.

Theorem 2.7 ([6, p.570 Theorem 1.2])**.**
There exists a constant $C_{\mathbf{N}_+}(\mathbb{Q}) > 0$ *such that we have* $X_{\mathbf{N}_+}(p)(\mathbb{Q}) \subseteq \{$*cusps, CM points*$\}$ *for any prime* $p > C_{\mathbf{N}_+}(\mathbb{Q})$.

Remark.
In [6] the constant $C_{\mathbf{N}_+}(\mathbb{Q})$ is effectively estimated, but the value obtained there is quite huge.

Recently, by using the Gross vectors method in the previous works [40] and [42] together with the aid of a computer, the estimate has been greatly improved.

Theorem 2.8 ([7])**.**
We have $X_{\mathbf{N}_+}(p)(\mathbb{Q}) \subseteq \{$*cusps, CM points*$\}$ *for any prime* $p \geq 11$, $p \neq 13$.

For $X_{\mathbf{N}_-}(p)(\mathbb{Q})$, little seems to be known.
Question **Ex** is solved for any number field K.

Theorem 2.9 ([27, p.118])**.**
For any number field K*, there exists a constant* $C_{\mathbf{Ex}}(K)$ *satisfying the following.*
"For any prime $p > C_{\mathbf{Ex}}(K)$*, we have* $X_{\mathbf{Ex}}(p)(K) = \emptyset$*."*

Note that Theorem 2.9 is proved by a local method, which in particular leads to the following.

Theorem 2.10 ([27, p.118])**.**
If $p > 13$*, then* $X_{\mathbf{Ex}}(p)(\mathbb{Q}_p) = \emptyset$.

§ 3. Variant: Points on $X_0^+(N)$

Let $N \geq 1$ be an integer. For rational points on $X_0(N)$, we know the following.

Theorem 3.1.
([30, p.745 Théorème], [26, p.63 (5.2.3.1)], [25, p.221 Proposition IV.3.5, p.222 Proposition IV.3.10], [28, p.131], [19, p.23], [20, p.18 Theorem 6, p.20 Theorem 7], [21, p.241 Theorem 1], [22, p.423 Theorem 1])

We have $X_0(N)(\mathbb{Q}) = \{cusps\}$ *if and only if* N *does not belong to the following set:* $\{N \mid N \leq 19\} \cup \{21, 25, 27, 37, 43, 67, 163\}$.

Now we consider the modular curve $X_0^+(N)$ defined by taking a quotient:

$$X_0^+(N) := X_0(N)/w_N.$$

Then $X_0^+(N)$ is a proper smooth curve over $\mathbb{Q}$. Note that if $N = p^2$ for a prime p, then the natural map $X_0(p^2) \longrightarrow X_{\mathrm{split}}(p)$ defined by $(E, A) \longmapsto (E/A[p], \{A/A[p], E[p]/A[p]\})$ induces an isomorphism $X_0^+(p^2) \cong X_{\mathrm{split}}(p)$. We have the following open question.

Question 3.2.
For a number field K, does there exist a constant $C_0^+(K) > 0$ satisfying the following?
"For any integer $N > C_0^+(K)$, we have $X_0^+(N)(K) \subseteq \{\text{cusps, CM points}\}$."

Notice that even if N is an arbitrarily large, the equality $X_0^+(N)(\mathbb{Q}) = \{\text{cusps}\}$ does not hold. We know the following partial answer to Question 3.2.

Theorem 3.3 ([32, p.269 Theorem (0.1)])**.**
Let N *be a composite number. If* N *has a prime divisor* p *which satisfies the following two conditions, then* $X_0^+(N)(\mathbb{Q}) \subseteq \{cusps,\ CM\ points\}$.
(i) $(p = 11$ *or* $p \geq 17)$ *and* $p \neq 37$.
(ii) $\sharp J_0^-(p)(\mathbb{Q}) < \infty$.

Remark.
When $N \in \{73, 91, 103, 125, 137, 191, 311\}$, the modular curve $X_0^+(N)$ has an exceptional rational point i.e. a rational point which is neither a cusp nor a CM point ([15, p.206], cf. [14]).

The assumption $p \neq 37$ in Theorem 3.3 was shown to be superfluous.

Theorem 3.4 ([3, p.2273 Theorem 1.2])**.**
Let $M \geq 2$ *be an integer. Let* K *be* $\mathbb{Q}$ *or an imaginary quadratic field. If* $K \neq \mathbb{Q}$, *assume* 37 *does not split in* K *and* 3 *does not divide* h_K. *Then* $X_0^+(37M)(K) \subseteq \{cusps,\ CM\ points\}$.

Remark.
Theorem 3.4 for $M = 37$ and $K = \mathbb{Q}$ implies Theorem 2.6.

Theorem 3.3 is generalized to certain quadratic fields.

Theorem 3.5 ([4, Theorem 1.6])**.**
Let N be a composite number. Let K be a quadratic field satisfying $X_0(N)(K) = \{cusps\}$. If N has a prime divisor p which satisfies the following four conditions, then $X_0^+(N)(K) \subseteq \{cusps,\ CM\ points\}$.
(i) ($p = 11$ or $p \geq 17$) and $p \neq 37$.
(ii) If $p = 11$, then $\mathrm{ord}_p N = 1$.
(iii) p is unramified in K.
(iv) $J_0^-(p)(K) = J_0^-(p)(\mathbb{Q})$ and $\sharp J_0^-(p)(\mathbb{Q}) < \infty$.

§ 4. Galois images associated to QM-abelian surfaces

Let B be an indefinite quaternion division algebra over $\mathbb{Q}$. Let

$$d = \mathrm{disc}(B)$$

be the discriminant of B. Then $d > 1$ and d is the product of an even number of distinct primes. Choose and fix a maximal order $\mathcal{O}$ of B. If a prime p does not divide d, fix an isomorphism $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{M}_2(\mathbb{Z}_p)$ of $\mathbb{Z}_p$-algebras.

Definition 4.1 (cf. [8, p.591])**.**
Let S be a scheme over $\mathbb{Q}$. A QM-abelian surface by $\mathcal{O}$ over S is a pair (A, i) where A is an abelian surface over S (i.e. A is an abelian scheme over S of relative dimension 2), and $i : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$ is an injective ring homomorphism (sending 1 to id). We consider that A has a left $\mathcal{O}$-action. We sometimes omit "by $\mathcal{O}$" and simply write "a QM-abelian surface".

Let k be a field of characteristic 0. As explained below, a QM-abelian surface (A, i) over k where i is an isomorphism has a Galois representation which looks like that of an elliptic curve (cf. [37]). By this reason, a QM-abelian surface is also called a fake elliptic curve or a false elliptic curve.

Let (A, i) be a QM-abelian surface over k. Suppose that (A, i) satisfies the following condition:

$$i : \mathcal{O} \xrightarrow{\cong} \mathrm{End}_k(A) = \mathrm{End}(A). \tag{4.1}$$

Note that the condition (4.1) corresponds to "no CM" in the case of an elliptic curve. Now we consider Galois representations associated to (A, i). Take a prime p not dividing d. We have isomorphisms of $\mathbb{Z}_p$-modules:

$$\mathbb{Z}_p^4 \cong T_p A \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{M}_2(\mathbb{Z}_p).$$

The middle is also an isomorphism of left $\mathcal{O}$-modules ([37, p.300 Proposition 1.1 (1)]); the last is also an isomorphism of $\mathbb{Z}_p$-algebras (which is fixed as above). We sometimes identify these $\mathbb{Z}_p$-modules. Take a $\mathbb{Z}_p$-basis

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ e_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ e_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

of $\mathrm{M}_2(\mathbb{Z}_p)$. Then the image of the natural map

$$\mathrm{M}_2(\mathbb{Z}_p) \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \mathrm{End}(T_pA) \cong \mathrm{M}_4(\mathbb{Z}_p)$$

lies in $\left\{ \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} \middle| X \in \mathrm{M}_2(\mathbb{Z}_p) \right\}$. The G_k-action on T_pA induces a representation

$$\rho : \mathrm{G}_k \longrightarrow \mathrm{Aut}_{\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_pA) \subseteq \mathrm{Aut}(T_pA) \cong \mathrm{GL}_4(\mathbb{Z}_p),$$

where $\mathrm{Aut}_{\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_pA)$ is the group of automorphisms of T_pA commuting with the action of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. The above observation implies

$$\mathrm{Aut}_{\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_pA) = \left\{ \begin{pmatrix} aI_2 & bI_2 \\ cI_2 & dI_2 \end{pmatrix} \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \right\} \subseteq \mathrm{GL}_4(\mathbb{Z}_p),$$

where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then the representation ρ factors through

$$\rho : \mathrm{G}_k \longrightarrow \left\{ \begin{pmatrix} aI_2 & bI_2 \\ cI_2 & dI_2 \end{pmatrix} \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \right\} \subseteq \mathrm{GL}_4(\mathbb{Z}_p).$$

Let

$$\rho_{(A,i)/k,p} : \mathrm{G}_k \longrightarrow \mathrm{GL}_2(\mathbb{Z}_p)$$

denote the Galois representation determined by "$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$", so that we have $\rho_{(A,i)/k,p}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ if $\rho(\sigma) = \begin{pmatrix} aI_2 & bI_2 \\ cI_2 & dI_2 \end{pmatrix}$ for $\sigma \in \mathrm{G}_k$. Let

$$\overline{\rho}_{(A,i)/k,p} : \mathrm{G}_k \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

denote the reduction of $\rho_{(A,i)/k,p}$ modulo p. Note that the determinant

$$\det \rho_{(A,i)/k,p} : \mathrm{G}_k \longrightarrow \mathbb{Z}_p^{\times}$$

is the p-adic cyclotomic character ([37, p.300 Proposition 1.1 (2)]).

As an analogue of Theorem 1.1, we have the following.

Theorem 4.2 ([37, p.299 Theorem (below)])**.**

Let K be a number field and (A, i) be a QM-abelian surface by $\mathcal{O}$ over K satisfying (4.1) (with $k = K$). Then the following assertions hold.
(1) Take a prime p not dividing d. Then the representation $\rho_{(A,i)/K,p}$ has an open image i.e. there exists an integer $n \geq 1$ depending on $K, \mathcal{O}, (A, i)/K$ and p such that $\rho_{(A,i)/K,p}(\mathrm{G}_K) \supseteq 1 + p^n \mathrm{M}_2(\mathbb{Z}_p)$.
(2) For all but finitely many primes p (with $p \nmid d$), we have $\rho_{(A,i)/K,p}(\mathrm{G}_K) = \mathrm{GL}_2(\mathbb{Z}_p)$.

Remark.
In [37], the case where p divides d is also treated.

The representation $\rho_{(A,i)/K,p}$ also has a uniform lower bound.

Theorem 4.3 ([1, p.167 Theorem 2.3], cf. [9, Theorem 1.1])**.**

Let K be a number field, and let p be a prime not dividing d. Then there exists an integer $n \geq 1$ depending on $K, \mathcal{O}$ and p satisfying the following.
"For any QM-abelian surface (A, i) by $\mathcal{O}$ over K satisfying (4.1) (with $k = K$), we have $\rho_{(A,i)/K,p}(\mathrm{G}_K) \supseteq 1 + p^n \mathrm{M}_2(\mathbb{Z}_p)$. "

As an analogue of Theorem 1.4, we have the following generalization of Theorem 4.3.

Theorem 4.4 (Corollary of [10, Theorem 1.1])**.**

Let $g \geq 1$ be an integer, and let p be a prime not dividing d. Then there exists an integer $n \geq 1$ depending on $g, \mathcal{O}$ and p satisfying the following.
"For any number field K with $[K : \mathbb{Q}] \leq g$ and for any QM-abelian surface (A, i) by $\mathcal{O}$ over K satisfying (4.1) (with $k = K$), we have $\rho_{(A,i)/K,p}(\mathrm{G}_K) \supseteq 1 + p^n \mathrm{M}_2(\mathbb{Z}_p)$. "

§ 5. Points on Shimura curves of $\Gamma_0(p)$-type

We keep the notation and the convention in §4. Let M^B be the coarse moduli scheme over $\mathbb{Q}$ parameterizing isomorphism classes of QM-abelian surfaces by $\mathcal{O}$. Then M^B is a proper smooth curve over $\mathbb{Q}$, called a Shimura curve (cf. [8], [17]). For a number field K, a QM-abelian surface (A, i) by $\mathcal{O}$ over K determines a K-rational point on M^B. Conversely, a K-rational point on M^B corresponds to the $\overline{K}$-isomorphism class of a QM-abelian surface (A, i) by $\mathcal{O}$ over some finite extension L of K (contained in $\overline{K}$). Here we can take $L = K$ if and only if $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$ ([17, p.93 Theorem (1.1)]). Let p be a prime not dividing d. Let $M_0^B(p)$ be the coarse moduli scheme over $\mathbb{Q}$ parameterizing isomorphism classes of triples (A, i, V) where (A, i) is a QM-abelian surface by $\mathcal{O}$ and V is a left $\mathcal{O}$-submodule of $A[p]$ with $\mathbb{F}_p$-dimension 2. Then $M_0^B(p)$ is a proper smooth

curve over $\mathbb{Q}$, which we call a Shimura curve of $\Gamma_0(p)$-type. For a number field K, a triple (A, i, V) as above over K (i.e. (A, i) is a QM-abelian surface by $\mathcal{O}$ over K, and V is a left $\mathcal{O}$-submodule of $A[p](\overline{K})$ with $\mathbb{F}_p$-dimension 2 which is stable under the action of G_K) determines a K-rational point on $M_0^B(p)$. Conversely, a K-rational point on $M_0^B(p)$ corresponds to the $\overline{K}$-isomorphism class of a triple (A, i, V), where there is a finite extension L of K (contained in $\overline{K}$) such that (A, i) is a QM-abelian surface by $\mathcal{O}$ over L and V is a left $\mathcal{O}$-submodule of $A[p](\overline{K})$ with $\mathbb{F}_p$-dimension 2 stable under the action of G_L. Here we can take $L = K$ if $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$ and $\mathrm{Aut}_{\mathcal{O}}(A) = \{\pm 1\}$, where $\mathrm{Aut}_{\mathcal{O}}(A)$ is the group of automorphisms of A defined over $\overline{K}$ compatible with the action of $\mathcal{O}$. The curve $M_0^B(p)$ is an analogue of the modular curve $X_0(p)$. In fact, for a triple (A, i, V) as above over a number field K, the representation $\overline{\rho}_{(A,i)/K,p}$ is reducible just like the mod p representation $\overline{\rho}_{E/K,p}$ associated to an elliptic curve E over K with a K-rational cyclic subgroup of order p (which determines a K-rational point on $X_0(p)$) ([5]).

For real points on M^B, we know the following.

Theorem 5.1 ([47, p.136 Theorem 0])**.**
We have $M^B(\mathbb{R}) = \emptyset$.

Remark.

For any prime p we have $M_0^B(p)(\mathbb{R}) = \emptyset$, because there is a natural map $M_0^B(p) \longrightarrow M^B$ defined over $\mathbb{Q}$. So for a number field K having a real place, we have $M_0^B(p)(K) = \emptyset$.

Here we recall the notion of CM (complex multiplication) on an abelian variety. Let k be a field, and let A be an abelian variety over k. For a field extension k'/k, the abelian variety A is said to have CM over k' if $\mathrm{End}_{k'}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a product R of number fields satisfying $\dim_{\mathbb{Q}} R = 2 \dim A$. Conventionally A is said to have CM if it has CM over $\overline{k}$.

Consider the case where the characteristic of k is 0. If A is $\overline{k}$-simple and has CM (by R), then $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong R$ ([35, p.202 Table (Chapter IV Section 21)]). If (A, i) is a QM-abelian surface over k, then either A has CM or A is $\overline{k}$-simple. If (A, i) is a QM-abelian surface over k with CM, then A is $\overline{k}$-isogenous to $E \times E$ where E is an elliptic curve over $\overline{k}$ with CM. A point on $M_0^B(p)$ is called a CM point if it corresponds to a QM-abelian surface with CM.

As an analogue of Theorem 2.4, we know the following.

Theorem 5.2 ([5])**.**
Let K be an imaginary quadratic field with $h_K \geq 2$. Then there exists a constant $C_0^{QM}(K) > 0$ depending only on K satisfying the following conditions.

(1) (a) *If $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$, then $M_0^B(p)(K) = \emptyset$ holds for any prime $p > C_0^{QM}(K)$ with $p \nmid d$.*

(b) *If* $B \otimes_{\mathbb{Q}} K \ncong \mathrm{M}_2(K)$, *then* $M_0^B(p)(K) \subseteq \{CM\ points\}$ *holds for any prime* $p > C_0^{QM}(K)$ *with* $p \nmid d$.

(2) *For any prime* $p > C_0^{QM}(K)$ *with* $p \nmid d$ *and for any QM-abelian surface* (A, i) *by* $\mathcal{O}$ *over* K *satisfying (4.1) (with* $k = K$*), the representation* $\overline{\rho}_{(A,i)/K,p} : \mathrm{G}_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ *is irreducible.*

§ 6. Application to a finiteness conjecture on abelian varieties

For a number field K and a prime p, let $\widetilde{K}_p$ denote the maximal pro-p extension of $K(\boldsymbol{\mu}_p)$ which is unramified away from p, where $\boldsymbol{\mu}_p$ is the group of p-th roots of unity in $\overline{K}$. For a number field K, an integer $g \geq 0$ and a prime p, let $\mathscr{A}(K, g, p)$ denote the set of K-isomorphism classes of abelian varieties A over K, of dimension g, which satisfy

$$K(A[p^\infty]) \subseteq \widetilde{K}_p,$$

where $K(A[p^\infty])$ is the field generated over K by the p-power torsion of A. By [46, p.493 Theorem 1] we know that an abelian variety A over K whose class belongs to $\mathscr{A}(K, g, p)$ has good reduction at any prime of K not dividing p, because the extension $K(A[p^\infty])/K(\boldsymbol{\mu}_p)$ is unramified away from p. So the solution of the Shafarevich conjecture ([13, p.363 Satz 6]) implies that $\mathscr{A}(K, g, p)$ is a finite set. For fixed K and g, define the set

$$\mathscr{A}(K, g) := \{([A], p) \mid [A] \in \mathscr{A}(K, g, p)\}.$$

We have the following finiteness conjecture on abelian varieties.

Conjecture 6.1 ([41, p.1224 Conjecture 1])**.**
Let K be a number field, and let $g \geq 0$ be an integer. Then the following two equivalent conditions hold.
(1) The set $\mathscr{A}(K, g)$ is finite.
(2) There exists a constant $C_{\mathrm{RT}}(K, g) > 0$ depending on K and g such that we have $\mathscr{A}(K, g, p) = \emptyset$ for any prime $p > C_{\mathrm{RT}}(K, g)$.

As an application of Theorem 2.3 and Theorem 2.4, we know the following.

Theorem 6.2 ([41, p.1224 Theorem 2, p.1227 Theorem 4])**.**
Let K *be* $\mathbb{Q}$ *or a quadratic field which is not an imaginary quadratic field of class number one. Then the set* $\mathscr{A}(K, 1)$ *is finite.*

Let B be an indefinite quaternion division algebra over $\mathbb{Q}$. Let $\mathscr{A}(K, 2, p)_B$ be the set of K-isomorphism classes of abelian varieties A over K in $\mathscr{A}(K, 2, p)$ whose

endomorphism algebra $\mathrm{End}_K(A)$ contains a maximal order $\mathcal{O}$ of B as a subring. Define also the set

$$\mathscr{A}(K,2)_B := \{([A],p) \mid [A] \in \mathscr{A}(K,2,p)_B\},$$

which is a subset of $\mathscr{A}(K,2)$. If one of the following two conditions is satisfied, we know that the set $\mathscr{A}(K,2)_B$ is empty (Remark after Theorem 5.1, [17, p.93 Theorem (1.1)]).
(i) K has a real place.
(ii) $B \otimes_{\mathbb{Q}} K \ncong \mathrm{M}_2(K)$.

As an application of Theorem 5.2 (2), we have the following.

Theorem 6.3 ([5])**.**
Let K be an imaginary quadratic field with $h_K \geq 2$. Then the set $\mathscr{A}(K,2)_B$ is finite.

Let $\mathcal{QM}$ be the set of isomorphism classes of indefinite quaternion division algebras over $\mathbb{Q}$. Define the set

$$\mathscr{A}(K,2)_{\mathcal{QM}} := \bigcup_{B \in \mathcal{QM}} \{([A],p) \mid [A] \in \mathscr{A}(K,2,p)_B\},$$

which is a subset of $\mathscr{A}(K,2)$. As a corollary of Theorem 6.3, we know the following.

Corollary 6.4 ([5])**.**
Let K be an imaginary quadratic field with $h_K \geq 2$. Then the set $\mathscr{A}(K,2)_{\mathcal{QM}}$ is finite.

Conjecture 6.1 is partly solved for any K and any g as seen in Theorem 6.5 and Theorem 6.6 below. Let $\mathscr{A}(K,g,p)_{\mathrm{st}}$ be the set of K-isomorphism classes of semi-stable abelian varieties in $\mathscr{A}(K,g,p)$. Define also the set

$$\mathscr{A}(K,g)_{\mathrm{st}} := \{([A],p) \mid [A] \in \mathscr{A}(K,g,p)_{\mathrm{st}}\},$$

which is a subset of $\mathscr{A}(K,g)$.

Theorem 6.5 ([38, p.2392 Corollary 4.5])**.**
For any number field K and for any integer $g \geq 0$, the set $\mathscr{A}(K,g)_{st}$ is finite.

For a prime p and an abelian variety A of dimension g over a number field K, let

$$\rho_{A/K,p} : \mathrm{G}_K \longrightarrow \mathrm{Aut}(T_pA) \cong \mathrm{GL}_{2g}(\mathbb{Z}_p)$$

be the p-adic Galois representation determined by the action of G_K on the p-adic Tate module T_pA. Let $\mathscr{A}(K,g,p)_{\mathrm{ab}}$ be the set of K-isomorphism classes of abelian varieties

A over K in $\mathscr{A}(K,g,p)$ such that the image $\rho_{A/K,p}(\mathrm{G}_K)$ is an abelian group. Define also the set

$$\mathscr{A}(K,g)_{\mathrm{ab}} := \{([A],p) \mid [A] \in \mathscr{A}(K,g,p)_{\mathrm{ab}}\},$$

which is a subset of $\mathscr{A}(K,g)$.

Theorem 6.6 ([39])**.**
For any number field K and for any integer $g \geq 0$, the set $\mathscr{A}(K,g)_{ab}$ is finite.

References

[1] Arai, K., On the Galois images associated to QM-abelian surfaces, *Proceedings of the Symposium on Algebraic Number Theory and Related Topics*, 165–187, *RIMS Kôkyûroku Bessatsu*, **B4**, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007.

[2] Arai, K., On uniform lower bound of the Galois images associated to elliptic curves, *J. Théor. Nombres Bordeaux*, **20** (2008), no. 1, 23–43.

[3] Arai, K. and Momose, F., Rational points on $X_0^+(37M)$, *J. Number Theory* **130** (2010), no. 10, 2272–2282.

[4] Arai, K. and Momose, F., Points on $X_0^+(N)$ over quadratic fields, *Acta Arith.* **152** (2012), no. 2, 159–173.

[5] Arai, K. and Momose, F., Algebraic points on Shimura curves of $\Gamma_0(p)$-type, available from `http://arxiv.org/pdf/1202.4841.pdf`.

[6] Bilu, Y. and Parent, P., Serre's Uniformity Problem in the Split Cartan Case, *Ann. Math.* **173** (2011), no. 1, 569–584.

[7] Bilu, Y., Parent, P. and Rebolledo, M., Rational points on $X_0^+(p^r)$, *preprint* (2011), available at the web page (http://arxiv.org/PS_cache/arxiv/pdf/1104/1104.4641v1.pdf).

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

[9] Cadoret, A. and Tamagawa, A., A uniform open image theorem for l-adic representations I, to appear in *Duke. Math. J.*

[10] Cadoret, A. and Tamagawa, A., A uniform open image theorem for l-adic representations II, *preprint*, available at the web page (http://www.math.u-bordeaux1.fr/~cadoret/).

[11] David, A., Caractère d'isogénie et critères d'irréductibilité, *preprint* (2011), available at the web page (http://arxiv.org/PS_cache/arxiv/pdf/1103/1103.3892v1.pdf).

[12] Deligne, P. and Rapoport, M., Les schémas de modules de courbes elliptiques, *Modular functions of one variable II*, 143–316. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[13] Faltings, G., Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), no. 3, 349–366.

[14] Galbraith, S., Rational points on $X_0^+(p)$, *Experiment. Math.* **8** (1999), no. 4, 311–318.

[15] Galbraith, S., Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves, *J. Theor. Nombres Bordeaux* **14** (2002), no. 1, 205–219.

[16] Hibino, Y. and Murabayashi, N., Modular equations of hyperelliptic $X_0(N)$ and an application, *Acta Arith.* **82** (1997), no. 3, 279–291.

[17] Jordan, B., Points on Shimura curves rational over number fields, *J. Reine Angew. Math.* **371** (1986), 92–114.
[18] Kawamura, T., The effective surjectivity of mod l Galois representations of 1- and 2-dimensional abelian varieties with trivial endomorphism ring, *Comment. Math. Helv.* **78** (2003), no. 3, 486–493.
[19] Kenku, M. A., The modular curve $X_0(39)$ and rational isogeny, *Math. Proc. Cambridge Philos. Soc.* **85** (1979), no. 1, 21–23.
[20] Kenku, M. A., The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny, *Math. Proc. Cambridge Philos. Soc.* **87** (1980), no. 1, 15–20.
[21] Kenku, M. A., The modular curve $X_0(169)$ and rational isogeny, *J. London Math. Soc. (2)* **22** (1980), no. 2, 239–244.
[22] Kenku, M. A., On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$, *J. London Math. Soc. (2)* **23** (1981), no. 3, 415–427.
[23] Kraus, A., Courbes elliptiques semi-stables et corps quadratiques, *J. Number Theory* **60** (1996), no. 2, 245–253.
[24] Kraus, A., Courbes elliptiques semi-stables sur les corps de nombres, *Int. J. Number Theory* **3** (2007), no. 4, 611–633.
[25] Kubert, D., Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc. (3)* **33** (1976), no. 2, 193–237.
[26] Ligozat, G., Courbes modulaires de genre 1, *Bull. Soc. Math. France, Mém.* **43**. Supplément au Bull. Soc. Math. France Tome 103, no. 3. Société Mathématique de France, Paris, 1975. 1–80.
[27] Mazur, B., Rational points on modular curves, *Modular functions of one variable V*, Lecture Notes in Math., Vol. 601, Springer, Berlin (1977), 107–148.
[28] Mazur, B., Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.* **44** (1978), no. 2, 129–162.
[29] Mazur, B. and Swinnerton-Dyer, P., Arithmetic of Weil curves, *Invent. Math.* **25** (1974), 1–61.
[30] Mazur, B. and Vélu, J., Courbes de Weil de conducteur 26, *C. R. Acad. Sci. Paris Sér. A-B* **275** (1972), A743–A745.
[31] Momose, F., Rational points on the modular curves $X_{\mathrm{split}}(p)$, *Compositio Math.* **52** (1984), no. 1, 115–137.
[32] Momose, F., Rational points on the modular curves $X_0^+(N)$, *J. Math. Soc. Japan* **39** (1987), no. 2, 269–286.
[33] Momose, F., Isogenies of prime degree over number fields, *Compositio Math.* **97** (1995), no. 3, 329–348.
[34] Momose, F. and Shimura, M., Lifting of supersingular points on $X_0(p^r)$ and lower bound of ramification index, *Nagoya Math. J.* **165** (2002), 159–178.
[35] Mumford, D., Abelian varieties, *Tata Institute of Fundamental Research Studies in Mathematics*, No. 5 Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London 1970.
[36] Ogg, A., Über die Automorphismengruppe von $X_0(N)$, *Math. Ann.* **228** (1977), no. 3, 279–292.
[37] Ohta, M., On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **21** (1974), 299–308.
[38] Ozeki, Y., Non-existence of certain Galois representations with a uniform tame inertia weight, *Int. Math. Res. Not.* **2011** (2011), no. 11, 2377–2395.

[39] Ozeki, Y., Non-existence of certain CM abelian varieties with prime power torsion, available from `http://arxiv.org/pdf/1112.3097v1.pdf`.

[40] Parent, P., Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$, *Compos. Math.* **141** (2005), no. 3, 561–572.

[41] Rasmussen, C. and Tamagawa, A., A finiteness conjecture on abelian varieties with constrained prime power torsion, *Math. Res. Lett.* **15** (2008), no. 6, 1223–1231.

[42] Rebolledo, M., Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires, *Pacific J. Math.* **234** (2008), no. 1, 167–184.

[43] Serre, J.-P., Abelian l-adic representations and elliptic curves, *Lecture at McGill University, New York-Amsterdam, W. A. Benjamin Inc.* (1968).

[44] Serre, J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, **15** (1972), no. 4, 259–331.

[45] 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.

[46] Serre, J.-P. and Tate, J., Good reduction of abelian varieties, *Ann. of Math. (2)* **88** (1968), 492–517.

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

[48] Silverman, J., Advanced topics in the arithmetic of elliptic curves, *Graduate Texts in Mathematics* **151**. Springer-Verlag, New York, 1994.