IDEAL CLASS GROUPS OF NUMBER FIELDS AND BLOCH-KATO'S TATE-SHAFAREVICH GROUPS FOR SYMMETRIC POWERS OF ELLIPTIC CURVES

NAOTO DAINOBU

Abstract. For an elliptic curve E over $\mathbb{Q}$, putting $K = \mathbb{Q}(E[p])$ which is the p-th division field of E for an odd prime p, we study the ideal class group Cl_K of K as a $\mathrm{Gal}(K/\mathbb{Q})$-module. More precisely, for any j with $1 \leqslant j \leqslant p-2$, we give a condition that $\mathrm{Cl}_K \otimes \mathbb{F}_p$ has the symmetric power $\mathrm{Sym}^j E[p]$ of $E[p]$ as its quotient $\mathrm{Gal}(K/\mathbb{Q})$-module, in terms of Bloch-Kato's Tate-Shafarevich group of $\mathrm{Sym}^j V_pE$. Here V_pE denotes the rational p-adic Tate module of E. This is a partial generalization of a result of Prasad and Shekhar for the case $j = 1$.

1. Introduction

The ideal class groups of number fields, the Tate-Shafarevich groups and the Selmer groups of elliptic curves are central objects to study in number theory. Many people have noticed the existence of various relations between the class groups and the Tate-Shafarevich groups, or the class groups and the Selmer groups. For example in [14], Washington considered a specific elliptic curve defined by the equation of the simplest cubic, and studied a relation between its 2-Selmer group and the class group of its 2-division field. In [6], Nekovář studied a relation between the ideal class groups of certain quadratic fields and the Tate-Shafarevich groups of twists of the cubic Fermat curve. We note here that they studied the ideal class groups of abelian number fields over $\mathbb{Q}$. In this paper, for an elliptic curve E over $\mathbb{Q}$ and an odd prime p, we suppose that the group of p-torsion points $E[p]$ of E is irreducible as a Galois module, and study the ideal class group of the p-th division field $K = \mathbb{Q}(E[p])$ of E which is a *non-commutative* Galois extension of $\mathbb{Q}$. More precisely, we relate the ideal class group Cl_K of K with Bloch-Kato's Tate-Shafarevich groups for symmetric powers of V_pE, where V_pE denotes the rational p-adic Tate module of E.

Recently Prasad and Shekhar have proved the following theorem on Cl_K with $K = \mathbb{Q}(E[p])$, which we first recall. In the situation above, the Galois group $G := \mathrm{Gal}(K/\mathbb{Q})$ acts on the class group Cl_K. In [10], they considered Cl_K as a G-module and proved the following result relating Cl_K with the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ of E over $\mathbb{Q}$.

Theorem (Prasad-Shekhar)**.** *Let $\rho_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ be the $\mathbb{F}_p$-valued Galois representation associated to E. Suppose that the following conditions on E hold:*

- (a) *E has good reduction at p.*
- (b) *In the case that E has good ordinary reduction at p, $a_p(E) \equiv 1 \pmod{p}$, and E has no CM over an extension of $\mathbb{Q}_p$, then $\rho_{E,p}$ is wildly ramified at p.*
- (c) *For every prime number $l \neq p$, the Tamagawa number $c_l(E/\mathbb{Q}_l)$ of $E/\mathbb{Q}_l$ is prime to p.*
- (d) *$E[p]$ is an irreducible $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module.*

Then the condition $\dim_{\mathbb{F}_p}(\text{Ш}(E/\mathbb{Q})[p]) \geqslant 2$ implies that the $\mathbb{F}_p$-representation $\mathrm{Cl}_K \otimes \mathbb{F}_p$ of G has $E[p]$ as its quotient representation.

From the above theorem, we see that the $\mathbb{F}_p$-rank of $\text{Ш}(E/\mathbb{Q})[p]$ gives us the information on $\mathrm{Cl}_K \otimes \mathbb{F}_p$ as a G-module. We remark that they also studied in [10] the condition on which $\mathrm{Cl}_K \otimes \mathbb{F}_p$ has $E[p]$ as its quotient representation even if $\text{Ш}(E/\mathbb{Q})[p] = 0$.

The main result of this article is an analogy of the above theorem for the symmetric powers of $E[p]$. In the following, we further assume that the representation $\rho_{E,p}$ is surjective, so the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$. It is a well-known fact that any irreducible representation of $G = \mathrm{GL}_2(\mathbb{F}_p)$ in characteristic p is of the form $\mathrm{Sym}^j E[p] \otimes \det^i$ $(0 \leqslant j \leqslant p-1,\ 0 \leqslant i \leqslant p-2)$, where det denotes the determinant character of $\mathrm{GL}_2(\mathbb{F}_p)$. So taking the above theorem one step further, we consider the condition on which the $\mathbb{F}_p$-representation $\mathrm{Cl}_K \otimes \mathbb{F}_p$ of G has an irreducible representation $\mathrm{Sym}^j E[p]$ as its quotient representation.

Now we explain our main result. For any j with $1 \leqslant j \leqslant p-1$, we define $V_p^j := \mathrm{Sym}^j(V_p E)$ to simplify the notation. One of the key objects in the main result is Bloch-Kato's Tate-Shafarevich group $\text{Ш}^{BK}_{\mathbb{Q}}(V_p^j)$ of V_p^j whose definition we shall recall in Definition 2.2 in Section 2. See also [1, Definition 5.1]. The main result of this article is as follows.

Theorem 1.1. *Let $p > 3$. For any j with $1 \leqslant j \leqslant p-2$, suppose that the following conditions on E hold:*

- (a') *E has good reduction at p.*
- (b') *In the case that E has good ordinary reduction at p, $a_p(E)^j \equiv 1 \pmod{p}$, and E has no CM over an extension of $\mathbb{Q}_p$, then $\rho_{E,p}$ is wildly ramified at p.*
- (c') *If E has potentially multiplicative reduction at $l \neq p$, then $v_l(j(E))$ is prime to p, where v_l denotes the normalized l-adic valuation and $j(E)$ the j-invariant of E.*
- (d') *The representation $\rho_{E,p}$ is surjective.*

Then the condition $\dim_{\mathbb{F}_p}(Ш^{BK}_{\mathbb{Q}}(V_p^j)[p]) \geqslant j+1$ *implies that the* $\mathbb{F}_p$*-representation* $\mathrm{Cl}_K \otimes \mathbb{F}_p$ *of* G *has* $\mathrm{Sym}^j E[p]$ *as its quotient representation.*

Remark 1.2. The assumptions (a') in Theorem 1.1 and (a) in the theorem of Prasad and Shekhar are the same. The assumption (b') for $j=1$ is exactly (b). The assumption (c') implies the assumption (c) when E has good or split multiplicative reduction at every prime since we have $c_l(E/\mathbb{Q}_l) = -v_l(j(E))$ when E has split multiplicative reduction at l. The assumption (d') also implies the assumption (d). Hence when $j=1$, we can deduce the theorem of Prasad and Shekhar from our Theorem 1.1 if E has only good or split multiplicative reduction at any prime and the representation $\rho_{E,p}$ is surjective. So interestingly, using Bloch-Kato's Tate-Shafarevich groups $Ш^{BK}_{\mathbb{Q}}(V_p^j)$ for various j other than $j=1$, we can get more information about the structure of $\mathrm{Cl}_K \otimes \mathbb{F}_p$ as a G-module.

Remark 1.3. We can generalize the argument in this paper for more general Galois representations other than $\mathrm{Sym}^j E[p]$. In Remark 2.3, we explain that we can show a result analogous to Theorem 1.1 for the $\mathbb{F}_p$-valued Galois representations attached to modular forms using a similar argument in this article.

We give a sketch of the proof of Theorem 1.1 in Section 2 dividing it into 3 steps. We prove step 1 in Section 3, step 2 in Section 4 and step 3 in Sections 5 and 6.

2. A sketch of the proof

We mainly follow the strategy of the proof of Prasad and Shekhar in [10]. They used the classical p-Selmer group $\mathrm{Sel}_p(E/\mathbb{Q})$ but, to treat representations such as $\mathrm{Sym}^j E[p]$, we have to deal with Bloch-Kato's Selmer group H^1_f which we first recall.

For a field F, G_F denotes its absolute Galois group $\mathrm{Gal}(\overline{F}/F)$. We define $T_p^j := \mathrm{Sym}^j(T_pE)$, $A_p^j := V_p^j/T_p^j \cong \mathrm{Sym}^j E[p^\infty]$, where T_pE is the integral p-adic Tate module of E. For every prime l, we define a local condition $H^1_f(\mathbb{Q}_l, V_p^j)$ in $H^1(\mathbb{Q}_l, V_p^j)$ as

$$\begin{cases} H^1_f(\mathbb{Q}_l, V_p^j) := \mathrm{Ker}\left(H^1(\mathbb{Q}_l, V_p^j) \to H^1(\mathbb{Q}_l^{\mathrm{ur}}, V_p^j)\right) & (l \neq p) \\ H^1_f(\mathbb{Q}_p, V_p^j) := \mathrm{Ker}\left(H^1(\mathbb{Q}_p, V_p^j) \to H^1(\mathbb{Q}_p, V_p^j \otimes \mathbf{B}_{\mathrm{crys}})\right) & (l = p). \end{cases}$$

Here $\mathbb{Q}_l^{\mathrm{ur}}$ is the maximal unramified extension of $\mathbb{Q}_l$ and $\mathbf{B}_{\mathrm{crys}}$ denotes Fontaine's crystalline period ring which is defined in [1, Section 1]. Then we define $H^1_f(\mathbb{Q}_l, A_p^j) := \pi\left(H^1_f(\mathbb{Q}_l, V_p^j)\right)$ for each prime l, where $\pi : H^1(\mathbb{Q}_l, V_p^j) \to H^1(\mathbb{Q}_l, A_p^j)$ is the homomorphism induced by the natural map $\pi : V_p^j \to A_p^j$. We define Bloch-Kato's Selmer group for V_p^j and A_p^j using these local conditions.

Definition 2.1. *For $V_p^j = \mathrm{Sym}^j(V_pE)$ and $A_p^j = V_p^j/T_p^j \cong \mathrm{Sym}^j E[p^\infty]$, we define Bloch-Kato's Selmer groups as*

$$H^1_f(\mathbb{Q}, V_p^j) := \mathrm{Ker}\left(H^1(\mathbb{Q}, V_p^j) \xrightarrow{\prod \mathrm{Loc}_l} \prod_l \frac{H^1(\mathbb{Q}_l, V_p^j)}{H^1_f(\mathbb{Q}_l, V_p^j)} \right),$$

$$H^1_f(\mathbb{Q}, A_p^j) := \mathrm{Ker}\left(H^1(\mathbb{Q}, A_p^j) \xrightarrow{\prod \mathrm{Loc}_l} \prod_l \frac{H^1(\mathbb{Q}_l, A_p^j)}{H^1_f(\mathbb{Q}_l, A_p^j)} \right),$$

where Loc_l denotes the restriction of cohomology classes to the decomposition group at l and the products run over all prime numbers.

The p-part of Bloch-Kato's Tate-Shafarevich group $Ш^{BK}_{\mathbb{Q}}(V_p^j)$ is defined in [1, Definition 5.1] as follows.

Definition 2.2. *We define the p-part of Bloch-Kato's Tate-Shafarevich group for $V_p^j(= \mathrm{Sym}^j(V_pE))$ as*

$$Ш^{BK}_{\mathbb{Q}}(V_p^j) := \frac{H^1_f(\mathbb{Q}, A_p^j)}{\pi(H^1_f(\mathbb{Q}, V_p^j))},$$

where the cohomology groups $H^1_f(\mathbb{Q}, A_p^j), H^1_f(\mathbb{Q}, V_p^j)$ are defined as in Definition 2.1 and $\pi : H^1(\mathbb{Q}, V_p^j) \to H^1(\mathbb{Q}, A_p^j)$ is the canonical homomorphism induced by the natural map $\pi : V_p^j \to A_p^j$. In other words, $Ш^{BK}_{\mathbb{Q}}(V_p^j)$ is defined by the exact sequence

$$0 \to \pi(H^1_f(\mathbb{Q}, V_p^j)) \to H^1_f(\mathbb{Q}, A_p^j) \to Ш^{BK}_{\mathbb{Q}}(V_p^j) \to 0.$$

Now we give a sketch of the proof of Theorem 1.1. In the following argument, we assume that the conditions $(a'), (b'), (c')$ and (d') in Theorem 1.1 hold.

(Step1) We show the restriction map

$$\mathrm{Res}_{K/\mathbb{Q}} : H^1(\mathbb{Q}, \mathrm{Sym}^j E[p]) \to H^1(K, \mathrm{Sym}^j E[p])^G$$

is an isomorphism where G denotes $\mathrm{Gal}(K/\mathbb{Q})$.

For a number field F, we define the unramified cohomology group $H^1_{\mathrm{ur}}(F, \mathrm{Sym}^j E[p])$ as the subgroup of cohomology classes in $H^1(F, \mathrm{Sym}^j E[p])$ which are trivial on the inertia group at every place of F. Assuming the claim in (Step1), the restriction $\mathrm{Res}_{K/\mathbb{Q}}$ induces an injective homomorphism between unramified cohomology groups

$$\mathrm{Res}_{K/\mathbb{Q}} : H^1_{\mathrm{ur}}(\mathbb{Q}, \mathrm{Sym}^j E[p]) \to H^1_{\mathrm{ur}}(K, \mathrm{Sym}^j E[p])^G.$$

Using class field theory, we have $H^1_{\mathrm{ur}}(K, \mathrm{Sym}^j E[p])^G = \mathrm{Hom}_G(\mathrm{Cl}_K \otimes \mathbb{F}_p, \mathrm{Sym}^j E[p])$. Every nontrivial homomorphism in $\mathrm{Hom}_G(\mathrm{Cl}_K \otimes \mathbb{F}_p, \mathrm{Sym}^j E[p])$ is surjective since $\mathrm{Sym}^j E[p]$ is irreducible. Thus the condition $H^1_{\mathrm{ur}}(\mathbb{Q}, \mathrm{Sym}^j E[p]) \neq 0$ implies that

$\mathrm{Cl}_K \otimes \mathbb{F}_p$ has $\mathrm{Sym}^j E[p]$ as its quotient G-module. We will construct nontrivial elements in $H^1_{\mathrm{ur}}(\mathbb{Q}, \mathrm{Sym}^j E[p])$ using Bloch-Kato's Selmer group in the succeeding steps.

(Step2) We show that the image of $H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p])$ in $H^1(\mathbb{Q}_l^{\mathrm{ur}}, \mathrm{Sym}^j E[p])$ is zero for any prime number $l \neq p$.

Here the cohomology group $H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p])$ is defined as follows. We have an exact sequence

$$0 \to \mathrm{Sym}^j E[p] \xrightarrow{\iota} A_p^j \xrightarrow{\times p} A_p^j \to 0$$

from which we obtain an exact sequence

$$0 \to \frac{H^0(\mathbb{Q}, A_p^j)}{pH^0(\mathbb{Q}, A_p^j)} \to H^1(\mathbb{Q}, \mathrm{Sym}^j E[p]) \xrightarrow{\iota} H^1(\mathbb{Q}, A_p^j)[p] \to 0,$$

where the map ι in the first exact sequence denotes the inclusion. We define the cohomology group $H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p])$ as the inverse image of the p-torsion part of Bloch-Kato's Selmer group $H^1_f(\mathbb{Q}, A_p^j)[p]$ under ι. Assuming the claim in (Step2), for the restriction map

$$\mathrm{Res}_p^{\mathrm{ur}} : H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p]) \to H^1(\mathbb{Q}_p^{\mathrm{ur}}, \mathrm{Sym}^j E[p]),$$

we have $\mathrm{Ker}(\mathrm{Res}_p^{\mathrm{ur}}) \subset H^1_{\mathrm{ur}}(\mathbb{Q}, \mathrm{Sym}^j E[p])$. Thus it suffices to show $\mathrm{Ker}(\mathrm{Res}_p^{\mathrm{ur}}) \neq 0$ to get the main theorem.

(Step3) We study the image of $\mathrm{Res}_p^{\mathrm{ur}}$ and prove that $\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Res}_p^{\mathrm{ur}})) \leqslant j$.

In Definition 2.2, we have an exact sequence

$$0 \to \pi(H^1_f(\mathbb{Q}, V_p^j)) \to H^1_f(\mathbb{Q}, A_p^j) \to Ш_{\mathbb{Q}}^{BK}(V_p^j) \to 0.$$

Since the group $\pi(H^1_f(\mathbb{Q}, V_p^j))$ is p-divisible, the above homomorphism $H^1_f(\mathbb{Q}, A_p^j) \to Ш_{\mathbb{Q}}^{BK}(V_p^j)$ is still surjective when restricted on the p-torsion parts. Since $H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p])$ is defined as the inverse image of $H^1_f(\mathbb{Q}, A_p^j)[p]$ under the surjection ι, we have a surjective map $H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p]) \twoheadrightarrow Ш_{\mathbb{Q}}^{BK}(V_p^j)[p]$. So if we assume the condition $\dim_{\mathbb{F}_p}(Ш_{\mathbb{Q}}^{BK}(V_p^j)[p]) \geqslant j+1$ in Theorem 1.1, then we have $\dim_{\mathbb{F}_p}(H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p])) \geqslant j+1$. From the claim in (Step3), we have $\mathrm{Ker}(\mathrm{Res}_p^{\mathrm{ur}}) \neq 0$ and the theorem follows.

Remark 2.3. We can apply the above argument to more general p-adic Galois representations. For example, the representations attached to modular forms can be treated. Let f be a normalized new eigen cusp form whose coefficients are in $\mathbb{Q}$ and level prime to p. For this modular form f, we have an associated integral p-adic Galois representation $\rho_{f,p} : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_{f,p}) \cong \mathrm{GL}_2(\mathbb{Z}_p)$, where $T_{f,p}$ is its representation space which is a free $\mathbb{Z}_p$ module of rank 2. Let $\overline{\rho}_{f,p} : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_p}(\overline{T}_{f,p}) \cong \mathrm{GL}_2(\mathbb{F}_p)$ be the mod p reduction of $\rho_{f,p}$. We consider twists of these representations. For a square-free integer D and $j \in \mathbb{Z}$, let $\rho_{f,p}(j,D) := \rho_{f,p} \otimes \chi_D \otimes \chi_{\mathrm{cyc}}^j : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_{f,p}(j,D)) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ be a twist of $\rho_{f,p}$ by a quadratic Dirichlet character χ_D associated to D and χ_{cyc}^j, where χ_{cyc} is the p-adic cyclotomic character. Let $\overline{\rho}_{f,p}(j,D) : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ be the mod p reduction of $\rho_{f,p}(j,D)$ corresponding to $\overline{T}_{f,p}(j,D) := T_{f,p}(j,D) \otimes \mathbb{Z}/p$. For the $\mathbb{F}_p$-valued representation $\overline{\rho}_{f,p}(j,D)$, we have a number field $K_{f,p,(j,D)}$ corresponding to the kernel of $\overline{\rho}_{f,p}(j,D)$. Let $\mathrm{Cl}_{f,p,(j,D)}$ be the ideal class group of $K_{f,p,(j,D)}$. We can apply the same argument in this article to the p-adic representation $V_{f,p}(j,D) := T_{f,p}(j,D) \otimes \mathbb{Q}_p$ under similar assumptions to those in Theorem 1.1. Then we can deduce that the condition $\dim_{\mathbb{F}_p}(\text{Ш}_{\mathbb{Q}}^{BK}(V_{f,p}(j,D))[p]) \geqslant 2$ implies that the $\mathbb{F}_p$-representation $\mathrm{Cl}_{f,p,(j,D)} \otimes \mathbb{F}_p$ of $\mathrm{Gal}(K_{f,p,(j,D)}/\mathbb{Q})$ has $\overline{T}_{f,p}(j,D)$ as its quotient representation. Assuming the Bloch-Kato conjecture, we can make some numerical examples of the above result with some calculations of special values of L-functions attached to f and various χ_D. We will describe the details of this result in our forthcoming paper.

3. Injectivity of the restriction map

In this section, we prove the claim in (Step1) in the previous section.

Proposition 3.1. *Suppose the representation $\rho_{E,p}$ is surjective. Then the restriction map*

$$\mathrm{Res}_{K/\mathbb{Q}} : H^1(\mathbb{Q}, \mathrm{Sym}^j E[p]) \to H^1(K, \mathrm{Sym}^j E[p])^G$$

is an isomorphism.

(Proof of Proposition 3.1)

It suffices to show that $H^1(G, \mathrm{Sym}^j E[p]) = H^2(G, \mathrm{Sym}^j E[p]) = 0$. We use the following lemma.

Lemma 3.2. *Let G be a finite group and V a finite dimensional representation of G over a field F of characteristic p. If there is a normal subgroup H of G such that*

(1) *$\#H$ is prime to p*
(2) *$V^H = 0$*

then $H^i(G,V) = 0$ for all $i \geqslant 0$.

(Proof of lemma 3.2)

The condition (2) implies $H^0(G,V) = 0$. We have the inflation-restriction exact sequence

$$0 \to H^1(G/H, V^H) \xrightarrow{\mathrm{inf}} H^1(G,V) \xrightarrow{\mathrm{res}} H^1(H,V)^G.$$

Since $V^H = 0$ and $\#H$ is prime to p, the first and the third term in the above sequence are 0 and we get $H^1(G,V) = 0$. Since $H^1(H,V) = 0$, we also have the inflation-restriction exact sequences for the cohomology groups of higher degree inductively to get $H^i(G,V) = 0$ for $i \geqslant 0$. □

We go back to the proof of the proposition. Since we assume $1 \leqslant j \leqslant p-2$, there is an element $c \in \mathbb{F}_p^\times$ such that $c^j \neq 1$. The central element cI acts on $E[p]$ by multiplication by c, here I denotes the unit matrix in $\mathrm{GL}_2(\mathbb{F}_p)$. Then cI acts on $\mathrm{Sym}^j E[p]$ by multiplication by $c^j (\neq 1)$. Let C be the subgroup of G generated by cI. Since cI is a central element and $c \in \mathbb{F}_p^\times$, C is a normal subgroup of G and $\#C$ is prime to p. So the subgroup C satisfies the conditions (1), (2) of Lemma 3.2, then we have $H^i(G, \mathrm{Sym}^j E[p]) = 0$ for $i \geqslant 0$ and $1 \leqslant j \leqslant p-2$. Hence the injectivity of $\mathrm{Res}_{K/\mathbb{Q}} : H^1(\mathbb{Q}, \mathrm{Sym}^j E[p]) \to H^1(K, \mathrm{Sym}^j E[p])^G$ follows. □

4. The cohomology group $H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p])$

Next we show the claim in (Step2) in Section 2.

Proposition 4.1. *For a prime $l \neq p$, suppose $v_l(j(E))$ is prime to p when E has potentially multiplicative reduction at l. Then the elements in $H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p])$ are unramified outside p.*

(Proof of Proposition 4.1)

Since p is an odd prime, any elements in $H^1(\mathbb{Q}, \mathrm{Sym}^j E[p])$ are unramified at the infinite place of $\mathbb{Q}$ automatically.

For every prime number $l \neq p$, we have the following commutative diagram

$$\begin{tikzcd}
 & & H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p]) \arrow[r, "\iota"] \arrow[d, "\mathrm{Res}_l^{\mathrm{ur}}"] & H^1_f(\mathbb{Q}, A_p^j)[p] \arrow[r] \arrow[d, "\mathrm{res}_l^{\mathrm{ur}}"] & 0 \\
0 \arrow[r] & \dfrac{H^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j)}{pH^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j)} \arrow[r] & H^1(\mathbb{Q}_l^{\mathrm{ur}}, \mathrm{Sym}^j E[p]) \arrow[r, "\iota"] & H^1(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j)[p] \arrow[r] & 0.
\end{tikzcd}$$

Here $\mathrm{Res}_l^{\mathrm{ur}}$ denotes the restriction of cohomology classes to the inertia at l and ι is the homomorphism induced by the inclusion $\mathrm{Sym}^j E[p] \hookrightarrow A_p^j$. What we have to show is that for any cohomology classes $c \in H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p])$, we have $\mathrm{Res}_l^{\mathrm{ur}}(c) = 0$. So it suffices to show $\frac{H^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j)}{pH^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j)} = 0$.

(Case 1) E has good reduction at l.

In this case, $\mathrm{Sym}^j E[p^n]$ is unramified at l for any positive integer n. So we have $H^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j) = (\mathbb{Q}_p/\mathbb{Z}_p)^{\oplus(j+1)}$ to get $\frac{H^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j)}{pH^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j)} = 0$.

(Case 2) E has split multiplicative reduction at l.

In this case, using the result of Tate, we have an isomorphism $E(\overline{\mathbb{Q}_l}) \cong \overline{\mathbb{Q}_l}^\times / \langle q \rangle$ as $G_{\mathbb{Q}_l}$-modules, here q is the Tate period for E in $\mathbb{Q}_l$. Then for a positive integer n, the group of p^n-torsion points $E[p^n]$ is isomorphic to a free $\mathbb{Z}/p^n$-module generated by ζ_{p^n} and $\sqrt[p^n]{q}$, where ζ_{p^n} and $\sqrt[p^n]{q}$ denote a primitive p^n-th root of unity and a p^n-th root of q respectively. So with respect to this basis, $G_{\mathbb{Q}_l^{\mathrm{ur}}}$ acts on $E[p^n]$ via

$$\begin{pmatrix} 1 & \tau_{q,n} \\ 0 & 1 \end{pmatrix},$$

where $\tau_{q,n} : G_{\mathbb{Q}_l^{\mathrm{ur}}} \to \mathbb{Z}/p^n$ is the map defined by $g(\sqrt[p^n]{q}) = \sqrt[p^n]{q} \cdot \zeta_{p^n}^{\tau_{q,n}(g)}$ $(g \in G_{\mathbb{Q}_l^{\mathrm{ur}}})$. For a positive integer n, we compute $H^0(\mathbb{Q}_l^{\mathrm{ur}}, \mathrm{Sym}^j E[p^n])$ explicitly. First, we fix a basis of $\mathrm{Sym}^j E[p^n]$ over $\mathbb{Z}/p^n$ as

$$u_0 := \zeta_{p^n}^{\otimes j},\ u_1 := \zeta_{p^n}^{\otimes j-1} \otimes \sqrt[p^n]{q},\ \ldots, u_i := \zeta_{p^n}^{\otimes j-i} \otimes \sqrt[p^n]{q}^{\otimes i},\ \ldots,\ u_j := \sqrt[p^n]{q}^{\otimes j}.$$

Lemma 4.2. *For an element $x := a_0u_0 + a_1u_1 + \cdots + a_ju_j \in \mathrm{Sym}^j E[p^n]$ with $a_i \in \mathbb{Z}/p^n$, the condition $x \in \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_l^{\mathrm{ur}}}}$ is equivalent to the condition*

$$a_0 \in \mathbb{Z}/p^n,\ a_1\tau_{q,n}(g) = a_2\tau_{q,n}(g) = \cdots = a_j\tau_{q,n}(g) = 0 \quad \textit{in } \mathbb{Z}/p^n \quad (\forall g \in G_{\mathbb{Q}_l^{\mathrm{ur}}}).$$

(Proof of Lemma 4.2)
This can be proved by an explicit calculation. For i with $0 \leqslant i \leqslant j$ and $g \in G_{\mathbb{Q}_l^{\mathrm{ur}}}$, we have

$$g(u_i) = g(\zeta_{p^n}^{\otimes j-i} \otimes \sqrt[p^n]{q}^{\otimes i}) \ = \ \zeta_{p^n}^{\otimes j-i} \otimes (\tau_{q,n}(g)\zeta_{p^n} + \sqrt[p^n]{q})^{\otimes i} = \sum_{k=0}^{i} \binom{i}{k} \tau_{q,n}(g)^k u_{i-k}.$$

So for $x := a_0u_0 + a_1u_1 + \cdots + a_ju_j \in \mathrm{Sym}^j E[p^n]$, we can deduce that the condition $x \in \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_l^{\mathrm{ur}}}}$ is equivalent to the condition

$$\sum_{k=i+1}^{j} \binom{k}{i} a_k \tau_{q,n}(g)^{k-i} = 0 \quad \textit{in } \mathbb{Z}/p^n \quad (0 \leqslant i \leqslant j-1) \tag{1}$$

for all $g \in G_{\mathbb{Q}_l^{\mathrm{ur}}}$. When $i = j-1$, we have $\binom{j}{j-1} a_j\tau_{q,n}(g) = 0$ from the equation (1) to get $a_j\tau_{q,n}(g) = 0$ since $j \leqslant p-2$. When $i = j-2$, we have

$$\binom{j-1}{j-2} a_{j-1}\tau_{q,n}(g) + \binom{j}{j-2} a_j\tau_{q,n}(g)^2 = 0$$

from (1). Since $a_j\tau_{q,n}(g) = 0$ and $j \leqslant p-2$, we also have $a_{j-1}\tau_{q,n}(g) = 0$. By backward induction on i, we can get $a_i\tau_{q,n}(g) = 0$ for $1 \leqslant i \leqslant j$. □

We go back to the proof of Proposition 4.1. If there is an element $g \in G_{\mathbb{Q}_l^{\mathrm{ur}}}$ such that $\tau_{q,n}(g) \in (\mathbb{Z}/p^n)^\times$, then we have $a_1 = a_2 = \cdots = a_j = 0$ and $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_l^{\mathrm{ur}}}} \cong \mathbb{Z}/p^n$ for any n from Lemma 4.2. Thus we have $H^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j) \cong \mathbb{Q}_p/\mathbb{Z}_p$ and $\frac{H^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j)}{pH^0(\mathbb{Q}_l^{\mathrm{ur}}, A_p^j)} = 0$. So we will show in the following that there exists such $g \in G_{\mathbb{Q}_l^{\mathrm{ur}}}$ under the assumptions in Proposition 4.1. It is a well-known fact that if an elliptic curve E over $\mathbb{Q}_l$

has split multiplicative reduction, then $v_l(j(E)) = -v_l(q)$ where v_l is the normalized l-adic valuation on $\mathbb{Q}_l$ and q is the Tate period for E. Since we assume $v_l(j(E))$ is prime to p, q is not a p-th power in $\mathbb{Q}_l$. So we have $\sqrt[p^n]{q} \notin \mathbb{Q}_l$ for any $n \in \mathbb{Z}_{>0}$ and $\sqrt[p^n]{q} \notin \mathbb{Q}_l^{\mathrm{ur}}$ since $v_l(q) > 0$. Then there exists $g \in G_{\mathbb{Q}_l^{\mathrm{ur}}}$ such that $\tau_{q,n}(g) \in (\mathbb{Z}/p^n)^\times$ for any n and the proposition follows in this case.

(Case 3) E has non-split multiplicative reduction at l.

In this case, E has split multiplicative reduction at l over the unramified quadratic extension F of $\mathbb{Q}_l$. So we can imitate the argument in the (Case 2) over F to get the desired result.

(Case 4) E has additive potentially multiplicative reduction at l.

In this case, E has split multiplicative reduction at a prime above l over a ramified quadratic extension L of $\mathbb{Q}_l$. So there exists some quadratic twist E' of the elliptic curve E, which has split multiplicative reduction at l and for each positive integer n, as $G_{\mathbb{Q}_l}$-modules, we have

$$E[p^n] \cong E'[p^n] \otimes \chi$$

here χ denotes the ramified quadratic character corresponds to L. Taking the Tate period q for E', for some suitable basis $\{v_1, v_2\}$, we know that the action of $G_{\mathbb{Q}_l^{\mathrm{ur}}}$ on $E[p^n]$ is of the form:

$$\begin{pmatrix} 1 & \tau_{q,n} \\ 0 & 1 \end{pmatrix} \otimes \chi$$

as in the argument in (Case 2). We again fix a basis of $\mathrm{Sym}^j E[p^n]$ over $\mathbb{Z}/p^n\mathbb{Z}$ as

$$u_0 := v_1^{\otimes j},\ u_1 := v_1^{\otimes j-1} \otimes v_2,\ \ldots, u_i := v_1^{\otimes j-i} \otimes v_2^{\otimes i},\ \ldots,\ u_j := v_2^{\otimes j}.$$

For an element $x := a_0u_0 + a_1u_1 + \cdots + a_ju_j \in \mathrm{Sym}^j E[p^n]$ with $a_i \in \mathbb{Z}/p^n\mathbb{Z}$, we can show that the condition $x \in \mathrm{Sym}^j E[p^n]^{G_{L\cdot\mathbb{Q}_l^{\mathrm{ur}}}}$ is equivalent to the condition

$$a_0 \in \mathbb{Z}/p^n\mathbb{Z},\ a_1\tau_{q,n}(g) = a_2\tau_{q,n}(g) = \cdots = a_j\tau_{q,n}(g) = 0 \ \text{ in } \mathbb{Z}/p^n \quad (\forall g \in G_{L\cdot\mathbb{Q}_l^{\mathrm{ur}}})$$

by the same calculation as in the proof of Lemma 4.2 since χ is trivial on $G_{L\cdot\mathbb{Q}_l^{\mathrm{ur}}}$. On the other hand, we have $\sqrt[p^n]{q} \notin \mathbb{Q}_l^{\mathrm{ur}}$ for any positive integer n by the assumption that p does not divide $v_l(q) = -v_l(j(E')) = -v_l(j(E))$. We know $\sqrt[p^n]{q}$ is also not contained in $L \cdot \mathbb{Q}_l^{\mathrm{ur}}$ because $L \cdot \mathbb{Q}_l^{\mathrm{ur}}/\mathbb{Q}_l^{\mathrm{ur}}$ is a quadratic extension and $p \neq 2$. So there exists $g \in G_{L\cdot\mathbb{Q}_l^{\mathrm{ur}}}$ such that $\tau_{q,n}(g) \in (\mathbb{Z}/p^n)^\times$ for every n and we get $a_1 = a_2 = \ldots = a_j = 0$ as in the argument in (Case 2). Thus we get $(\mathrm{Sym}^j E[p^n])^{G_{L\cdot\mathbb{Q}_l^{\mathrm{ur}}}} = \mathbb{Z}/p^n \cdot u_0$ and $(\mathrm{Sym}^j E[p^n])^{G_{\mathbb{Q}_l^{\mathrm{ur}}}} = (\mathbb{Z}/p^n \cdot u_0)^{\mathrm{Gal}(L/\mathbb{Q}_l)}$. Let τ denote a generator of the Galois group $\mathrm{Gal}(L/\mathbb{Q}_l)$. Then $\tau(u_0) = \chi(\tau)^j u_0 = (-1)^j u_0$. So we have

$$\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_l^{\mathrm{ur}}}} = \begin{cases} 0 & (j \text{ is odd}) \\ \mathbb{Z}/p^n \cdot u_0 & (j \text{ is even}). \end{cases}$$

We have $\frac{H^0(\mathbb{Q}_l^{\mathrm{ur}},A_p^j)}{pH^0(\mathbb{Q}_l^{\mathrm{ur}},A_p^j)}=0$ in both cases.

(Case 5) E has additive potentially good reduction at l.

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ be the representation associated to the integral p-adic Tate module of E. It is a well-known fact that when E has potentially good reduction at l, then $\#\rho(G_{\mathbb{Q}_l^{\mathrm{ur}}})$ is finite and its possible prime divisors are only 2 and 3. See for example, [2, Section 3.3]. So we get $p \nmid \#\rho(G_{\mathbb{Q}_l^{\mathrm{ur}}})$ since we assume $p \geqslant 5$. Let $\rho_j : G_{\mathbb{Q}} \to \mathrm{GL}_{j+1}(\mathbb{Z}_p)$ be the representation attached to T_p^j. Then we have $\mathrm{Ker}(\rho) \subset \mathrm{Ker}(\rho_j)$ to get a natural surjection $\rho(G_{\mathbb{Q}_l^{\mathrm{ur}}}) \twoheadrightarrow \rho_j(G_{\mathbb{Q}_l^{\mathrm{ur}}})$. Thus we also get $p \nmid \#\rho_j(G_{\mathbb{Q}_l^{\mathrm{ur}}})$. This implies that there is an open normal subgroup U of $G_{\mathbb{Q}_l^{\mathrm{ur}}}$ such that $\rho_j(U)=0$ and $[G_{\mathbb{Q}_l^{\mathrm{ur}}} : U]$ is prime to p. Then we have the inflation-restriction exact sequence

$$0 \to H^1(G_{\mathbb{Q}_l^{\mathrm{ur}}}/U, (T_p^j)^U) \to H^1(G_{\mathbb{Q}_l^{\mathrm{ur}}}, T_p^j) \to H^1(U, T_p^j)^{G_{\mathbb{Q}_l^{\mathrm{ur}}}/U} \to H^2(G_{\mathbb{Q}_l^{\mathrm{ur}}}/U, (T_p^j)^U).$$

Since the order of $G_{\mathbb{Q}_l^{\mathrm{ur}}}/U$ is prime to p, we have $H^i(G_{\mathbb{Q}_l^{\mathrm{ur}}}/U, (T_p^j)^U)=0$ for $i=1,2$ and obtain an isomorphism

$$H^1(G_{\mathbb{Q}_l^{\mathrm{ur}}}, T_p^j) \cong H^1(U, T_p^j)^{G_{\mathbb{Q}_l^{\mathrm{ur}}}/U}$$

induced by the restriction map. We know that U acts trivially on T_p^j to get $H^1(U,T_p^j) = \mathrm{Hom}(U,T_p^j)$. Since T_p^j is torsion-free, this group $\mathrm{Hom}(U,T_p^j)$ and of course its subgroup $H^1(U,T_p^j)^{G_{\mathbb{Q}_l^{\mathrm{ur}}}/U}$ are torsion-free. On the other hand, we have an exact sequence $0 \to T_p^j \to V_p^j \to A_p^j \to 0$ from which we also have an exact sequence

$$0 \to (T_p^j)^{G_{\mathbb{Q}_l^{\mathrm{ur}}}} \otimes \mathbb{Q}_p/\mathbb{Z}_p \to (A_p^j)^{G_{\mathbb{Q}_l^{\mathrm{ur}}}} \to H^1(G_{\mathbb{Q}_l^{\mathrm{ur}}}, T_p^j)[p^\infty] \to 0.$$

Since $H^1(G_{\mathbb{Q}_l^{\mathrm{ur}}}, T_p^j)[p^\infty]=0$ from the above argument, we have $(T_p^j)^{G_{\mathbb{Q}_l^{\mathrm{ur}}}} \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (A_p^j)^{G_{\mathbb{Q}_l^{\mathrm{ur}}}}$ and $(A_p^j)^{G_{\mathbb{Q}_l^{\mathrm{ur}}}} = H^0(G_{\mathbb{Q}_l^{\mathrm{ur}}}, A_p^j)$ is divisible. Thus $\frac{H^0(\mathbb{Q}_l^{\mathrm{ur}},A_p^j)}{pH^0(\mathbb{Q}_l^{\mathrm{ur}},A_p^j)}=0$. We have proved the Proposition 4.1 in all cases. □

5. The image of the restriction map $\mathrm{Res}_p^{\mathrm{ur}}$

We finally prove the following proposition which is the claim in (Step 3).

Proposition 5.1. *For the restriction map*

$$\mathrm{Res}_p^{\mathrm{ur}} : H_f^1(\mathbb{Q}, \mathrm{Sym}^j E[p]) \to H^1(\mathbb{Q}_p^{\mathrm{ur}}, \mathrm{Sym}^j E[p]),$$

we have

$$\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Res}_p^{\mathrm{ur}})) \leqslant j.$$

For the above restriction map, we have a decomposition

$$\mathrm{Res}_p^{\mathrm{ur}} : H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p]) \xrightarrow{\mathrm{Loc}_p} H^1(\mathbb{Q}_p, \mathrm{Sym}^j E[p]) \xrightarrow{\mathrm{Res}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p}} H^1(\mathbb{Q}_p^{\mathrm{ur}}, \mathrm{Sym}^j E[p]).$$

Here the homomorphism Loc_p is the restriction of cohomology classes to the decomposition group at p, and $\mathrm{Res}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p}$ is the restriction of them to the inertia group at p. So first we study the image of Loc_p. We have the following commutative diagram

$$\begin{tikzcd}
 & H^1_f(\mathbb{Q}, \mathrm{Sym}^j E[p]) \arrow[r, "\iota"] \arrow[d, "\mathrm{Loc}_p"] & H^1_f(\mathbb{Q}, A_p^j)[p] \arrow[r] \arrow[d, "\mathrm{loc}_p"] & 0 \\
0 \arrow[r] & \dfrac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)} \arrow[r] & H^1(\mathbb{Q}_p, \mathrm{Sym}^j E[p]) \arrow[r, "\iota"] & H^1(\mathbb{Q}_p, A_p^j)[p] \arrow[r] & 0.
\end{tikzcd}$$

So we have $\mathrm{Im}(\mathrm{Loc}_p) \subset \iota^{-1}(H^1_f(\mathbb{Q}_p, A_p^j)[p])$ and there is an exact sequence

$$0 \to \frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)} \to \iota^{-1}(H^1_f(\mathbb{Q}_p, A_p^j)[p]) \xrightarrow{\iota} H^1_f(\mathbb{Q}_p, A_p^j)[p] \to 0. \tag{2}$$

So we have an inequality

$$\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Loc}_p)) \leqslant \dim_{\mathbb{F}_p}\left(\frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)}\right) + \dim_{\mathbb{F}_p}\left(H^1_f(\mathbb{Q}_p, A_p^j)[p]\right). \tag{3}$$

The dimension of $H^1_f(\mathbb{Q}_p, A_p^j)[p]$ can be computed by p-adic Hodge theory. We use the following fact in [8, Section 9.2.2].

Proposition 5.2. *Let V be a p-adic representation of $G_{\mathbb{Q}_p}$ and $\mathbf{D}_{\mathrm{dR}}(V) := (V \otimes \mathbf{B}_{\mathrm{dR}})^{G_{\mathbb{Q}_p}}, \mathbf{D}^+_{\mathrm{dR}}(V) := (V \otimes \mathbf{B}^+_{\mathrm{dR}})^{G_{\mathbb{Q}_p}}$, where $\mathbf{B}_{\mathrm{dR}}$ is the Fontaine's de Rham period ring. If V is a de Rham representation, then*

$$\dim_{\mathbb{Q}_p}(H^1_f(\mathbb{Q}_p, V)) = \dim_{\mathbb{Q}_p}(\mathbf{D}_{\mathrm{dR}}(V)/\mathbf{D}^+_{\mathrm{dR}}(V)) + \dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V). \tag{4}$$

The p-adic representation V_pE is crystalline with Hodge-Tate weight {0,1} because of the assumption that E has good reduction at p. Since the functor $\mathbf{D}_{\mathrm{dR}}$ is compatible with taking symmetric powers, we can compute that $\dim_{\mathbb{Q}_p}(\mathbf{D}_{\mathrm{dR}}(V_p^j)/\mathbf{D}^+_{\mathrm{dR}}(V_p^j)) = (j+1) - 1 = j$. By the equality (4) and the definition of $H^1_f(\mathbb{Q}_p, A_p^j)$, we have

$$\dim_{\mathbb{F}_p}\left(H^1_f(\mathbb{Q}_p, A_p^j)[p]\right) = j + \dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V). \tag{5}$$

From (3), (5), we have

$$\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Loc}_p)) \leqslant \dim_{\mathbb{F}_p}\left(\frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)}\right) + j + \dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V). \tag{6}$$

In the following, we compute the first term and the third term of the right-hand side of (6).

Proposition 5.3. *Suppose that E has good supersingular reduction at p. Then*

$$\dim_{\mathbb{F}_p}\left(\frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)}\right) = \dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V) = 0.$$

(Proof of Proposition 5.3)

Since the computations of $\dim_{\mathbb{F}_p} \frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)}$ and $\dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V_p^j)$ are very similar, we only describe precise computations for $\dim_{\mathbb{F}_p} \frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)}$.

If E has good supersingular reduction at p, for every positive integer n, $E[p^n]$ is isomorphic to the group of the p^n-torsion points of the Lubin-Tate formal group associated to a prime $-p$ over an unramified quadratic extension F of $\mathbb{Q}_p$ ([3, Proposition 8.6]). So $E[p^n]$ is a free $\mathcal{O}_F/p^n$-module of rank 1 and we take its basis z_n over $\mathcal{O}_F/p^n$, where $\mathcal{O}_F$ denotes the ring of integers of F. The Galois group $G_{\mathbb{Q}_p^{\mathrm{ur}}}$ acts on z_n via the character $\overline{\chi_{LT}} := \chi_{LT} \mod p^n$. Here $\chi_{LT} : G_{\mathbb{Q}_p^{\mathrm{ur}}} \twoheadrightarrow \mathcal{O}_F^\times$ is the Lubin-Tate character associated to the prime element $-p$ of F. We take $y_n := z_n^{\otimes j}$ as a basis of $\mathrm{Sym}^j E[p^n]$ over $\mathcal{O}_F/p^n$. For an element $x = ay_n$ ($a \in \mathcal{O}_F/p^n$) in $\mathrm{Sym}^j E[p^n]$, the condition that $x \in \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}}$ is equivalent to the condition that $a(\overline{\chi_{LT}}^j(g) - 1) = 0$ for all $g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}$. Since we assume $j < p-1$, there exists $g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}$ such that $\overline{\chi_{LT}}^j(g) - 1 \in (\mathcal{O}_F/p^n)^\times$ and we get $a = 0$. Hence we have $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} = \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}} = 0$ for all n and $H^0(\mathbb{Q}_p, A_p^j) = \mathrm{Sym}^j E[p^\infty]^{G_{\mathbb{Q}_p}} = 0$. □

Here we introduce some notations for the good ordinary reduction case. If E has good ordinary reduction at p, we have an exact sequence

$$0 \to T_p\widehat{E} \to T_pE \to T_p\widetilde{E}_p \to 0,$$

where $\widetilde{E}_p$ is the mod p reduction of the curve E and $\widehat{E}$ is the kernel of the reduction. We take a basis $\{v_1, v_2\}$ of T_pE as a $\mathbb{Z}_p$-module such that $T_p\widehat{E} = \mathbb{Z}_pv_1$ and we have the representation $\rho_E : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{Z}_p)$ with respect to this basis. For each positive integer n, $\{v_1 \mod p^n,\ v_2 \mod p^n\}$ form a basis of the free $\mathbb{Z}/p^n$-module $E[p^n]$ and this basis yields the representation $\rho_{E,p^n} : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{Z}/p^n)$. The action of $g \in G_{\mathbb{Q}_p}$ on T_pE can be written as the matrix

$$\begin{pmatrix} \chi_{\mathrm{cyc}}(g)\psi^{-1}(g) & u(g) \\ 0 & \psi(g) \end{pmatrix}. \tag{7}$$

Here χ_{cyc} denotes the p-adic cyclotomic character, ψ is the unramified character determined by the action of $G_{\mathbb{Q}_p}$ on $T_p\widetilde{E}_p$, and $u(g) \in \mathbb{Z}_p$. Also the action of $g \in G_{\mathbb{Q}_p}$

on $E[p^n]$ is written as

$$(8) \qquad \begin{pmatrix} \chi_{p^n}(g)\psi_n^{-1}(g) & u_n(g) \\ 0 & \psi_n(g) \end{pmatrix}.$$

Here χ_{p^n} denotes the mod p^n cyclotomic character, ψ_n is the mod p^n reduction of ψ, and $u_n(g) = u(g) \bmod p^n$.

Proposition 5.4. *Suppose that E has good ordinary reduction at p. Consider the following 4 cases.*

(*A*) $a_p^j \not\equiv 1 \mod p$.

(*B*) $a_p^j \equiv 1 \mod p$*, E has CM over an extension of $\mathbb{Q}_p$.*

(*C*) $a_p^j \equiv 1 \mod p$*, E does not have CM over an extension of $\mathbb{Q}_p$ and $\rho_{E,p}(G_{\mathbb{Q}_p})$ is not diagonalizable.*

(*D*) $a_p^j \equiv 1 \mod p$*, E does not have CM over an extension of $\mathbb{Q}_p$, $\rho_{E,p}(G_{\mathbb{Q}_p})$ is diagonalizable.*

Then, in each case, the dimensions $\dim_{\mathbb{F}_p} \frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)}$ *and* $\dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V_p^j)$ *are as in the table below.*

dimension *Case*	$\dim_{\mathbb{F}_p} \frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)}$	$\dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V_p^j)$
(*A*)	*0*	*0*
(*B*)	*1*	*0*
(*C*)	*0*	*0*
(*D*)	*1*	*0*

(Proof of Proposition 5.4)

Here we also describe precise computations only for $\dim_{\mathbb{F}_p} \frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)}$. First we assume that E has CM over some extension of $\mathbb{Q}_p$. For each positive integer n, we take $\overline{v_1} := v_1 \bmod p^n$, $\overline{v_2} := v_2 \bmod p^n$ as a basis of $E[p^n]$ over $\mathbb{Z}/p^n$, and we take a basis of $\mathrm{Sym}^j E[p^n]$ over $\mathbb{Z}/p^n$ as follows:

$$w_0 := \overline{v_1}^{\otimes j}, w_1 := \overline{v_1}^{\otimes j-1} \otimes \overline{v_2}, \ldots, w_i := \overline{v_1}^{\otimes j-i} \otimes \overline{v_2}^{\otimes i}, \ldots, w_j := \overline{v_2}^{\otimes j}.$$

Since E has CM, we may assume that $u(g)$ in (8) is 0 for all $g \in G_{\mathbb{Q}_p}$. Then we have

$$g(w_i) = g(\overline{v_1}^{\otimes j-i} \otimes \overline{v_2}^{\otimes i}) = (\chi_{p^n}(g)\overline{v_1})^{\otimes j-i} \otimes \overline{v_2}^{\otimes i} = \chi_{p^n}(g)^{j-i} w_i \quad (g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}).$$

For an element $x := a_0 w_0 + a_1 w_1 + \cdots + a_j w_j$ ($a_i \in \mathbb{Z}/p^n$) in $\mathrm{Sym}^j E[p^n]$, the condition $x \in \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}}$ is equivalent to the condition

$$a_0 \chi_{p^n}(g)^j = a_0,\ a_1 \chi_{p^n}(g)^{j-1} = a_1, \ldots, a_{j-1}\chi_{p^n}(g) = a_{j-1},\ a_j \in \mathbb{Z}/p^n \quad (\forall g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}).$$

Since $j \leqslant p-2$, for each i there exists $g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}$ such that $\chi_{p^n}(g)^{j-i}-1 \in (\mathbb{Z}/p^n)^{\times}$. Thus we have $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}} = \mathbb{Z}/p^n \cdot w_j$ to get $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} = (\mathbb{Z}/p^n \cdot w_j)^{\mathrm{Frob}_p=1}$. We know Frob_p acts on w_j via the character $\psi_n^j = \psi^j \mod p^n$ in (8). Since ψ is an infinite order character, there exists a non-negative integer s such that $\psi(\mathrm{Frob}_p)^j \equiv 1 \mod p^s$ and $\psi(\mathrm{Frob}_p)^j \not\equiv 1 \mod p^{s+1}$. Then

$$\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} = \begin{cases} \mathbb{Z}/p^n w_j & (n \leqslant s) \\ p^{n-s}\mathbb{Z}/p^n w_j & (n \geqslant s+1). \end{cases}$$

Especially if $s=0$, in other words if $a_p^j \equiv \psi(\mathrm{Frob}_p)^j \not\equiv 1 \mod p$, then we have $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} = 0$ for all n, and we get

$$(A_p^j)^{G_{\mathbb{Q}_p}} \cong \begin{cases} 0 & (a_p^j \not\equiv 1 \mod p) \\ \dfrac{1}{p^s}\mathbb{Z}/\mathbb{Z} & (1 \leqslant s < \infty). \end{cases}$$

Thus we get the desired result in the case (B) and partially in the case (A) when E has CM.

Next we consider the case where E does not have CM over an extension of $\mathbb{Q}_p$. In this case, there exists a non-negative integer m such that $\rho_{E,p^m}(G_{\mathbb{Q}_p})$ is diagonalizable and $\rho_{E,p^{m+1}}(G_{\mathbb{Q}_p})$ is not diagonalizable. For each n, we take the basis $w_0, w_1, \ldots, w_j$ for $\mathrm{Sym}^j E[p^n]$ over $\mathbb{Z}/p^n$ as in the previous argument.

For any $n \leqslant m$, we may assume $u_n(g)=0$ in (8) for all $g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}$. So we can imitate the argument in the case where E has CM, and get $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} = (\mathbb{Z}/p^n \cdot w_j)^{\mathrm{Frob}_p=1}$.

For $n \geqslant m+1$, we have $u_n(G_{\mathbb{Q}_p}) \neq 0$ and $u_n(G_{\mathbb{Q}_p}) \subset p^m\mathbb{Z}/p^n\mathbb{Z}$. We first consider $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ab}}}}$. With respect to the basis $\{\overline{v_1}, \overline{v_2}\}$, the group $G_{\mathbb{Q}_p^{\mathrm{ab}}}$ acts on $E[p^n]$ via

$$\begin{pmatrix} 1 & u_n(g) \\ 0 & 1 \end{pmatrix}.$$

For an element $x := a_0w_0 + a_1w_1 + \cdots + a_jw_j$ ($a_i \in \mathbb{Z}/p^n$) in $\mathrm{Sym}^j E[p^n]$, we can show that the condition $x \in \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ab}}}}$ is equivalent to the condition

$$\text{(9)} \qquad a_0 \in \mathbb{Z}/p^n\mathbb{Z},\ a_1u_n(g) = a_2u_n(g) = \ldots = a_ju_n(g) = 0 \ \ (\forall g \in G_{\mathbb{Q}_p^{\mathrm{ab}}})$$

by exactly the same computation to the one in the proof of Lemma 4.2 if we think u_n as $\tau_{q,n}$. We have $u_n(G_{\mathbb{Q}_p^{\mathrm{ur}}}) = p^m\mathbb{Z}/p^n\mathbb{Z}$ by the definition of the integer m and [5, Lemma 3.5]. Here we study the image of $G_{\mathbb{Q}_p^{\mathrm{ab}}}$ under the map u_n.

Lemma 5.5. *For $n \geqslant m+1$, $u_n(G_{\mathbb{Q}_p^{\mathrm{ab}}}) = p^m\mathbb{Z}/p^n\mathbb{Z}$.*

(Proof of Lemma 5.5)

When $n = m+1$, $u_{m+1}(G_{\mathbb{Q}_p^{\mathrm{ab}}}) = p^m\mathbb{Z}/p^{m+1}\mathbb{Z}$ or 0 since $u_{m+1}(G_{\mathbb{Q}_p^{\mathrm{ab}}})$ forms an additive group. If $u_{m+1}(G_{\mathbb{Q}_p^{\mathrm{ab}}}) = 0$, then $\rho_{E,m+1}(G_{\mathbb{Q}_p^{\mathrm{ur}}})$ is abelian but we can show that this can not be happen using [5, Lemma 3.5] and the definition of the integer m. Thus we have $u_{m+1}(G_{\mathbb{Q}_p^{\mathrm{ab}}}) = p^m\mathbb{Z}/p^{m+1}\mathbb{Z}$. For $n \geqslant m+1$, taking compatible bases of $E[p^n]$ for all n as in [5, Lemma 3.5], we have $u_n(g) \equiv u_{m+1}(g) \pmod{p^{m+1}}$ for $g \in G_{\mathbb{Q}_p^{\mathrm{ab}}}$ and obtain $u_n(G_{\mathbb{Q}_p^{\mathrm{ab}}}) = p^m\mathbb{Z}/p^n\mathbb{Z}(= u_n(G_{\mathbb{Q}_p^{\mathrm{ur}}}))$. □

Hence if $x \in \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ab}}}}$, we have $a_1, a_2, \dots, a_j \in p^{n-m}\mathbb{Z}/p^n\mathbb{Z}$ from (9) and

$$a_1u_n(g) = a_2u_n(g) = \ldots = a_ju_n(g) = 0 \text{ in } \mathbb{Z}/p^n\mathbb{Z} \tag{10}$$

still for $g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}$ since $u_n(G_{\mathbb{Q}_p^{\mathrm{ur}}}) = p^m\mathbb{Z}/p^n\mathbb{Z}$.

We next consider a condition on $a_0, a_1, \dots, a_j$ such that $x = a_0w_0 + \cdots + a_jw_j \in \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}}$. For $g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}$ and i with $1 \leqslant i \leqslant j$,

$$\begin{aligned} g(a_iw_i) = a_ig(\overline{v_1}^{\otimes j-i} \otimes \overline{v_2}^{\otimes i}) &= a_i(\chi_{p^n}(g)\overline{v_1})^{\otimes j-i} \otimes (u_n(g)\overline{v_1} + \overline{v_2})^{\otimes i} \\ &= a_i\chi_{p^n}^{j-i}(g)\overline{v_1}^{\otimes j-i} \otimes \left(\sum_{k=0}^{i} \binom{i}{k} u_n(g)^{i-k}\overline{v_1}^{\otimes i-k} \otimes \overline{v_2}^{\otimes k}\right) \\ &= a_i\chi_{p^n}^{j-i}(g)\overline{v_1}^{\otimes j-i} \otimes \overline{v_2}^{\otimes i} = a_i\chi_{p^n}^{j-i}(g)w_i. \end{aligned}$$

Here we use (10) in the fourth equality for i with $1 \leqslant i \leqslant j$ since $x \in \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}} \subset \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ab}}}}$. For $i = 0$, we also have $g(a_0w_0) = a_0\chi_{p^n}^j(g)w_0$ for $g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}$. So the condition $x \in \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}}$ is equivalent to the condition

$$a_0\chi_{p^n}(g)^j = a_0, \dots, a_{j-1}\chi_{p^n}(g) = a_{j-1},\ a_j \in p^{n-m}\mathbb{Z}/p^n\mathbb{Z} \tag{11}$$

for all $g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}$. Again we can take $g \in G_{\mathbb{Q}_p^{\mathrm{ur}}}$ such that $\chi_{p^n}(g)^{j-i} - 1 \in (\mathbb{Z}/p^n)^\times$ for each i to get $a_0 = a_1 = \ldots = a_{j-1} = 0$. Thus we get $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} = (p^{n-m}\mathbb{Z}/p^n \cdot w_j)^{\mathrm{Frob}_p=1}$ for $n \geqslant m+1$.

If $\rho_{E,p}(G_{\mathbb{Q}_p})$ is not diagonalizable, in other words if $m = 0$, $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} = \mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}} = 0$ for all n from the above computations and $(A_p^j)^{G_{\mathbb{Q}_p}} = 0$. Thus we get the desired result in the case (C) and partially in the case (A).

If $m \geqslant 1$, from the above argument, we have

$$\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} = \begin{cases} (\mathbb{Z}/p^nw_j)^{\mathrm{Frob}_p=1} & (n \leqslant m) \\ (p^{n-m}\mathbb{Z}/p^n\mathbb{Z} \cdot w_j)^{\mathrm{Frob}_p=1} & (n \geqslant m+1). \end{cases}$$

We know that Frob_p acts on $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}}$ via the character $\psi_n^j = \psi^j \mod p^n$ for all n. We again take a non-negative integer s such that $\psi(\mathrm{Frob}_p)^j \equiv 1 \mod p^s$ and $\psi(\mathrm{Frob}_p)^j \not\equiv 1 \mod p^{s+1}$. If $s = 0$, in other words if $a_p^j \not\equiv 1 \mod p$, then we have $\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} = 0$ for all n. If $s > 0$ we have

$$\mathrm{Sym}^j E[p^n]^{G_{\mathbb{Q}_p}} \cong \begin{cases} \mathbb{Z}/p^nw_j & (n \leqslant \min\{m, s\}) \\ p^{n-\min\{m,s\}}\mathbb{Z}/p^nw_j & (n > \min\{m, s\}). \end{cases}$$

Thus we get

$$(A_p^j)^{G_{\mathbb{Q}_p}} \cong \begin{cases} 0 & (a_p^j \not\equiv 1 \mod p) \\ \dfrac{1}{p^{\min\{m,s\}}}\mathbb{Z}/\mathbb{Z} & (1 \leqslant s < \infty). \end{cases}$$

So finally, we have the desired result in the case (D) and the case (A) completely.

□

6. Non-injectivity of the restriction map $\mathrm{Res}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p}$

From (6) and Proposition 5.4, we deduce Proposition 5.1 in the case (A) and (C), and the main theorem follows. Since we assume (b') in Theorem 1.1, (D) in the table in Proposition 5.4 does not occur. For the case (B), we prove the following proposition.

Proposition 6.1. *In the case* (B)*, the restriction map*

$$\mathrm{Res}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p} : \iota^{-1}(H_f^1(\mathbb{Q}_p, A_p^j)[p]) \to H^1(\mathbb{Q}_p^{\mathrm{ur}}, \mathrm{Sym}^j E[p])$$

is not injective.

From this proposition, also in the case (B), we can deduce Proposition 5.1 and the main theorem follows. Thus the main theorem follows in all possible cases $(A), (B)$ and (C) under the assumptions in Theorem 1.1.

(Proof of Proposition 6.1)
We have the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)} \arrow[r] \arrow[d] & \iota^{-1}(H_f^1(\mathbb{Q}_p, A_p^j)[p]) \arrow[d, "\mathrm{Res}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p}"] \\
0 \arrow[r] & \dfrac{H^0(\mathbb{Q}_p^{\mathrm{ur}}, A_p^j)}{pH^0(\mathbb{Q}_p^{\mathrm{ur}}, A_p^j)} \arrow[r] & H^1(\mathbb{Q}_p^{\mathrm{ur}}, \mathrm{Sym}^j E[p]).
\end{tikzcd}$$

From the table in Proposition 5.4, we have $\dim_{\mathbb{F}_p}\left(\frac{H^0(\mathbb{Q}_p, A_p^j)}{pH^0(\mathbb{Q}_p, A_p^j)}\right) = 1$ in the case (B). Since we have already computed $\mathrm{Sym}^j E[p^\infty]^{G_{\mathbb{Q}_p^{\mathrm{ur}}}}$ in the case in the proof of Proposition 5.4, we also get $\dim_{\mathbb{F}_p}\left(\frac{H^0(\mathbb{Q}_p^{\mathrm{ur}}, A_p^j)}{pH^0(\mathbb{Q}_p^{\mathrm{ur}}, A_p^j)}\right) = 0$. So by the above commutative diagram, the dimension of the kernel of $\mathrm{Res}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p}$ is at least 1. Thus the proposition follows.

□

acknowledgement. The author would like to thank his supervisor Professor Masato Kurihara heartily for guiding him to the topics in this paper, careful reading of the draft of this paper and helpful discussions with him. He also would like to express his sincere gratitude to Professor Dipendra Prasad and Professor Sudhanshu Shekhar for many valuable comments on his work. Thanks are also due to Ryotaro Sakamoto for answering his questions precisely concerning Proposition 2. Lastly, he is also grateful to the referees for their careful reading of his draft. This research was supported by JSPS KAKENHI Grant Number 21J13502.

References

[1] S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives, The Grothendieck Festschrift Volume I, 333 – 400, Progress in Mathematics, 86, Birkhuser, Boston, (1990).

[2] N. Freitas, A. Kraus, On the symplectic type of isomorphisms of the p-torsion of elliptic curves, preprint. arXiv:1607.01218. to appear in Memoirs of AMS.

[3] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. Math., 152 1-36 (2003).

[4] T. Lawson, C. Wuthrich, Vanishing of some Galois cohomology groups for elliptic curves , in Elliptic Curves, Modular Forms and Iwasawa Theory edited by David Loeffler and Sarah Livia Zerbes, Springer Proceedings in Mathematics and Statistics, Volume 188, Springer, (2017), 373 - 399.

[5] A. Lozano-Robledo, Division fields of elliptic curves with minimal ramification, Revista Matematica Iberoamericana, vol. 31, no. 4, (2015).

[6] J. Nekovář, Class numbers of quadratic fields and Shimura's correspondence. Math. Ann., 287(4):577-594, (1990).

[7] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Springer-Verlag, (2008).

[8] T. Nguyen Quang Do, On the Determinantal Approach to the Tamagawa Number Conjecture. In J. Coates, A. Raghuram, A. Saikia, R. Sujatha (Eds.), The Bloch-Kato Conjecture for the Riemann Zeta Function (London Mathematical Society Lecture Note Series, pp. 154-192). Cambridge: Cambridge University Press.

[9] D. Prasad, A mod p Artin-Tate conjecture and generalizing the Herbrand-Ribet theorem; Pacific Journal of Mathematics, vol. 303, no. 1, 299-316 (2019).

[10] D. Prasad, S. Shekhar, Relating Tate-Shafarevich group of an elliptic curve with class group, preprint. arXiv:1912. 12928v1.

[11] K. Rubin, Euler systems, Hermann Weyl Lectures, Ann. of Math. Studies, vol. 147, Princeton Univ. Press, (2000).

[12] J. P. Serre, Abelian l-adic Representations and Elliptic Curves. W. A. Benjamin, Inc., (1968).

[13] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts inMathematics, 106. Springer-Verlag, New York, (1986).

[14] L. C. Washington, Class numbers of the simplest cubic fields, Math.Comp.48, No.177(1987).

Department of Mathematics, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa 223-8522 Japan

Email address: `vicarious@keio.jp`