ON IDEAL CLASS GROUPS OF NUMBER FIELDS AND SELMER GROUPS OF MODULAR GALOIS REPRESENTATIONS

NAOTO DAINOBU

Abstract. Let p be an odd prime number and $M_{f,D}$ a quadratic twist by a square-free integer D of an $\mathbb{F}_p$-valued representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to a modular form f. Putting $K_{f,D}$ as a number field cut out by $M_{f,D}$, we study the ideal class group $\mathrm{Cl}_{K_{f,D}}$ of $K_{f,D}$. We give a condition that $\mathrm{Cl}_{K_{f,D}} \otimes \mathbb{F}_p$ has $M_{f,D}$ as its quotient $\mathrm{Gal}(K_{f,D}/\mathbb{Q})$-module in terms of Bloch-Kato's Selmer group of $M_{f,D}$. This is a generalization of the result of Prasad and Shekhar on elliptic curves for modular forms of higher weight.

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. Various relations between them have been studied by many people. For example in [23], 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 [14], 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 $\mathbb{Q}$. Recently, *non-abelian* number fields over $\mathbb{Q}$ have been also studied well. Let E be an elliptic curve over $\mathbb{Q}$ and p an odd prime number. Hiranouchi [10] studied the class number of the p^n-th division field $\mathbb{Q}(E[p^n])$ in terms of the Morell-Weil group $E(\mathbb{Q})$, where the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is *non-abelian* in general. Ohshita [17] further generalize Hiranouchi's result for a number field F cut out by a general p-adic Galois representation. He studied the class number of F using the Selmer group of the p-adic representation.

On the other hand, Prasad and Shekhar [19] studied the *structure* of the ideal class group of the p-th division field $\mathbb{Q}(E[p])$ as a $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-module rather than the class number. Here we briefly introduce their result.

Theorem (Prasad-Shekhar). *Let $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ be a $\mathbb{F}_p$-valued Galois representation associated to $E[p]$ where $G_{\mathbb{Q}}$ denotes the absolute Galois group of $\mathbb{Q}$. Suppose that the following conditions on E hold:*

(1) *E has good reduction at p.*
(2) *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.*
(3) *For every finite prime $\ell \neq p$, the Tamagawa number $c_\ell(E/\mathbb{Q}_\ell)$ of $E/\mathbb{Q}_\ell$ is a p-adic unit.*
(4) *The $\mathbb{F}_p$-representation $\bar{\rho}_{E,p}$ of $G_{\mathbb{Q}}$ is irreducible.*

Then $\dim_{\mathbb{F}_p}(\mathrm{Sel}(\mathbb{Q}, E[p])) \geqslant 2$ implies that the $\mathbb{F}_p$-representation $\mathrm{Cl}_{\mathbb{Q}(E[p])} \otimes \mathbb{F}_p$ of $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ has $E[p]$ as its quotient representation.

In this article, we study a higher weight analogue of the above theorem of Prasad and Shekhar. In other words, we consider $\mathbb{F}_p$-valued representations attached to modular forms rather than those associated to elliptic curves. Here we describe the details. Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$ be a normalized Hecke eigen newform of even weight $k \geqslant 2$ and level $\Gamma_0(N)$ where $q := e^{2\pi\sqrt{-1}z}$ and the parameter z is in the complex upper half plane. We fix p again as an odd prime number and assume p splits completely in the Hecke field of f. Then there is an associated p-adic representation $\rho_f^0 : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Q}_p}(V_f^0) \cong \mathrm{GL}_2(\mathbb{Q}_p)$ where V_f^0 denotes its representation space. Note that we take V_f^0 as the one with the Hodge-Tate weight $\{0, k-1\}$. Fixing a Galois stable $\mathbb{Z}_p$-lattice T_f^0 of V_f^0, we put $A_f^0 := V_f^0/T_f^0$, $M_f^0 := T_f^0/pT_f^0$ and $\bar{\rho}_f^0 : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_p}(M_p^0) \cong \mathrm{GL}_2(\mathbb{F}_p)$ as a group homomorphism corresponding to M_f^0. We take twists of these representations to make them self-dual. Let χ_{cyc} (resp. ω_{cyc}) denotes the p-adic (resp. mod p) cyclotomic character. We define $\rho_f := \rho_f^0 \otimes \chi_{\mathrm{cyc}}^{1-\frac{k}{2}}$, $\bar{\rho}_f := \bar{\rho}_f^0 \otimes \omega_{\mathrm{cyc}}^{1-\frac{k}{2}}$. Next we consider various quadratic twists of ρ_f and $\bar{\rho}_f$. Taking a quadratic discriminant D and corresponding quadratic character χ_D of $G_{\mathbb{Q}}$, we put $\rho_{f,D} := \rho_f \otimes \chi_D$, $\bar{\rho}_{f,D} := \bar{\rho}_f \otimes \chi_D$ and write $V_{f,D}, M_{f,D}$ as their representation spaces. We take $T_{f,D}$ as the Galois stable $\mathbb{Z}_p$-lattice of $V_{f,D}$ which is the same as T_f^0 as a $\mathbb{Z}_p$-module and put $A_{f,D} := V_{f,D}/T_{f,D}$. Let $K_{f,D}$ be the Galois extension of $\mathbb{Q}$ cut out by $\bar{\rho}_{f,D}$. Note that we consider the representation $\bar{\rho}_{f,D}$ and the number field $K_{f,D}$ as analogues of $\bar{\rho}_{E,p}$ and $\mathbb{Q}(E[p])$ in the theorem of Prasad and Shekhar respectively. The main theorem of this article is the following.

Theorem 1.1. *Under the above setting, we further assume the following conditions are satisfied.*

(1) *$p \nmid N$.*
(2) *If f is supersingular at p, then $k \leqslant p+1$.*
If f is ordinary at p, then $p-1 \nmid k-1$ and the conditions in Proposition 5.11 do not occur.
(3) $\mathrm{Im}(\bar{\rho}_f^0) \supset \mathrm{SL}_2(\mathbb{F}_p)$
(4) *$c(\mathbb{Q}_\ell, A_{f,D}) = 1$ for all prime $\ell \mid N$.*

Then $\dim_{\mathbb{F}_p}\left(H^1_f(\mathbb{Q}, M_{f,D})\right) \geqslant 2$ *implies that the* $\mathbb{F}_p$*-representation* $\mathrm{Cl}_{K_{f,D}} \otimes \mathbb{F}_p$ *of* $\mathrm{Gal}(K_{f,D}/\mathbb{Q})$ *has* $M_{f,D}$ *as its quotient representation. Here* $c(\mathbb{Q}_\ell, A_{f,D})$ *denotes the Tamagawa factor of* $A_{f,D}$ *at* ℓ *and* $H^1_f(\mathbb{Q}, M_{f,D})$ *is Bloch-Kato's Selmer group of* $M_{f,D}$*.*

Remark 1.2. *Due to Bloch and Kato's conjecture, the order of* $Ш^{BK}_p(\mathbb{Q}, A_{f,D})$ *is related to the central value* $L(k/2, \chi_D, f)$ *of twisted L function of* f *if it does not vanish. Here* $Ш^{BK}_p(\mathbb{Q}, A_{f,D})$ *denotes the* p*-part of Bloch-Kato's Tate-Shafarevich group of* $A_{f,D}$*. Especially, if* p *divides the algebraic part* $L^{alg}(k/2, \chi_D, f)$ *of* $L(k/2, \chi_D, f)$*, then we have* $Ш^{BK}_p(\mathbb{Q}, A_{f,D}) \neq 0$ *assuming the conjecture. On the other hand, we know that if* $Ш^{BK}_p(\mathbb{Q}, A_{f,D}) \neq 0$*, then we have* $\dim_{\mathbb{F}_p}\left(H^1_f(\mathbb{Q}, M_{f,D})\right) \geqslant 2$ *because of the existence of the generalized Cassels-Tate pairing for* $A_{f,D}$*. Hence, under Bloch and Kato's conjecture, if* p *divides* $L^{alg}(k/2, \chi_D, f)$*, we can see that the class group* $\mathrm{Cl}_{K_{f,D}}$ *has the representation* $M_{f,D}$ *as its quotient from our main result. Thus we conjectually obtain an Herbrand-Ribet type phenomenon for a representation associated to a modular form.*

At the end of this section, we write the outline of this paper. In section 2, we recall the definition of Bloch-Kato's Selmer groups and Tate-Shafarevich groups for p-adic representations and write a sketch of the proof of Theorem 1.1 dividing it into 3 steps. In section 3, we prove the first step of the proof. In section 4, the basic notions of Tamagawa factor are explained and the second step is proved. In section 5, we prove the third step and complete the proof. Finally in section 6, we introduce two numerical examples of Theorem 1.1.

Acknowlegement. The author would like to thank his supervisor Professor Masato Kurihara heartily for his continued support, guiding the author to the topic in this paper and helpful discussions. He also would like to express his sincere gratitude to Professors Dipendra Prasad and Sudhanshu Shekhar for valuable comments on his previous paper [3]. Thanks are also due to Dr. Ryotaro Sakamoto who teaches him the basic properties of Tamagawa factors which are used in Section 4. He is also grateful to Professor Neil Dummigan for introducing his paper [4] kindly to the author, which was really helpful to make some numerical examples in Section 6.

2. A sketch of the proof

In this section, we describe a sketch of the proof of Theorem 1.1. We mainly follow the strategy used in [3] in which we gave a condition that $\mathrm{Cl}_{\mathbb{Q}(E[p])} \otimes \mathbb{F}_p$ has other irreducible $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-representation than $E[p]$ as its quotient representation in the same setting as [19]. In [19], they used the classical p-Selmer group $\mathrm{Sel}_p(E/\mathbb{Q})$ for an elliptic curve but, to treat representations coming from modular forms, we have to deal with Bloch-Kato's Selmer group H^1_f which we first recall.

2.1. **Bloch-Kato's Selmer groups and Tate-Shafarevich groups.** For a field F, G_F denotes its absolute Galois group $\mathrm{Gal}(\overline{F}/F)$. For every prime number ℓ and the p-adic representation $V_{f,D}$ which we define in Section 1, we fix a local condition $H^1_f(\mathbb{Q}_\ell, V_{f,D})$ in $H^1(\mathbb{Q}_\ell, V_{f,D})$ as

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

Here $\mathbb{Q}_\ell^{\mathrm{ur}}$ is the maximal unramified extension of $\mathbb{Q}_\ell$ and $\mathbf{B}_{\mathrm{crys}}$ denotes Fontaine's crystalline period ring which is defined in [1, Section 1]. We also define $H^1_f(\mathbb{Q}_\ell, A_{f,D}) := \pi\left(H^1_f(\mathbb{Q}_\ell, V_{f,D})\right)$ for every ℓ, where $\pi : H^1(\mathbb{Q}_\ell, V_{f,D}) \to H^1(\mathbb{Q}_\ell, A_{f,D})$ is a homomorphism induced by a natural map $\pi : V_{f,D} \to A_{f,D}$.

Definition 2.1. *For $V_{f,D}$ and $A_{f,D}$, we define Bloch-Kato's Selmer groups as*

$$H^1_f(\mathbb{Q}, V_{f,D}) := \mathrm{Ker}\left(H^1(\mathbb{Q}, V_{f,D}) \xrightarrow{\prod \mathrm{Loc}_\ell} \prod_\ell \frac{H^1(\mathbb{Q}_\ell, V_{f,D})}{H^1_f(\mathbb{Q}_\ell, V_{f,D})}\right),$$

$$H^1_f(\mathbb{Q}, A_{f,D}) := \mathrm{Ker}\left(H^1(\mathbb{Q}, A_{f,D}) \xrightarrow{\prod \mathrm{Loc}_\ell} \prod_\ell \frac{H^1(\mathbb{Q}_\ell, A_{f,D})}{H^1_f(\mathbb{Q}_\ell, A_{f,D})}\right),$$

where for every prime number ℓ, 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 for $A_{f,D}$ which we write as $Ш^{BK}_p(\mathbb{Q}, A_{f,D})$ is defined in [1, Section 5] as follows.

Definition 2.2. *We define the p-part of Bloch-Kato's Tate-Shafarevich group for $A_{f,D}$ as*

$$Ш^{BK}_p(\mathbb{Q}, A_{f,D}) := \frac{H^1_f(\mathbb{Q}, A_{f,D})}{\pi(H^1_f(\mathbb{Q}, V_{f,D}))},$$

where $\pi : H^1(\mathbb{Q}, V_{f,D}) \to H^1(\mathbb{Q}, A_{f,D})$ is a homomorphism induced by a natural map $\pi : V_{f,D} \to A_{f,D}$. In other words, $Ш^{BK}_p(\mathbb{Q}, A_{f,D})$ is defined by an exact sequence

$$0 \to \pi(H^1_f(\mathbb{Q}, V_{f,D})) \to H^1_f(\mathbb{Q}, A_{f,D}) \to Ш^{BK}_p(\mathbb{Q}, A_{f,D}) \to 0.$$

We note that $\pi(H^1_f(\mathbb{Q}, V_{f,D}))$ is the maximal divisible subgroup of $H^1_f(\mathbb{Q}, A_{f,D})$, so their quotient $Ш^{BK}_p(\mathbb{Q}, A_{f,D})$ is always finite which is a well-known conjecture for classical Tate-Shafarevich groups for elliptic curves.

We also define Bloch-Kato's Selmer group for the finite module $M_{f,D}$. We have an exact sequence of $G_\mathbb{Q}$-modules

$$0 \to M_{f,D} \xrightarrow{\iota} A_{f,D} \xrightarrow{\times p} A_{f,D} \to 0$$

from which we obtain an exact sequence

$$0 \to (A_{f,D})^{G_{\mathbb{Q}}} \otimes \mathbb{F}_p \to H^1(\mathbb{Q}, M_{f,D}) \xrightarrow{\iota} H^1(\mathbb{Q}, A_{f,D})[p] \to 0, \tag{1}$$

where the map ι in the first exact sequence denotes the inclusion and the second denotes the one which induced by the first one.

Definition 2.3. *We define Bloch-Kato's Selmer group for $M_{f,D}$ as*

$$H^1_f(\mathbb{Q}, M_{f,D}) := \iota^{-1}(H^1_f(\mathbb{Q}, A_{f,D})[p]).$$

The Selmer group $H^1_f(\mathbb{Q}, M_{f,D})$ can be also defined by using local conditions. In fact, we define local conditions for $M_{f,D}$ at ℓ as $H^1_f(\mathbb{Q}_\ell, M_{f,D}) := \iota^{-1}(H^1_f(\mathbb{Q}_\ell, A_{f,D}))$. Then we have

$$H^1_f(\mathbb{Q}, M_{f,D}) = \mathrm{Ker}\left(H^1(\mathbb{Q}, M_{f,D}) \xrightarrow{\prod \mathrm{Loc}_\ell} \prod_\ell \frac{H^1(\mathbb{Q}_\ell, M_{f,D})}{H^1_f(\mathbb{Q}_\ell, M_{f,D})} \right)$$

as in Definition 2.1.

2.2. **A sketch of the proof of Theorem 1.1.** Now we describe a sketch of the proof of Theorem 1.1. In the following, we fix a modular form f and a quadratic discriminant D and omit the suffixes of $V_{f,D}, T_{f,D}, A_{f,D}, M_{f,D}, K_{f,D}$ as V, T, A, M, K when no confusion occurs.

(Step1) *We show that a restriction map*

$$\mathrm{Res}_{K/\mathbb{Q}} : H^1(\mathbb{Q}, M) \to H^1(K, M)^{\mathrm{Gal}(K/\mathbb{Q})}$$

is injective under the assumption (3) *in Theorem 1.1.*

Let F be a number field or a local field and N a G_F-module. We define the unramified cohomology group $H^1_{\mathrm{ur}}(F, N)$ as a subgroup of cohomology classes in $H^1(F, N)$ which are trivial on the inertia subgroup at every place of F. Assuming the claim in (Step1), the restriction map $\mathrm{Res}_{K/\mathbb{Q}}$ induces an injective homomorphism between unramified cohomology groups

$$\mathrm{Res}_{K/\mathbb{Q}} : H^1_{\mathrm{ur}}(\mathbb{Q}, M) \hookrightarrow H^1_{\mathrm{ur}}(K, M)^{\mathrm{Gal}(K/\mathbb{Q})}.$$

Using class field theory, we have $H^1_{\mathrm{ur}}(K, M)^{\mathrm{Gal}(K/\mathbb{Q})} = \mathrm{Hom}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathrm{Cl}_K \otimes \mathbb{F}_p, M)$. Every nontrivial homomorphism in $\mathrm{Hom}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathrm{Cl}_K \otimes \mathbb{F}_p, M)$ is surjective since we assume the condition (3) in Theorem 1.1 which implies that M^0_f and so $M = M_{f,D}$ are irreducible. Hence every non-trivial homomorphism in $\mathrm{Hom}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathrm{Cl}_K \otimes \mathbb{F}_p, M)$ realizes M as a quotient $\mathrm{Gal}(K/\mathbb{Q})$-module of $\mathrm{Cl}_K \otimes \mathbb{F}_p$. From this observation and the above injection between unramified cohomology groups, we obtain an implication,

$$H^1_{\mathrm{ur}}(\mathbb{Q}, M) \neq 0 \Rightarrow \mathrm{Cl}_K \otimes \mathbb{F}_p \text{ has } M \text{ as its quotient } \mathrm{Gal}(K/\mathbb{Q})\text{-module}.$$

We will show the existence of non-trivial elements in $H^1_{\mathrm{ur}}(\mathbb{Q}, M)$ using Bloch-Kato's Selmer group of M in the succeeding steps.

(Step2) *Under the assumption* (4) *in Theorem 1.1, we show that the image of* $H^1_f(\mathbb{Q}, M)$ *in* $H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, M)$ *is zero for any* $\ell \neq p$. *In other words, we show that elements in* $H^1_f(\mathbb{Q}, M)$ *are unramified outside* p.

Here $H^1_f(\mathbb{Q}, M)$ is the Selmer group of M defined in Definition 2.3. Assuming the claim in (Step2), for a restriction map

$$\mathrm{Res}_p^{\mathrm{ur}} : H^1_f(\mathbb{Q}, M) \to H^1(\mathbb{Q}_p^{\mathrm{ur}}, M),$$

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

(Step3) *We study the image of* $\mathrm{Res}_p^{\mathrm{ur}}$ *and show that* $\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Res}_p^{\mathrm{ur}})) \leqslant 1$.

This completes the proof since we assume $\dim_{\mathbb{F}_p}(H^1_f(\mathbb{Q}, M)) \geqslant 2$.

3. Injectivity of the restriction map

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

Proposition 3.1. *Suppose that* $\mathrm{Im}(\bar{\rho}_f^0)$ *contains* $\mathrm{SL}_2(\mathbb{F}_p)$ *(the assumption* (3) *in Theorem 1.1). Then the restriction map*

$$\mathrm{Res}_{K/\mathbb{Q}} : H^1(\mathbb{Q}, M) \to H^1(K, M)^{\mathrm{Gal}(K/\mathbb{Q})}$$

is injective.

(Proof of Proposition 3.1)
It suffices to show that $H^1(\mathrm{Gal}(K/\mathbb{Q}), M) = 0$. We use the following lemma.

Lemma 3.2. *Let* G *be a finite group and* N *a finite dimensional representation of* G *over* $\mathbb{F}_p$. *If there is a normal subgroup* H *of* G *such that*

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

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

For a proof of this lemma, see [3, Lemma 3.2]. We divide a proof of Proposition 3.1 into two cases.
(Case 1: $p \geqslant 5$)
Let $L := \mathbb{Q}(\zeta_p, \sqrt{D})$ where ζ_p is a primitive p-th root of unity. First we show that the image of $\bar{\rho}_f^0 : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ still contains $\mathrm{SL}_2(\mathbb{F}_p)$ when restricted to G_L. Let F and F_L be the fields corresponding to the kernel of $\bar{\rho}_f^0$ and $\bar{\rho}_f^0|_{G_L}$ in Galois theory respectively. So we have $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{Im}(\bar{\rho}_f^0) \supset \mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{Gal}(F_L/L) \cong$

$\mathrm{Gal}(F/F\cap L)\cong \mathrm{Im}(\bar{\rho}_f^0|_{G_L})$. Let F' be the intermediate field of the Galois extension $F/\mathbb{Q}$ corresponding to $\mathrm{SL}_2(\mathbb{F}_p)$. Then $F'\cdot(F\cap L)/F'$ is an abelian extension as the extension $F\cap L/\mathbb{Q}$ is. Since we assume $p\geqslant 5$, $\mathrm{SL}_2(\mathbb{F}_p)$ is a perfect group. In other words, $\mathrm{SL}_2(\mathbb{F}_p)$ has no non-trivial abelian quotients. So we have $F'\cdot(F\cap L)=F'$ and hence $\mathrm{Gal}(F/F\cap L)\cap\mathrm{SL}_2(\mathbb{F}_p)=\mathrm{SL}_2(\mathbb{F}_p)$ from Galois theory. Thus $\mathrm{Im}(\bar{\rho}_f^0|_{G_L})\cong\mathrm{Gal}(F/F\cap L)\supset\mathrm{SL}_2(\mathbb{F}_p)$. Since $\bar{\rho}_{f,D}|_{G_L}=\bar{\rho}_f^0|_{G_L}$, the image of $\bar{\rho}_{f,D}$ also contains $\mathrm{SL}_2(\mathbb{F}_p)$ which implies that $-I\in\mathrm{Im}(\bar{\rho}_{f,D})\cong\mathrm{Gal}(K/\mathbb{Q})$, where I denotes the unit matrix in $\mathrm{SL}_2(\mathbb{F}_p)$. Let $H\subset\mathrm{Gal}(K/\mathbb{Q})$ be the order 2 subgroup generated by $-I$. Then H satisfies the conditions (1), (2) in Lemma 3.2 and we have $H^i(\mathrm{Gal}(K/\mathbb{Q}),M)=0$ for all $i\geqslant 0$.

(Case 2: $p=3$)

In this case, we know $\#\mathrm{SL}_2(\mathbb{F}_3)=8$ and the elements in $\mathrm{SL}_2(\mathbb{F}_3)$ are the following:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&-1\end{pmatrix},\begin{pmatrix}-1&1\\1&1\end{pmatrix},\begin{pmatrix}0&-1\\1&0\end{pmatrix},$$

$$\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&-1\\-1&1\end{pmatrix},\begin{pmatrix}1&-1\\-1&-1\end{pmatrix},\begin{pmatrix}0&1\\-1&0\end{pmatrix}$$

We put

$$A_1=\begin{pmatrix}1&1\\1&-1\end{pmatrix},A_2=\begin{pmatrix}-1&-1\\-1&1\end{pmatrix}.$$

Since we assume that $\mathrm{Im}(\bar{\rho}_f^0)\supset\mathrm{SL}_2(\mathbb{F}_3)$, we can take $\sigma\in G_{\mathbb{Q}}$ such that $\bar{\rho}_f^0(\sigma)=A_1$. Since both mod 3 cyclotomic character ω_{cyc} and χ_D are order 2, we have $\bar{\rho}_{f,D}(\sigma)=A_1$ or A_2. We can show that there are no non-trivial elements in M which fixed by A_1 or A_2 by direct computation. So if $A_1=\bar{\rho}_{f,D}(\sigma)\in\mathrm{Gal}(K/\mathbb{Q})$ (resp. $A_2\in\mathrm{Gal}(K/\mathbb{Q})$), then the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ generated by A_1 (resp. A_2) satisfies the conditions (1), (2) in Lemma 3.2 since every subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ is normal and 2-group. Thus we have $H^i(\mathrm{Gal}(K/\mathbb{Q}),M)=0$ for all $i\geqslant 0$ from Lemma 3.2. □

Thus the restriction map $\mathrm{Res}_{K/\mathbb{Q}}: H^1(\mathbb{Q},M)\to H^1(K,M)^{\mathrm{Gal}(K/\mathbb{Q})}$ is in fact an isomorphism although its injectivity is enough for the proof of the Theorem 1.1.

4. Unramifiedness of $H^1_f(\mathbb{Q},M)$ outside p

4.1. **Tamagawa factor of $A_{f,D}$ at $\ell(\neq p)$.** First, we introduce some basic notions on the Tamagawa factor of A. For a prime number $\ell\neq p$, let I_ℓ denotes the inertia subgroup of $G_{\mathbb{Q}_\ell}$ and $\mathcal{A}:=A^{I_\ell}/(A^{I_\ell})_{\mathrm{div}}$, where $(A^{I_\ell})_{\mathrm{div}}$ denotes the maximal divisible subgroup of A^{I_ℓ}. So $\mathcal{A}$ is a finite group.

Definition 4.1. *We define the p-part of the Tamagawa factor of A at ℓ as*

$$c(\mathbb{Q}_\ell,A):=\#\mathcal{A}/(\mathrm{Frob}_\ell-1)\mathcal{A}=\#\mathcal{A}^{\mathrm{Frob}_\ell=1}.$$

Here Frob_ℓ denotes the Frobenius element in $\mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell)$. Note that for an endmorphism g of $\mathcal{A}$, the orders of $\ker(g)$ and $\mathrm{coker}(g)$ are the same since $\mathcal{A}$ is finite, hence the second equality in the definition holds. Roughly speaking, this Tamagawa factor of A can be used to measure the difference $H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M)$ and the local condition $H^1_f(\mathbb{Q}_\ell, M)$.

Proposition 4.2. *If $c(\mathbb{Q}_\ell, A) = 1$, then $H^1_f(\mathbb{Q}_\ell, M) = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M)$.*

(Proof of Proposition 4.2)

We first consider the local condition with the coefficient in A.

$$\begin{aligned} H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, A)/H^1_f(\mathbb{Q}_\ell, A) &\xrightarrow{\sim} \mathrm{coker}\left(H^1_f(\mathbb{Q}_\ell, V) = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, V) \xrightarrow{\pi} H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, A)\right) \\ &\xrightarrow{\sim} \mathrm{coker}\left(V^{I_\ell}/(\mathrm{Frob}_\ell - 1)(V^{I_\ell}) \xrightarrow{\pi} A^{I_\ell}/(\mathrm{Frob}_\ell - 1)(A^{I_\ell})\right) \\ &\xrightarrow{\sim} \mathcal{A}/(\mathrm{Frob}_\ell - 1)\mathcal{A}. \end{aligned}$$

Here we use the following identification in the second isomorphism above.

$$H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, V) = H^1(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell, V^{I_\ell}) \underset{\mathrm{ev}}{\xrightarrow{\sim}} V^{I_\ell}/(\mathrm{Frob}_\ell - 1)(V^{I_\ell})$$

where the isomorphism ev is given by evaluating every 1-cocycle with Frob_ℓ. Thus if $c(\mathbb{Q}_\ell, A) = \#\mathcal{A}/(\mathrm{Frob}_\ell - 1)\mathcal{A} = 1$, we have $H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, A) = H^1_f(\mathbb{Q}_\ell, A)$. On the other hand, since $H^1_f(\mathbb{Q}_\ell, M)$ is the inverse image of $H^1_f(\mathbb{Q}_\ell, A) = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, A)$ under $\iota : H^1_f(\mathbb{Q}_\ell, M) \to H^1_f(\mathbb{Q}_\ell, A)$, we have

$$\begin{aligned} H^1_f(\mathbb{Q}_\ell, M) &= \ker(H^1(\mathbb{Q}_\ell, M) \to H^1(\mathbb{Q}_\ell, A) \to H^1_f(\mathbb{Q}_\ell^{\mathrm{ur}}, A)^{\mathrm{Frob}_\ell = 1}) \\ &= \ker(H^1(\mathbb{Q}_\ell, M) \to H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, M)^{\mathrm{Frob}_\ell = 1} \xrightarrow{g} H^1_f(\mathbb{Q}_\ell^{\mathrm{ur}}, A)^{\mathrm{Frob}_\ell = 1}). \end{aligned}$$

Here the homomorphism g is injective. In fact, from an exact sequence of I_ℓ-modules

$$0 \to M \longrightarrow A \xrightarrow{\times p} A \to 0,$$

we have an exact sequence

$$0 \to (A^{I_\ell} \otimes \mathbb{F}_p)^{\mathrm{Frob}_\ell = 1} \longrightarrow H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, M)^{\mathrm{Frob}_\ell = 1} \xrightarrow{g} H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, A)^{\mathrm{Frob}_\ell = 1}.$$

Since $A^{I_\ell} \otimes \mathbb{F}_p = \mathcal{A} \otimes \mathbb{F}_p$, we obtain

$$\ker(g) = (A^{I_\ell} \otimes \mathbb{F}_p)^{\mathrm{Frob}_\ell = 1} = (\mathcal{A} \otimes \mathbb{F}_p)^{\mathrm{Frob}_\ell = 1} = \mathcal{A}^{\mathrm{Frob}_\ell = 1} \otimes \mathbb{F}_p = 0.$$

In the third equality above, we use the assumption $c(\mathbb{Q}_\ell, A) = \#\mathcal{A}^{\mathrm{Frob}_\ell = 1} = 1$ to get $H^1(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell, \mathcal{A}) = 0$. Thus the homomorphism g is injective and we get

$$H^1_f(\mathbb{Q}_\ell, M) = \ker(H^1(\mathbb{Q}_\ell, M) \to H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, M)^{\mathrm{Frob}_\ell = 1}) = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M).$$

□

4.2. **Unramifiedness of H^1_f outside p.** Now we prove the following proposition which is the claim in (Step 2).

Proposition 4.3. *If the Tamagawa factor $c(\mathbb{Q}_\ell, A)$ of A at ℓ is trivial for every prime ℓ with $\ell \mid N$ (the assumption (4) in Theorem 1.1), then the elements in $H^1_f(\mathbb{Q}, M)$ are unramified outside p.*

(Proof of Proposition 4.3)

Since $p \geqslant 3$, there is nothing to prove for unramifiedness at the infinite place of $\mathbb{Q}$. If $\ell \nmid N$, the inertia subgroup I_ℓ at ℓ acts on $A^0_f = V^0_f/T^0_f$ trivially. So we have

$$A^{I_\ell}_{f,D} = \begin{cases} A_{f,D} & (\sqrt{D} \in \mathbb{Q}^{\mathrm{ur}}_\ell), \\ 0 & (\text{otherwise}). \end{cases}$$

Hence we have $c(\mathbb{Q}_\ell, A) = 1$ in both cases to get $H^1_f(\mathbb{Q}_\ell, M) = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M)$ from Proposition 4.2. While for $\ell \mid N$, we assume that $c(\mathbb{Q}_\ell, T) = 1$ and obtain $H^1_f(\mathbb{Q}_\ell, M) = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M)$. Thus elements in the Selmer group $H^1_f(\mathbb{Q}, M)$ are unramified outside p. □

Finally, we introduce a sufficient condition on $M = A[p]$ for $c(\mathbb{Q}_\ell, A) = 1$.

Proposition 4.4. *For a prime number $\ell \neq p$, if $M^{G_{\mathbb{Q}_\ell}} = 0$, then $c(\mathbb{Q}_\ell, A) = 1$.*

(Proof of Proposition 4.3)

We have an commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (A^{I_\ell})_{\mathrm{div}} & \longrightarrow & A^{I_\ell} & \longrightarrow & \mathcal{A} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Frob}_p - 1} & & \downarrow{\scriptstyle \mathrm{Frob}_p - 1} & & \downarrow{\scriptstyle \mathrm{Frob}_p - 1} & & \\ 0 & \longrightarrow & (A^{I_\ell})_{\mathrm{div}} & \longrightarrow & A^{I_\ell} & \longrightarrow & \mathcal{A} & \longrightarrow & 0. \end{array}$$

Since we assume $M^{G_{\mathbb{Q}_\ell}} = 0$ and this is equivalent to the condition $H^0(\mathbb{Q}_\ell, A) = 0$, the middle vertical arrow is injective and so is the left vertical arrow. While $(A^{I_\ell})_{\mathrm{div}}$ is the direct sum of finite number of $\mathbb{Q}_p/\mathbb{Z}_p$, the injective left vertical arrow is in fact an isomorphism. So the right vertical arrow is injective by Snake lemma which implies $c(\mathbb{Q}_\ell, A) = \#\mathcal{A}^{\mathrm{Frob}_p = 1} = 1$. □

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

5.1. **Image of the localization at p.** In this section, we consider the restriction map $\mathrm{Res}^{\mathrm{ur}}_p : H^1_f(\mathbb{Q}, M) \to H^1(\mathbb{Q}^{\mathrm{ur}}_p, M)$ at p and show that its image has at most dimension 1 over $\mathbb{F}_p$ under the assumptions (2) in Theorem 1.1. We decompose the restriction map as

$$\mathrm{Res}^{\mathrm{ur}}_p : H^1_f(\mathbb{Q}, M) \xrightarrow{\mathrm{Loc}_p} H^1(\mathbb{Q}_p, M) \xrightarrow{\mathrm{Res}_{\mathbb{Q}^{\mathrm{ur}}_p/\mathbb{Q}_p}} H^1(\mathbb{Q}^{\mathrm{ur}}_p, M),$$

and study the image of Loc_p which is the restriction of cohomology classes to the decomposition group at p. The image of $H^1_f(\mathbb{Q}, M)$ under Loc_p is in the local condition $H^1_f(\mathbb{Q}_p, M)$ at p. By the definition of the local condition and the exact sequence (1), we have an exact sequence

$$0 \to A^{G_{\mathbb{Q}_p}} \otimes \mathbb{F}_p \to H^1_f(\mathbb{Q}_p, M) \xrightarrow{\iota} H^1_f(\mathbb{Q}_p, A)[p] \to 0.$$

So we have an inequality

$$\begin{aligned} \dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Loc}_p)) &\leqslant \dim_{\mathbb{F}_p}(H^1_f(\mathbb{Q}_p, M)) \\ &\leqslant \dim_{\mathbb{F}_p}\left(A^{G_{\mathbb{Q}_p}} \otimes \mathbb{F}_p\right) + \dim_{\mathbb{F}_p}\left(H^1_f(\mathbb{Q}_p, A)[p]\right). \end{aligned} \tag{2}$$

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

Proposition 5.1 ([1], Corollary 3.8.4)**.** *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 Fontaine's de Rham period ring and $\mathbf{B}^+_{\mathrm{dR}}$ is its valuation ring. If V is a de Rham representation, then*

$$\dim_{\mathbb{Q}_p}(H^1_f(\mathbb{Q}_p, V)) = \dim_{\mathbb{Q}_p}(\mathbf{D}_{\mathrm{dR}}(V)/\mathbf{D}^+_{\mathrm{dR}}(V)) + \dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V). \tag{3}$$

Since we assume $p \nmid N$, the p-adic representation V^0_f of $G_{\mathbb{Q}_p}$ is crystalline and its Hodge-Tate weight is $\{0,\, k-1\}$. So $V = V_{f,D}$ is also crystalline with Hodge-Tate weight $\{1-k/2,\, k/2\}$, hence we obtain $\dim_{\mathbb{Q}_p}(\mathbf{D}_{\mathrm{dR}}(V)/\mathbf{D}^+_{\mathrm{dR}}(V)) = 2-1 = 1$. Since $H^1_f(\mathbb{Q}_p, A)$ is the image of $H^1_f(\mathbb{Q}_p, V)$ and cofinitely generated as a $\mathbb{Z}_p$-module, we have $\dim_{\mathbb{F}_p}\left(H^1_f(\mathbb{Q}_p, A)[p]\right) = \dim_{\mathbb{Q}_p}(H^1_f(\mathbb{Q}_p, V))$. Then by (3), we obtain

$$\dim_{\mathbb{F}_p}(H^1_f(\mathbb{Q}_p, A)[p]) = 1 + \dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V). \tag{4}$$

From (2), (4), we have

$$\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Loc}_p)) \leqslant \dim_{\mathbb{F}_p}\left(A^{G_{\mathbb{Q}_p}} \otimes \mathbb{F}_p\right) + 1 + \dim_{\mathbb{Q}_p} H^0(\mathbb{Q}_p, V). \tag{5}$$

In the following, we compute the first and the third terms in the above equality.

5.2. **Supersingular case.**

Proposition 5.2. *If f is supersingular at p and $k \leqslant p+1$, then we have*

$$A^{G_{\mathbb{Q}_p}} \otimes \mathbb{F}_p = V^{G_{\mathbb{Q}_p}} = 0.$$

We use the following result of Fontaine and Edixhoven.

Theorem (Fontaine-Edixhoven)**.**
If the weight k of f satisfies $2 \leqslant k \leqslant p+1$, then $\bar{\rho}^0_f|_{G_{\mathbb{Q}_p}}$ is irreducible.

Remark 5.3. *Note that we cite their result as far as we use it. Their result describe a more precise local behavior of $\bar{\rho}^0_f$ at a supersingular prime. See for example* [6].

(Proof of Proposition 5.2)

From the above result, M_f^0 and its twist $M = M_{f,D}$ are irreducible $G_{\mathbb{Q}_p}$-modules. Hence we obtain $M^{G_{\mathbb{Q}_p}} = A[p]^{G_{\mathbb{Q}_p}} = 0$ and $A^{G_{\mathbb{Q}_p}} = 0$ to get $A^{G_{\mathbb{Q}_p}} \otimes \mathbb{F}_p = 0$. Since the residual representation M is irreducible, the p-adic representation V is also irreducible as a $G_{\mathbb{Q}_p}$-module which implies $V^{G_{\mathbb{Q}_p}} = 0$. □

5.3. **Ordinary case.**

Proposition 5.4. *Suppose f is ordinary at p. Then we have $V^{G_{\mathbb{Q}_p}} = 0$.*

(Proof of Proposition 5.4)

We fix a basis of T_f^0 over $\mathbb{Z}_p$ and this also yields a basis of V_f^0 over $\mathbb{Q}_p$. Taking corresponding bases $\{v_1, v_2\}$ for its twist $V = V_{f,D}$, we know $g \in G_{\mathbb{Q}_p}$ acts on it as

$$\begin{pmatrix} \chi_{\mathrm{cyc}}^{k/2}(g)\psi^{-1}(g) & u(g) \\ 0 & \psi(g)\chi_{\mathrm{cyc}}^{1-k/2} \end{pmatrix} \cdot \chi_D(g), \tag{6}$$

where $\psi : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ is an unramified character and $u(g) \in \mathbb{Z}_p$. We have a subspace $W_1 := \mathbb{Q}_p v_1$ of V on which $G_{\mathbb{Q}_p}$ acts via the character $\chi_{\mathrm{cyc}}^{k/2}\chi_D\psi^{-1} : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$. If $V^{G_{\mathbb{Q}_p}} \neq 0$, in other words, there is a non-trivial subspace W_0 of V on which $G_{\mathbb{Q}_p}$ acts trivially, then that is 1-dimensional and linearly independent with W_1 since $\chi_{\mathrm{cyc}}^{k/2}\chi_D\psi^{-1} \neq 1$. Then the matrix (6) is similar to

$$\begin{pmatrix} \chi_{\mathrm{cyc}}^{k/2}(g)\chi_D\psi^{-1}(g) & 0 \\ 0 & 1 \end{pmatrix}.$$

Taking determinants of above matrices, we have

$$\chi_{\mathrm{cyc}}(g) = \chi_{\mathrm{cyc}}^{k/2}(g)\chi_D(g)\psi^{-1}(g) \quad \text{for all } g \in G_{\mathbb{Q}_p},$$

but this equality can not be hold. This is a contradiction and hence we obtain $V^{G_{\mathbb{Q}_p}} = 0$. □

Proposition 5.5. *Suppose f is ordinary at p and $p-1 \nmid k-1$. Then we have $M^{G_{\mathbb{Q}_p}} = 0$ if and only if the following situations depending on D do not happen:*
(When $p \nmid D$)

(*a*) *M does not split as a $G_{\mathbb{Q}_p}$-module and $p-1 \mid k/2$ and $a_p \equiv 1 \pmod{p}$.*
(*b*) *M splits as a $G_{\mathbb{Q}_p}$-module and $p-1 \mid k/2$ or $1-k/2$ and $a_p \equiv 1 \pmod{p}$.*

(When $D = p^* := (-1)^{\frac{p-1}{2}}p$)

(*c*) *M does not split as a $G_{\mathbb{Q}_p}$-module and $p-1 \mid \frac{k-p+1}{2}$ and $a_p \equiv 1 \pmod{p}$.*
(*d*) *M splits as a $G_{\mathbb{Q}_p}$-module and $p-1 \mid \frac{k-p+1}{2}$ or $\frac{k+p-3}{2}$ and $a_p \equiv 1 \pmod{p}$.*

(Proof of Proposition 5.5)

We fix a basis of T_f^0 over $\mathbb{Z}_p$ as in the proof of Proposition 5.4 and this yields a basis of M_f^0 over $\mathbb{F}_p$. Taking a corresponding basis $\{m_1, m_2\}$ for its twist $M = M_{f,D}$ over $\mathbb{F}_p$, we know $g \in G_{\mathbb{Q}_p}$ acts on M as

$$\begin{pmatrix} \omega_{\mathrm{cyc}}^{k/2}(g)\bar{\psi}^{-1}(g) & \bar{u}(g) \\ 0 & \bar{\psi}(g)\omega_{\mathrm{cyc}}^{1-k/2} \end{pmatrix} \cdot \chi_D(g), \tag{7}$$

where ψ and $u(g) \in \mathbb{Z}_p$ are as in (6) and $\bar{\psi}$ and $\bar{u}(g)$ are their reduction modulo p. We show that $M^{G_{\mathbb{Q}_p}} = 0$ if the situations described in Proposition 5.5 do not occur by a case-by-case computation.

(Case 1 : $p \nmid D$)

In this case we have $\sqrt{D} \in \mathbb{Q}_p^{\mathrm{ur}}$. So $g \in I_p$ acts on M via a matrix

$$\begin{pmatrix} \omega_{\mathrm{cyc}}^{k/2}(g) & \bar{u}(g) \\ 0 & \omega_{\mathrm{cyc}}^{1-k/2} \end{pmatrix}.$$

First, suppose M splits as a $G_{\mathbb{Q}_p}$-module, in other words $\bar{u} = 0$. For $a, b \in \mathbb{F}_p$, an element $x = am_1 + bm_2 \in M$ and $g \in I_p$,

$$g(x) = g(av_1 + bv_2) = a\omega_{\mathrm{cyc}}^{k/2}(g)m_1 + b\omega_{\mathrm{cyc}}^{1-k/2}(g)m_2.$$

Thus $x \in M^{I_p}$ if and only if

$$a\omega_{\mathrm{cyc}}^{k/2}(g) = a,\ b\omega_{\mathrm{cyc}}^{1-k/2}(g) = b \ \text{ for all } g \in I_p. \tag{8}$$

If $p-1 \nmid k/2$ and $p-1 \nmid 1-k/2$, then conditions in (8) implies $a = b = 0$ and we get $M^{G_{\mathbb{Q}_p}} \subset M^{I_p} = 0$. If one of the conditions $p-1 \mid k/2$ or $p-1 \mid 1-k/2$ holds, then $M^{I_p} = \mathbb{F}_p m_1$ or $M^{I_p} = \mathbb{F}_p m_2$ respectively. We know that the Frobenius element Frob_p acts on $\mathbb{F}_p m_1$ and $\mathbb{F}_p m_2$ via multiplication by $a_p(f)^{-1}$ mod p and $a_p(f)$ mod p respectively, where $a_p(f)$ is the p-th Fourier coefficient of f. Thus $M^{G_{\mathbb{Q}_p}} = (M^{I_p})^{\mathrm{Frob}_p=1} = 0$ if we have $a_p(f) \not\equiv 1 \pmod{p}$. If $a_p(f) \equiv 1 \pmod{p}$, $M^{G_{\mathbb{Q}_p}}$ is a 1-dimensional subspace of M.

Next, suppose M does not split as a $G_{\mathbb{Q}_p}$-module, we use the following lemma.

Lemma 5.6. *Suppose M does not split as a $G_{\mathbb{Q}_p}$-module. If $p-1 \nmid k-1$, then we have $\bar{u}(G_{\mathbb{Q}_p^{\mathrm{ab}}}) \neq 0$ for a suitable basis of M, where $\mathbb{Q}_p^{\mathrm{ab}}$ denotes the maximal abelian extension of $\mathbb{Q}_p$.*

We prove this lemma later. From (7), $G_{\mathbb{Q}_p^{\mathrm{ab}}}$ acts on M via $\begin{pmatrix} 1 & \bar{u}(g) \\ 0 & 1 \end{pmatrix}$. By a similar argument with which we obtain the condition (8), we can show that an element $x = am_1 + bm_2 \in M$ is fixed by $G_{\mathbb{Q}_p^{\mathrm{ab}}}$ if and only if

$$a = a + b\bar{u}(g) \text{ for all } g \in G_{\mathbb{Q}_p^{\mathrm{ab}}}.$$

From Lemma 5.7, once we retake a suitable basis of M, there exist $g \in G_{\mathbb{Q}_p^{\mathrm{ab}}}$ such that $\bar{u}(g) \neq 0$ which implies $b = 0$ and we obtain $M^{I_p} = (M^{G_{\mathbb{Q}_p^{\mathrm{ab}}}})^{I_p} = (\mathbb{F}_p m_1)^{I_p}$. Since retaking the basis of M in Lemme 5.7 changes only the upper right component $\bar{u}$ of (7) from the proof of Lemma 5.7, I_p acts on $\mathbb{F}_p m_1$ still via the character $\omega_{\mathrm{cyc}}^{k/2}$. Hence if $p-1 \nmid k/2$, then $M^{G_{\mathbb{Q}_p}} \subset M^{I_p} = 0$. If $p-1 \mid k/2$, then $M^{I_p} = \mathbb{F}_p m_1$ and Frob_p acts on this space via multiplication by $a_p(f)^{-1}$ mod p. Thus if $a_p(f) \not\equiv 1 \pmod{p}$, we have $M^{G_{\mathbb{Q}_p}} = (M^{I_p})^{\mathrm{Frob}_p = 1} = 0$ otherwise $M^{G_{\mathbb{Q}_p}} = \mathbb{F}_p m_1$.

(Case 2 : $p \mid D$ and $D \neq p^*$)

In this case, $\mathbb{Q}_p^{\mathrm{ur}}(\sqrt{D})$ and $\mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)$ are linearly disjoint over $\mathbb{Q}_p^{\mathrm{ur}}$. Hence there exists $\sigma \in G_{\mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)}$ such that $\chi_D(\sigma) = -1$. From (7), $G_{\mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)}$ acts on M via

$$\begin{pmatrix} 1 & \bar{u}(g) \\ 0 & 1 \end{pmatrix} \cdot \chi_D(g).$$

Thus an element $x = am_1 + bm_2 \in M$ fixed by $G_{\mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)}$ if and only if

$$\chi_D(g)(a + b\bar{u}(g)) = a, \ \chi_D(g)b = b \text{ for all } g \in G_{\mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)}. \tag{9}$$

Putting $g = \sigma$, we obtain $b = 0$ from the second equality in (9) since p is odd and then we get $a = 0$ from the first equality. Thus we have $M^{G_{\mathbb{Q}_p}} \subset M^{G_{\mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)}} = 0$.

(Case 3 : $D = p^*$)

In this case we have an inclusion $\mathbb{Q}_p^{\mathrm{ur}}(\sqrt{D}) \subset \mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)$. Suppose M splits as a $G_{\mathbb{Q}_p}$-module. As the calculation in (Case 1), an element $x = am_1 + bm_2 \in M$ fixed by I_p if and only if

$$a\omega_{\mathrm{cyc}}^{k/2}(g)\chi_D(g) = a, \ b\omega_{\mathrm{cyc}}^{1-k/2}(g)\chi_D(g) = b \text{ for all } g \in I_p. \tag{10}$$

This condition is equivalent to the condition that the same equations hold for a generator τ of the Galois group $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)/\mathbb{Q}_p^{\mathrm{ur}})$. We have $\chi_D(\tau) = -1$ and $\omega_{\mathrm{cyc}}(\tau)$ is order $p-1$. Thus (10) is equivalent to the condition

$$-a\omega_{\mathrm{cyc}}^{k/2}(\tau) = a, \ -b\omega_{\mathrm{cyc}}^{1-k/2}(\tau) = b. \tag{11}$$

If $\frac{p-1}{2} \not\equiv k/2 \pmod{p-1}$ and $\frac{p-1}{2} \not\equiv 1 - k/2 \pmod{p-1}$, then $a = b = 0$ from the above condition and we get $M^{G_{\mathbb{Q}_p}} \subset M^{I_p} = 0$. If one of the conditions $\frac{p-1}{2} \equiv k/2 \pmod{p-1}$ and $\frac{p-1}{2} \equiv 1-k/2 \pmod{p-1}$ holds, then $M^{I_p} = \mathbb{F}_p m_1$ and $M^{I_p} = \mathbb{F}_p m_2$ respectively. As in the argument in (Case 1), if $a_p(f) \not\equiv 1 \pmod{p}$, then $M^{G_{\mathbb{Q}_p}} = (M^{I_p})^{\mathrm{Frob}_p = 1} = 0$ otherwise $M^{G_{\mathbb{Q}_p}}$ is a 1-dimensional subspace of M.

Finally, suppose M does not split as a $G_{\mathbb{Q}_p}$-module. By the same argument in (Case 1), we can show that an element $x = am_1 + bm_2 \in M$ is fixed by $G_{\mathbb{Q}_p^{ab}}$ if and only if

$$a = a + b\bar{u}(g) \text{ for all } g \in G_{\mathbb{Q}_p^{ab}}.$$

and this implies $b = 0$ from Lemma 5.7 after retaking a suitable basis of M. Then $M^{I_p} = (M^{G_{\mathbb{Q}_p^{ab}}})^{I_p} = (\mathbb{F}_p m_1)^{I_p}$ and I_p acts on $\mathbb{F}_p m_1$ via $\omega_{\text{cyc}}^{k/2}\chi_D$. So we can see that $x = am_1 \in M^{G_{\mathbb{Q}_p^{ab}}}$ is fixed by I_p if and only if

$$-a\omega_{\text{cyc}}^{k/2}(\tau) = a$$

as we get the condition (11). If $\frac{p-1}{2} \not\equiv k/2 \pmod{p-1}$, then $a = 0$ from this equality and we obtain $M^{G_{\mathbb{Q}_p}} \subset M^{I_p} = 0$. If $\frac{p-1}{2} \equiv k/2 \pmod{p-1}$, then $M^{I_p} = \mathbb{F}_p m_1$ and we have $M^{G_{\mathbb{Q}_p}} = (M^{I_p})^{\text{Frob}_p = 1} = (\mathbb{F}_p m_1)^{\text{Frob}_p = 1}$. This is trivial if $a_p(f) \not\equiv 1 \pmod{p}$ otherwise $M^{G_{\mathbb{Q}_p}} = \mathbb{F}_p m_1$. □

To finish the proof of Proposition 5.5 completely, we prove the Lemma 5.7.

Lemma 5.7. *Suppose M does not split as a $G_{\mathbb{Q}_p}$-module. If $p - 1 \nmid k - 1$, then we have $\bar{u}(G_{\mathbb{Q}_p^{ab}}) \neq 0$ for a suitable basis of M, where $\mathbb{Q}_p^{ab}$ denotes the maximal abelian extension of $\mathbb{Q}_p$.*

(Proof of Lemma 5.7)

If $M = M_{f,D}$ does not split as a $G_{\mathbb{Q}_p}$-module, then so does M_f^0. Recall that I_p acts on M_f^0 via a homomorphism $\bar{\rho}_f^0$ and the image of $g \in I_p$ under this is a matrix

$$\begin{pmatrix} \omega_{\text{cyc}}^{k-1}(g) & \bar{v}(g) \\ 0 & 1 \end{pmatrix}, \tag{12}$$

where $\bar{v}(g) \in \mathbb{F}_p$. We show that $\bar{v}(G_{\mathbb{Q}_p^{ab}}) \neq 0$ which immediately implies $\bar{u}(G_{\mathbb{Q}_p^{ab}}) \neq 0$ since $\bar{v}$ differs from $\bar{u}$ by a character $\omega_{\text{cyc}}^{1-k/2} \otimes \chi_D$. We use the following fact.

Proposition 5.8 ([13], Lemma 2.2)**.** *Let $p > 2$ be a prime number and $B \subset \mathrm{GL}_2(\mathbb{F}_p)$ a Borel subgroup such that B contains a matrix $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ with $a \not\equiv c \pmod{p}$. Let $B' := h^{-1}Bh$ with $h = \begin{pmatrix} 1 & b/(c-a) \\ 0 & 1 \end{pmatrix}$.*

(1) *We can decompose B' which is conjugate to B as*

$$B' = B'_d \cdot B'_1,$$

and $B/[B,B] \cong B'/[B',B']$. Here groups B'_d, B'_1 are defined as

$$B'_d = B' \cap \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \middle| \, a, c \in \mathbb{F}_p^\times \right\},$$

$$B'_1 = B' \cap \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{F}_p \right\}.$$

(2) $[B', B'] = B'_1$.

We put $\mathcal{D}_p := \bar{\rho}_f^0(G_{\mathbb{Q}_p}), \mathcal{I}_p := \bar{\rho}_f^0(I_p)$. Since we assume $p-1 \nmid k-1$, $\omega_{\mathrm{cyc}}^{k-1}$ is not a trivial character. Then there exist a matrix $A \in \mathcal{I}_p \subset \mathcal{D}_p$ such that $A = \begin{pmatrix} a & * \\ 0 & 1 \end{pmatrix}$, and $a \not\equiv 1 \pmod{p}$. Thus $\mathcal{D}_p$ satisfies the assumptions in Proposition 5.8 and we have a decomposition of $\mathcal{D}_p$ as in Proposition 5.8 for a suitable basis of M_f^0.

$$\begin{aligned} \mathcal{D}_p &= (\mathcal{D}_p)_d \cdot (\mathcal{D}_p)_1 \\ &= \left\{ \begin{pmatrix} \omega_{\mathrm{cyc}}^{k-1}(g)\psi^{-1}(g) & 0 \\ 0 & \psi(g) \end{pmatrix} \middle| \, g \in G_{\mathbb{Q}_p} \right\} \cdot \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{F}_p \right\}. \end{aligned}$$

Since we assume that M_f^0 does not split, we have $(\mathcal{D}_p)_1 \neq \{I\}$. From Proposition 5.8 (2), this means the commutator subgroup of $\mathcal{D}_p$ is non-trivial which implies $\mathcal{D}_p$ is non-abelian. Thus we obtain $\bar{v}(G_{\mathbb{Q}_p^{\mathrm{ab}}}) \neq 0$ in (12). □

Thus we get conditions on which we have $M^{G_{\mathbb{Q}_p}} = (A[p])^{G_{\mathbb{Q}_p}} = 0$ in Proposition 5.2 and 5.5. Under such conditions, we especially have $A^{G_{\mathbb{Q}_p}} \otimes \mathbb{F}_p = 0$. Then from the inequality (5), Proposition 5.2, 5.4 and 5.5, we obtain the desired inequality

$$\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Res}_p^{\mathrm{ur}})) \leqslant \dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Loc}_p)) \leqslant 1$$

which is the claim of (Step 3) under the assumptions of the propositions.

5.4. **CM case.** However, in the ordinary case, if $k = 2$ and T/p^nT splits for all n, we still have the above inequality $\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Res}_p^{\mathrm{ur}})) \leqslant 1$ even when the situation (b) in Proposition 5.5 occurs.

Proposition 5.9. *If $k = 2$ and T/p^nT splits as a $G_{\mathbb{Q}_p}$-module for all n, then we have $\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Res}_p^{\mathrm{ur}})) \leqslant 1$.*

(Proof of Proposition 5.9)

When the situation (b) occurs, we know that $M^{G_{\mathbb{Q}_p}}$ is 1-dimensional over $\mathbb{F}_p$ from the proof of Proposition 5.5 which implies $A^{G_{\mathbb{Q}_p}} \otimes \mathbb{F}_p$ is also 1-dimensional. Thus we have $\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Loc}_p)) \leqslant \dim_{\mathbb{F}_p}(H^1_f(\mathbb{Q}_p, M)) = 1 + 1 = 2$ from (5).

For every $n \in \mathbb{Z}_{\geqslant 1}$, I_p acts on T/p^nT via a diagonal matrix

$$\begin{pmatrix} \chi_{\mathrm{cyc}}^{(n)}(g) & 0 \\ 0 & 1 \end{pmatrix}$$

since $k = 2$ and we assume that T/p^nT splits as a $G_{\mathbb{Q}_p}$-module. Here $\chi_{\mathrm{cyc}}^{(n)}$ denotes the mod p^n cyclotomic character. Note that in the situation (b), we assume $p \nmid D$ and hence χ_D is trivial when restricted to the inertia subgroup I_p. So we have $(A[p^n])^{I_p} \cong (T/p^nT)^{I_p} \cong \mathbb{Z}/p^n\mathbb{Z}$ and $A^{I_p} \otimes \mathbb{F}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{F}_p = 0$. On the other hand, there is a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & A^{G_{\mathbb{Q}_p}} \otimes \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} & \longrightarrow & H^1_f(\mathbb{Q}_p, M) \\ & & \downarrow & & \downarrow {\scriptstyle \mathrm{Res}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p}} \\ 0 & \longrightarrow & A^{I_p} \otimes \mathbb{F}_p = 0 & \longrightarrow & H^1(\mathbb{Q}_p^{\mathrm{ur}}, M). \end{array}$$

Thus the restriction map $\mathrm{Res}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p}$ is not injective and its kernel has at least dimension 1 over $\mathbb{F}_p$. Since we have a decomposition $\mathrm{Res}_p^{\mathrm{ur}} = \mathrm{Res}_{\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p} \circ \mathrm{Loc}_p$, we get the desired inequality $\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Res}_p^{\mathrm{ur}})) \leqslant 2 - 1 = 1$. □

Remark 5.10. *The splitting condition in Proposition 5.9 corresponds to the condition* (2) *in the theorem of Prasad and Shekhar. Let T be an integral p-adic Tate module of an elliptic curve E over $\mathbb{Q}$ and suppose E has complex multiplication over an extension of $\mathbb{Q}_p$. Then T/p^nT splits as a $G_{\mathbb{Q}_p}$-module for every n. Thus the splitting condition in Proposition 5.9 holds for T. It is conjectured by Ghate that for a modular form f which is ordinary at p, T_f^0/p^n splits as a $G_{\mathbb{Q}_p}$-module for all n if and only if f has complex multiplication. For detail, see* [9] *for example.*

To summarize, we obtain the following proposition.

Proposition 5.11. *We assume the following:*

- *If f is supersingular at p, then $k \leqslant p+1$ holds.*
- *If f is ordinary at p, then $p-1 \nmid k-1$ and the conditions below do not occur:*

  (*If $p \nmid D$.*)
  (*a*) *M does not split as a $G_{\mathbb{Q}_p}$-module and $p-1 \mid k/2$ and $a_p \equiv 1 \pmod{p}$.*
  (*b_1*) *$k > 2$ and M splits as a $G_{\mathbb{Q}_p}$-module and $p-1 \mid k/2$ or $1-k/2$ and $a_p \equiv 1 \pmod{p}$.*
  (*b_2*) *$k = 2$ and M splits as a $G_{\mathbb{Q}_p}$-module and T/p^nT does not split for some n.*
  (*If $D = p^* := (-1)^{\frac{p-1}{2}}p$.*)
  (*c*) *M does not split as a $G_{\mathbb{Q}_p}$-module and $p-1 \mid \frac{k-p+1}{2}$ and $a_p \equiv 1 \pmod{p}$.*
  (*d*) *M splits as a $G_{\mathbb{Q}_p}$-module and $p-1 \mid \frac{k-p+1}{2}$ or $\frac{k+p-3}{2}$ and $a_p \equiv 1 \pmod{p}$.*

Then we have an equality $\dim_{\mathbb{F}_p}(\mathrm{Im}(\mathrm{Res}_p^{\mathrm{ur}})) \leqslant 1$.

This completes the proof of Theorem 1.1 as we explain in Section 2.

6. Numerical examples

We finally introduce some numerical examples of Theorem 1.1. To do this, we consider situations in which the inequality

$$\dim_{\mathbb{F}_p}\left(Ш_p^{BK}(\mathbb{Q}, A_{f,D})[p]\right) \geqslant 2 \tag{13}$$

holds. This inequality implies the condition $\dim_{\mathbb{F}_p}\left(H^1_f(\mathbb{Q}, M_{f,D})\right) \geqslant 2$ in Theorem 1.1. Since the p-adic representation $V_{f,D}$ is self-dual, the $\mathbb{F}_p$-dimension of $Ш_p^{BK}(\mathbb{Q}, A_{f,D})[p]$ is even due to the existence of the generalized Cassels-Tate pairing in [7]. Hence the inequality (13) holds if and only if $Ш_p^{BK}(\mathbb{Q}, A_{f,D})$ is non-trivial. We study when this occurs assuming the Bloch-Kato conjecture.

6.1. **Ratios of central L-values.** In the following, we assume $N = 1$. For a quadratic discriminant D and a modular form $f(\tau) = \sum a_n q^n$, we consider a twisted L-function of f by a quadratic character χ_D

$$L(f, \chi_D, s) := \sum_{n=1}^{\infty} \frac{\chi_D(n) a_n}{n^s}$$

which converges absolutely when the real part of s is sufficiently large. This complex L-function can be continued analytically to the whole complex plane and we can consider its central value $L(f, \chi_D, k/2)$.

Let $D, D' \in \mathbb{Z}$ be two quadratic discriminants. We think the ratio of central values of twisted L-functions $L(f, \chi_D, k/2)$ and $L(f, \chi_{D'}, k/2)$. Suppose that $L(f, \chi_D, k/2) \neq 0$. Then the Bloch-Kato conjecture predicts such a value in terms of arithmetic invariants including the order of Bloch-Kato's Tate-Shafarevich group $Ш_p^{BK}(\mathbb{Q}, A_{f,D})$, and implies an equality of the following p-adic valuations:

$$v_p\left(\frac{L(f,\chi_D,k/2)}{\mathrm{vol}_\infty(\chi_D,1-k/2)}\right)=v_p\left(\frac{\#\text{Ш}_p^{BK}(\mathbb{Q},A_{f,D})}{(\#\Gamma_{\mathbb{Q}}(A_{f,D}))^2}\right). \tag{14}$$

Here $\mathrm{vol}_\infty(\chi_D,1-k/2)$ denotes certain transcendental part of the value $L(f,\chi_D,k/2)$ and $\Gamma_{\mathbb{Q}}(A_{f,D}) := H^0(\mathbb{Q},A_{f,D})$. For the precise definitions, see [5, Section2]. Note that the product of Tamagawa factor does not appear in the above equality since we assume $N=1$.

Suppose f satisfies the conditions in Theorem 1.1. Then $M_{f,D}=A_{f,D}[p]$ is irreducible as a $G_{\mathbb{Q}}$-module which implies $\#\Gamma_{\mathbb{Q}}(A_{f,D})=1$. Thus (14) yields

$$v_p\left(\frac{L(f,\chi_D,k/2)}{\mathrm{vol}_\infty(\chi_D,1-k/2)}\right)=v_p\left(\#\text{Ш}_p^{BK}(\mathbb{Q},A_{f,D})\right). \tag{15}$$

For the transcendental factor $\mathrm{vol}_\infty(\chi_D,1-k/2)$, we have the following property.

Lemma 6.1 ([4], Lemma 6.1)**.** *For $D>0$, we have $\mathrm{vol}_\infty(\chi_D,1-k/2)=\dfrac{\mathrm{vol}_\infty(1-k/2)}{\sqrt{D}}$. Here $\mathrm{vol}_\infty(1-k/2)$ denotes the transcendental part of the L-value $L(f,\mathbf{1},k/2)$ for a trivial character $\mathbf{1}$.*

Suppose we take two positive quadratic discriminants D,D'. Using Lemma 6.1 and taking a quotient of (15) for D and D', we have

$$v_p\left(\frac{\sqrt{D}}{\sqrt{D'}}\cdot\frac{L(f,\chi_D,k/2)}{L(f,\chi_{D'},k/2)}\right)=v_p\left(\frac{\#\text{Ш}_p^{BK}(\mathbb{Q},A_{f,D})}{\#\text{Ш}_p^{BK}(\mathbb{Q},A_{f,D'})}\right). \tag{16}$$

On the other hand, the twisted L-value $L(f,\chi_D,k/2)$ is studied by Kohnen and Zagier in [12] in terms of Shimura's theory of modular forms of half integral weight. Shimura's theory gives a correspondence between modular forms of half integral weight and modular forms of even integral weight. Let $S_k(\mathrm{SL}_2(\mathbb{Z}))$ be the space of cusp forms of even weight k on the full modular group $\mathrm{SL}_2(\mathbb{Z})$ and $S_{\frac{k+1}{2}}(\Gamma_0(4))$ the space of cusp forms of weight $\frac{k+1}{2}$ on the congruence subgroup $\Gamma_0(4)$. In [11], Kohnen defined a certain subspace $S^+_{\frac{k+1}{2}}(\Gamma_0(4))$ of $S_{\frac{k+1}{2}}(\Gamma_0(4))$ and showed Shimura's correspondence induces an isomorphism $\kappa : S^+_{\frac{k+1}{2}}(\Gamma_0(4)) \xrightarrow{\sim} S_k(\mathrm{SL}_2(\mathbb{Z}))$. In [12], Kohnen and Zagier gave a formula of the value $L(f,\chi_D,k/2)$ for $f\in S_k(\mathrm{SL}_2(\mathbb{Z}))$ in terms of the $|D|$-th Fourier coefficient of $\kappa^{-1}(f)$.

Theorem (Kohnen-Zagier)**.** *Let $f\in S_k(\mathrm{SL}_2(\mathbb{Z}))$ be a normalized Hecke eigenform, $g:=\kappa^{-1}(f)=\sum_{n=1}^\infty c_nq^n\in S^+_{\frac{k+1}{2}}(\Gamma_0(4))$ the inverse image of f under the Kohnen's* *isomorphism κ. Let D be a quadratic discriminant with $(-1)^{k/2}D > 0$. Then*

$$\frac{c_{|D|}^2}{\langle g, g\rangle} = \frac{(k/2-1)!}{\pi^{k/2}}|D|^{(k-1)/2}\frac{L(f,D,k/2)}{\langle f, f\rangle},$$

where $\langle \cdot, \cdot \rangle$ denotes the Petersson inner product.

Now we put $f = \Delta(z) := \sum_{n=1}^{\infty} \tau_n q^n$ $(q = e^{2\pi i z})$, Ramanujan's cusp form of weight $k = 12$ and level $N = 1$. Using the theorem of Kohnen and Zagier for $f = \Delta(z), k = 12$ and the quadratic discriminants D, D' we take before, we have

$$\frac{\sqrt{D}}{\sqrt{D'}} \cdot \frac{L(\Delta, \chi_D, 6)}{L(\Delta, \chi_{D'}, 6)} = \frac{c_D^2}{c_{D'}^2} \cdot \left(\frac{D'}{D}\right)^5,$$

where $c_D, c_{D'}$ are the D and D'-th Fourier coefficients of $\kappa^{-1}(\Delta(z))$ respectively. From (16) we obtain an equality of p-adic valuations

$$v_p\left(\frac{\#\text{Ш}_p^{BK}(\mathbb{Q}, A_{f,D})}{\#\text{Ш}_p^{BK}(\mathbb{Q}, A_{f,D'})}\right) = v_p\left(\frac{c_D^2}{c_{D'}^2} \cdot \left(\frac{D'}{D}\right)^5\right). \tag{17}$$

The main example in [12] provides a formula

$$\kappa^{-1}(\Delta(z)) = \frac{60}{2\pi i}\left(2G_4(4z)\theta'(z) - G_4'(4z)\theta(z)\right),$$

where $G_4(z) := \frac{1}{240} + \sum_{n=1}^{\infty} \sigma_3(n) q^n$ $(\sigma_3(n) = \sum_{d|n} d^3)$ and $\theta(z) := 1 + 2\sum_{n=1}^{\infty} q^{n^2}$. Thus we can compute the coefficients of $\kappa^{-1}(\Delta(z))$ explicitly and hence the right-hand side of (17).

6.2. **Mod p representations attached to elliptic curves with bad reduction at p.** We set $p = 11$. This is an ordinary prime of $\Delta(z)$. We consider quadratic discriminants which are proper multiples of 11 since we assume no conditions in (2) in Theorem 1.1 for these cases. From the formula

$$\kappa^{-1}(\Delta(z)) = \frac{60}{2\pi i}\left(2G_4(4z)\theta'(z) - G_4'(4z)\theta(z)\right),$$

we compute the $11i$-th Fourier coefficient of $\kappa^{-1}(\Delta(z)) = \sum_{n=1}^{\infty} c_n q^n$ for $2 \leqslant i \leqslant 7$ as follows:

i	$11i$	c_{11i}
2	22	0
3	33	$-6480 = -2^4 \cdot 3^4 \cdot 5$
4	44	$-43680 = -2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 13$
5	55	0
6	66	0

Continued on next page

Table 1 – *Continued from previous page*

i	$11i$	c_{11i}
7	77	$110880 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$

We take $11 \times 7 = 77$-th and $11 \times 3 = 33$-th Fourier coefficients of $\kappa^{-1}(\Delta(z))$. We have $33, 77 \equiv 1 \pmod 4$, so they are both quadratic discriminants. We set $D = 77$, $D' = 33$. From (17) for $D = 77, D' = 33, p = 11$, we have

$$v_{11}\left(\frac{\#\text{Ш}_{11}^{BK}(\mathbb{Q}, A_{\Delta,77})}{\#\text{Ш}_{11}^{BK}(\mathbb{Q}, A_{\Delta,33})}\right) = v_{11}\left(\frac{c_{77}^2}{c_{33}^2} \cdot \left(\frac{3}{7}\right)^5\right).$$

We know $11 \mid c_{77}$ and $11 \nmid c_{33}$ from the above table. Thus we have $11 \mid \#\text{Ш}_{11}^{BK}(\mathbb{Q}, A_{\Delta,77})$ which implies $\mathrm{rk}_{\mathbb{F}_{11}}(\text{Ш}_{11}^{BK}(\mathbb{Q}, A_{\Delta,77})[11]) \geqslant 2$. Now we check that $p = 11, f = \Delta, k = 12, D = 77, D' = 33$ satisfies the assumptions of Theorem 1.1. Since we assume $N = 1$, there is nothing to check for the conditions (1), (4) in Theorem 1.1. It is known that the image of the representation $\overline{\rho}_\Delta^0 : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ contains $\mathrm{SL}_2(\mathbb{F}_p)$ except for the cases $p = 2, 3, 5, 7, 23$ and 691. Thus the assumption (3) is now satisfied. Since our quadratic discriminants $D = 77, D' = 33$ are proper multiples of 11, we are not in the situations described in Proposition 5.11, and this is the assumption (2). Thus we can apply our Theorem 1.1 in this situation and see that the $\mathbb{F}_{11}$-representation $\mathrm{Cl}_{K_{\Delta,77}} \otimes \mathbb{F}_{11}$ has $M_{\Delta,77}$ as its quotient representation.

We note that this $\mathbb{F}_{11}$-representation $M_{\Delta,77}$ of $G_{\mathbb{Q}}$ comes from an elliptic curve over $\mathbb{Q}$. Let E be the modular curve $X_0(11)$ and $f_E = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(11))$ the corresponding cusp form. For $\Delta(z) = \sum_{n=1}^{\infty} \tau_n q^n$ and f_E, we have a congruence of coefficients $\tau_n \equiv a_n \pmod{11}$ which induces an isomorphism between $\mathbb{F}_{11}$ representations M_Δ^0 and $E[11]$. Thus we have an isomorphism $M_{\Delta,77} \cong E_{77}[11] \otimes \omega_{\mathrm{cyc}}^5$ as $G_{\mathbb{Q}}$-modules where E_{77} denotes the quadratic twist of E by 77, and $M_{\Delta,77}$ comes from an elliptic curve. However, we can not treat $M_{\Delta,77}$ by the theorem of Prasad and Shekhar or its generalization in [3] since E_{77} is bad at 11 and their theorem and ours in [3] can be used for only good primes.

6.3. **Mod p representations attached to modular forms.** In the second example, we put $p = 67$. This is also an ordinary prime of $\Delta(z)$ as the first example and we consider quadratic discriminants which are proper multiples of 67. For $i \in \mathbb{Z}$, $2 \leqslant i \leqslant 43$, the $67i$-th Fourier coefficient of $\kappa^{-1}(\Delta(z)) = \sum_{n=1}^{\infty} c_n q^n$ is computed as follows:

i	$67i$	c_{67i}
2	134	0
3	201	$-2686320 = -2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 41$
4	268	$-4016160 = -2^5 \cdot 3^2 \cdot 5 \cdot 2789$
5	335	0
6	402	0
7	469	$-32215680 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 \cdot 47$
8	536	$24612000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7 \cdot 293$
9	603	0
10	670	0
11	737	$52764720 = 2^4 \cdot 3 \cdot 5 \cdot 109 \cdot 2017$
12	804	$150433920 = 2^7 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13 \cdot 41$
13	871	0
14	938	0
15	1005	$380298240 = 2^{10} \cdot 3^4 \cdot 5 \cdot 7 \cdot 131$
16	1072	$96387840 = 2^8 \cdot 3^3 \cdot 5 \cdot 2789$
17	1139	0
18	1206	0
19	1273	$293666160 = 2^4 \cdot 3 \cdot 5 \cdot 17 \cdot 167 \cdot 431$
20	1340	$-197892480 = -2^7 \cdot 3 \cdot 5 \cdot 103069$
21	1407	0
22	1474	0
23	1541	$1340143920 = 2^4 \cdot 3^3 \cdot 5 \cdot 620437$
24	1608	$122186880 = 2^7 \cdot 3^4 \cdot 5 \cdot 2357$
25	1675	0
26	1742	0
27	1809	$-67695264 = -2^5 \cdot 3^4 \cdot 7^2 \cdot 13 \cdot 41$
28	1876	$-257725440 = -2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 \cdot 47$
29	1943	0
30	2010	0
31	2077	$-1106652480 = -2^6 \cdot 3 \cdot 5 \cdot 1152763$
32	2144	$-590688000 = -2^8 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 293$
33	2211	0
34	2278	0
35	2345	$-743484000 = -2^5 \cdot 3 \cdot 5^3 \cdot 7 \cdot 53 \cdot 167$
36	2412	$-36145440 = -2^5 \cdot 3^4 \cdot 5 \cdot 2789$
37	2479	0

Continued on next page

Table 2 – *Continued from previous page*

i	$67i$	c_{67i}
38	2546	0
39	2613	$-981246240 = -2^5 \cdot 3^2 \cdot 5 \cdot 13 \cdot 23 \cdot 43 \cdot 53$
40	2680	$3359129280 = 2^6 \cdot 3 \cdot 5 \cdot 13 \cdot 17 \cdot 71 \cdot 223$
41	2747	0
42	2814	0
43	2881	$-2622438960 = -2^4 \cdot 3 \cdot 5 \cdot 67 \cdot 71 \cdot 2297$

We take $67 \times 3 = 201$-th and $67 \times 43 = 2881$-th Fourier coefficients of $\kappa^{-1}(\Delta(z))$. Since $201, 2881 \equiv 1 \pmod 4$, they are both quadratic discriminants. We set $D = 2881, D' = 201$. Then from (17) for $D = 2881, D' = 201, p = 67$, we have

$$v_{67}\left(\frac{\#\text{Ш}_{67}^{BK}(\mathbb{Q}, A_{\Delta,2881})}{\#\text{Ш}_{67}^{BK}(\mathbb{Q}, A_{\Delta,201})}\right) = v_{67}\left(\frac{c_{2881}^2}{c_{201}^2} \cdot \left(\frac{3}{43}\right)^5\right).$$

From the above table for $i = 43, 3$, we know $67 \mid c_{2881}$ and $67 \nmid c_{201}$ to get $67 \mid \#\text{Ш}_{67}^{BK}(\mathbb{Q}, A_{\Delta,2881})$. Thus $\mathrm{rk}_{\mathbb{F}_{67}}(\text{Ш}_{67}^{BK}(\mathbb{Q}, A_{\Delta,2881})[67]) \geqslant 2$. Now we check that the assumptions in Theorem 1.1 satisfied for $p = 67, f = \Delta(z), k = 12, D = 2881, D' = 201, N = 1$. As in the first example, we see that the conditions (1), (3), (4) are satisfied. The assumption (2) is also satisfied since $\Delta(z)$ is good ordinary at 67 and our quadratic discriminants 2881, 201 are proper multiples of 67. Hence we can apply our main theorem and we can see that the $\mathbb{F}_{67}$-representation $\mathrm{Cl}_{K_{\Delta,2881}} \otimes \mathbb{F}_{67}$ has $M_{\Delta,2881}$ as its quotient representation.

In this case, unlike the first example, we can show that the $\mathbb{F}_{67}$-representation $M_{\Delta,2881}$ never comes from elliptic curve over $\mathbb{Q}$. In other words, $M_{\Delta,2881}$ can not be isomorphic to $E[67] \otimes \omega_{\mathrm{cyc}}^i$ for some elliptic curve E over $\mathbb{Q}$ and $i \in \mathbb{Z}$ with $0 \leqslant i \leqslant p-2$. We prove this when $i = 0$ and the other cases can be proved similarly. Since Δ is good ordinary at 67, elements of the inertia subgroup $g \in I_{67}$ at 67 acts on $M_{\Delta,2881}$ as

$$\begin{pmatrix} \omega_{\mathrm{cyc}}^6(g) & \bar{u}(g) \\ 0 & \omega_{\mathrm{cyc}}^{-5} \end{pmatrix} \cdot \chi_{2881}(g). \tag{18}$$

Hence $M_{\Delta,2881}$ has a one dimensional subspace N_1 on which I_{67} acts via $\omega_{\mathrm{cyc}}^6 \cdot \chi_{2881}$. Suppose this representation $M_{\Delta,2881}$ comes from a group of 67-torsion points of an elliptic curve E over $\mathbb{Q}$. Suppose E has good reduction at 67. Then the representation $E[67]$ has a 1-dimensional subrepresentation when we see it as a $G_{\mathbb{Q}_{67}}$-module. So E is good ordinary at 67 and the above matrix (18) is similar to $\begin{pmatrix} \omega_{\mathrm{cyc}}(g) & \bar{v}(g) \\ 0 & 1 \end{pmatrix}$ for all

$g \in I_{67}$ where $\bar{v}(g) \in \mathbb{F}_{67}$. Then $M_{\Delta,2881}$ has a 1-dimensional subspace N_2 on which I_{67} acts via $\omega_{\rm cyc}$. Since it is known that $M_{\Delta,2881}$ does not split as a $G_{\mathbb{Q}_{67}}$-representation, we have $N_1 = N_2$ which implies $\omega_{\rm cyc}^6 \cdot \chi_{2881} = \omega_{\rm cyc} \iff \omega_{\rm cyc}^5 \cdot \chi_{2881} = 1$. However, $\omega_{\rm cyc}^5$ and χ_{2881} have orders 66 and 2 respectively and their product is never trivial. This is a contradiction. Next we suppose E has bad reduction at 67. First we assume the reduction is potentially multiplicative. Then the theory of the Tate curve says that $g \in I_{67}$ acts on $E[67]$ via $\begin{pmatrix} \omega_{\rm cyc}(g) & \bar{w}(g) \\ 0 & 1 \end{pmatrix}$, where $\bar{w}(g) \in \mathbb{F}_{67}$. Hence we get the same conclusion as in the case E is good ordinary at 67. Finally we assume that E has bad and potentially good reduction at 67. It is a well-known fact that for an elliptic curve E over $\mathbb{Q}_\ell$ which has potentially good reduction at ℓ, E acquires good reduction over a totally ramified extension of degree 4 or 6 over $\mathbb{Q}_\ell$. Let L be such an extension. Then $g \in G_{\mathbb{Q}_{67}^{\rm ur}\cdot L}$ acts on $E[67]$ via a matrix $\begin{pmatrix} \omega_{\rm cyc}(g) & \bar{x}(g) \\ 0 & 1 \end{pmatrix}$, where $\bar{x}(g) \in \mathbb{F}_{67}$. Hence this matrix and (18) are similar for all $g \in G_{\mathbb{Q}_{67}^{\rm ur}\cdot L}$ and this yields a equation $\omega_{\rm cyc}^5 \cdot \chi_{2881} = 1$ on $G_{\mathbb{Q}_{67}^{\rm ur}\cdot L}$ as in the above argument. Then, putting F as the Galois extension of $\mathbb{Q}_{67}^{\rm ur}$ cut out by the character $\omega_{\rm cyc}^5 \cdot \chi_{2881}$ of I_{67}, we have $F \subset L$. However we know $[F : \mathbb{Q}_{67}^{\rm ur}] = 66$ since $\mathbb{Q}_{67}^{\rm ur}(\zeta_{67})$ and $\mathbb{Q}_{67}^{\rm ur}(\sqrt{2881})$ are linearly disjoint over $\mathbb{Q}_{67}^{\rm ur}$. This is a contradiction and hence the representation $M_{\Delta,2881}$ never comes from an elliptic curve over $\mathbb{Q}$.

References

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

[2] K. Buzzard, T. Gee, Explicit reduction modulo p of certain two-Dimensional crystalline representations, International Mathematics Research Notices, Volume 2009, Issue 12 (2009): 2303-2317.

[3] N. Dainobu, Ideal class groups of number fields and Bloch-Kato's Tate-Shafarevich groups for symmetric powers of elliptic curves. to appear in Tokyo Journal of Mathematics. arXiv:2204.07759

[4] N. Dummigan, Congruences of modular forms and Selmer groups. Mathematical Research Letters 8 (2001): 479-494.

[5] N. Dummigan, W. Stein, M. Watkins, Constructing elements in Shafarevich-Tate groups of modular motives, Number Theory and Algebraic Geometry (2004).

[6] B. Edixhoven, The weight in Serre's conjectures on modular forms. Invent Math 109 (1992): 563-594.

[7] M. Flach, A generalisation of the Cassels-Tate pairing, J. reine angew. Math. 412 (1990): 113-127.

[8] N. Freitas, A. Kraus, On the degree of the p-torsion field of elliptic curves over $\mathbb{Q}_\ell$ for $\ell \neq p$, preprint, arXiv:1804.07627v1.

[9] R. Ghate, On the local behavior of ordinary modular Galois representations, Modular curves and abelian varieties, Progress in Mathematics vol. 224, Birkhäuser (2004): 105-124.

[10] T. Hiranouchi, Local torsion primes and the class numbers associated to an elliptic curve over $\mathbb{Q}$, Hiroshima Math. J. 49 (2019), no. 1, 117-127, DOI 10.32917/hmj/1554516039. MR3936649
[11] W. Kohnen, Modular forms of half-integral weight on $\Gamma_0(4)$. Math. Ann. 248 (1980): 249-266
[12] W. Kohnen, D. Zagier, Values of L-series of modular forms at the center of the critical strip, Invent. Math. 64 (1981): 173-198.
[13] A.Lozano-Robledo, Division fields of elliptic curves with minimal ramification, Revista Matematica Iberoamericana, vol. 31, no. 4 (2015): 1311-1332
[14] J. Nekovář, Class numbers of quadratic fields and Shimura's correspondence. Math. Ann., 287(4):577-594, (1990).
[15] J.Neukirch, A.Schmidt, K.Wingberg, Cohomology of Number Fields, Springer-Verlag (2008).
[16] 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, Cambridge University Press (2015): 154-192.
[17] T. Ohshita, Asymptotic lower bound of class numbers along a Galois representation, J. Number Theory 211 (2020), 95-112, DOI 10.1016/j.jnt.2019.09.024. MR4074549
[18] D. Prasad, A mod p Artin-Tate conjecture and generalizing the Herbrand-Ribet theorem, Pacific Journal of Mathematics, vol. 303, no.1 (2019): 299-316.
[19] D. Prasad, S. Shekhar, Relating the Tate-Shafarevich group of an elliptic curve with the class group, Pacific Journal of Mathematics, vol. 312, no.1 (2021): 203-218.
[20] K. Rubin, Euler systems, Hermann Weyl Lectures, Ann. of Math. Studies, vol. 147, Princeton Univ. Press (2000).
[21] T. Shintani, On construction of holomorphic cusp forms of half integral weight, Nagoya Math. J. 58 (1975): 83-126.
[22] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts inMathematics, 106. Springer-Verlag, New York, (1986).
[23] 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