RELATING TATE-SHAFAREVICH GROUP OF AN ELLIPTIC CURVE
WITH CLASS GROUP

DIPENDRA PRASAD AND SUDHANSHU SHEKHAR

January 1, 2020

ABSTRACT. The paper formulates a precise relationship between the Tate-Shafarevich

group $X(E)$ of an elliptic curve $E$ over $\mathbb{Q}$ with a quotient of the classgroup of

$\mathbb{Q}(E[p])$ on which $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = \text{GL}_2(\mathbb{Z}/p)$ operates by its standard 2 dimensional

representation over $\mathbb{Z}/p$. We establish such a relationship in most cases when $E$ has good

reduction at $p$.

CONTENTS

1. Introduction 1
2. Main question 3
3. Class group and Tate-Shafarevich group 5
4. The converse 9
References 12

1. INTRODUCTION

Let $E$ be an elliptic curve over $\mathbb{Q}$, $p$ an odd prime number, and $ho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_p)$ the associated Galois representation on elements of order $p$ on $E$. Assume that the image of the Galois representation is all of $\text{GL}_2(\mathbb{F}_p)$. The representation $\rho$ then gives rise to an extension $K$ of $\mathbb{Q}$ with Galois group $\text{GL}_2(\mathbb{F}_p)$. Let $\text{Cl}_K$ denote the class group of $K$. The group $\text{GL}_2(\mathbb{F}_p)$ being the Galois group of $K$ over $\mathbb{Q}$, operates on $\text{Cl}_K$, hence on the $p$-vector space $\text{Cl}_K/p\text{Cl}_K$. Write the semi-simplification of the representation of $\text{GL}_2(\mathbb{F}_p)$ on $\text{Cl}_K/p\text{Cl}_K$ as $\sum V_\alpha$, where $V_\alpha$’s are the various irreducible representations of $\text{GL}_2(\mathbb{F}_p)$ in characteristic $p$. It is a well-known fact that any irreducible representation of $\text{GL}_2(\mathbb{F}_p)$ in characteristic $p$ is of the form $V_{i,j} = \text{Sym}^i \otimes \text{det}^j$, $0 \leq i \leq p - 1$, $0 \leq j \leq p - 2$ where $\text{Sym}^i$ refers to the $i$-th symmetric power of the standard 2 dimensional representation of $\text{GL}_2(\mathbb{F}_p)$, and $\text{det}$ denotes the determinant character of $\text{GL}_2(\mathbb{F}_p)$.

It is a natural question to understand which $V_{i,j}$’s appear in $\text{Cl}_K/p\text{Cl}_K$. The aim of this note is to formulate some questions in this direction which can be viewed as a $\text{GL}_2$ analogue of the famous theorem of Herbrand-Ribet, [Ri1], and [Was] for an exposition. One is hoping for a conjectural answer along the lines of Herbrand-Ribet to say that the representation $\text{Sym}^i(\mathbb{F}_p + \mathbb{F}_p) \otimes \text{det}^j$ of $\text{GL}_2(\mathbb{F}_p)$ appears in $\text{Cl}_K/p\text{Cl}_K$ if and only if the ‘algebraic part’ of the first nonzero derivative of $L(s, \text{Sym}^i(E) \otimes \text{det}^j)$ at 0 is divisible by $p$ (in some favorable situations such as when $E$ has good reduction at $p$).
The authors have not seen any computation of the $GL_2(F_p)$ representation on $\text{Cl}_K/p\text{Cl}_K$ into a sum of irreducible pieces (after semi-simplification) where $K = \mathbb{Q}(E[p])$ is a Galois extension of $\mathbb{Q}$, say with $\text{Gal}(K/\mathbb{Q}) = GL_2(F_p)$. Presumably it is not beyond present computational powers to do such a computation say for $p = 5$; this would be very useful data to have for the problems discussed in this paper. There are examples known due to K. Rubin and A. Silverberg [RS] of families of elliptic curves with the same $\mathbb{Q}(E[5])$ with Galois group $GL_2(F_5)$. Are there elliptic curves of the same rank, say $0$, in this family, for which the 5-valuation of the algebraic part of $L(E, 1)$ as in the Birch-Swinnerton-Dyer conjecture are different? If our suggestions in this paper are correct then this should not happen!

In an unfinished manuscript of the first author [P2], a heuristic relating representations of $GL_2(F_p)$ on $H_K/pH_K$ and divisibility of certain $L$-values was given based on factorisation of the class number formula for the Dedekind zeta function $\zeta_K(s)$:

$$\zeta_K(s) = -\frac{hr}{w} s^{r_1+r_2-1} + \text{higher order terms...},$$

in terms of the complex representation theory of $GL_2(F_p)$ on the left hand side of the class number formula, and in terms of mod $p$ representation theory on the right hand side of the class number formula involving $H_K/pH_K$. We will not detail the heuristic considerations made in [P2] except to say a few words on congruences of automorphic representations and of their $L$-values.

We first fix some notation. We will fix an isomorphism of $\mathbb{Q}_p$ with $\mathbb{C}$ where $\mathbb{Q}_p$ is a fixed algebraic closure of $\mathbb{Q}_p$, the field of $p$-adic numbers. This allows one to define $p$, a prime ideal in $\mathbb{Z}$, the integral closure of $\mathbb{Z}$ in $\mathbb{C}$, over the prime ideal generated by $p$ in $\mathbb{Z}$.

One defines congruence modulo a prime $p$ in $\mathbb{Q}$, of automorphic representations of $G(\mathbb{A})$ for $G$ a reductive algebraic group over $\mathbb{Q}$ most simply through congruence of Hecke eigenvalues (i.e., of the algebra $\mathcal{H}(G(\mathbb{Z}_p)\backslash G(\mathbb{Q}_p)/G(\mathbb{Z}_p), \mathbb{Z})$) at places of $\mathbb{Q}$ where $G$ is unramified, i.e., is quasi-split and splits over an unramified extension; for the notion of congruences of automorphic representations, it is best to demand congruence of Hecke eigenvalues only at almost all places of $\mathbb{Q}$ where $G$ is unramified, omitting an unspecified finite set of places of $\mathbb{Q}$ including those where the group is ramified. (To be able to talk of congruences presupposes algebraicity of Hecke eigenvalues.) Observe that transferring representations on a group $G_1(\mathbb{A})$ to $G_2(\mathbb{A})$ via a map of the $L$-groups $^LG_1(\mathbb{C}) \rightarrow ^LG_2(\mathbb{C})$ which carries congruent automorphic representations of $G_1(\mathbb{A})$ to congruent automorphic representations of $G_2(\mathbb{A})$, allows one to talk of congruences of automorphic representations on two very different groups by embedding their $L$-groups in a (suitable) common $L$-group!

For $GL_2(F)$, where $F$ is a totally real number field, congruences for holomorphic elliptic modular forms are usually defined using Fourier expansions. For the symplectic similitude group $GSp_{2n}(F)$, and the symplectic group $Sp_{2n}(F)$, $F$ a totally real number field, there is still the notion of Fourier expansion, and one can hope that at least for these groups, algebraicity (resp. $p$-integrality) of Hecke eigenvalues is equivalent to algebraicity (resp. $p$-integrality) of Fourier coefficients (up to a scaling) of an appropriate ‘newform’, and that further, congruences too can be read off from Fourier expansion. The recent work of Furusawa and Morimoto [FM] building on earlier work of Dickson, Pitale, Saha and Schmidt on ‘Böcherer conjecture’ for $GSp_{4}(\mathbb{A}_Q)$ relating Fourier coefficients...
to central $L$-values (which themselves are supposed to have rationality and congruence properties) lends support to such an expectation, although many others have advocated a contrary expectation, see for example, end of page 251 of [Ha]. Modular forms of half integral weight for $GL_2(F)$, where $F$ is a totally real number field, have very similar general features in that their Fourier coefficients too are related to central $L$-values (by the work of Waldspurger), presumably rationality and integrality up to a scalar are the same as that of the Hecke-operators.

If there was a ($p$-adic) Galois representation associated to the automorphic representations under consideration, one could call two automorphic representations congruent if the associated Galois representations with values in $GL_n(\mathbb{Q}_p)$ were isomorphic modulo $p$ (after semi-simplification).

We next briefly talk about $L$-values. According to the conjectures of Bloch and Kato [BK], the highest nonzero derivative of a motivic $L$-function at any integral point can be written canonically as a product of an algebraic part, and a transcendental part, allowing one to talk of primes of $\mathbb{Q}$ dividing an $L$-value, which would be a short form for talking of primes of $\mathbb{Q}$ dividing the algebraic part of the (highest nonzero derivatives of) the $L$-function at an integer. We recall, as is standard in the subject, that when speaking of $L$-functions of automorphic representations which are congruent modulo $p$, the Euler factors above $p$ are to be removed. In some cases, we could be lucky to be dealing with an $L$-value which is itself algebraic. This is for instance the case for Herbrand-Ribet’s theorem [Ri1], and [P] for a more general context involving $L$-values of finite Artin representations cutting out CM number fields. (Perhaps, highest nonzero derivative of an irreducible $L$-function at an integer point is never algebraic unless one is dealing with these CM Artin representations!) In this paper, we will be comparing an Artin $L$-function with one of an Elliptic curve which by the Birch-Swinnerton-Dyer conjecture has a well-formulated algebraic part $L(1,E)^{\text{alg}}$.

The questions formulated in [P2] are predicated on the following, general but somewhat vague principle, which seems to lie at the basis of being able to define $p$-adic $L$-functions: if two automorphic representations are congruent modulo $p$, then the algebraic parts of their $L_S$-values (where $L_S$ denotes partial $L$-function, removing Euler factors at $S$ which is any finite set of places of $\mathbb{Q}$ containing $p, \infty$ and any prime where either of the two representations is ramified) at any integral point are both $p$-integral, or neither are $p$-integral, and if $p$-integral, they are congruent modulo $p$.

2. MAIN QUESTION

The following question from [P2] is at the basis of this paper.

**Question 2.1.** Let $E$ be an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q}) = 0$. Let $K = \mathbb{Q}(E[p])$ be the Galois extension of $\mathbb{Q}$ obtained by attaching elements of order $p$ on $E$ where $p$ is an odd prime. We assume that $\text{Gal}(K/\mathbb{Q}) = GL_2(\mathbb{F}_p)$, and also that $p$ is coprime to $c_\ell = [E(\mathbb{Q}_\ell) : E(\mathbb{Q}_\ell)^0]$, the so-called Tamagawa factors, for all finite primes $\ell$. Let $\text{Cl}_K$ denote the class group of $K$ which comes equipped with a natural action of $\text{Gal}(K/\mathbb{Q}) = GL_2(\mathbb{F}_p)$. Then if $p\nmid \#(E(\mathbb{Q}))$, is it true that the $GL_2(\mathbb{F}_p)$ representation $\text{Cl}_K/p\text{Cl}_K$ contains the standard 2-dimensional representation of $GL_2(\mathbb{F}_p)$ as a quotient? What about the converse?
There are two natural approaches to attack this question: one which is what we will discuss in greater detail from next section, using Selmer groups, and the machinery of Galois cohomology available to deal with it. The other approach, as in the pioneering work of Ribet [Ri1] is by looking at the congruence of cusp forms with an Eisenstein series. The method of Ribet has two basic steps:

1. finding cusp forms on $\text{GL}_2(\mathbb{A}_\mathbb{Q})$ which are congruent to a given Eisenstein series if the constant term of the Eisenstein series is zero mod $p$,
2. proving that the associated mod $p$ representation of the cusp form serves the purpose of constructing everywhere unramified extension of $\mathbb{Q}(\mu_p)$ of the desired kind.

Neither of the two steps is understood for $\text{GSp}(4)$ (perhaps not even for $\text{GL}_2(\mathbb{A}_\mathbb{Q})$ in some generality?), except that there is a recent work due to Bergström and Dummigan, [BD] where they formulate some general questions along these lines. Note that there are two conjugacy classes of maximal parabolic subgroups in $\text{GSp}(4)$ and both could be sources of such congruences, and therefore could have applications to Galois representations. We make very brief comment on what the method of Ribet will give if the two steps above were accomplished.

We first take up the case when the Eisenstein series is one on Klingen parabolic associated to a cusp form (on the Levi subgroup of the Klingen parabolic) so that the associated Galois representation lands inside the dual parabolic which is the Siegel parabolic. In this case, a congruence between Eisenstein series and a cusp form will be a source of $\text{Sym}^2(\mathbb{F}_p + \mathbb{F}_p) \otimes \text{det}^j$ appearing in $\text{Cl}_K/p\text{Cl}_K$.

Next we consider an Eisenstein series supported on a Siegel parabolic (so that the associated Galois representation lands inside the Levi of the Klingen parabolic). The Klingen parabolic $P$ in $\text{GSp}(4)$ looks like

$$1 \to N \to P \to \text{GL}(2) \times \mathbb{G}_m \to 1,$$

with $N$ a non-abelian unipotent group of dimension 3 which is the 3-dimensional Heisenberg group, and thus has a centre of dimension 1. Dividing $N$ by the center one gets 2 dimensional representation of $\text{GL}(2)$ which thus seems ideally suited to give rise to extensions of $K$ on which the Galois group of $K$, i.e., $\text{GL}_2(\mathbb{F}_p)$, operates by a twist of the 2 dimensional standard representation.

The specific question thus is that if $p$ divides (the algebraic part of) $L(1, \pi \otimes \omega^j)$, there is a cusp form on $\text{GSp}(4)$ which is congruent to an Eisenstein series.

For a specific example of such a congruence, see the paper of Harder [Ha] where for the unique elliptic modular form $f$ for $\text{SL}_2(\mathbb{Z})$ of weight 22, he conjectured existence (which was later confirmed) of certain cuspidal eigenform on $\text{GSp}(4, \mathbb{A}_\mathbb{Q})$ with the following congruence for Hecke eigenvalues, which we just write down from his paper without further explanations:

$$\lambda(p) \equiv p^8 + a_f(p) + p^{13} \mod 41,$$

for all primes $p$, except to note that $\frac{\Lambda(f, 14)}{\Omega_f}$ is an integer, and the crucial reason for the prime 41 is:

$$41 | \frac{\Lambda(f, 14)}{\Omega_f}.$$
In the context of Harder’s example, an optimistic hope will be that the mod 41 Galois representation associated to the eigenform $f$ of weight 22 for $\text{SL}_2(\mathbb{Z})$ cuts out a $\text{GL}_2(\mathbb{F}_{41})$ extension $K_f$ of $\mathbb{Q}$ which has an unramified abelian extension on which $\text{GL}_2(\mathbb{F}_{41})$ acts by $\text{Sym}^1 \otimes \det^{-8}$ (or, is it $\text{Sym}^1 \otimes \det^{-13/2}$).

3. Class Group and Tate-Shafarevich Group

Rest of this paper deals exclusively with constructing the standard 2-dimensional representation of $\text{GL}_2(\mathbb{F}_p)$ on the class group $\text{Cl}_K/p\text{Cl}_K$ using Selmer group of $E$, an elliptic curve defined over $\mathbb{Q}$.

Let $\text{Sel}_p(E/\mathbb{Q})$ be the $p$-Selmer group of $E$ over $\mathbb{Q}$ defined by the exact sequence

$$0 \rightarrow \text{Sel}_p(E/\mathbb{Q}) \rightarrow H^1(\mathbb{Q}, E[p]) \rightarrow \prod_v H^1(\mathbb{Q}_v, E(\overline{\mathbb{Q}_v})), \tag{3.2}$$

where $v$ varies over primes of $\mathbb{Q}$. Since the restriction map $H^1(\mathbb{Q}, E[p]) \rightarrow H^1(\mathbb{Q}_v, E(\overline{\mathbb{Q}_v}))$ factors through $H^1(\mathbb{Q}, E[p]) \rightarrow H^1(\mathbb{Q}_v, E[p])$, we also have the following exact sequence

$$0 \rightarrow \text{Sel}_p(E/\mathbb{Q}) \rightarrow H^1(\mathbb{Q}, E[p]) \rightarrow \prod_v H^1(\mathbb{Q}_v, E[p])/\text{Im}(\kappa_v),$$

where

$$\kappa_v : E(\mathbb{Q}_v)/pE(\mathbb{Q}_v) \rightarrow H^1(\mathbb{Q}_v, E[p])$$

is associated to the multiplication by $p$ map (called the Kummer map of $E$) on the Galois cohomology groups

$$0 \rightarrow E[p] \rightarrow E \rightarrow E/p \rightarrow 0.$$

Let

$$\kappa_v^{ur} : E(\mathbb{Q}_v^{ur})/pE(\mathbb{Q}_v^{ur}) \rightarrow H^1(\mathbb{Q}_v^{ur}, E[p])$$

be the Kummer map of $E$ over the maximal unramified extension $\mathbb{Q}_v^{ur}$ of $\mathbb{Q}_v$.

For every prime $v$ of $\mathbb{Q}$, we get restriction maps

$$\text{Sel}_p(E/\mathbb{Q}) \xrightarrow{\text{res}_v} \text{Im}(\kappa_v)$$

and

$$\text{Sel}_p(E/\mathbb{Q}) \xrightarrow{\text{res}_v^{ur}} \text{Im}(\kappa_v^{ur}).$$

For every prime $v \neq p$ of $\mathbb{Q}$, let $c_v(E)$ denote the Tamagawa number of $E$ over $\mathbb{Q}$. Under the assumption that $c_v$ is $p$-adic unit for every $v \neq p$, we shall show that $\text{res}_v^{ur}$ is the zero map. In particular, this implies that elements of $\text{Sel}_p(E/\mathbb{Q})$ are unramified outside $p$. Further, if $\mathbb{Z}/p\mathbb{Z}$-rank of $\text{Sel}_p(E/\mathbb{Q})$ is at least two then we shall show that the kernel of $\text{res}_v^{ur}$ is non-trivial. Thus we get elements in $\text{Sel}_p(E/\mathbb{Q})$ which is unramified everywhere allowing us to construct quotients of $\text{Cl}_K/p\text{Cl}_K$ isomorphic to $E[p]$ as $\text{Gal}(K/\mathbb{Q}) = \text{GL}_2(\mathbb{Z}/p)$-modules.

Suppose that $E$ has good ordinary reduction at $p$. Then $\tilde{E}_p[p]$ is a rank one $\mathbb{F}_p$-vector space, and is the maximal unramified quotient of $E[p]$ considered as a $G_p = \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-module. Put, $a_p(E) := p + 1 - \tilde{E}_p(\mathbb{F}_p)$. Since, $E$ has good ordinary reduction at $p$, $a_p(E)$ is $p$-adic unit and therefore the polynomial $X^2 - a_p(E)X + p$ has a unique $p$-adic unit root. Let $\alpha_p$ be such a root. Then, we have $a_p(E) \equiv \alpha_p \mod p$. The Frobenius at $p$ acts on $\tilde{E}_p[p]$ via multiplication by $\alpha_p \equiv a_p(E) \mod p$. Let $C_p$ be the kernel of the natural
quotient map $E[p] \rightarrow \tilde{E}_p[p]$. Then, $G_p$ acts on $C_p$ via the character $\omega_p\psi^{-1}$ where $\omega_p$ is the Teichmuller character at $p$.

Put $K = \mathbb{Q}(E[p])$. Let

$$\tilde{\rho} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_p)$$

be the Galois representation given by the action of $\text{Gal}(K/\mathbb{Q})$ on $E[p]$. If $E$ has good ordinary reduction at $p$, the restriction of $\tilde{\rho}$ to $G_p$ is equivalent to the form

$$(3.1) \left( \begin{array}{cc} \omega_p\psi^{-1} & \ast \\ 0 & \psi \end{array} \right).$$

Now suppose that $E[p]$ is an irreducible $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. We shall need the following well-known lemma whose proof shall be omitted.

**Lemma 3.2.** Let $G$ be a group operating on a vector space $V$ over a field $F$. If $G$ has a central element which acts on $V$ by multiplication by an element of $F$ not equal to 1, then $H^i(G, V) = 0$ for all $i \geq 0$.

As a consequence of the above Lemma we have the following (see [LW]).

**Lemma 3.3.** Let $G$ be a finite subgroup of $\text{GL}_2(\mathbb{F}_p)$ operating irreducibly on $E[p] = \mathbb{F}_p + F_p$, then $H^i(G, E[p]) = 0$ for all $i$.

**Proof.** First suppose that $p \nmid |G|$. Then $H^i(G, E[p]) = 0$ for all $i$ as $|G|$ annihilates $H^i(G, E[p])$. Now suppose that $G$ contains a non-trivial $p$-Sylow subgroup. If a $p$-Sylow subgroup of $G$ is normal in $G$, then, up to conjugacy, $G$ is contained in the group of upper triangular matrices. In particular, the action of $G$ on $E[p]$ is reducible, contrary to our assumption. Therefore a $p$-Sylow subgroup cannot be normal in $G$, so there are at least 2 distinct $p$-Sylow subgroups in $G$ which can be assumed to be the group of upper and lower triangular unipotent matrices in $\text{SL}_2(\mathbb{F}_p)$. Since $\text{SL}_2(\mathbb{F}_p)$ is generated by the group of upper and lower triangular unipotent matrices we get that $\text{SL}_2(\mathbb{F}_p)$ is contained in $G$. In particular, $-I$ is also contained in $G$. Therefore the action of $Z(G)$ on $E[p]$ is non-trivial. Lemma 3.2 therefore proves this lemma.

As a consequence of Lemma 1 if $E[p]$ is an irreducible representation of $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$, the restriction map

$$H^1(\mathbb{Q}, E[p]) \xrightarrow{\text{res}} H^1(K, E[p])$$

is injective. Let $f \in H^1(\mathbb{Q}, E[p])$ be a non-trivial element. Then $\text{res}_K(f) : \text{Gal}(\overline{\mathbb{K}}/K) \rightarrow E[p]$ is a non-trivial homomorphism. Let $K_f$ be the field defined by the kernel of $\text{res}_K(f)$.

**Theorem 3.1.** Suppose that the following holds:

(a) $E$ has good reduction at $p$.
(b) If $E$ has ordinary reduction at $p$, $a_p(E) = 1 \mod p$ and $E$ has no CM then $\tilde{\rho}$ is wildly ramified at $p$.
(c) $c_v(E)$ is a $p$-adic unit for every finite prime $v \neq p$.
(d) $E[p]$ is an irreducible $\text{Gal}(\mathbb{Q}/\mathbb{Q})$-module.

Then, \( \text{rank}_{\mathbb{F}_p}(\text{Ker}(\text{res}_p^{ur})) \geq \text{rank}_{\mathbb{F}_p}(\text{Sel}_p(E/\mathbb{Q}))-1 \). Furthermore, $\text{res}_K$ induces an injective homomorphism

$$\text{res}_K : \text{Ker}(\text{res}_p^{ur}) \rightarrow \text{Hom}_{\text{Gal}(K/\mathbb{Q})}(\text{Cl}_K, E[p]) \subset H^1(K, E[p]).$$
Proof. Let \( f \in \text{Sel}_p(E/\mathbb{Q}) \). First we shall show that \( f \) is unramified outside \( p \). Let \( v \neq p \) be a finite prime of \( \mathbb{Q} \). Consider the commutative diagram

\[
\begin{array}{ccc}
0 & \rightarrow & \mathbb{E}(\mathbb{Q}_v)/p\mathbb{E}(\mathbb{Q}_v) \\
\downarrow \lambda & & \downarrow \mu \\
0 & \rightarrow & \mathbb{E}(\mathbb{Q}^\text{ur}_v)/p\mathbb{E}(\mathbb{Q}^\text{ur}_v)
\end{array}
\]

To show that \( f \) is unramified at \( v \) it is enough to show that \( f \) is \( p \)-divisible in \( \mathbb{E}(\mathbb{Q}_v^\text{ur}) \). This follows from the assumption that \( v \) is coprime to \( p \) and \( c_v(E) \) is an \( p \)-adic unit; see for example, [BLR, Lemma 2] and [AS, Lemma 3.4, Lemma 3.6]. (Basically, this result follows from the fact that \( \mathbb{E}(\mathbb{Q}_v^\text{ur}) \) can be treated as an extension of \( \mathbb{Z}^\text{ur}_v \) by one of the groups \( \mathbb{G}_a(\mathbb{F}_v), \mathbb{G}_m(\mathbb{F}_v), \mathbb{E}(\mathbb{F}_v) \) depending on the reduction of \( E \) mod \( v \), and a finite group of order \( c_v(E) \). Observe too, that this crucial fact \( \mathbb{E}(\mathbb{Q}_v^\text{ur})/p\mathbb{E}(\mathbb{Q}_v^\text{ur}) = 0 \) say at places of good reduction uses projectivity of the group variety \( E \), and in particular, it does not hold for \( \mathbb{G}_m \).)

If \( v \) is an infinite place then since \( p \) is odd we again get that \( f \) is unramified.

If \( f \in \text{Ker}(\text{res}_{\mathbb{Q}^\text{ur}}^p) \), then \( f \) is unramified at \( p \) and therefore it is unramified at all primes of \( \mathbb{Q} \). In this case, \( \text{res}_K(f) \) is a \( \text{Gal}(\bar{K}/\mathbb{Q}) \)-equivariant homomorphism from \( \text{Gal}(\bar{K}/\mathbb{Q}) \rightarrow \mathbb{E}[p] \) which is unramified at all prime of \( K \) and which by Corollary 3.3 induces an injective homomorphism from

\[
\text{Ker}(\text{res}_{\mathbb{Q}^\text{ur}}^p) \rightarrow \text{Hom}_{\text{Gal}(\bar{K}/\mathbb{Q})}(\text{Cl}_K, E[p]).
\]

Next we show that \( \text{Im}(\text{res}_{\mathbb{Q}^\text{ur}}^p) \) has \( \mathbb{F}_p \)-rank at most 1, and hence \( \text{rank}_{\mathbb{F}_p}(\text{Ker}(\text{res}_{\mathbb{Q}^\text{ur}}^p)) \geq \text{rank}_{\mathbb{F}_p}(\text{Sel}_p(E/\mathbb{Q})) - 1 \) which will prove the theorem.

From the structure theory of rational points of an elliptic curve over a local field, we have that \( E(\mathbb{Q}_p) = \mathbb{Z}_p \oplus \bar{E}(\mathbb{Q}_p)(\text{torsion}) \). If \( a_p(E) \neq 1 \) mod \( p \) or \( \rho \) is wildly ramified then we shall show that \( E(\mathbb{Q}_p)[p] = 0 \). This implies that \( \text{Im}(\kappa_p) \) has has \( \mathbb{F}_p \)-rank 1. Since \( \text{Im}(\text{res}_p) \subset \text{Im}(\kappa_p) \) and \( \text{res}_{\mathbb{Q}^\text{ur}}^p \) factors through \( \text{res}_p \), proving that the \( \text{Im}(\text{res}_{\mathbb{Q}^\text{ur}}^p) \) has \( \mathbb{F}_p \) rank at most 1.

First we consider the case when \( E \) has good ordinary reduction at \( p \) and \( a_p(E) \neq 1 \) mod \( p \). From the assumption that \( a_p(E) \neq 1 \) mod \( p \), we have \( H^0(\mathbb{Q}_p, \tilde{E}_p[p]) = 0 \). On the other hand since \( \omega_p \) is ramified at \( p \) and \( \psi \) is unramified, \( G_p \) acts on \( C_p \) non-trivially. Thus \( H^0(\mathbb{Q}_p, C_p) = 0 \). This shows that \( H^0(\mathbb{Q}_p, E[p]) = E(\mathbb{Q}_p)[p] = 0 \). If \( \star \) in equation (1) above is non-trivial, then since \( \omega_p \) is non-trivial, we again see that \( H^0(\mathbb{Q}_p, E[p]) = E(\mathbb{Q}_p)[p] = 0 \).

In the supersingular case, it is well-known that \( E(\mathbb{Q}_p)[p] = 0 \) (see for example, [E], [K, Proposition 8.7]). This again implies that \( \text{rank}_{\mathbb{F}_p}(\text{Im}\kappa_p^\text{ur}) = 1 \).

Finally we consider the case when \( E \) has CM and \( a_p(E) = 1 \) mod \( p \). This implies that in representation \( (3.1) \), \( \psi \) is the trivial character. For elliptic curves with CM we donot need to assume that \( p \) is wildly ramified, even if \( a_p(E) = 1 \) mod \( p \) in which case we have \( H^0(\mathbb{Q}_p, \bar{E}_p[p^\infty]) \cong \mathbb{Z}/p\mathbb{Z} \).

Since \( E \) has good ordinary reduction at \( p \), we have an exact sequence of \( G_p \)-modules (see [Gr, Section 2]),

\[
0 \rightarrow E^+[p^\infty] \rightarrow E[p^\infty] \rightarrow \tilde{E}_p[p^\infty] \rightarrow 0.
\]
Both groups, $\hat{E}_p[p^\infty]$ and $E^+[p^\infty]$ are isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. The $G_p$-module $\hat{E}_p[p^\infty]$ is unramified and the inertia group $I_p$ at $p$ acts on $E^+[p^\infty]$ via the $p$-th cyclotomic character $\chi_p$. Further, since $E$ has CM, the corresponding dual exact sequence is split exact sequence when tensored with $\mathbb{Q}$, from which we deduce that $H^0(\mathbb{Q}^{ur}_p, E[p^\infty]) \cong \mathbb{Q}_p/\mathbb{Z}_p \subset H^0(\mathbb{Q}^{ur}_p, E[p^\infty])$. From the structure theorem of submodules of $\mathbb{Q}_p/\mathbb{Z}_p + \mathbb{Q}_p/\mathbb{Z}_p$ and using the fact that $\mathbb{Z}_p/\mathbb{Z}_p \oplus \mathbb{Z}_p/\mathbb{Z}_p$ cannot be contained in $H^0(\mathbb{Q}^{ur}_p, E[p^\infty])$, it follows that $H^0(\mathbb{Q}^{ur}_p, E[p^\infty]) \cong \mathbb{Q}_p/\mathbb{Z}_p$. Therefore, a non-zero element in $H^0(\mathbb{Q}^{ur}_p, E[p^\infty]) \cong \mathbb{Z}_p/\mathbb{Z}_p$ is not $p$-divisible, but it is $p$-divisible in $H^0(\mathbb{Q}^{ur}_p, E[p^\infty])$. Thus we get an element in $E(\mathbb{Q}_p)$ which is non $p$-divisible, but $p$-divisible in $E(\mathbb{Q}_p^{ur})$. In particular, the natural map

$$\phi : E(\mathbb{Q}_p)/pE(\mathbb{Q}_p) \longrightarrow E(\mathbb{Q}_p^{ur})/pE(\mathbb{Q}_p^{ur})$$

is not injective. Since $H^0(\mathbb{Q}_p, E[p^\infty]) \cong \mathbb{Z}_p/\mathbb{Z}_p$, we get that $E(\mathbb{Q}_p) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p/\mathbb{Z}_p$. Therefore, $\mathbb{F}_p$-rank of $E(\mathbb{Q}_p)/pE(\mathbb{Q}_p)$ is two. Since $\text{res}_p^{ur}$ factors through $\phi$ and $\kappa_p^{ur}$ and $\phi$ is not injective, we get that the $\text{Im}(\text{res}_p^{ur})$ has $\mathbb{F}_p$-rank $\leq 1$. Hence, the claim follows. \qed

**Corollary 3.7.** Under the hypothesis of the theorem on the elliptic curve $E$ over $\mathbb{Q}$, if either $\text{rank}_{\mathbb{F}_p}(\text{III}(E)[p]) > 1$, or $\text{III}(E)[p] \neq 0$, and $\text{III}(E)[p^\infty] < \infty$, then there exists an unramified abelian extension of $\mathbb{Q}(E[p])$ with Galois group $E[p]$. Galois over $\mathbb{Q}$, on which $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \subset \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ operates by the standard 2 dimensional representation of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ over $\mathbb{Z}/p\mathbb{Z}$. If $\text{III}(E)[p] = 0$ but then if Mordell-Weil rank of $E$ over $\mathbb{Q}$ is $\geq 2$, then also there exists such an unramified abelian extension of $\mathbb{Q}(E[p])$ with Galois group $E[p]$.

**Proof.** Observe that if $\text{III}(E)[p^\infty] < \infty$, then $\text{III}(E)[p]$ has order which is a square, in particular, if $\text{III}(E)[p]$ is nonzero, its rank over $\mathbb{Z}/p\mathbb{Z}$ is at least 2. Note also that under the hypothesis of the Theorem 3.1, the action of $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \subset \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ on $E[p]$ is irreducible, and hence any non-trivial homomorphism $\text{res}_K(f) : \text{Gal}(\overline{K}/K) \longrightarrow E[p]$ which is $\text{Gal}(K/\mathbb{Q})$-equivariant must be surjective, constructing an unramified extension of $K$ with Galois group $E[p]$.

**Remark 3.8.** In Theorem 3.1, all our analysis is done with the Selmer group, not distinguishing the part of it coming from the Mordell-Weil group, and the part coming from III. In fact there have been papers constructing unramified extensions of $\mathbb{Q}(E[p])$ using the Mordell-Weil group, see e.g. [SY] and [TH], which give conclusions of the form that if the Mordell-Weil group is sufficiently large compared to number of places of $\mathbb{Q}$ where $E$ has bad reduction, then the classgroup of $\mathbb{Q}(E[p])$ is nonzero. It may be remarked that dealing with extensions of $\mathbb{Q}(E[p])$ using the Mordell-Weil group is easier in the sense that these extensions come from extensions of $\mathbb{Q}$.

**Example 1** Let $E$ be the elliptic curve defined by the equation

$$y^2 + xy = x^3 - x^2 - 332311x - 73733731.$$  

The Cremona level of $E$ is $1058d1$. Then it follows from [LMFDB] that $E[5]$ is an irreducible representation with full image of Galois representation equal to $\text{GL}_2(\mathbb{F}_5)$. Further the Tamagawa number is equal to 1 at primes of bad reduction 2 and 23. Again from [LMFDB], we have that $\text{III}(E/Q)[5]$ has $\mathbb{F}_5$-rank two and $a_5(E) = -2 \neq 1 \mod 5$. As a consequence we get that the ideal class group $\text{Cl}_K$ for $K = \mathbb{Q}(E[5])$ has a quotient isomorphic to $E[5]$ as $\text{Gal}(K/\mathbb{Q})$-module.
We mention that to produce a quotient of $\text{Cl}_K/p\text{Cl}_K$ isomorphic to $E[p]$, it is not necessary to assume that $\text{III}(E/\mathbb{Q})[p]$ is non-trivial. The elliptic curve,

$$F : y^2 + xy + y = x^3 + 2$$

given by Cremona number 1058c1 satisfy assumptions (a) to (d) of Theorem 3.1. In fact, $F[5] \cong E[5]$ as $\text{Gal}(\mathbb{Q}/\mathbb{Q})$-module (see [CM, Table, page 25]). The Mordell-Weil rank of $F$ is two and $\text{III}(F/\mathbb{Q})[5] = 0$.

4. The Converse

In this section, we address the converse part of Question 2.1.

Let $R_p(E/\mathbb{Q})$ be the subgroup of $H^1(\mathbb{Q}, E[p])$ defined by the exact sequence

$$0 \longrightarrow R_p(E/\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, E[p]) \longrightarrow \prod_v H^1(Q_v^\text{ur}, E[p])$$

**Lemma 4.1.** Suppose that the following holds

(a) $E$ has good reduction at $p$.

(b) If $E$ has ordinary reduction at $p$ and $a_p(E) \neq 1 \mod p$ then $E[p]$ is wildly ramified at $p$.

(c) $c_v(E)$ is a $p$-adic unit for every finite prime $v \neq p$.

Then $R_p(E/\mathbb{Q}) \subset \text{Sel}_p(E/\mathbb{Q})$.

**Proof.** Let $f \in R_p(E/\mathbb{Q})$. Then $f|_{I_v}$ is zero in $H^1(Q_v^\text{ur}, E[p])$ and therefore the image of $f$ in $H^1(Q_v^\text{ur}, E)$ is also zero. We suppose first that $v \neq p$. Since $c_v(E)$ is a $p$-adic unit, $H^1(Q_v, E) \longrightarrow H^1(Q_v^\text{ur}, E)$ is injective and therefore the image of $f$ in $H^1(Q_v, E)$ is zero. Thus to show that $f \in \text{Sel}_p(E/\mathbb{Q})$, it is enough to show that the image of $f$ in $H^1(Q_p, E)$ is also zero, which is what we do next.

Suppose that $E$ has good and ordinary reduction at $p$. If $\star$ in representation 3.1 is non-zero then $E[p]^{I_p} = 0$ and we get that $H^1(Q_p^\text{ur}/Q_p, E[p]^{I_p}) = 0$. If $\star$ is zero, from the assumption $a_p(E) \neq 1 \mod p$, the Frobenius at $p$ acts on $E[p]^{I_p}$ by a non-trivial character of order prime to $p$. This implies that $H^0(Q_p^\text{ur}/Q_p, E[p]^{I_p}) = 0$. Since $\text{Gal}(Q_p^\text{ur}/Q_p)$ is procyclic, we get that $H^1(Q_p^\text{ur}/Q_p, E[p]^{I_p}) = 0$. Therefore $H^1(Q_p, E[p]) \longrightarrow H^1(Q_p^\text{ur}, E[p])$ is injective. This implies that $f$ is trivial in $H^1(Q_p, E[p])$. Therefore the image of $f$ in $H^1(Q_p, E)$ is zero.

Next, consider the case when $E$ has supersingular reduction at $p$. Then, as is well-known, $E(F)[p] = 0$ for every finite unramified extension $F$ of $\mathbb{Q}_p$, (see for example [E]). This implies that $E(Q_p^{ur})[p] = 0$. Therefore the restriction map from $H^1(Q_p, E[p]) \longrightarrow H^1(Q_p^{ur}, E[p])$ is injective. Again we have that the image of $f$ in $H^1(Q_p, E[p])$ trivial. In particular, its image in $H^1(Q_p, E)$ is also trivial. This proves that $f \in \text{Sel}_p(E/\mathbb{Q})$. □

For the next lemma, we will keep the notation $K = \mathbb{Q}(E[p])$, $I_v$ the inertia subgroup of $\text{Gal}(\mathbb{Q}_v/\mathbb{Q}_v)$ for a prime $v$ of $\mathbb{Q}$, and for a prime $w|v$ of $K$, $I_w^K$ will denote the corresponding inertia subgroup of $\text{Gal}(\mathbb{K}_w/\mathbb{K}_w)$.

**Lemma 4.2.** Let $\mathcal{S}$ be the set of finite primes $v$ of $\mathbb{Q}$ not equal to $p$ such that $E$ has multiplicative reduction at $v$ and $E(Q_v^{ur})[p]$ has $\mathbb{F}_p$-rank one. In the case $p = 3$, we also assume that $\mathcal{S}$ contains the set of prime $v$ such that $E$ has additive potentially good reduction with $E(Q_v^{ur})[p]$ has $\mathbb{F}_p$-rank one. Let $v \neq p$ be a finite prime of $\mathbb{Q}$ for which
\[ c_v(E) \text{ is a } p\text{-adic unit. Then } H^1(I_v/I^K_v, E[p]) \text{ is non-trivial for a prime } w | v \text{ of } K \text{ if and only if } v \in \mathfrak{T}. \text{ Further, in this case the } \mathbb{F}_p\text{-rank of } H^1(I_v/I^K_v, E[p]) \text{ is also one.} \]

**Proof.** First suppose that \( E \) has additive reduction at \( v \neq p \). If \( E \) has potentially multiplicative reduction at \( v \), there exist a ramified quadratic extension of \( \mathbb{Q}_v \) over which \( E \) has split multiplicative reduction. Let \( \chi \) be the corresponding ramified quadratic character of the absolute Galois group of \( \mathbb{Q}_v \). This implies that \( E \) is a ramified quadratic twist of an elliptic curve \( E' \) with split multiplicative reduction at \( v \) and \( E[p] \cong E'[p] \otimes \chi \) as \( \text{Gal}(\overline{\mathbb{Q}_v}/\mathbb{Q}_v) \)-modules. Recall that \( \bar{\rho} \) denote the Galois representation associated to \( E[p] \) and let \( \bar{\rho}' \) denote the Galois representation associated to \( E'[p] \). Since \( E' \) has split multiplicative reduction, \( E'[p] \) is a semistable Galois representation. Therefore \( \bar{\rho}' \) restricted to \( I_v \) is represented by matrices of the form \( \begin{pmatrix} 1 & \ast \\ 0 & 1 \end{pmatrix} \). This implies that \( \bar{\rho} \) is represented by matrices of the form \( \begin{pmatrix} \chi & \ast \\ 0 & \chi \end{pmatrix} \). Since \( \chi \) is a ramified character, we get that \( E[p]^{I_v} = 0 \).

Next suppose that \( E \) has additive reduction at \( v \neq p \) which is potentially good. In this case it is well-known that \( I_v/I^K_v \) is a cyclic group of order at most 6. Thus if \( p \geq 5 \) then \( I_v/I^K_v \), has order prime to \( p \) and therefore \( H^1(I_v/I^K_v, E[p]) = 0 \). Finally, suppose that \( p = 3 \) and \( E \) has additive and potentially good reduction at \( v \). In this case \( I_v \) acts on \( E[p] \) non-trivially (see for example [ST, Corollaries 2(b), 3]). Since \( I_v/I^K_v \) is cyclic, the cardinality of \( H^1(I_v/I^K_v, E[p]) \) and \( H^0(I_v/I^K_v, E[p]) = E(\mathbb{Q}_v) \) are the same. As \( I_v \) acts non-trivially on \( E[p] \), the \( \mathbb{F}_p \)-rank of \( E[p]^{I_v} \) is at most one. Therefore if \( E[p]^{I_v} \) is non-zero, the \( \mathbb{F}_v \)-rank of \( H^1(I_v/I^K_v, E[p]) \) is one. We mention that it is well-known that \( E(\mathbb{Q}_v)[p] \neq 0 \) only when 3 divides the Tamagawa number of \( E \) over \( \mathbb{Q}_v(\mu_3) \).

Next, we suppose that \( E \) has multiplicative reduction at \( v \neq p \). If \( E \) has non-split multiplicative reduction at \( v \), then there exists a quadratic unramified extension of \( \mathbb{Q}_v \) over which \( E \) has split multiplicative reduction. Thus if \( E \) has multiplicative reduction at \( v \) then it has split multiplicative reduction over \( \mathbb{Q}_v^{ur} \). This implies that \( \mu_p \subset E(\mathbb{Q}_v^{ur})[p] \). Thus \( E[p]^{I_v} \neq 0 \). If \( E[p]^{I_v} \) has \( \mathbb{F}_p \)-rank two then \( I_v/I^K_v \) is a trivial group. Thus \( H^1(I_v/I^K_v, E[p]) \) can be non trivial only when \( E(\mathbb{Q}_v^{ur})[p] \) has \( \mathbb{F}_p \)-rank one.

Now suppose that \( E(\mathbb{Q}_v^{ur})[p] = E[p]^{I_v} \) has \( \mathbb{F}_p \)-rank one and \( E \) has multiplicative reduction at \( v \). Since \( \mu_p \subset \mathbb{Q}_v^{ur} \), and the determinant of the Galois representation \( \bar{\rho} \) associated to \( E[p] \) is the cyclotomic character mod \( p \), we get that \( \bar{\rho} \) restricted to \( I_v \) is equivalent to the matrices of the form \( \begin{pmatrix} 1 & \ast \\ 0 & 1 \end{pmatrix} \) for \( \ast \in \mathbb{F}_p \). Further, since \( E[p]^{I_v} \neq E[p] \), \( I_v \) acts on \( E[p] \)-nontrivially. Therefore the image of \( \bar{\rho} \) has order \( p \) and it is a \( p \)-Sylow subgroup of \( G = \text{Gal}(K/\mathbb{Q}) \). In particular, \( I_v/I^K_v \) is a cyclic group of order \( p \). This implies that the \( \mathbb{F}_p \)-rank of \( H^1(I_v/I^K_v, E[p]) \) is one. This proves the lemma. \( \square \)

**Theorem 4.1.** Suppose that the following holds

(a) \( E \) has good reduction at \( p \).

(b) If \( E \) has ordinary reduction at \( p \) and \( a_p(E) \neq 1 \mod p \) then that \( E[p] \) is wildly ramified at \( p \).

(c) \( c_v(E) \) is a \( p \)-adic unit for every finite prime \( v \neq p \).

(d) \( E[p] \) is an irreducible \( \text{Gal}(\mathbb{Q}/\mathbb{Q}) \)-representation.
Then
\[ \text{rank}_{\mathbb{F}_p} \text{Hom}_G(\text{Cl}_K/p\text{Cl}_K, E[p]) \leq \text{rank}_{\mathbb{F}_p} \text{Sel}_p(E/\mathbb{Q}) + \#\mathfrak{S}. \]

**Proof.** Consider the commutative diagram

\[
\begin{array}{cccccc}
0 & \rightarrow & \text{Hom}(\text{Cl}_K/p\text{Cl}_K, E[p])^G & \rightarrow & H^1(K, E[p])^G & \rightarrow & \prod_v (\prod_{w|v} H^1(K_{w}^\ur, E[p]))^G \\
& & \uparrow & & \uparrow & & \\
0 & \rightarrow & R_p(E/\mathbb{Q}) & \rightarrow & H^1(\mathbb{Q}, E[p]) & \rightarrow & \prod_v H^1(\mathbb{Q}_{v}^\ur, E[p])
\end{array}
\]

where \( v \) varies over the primes of \( \mathbb{Q} \) and \( w \) varies over primes of \( K \). From Lemma 3.3, \( \beta \) is an isomorphism.

The kernel of \( \gamma_v : H^1(\mathbb{Q}_{v}^\ur, E[p]) \rightarrow \prod_{w|v} H^1(K_{w}^\ur, E[p]))^G \) is same as the kernel of \( H^1(\mathbb{Q}_{v}^\ur, E[p]) \rightarrow H^1(K_{w}^\ur, E[p])) \) for fixed prime \( w|v \) of \( K \), which is equal to \( H^1(I_v/I_w^K, E[p]) \).

Let \( w|p \) be a prime of \( K \). We shall show that \( H^1(I_p/I_w^K, E[p]) = 0 \). First we consider the case when \( E \) has supersingular reduction at \( p \). It is well-known that the action of \( I_p \) on \( E[p] \) factors through a cyclic group of order prime to \( p \), see for example [E], and also [BG, Theorem 1.2] for an exposition. As a consequence, we get that \( H^1(I_p/I_w^K, E[p]) = 0 \).

Next, consider the case when \( E \) has ordinary reduction at \( p \). If \( E \) is an irreducible \( p \)-module with the image of \( \gamma_v \) is the kernel of \( H^1(I_p/I_w^K, E[p]) \), then it is enough to show that \( H^1(P, E[p]) \) is empty. From Lemma 3.1, \( R_p(E/\mathbb{Q}) \subset \text{Sel}(E/\mathbb{Q}) \) and this proves the theorem.

**Example 2:** Consider the following elliptic curve with Cremona number 423801ci1 and conductor \( 3^2 \cdot 7^2 \cdot 31^2 \) from [LMFDB].

\[ E : y^2 + y = x^3 - 17034726259173x - 27061436852750306309 \]

From [LMFDB], we get that \( E[5] \) is an irreducible \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \)-module with the image of associated Galois representation as \( \text{GL}_2(\mathbb{F}_5) \). The curve \( E \) has additive reduction at the primes 3, 7 and 31 and has good and ordinary reduction at 5 with \( a_5(E) = 4 \neq 1 \) mod 5. The Tamagawa numbers are 5-adic unit at all primes of bad reduction. In this case the set \( \mathfrak{S} \) is empty. The Mordell-Weil rank of \( E \) is 0 and \( \text{III}(E/\mathbb{Q}) \) has cardinality 625. We do not
know if \( III(E/Q) \cong \mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z} \) or \( III(E/Q) \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \). In any case, as a consequence of Theorem 3.1, we get that \( \text{rank}_{\mathbb{F}_5} \text{Hom}_G(\text{Cl}_{K/5}\text{Cl}_{K}, E[5]) \) is at least one. Further, since \( \mathcal{F} \) is empty, from Theorem 4.1 we get that \( R_{\mathbb{F}_5}(E/Q) \cong \text{Hom}_G(\text{Cl}_{K/5}\text{Cl}_{K}, E[5]) \) and it is a non-trivial group. We also mention that being a subgroup of \( \text{Sel}_p(E/Q) \), in general \( R_{\mathbb{F}_5}(E/Q) \) may be the trivial group even if \( \text{Sel}_p(E/Q) \) is non-trivial. But in this particular example, \( R_{\mathbb{F}_5}(E/Q) \) is a non trivial group and every element of \( \text{Hom}_G(\text{Cl}_{K/5}\text{Cl}_{K}, E[5]) \) is in the image of \( R_{\mathbb{F}_5}(E/Q) \) under the natural restriction map of Galois cohomology.

**Acknowledgement:** The authors must thank Harish-Chandra Research Institute, Allahabad for the hospitality, and Prof. Kalyan Chakraborty for the conference on Class groups at the Harish-Chandra Research Institute in October 2019, Allahabad where our collaboration on this work took place. The authors also thank N. Dummigan, H. Katsurada, and C. Wuthrich for their interest and encouragement.

**REFERENCES**

[AS] Amod Agashe, William Stein, *Visibility of Shafarevich-Tate Groups of Abelian Varieties*, Journal of Number Theory, 97, 171-185 (2002)

[BD] J. Bergström, N. Dummigan, *Eisenstein congruences for split reductive groups*, Selecta Math. (N.S.) 22 (2016), no. 3, 1073-1115.

[BG] Kevin Buzzard, Toby Gee, *Explicit reduction modulo p of certain 2 dimensional crystalline representations*, International Mathematics Research Letter, Volume 2009, 12, 2303-2317 (2009).

[BK] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, vol. I, Progr. Math., vol. 86, Birkhuser, Boston (1990), pp. 333–400.

[BLR] S. Bosch, W. Lütkebohmert, and M. Raynaud, ”Neron Models,” Springer-Verlag, Berlin, 1990.

[CM] John E. Cremona and Barry Mazur, *Visualizing Elements in the Shafarevich-Tate Group*, Experimental Mathematics, Vol. 9 (2000), No. 1.

[DIK] N. Dummigan, T. Ibukiyama, H. Katsurada *Some Siegel modular standard L-values, and Shafarevich–Tate groups*, Journal of Number Theory, vol 131, no. 7, 1296-1330 (2011).

[E] Bas Edixhoven, *The weight in Serres conjectures on modular forms*, Invent. Math. 109 (1992), no. 3, 563594.

[FM] Masaaki Furusawa, Kazuki Morimoto: *Refined global Gross-Prasad conjecture on special Bessel periods and Böcherer's conjecture*, arXiv:1611.05567.

[Gr] Ralph Greenberg, *Iwasawa theory of elliptic curves*, Springer, Lecture Notes in Mathematics, Volume 1716(1999), 51-144.

[Ha] G. Harder: *A congruence between a Siegel and an elliptic modular form*, manuscript, 2003, reproduced J.H. Bruinier, et al. (Eds.), The 1-2-3 of Modular Forms, Springer-Verlag, Berlin, Heidelberg (2008), pp. 247–262.

[K] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. math., 152 1-36 (2003).

[LMFDB] LMFDB, http://www.lmfdb.org/EllipticCurve/Q/1058d1/.

[LW] Tyler Lawson, Christian 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.

[Mi] J. S. Milne, *Arithmetic duality theorems*, https://www.jmilne.org/math/Books/ADTnot.pdf.

[P] 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).

[P2] D. Prasad, *A proposal for non-abelian Herbrand-Ribet*; still in preliminary form, available at http://www.math.tifr.res.in/dprasad/.
[Ri1] K. Ribet, A modular construction of unramified $p$-extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.*, 34, 151-162 (1976).

[Ri2] K. Ribet, *Mod p Hecke operators and congruences between modular forms*. Invent. Math. 71 (1983), no. 1, 193–205.

[RS] K. Rubin, A. Silverberg, *Families of elliptic curves with constant mod p representations*. Elliptic curves, modular forms, and Fermat’s last theorem (Hong Kong, 1993), 148–161, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

[SY] Fumio Sairaiji, Takuyu Yamauchi *On the class numbers of the fields of the $p^n$-torsion points of certain elliptic curves over $\mathbb{Q}$*. Journal of Number Theory, 156, 2015, 277-289.

[TH] Toshiro Hiranouchi, *Torsion primes and the class numbers associated to an elliptic curve over $\mathbb{Q}$*. Hiroshima Math. Journal, 49, (2019), 117-127.

[ST] Jean-Pierre Serre, John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2), 88, 492-517, 1968.

[Was] L. C. Washington, *Introduction to Cyclotomic Fields*, GTM, Springer-Verlag, vol. 83, (1982).

D.P.: INDIAN INSTITUTE OF TECHNOLOGY BOMBAY, POWAI, MUMBAI-400076

D.P.: TATA INSTITUTE OF FUNDAMENTAL RESEARCH, COLABA, MUMBAI-400005.

E-mail address: prasad.dipendra@gmail.com

S.S.: INDIAN INSTITUTE OF TECHNOLOGY, KANPUR.

E-mail address: sshekhrs2012@gmail.com