Relating the Tate-Shafarevich group of an Elliptic curve with the class group

Dipendra Prasad
IIT Bombay
(Report on joint work with Sudhanshu Shekhar)

July 03, 2020

Setting-up the problem

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

Setting-up the problem

It is a natural question to understand which $V_{i,j}$'s appear in $\mathcal{C}_K/p\mathcal{C}_K$.
The aim of this work is to formulate some questions in this direction which can be viewed as a GL_2 analogue of the famous theorem of Herbrand-Ribet.
One is hoping for a conjectural answer along the lines of Herbrand-Ribet to say that the representation $\mathrm{Sym}^i(\mathbb{Z}/p + \mathbb{Z}/p) \otimes \det^j$ of $\mathrm{GL}_2(\mathbb{Z}/p)$ appears in $\mathcal{C}_K/p\mathcal{C}_K$ if and only if the 'algebraic part' of the first nonzero derivative of $L(s, \mathrm{Sym}^i(E) \otimes \det^j)$ at $s = 0$ is divisible by p (in some favorable situations to be carefully identified).

Recalling Herbrand-Ribet

By the class number formula:

$$\zeta_{\mathbb{Q}(\zeta_p)}/\zeta_{\mathbb{Q}(\zeta_p)^+}(s) = \frac{h/h^+}{p} + \quad \text{higher order terms...},$$

from which one gets,

$$\prod_{\chi} L(0,\chi) = \prod_{\chi} |\mathcal{C}_{\mathbb{Q}(\zeta_p)}(\chi)|,$$

where $\chi : (\mathbb{Z}/p)^\times \to \mathbb{C}^\times, \chi(-1) = -1$, with $\chi \neq \omega^{-1}$.

The statements so far are due to Kummer. The theorem of Herbrand-Ribet is that not only are the products on the two sides equal, but the terms on the two sides are individually equal, at least $p|L(0,\chi)$ if and only if p divides $|\mathcal{C}_{\mathbb{Q}(\zeta_p)}(\chi^{-1})|$.

Main question

In one of my manuscripts, a heuristic relating the representation of $\mathrm{GL}_2(\mathbb{Z}/p)$ on $\mathcal{C}_K/p\mathcal{C}_K$ and the divisibility of certain L-values by p was given based on factorisation of the class number formula for the Dedekind zeta function $\zeta_K(s)$:

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

in terms of the complex representation theory of $\mathrm{GL}_2(\mathbb{Z}/p)$ 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 $\mathcal{C}_K/p\mathcal{C}_K$. We will not detail the heuristic considerations made, except to recall the Birch-Swinnerton-Dyer conjecture.

According to the Birch-Swinnerton-Dyer conjecture, in the rank $= 0$ case (which is essentially known in the analytic rank $= 0$ case now?),

$$L(1, E) = \frac{\Omega_E \cdot |Ш(E)| \prod c_\ell}{|E_{tors}|^2},$$

where c_ℓ is the cardinality of the group of connected components of the Neron model of E at $\mathbb{Q}_\ell$, also called the Tamagawa factors; it is known that c_ℓ is less than or equal to 4 except when E has split multiplicative reduction at ℓ in which case it is the negative of the valuation of $j(E)$ at the place ℓ.

Thus if p is coprime to the Tamagawa factors at all places, and E does not have p-torsion, then p divides the algebraic part of $L(1, E)$ if and only if $p|Ш(E)$.

Main question, cont'd

The following question is at the basis of this work.

Question

Let E be an elliptic curve over $\mathbb{Q}$ with $E(\mathbb{Q}) = 0$, $K = \mathbb{Q}(E[p])$ the Galois extension of $\mathbb{Q}$ obtained by attaching elements of order p on E where p is an odd prime. We assume that $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/p)$, and also that p is coprime to $c_\ell = [E(\mathbb{Q}_\ell) : E(\mathbb{Q}_\ell)^0]$, the so-called Tamagawa numbers, for all finite primes ℓ. Let $\mathcal{C}_K$ denote the class group of K which comes equipped with a natural action of $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/p)$. Then if $p||Ш(E)(\mathbb{Q})|$, is it true that the $\mathrm{GL}_2(\mathbb{Z}/p)$ representation $\mathcal{C}_K/p\mathcal{C}_K$ contains the standard 2-dimensional representation of $\mathrm{GL}_2(\mathbb{Z}/p)$ as a quotient? What about the converse (assuming $E(\mathbb{Q}) = 0$ as well as p coprime to the Tamagawa numbers c_ℓ)?

A remark

Remark

Although the question above has been formulated for an elliptic curve, one can also formulate a similar question for holomorphic modular forms which give rise to similar Galois representations with values in $\mathrm{GL}_2(\mathbb{Z}/p)$, or more generally in $\mathrm{GL}_2(\mathbb{F}_q)$. In fact much of the work, formulated in terms of the Selmer groups, does not need an elliptic curve.

A reality check

There are examples due to K. Rubin and A. Silverberg of families of elliptic curves with the same field $\mathbb{Q}(E[5])$ with Galois group $\mathrm{GL}_2(\mathbb{Z}/5)$. 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? Hopefully, this does not happen!

By classfield theory, the question being discussed amounts to constructing an Galois extension L of $\mathbb{Q}$ containing $K = \mathbb{Q}(E[p])$ with $\mathrm{Gal}(L/\mathbb{Q}) = G$, which sits in an exact sequence:

$$1 \to E[p] \to G \to \mathrm{GL}_2(\mathbb{Z}/p) \to 1 \quad (\star)$$

such that $\mathrm{GL}_2(\mathbb{Z}/p)$ acts on $E[p]$ through its standard 2-dim'l rep'n, and the extension of $\mathbb{Q}(E[p])$ defined by the subgroup $E[p] \subset G$ is everywhere unramified.

As we will see later, $H^2(\mathrm{GL}_2(\mathbb{Z}/p), E[p]) = 0$, thus any extension as in $(\star)$ splits.

Possible approaches

There are two natural appoaches 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 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 $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ 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 a suitable cusp form as in (1) serves the purpose of constructing everywhere unramified extension of $\mathbb{Q}(\mu_p)$ of the desired kind.

Congruence of Siegel modular forms

Neither of the two steps is understood for $\mathrm{GSp}(4)$ — second step not even in one case!— (perhaps not even for $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ in some generality?), except that there is a recent work due to Bergström and Dummigan where they formulate some general questions along these lines.

Note that there are two conjugacy classes of maximal parabolic subgroups in $\mathrm{GSp}(4)$ and both could be sources of such congruences, and therefore could have applications to Galois representations.

For our case, an Eisenstein series supported on a Siegel parabolic is what will be useful (so that the associated Galois representation lands inside the Levi of the Klingen parabolic).

The Klingen parabolic P in $\mathrm{GSp}(4)$ looks like

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

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 $\mathrm{GL}(2)$ which thus seems ideally suited to give rise to extensions of K on which the Galois group of K, i.e., $\mathrm{GL}_2(\mathbb{Z}/p)$, operates by a twist of the 2 dimensional standard representation.
The specific question thus is that if p divides (the algebraic part of) $L(1, \pi \otimes \omega^j)$, π a holomorphic cusp form on $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$, there is a cusp form on $\mathrm{GSp}(4)$ which is congruent to an Eisenstein series on $\mathrm{GSp}(4)$ induced from the cuspform π on $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ treated as the Levi subgroup of the Siegel parabolic in $\mathrm{GSp}(4)$.

An example of Harder

Around the turn of the new millenium, Harder proposed an example of such a congruence through numerical computations (which was later confirmed).
For the unique elliptic modular form f for $\mathrm{SL}_2(\mathbb{Z})$ of weight 22, Harder conjectured the existence of a cuspidal eigenform on $\mathrm{GSp}(4, \mathbb{A}_{\mathbb{Q}})$ with the following congruence for Hecke eigenvalues, which we just write down from his paper without further explanations:

$$\lambda(p) \equiv p^8 + a_f(p) + p^{13} \bmod 41, \qquad \text{for all primes } p,$$

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

$$41 | \frac{\Lambda(f,14)}{\Omega_+},$$

which allows Ramanujan like congruence $\Delta \equiv E_{12} \mod 691$, between an Eisenstein series and a cusp form on $\mathrm{GSp}(4)$.

Example of Harder, cont'd

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 $\mathrm{SL}_2(\mathbb{Z})$ cuts out a $\mathrm{GL}_2(\mathbb{Z}/41)$ extension K_f of $\mathbb{Q}$ which has an unramified abelian extension on which $\mathrm{GL}_2(\mathbb{Z}/41)$ acts by $\mathrm{Sym}^1 \otimes \det^{-8}$ (or, is it $\mathrm{Sym}^1 \otimes \det^{-13}$?) using the Galois representation associated to the cuspform.
Although there has been much work extending Ribet's work to higher dimensional groups, e.g. due to Skinner and Urban, we are not sure if this question has been considered.

The work uses cohomological methods needing some generalities as well as some results related to elliptic curves which we put together in this section. We will follow the general notation on Galois cohomology to denote, for K any field with $\bar{K}$ its algebraic closure, $H^1(\mathrm{Gal}(\bar{K}/K), A(\bar{K}))$ by $H^1(K, A)$ where A is any group scheme defined over K which in this work will always be an abelian group scheme.
The following Lemma will play a rather important role in several places in this work.

Lemma

Let G be a finite subgroup of $\mathrm{GL}_2(\mathbb{Z}/p)$ operating irreducibly on $E[p] = \mathbb{Z}/p + \mathbb{Z}/p$, then $H^i(G, E[p]) = 0$ for all i.

Corollary

If the representation of $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ *on* $E[p]$ *is irreducible, the restriction map*

$$H^1(\mathbb{Q}, E[p]) \xrightarrow{\mathrm{res}_K} H^1(K, E[p])^{\mathrm{Gal}(K/\mathbb{Q})} = \mathrm{Hom}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathrm{Gal}(\bar{\mathbb{Q}}/K), E[p]),$$

is an isomorphism.

This corollary allows one to use elements of $f \in H^1(\mathbb{Q}, E[p])$, to construct extensions K_f of $K = \mathbb{Q}(E[p])$ with Galois group $\mathrm{Gal}(K_f/K) \cong E[p]$ which we will see under appropriate conditions on $f \in H^1(\mathbb{Q}, E[p])$ belonging to the Selmer group, gives the desired unramified extension of $K = \mathbb{Q}(E[p])$.

Selmer groups

In the rest of this lecture, we construct the standard 2-dimensional representation of $\mathrm{GL}_2(\mathbb{Z}/p)$ on the class group $\mathcal{C}_K/p\mathcal{C}_K$ using the Selmer group of E.
Let $\mathrm{Sel}_p(E/\mathbb{Q})$ be the p-Selmer group of E over $\mathbb{Q}$ defined by the exact sequence

$$0 \longrightarrow \mathrm{Sel}_p(E/\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, E[p]) \longrightarrow \prod_{\ell} H^1(\mathbb{Q}_\ell, E),$$

where ℓ varies over primes of $\mathbb{Q}$, including the infinite prime. Since the restriction map $H^1(\mathbb{Q}, E[p]) \longrightarrow H^1(\mathbb{Q}_\ell, E)$ factors through $H^1(\mathbb{Q}, E[p]) \longrightarrow H^1(\mathbb{Q}_\ell, E[p])$, we also have the following exact sequence

$$0 \longrightarrow \mathrm{Sel}_p(E/\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, E[p]) \longrightarrow \prod_{\ell} H^1(\mathbb{Q}_\ell, E[p])/\mathrm{Im}(\kappa_\ell),$$

Selmer groups, cont'd

where

$$\kappa_\ell : E(\mathbb{Q}_\ell)/pE(\mathbb{Q}_\ell) \longrightarrow H^1(\mathbb{Q}_\ell, E[p])$$

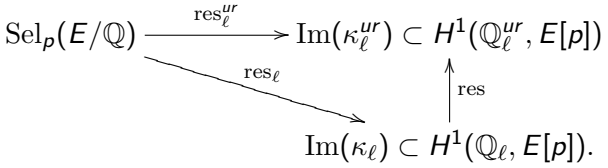
is called the *Kummer map* of E associated to multiplication by p map on E

$$0 \longrightarrow E[p] \longrightarrow E \xrightarrow{p} E \longrightarrow 0.$$

Let

$$\kappa_\ell^{ur} : E(\mathbb{Q}_\ell^{ur})/pE(\mathbb{Q}_\ell^{ur}) \longrightarrow H^1(\mathbb{Q}_\ell^{ur}, E[p])$$

be the Kummer map of E over the maximal unramified extension $\mathbb{Q}_\ell^{ur}$ of $\mathbb{Q}_\ell$.
For every prime ℓ of $\mathbb{Q}$, we get restriction maps



Selmer groups, cont'd

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

Constructing unramified extensions

Theorem

Suppose that the following holds:

(a) $E[p]$ *is an irreducible* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-module.*

(b) $c_\ell(E)$ *is a p-adic unit for every finite prime* $\ell \neq p$.

(c) $E(\mathbb{Q}_p)[p] = 0$.

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

$$\mathrm{res}_K : \mathrm{Ker}(\mathrm{res}_p^{ur}) \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathcal{C}_K, E[p]) \subset H^1(K, E[p]).$$

Idea of the proof

Let $f \in \mathrm{Sel}_p(E/\mathbb{Q}) \subset H^1(\mathbb{Q}, E[p])$. First we shall show that f is unramified outside p, i.e., the restriction of f to $H^1(K, E[p]) = \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbb{Q}}/K), E[p])$ defines an extension of K, call it K_f, which is unramified at any place of K not dividing p. This will follow if we can show that the restriction of $f \in \mathrm{Sel}_p(E/\mathbb{Q}) \subset H^1(\mathbb{Q}, E[p])$ to $H^1(\mathbb{Q}_\ell^{ur}, E[p])$ is trivial which is what we shall do.
Let $\ell \neq p$ be a finite prime of $\mathbb{Q}$. Consider the commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & E(\mathbb{Q}_\ell)/pE(\mathbb{Q}_\ell) & \xrightarrow{\kappa_\ell} & H^1(\mathbb{Q}_\ell, E[p]) \\ & & \downarrow \lambda & & \downarrow \mu \\ 0 & \longrightarrow & E(\mathbb{Q}_\ell^{ur})/pE(\mathbb{Q}_\ell^{ur}) & \xrightarrow{\kappa_\ell^{ur}} & H^1(\mathbb{Q}_\ell^{ur}, E[p]). \end{array} \tag{1}$$

Idea of the proof

The essence of the proof is that for $\ell \neq p$ with $(c_\ell, p) = 1$, λ is the zero map, hence by the above commutative diagram, the restriction of $f \in \mathrm{Sel}_p(E/\mathbb{Q}) \subset H^1(\mathbb{Q}, E[p])$ to $H^1(\mathbb{Q}_\ell^{ur}, E[p])$ is trivial for any $\ell \neq p$.

To see that for $\ell \neq p$ with $(c_\ell, p) = 1$, λ is the zero map, we in fact prove that $E(\mathbb{Q}_\ell^{un})/pE(\mathbb{Q}_\ell^{un}) = 0$. For this, note the well-known fact that $E(\mathbb{Q}_\ell^{un})$ is a successive extension of $\mathbb{Z}_\ell^{un}$ with one of $E(\bar{\mathbb{F}}_\ell)$ (if E has good reduction), or $\bar{\mathbb{F}}_\ell^\times$, $\bar{\mathbb{F}}_\ell$, and a finite group of order c_ℓ; each one is p-divisible (i.e., multiplication by p is surjective).

Since p is odd, $K = \mathbb{Q}(E[p]) \supset \mathbb{Q}(\mu_p)$ is an imaginary field, hence K_f is automatically unramified at the infinite places of K.
Finally, we deal with the ramification property of K_f at primes of K above p. From the structure theory of rational points of an elliptic curve over a local field, we know that $E(\mathbb{Q}_p) \cong \mathbb{Z}_p \oplus E(\mathbb{Q}_p)(\mathrm{torsion})$. Therefore if $E(\mathbb{Q}_p)[p] = 0$, $\mathrm{Im}(\kappa_p) \subset H^1(\mathbb{Q}_p, E[p])$ has $\mathbb{F}_p$-rank 1. Since $\mathrm{Im}(\mathrm{res}_p) \subset \mathrm{Im}(\kappa_p)$ and res_p^{ur} factors through res_p, $\mathrm{Im}(\mathrm{res}_p^{ur})$ has $\mathbb{F}_p$-rank at most 1, and hence $\mathrm{rank}_{\mathbb{F}_p}(\mathrm{Ker}(\mathrm{res}_p^{ur})) \geq \mathrm{rank}_{\mathbb{F}_p}(\mathrm{Sel}_p(E/\mathbb{Q})) - 1$ which proves the theorem.

Unramified extensions of $\mathbb{Q}(E[p])$

Corollary

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

Some remarks

Remark

There seems no simple way to say for which elliptic curves E over $\mathbb{Q}_p$, $E(\mathbb{Q}_p)[p] = 0$, $p \geq 3$. If E has split multiplicative reduction at p, then $(p, c_p(E)) = 1$ implies $E(\mathbb{Q}_p)[p] = 0$; more precisely, $(p, c_p(E)) = 1$ if and only if $E(\mathbb{Q}_p^{ur})[p] = 0$. If E has good ordinary reduction at p with $a_p(E) \not\equiv 1 \bmod p$ or E has good supersingular reduction at p, then it is easy to see that $E(\mathbb{Q}_p)[p] = 0$. Even if $a_p(E) \equiv 1 \bmod p$, it is possible that $E(\mathbb{Q}_p)[p] = 0$, when $E[p]$ a wildly ramified Galois representation at p.

Remark

For the Theorem, we used $E(\mathbb{Q}_p)[p] = 0$ to bound the image of res_p^{ur} to have rank at most 1. However, there are other cases when the image of res_p^{ur} has rank at most 1. For example, the assertion of the Theorem holds for a CM elliptic curve with good ordinary reduction at p, even if $E(\mathbb{Q}_p)[p] \neq 0$. In this case, the image of res_p^{ur} has rank at most 1 as can be checked using the fact that $H^0(\mathbb{Q}_p^{ur}, E_{p^\infty})$ is a p-divisible group.

Some remarks, cont'd

Remark

In the Theorem, all our analysis is done with the Selmer group, not distiguishing the part of it coming from the Mordell-Weil group, and the part coming from $Ш$*. In fact there have been papers constructing unramified extensions of* $\mathbb{Q}(E[p])$ *using the Mordell-Weil group 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, much like the Kummer theory for* G_m*, is much better understood, and has the simplifying feature that these extensions come from extensions of* $\mathbb{Q}$*.*

Fine Selmer group

Let $R_p(E/\mathbb{Q})$, a variant of what has been called the *fine Selmer group* in the literature, be the subgroup of $H^1(\mathbb{Q}, E[p])$ defined by the exact sequence

$$0 \longrightarrow R_p(E/\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, E[p]) \longrightarrow \prod_{\ell} H^1(\mathbb{Q}_\ell^{ur}, E[p]).$$

Lemma

Let E be an elliptic curve defined over $\mathbb{Q}$ such that

(a) $E(\mathbb{Q}_p)[p] = 0$.

(b) $c_\ell(E)$ *is coprime to* p *for all primes* $\ell \neq p$.

Then $R_p(E/\mathbb{Q}) \subset \mathrm{Sel}_p(E/\mathbb{Q})$, *and* $R_p(E/\mathbb{Q}) = \mathrm{Ker}(\mathrm{res}_p^{ur})$.

Main theorem

In this section we discuss the main theorem of this work which estimates how much of the classgroup of $\mathbb{Q}(E[p])$ on which $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ operates as it does on $E[p]$) can be obtained using the Selmer group of E.

Theorem

Suppose that E is an elliptic curve over $\mathbb{Q}$ such that the following holds:

(a) *E has either good or multiplicative reduction reduction at p.*

(b) *$E(\mathbb{Q}_p)[p] = 0$.*

(c) *$c_\ell(E)$ is a p-adic unit for every finite prime $\ell \neq p$.*

(d) *$E[p]$ is an irreducible $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-representation.*

Then for a set $\mathfrak{T}$ of places of $\mathbb{Q}$ contained in the set of places of multiplicative reduction,

$$\mathrm{rank}_{\mathbb{F}_l}\mathrm{Sel}_p(E/\mathbb{Q}) - 1 \leq \mathrm{rank}_{\mathbb{F}_p}\mathrm{Hom}_G(\mathcal{C}_K/p\mathcal{C}_K, E[p]) \leq \mathrm{rank}_{\mathbb{F}_l}\mathrm{Sel}_p(E/\mathbb{Q}) + \#\mathfrak{T}.$$

Proof

The proof follows by analysing the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_G(\mathcal{C}_K/p\mathcal{C}_K, E[p]) & \longrightarrow & H^1(K, E[p])^G & \longrightarrow & \prod_{w_0}(H^1(K_{w_0}^{ur}, E[p])^{\mathrm{Gal}(K_{w_0}^{ur}/K_{w_0})})^{G_{w_0}}, \\ & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \gamma'} \\ 0 & \longrightarrow & R_p(E/\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, E[p]) & \xrightarrow{\delta} & \delta(H^1(\mathbb{Q}, E[p])) \to 0, \end{array}$$

where w_0 runs over places of K, taking only one place of K over any place of $\mathbb{Q}$, and where

$$\delta : H^1(\mathbb{Q}, E[p]) \to \prod_{\ell} H^1(\mathbb{Q}_\ell^{ur}, E[p])^{\mathrm{Gal}(\mathbb{Q}_\ell^{ur}/\mathbb{Q}_\ell)}.$$

Unramified Cohomology

For any Galois module M for $\mathrm{Gal}(\bar{K}/K)$, define the unramified cohomology of M by the exact sequence:

$$0 \longrightarrow H^1_{ur}(K, M) \longrightarrow H^1(K, M) \longrightarrow \prod_v H^1(K_v^{ur}, M).$$

In our work above, we have proved that $H^1_{ur}(\mathbb{Q}, E[p]) \neq 0$, for elliptic curves E with Tamagawa factors coprime to p. This immediately gives the unramified extension of $\mathbb{Q}(E[p])$ with Galois group $E[p]$.

It appears to us that unramified cohomology $H^1_{ur}(K, M)$ of, say finite Galois module M, are objects of independent interest, for which there may be some "abstract" structure theorems at least in some cases. For example, if $M = \mu_p$, and K contains p-th roots of unity, then $H^1_{ur}(K, \mu_p) = \mathcal{C}_K/p\mathcal{C}_K$. But if K does not contain p-th roots of unity, what is $H^1_{ur}(K, \mu_p)$ is an interesting exercise? (At least it is easy to see that $H^1_{ur}(\mathbb{Q}, \mu_p) = 0$.)

Thank you for your attention!