Control Theorems for Fine Selmer Groups

Debanjana Kundu

Quebec-Maine Number Theory Conference 2020

September 27, 2020

Table of Contents

Iwasawa Theory

Iwasawa theory involves studying the growth of Galois modules over infinite towers of number fields.

Iwasawa Theory

Iwasawa theory involves studying the growth of Galois modules over infinite towers of number fields.

Key Idea: Studying class groups or Selmer groups in isolation is hard. But, growth properties stabilize in *certain* (p-adic analytic) towers; in such cases studying them becomes easier.

Iwasawa Theory

Iwasawa theory involves studying the growth of Galois modules over infinite towers of number fields.

Key Idea: Studying class groups or Selmer groups in isolation is hard. But, growth properties stabilize in *certain* (p-adic analytic) towers; in such cases studying them becomes easier.

While studying rational points on Abelian varieties (or elliptic curves), the Selmer group plays an important role.

Iwasawa Theory

Iwasawa theory involves studying the growth of Galois modules over infinite towers of number fields.

Key Idea: Studying class groups or Selmer groups in isolation is hard. But, growth properties stabilize in *certain* (p-adic analytic) towers; in such cases studying them becomes easier.

While studying rational points on Abelian varieties (or elliptic curves), the Selmer group plays an important role. In 1972, Mazur introduced the Iwasawa theory of Selmer groups of Abelian varieties.

Iwasawa Theory

Iwasawa theory involves studying the growth of Galois modules over infinite towers of number fields.

Key Idea: Studying class groups or Selmer groups in isolation is hard. But, growth properties stabilize in *certain* (p-adic analytic) towers; in such cases studying them becomes easier.

While studying rational points on Abelian varieties (or elliptic curves), the Selmer group plays an important role. In 1972, Mazur introduced the Iwasawa theory of Selmer groups of Abelian varieties.

The key player in today's talk will be a subgroup of the Selmer group called the **fine Selmer group**.

Iwasawa Theory

Iwasawa theory involves studying the growth of Galois modules over infinite towers of number fields.

Key Idea: Studying class groups or Selmer groups in isolation is hard. But, growth properties stabilize in *certain* (p-adic analytic) towers; in such cases studying them becomes easier.

While studying rational points on Abelian varieties (or elliptic curves), the Selmer group plays an important role. In 1972, Mazur introduced the Iwasawa theory of Selmer groups of Abelian varieties.

The key player in today's talk will be a subgroup of the Selmer group called the **fine Selmer group**. This subgroup interpolates the growth of class group and the Selmer group.

Definition: Selmer Groups of Elliptic Curves

Let F be a number field. Consider an elliptic curve E/F and p be any prime. Define the classical Selmer group of E relative to p^n by

$$0 \to \mathrm{Sel}_{p^n}(E/F) \to H^1(F, E[p^n]) \to \prod_v H^1(F_v, E)$$

where v runs through all the non-archimedean places of K. Then

Definition: Selmer Groups of Elliptic Curves

Let F be a number field. Consider an elliptic curve E/F and p be any prime. Define the classical Selmer group of E relative to p^n by

$$0 \to \mathrm{Sel}_{p^n}(E/F) \to H^1(F, E[p^n]) \to \prod_v H^1(F_v, E)$$

where v runs through all the non-archimedean places of K. Then

$$\mathrm{Sel}(E/F) = \mathrm{Sel}_{p^\infty}(E/F) = \varinjlim_n \mathrm{Sel}_{p^n}(E/F),$$

Definition: Selmer Groups of Elliptic Curves

Let F be a number field. Consider an elliptic curve E/F and p be any prime. Define the classical Selmer group of E relative to p^n by

$$0 \to \mathrm{Sel}_{p^n}(E/F) \to H^1(F, E[p^n]) \to \prod_v H^1(F_v, E)$$

where v runs through all the non-archimedean places of K. Then

$$\mathrm{Sel}(E/F) = \mathrm{Sel}_{p^\infty}(E/F) = \varinjlim_n \mathrm{Sel}_{p^n}(E/F),$$

$$\mathrm{Sel}(E/\mathcal{L}) = \mathrm{Sel}_{p^\infty}(E/\mathcal{L}) := \varinjlim_L \mathrm{Sel}_{p^\infty}(E/L)$$

where L runs over all finite extensions of F contained in a pro-p p-adic Lie extension, $\mathcal{L}$.

Definition: Fine Selmer Group

We define

$$R_{p^n}(E/F) := \ker\left(\mathrm{Sel}_{p^n}(E/F) \to \bigoplus_{v|p} H^1(F_v, E[p^n])\right).$$

Definition: Fine Selmer Group

We define

$$R_{p^n}(E/F) := \ker\left(\mathrm{Sel}_{p^n}(E/F) \to \bigoplus_{v|p} H^1(F_v, E[p^n])\right).$$

Then we take direct limits as before to define

$$R(E/F) = R_{p^\infty}(E/F) := \varinjlim_n R_{p^n}(E/F)$$

Definition: Fine Selmer Group

We define

$$R_{p^n}(E/F) := \ker \left(\mathrm{Sel}_{p^n}(E/F) \to \bigoplus_{v|p} H^1(F_v, E[p^n]) \right).$$

Then we take direct limits as before to define

$$R(E/F) = R_{p^\infty}(E/F) := \varinjlim_n R_{p^n}(E/F)$$

$$R(E/\mathcal{L}) = R_{p^\infty}(E/\mathcal{L}) := \varinjlim_L R_{p^\infty}(E/L)$$

where L runs over all finite extensions of F contained in $\mathcal{L}$.

Table of Contents

Control Problem

Let F be a number field and $\mathcal{L}/F$ be a pro-p p-adic Lie extension with Galois group $\mathrm{Gal}(\mathcal{L}/F) \simeq G$. Let E be an elliptic curve defined over F. The study of the natural restriction map

$$s_{\mathcal{L}/F} : \mathrm{Sel}\left(E/F\right) \to \mathrm{Sel}\left(E/\mathcal{L}\right)^G$$

is called the **control problem**.

Mazur's Control Theorem

Theorem (Mazur (1972))

Let $\mathcal{L}/F$ be a $\mathbb{Z}_p$-extension and let E be an elliptic curve defined over F with good ordinary reduction at primes above p. Then both $\ker(s_{\mathcal{L}/L})$ and $\mathrm{coker}(s_{\mathcal{L}/L})$ are finite and bounded as L/F varies over all finite extensions inside $\mathcal{L}$.

Application: Growth of the Shafarevich-Tate Group

Theorem

Assume that E has good, ordinary reduction at all primes of F lying over p. Assume that $\mathrm{Sel}\left(E/\mathcal{L}\right)$ is Λ-cotorsion and that $\text{Ш}(F_n)[p^\infty]$ is finite for all $n \geq 0$. Then $\left|\text{Ш}(E/F_n)[p^\infty]\right| = p^{e_n}$ and there exist constants λ, μ, and ν such that

$$e_n = \lambda n + \mu p^n + \nu \textit{ for all } n \gg 0.$$

Greenberg's Control Theorem(s)

Theorem (Greenberg (2003))

Assume E has potentially ordinary reduction at all primes of F lying over p. Assume that $\mathcal{L}/F$ is a p-adic Lie extension satisfying the property that $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ above p. Further suppose that $\mathfrak{g}$ is reductive or $E(\mathcal{L})[p^\infty]$ is finite. Then both $\ker(s_{\mathcal{L}/L})$ and $\mathrm{coker}(s_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.

Greenberg's Control Theorem(s)

Theorem (Greenberg (2003))

Assume E has potentially ordinary reduction at all primes of F lying over p. Assume that $\mathcal{L}/F$ is a p-adic Lie extension satisfying the property that $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ above p. Further suppose that $\mathfrak{g}$ is reductive or $E(\mathcal{L})[p^\infty]$ is finite. Then both $\ker(s_{\mathcal{L}/L})$ and $\operatorname{coker}(s_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.

Some examples of p-adic Lie extensions $\mathcal{L}/F$, where the property $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ holds for all primes $\mathfrak{p} \mid p$, include:

- when $G = \mathrm{Gal}(\mathcal{L}/F)$ is Abelian.

Greenberg's Control Theorem(s)

Theorem (Greenberg (2003))

Assume E has potentially ordinary reduction at all primes of F lying over p. Assume that $\mathcal{L}/F$ is a p-adic Lie extension satisfying the property that $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ above p. Further suppose that $\mathfrak{g}$ is reductive or $E(\mathcal{L})[p^\infty]$ is finite. Then both $\ker(s_{\mathcal{L}/L})$ and $\operatorname{coker}(s_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.

Some examples of p-adic Lie extensions $\mathcal{L}/F$, where the property $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ holds for all primes $\mathfrak{p} \mid p$, include:

- when $G = \operatorname{Gal}(\mathcal{L}/F)$ is Abelian.
- when the inertia subgroup has finite index in G for all $\mathfrak{p} \mid p$.

Greenberg's Control Theorem(s)

Theorem (Greenberg (2003))

Assume E has potentially ordinary reduction at all primes of F lying over p. Assume that $\mathcal{L}/F$ is a p-adic Lie extension satisfying the property that $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ above p. Further suppose that $\mathfrak{g}$ is reductive or $E(\mathcal{L})[p^\infty]$ is finite. Then both $\ker(s_{\mathcal{L}/L})$ and $\operatorname{coker}(s_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.

Some examples of p-adic Lie extensions $\mathcal{L}/F$, where the property $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ holds for all primes $\mathfrak{p} \mid p$, include:

- when $G = \mathrm{Gal}(\mathcal{L}/F)$ is Abelian.
- when the inertia subgroup has finite index in G for all $\mathfrak{p} \mid p$.
- when G admits a faithful, finite-dimensional p-adic representation of Hodge-Tate type at $\mathfrak{p} \mid p$.

Table of Contents

Control Problem for Fine Selmer Groups

Let F be a number field and $\mathcal{L}/F$ be a pro-p p-adic Lie extension with Galois group $\mathrm{Gal}(\mathcal{L}/F) \simeq G$. Let E be an elliptic curve defined over F. The study of the natural restriction map

$$r_{\mathcal{L}/F} : R\left(E/F\right) \to R\left(E/\mathcal{L}\right)^{G}$$

is called the **control problem**.

Known Results

Theorem (Rubin (2000?))

Let F be a number field and E be an elliptic curve defined over F. Let $\mathcal{L}/F$ be a $\mathbb{Z}_p^d$-extension where $d \geq 1$, and suppose all primes of bad reduction of E and all primes above p are finitely decomposed. Then both $\ker(r_{\mathcal{L}/L})$ and $\mathrm{coker}(r_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.

Known Results

Theorem (Rubin (2000?))

Let F be a number field and E be an elliptic curve defined over F. Let $\mathcal{L}/F$ be a $\mathbb{Z}_p^d$-extension where $d \geq 1$, and suppose all primes of bad reduction of E and all primes above p are finitely decomposed. Then both $\ker(r_{\mathcal{L}/L})$ and $\operatorname{coker}(r_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.

Remarks.

1. The Control Theorem for fine Selmer groups is independent of the reduction type at p.

Known Results

Theorem (Rubin (2000?))

Let F be a number field and E be an elliptic curve defined over F. Let $\mathcal{L}/F$ be a $\mathbb{Z}_p^d$-extension where $d \geq 1$, and suppose all primes of bad reduction of E and all primes above p are finitely decomposed. Then both $\ker(r_{\mathcal{L}/L})$ and $\operatorname{coker}(r_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.

Remarks.

1. The Control Theorem for fine Selmer groups is independent of the reduction type at p.
2. When $d = 1$, the Control Theorem is proved for *all* $\mathbb{Z}_p$-extensions by Wuthrich (2004).

Known Results

Theorem (Rubin (2000?))

Let F be a number field and E be an elliptic curve defined over F. Let $\mathcal{L}/F$ be a $\mathbb{Z}_p^d$-extension where $d \geq 1$, and suppose all primes of bad reduction of E and all primes above p are finitely decomposed. Then both $\ker(r_{\mathcal{L}/L})$ and $\operatorname{coker}(r_{\mathcal{L}/L})$ are finite as L varies over all finite extensions of F inside $\mathcal{L}$.

Remarks.

1. The Control Theorem for fine Selmer groups is independent of the reduction type at p.
2. When $d = 1$, the Control Theorem is proved for *all* $\mathbb{Z}_p$-extensions by Wuthrich (2004). Moreover, the order of $\ker(r_{\mathcal{L}/L})$ and $\operatorname{coker}(r_{\mathcal{L}/L})$ are *bounded* independent of L.

Our Results

- Prove a very general Control Theorem for fine Selmer groups (without any hypothesis).

Our Results

- Prove a very general Control Theorem for fine Selmer groups (without any hypothesis).
- We can give growth estimates for the order of the kernel and cokernel when specializing to
  - multi $\mathbb{Z}_p$-extensions
  - multi false Tate extensions
  - trivializing extensions.

Our Results

- Prove a very general Control Theorem for fine Selmer groups (without any hypothesis).
- We can give growth estimates for the order of the kernel and cokernel when specializing to
  - multi $\mathbb{Z}_p$-extensions
  - multi false Tate extensions
  - trivializing extensions.
- Asymptotic growth formula in finite layers.*

*Thank you Antonio Lei!

Our Results: Multi $\mathbb{Z}_p$-Extension Case

Theorem

Let E be an elliptic curve defined over F, and $\mathcal{L} = F_\infty$ be a $\mathbb{Z}_p^d$-extension of F, with $d \geq 2$. Then the kernel and cokernel of the restriction map

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite. Furthermore,

$$\mathrm{ord}_p|\ker r_n| = O(n) \quad \textit{and} \quad \mathrm{ord}_p|\mathrm{coker}\, r_n| = O(p^{(d-1)n})^{*}.$$

Our Results: Multi $\mathbb{Z}_p$-Extension Case

Theorem

Let E be an elliptic curve defined over F, and $\mathcal{L} = F_\infty$ be a $\mathbb{Z}_p^d$-extension of F, with $d \geq 2$. Then the kernel and cokernel of the restriction map

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite. Furthermore,

$$\mathrm{ord}_p|\ker r_n| = O(n) \quad \textit{and} \quad \mathrm{ord}_p|\mathrm{coker}\, r_n| = O(p^{(d-1)n})^{*}.$$

*can do better if additional properties are known!

Application: Asymptotic Growth

For any finitely generated (not necessarily torsion) $\mathbb{Z}_p[\![G]\!]$-module, M, denote by $e(M)$ the p-exponent of the *torsion subgroup* of M.

Application: Asymptotic Growth

For any finitely generated (not necessarily torsion) $\mathbb{Z}_p[\![G]\!]$-module, M, denote by $e(M)$ the p-exponent of the *torsion subgroup* of M.

Corollary

Let E be an elliptic curve defined over F, and $\mathcal{L} = F_\infty$ be a $\mathbb{Z}_p^d$-extension of F, with $d \geq 2$. Then

$$e\left(R\left(E/F_n\right)\right) = \mu_G\left(\left(R\left(E/F_\infty\right)^\vee\right)\right)p^{dn} + O(np^{(d-1)n}).$$

Application: Asymptotic Growth

For any finitely generated (not necessarily torsion) $\mathbb{Z}_p[\![G]\!]$-module, M, denote by $e(M)$ the p-exponent of the *torsion subgroup* of M.

Corollary

Let E be an elliptic curve defined over F, and $\mathcal{L} = F_\infty$ be a $\mathbb{Z}_p^d$-extension of F, with $d \geq 2$. Then

$$e\left(R\left(E/F_n\right)\right) = \mu_G\left(\left(R\left(E/F_\infty\right)^\vee\right)\right)p^{dn} + O(np^{(d-1)n}).$$

Unfortunately, this does not automatically translate to an asymptotic growth formula for the fine Shafarevich-Tate group.

Our Results: Trivializing Extension (CM) Case

Theorem

Let E be an elliptic curve with complex multiplication defined over the number field, F. Suppose that $F_\infty = F\left(E[p^\infty]\right)$ and $G = \mathrm{Gal}(F_\infty/F)$ is uniform. Then the kernel and cokernel of the restriction maps

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite. Furthermore, the $\mathrm{ord}_p|\ker r_n| = O(n)^*$ *and* $\mathrm{ord}_p|\mathrm{coker}\, r_n| = O(n)$.

Our Results: Trivializing Extension (CM) Case

Theorem

Let E be an elliptic curve with complex multiplication defined over the number field, F. Suppose that $F_\infty = F\left(E[p^\infty]\right)$ and $G = \mathrm{Gal}(F_\infty/F)$ is uniform. Then the kernel and cokernel of the restriction maps

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite. Furthermore, the $\mathrm{ord}_p|\ker r_n| = O(n)^*$ *and* $\mathrm{ord}_p|\mathrm{coker}\, r_n| = O(n)$.

*If p is a prime of potential ordinary reduction, then $\mathrm{ord}_p|\ker r_n| = O(1)$.

Our Results: Trivializing Extension (non-CM) Case

Theorem

Let E be an elliptic curve without complex multiplication defined over F. Suppose that $F_\infty = F\left(E[p^\infty]\right)$ and $G = \mathrm{Gal}(F_\infty/F)$ is uniform. Then the kernel and cokernel of the restriction maps

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite. Further, the $\mathrm{ord}_p|\ker r_n| = O(n)^*$ *and* $\mathrm{ord}_p|\mathrm{coker}\, r_n| = O(np^{2n})$.

Our Results: Trivializing Extension (non-CM) Case

Theorem

Let E be an elliptic curve without complex multiplication defined over F. Suppose that $F_\infty = F\left(E[p^\infty]\right)$ and $G = \mathrm{Gal}(F_\infty/F)$ is uniform. Then the kernel and cokernel of the restriction maps

$$r_n : R\left(E/F_n\right) \longrightarrow R\left(E/F_\infty\right)^{G_n}$$

are finite. Further, the $\mathrm{ord}_p|\ker r_n| = O(n)^*$ *and* $\mathrm{ord}_p|\mathrm{coker}\, r_n| = O(np^{2n})$.

*If p is a prime of potential ordinary reduction, then $\mathrm{ord}_p|\ker r_n| = O(1)$.

Thank you!

Idea of the Proof

Consider the following fundamental diagram

$$
\begin{array}{ccccccc}
0 & \to & R(E/F_n) & \to & H^1\left(G_S(F_n),\ E[p^\infty]\right) & \to & \bigoplus_{v_n \in S(F_n)} H^1\left(F_{n,v_n},\ E[p^\infty]\right) \\
 & & \downarrow r_n & & \downarrow h_n & & \downarrow g_n \\
0 & \to & R\left(E/F_\infty\right)^{G_n} & \to & H^1\left(G_S(F_\infty),\ E[p^\infty]\right)^{G_n} & \to & \bigoplus_{w \in S(F_\infty)} H^1\left(F_{\infty,w},\ E[p^\infty]\right)^{G_n}
\end{array}
$$

with exact rows.