Some corollaries of Mazur's Control Theorem

July 16, 2008

Selmer and Thate-Shafarevich groups

Let E be an elliptic curve over a number field K and v a prime in K. Consider the commutative diagram below obtain by using Kummer sequences.

$$\begin{tikzcd}
0 \arrow[r] & E(K) \otimes (\mathbb{Q}/\mathbb{Z}) \arrow[r, "\kappa"] \arrow[d, "a_v"'] & H^1(K, E(\overline{K})_{tors}) \arrow[r, "\lambda"] \arrow[d, "b_v"'] & H^1(K, E(\overline{K})) \arrow[r] \arrow[d, "c_v"'] & 0 \\
0 \arrow[r] & E(K_v) \otimes (\mathbb{Q}/\mathbb{Z}) \arrow[r, "\kappa_v"] & H^1(K_v, E(\overline{K_v})_{tors}) \arrow[r, "\lambda_v"] & H^1(K_v, E(\overline{K_v})) \arrow[r] & 0
\end{tikzcd}$$

Selmer and Thate-Shafarevich groups

The Selmer group is defined by

$$\mathrm{Sel}_E(K) = \ker\left(H^1(K, E(\overline{K})_{tors}) \to \prod_v (H^1(K_v, E(\overline{K_v})_{tors})/\mathrm{im}(\kappa_v))\right).$$

The Tate-Shafarevich group is defined by

$$\text{Ш}_E(K) = \ker\left(H^1(K, E(\overline{K})) \to \prod_v H^1(K_v, E(\overline{K_v}))\right).$$

They fit into the exact sequence

$$0 \to E(K) \otimes (\mathbb{Q}/\mathbb{Z}) \to \mathrm{Sel}_E(K) \to \text{Ш}_E(K) \to 0.$$

Selmer and Thate-Shafarevich groups

The Selmer group is defined by

$$\mathrm{Sel}_E(K) = \ker\left(H^1(K, E(\overline{K})_{tors}) \to \prod_v (H^1(K_v, E(\overline{K_v})_{tors})/\mathrm{im}(\kappa_v))\right).$$

The Tate-Shafarevich group is defined by

$$\text{Ш}_E(K) = \ker\left(H^1(K, E(\overline{K})) \to \prod_v H^1(K_v, E(\overline{K_v}))\right).$$

They fit into the exact sequence

$$0 \to E(K) \otimes (\mathbb{Q}/\mathbb{Z}) \to \mathrm{Sel}_E(K) \to \text{Ш}_E(K) \to 0.$$

Selmer and Thate-Shafarevich groups

The Selmer group is defined by

$$\mathrm{Sel}_E(K) = \ker\left(H^1(K, E(\overline{K})_{tors}) \to \prod_v (H^1(K_v, E(\overline{K_v})_{tors})/\mathrm{im}(\kappa_v))\right).$$

The Tate-Shafarevich group is defined by

$$Ш_E(K) = \ker\left(H^1(K, E(\overline{K})) \to \prod_v H^1(K_v, E(\overline{K_v}))\right).$$

They fit into the exact sequence

$$0 \to E(K) \otimes (\mathbb{Q}/\mathbb{Z}) \to \mathrm{Sel}_E(K) \to Ш_E(K) \to 0.$$

Selmer and Thate-Shafarevich groups

- The p-primary part of $E(K) \otimes (\mathbb{Q}/\mathbb{Z})$ is simply $E(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$.
- And the p-primary part of $\mathrm{Sel}_E(K)$ is

$$\mathrm{Sel}_E(K)_p = \ker\left(H^1(K, E[p^\infty])) \to \prod_v (H^1(K_v, E[p^\infty]))/\mathrm{im}(\kappa_v))\right).$$

One natural question that arises in the arithmetic of elliptic curves is understanding the growth of the Mordell-Weil group. Which in light of the exact sequence above is the same as understanding the growth of the Selmer and Tate-Shafaverich groups of such curves.

Selmer and Thate-Shafarevich groups

- The p-primary part of $E(K) \otimes (\mathbb{Q}/\mathbb{Z})$ is simply $E(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$.
- And the p-primary part of $\mathrm{Sel}_E(K)$ is

$$\mathrm{Sel}_E(K)_p = \ker\left(H^1(K, E[p^\infty])) \to \prod_v (H^1(K_v, E[p^\infty]))/\mathrm{im}(\kappa_v))\right).$$

One natural question that arises in the arithmetic of elliptic curves is understanding the growth of the Mordell-Weil group. Which in light of the exact sequence above is the same as understanding the growth of the Selmer and Tate-Shafaverich groups of such curves.

Selmer and Thate-Shafarevich groups

- The p-primary part of $E(K) \otimes (\mathbb{Q}/\mathbb{Z})$ is simply $E(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$.
- And the p-primary part of $\mathrm{Sel}_E(K)$ is

$$\mathrm{Sel}_E(K)_p = \ker\left(H^1(K, E[p^\infty])) \to \prod_v (H^1(K_v, E[p^\infty]))/\mathrm{im}(\kappa_v))\right).$$

One natural question that arises in the arithmetic of elliptic curves is understanding the growth of the Mordell-Weil group. Which in light of the exact sequence above is the same as understanding the growth of the Selmer and Tate-Shafaverich groups of such curves.

The structure theorems of Λ-modules

Let $\Lambda = \mathbb{Z}_p[[T]]$, and $\mathfrak{m} = (p,\ T)$ the maximal ideal.

Theorem (Structure Theorem)

Let X be a finitely generated Λ-module. Then, there exists a Λ-module homomorphism

$$\varphi : X \to \Lambda^r \times \prod_{i=1}^{t} \Lambda/(f_i(T)^{e_i})$$

with finite kernel and cokernel, where $r \geq 0$, $f_1(T), \ldots, f_t(T)$ are irreducible elements of Λ, and $e_1, \ldots, e_t$ are positive integers. The parameter r, the prime ideals $(f_i(T))$ and their corresponding exponents e_i are uniquely determined by X.

The structure theorems of Λ-modules

Theorem (Nakayama)

Let X be and abelian pro-p group on which Γ acts continuously. We endow X with the resulting Λ-module structure. Then

1. $X = 0 \iff X/TX = 0 \iff X/\mathfrak{m}X = 0.$
2. *X is finitely generated as a Λ-module if and only if $X/\mathfrak{m}X$ is a finite dimensional $\mathbb{F}_p$-vectore space. The minimum number of generators of X as a Λ-module is $\dim_{\mathbb{F}_p}(X/\mathfrak{m}X)$.*
3. *If X/TX is finite, then X is a torsion Λ-module.*

Corollaries to Mazur's control theorem

In the rest of this talk, we make the following notations.

Notations.

- F is a number field.
- E is an elliptic curve over F
- $F_\infty = \bigcup_n F_n$ is a $\mathbb{Z}_p$-extension.

Theorem (Mazur)

Let p be a prime and assume that for every place $v \mid p$ in F, E has good ordinary reduction at v. Then the natural maps

$$\mathrm{Sel}_E(F_n)_p \to \mathrm{Sel}_E(F_\infty)_p^{\mathrm{Gal}(F_\infty/F_n)}.$$

have finite kernels and cokernels. Their orders are bounded as n tends to ∞.

Corollaries to Mazur's control theorem

In the rest of this talk, we make the following notations.

Notations.

- F is a number field.
- E is an elliptic curve over F
- $F_\infty = \bigcup_n F_n$ is a $\mathbb{Z}_p$-extension.

Theorem (Mazur)

Let p be a prime and assume that for every place $v \mid p$ in F, E has good ordinary reduction at v. Then the natural maps

$$\mathrm{Sel}_E(F_n)_p \to \mathrm{Sel}_E(F_\infty)_p^{\mathrm{Gal}(F_\infty/F_n)}.$$

have finite kernels and cokernels. Their orders are bounded as n tends to ∞.

Corollaries to Mazur's control theorem

Corollary

Let E be an elliptic curve defined over F. Let p be a prime and assume that for every place $v \mid p$ in F, E has good ordinary reduction at v. Assume that $\mathrm{Sel}_E(F)_p$ is finite. Then $\mathrm{Sel}_E(F_\infty)_p$ is Λ-cotorsion. Consequently, $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ is bounded as n varies.

Ingredients of the proof.

- Mazur's control theorem.
- Structure Theorem of Λ-modules.
- Nakayama's Lemma for Λ-modules.

Corollaries to Mazur's control theorem

Proof. The hypotheses of Mazur's control theorem (Theorem 4.1) imply that $\mathrm{Sel}_E(F_\infty)_p^\Gamma$ is finite.

Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. We can view it as a Λ-module (see Eduardo's talk). Consider the quotient X/TX.

Then, by construction, X/TX is the maximal quotient of X on which Γ acts trivially. So, by previous talks (Eduardo), it is the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p^\Gamma$. Hence, it is **finite**.

By the Nakayama's Lemma for Λ-module (Theorem 3.9), it follows that X is a finitely generated torsion Λ-module. Same as saying that $\mathrm{Sel}_E(F_\infty)_p$ is a cotorsion Λ-module.

Corollaries to Mazur's control theorem

Proof. The hypotheses of Mazur's control theorem (Theorem 4.1) imply that $\mathrm{Sel}_E(F_\infty)_p^\Gamma$ is finite.

Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. We can view it as a Λ-module (see Eduardo's talk). Consider the quotient X/TX.

Then, by construction, X/TX is the maximal quotient of X on which Γ acts trivially. So, by previous talks (Eduardo), it is the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p^\Gamma$. Hence, it is **finite**.

By the Nakayama's Lemma for Λ-module (Theorem 3.9), it follows that X is a finitely generated torsion Λ-module. Same as saying that $\mathrm{Sel}_E(F_\infty)_p$ is a cotorsion Λ-module.

Corollaries to Mazur's control theorem

Proof. The hypotheses of Mazur's control theorem (Theorem 4.1) imply that $\mathrm{Sel}_E(F_\infty)_p^\Gamma$ is finite.

Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. We can view it as a Λ-module (see Eduardo's talk). Consider the quotient X/TX.

Then, by construction, X/TX is the maximal quotient of X on which Γ acts trivially. So, by previous talks (Eduardo), it is the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p^\Gamma$. Hence, it is **finite**.

By the Nakayama's Lemma for Λ-module (Theorem 3.9), it follows that X is a finitely generated torsion Λ-module. Same as saying that $\mathrm{Sel}_E(F_\infty)_p$ is a cotorsion Λ-module.

Corollaries to Mazur's control theorem

Proof. The hypotheses of Mazur's control theorem (Theorem 4.1) imply that $\mathrm{Sel}_E(F_\infty)_p^\Gamma$ is finite.

Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. We can view it as a Λ-module (see Eduardo's talk). Consider the quotient X/TX.

Then, by construction, X/TX is the maximal quotient of X on which Γ acts trivially. So, by previous talks (Eduardo), it is the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p^\Gamma$. Hence, it is **finite**.

By the Nakayama's Lemma for Λ-module (Theorem 3.9), it follows that X is a finitely generated torsion Λ-module. Same as saying that $\mathrm{Sel}_E(F_\infty)_p$ is a cotorsion Λ-module.

Corollaries to Mazur's control theorem

Proof (cont'd). By the structure theorem of Λ-modules (Theorem 3.1), we see that $X/X_{\mathbb{Z}_p\text{-tors}} \cong \mathbb{Z}_p^\lambda$ for some $\lambda \geq 0$. And so

$$(\mathrm{Sel}_E(F_\infty)_p)_{div} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda.$$

Now, since the kernels of the maps in Theorem 4.1 are finite, it follows that

$$(\mathrm{Sel}_E(F_n)_p)_{div} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n},$$

for some integer $t_n \leq \lambda$.

By recalling that

$$E(F_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rank}_{\mathbb{Z}}(E_n)}$$

is a subgroup of $(\mathrm{Sel}_E(F_n)_p)_{div}$, we obtain that $\mathrm{rank}_{\mathbb{Z}}(E_n) \leq \lambda$ for all $n \geq 0$. □

Corollaries to Mazur's control theorem

Proof (cont'd). By the structure theorem of Λ-modules (Theorem 3.1), we see that $X/X_{\mathbb{Z}_p\text{-tors}} \cong \mathbb{Z}_p^{\lambda}$ for some $\lambda \geq 0$. And so

$$(\mathrm{Sel}_E(F_\infty)_p)_{div} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda}.$$

Now, since the kernels of the maps in Theorem 4.1 are finite, it follows that

$$(\mathrm{Sel}_E(F_n)_p)_{div} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n},$$

for some integer $t_n \leq \lambda$.

By recalling that

$$E(F_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rank}_{\mathbb{Z}}(E_n)}$$

is a subgroup of $(\mathrm{Sel}_E(F_n)_p)_{div}$, we obtain that $\mathrm{rank}_{\mathbb{Z}}(E_n) \leq \lambda$ for all $n \geq 0$. □

Corollaries to Mazur's control theorem

Proof (cont'd). By the structure theorem of Λ-modules (Theorem 3.1), we see that $X/X_{\mathbb{Z}_p\text{-tors}} \cong \mathbb{Z}_p^\lambda$ for some $\lambda \geq 0$. And so

$$(\mathrm{Sel}_E(F_\infty)_p)_{div} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda.$$

Now, since the kernels of the maps in Theorem 4.1 are finite, it follows that

$$(\mathrm{Sel}_E(F_n)_p)_{div} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n},$$

for some integer $t_n \leq \lambda$.

By recalling that

$$E(F_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rank}_{\mathbb{Z}}(E_n)}$$

is a subgroup of $(\mathrm{Sel}_E(F_n)_p)_{div}$, we obtain that $\mathrm{rank}_{\mathbb{Z}}(E_n) \leq \lambda$ for all $n \geq 0$. $\square$

Corollaries to Mazur's control theorem

The second corollary of the Mazur control theorem.

Corollary

Let E be an elliptic curve defined over F. Let p be a prime and assume that for every place $v \mid p$ in F, E has good ordinary reduction at v. Assume that both $E(F)$ and $\text{Ш}_E(F)_p$ are finite. Let F_∞/F be a $\mathbb{Z}_p$-extension. Then $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ is bounded for $n \geq 0$.

Proof. This follows from the first corollary and the fact that finiteness of of $E(F)$ and $\text{Ш}_E(F)_p$ is equivalent to that of $\mathrm{Sel}_E(F)_p$. $\square$

Corollaries to Mazur's control theorem

The second corollary of the Mazur control theorem.

Corollary

Let E be an elliptic curve defined over F. Let p be a prime and assume that for every place $v \mid p$ in F, E has good ordinary reduction at v. Assume that both $E(F)$ and $\text{Ш}_E(F)_p$ are finite. Let F_∞/F be a $\mathbb{Z}_p$-extension. Then $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ is bounded for $n \geq 0$.

Proof. This follows from the first corollary and the fact that finiteness of of $E(F)$ and $\text{Ш}_E(F)_p$ is equivalent to that of $\mathrm{Sel}_E(F)_p$. $\square$

Corollaries to Mazur's control theorem

The Tate-Shafarevich group is conjectured to be finite. Assuming this, the corollary below explains how it order grows in a $\mathbb{Z}_p$-extension.

Corollary

Let E be an elliptic curve defined over F. Let p be a prime and assume that for every place $v \mid p$ in F, E has good ordinary reduction at v. Let F_∞/F be a $\mathbb{Z}_p$-extension. Assume that both $\mathrm{Sel}_E(F_n)_p$ and $\text{Ш}_E(F_n)$ are finite for all n. Then there exist integers $\lambda, \mu \geq 0$ depending only on E and F_∞/F such that

$$|\text{Ш}_E(F_n)| = p^{\lambda n + \mu p^n + O(1)}, \text{ as } n \to \infty.$$

Corollaries to Mazur's control theorem

The following result is more refine than our first corollary. It explains that not only $\mathrm{rank}_{\mathbb{Z}}(E_n)$ can be unbounded in a $\mathbb{Z}_p$-extension, but that the growth is controlled by the p-primary part of the Selmer group.

Corollary

Let E be an elliptic curve defined over F. Let p be a prime and assume that for every place $v \mid p$ in F, E has good ordinary reduction at v. Let F_∞/F be a $\mathbb{Z}_p$-extension. Let $r = \mathrm{corank}_\Lambda(\mathrm{Sel}_E(F_\infty)_p)$. Then

$$\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_E(F_n)_p) = rp^n + O(1),$$

as $n \to \infty$. In particular, if $\text{Ш}_E(F_n)_p$ is finite for all n, then

$$\mathrm{rank}_{\mathbb{Z}}(E(F_n)) = rp^n + O(1), \text{ as } n \to \infty.$$