Root numbers & parity of local Iwasawa invariants

Suman Ahmed

Postdoctoral Fellow
IISER, Mohali

22nd December, 2016

(Joint work with Sudhanshu Shekhar & Aribam Chandrakant)

Contents

Introduction

Definition

An elliptic curve $E/\mathbb{Q}$ is the locus of an equation

$$E : y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{Q}$, together with a point ∞ (whose homogeneous coordinates are $[0 : 1 : 0]$), called the point at infinity and $-16\left(4a^3 + 27b^2\right) \neq 0$.

Introduction

Definition

An elliptic curve $E/\mathbb{Q}$ is the locus of an equation

$$E : y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{Q}$, together with a point ∞ (whose homogeneous coordinates are $[0 : 1 : 0]$), called the point at infinity and $-16(4a^3 + 27b^2) \neq 0$.

Mordell-Weil Theorem

Let E be an elliptic curve defined over a number field K. Then

$$E(K) \cong \mathbb{Z}^r \times T.$$

We call r the rank of E over K, and T the torsion subgroup of $E(K)$.

Torsion points on elliptic curves & Galois module structure

Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geq 2$ be an integer. Then

$$E[n](\bar{\mathbb{Q}}) \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

the isomorphism being one between abstract groups.

Torsion points on elliptic curves & Galois module structure

Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geq 2$ be an integer. Then

$$E[n](\bar{\mathbb{Q}}) \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

the isomorphism being one between abstract groups.

The absolute Galois group $G_{\bar{\mathbb{Q}}/\mathbb{Q}} \circlearrowright E[n]$, since if $[n]P = O$, then

$$[n](P^{\sigma}) = ([n]P)^{\sigma} = O^{\sigma} = O, \ \ \sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}$$

We thus obtain a mod n Galois representation

$$\bar{\rho}_{E,n} : G_{\bar{\mathbb{Q}}/\mathbb{Q}} \longrightarrow Aut(E[n]) \cong GL_2(\mathbb{Z}/n\mathbb{Z}),$$

where the later isomorphism involves choosing a basis for $E[n]$.

Iwasawa Theory

Iwasawa theory is the study of $\mathbb{Z}_p$-extensions of fields where $\mathbb{Z}_p$ denotes the set of p-adic integers.

If F/K is a $\mathbb{Z}_p$-extension, Galois theory shows that for each integer $n \geq 0$ there is a unique intermediate field $K_n, K \subset K_n \subset F$, with $\mathrm{Gal}(K_n/K) = \mathbb{Z}/p^n\mathbb{Z}$, and then $F = \bigcup K_n$.

Write $\Gamma = Gal(F/K)$ and

$$\Lambda = \mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[Gal(K_n/K)].$$

Theorem

Λ is isomorphic to a power series ring $\mathbb{Z}_p[[T]]$.

Iwasawa Modules

Definition

Two $\Lambda-$modules M and N are said to be *pseudo-isomorphic* $(M \sim N)$ if there is a homomorphism $M \longrightarrow N$ with finite kernel and co-kernel.

Iwasawa Modules

Definition

Two Λ−modules M and N are said to be *pseudo-isomorphic* $(M \sim N)$ if there is a homomorphism $M \longrightarrow N$ with finite kernel and co-kernel.

Structure theorem of finitely generated Λ−modules

Let M be a finitely generated Λ−module. Then

$$M \sim \Lambda^r \oplus (\oplus_{i=1}^{s} \Lambda/(p^{n_i})) \oplus (\oplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j}))$$

where $r, s, t, n_i, m_j \in \mathbb{N}$ and $f_j(T)$ are distinguished and irreducible. This decomposition is uniquely determined by M.

Selmer Group

Let v runs over all primes of K, archimedean and non-archimedean. If $[K:\mathbb{Q}] < \infty$ then K_v is the completion of K at v. Otherwise, we take K_v to be the union of the completions at v of all finite extensions of $\mathbb{Q}$ contained in K. Then the Selmer and Tate-Shafarevich groups for E over K are defined by

$$\mathrm{Sel}_E(K) := \ker\left(\mathrm{H}^1(K, E(\bar{K})_{\mathrm{tors}}) \longrightarrow \prod_v \mathrm{H}^1(K_v, E(\bar{K}_v))\right)$$

and

$$\text{Ш}_E(K) := \ker\left(\mathrm{H}^1(K, E(\bar{K})) \longrightarrow \prod_v \mathrm{H}^1(K_v, E(\bar{K}_v))\right)$$

Selmer Group

Let v runs over all primes of K, archimedean and non-archimedean. If $[K:\mathbb{Q}]<\infty$ then K_v is the completion of K at v. Otherwise, we take K_v to be the union of the completions at v of all finite extensions of $\mathbb{Q}$ contained in K. Then the Selmer and Tate-Shafarevich groups for E over K are defined by

$$\mathrm{Sel}_E(K) := \ker\left(\mathrm{H}^1(K, E(\bar{K})_{\mathrm{tors}}) \longrightarrow \prod_v \mathrm{H}^1(K_v, E(\bar{K}_v))\right)$$

and

$$Ш_E(K) := \ker\left(\mathrm{H}^1(K, E(\bar{K})) \longrightarrow \prod_v \mathrm{H}^1(K_v, E(\bar{K}_v))\right)$$

The p-primary subgroup of $\mathrm{Sel}_E(K)$ is given by

$$\mathrm{Sel}_E(K)_p = \ker\left(\mathrm{H}^1(K, E[p^\infty]) \longrightarrow \prod_v \mathrm{H}^1(K_v, E(\bar{K}_v))\right)$$

Selmer Group

The Selmer and Tate-Shafarevich groups for E over K fit into the following short exact sequence

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

Notice that

$$E(K) \otimes \mathbb{Q}/\mathbb{Z} \cong (\mathbb{Z}^r \times T) \otimes \mathbb{Q}/\mathbb{Z} \cong (\mathbb{Q}/\mathbb{Z})^r$$

Therefore finiteness of $Ш_E(K)$ and knowledge of the structure of $\mathrm{Sel}_E(K)$ would give an upper bound on the rank of E over K.

Iwasawa Invariants

Let p be a prime where E has good ordinary reduction. Let $\mathbb{Z}_p$ denote the ring of p-adic integers, and $\mathbb{Q}^{cyc}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ with $\Gamma = \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) \cong \mathbb{Z}_p$.

The *Pontryagin dual* $X(E/\mathbb{Q}^{cyc})$ of $Sel(E[p^\infty]/\mathbb{Q}^{cyc})$ is a finitely generated torsion Λ-module where $\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$. Hence, by the classification of finitely generated Λ-modules one has a pseudo isomorphism

$$X(E/\mathbb{Q}^{cyc}) \sim (\oplus_{i=1}^{s} \Lambda/(f_i(T)^{a_i})) \oplus (\oplus_{j=1}^{t} \Lambda/(p^{\mu_E^j}))$$

where $s, t, a_i, \mu_j \in \mathbb{N}$, f_i is distinguished and irreducible for all i.

Iwasawa Invariants

Let p be a prime where E has good ordinary reduction. Let $\mathbb{Z}_p$ denote the ring of p-adic integers, and $\mathbb{Q}^{cyc}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ with $\Gamma = \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) \cong \mathbb{Z}_p$.

The *Pontryagin dual* $X(E/\mathbb{Q}^{cyc})$ of $Sel(E[p^\infty]/\mathbb{Q}^{cyc})$ is a finitely generated torsion Λ-module where $\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$. Hence, by the classification of finitely generated Λ-modules one has a pseudo isomorphism

$$X(E/\mathbb{Q}^{cyc}) \sim (\oplus_{i=1}^{s} \Lambda/(f_i(T)^{a_i})) \oplus (\oplus_{j=1}^{t} \Lambda/(p^{\mu_E^j}))$$

where $s, t, a_i, \mu_j \in \mathbb{N}$, f_i is distinguished and irreducible for all i.

Since, the a_i's and the μ_E^j's are positive integers, one can define the algebraic Iwasawa invariants λ_E and μ_E by

$$\lambda_E = \sum_{i=1}^{s} a_i.deg(f_i(T)), \quad \mu_E = \sum_{j=1}^{t} \mu_E^j.$$

Motivation

For $i = 1, 2$, let

- E_i - Elliptic curve defined over $\mathbb{Q}$ with good and ordinary reduction at p.
- N_i - Conductor of E_i over F.
- $\overline{N_i}$ - The prime to p conductor of the Galois module $E_i[p]$.
- Σ - The finite set of primes of F containing the primes of bad reduction of E_1 and E_2, the infinite primes and the primes above p.
- Put
$$\Sigma_0 := \{v \in \Sigma \mid v \mid N_1/\overline{N_1} \text{ or } v \mid N_2/\overline{N_2}\}.$$
- S_{E_i} - Set of primes $v \in \Sigma_0$ such that E_i has split multiplicative reduction at v.
- $s_p(E_i/F)$ - Rank of the Pontryagin dual of $\mathrm{Sel}_p(E_i/F)$.

Motivation

Theorem (Shekhar, 2015)

Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ with good and ordinary reduction at an odd prime p. Further assume the following
(a) $E_1[p]$ is an irreducible $\mathrm{Gal}(\overline{F}/F)$-module.
(b) $\mu_p \subseteq F$ where μ_p denotes the group of p-th roots of unity.
(c) $\mathrm{Sel}_p(E_1/F_{cyc})[p]$ is finite where F_{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of F.
If $E_1[p] \cong E_2[p]$ as $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ modules then

$$s_p(E_1/F) + |S_{E_1}| \equiv s_p(E_2/F) + |S_{E_2}| \pmod 2.$$

Motivation

Theorem (Shekhar, 2015)

Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ with good and ordinary reduction at an odd prime p. Further assume the following
(a) $E_1[p]$ is an irreducible $\mathrm{Gal}(\overline{F}/F)$-module.
(b) $\mu_p \subseteq F$ where μ_p denotes the group of p-th roots of unity.
(c) $\mathrm{Sel}_p(E_1/F_{cyc})[p]$ is finite where F_{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of F.
If $E_1[p] \cong E_2[p]$ as $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ modules then

$$s_p(E_1/F) + \mid S_{E_1} \mid \equiv s_p(E_2/F) + \mid S_{E_2} \mid \pmod 2.$$

p-parity Conjecture

$$s_p(E/F) \equiv a(E/F) \pmod 2$$

where $a(E/F)$ denotes the order of zero of $L(E/F, s)$ (the Hasse-Weil L-function of E over F) at $s = 1$.

Proof

Definition of Imprimitive Σ_0–Selmer group

Let $\Sigma_0 \subset \Sigma \setminus \{$ primes above p and the infinite primes$\}$. Then

$$\mathrm{Sel}_p^{\Sigma_0}(E/F_{\mathrm{cyc}}) := \mathrm{Ker}\left(\mathrm{H}^1(F_\Sigma/F_{\mathrm{cyc}}, E[p^\infty]) \longrightarrow \prod_{l \in \Sigma - \Sigma_0} \mathcal{H}_v(F_{\mathrm{cyc}}, E[p^\infty])\right).$$

Proof

Definition of Imprimitive Σ_0−Selmer group

Let $\Sigma_0 \subset \Sigma \setminus \{$ primes above p and the infinite primes$\}$. Then

$$\mathrm{Sel}_p^{\Sigma_0}(E/F_{\mathrm{cyc}}) := \mathrm{Ker}\left(\mathrm{H}^1(F_\Sigma/F_{\mathrm{cyc}}, E[p^\infty]) \longrightarrow \prod_{l \in \Sigma - \Sigma_0} \mathcal{H}_v(F_{\mathrm{cyc}}, E[p^\infty])\right).$$

Under the assumptions (a) and (c),we have $\lambda_{E_1}^{\Sigma_0} = \lambda_{E_2}^{\Sigma_0}$.

For a prime $v \nmid p$ of F, let $\tau_{E_1}^{v}$ denote the $\mathbb{Z}_p$-rank of the Pontryagin dual of $\mathcal{H}_v(F_{\mathrm{cyc}}, E_1)$ where

$$\mathcal{H}_v(F_{\mathrm{cyc}}, E_1) := \prod_{w|v} \mathrm{H}^1(F_{\mathrm{cyc},w}, E_1[p^\infty]).$$

From [**Sh, Lemma 3.1**], we have

$$\lambda_{E_i}^{\Sigma_0} = \lambda_{E_i} + \sum_{v \in \Sigma_0} \tau_{E_i}^{v}, i = 1, 2.$$

Proof

Now for each $v \in \Sigma_0$, choose a prime w of F_{cyc} dividing v. Let P be the set consisting of all such w and

$$\sigma_{E_i}^{w} := \mathrm{corank}_{\mathbb{Z}_p} \mathrm{H}^1(F_{cyc,w}, E_i[p^\infty]).$$

Then [**Sh, Lemma 3.2**] implies

$$\lambda_{E_i}^{\Sigma_0} \equiv \lambda_{E_i} + \sum_{w \in P} \sigma_{E_i}^{w} \pmod 2, \ i = 1, 2.$$

Therefore

$$\lambda_{E_1} + \sum_{w \in P} \sigma_{E_1}^{w} \equiv \lambda_{E_2} + \sum_{w \in P} \sigma_{E_2}^{w} \pmod 2.$$

From the comparisons of $\sigma_{E_i}^{w}, i = 1, 2$, we have

$$\lambda_{E_1} + | S_{E_1} | \equiv \lambda_{E_2} + | S_{E_2} | \pmod 2.$$

Proof

Now for each $v \in \Sigma_0$, choose a prime w of F_{cyc} dividing v. Let P be the set consisting of all such w and

$$\sigma_{E_i}^{w} := \mathrm{corank}_{\mathbb{Z}_p} \mathrm{H}^1(F_{cyc,w}, E_i[p^\infty]).$$

Then [**Sh, Lemma 3.2**] implies

$$\lambda_{E_i}^{\Sigma_0} \equiv \lambda_{E_i} + \sum_{w \in P} \sigma_{E_i}^{w} \pmod 2, \; i = 1, 2.$$

Therefore

$$\lambda_{E_1} + \sum_{w \in P} \sigma_{E_1}^{w} \equiv \lambda_{E_2} + \sum_{w \in P} \sigma_{E_2}^{w} \pmod 2.$$

From the comparisons of $\sigma_{E_i}^{w}, i = 1, 2$, we have

$$\lambda_{E_1} + | S_{E_1} | \equiv \lambda_{E_2} + | S_{E_2} | \pmod 2.$$

Theorem (Guo)

Let E be an elliptic curve defined over F and suppose that the Pontryagin dual of $\mathrm{Sel}_p(E_1/F_{cyc})$ is $\Lambda-$ torsion. Then

$$s_p(E/F) \equiv \lambda_E \pmod 2.$$

Counterexamples

Assume $\mu_p \nsubseteq F$. Then for $p = 3$, we have the following counterexamples to the above theorem.

Example 1 :

$E_1 : y^2 + y = x^3 - x^2 - 10x - 20, \ \ (11a1)$

$E_2 : y^2 + xy = x^3 + x^2 - 2x - 7, \ \ (121c1)$

E_1 has split multiplicative reduction while E_2 has additive reduction at 11. Both have rank 0 and $E_1[3] \cong E_2[3]$.

Counterexamples

Assume $\mu_p \not\subseteq F$. Then for $p = 3$, we have the following counterexamples to the above theorem.

Example 1 :

$E_1 : y^2 + y = x^3 - x^2 - 10x - 20, \;\; (11a1)$

$E_2 : y^2 + xy = x^3 + x^2 - 2x - 7, \;\; (121c1)$

E_1 has split multiplicative reduction while E_2 has additive reduction at 11. Both have rank 0 and $E_1[3] \cong E_2[3]$.

Example 2 :

$E_3 : y^2 = x^3 - x^2 - 4133x + 186637, \;\; (4400m2)$

$E_4 : y^2 = x^3 - x^2 - 1008x + 48512, \;\; (48400ch1)$

E_3 has non-split multiplicative reduction at 11 and additive reduction at 2,5 while E_4 has additive reduction at 2,5,11. E_3 and E_4 have rank 0 and 1 respectively and $E_3[3] \cong E_4[3]$.

Main Theorem 1 (for ordinary elliptic curves)

Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ with good and ordinary reduction at an odd prime p. We further assume the following.
(a) $E_1[p]$ is an irreducible $\mathrm{Gal}(\overline{F}/F)$-module.
(b) $\mathrm{Sel}_p(E_1/F_{cyc})[p]$ is finite.
If $E_1[p] \cong E_2[p]$ as $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ modules then

$$s_p(E_1/F) + | S_{E_1} | \equiv s_p(E_2/F) + | S_{E_2} | + | T | \pmod{2}$$

where T denotes the set of primes v of F in Σ_0 such that $\mu_p \not\subset F_v$, one of the elliptic curves has multiplicative reduction and other has additive reduction at v.

Main Theorem 1 (for ordinary elliptic curves)

Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ with good and ordinary reduction at an odd prime p. We further assume the following.
(a) $E_1[p]$ is an irreducible $\mathrm{Gal}(\overline{F}/F)$-module.
(b) $\mathrm{Sel}_p(E_1/F_{cyc})[p]$ is finite.
If $E_1[p] \cong E_2[p]$ as $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ modules then

$$s_p(E_1/F) + \mid S_{E_1} \mid \equiv s_p(E_2/F) + \mid S_{E_2} \mid + \mid T \mid \pmod{2}$$

where T denotes the set of primes v of F in Σ_0 such that $\mu_p \not\subset F_v$, one of the elliptic curves has multiplicative reduction and other has additive reduction at v.

Note that T can be non-empty only when $p = 3$.

Supersingular elliptic curves

Definition

For $n \geq 0$, we define $\mathrm{Sel}_p^{\pm}(E/F_n)$ to be the kernel of

$$\mathbf{f_n} : \mathrm{H}^1(F_n, A) \longrightarrow \prod_v \frac{\mathrm{H}^1(F_{n,v}, A)}{E^{\pm}(F_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \tag{1}$$

and $\mathrm{Sel}_p^{\pm}(E/F_{cyc}) := \varinjlim_n \mathrm{Sel}_p^{\pm}(E/F_n)$. Here v ranges over all places of F_n, $F_{n,v}$ is the completion of F_n at v and the map is induced by the restrictions of the Galois cohomology groups. For notational convenience, let $F_{-1,v} = F_{0,v} = F_v$. Then

$$E^{+}(F_{n,v}) := \{P \in E(F_{n,v}) \,|\, \mathrm{Tr}_{n/m+1} P \in E(F_{m,v}) \text{ for even } m \ (0 \leq m < n)\}$$

$$E^{-}(F_{n,v}) := \{P \in E(F_{n,v}) \,|\, \mathrm{Tr}_{n/m+1} P \in E(F_{m,v}) \text{ for odd } m \ (-1 \leq m < n)\}$$

where $\mathrm{Tr}_{n/m} : E(F_{n,v}) \longrightarrow E(F_{m,v})$ denotes the trace map for $n \geq m$.

Remark

For $n = 0$, we have $E^-(F_v) = E(F_v)$ hence $\mathrm{Sel}_p^-(E/F) = \mathrm{Sel}_p(E/F)$.

Assumption

For $E = E_1$ or E_2

(i) $E[p]$ is an irreducible $Gal(\overline{F}/F)$-module.

(ii) $\mathrm{Sel}_p^-(E/F_{cyc})[p]$ is a finite group.

Remark

For $n = 0$, we have $E^-(F_v) = E(F_v)$ hence $\mathrm{Sel}_p^-(E/F) = \mathrm{Sel}_p(E/F)$.

Assumption

For $E = E_1$ or E_2

(i) $E[p]$ is an irreducible $Gal(\overline{F}/F)$-module.

(ii) $\mathrm{Sel}_p^-(E/F_{cyc})[p]$ is a finite group.

Main Theorem 2 (for supersingular elliptic curves)

Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ with good, supersingular reduction at an odd prime p and $a_p = 0$. We further assume the following.

(a) $E_1[p]$ is an irreducible $\mathrm{Gal}(\overline{F}/F)$-module.

(b) $\mathrm{Sel}_p^-(E_1/F_{cyc})[p]$ is finite.

(c) p splits completely over F.

If $E_1[p] \cong E_2[p]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ modules then

$$s_p(E_1/F) + |S_{E_1}| \equiv s_p(E_2/F) + |S_{E_2}| + |T| \pmod 2$$

Guo's theorem for supersingular elliptic curves

Theorem

Let E be an elliptic curve defined over a number field F with good, supersingular reduction at primes dividing p. Assume that $\mathrm{Sel}_p^-(E/F_{cyc})$ is Λ-cotorsion. Then

$$corank_{\mathbb{Z}_p}(\mathrm{Sel}_p^-(E/F)) \equiv \lambda_E^- (mod\ 2)$$

where λ_E^- denotes the Iwasawa λ-invariant of the Pontryagin dual of $\mathrm{Sel}_p^-(E/F_{cyc})$.

Corollary

Let E be an elliptic curve defined over a number field F with good, supersingular reduction at primes dividing p. Assume that $\mathrm{Sel}_p^-(E/F_{cyc})$ is Λ-cotorsion. Then

$$s_p(E/F) \equiv \lambda_E^- (mod\ 2)$$

Comparison of local Iwasawa invariants

Theorem (Hachimori-Matsuno)

Let $p \neq \ell$ be prime numbers. Let k be a finite extension of $\mathbb{Q}_\ell$ containing μ_p. Put $k_\infty = k(\mu_{p^\infty})$. Let E be an elliptic curve defined over k. Then we have the following.
(1) If E has good reduction over k_∞, then

$$E(k_\infty)_{p^\infty} \cong \begin{cases} E_{p^\infty} & \text{if } E(k)_p \neq 0, \\ 0 & \text{if } E(k)_p = 0. \end{cases}$$

(2) If E has split multiplicative reduction over k_∞, then there exists an element $q \in k^\times$ and $m \in \mathbb{Z}^+ \cup \{0\}$ s.t. $E(k_\infty)_{p^\infty}$ is isomorphic to the subgroup of $k_\infty^\times / q^{\mathbb{Z}}$ generated by μ_{p^∞} and q^{1/p^m} as a $\mathrm{Gal}(k_\infty/k_1)$-module.

(3) If E has non-split multiplicative or additive reduction over k_∞, then $E(k_\infty)_{p^\infty}$ is finite. Moreover, if $p \geq 5$ or E has non-split multiplicative reduction, then $E(k_\infty)_{p^\infty} = 0$.

Comparison of local Iwasawa invariants

Lemma 1 (Good – Good)

Let v be a finite prime of F with $v \nmid p$ and w be a prime of F_{cyc} with $w \mid v$. Let E_1 and E_2 be two elliptic curves with good reduction at v and $E_1[p] \cong E_2[p]$, then $\sigma_{E_1}^{w} = \sigma_{E_2}^{w}$.

For an elliptic curve E over F, consider the following exact sequence of Galois modules

$$0 \longrightarrow E[p] \longrightarrow E[p^\infty] \xrightarrow{p} E[p^\infty] \longrightarrow 0$$

where the map p denotes multiplication by p. From the long exact sequence of Galois cohomology w.r.t. $G = \mathrm{Gal}(\overline{F}_v/F_{cyc,w})$, we get the following exact sequence

$$0 \longrightarrow \frac{\mathrm{H}^0(G, E[p^\infty])}{p\mathrm{H}^0(G, E[p^\infty])} \longrightarrow \mathrm{H}^1(G, E[p]) \longrightarrow \mathrm{H}^1(G, E[p^\infty])[p] \longrightarrow 0$$

- Since E_i has good reduction at $v, \mathrm{H}^0(G, E_i[p^\infty])$ is divisible for $i = 1, 2$.
- $\mathrm{H}^1(G, E[p^\infty])$ is divisible, therefore

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{H}^1(G, E[p^\infty]) = \dim_{\mathbb{F}_p} \mathrm{H}^1(G, E[p^\infty])[p].$$

Comparison of local Iwasawa invariants

Lemma 3 (Good – Additive)

(1) Let v be a finite prime of F with $v \nmid p$. Then it is not possible to have elliptic curves E_1 and E_2 such that E_1 has good reduction at v, E_2 has additive reduction at v and $E_1[p] \cong E_2[p]$.

Comparison of local Iwasawa invariants

Lemma 3 (Good – Additive)

(1) Let v be a finite prime of F with $v \nmid p$. Then it is not possible to have elliptic curves E_1 and E_2 such that E_1 has good reduction at v, E_2 has additive reduction at v and $E_1[p] \cong E_2[p]$.

Assume E has multiplicative reduction at p and v be a finite prime of F with $v \nmid p$. Let $\delta : G_v/I_v \longrightarrow \{\pm 1\}$ be the unique non-trivial unramified quadratic character of G_v if E has non-split multiplicative reduction, and let δ be the trivial character if E has split multiplicative reduction. Then we have

$$\rho_{E,p}|_{G_v} \sim \begin{pmatrix} \epsilon_p & * \\ 0 & 1 \end{pmatrix} \otimes \delta$$

where ϵ_p is the p-adic cyclotomic character and

$$\overline{\rho}_{E,p}|_{G_v} \sim \begin{pmatrix} \overline{\epsilon_p} & \psi \\ 0 & 1 \end{pmatrix} \otimes \delta.$$

Comparison of local Iwasawa invariants

Lemma 4 (Multiplicative – Additive)

Let $p \geq 5$ and v be a finite prime of F with $v \nmid p$. Then it is not possible to have elliptic curves E_1 and E_2 such that E_1 has multiplicative reduction at v, E_2 has additive reduction at v and $E_1[p] \cong E_2[p]$.

Proof : First, suppose that E_1 has split multiplicative reduction at v. Let $F' := F_v(\mu_p)$ and $G'' := \mathrm{Gal}(\overline{F}_v/F'_{cyc,w})$. Since F' is unramified outside p, the reduction type at v does not change for E_1 and E_2 over F'. Since $p \geq 5$, from [**HM**] we have $E_2[p^\infty](F_v(\mu_{p^\infty})) = 0$ hence $E_2(F'_{cyc,w})[p] = 0$. Now it follows from the above representation that

$$\overline{\rho}_{E_1,p}\,|_{G''} \sim \begin{pmatrix} 1 & \psi \\ 0 & 1 \end{pmatrix}$$

which implies $E_1(F'_{cyc,w})[p] \neq 0$, a contradiction to the fact that $E_1[p] \cong E_2[p]$. Hence it is not possible to have elliptic curves E_1 and E_2 with one having split multiplicative reduction and other having additive reduction at v.

Root number

- Let $E/\mathbb{Q}$ be an elliptic curve of conductor N.
- Let $L(s,E) := \prod_{p\nmid N}(1-a_p p^{-s}+p^{-2s})^{-1}\prod_{p\mid N}(\cdots)$ be the L-function attached to E.
- Let $\Lambda_E(s) = (2\pi)^{-s}\Gamma(s)N^{s/2}L(s,E)$.

Then by the Modularity Theorem,

$$\Lambda_E(s) = w(E)\Lambda_E(2-s), \quad w(E) = \pm 1.$$

Root number

- Let $E/\mathbb{Q}$ be an elliptic curve of conductor N.
- Let $L(s,E) := \prod_{p\nmid N}(1-a_p p^{-s}+p^{-2s})^{-1}\prod_{p|N}(\cdots)$ be the L-function attached to E.
- Let $\Lambda_E(s) = (2\pi)^{-s}\Gamma(s)N^{s/2}L(s,E)$.

Then by the Modularity Theorem,

$$\Lambda_E(s) = w(E)\Lambda_E(2-s), \quad w(E) = \pm 1.$$

Theorem

Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ with good reduction at an odd prime p and $E_1[p] \cong E_2[p]$. Then

$$\frac{w(E_1/F)}{w(E_2/F)} = (-1)^{|S_{E_1}|-|S_{E_2}|+|T|}. \tag{2}$$

Root number

Corollary

Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ with good reduction at p and $E_1[p] \cong E_2[p]$. Then under the assumptions of main theorem 1 (E_i have ordinary reduction at p) or main theorem 2 (E_i have supersingular reduction at p), we have

$$\frac{w(E_1/F)}{w(E_2/F)} = \frac{(-1)^{s_p(E_1/F)}}{(-1)^{s_p(E_2/F)}}$$

Root number

Corollary

Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ with good reduction at p and $E_1[p] \cong E_2[p]$. Then under the assumptions of main theorem 1 (E_i have ordinary reduction at p) or main theorem 2 (E_i have supersingular reduction at p), we have

$$\frac{w(E_1/F)}{w(E_2/F)} = \frac{(-1)^{s_p(E_1/F)}}{(-1)^{s_p(E_2/F)}}$$

In this context, we also recall the *p-parity conjecture* which states that for every elliptic curve E defined over F,

$$w(E/F) = (-1)^{s_p(E/F)}.$$

The above corollary implies that if the p-parity conjecture is true for one of the congruent elliptic curves then it is also true for the other elliptic curve.

Thank You