The Iwasawa Main Conjecture for Elliptic Curves at Supersingular Primes

elliptic curve: $E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{Q}$.

$p > 2$ a prime of good reduction

We say p is ordinary if $p \nmid a_p(E) = p + 1 - \#E(\mathbb{F}_p)$. It is supersingular if $p \mid a_p$.

Iwasawa theory is a connection between algebra and analysis.

Algebra:

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

finite?

$$E(\mathbb{Q}) \otimes \mathbb{Q}/\mathbb{Z} \cong (\mathbb{Q}/\mathbb{Z})^r.$$

Analysis:

$$L(E,s) = \prod_{p \text{ good}} (1 - a_p(E) p^{-s} + p^{1-2s})^{-1} \prod_{p \text{ bad}} L_p(s,E).$$

Conjecture (BSD):

1) $\mathrm{ord}_{s=1} L(E,s) = r$

2) $$\frac{L^{(r)}(E,1)}{\Omega_E \, r!} = \frac{\mathrm{Reg} \cdot \mathrm{Tam}}{\#E(\mathbb{Q})_{tors}^2} \#Ш(E/\mathbb{Q}).$$

Known:

$$\mathrm{ord}_{s=1} L(E,s) = \begin{cases} 0 \\ 1 \end{cases} \iff r = \begin{cases} 0 \\ 1 \end{cases} \text{ and } \#Ш(E/\mathbb{Q}) < \infty$$

"$\Rightarrow$" Coates-Wiles, Gross-Zagier, Kolyvagin

"$\Leftarrow$" Rubin, Skinner-Urban, W. Zhang

In the case $r = \begin{cases} 0 \\ 1 \end{cases}$, Iwasawa Theory at p $\Rightarrow$ $$\left| \frac{L^{(r)}(E,1)}{\Omega_E \, r!} \right|_p = \left| \frac{\#Ш(E/\mathbb{Q}) \, R_E \, \mathrm{Tam}_E}{\#E(\mathbb{Q})_{tors}^2} \right|_p$$

Iwasawa Theory for elliptic curves

$$
\begin{tikzcd}
\mathbb{Q}_\infty \arrow[d, dash] \arrow[dd, dash, bend right, "\cong \mathbb{Z}_p"'] \\
\mathbb{Q}_n \arrow[d, dash, "\mathbb{Z}/p^n\mathbb{Z}"] \\
\mathbb{Q}
\end{tikzcd}
$$

Now consider

$$0 \to \underbrace{E(\mathbb{Q}_n)\otimes \mathbb{Q}_p/\mathbb{Z}_p}_{\cong\, (\mathbb{Q}_p/\mathbb{Z}_p)^r} \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n) \to Ш_{p^\infty}(E/\mathbb{Q}_n) \to 0$$

Now take Pontryagin dual of inverse limit: $X = \left(\varprojlim_n \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)\right)^\vee$.

We have X is a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$-module. One has $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] \cong \mathbb{Z}_p[[T]]$.

$\Lambda = \mathbb{Z}_p[[T]]$ is power series ring of p-adic analytic functions.

<u>Fact:</u> If a module M is f.g. torsion as a Λ-module, then $\exists$ a short exact sequence

$$0 \to \bigoplus_i \Lambda/f_i\Lambda \to M \to (\text{finite}) \to 0.$$

<u>Def:</u> The char. ideal of M is $\mathrm{char}_\Lambda(M) = (\prod f_i) \subset \Lambda$.

An Iwasawa main conjecture is an equality $\mathrm{char}_\Lambda(M) \overset{?}{=} (\mathcal{L}_p) \subset \Lambda$ where $\mathcal{L}_p$ is a p-adic L-function.

① The case $p \nmid a_p(E)$.

<u>Thm (Kato):</u> X is f.g. torsion as a Λ-module.

On the analysis side; $\exists$ $\mathcal{L}_\alpha(T) \in \Lambda\otimes\mathbb{Q}$ (Mazur & Swinnerton-Dyer) so that $\mathcal{L}_\alpha(\zeta_{p^n}) = \dfrac{L(E, \psi_{p^{n+1}}, 1)}{\alpha^n(\cdots)}$

where α is the unit root of $y^2 - a_p(E)y + p$.

<u>Main Conjecture:</u> $(\mathcal{L}_\alpha) = \mathrm{char}_\Lambda(X)$.

Status:	$(\mathcal{L}_\#) \subset \mathrm{char}_\Lambda X^*$	Method	$\mathrm{char}_\Lambda(X^*) \subset (\mathcal{L}_\#)$	Method
$p\nmid a_p(E)$	Kato (1990's, 2000's)	Euler systems	Skinner-Urban ('14)	Eisenstein series congruences
$a_p(E)=0$	Kobayashi (2003)		Wan ('14)	E.S. + Euler systems of Kings & Loeffler + Zerbes
$p\mid a_p(E)$	S. ('12)		S ('15)	

② The case $p \mid a_p(E)$.

X is still f.g., but it is not torsion.

$\exists \mathcal{L}_\alpha, \mathcal{L}_\beta \in \Lambda \otimes \overline{\mathbb{Q}}_p$ satisfying right properties. (Amice & Vélu, Višik).

<u>Solutions:</u>

always true when $p \geq 5$ by $|a_p(E)| \leq 2\sqrt{p}$.

algebra: <u>Thm (Kobayashi $a_p = 0$)</u> $\exists$ appropriate $X^{\#}, X^{b}$ which are f.g. torsion Λ modules. (comes from "half" the rational points)

Can be generalized to $p \mid a_p(E)$. (S.)

Analysis: <u>Thm (Pollack $a_p(E)=0$, S. $p \mid a_p(E)$)</u>. $\exists \mathcal{L}_\#, \mathcal{L}_b \in \Lambda$ so that

$(\mathcal{L}_\alpha, \mathcal{L}_\beta) = (\mathcal{L}_\#, \mathcal{L}_b) \times \mathcal{L}og$ where $\mathcal{L}og$ explicit 2×2 matrix.

<u>Main Conjecture:</u> do $\mathrm{char}_\Lambda(X^{\#}) = (\mathcal{L}_\#)$ in Λ?

$\mathrm{char}_\Lambda(X^{b}) = (\mathcal{L}_b)$ in Λ?

(these are equivalent so one only need one of these.)

<u>Theorem:</u> $E/\mathbb{Q}$ elliptic curve, $p>2$ supersingular. N_E square-free, $Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow Aut(E[p])$,

then $\mathrm{char}_\Lambda(X^{\#}) = (\mathcal{L}_\#)$ and $\mathrm{char}_\Lambda(X^{b}) = (\mathcal{L}_b)$.

<u>Cor:</u> If $L(E,1) \neq 0$ and p and E satisfy the conditions in the theorem,

then $\left|\frac{L(E,1)}{\Omega}\right|_p = \left|\#Ш(E/\mathbb{Q}) \, Tam(E/\mathbb{Q})\right|_p$ (as predicted by BSD. other terms p-adically trivial in this case.)

<u>Cor:</u> BSD leading term formula holds up to a p-adic unit in the rank 1 case. (This depends on emerging work of Jetchev, Skinner, Wan.)

Sprung
10-1-15
p. 4

Other Applications

Miracle Theorem (Kato-Rohrlich): $r_n = \mathrm{rk}\, E(\mathbb{Q}_n)$

$$r_\infty = \lim_{n\to\infty} r_n < \infty.$$

Q: Bounded by what?

A: ($p \nmid a_p(E)$) $\mathrm{char}_\Lambda X = (p^\mu(X^\lambda + b_{\lambda-1}X^{\lambda-1} + \dots + b_1 X + b_0))$ with $b_i \in p\mathbb{Z}_p$. Then $r_\infty \le \lambda$. One also has $r \le r_\infty$, so using lots of primes one hopefully gets a good bound for r. (Mazur's idea).

($p \mid a_p(E)$) algebraic upper bound estimate as hand.

$\underset{\text{M.C.}}{\Leftrightarrow}$ analytic upper bound.

Thm: Let $\nu_\#$ be the ~~smallest~~ largest odd integer n so that

$q_n^\# + \lambda_\# \ge p^n - p^{n-1}$ where $\lambda_\# = \#$ of zeroes of $\mathcal{L}_\#$

and $\nu_\flat$ be the ~~smallest~~ largest even integer n so that

$q_n^\flat + \lambda_\flat \ge p^n - p^{n-1}$ where $\lambda_\flat = \#$ of zeroes of $\mathcal{L}_\flat$

$q_n^\# := p^{n-1} - p^{n-2} + \dots + p^2 - p$ (Kurihara terms) (odd)

$q_n^\flat := p^{n-1} - p^{n-2} + \dots + p - 1$. (even).

$\nu = \max(\nu_\#, \nu_\flat)$. Then $r_\infty \le \min(\lambda_\# + q_\nu^\#, \lambda_\flat + q_\nu^\flat)$.

Example: E37A $p = 3$. $a_3(E) = -3$.

$r = 1$. $\lambda_\# = 5$

$r_\infty = 7$ $\lambda_\flat = 1$.

$$r_\infty = 7 \le \min(5+3-1, 1+3^2-3)$$

Q: When does the rank jump?

$r = r_0 = 1$ $r_1 = 1$

$r_2 = 7$

Conj: $\lambda_\# \equiv \lambda_\flat \pmod 2$

Sketch of Proof of MC: Start w/ imag. quad. field K s.t. $p = \mathfrak{p}\bar{\mathfrak{p}}$ splits.

$$\begin{array}{l} K_\infty \\ \big| \ \mathbb{Z}_p^2\text{-ext.} \\ K \end{array} \qquad \left(\begin{array}{l} 2 \text{ MC's over } \mathbb{Q}. \\ \mathrm{char}(X^\#) \overset{?}{=} (\mathcal{L}_\#) \\ \qquad \supseteq \text{known.} \end{array} \right)$$

$$\Updownarrow$$

cond at $\mathfrak{p}$

cond at $\bar{\mathfrak{p}}$.

$$\left(\begin{array}{l} 4 \text{ MC. over } K \\ \mathrm{char}(X^{\#\#}) \overset{?}{=} (\mathcal{L}^{\#\#}) \\ \mathrm{char}(X^{\#\flat}) \overset{?}{=} (\mathcal{L}^{\#\flat}) \\ \vdots \end{array} \right)$$

$$\left(\begin{array}{c} (X^{\text{Greenberg}})^{MC} = (\mathcal{L}_p^{\text{Greenberg}}) \\ \uparrow \subseteq \end{array} \right)$$

Wan's $GU(3,1)$ - Eisenstein series method.

Tools to connect these: $(\Delta_\alpha, \Delta_\beta)$ Euler system of Kings, Loeffler-Zerbes.

This knows $\dfrac{L(E,\psi,1)}{(\ldots)}$ where $\psi : \mathrm{Gal}(K_\infty/K) \to \mathbb{C}^\times$.

It also knows $\mathcal{L}_p^{\text{Greenberg}}$.

These Euler systems sit in H^1 (where this is a rk 2 Λ_K-module $\otimes$ bad ring)

$\cong \mathbb{Z}_p[[X,Y]]$

One then must generalize the construction of Kobayashi of certain

Coleman maps