The GL_2 main conjecture for elliptic curves without complex multiplication

by Otmar Venjakob

Arithmetic of elliptic curves

E elliptic curve over $\mathbb{Q}$:

$$E : y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6, \;\; A_i \in \mathbb{Z}.$$

$$E(K) = \text{ ?}$$
for number fields, local fields, finite fields K

l any prime,
$\widetilde{E}$ reduction of E mod l,

$\#\widetilde{E}(\mathbb{F}_l) =: 1 - a_l + l$

Hasse-Weil L-function of E :

$$L(E/\mathbb{Q}, s) := \prod_l (1 - a_l l^{-s} + \epsilon(l) l^{1-2s})^{-1}, \; s \in \mathbb{C}, \; \Re(s) > \frac{3}{2},$$

where $\epsilon(l) := \begin{cases} 1 & E \text{ has good reduction at } l \\ 0 & \text{otherwise} \end{cases}$

Mordell-Weil Theorem

$E(\mathbb{Q})$ is a finitely generated abelian group

Birch & Swinnerton-Dyer Conjecture

I. $r := \text{ord}_{s=1} L(E/\mathbb{Q}, s) = \text{rk}_{\mathbb{Z}} E(\mathbb{Q})$

II. $\lim_{s \to 1} (s-1)^r L(E/\mathbb{Q}, s) = \Omega_+ R_E \frac{\# Ш(E/\mathbb{Q})}{(\# E(\mathbb{Q})_{tors})^2} \prod_l c_l$

$Ш(E/\mathbb{Q})$	Tate-Shafarevich group
$R_E = \det(< P_i, P_j >)_{i,j}$	regulator of E
ω	Néron Differential
$\Omega_+ = \int_{\gamma^+} \omega$	real period of E
$c_l = [E(\mathbb{Q}_l) : E^{ns}(\mathbb{Q}_l)]$	Tamagawa-number at l

The Selmer group of E

Assumption: $p \geq 5$ prime such that E has *good ordinary* reduction at p, i.e. $\#\widetilde{E}(\overline{\mathbb{F}_p})[p] = p$.

For any finite extension $K/\mathbb{Q}$ we have the (p-primary) *Selmer group* $Sel(E/K)$

$$0 \longrightarrow E(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow Sel(E/K) \longrightarrow Ш(E/K)(p) \longrightarrow 0$$

Thus, assuming $\#Ш(E/K) < \infty$, it holds for the Pontryagin dual of the Selmer group

$$Sel(E/K)^{\vee} := \mathrm{Hom}(Sel(E/K), \mathbb{Q}_p/\mathbb{Z}_p),$$

that

$$\mathrm{rk}_{\mathbb{Z}} E(K) = \mathrm{rk}_{\mathbb{Z}_p} Sel(E/K)^{\vee}$$

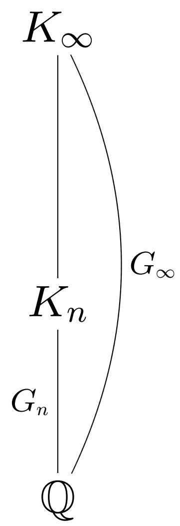
Towers of number fields

$K_n := \mathbb{Q}(E[p^n]), \quad 1 \leq n \leq \infty,$

$G_n := G(K_n/\mathbb{Q}) \quad G := G_\infty$

$G \subseteq GL_2(\mathbb{Z}_p)$ closed subgroup

i.e. a p-**adic Lie group**



$X(E/K_n) := Sel(E/K_n)^\vee$ is a compact $\mathbb{Z}_p[G_n]$-module

$X := X(E/K_\infty) := \varprojlim_n Sel(E/K_n)^\vee$ is a finitely generated $\Lambda(G)$-module, where

$$\Lambda(G) = \varprojlim_n \mathbb{Z}_p[G_n]$$

denotes the **Iwasawa algebra** of G,

a noehterian *possibly non-commutative* ring.

Twisted L-functions

Irr(G_n) irreducible representations of G_n, realized over a number field $\subseteq \mathbb{C}$ or a local field $\subseteq \overline{\mathbb{Q}_l}$

$R := \{p\} \cup \{l |\ E$ has bad reduction at $l\}$

$(\rho, V_\rho)\ \epsilon$ Irr$(G_n), n < \infty$

$L_R(E, \rho, s)$ L-function of $E \times \rho$ without Euler-factors of R,

From BSD to the Main Conjecture

algebraic		analytic
$X(E/K_n)$ as G_n-module	$\sim$	$L_R(E/K_n) = \prod_{\mathrm{Irr}(G_n)} L_R(E,\rho,s)^{n_\rho}$
	p-adic families	
$X(E/K_\infty)$	$\sim$	$(L_R(E,\rho,1))_{\rho\ \epsilon\ \mathrm{Irr}(G_n), n<\infty}$
	p-adic L-functions	
$F_E := F_X$ Characteristic Element		$\mathcal{L}_E$ analytic p-adic L-function

Main Conjecture

$$F_E \equiv \mathcal{L}_E$$

What is new?

Example (CM-case):

$$E : y^2 = x^3 - x$$

End(E) $\cong \mathbb{Z}[i] \neq \mathbb{Z}$, i.e. E admits complex multiplication (CM), thus

$$G \cong {\mathbb{Z}_p}^2 \times \text{finite group}$$

is **abelian.**

Main conjecture is a Theorem of Rubin in many cases,i.e. the theory is rather **well known!**

Example (GL_2-case):

$$E : y^2 + y = x^3 - x^2$$

End(E) $\cong \mathbb{Z}$, i.e. E does **not** admit complex multiplication, thus

$$G \subseteq_o GL_2(\mathbb{Z}_p) \quad \text{open subgroup}$$

is **not abelian.**

It was not even known how to formulate a main conjecture!

New: existence of **characteristic elements**

Structure Theory

$G \subseteq GL_n(\mathbb{Z}_p)$ compact p-adic Lie group without element of order p

Classical: $G \cong \mathbb{Z}_p{}^n$, $\Lambda = \Lambda(G) \cong \mathbb{Z}_p[[X_1, \ldots, X_n]]$

M torsion Λ-module, then up to pseudo-null modules

$$M \sim \prod_i \Lambda/\Lambda f_i^{n_i}, \quad f_i \text{ irreducible}, \qquad F_M := \prod f_i^{n_i}$$

Now: G non-abelian, but still notion of pseudo-null

Theorem (Coates, Schneider, Sujatha). *For every torsion Λ-module M one has up to pseudo-null modules*

$$M \sim \prod_i \Lambda/L_i, \quad L_i \text{ (reflexive) left ideal}$$

Problems:

(i) L_i not principal in general, i.e. no characteristic element

(ii) Euler characteristics do not behave well under pseudo-isomorphisms

Localization of Iwasawa algebras

(*joint work with: Coates, Fukaya, Kato and Sujatha*)

Assumption: $H \trianglelefteq G$ with $\Gamma := G/H \cong \mathbb{Z}_p$

(is satisfied in our application because K_∞ contains the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_{cyc}$ of $\mathbb{Q}$)

$\Lambda := \Lambda(G)$

We define a certain multiplicatively closed subset $\mathcal{T}$ of Λ.

Question Can one localize Λ with respect to $\mathcal{T}$?

In general, this is very difficult for **non-commutative** rings!

If yes, the localisation with respect to $\mathcal{T}$ should be related - by construction - to the following subcategory of the category of Λ-torsion modules:

$\mathfrak{M}_H(G)$	category of Λ-modules M such that modulo $\mathbb{Z}_p$-torsion M is finitely generated over $\Lambda(H) \subseteq \Lambda(G)$.

Characteristic Elements

Theorem. *The localization $\Lambda_{\mathcal{T}}$ of Λ with respect to $\mathcal{T}$ exists and there is a surjective map*

$$\partial : (\Lambda_{\mathcal{T}})^{\times} \twoheadrightarrow K_0(\mathfrak{M}_H(G))$$

arising from K-theory.

Definition. Any $F_M \in (\Lambda_{\mathcal{T}})^{\times}$ with $\partial[F_M] = [M]$ is called *characteristic element* of $M \in \mathfrak{M}_H(G)$.

Properties

(i) Any $f \in (\Lambda_{\mathcal{T}})^{\times}$ can be interpreted as a map on the isomorphism classes of (continuous) representations $\rho : G \to Gl_n(\mathcal{O}_K)$, $[K : \mathbb{Q}_p] < \infty$:

$$\rho \mapsto f(\rho) \in K \cup \{\infty\}.$$

(ii) The evaluation of F_M at ρ gives the generalized G-Euler characteristic $\chi(G, M(\rho))$

$$|F_M(\rho)|_p^{-[K:\mathbb{Q}_p]} = \chi(G, M(\rho))$$

if the Euler-characteristic is finite.

Numerical Example

$$\begin{aligned} E = X_1(11) \quad &: \quad y^2 + y = x^3 - x^2, \\ A \quad &: \quad y^2 + y = x^3 - x^2 - 7820x - 263580 \end{aligned}$$

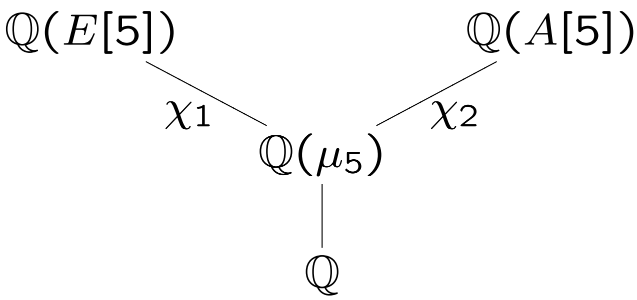
$p = 5$

One can show: $X \in \mathfrak{M}_H(G)$, i.e. F_X exists.

$G = G(\mathbb{Q}(E(5))/\mathbb{Q})$ has 2 irreducible Artin Representations of degree 4 :

$$\rho_i = \mathrm{Ind}\chi_i : G \to GL_4(\mathbb{Z}_5),$$

induced by χ_i, $i = 1, 2$.



Calculations show:

$$\chi(G, X(\rho_i)) = \begin{cases} 5^3 & i = 1 \\ 5 & i = 2 \end{cases},$$

i.e.

$$F_X(\rho_1) \sim 5^3, \quad F_X(\rho_2) \sim 5$$

up to $\mathbb{Z}_5^\times$.

Analytic p-adic L-function

Period - Conjecture: $\dfrac{L_R(E,\rho,1)}{\Omega(E,\rho)} \in \bar{\mathbb{Q}}$

Conjecture (Existence of analytic p-adic L-function). *Let $p \geq 5$ and assume that E has good ordinary reduction at p. Then there exists*

$$\mathcal{L}_E \in (\Lambda(G)_{\mathcal{T}})^{\times},$$

such that for all Artin representations ρ of G one has $\mathcal{L}_E(\rho) \neq \infty$ and

$$\mathcal{L}_E(\rho) \sim \frac{L_R(E,\rho,1)}{\Omega(E,\rho)}$$

up to some modifications of the Euler factor at p.

Conjecture (Main Conjecture). *Assume that* $p \geq 5$, E *has good ordinary reduction at* p, *and* $X(E/K_\infty)$ *belongs to* $\mathfrak{M}_H(G)$. *Granted the existence of the* p*-adic* L*-function,* $\mathcal{L}_E$ *is a characteristic element of* $X(E/K_\infty)$:

$$\partial[\mathcal{L}_E] = [X(E/K_\infty)].$$

Implications of the Main Conjecture

Assuming the existence of $\mathcal{L}_E$ and the main conjecture, one can show:

1)) GL_2 main conjecture $\Rightarrow$ 1-variable main conjecture (over $\mathbb{Q}_{cyc}$)

2)

$$\chi(G, X(\rho)) \text{ finite } \Leftrightarrow L_R(E, \rho, 1) \neq 0$$

In this case one has:

$$\chi(G, X(\rho)) = |\mathcal{L}_E(\rho)|_p^{-m_\rho}$$

3) If $L(E, 1) \neq 0$, then by Kolyvagin:

$$E(\mathbb{Q}), \quad Ш(E/\mathbb{Q}) \text{ are finite}$$

and the p-part of the BSD-conjecture holds.

Evidence for Main Conjecture

I CM-case

Existence of $\mathcal{L}_E$ follows from existence of 2-variable p-adic L-function (Manin-Vishik, Katz, Yager)

If $X \in \mathfrak{M}_H(G)$, then the main conjecture follows from 2-variable main conjecture (Rubin,Yager)

II GL_2-case

almost nothing is known!

Only weak numerical evidence by calculations of T. and V. Dokchitser:

$E = X_1(11)$,
$p = 5$,
ρ_i, $i = 1, 2$, the two unique irreducible Artin representations of degree 4

$$\chi(G, X(\rho_i)) = |\mathcal{L}_E(\rho_i)|_p^{-1}, \quad i = 1, 2$$