X International Workshop on Differential Equations, Number Theory, Data Analysis Methods and Geometry
University of Havana, February 19-23, 2007

From the Birch and Swinnerton Dyer Conjecture to the GL_2 Main Conjecture for elliptic curves

by Otmar Venjakob

Arithmetic of elliptic curves

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

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

$$E(K) = \ ?$$

for number fields, local fields, finite fields K

Arithmetic of elliptic curves

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

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

$$E(K) = \ ?$$

for number fields, local fields, finite fields K

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

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

Arithmetic of elliptic curves

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

$$E : y^2 + A_1 xy + A_3 y = x^3 + A_2 x^2 + A_4 x + A_6, \quad A_i \,\epsilon\, \mathbb{Z}.$$

$$E(K) = \ ?$$

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 :

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

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

Mordell-Weil Theorem

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

Birch & Swinnerton-Dyer Conjecture

If the Taylor expansion at $s = 1$ is

$$L(E/\mathbb{Q}, s) = L^*(E/\mathbb{Q})(s-1)^r + \ldots,$$

Mordell-Weil Theorem

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

Birch & Swinnerton-Dyer Conjecture

If the Taylor expansion at $s = 1$ is

$$L(E/\mathbb{Q}, s) = L^*(E/\mathbb{Q})(s-1)^r + \ldots,$$

then

I. $\quad r = \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) \quad$ (order of vanishing)

II. $$\frac{L^*(E/\mathbb{Q})}{\Omega_+ R_E} = \frac{\#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2} \prod_l c_l \in \mathbb{Q}$$

(rationality, integrality)

$\text{Ш}(E/\mathbb{Q})$	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 $Sel(E/K)$

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

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

$$\begin{tikzcd}[arrows=dash]
K_\infty \arrow[d] \arrow[dd, bend left, "G_\infty"] \\
K_n \arrow[d, "G_n"'] \\
\mathbb{Q}
\end{tikzcd}$$

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

$$\begin{tikzcd}
K_\infty \arrow[d, dash] \arrow[dd, dash, bend left, "G_\infty"] \\
K_n \arrow[d, dash, "G_n"'] \\
\mathbb{Q}
\end{tikzcd}$$

$X(E/K_n) := Sel(E/K_n)^\vee$ 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,

$$\rho : G \to GL(V_\rho),$$

realized over a number field $\subseteq \mathbb{C}$ or a local field $\subseteq \overline{\mathbb{Q}_l}$

(ρ, V_ρ) ϵ Irr$(G_n), n < \infty$

$L(E, \rho, s)$ L-function of $E \times \rho$

Twisted L-functions

$\mathrm{Irr}(G_n)$ irreducible representations of G_n,

$$\rho : G \to GL(V_\rho),$$

realized over a number field $\subseteq \mathbb{C}$ or a local field $\subseteq \overline{\mathbb{Q}_l}$

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

$L(E, \rho, s)$ L-function of $E \times \rho$:

$$L(E, \rho, s) := \prod_q \frac{1}{\det(1 - \mathrm{Frob}_q^{-1} T | (H_l^1(E) \otimes_{\mathbb{Q}} V_\rho)^{I_q})_{|T=q^{-s}}}$$

$$H_l^1(E) := \mathrm{Hom}(H_1(E(\mathbb{C}), \mathbb{Z}), \mathbb{Q}_l)$$

From BSD to the Main Conjecture

algebraic		analytic
$X(E/K_n)$ as G_n-module	$\sim$	$L(E/K_n) = \prod_{\mathrm{Irr}(G_n)} L(E,\rho,s)^{n_\rho}$
***p*-adic families**		
$X(E/K_\infty)$	$\sim$	$(L(E,\rho,1))_{\rho\ \in\ \mathrm{Irr}(G_n), n<\infty}$
***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):

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

$\mathrm{End}(E) \cong \mathbb{Z}[i] \neq \mathbb{Z}$, 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!**

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**

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 $\mathbb{Q}$)

We define a certain multiplicatively closed subset $\mathcal{T}$ of $\Lambda := \Lambda(G)$ associated with H.

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

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

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 $\mathbb{Q}$)

We define a certain multiplicatively closed subset $\mathcal{T}$ of $\Lambda := \Lambda(G)$ associated with H.

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

In general, this is a very difficult question 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 $\Lambda(H) \subseteq \Lambda(G)$.

$$\Longleftrightarrow$$

$$\Lambda_{\mathcal{T}} \otimes_\Lambda M = 0$$

Characteristic Elements

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

$$\partial : K_1(\Lambda_{\mathcal{T}}) \twoheadrightarrow K_0(\mathfrak{M}_H(G))$$

arising from K*-theory, whose kernel is the image of* $K_1(\Lambda)$.

Fact: $K_1(\Lambda_{\mathcal{T}}) \cong (\Lambda_{\mathcal{T}})^\times / [(\Lambda_{\mathcal{T}})^\times, (\Lambda_{\mathcal{T}})^\times]$

Characteristic Elements

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

$$\partial : K_1(\Lambda_{\mathcal{T}}) \twoheadrightarrow K_0(\mathfrak{M}_H(G))$$

arising from K*-theory, whose kernel is the image of* $K_1(\Lambda)$.

Fact: $K_1(\Lambda_{\mathcal{T}}) \cong (\Lambda_{\mathcal{T}})^\times/[(\Lambda_{\mathcal{T}})^\times, (\Lambda_{\mathcal{T}})^\times]$

Definition. Any $F_M \in K_1(\Lambda_{\mathcal{T}})$ with $\partial[F_M] = [M]$ is called characteristic element of $M \in \mathfrak{M}_H(G)$.

Property

Any $f \in K_1(\Lambda_{\mathcal{T}})$ can be interpreted as a map on the isomorphism classes of (continuous) representations $\rho : G \to Gl_n(\mathcal{O}_K)$, $[K : \mathbb{Q}_p] < \infty$:

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

Analytic p-adic L-function

Period - Conjecture: $$\frac{L(E,\rho^*,1)}{\Omega_\infty(E,\rho)} \;\epsilon\; \bar{\mathbb{Q}}$$

Analytic p-adic L-function

Period - Conjecture: $$\frac{L(E,\rho^*,1)}{\Omega_\infty(E,\rho)} \,\epsilon\, \bar{\mathbb{Q}}$$

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*

$$\mathcal{L}_E \,\epsilon\, K_1(\Lambda(G)_{\mathcal{T}}),$$

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

$$\mathcal{L}_E(\rho) \sim \frac{L(E,\rho^*,1)}{\Omega_\infty(E,\rho)}$$

up to some (precise) modifications of the Euler factors at p and where E has bad reduction.

Analytic p-adic L-function

Period - Conjecture: $\quad \dfrac{L(E,\rho^*,1)}{\Omega_\infty(E,\rho)} \,\epsilon\, \bar{\mathbb{Q}}$

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*

$$\mathcal{L}_E \,\epsilon\, K_1(\Lambda(G)_{\mathcal{T}}),$$

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

$$\mathcal{L}_E(\rho) \sim \frac{L(E,\rho^*,1)}{\Omega_\infty(E,\rho)}$$

up to some (precise) modifications of the Euler factors at p and where E has bad reduction.

Remark. The precise formula for $\mathcal{L}_E(\rho)$ is a consequence of the ζ-isomorphism conjecture of Fukaya and Kato.

Conjecture (Main Conjecture). *Assume that*

- E *has good ordinary reduction at* $\mathfrak{p}$,
- $X(E/K_\infty)$ *belongs to* $\mathfrak{M}_H(G)$ *and*
- *the* $\mathfrak{p}$*-adic* L*-function* $\mathcal{L}_E$ *exists.*

Then $\mathcal{L}_E$ *is a characteristic element of* $X(E/K_\infty)$:

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

Conjecture (Main Conjecture). *Assume that*

- E *has good ordinary reduction at* p,
- $X(E/K_\infty)$ *belongs to* $\mathfrak{M}_H(G)$ *and*
- *the* p*-adic* L*-function* $\mathcal{L}_E$ *exists.*

Then $\mathcal{L}_E$ *is a characteristic element of* $X(E/K_\infty)$:

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

$$\Longleftrightarrow$$

$$\mathcal{L}_E \equiv F_E \ \textit{mod} \quad \mathrm{im}(K_1(\Lambda)).$$

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)

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 who compare Euler characteristics of X with the p-adic valuation of the term showing up in the interpolation formula.

Leading coefficients

(*joint work with: D. Burns*)

What happens if $\quad \mathcal{L}_E(\rho) = L(E, \rho^*, 1) = 0$?

($\Leftrightarrow$ $(E(K_n) \otimes_{\mathbb{Q}} \mathbb{C})^{\rho^*} \neq 0$, if BSD holds)

Is there a leading coefficient $\mathcal{L}_E^*(\rho)$ of the (hypothetical) p-adic L-function $\mathcal{L}$ at ρ, analogous to the leading coefficient $L^*(E, \rho^*)$ of the complex L-function $L(E, \rho^*, s)$ at $s = 1$?

Leading coefficients

(*joint work with: D. Burns*)

What happens if $\mathcal{L}_E(\rho) = L(E, \rho^*, 1) = 0$?

($\Leftrightarrow$ $(E(K_n) \otimes_{\mathbb{Q}} \mathbb{C})^{\rho^*} \neq 0$, if BSD holds)

Is there a leading coefficient $\mathcal{L}_E^*(\rho)$ of the (hypothetical) p-adic L-function $\mathcal{L}$ at ρ, analogous to the leading coefficient $L^*(E, \rho^*)$ of the complex L-function $L(E, \rho^*, s)$ at $s = 1$?

We define for every $F \in K_1(\Lambda_{\mathcal{T}})$ the leading coefficient

$$F^*(\rho) \in \overline{\mathbb{Q}_p}$$

and the algebraic multiplicity

$$r_\rho(F) \in \mathbb{Z},$$

such that, if $r := r_\rho(F) \geq 0$, then

$$F^*(\rho) = \frac{1}{r!}(\frac{d}{ds})^r F(\rho\chi_{cyc}^s)_{|s=0}.$$

Refined interpolation property

Theorem. *Assume that*

- E *has good ordinary reduction at a fixed prime* $p \neq 2$.
- *the archimedean and* p*-adic height pairing for* $E(\rho^*)$ *are non-degenerate and*
- *that the* ζ*- and* ϵ*-isomorphim conjectures of Fukaya and Kato hold.*

Then the leading term $\mathcal{L}_E^*(\rho)$ *is equal to the product*

$$(-1)^{r_\rho(\mathcal{L}_E)} \frac{L^*(E(\rho^*))}{\Omega_\infty(E(\rho^*)) \cdot R_\infty(E(\rho^*))} \cdot \Omega_p(E(\rho^*)) \cdot R_p(E(\rho^*))$$

up to a (precise) modification of the Euler factors, where we use the following notation:

$\Omega_\infty(M(\rho^*))$, $R_\infty(E(\rho^*))$	*archimedean period, regulator*
$\Omega_p(M(\rho^*))$, $R_p(E(\rho^*))$	p*-adic period, regulator*

Implications of various Conjectures

$G \twoheadrightarrow G_n$ finite quotient

ζ-isomorphism conjecture

Fukaya/Kato

$+$ ϵ-conjecture Fukaya/Kato

GL_2 Main Conjecture

CFKSV

ETNC(E,G_n) $\forall\, n$?

Huber/Kings

?

ETNC(E,G_n)

Burns/Flach

$+$ $\#\text{Ш}(E/K_n)<\infty$

BSD

Main Conjecture $\Rightarrow$ ETNC

Theorem. *Assume that*

- *the Main Conjecture holds for E over K_∞.*
- *$X(E/K_\infty)$ is semisimple at all representations ρ of G_n.*
- *$\mathcal{L}_E$ satisfies the (refined) interpolation property for leading terms.*
- *the order of vanishing and rationality part of the ETNC(E,G_n) holds.*

Then the integrality statement of the ETNC(E,G_n), thus in particular, if $\#Ш(E/K_n) < \infty$, the BSD-formula for the leading coefficient $L^*(E, \rho^*)$, holds.