A supersingular tandem tale of two p-adic L-functions

florian spurg

BU number theory seminar
monday, oct. 5th, 2009

§0 Introduction

岩澤

- What is Iwasawa Theory? — It's a connection:

$$\{\text{(p-adic) analytic world}\} \xleftrightarrow{\text{fan}} \{\text{algebraic world}\}.$$

- Basic objects:

$$\begin{array}{ccc} \mathbb{Q}_\infty & \subset & \bigcup \mathbb{Q}(\zeta_{p^n}) \\ | & & \uparrow \text{prim. } p^n\text{-th roots of unity.} \\ \mathbb{Q}_n & & \\ | & & \\ \mathbb{Q} & & \end{array}$$

$\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$, $\quad \Gamma_n := \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$.

We look at the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ of $\mathbb{Q}$. It has Galois group $\Gamma \cong \mathbb{Z}_p$.

The Iwasawa algebra: $\mathbb{Z}_p[\![\Gamma]\!] \cong \mathbb{Z}_p[\![X]\!]$ allows us to look at p-adically ($\text{top. generator } \gamma \longmapsto (1+X)$) "good" functions.

Let $E/\mathbb{Q}$ be an elliptic curve and p be a prime of good reduction.
eg. $y^2+y = x^3-x$, $p \neq 37$

$$a_p := p+1-\#E(\mathbb{F}_p). \qquad (\text{eg. above, } a_2=-2,\ a_3=-3.)$$

Def A prime (of good reduction) is $\begin{cases} \text{ordinary if } p \nmid a_p \\ \text{supersingular if } p \mid a_p. \end{cases}$

§1 Iwasawa Theory for Elliptic Curves at Ordinary Primes ($p \nmid a_p$)

- In the analytic world, we encounter:
  - the Hasse-Weil L-function $L(E,s) = \prod_p (1-a_p p^{-s}+p^{1-2s})^{-1} = \sum_{n\geq 1} \frac{a_n}{n^s}$,
  - its twisted sister $L(E,\chi,s) = \sum_{n\geq 1} \frac{\chi(n)a_n}{n^s}$, χ a Dirichlet character.
  - there is also a p-adic version of the Hasse-Weil L-function:

- Mazur and Swinnerton-Dyer constructed a p-adic L-function $\mathcal{L}_p(E,X) \in \Lambda$ so that $\mathcal{L}_p(E, \zeta_{p^n} - 1)$ can be computed from $L(E, \overline{\chi}, 1)$, $\chi : (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \to \mathbb{C}^\times$ a Dirichlet character of conductor p^{n+1} (or p^{n+2} if $p=2$). [cf. work of Višik, Amice-Vélu]
  It is a function from the p-adic open unit disc $\mathbb{Z}_p \xrightarrow{to} \overline{\mathbb{Q}_p}$.
  Not only is it (p-adically) continuous, but p-adically analytic, and even better: it is an Iwasawa function (ie. lives in Λ).
  Also, it is nonzero (Rohrlich's theorem).
- In the algebraic world, we encounter:

- a group $Sel(E/\mathbb{Q}_n)$ called the Selmer group of the elliptic curve (w.r.to the $\mathbb{Q}_n$-rational points). It "contains" the $\mathbb{Q}_n$-rational points: there is a short exact sequence
$$0 \to E(\mathbb{Q}_n) \otimes \mathbb{Q}/\mathbb{Z} \to Sel(E/\mathbb{Q}_n) \to Ш(E/\mathbb{Q}_n) \to 0$$
  ↑ finite?
- the dual Selmer group $\mathcal{X} := \varprojlim \mathrm{Hom}(Sel(E/\mathbb{Q}_n), \mathbb{Q}_p/\mathbb{Z}_p)$. This contains information about $E(\mathbb{Q}_n)$ and the cyclotomic tower $\mathbb{Q}_\infty/\mathbb{Q}$, and furthermore has the following wonderful property:
- Thm (Mazur) $\mathcal{X}$ is finitely generated torsion as a Λ-module (if $p \nmid a_p$) (Kato)

We would like to compare $\mathcal{L}_p(E,X)$ with an invariant $\mathrm{Char}(\mathcal{X})$ called the characteristic ideal. What is a characteristic ideal?

⇝ If M was a finite abelian group, then its most important invariant would be its size #M. We have an exact sequence

$$0 \to \frac{\mathbb{Z}}{(b_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(b_m)} \to M \to 0$$

The characteristic ideal in $\mathbb{Z}$ is $(\#M) = (\prod_i b_i) \lhd \mathbb{Z}$.

⇝ For a finitely generated torsion Λ-module M, there is an exact sequence

$$0 \to \frac{\Lambda}{(b_1)} \oplus \dots \oplus \frac{\Lambda}{(b_m)} \to M \to (\text{finite}) \to 0 \quad \text{s.t. } b_{i+1} \mid b_i, \text{ and}$$

we define $\mathrm{Char}(M) := (\prod_i b_i) \lhd \Lambda$. This is well-defined (the b_i's aren't).

· **Main Conjecture** (Mazur, 1970's)
Let $p \nmid a_p$. Then $(\mathcal{L}_p(\mathcal{E},X)) = \mathrm{Char}(\mathcal{X}) \lhd \Lambda$.

· **Theorem** (Kato, 2004)
Let $p \nmid a_p$. Then $(\mathcal{L}_p(\mathcal{E},X)) \subset \mathrm{Char}(\mathcal{X})$.*
(His proof uses an Euler system, which he compares to a crane)

· A proof of the main conjecture has been announced by Skinner and Urban.

§ 2 Iwasawa Theory for Elliptic Curves at Supersingular Primes ($p \mid a_p$)

Thm (Elkies, 1987) There are infinitely many primes $p \mid a_p$.

◦ In the analytic world, we encounter:

· Let $\alpha, \bar{\alpha}$ be the roots of the Hecke polynomial $Y^2 - a_p Y + p = 0$.
Mazur, Tate, and Teitelbaum constructed p-adic L-functions
$\mathcal{L}_p(\mathcal{E},\alpha,X)$, $\mathcal{L}_p(\mathcal{E},\bar{\alpha},X) \in \overline{\mathbb{Q}}_p[\![X]\!]$ (not in Λ!! So we can't formulate a Main Conjecture yet)
↑ these again interpolate $\mathcal{L}(\mathcal{E},\bar{\chi},1)$

· **Thm** (Pollack, 2003) Let $a_p = 0$. Then there are $\mathcal{L}_p^+(\mathcal{E},X), \mathcal{L}_p^-(\mathcal{E},X) \in \Lambda$ so that
$\mathcal{L}_p(\mathcal{E},\alpha,X) = \log_p^+(1+X)\mathcal{L}_p^+(\mathcal{E},X) + \log_p^-(1+X)\mathcal{L}_p^-(\mathcal{E},X)\alpha$ if p is odd, and
$\mathcal{L}_2(\mathcal{E},\alpha,X) = \log_2^-(1+X)\mathcal{L}_2^+(\mathcal{E},X) + \frac{1}{2}\log_2^+(1+X)\mathcal{L}_2^-(\mathcal{E},X)\alpha$.
Here, $\log_p^+(1+X) = \frac{1}{p}\prod_{j\,\mathrm{even}} \frac{\Phi_{p^j}(1+X)}{p}$, $\log_p^-(1+X) = \frac{1}{p}\prod_{j\,\mathrm{odd}} \frac{\Phi_{p^j}(1+X)}{p}$, $\Phi_{p^j}(Y) = \frac{Y^{p^j}-1}{Y^{p^{j-1}}-1}$ the p^jth cyclotomic polynomial.

Pf (Idea) $a_p = 0 \Rightarrow \bar{\alpha} = -\alpha$. Look at the values at $\zeta_{p^j} - 1$ to conclude
$$\frac{\mathcal{L}_p(\mathcal{E},\alpha,X) + \mathcal{L}_p(\mathcal{E},\bar{\alpha},X)}{2} = \log_p^+(1+X)\mathcal{L}_p^+(\mathcal{E},X).$$
Pollack's proof is analytic.

◦ In the algebraic world, we encounter:
Denote by T the Tate module of $\mathcal{E}$, $H_n^1 := H^1(\mathbb{Q}_p(\zeta_{p^N}), T)$, $N = \begin{cases} n+1 & \text{if } p \text{ is odd} \\ n+2 & \text{if } p = 2 \end{cases}$.

Theorem (Kobayashi, 2003) Let $a_p = 0$. Then there are Λ-linear maps $\mathrm{Col}^{\pm}$ s.t.

$$H^1(T) = \varprojlim_n H_n^1 \xrightarrow{\mathrm{Col}^{\pm}} \Lambda$$
$$\text{Kato's zeta elements} \quad z \quad \longmapsto \quad \mathcal{L}_p^{\pm}$$

* Not quite, sometimes it's $(p^n \mathcal{L}_p(\mathcal{E},X)) \subset \mathrm{Char}(\mathcal{X})$ for some $n > 0$.

In the supersingular case, the usual dual $\mathcal{X}$ of the Selmer group is not Λ-torsion (it has rank 1), but Kobayashi's methods lead to "good" Selmer groups.

analyze $\ker \mathrm{Col}^{\pm}$ ⟿ construct new Selmer groups $\mathrm{Sel}^{\pm}$. This he did explicitly at each finite level!

Put $\mathcal{X}^{\pm} := \mathrm{Hom}(\mathrm{Sel}^{\pm}, \mathbb{Q}_p/\mathbb{Z}_p)$.

This is finitely generated torsion as a Λ-module, so it makes sense to define a characteristic ideal $\mathrm{Char}(\mathcal{X}^{\pm})$.

Main Conjecture (Kobayashi) Let $a_p = 0$ and p be odd. Then

$$(\mathcal{L}_p^{\pm}(\epsilon, X)) = \mathrm{Char}(\mathcal{X}^{\pm}) \lhd \Lambda$$

He showed $\subseteq$ ↑ Kato's result.

Questions: What about $a_p \neq 0$? Why are $\log_2^{\pm}$ switched? What's the factor of $\frac{1}{2}$ in Pollack's Theorem?

Remark (Hasse) $|a_p| < 2\sqrt{p}$. So if $p \mid a_p$ and $a_p \neq 0$, then $p = 2$ or $p = 3$.

General supersingular case:

Analytic Side: Thm (—, 2009) Let $p \mid a_p$. Then there are $\mathcal{L}_p^{\partial}(\epsilon, X), \mathcal{L}_p^{\nu}(\epsilon, X) \in \Lambda$ so that

$$\mathcal{L}_p(\epsilon, \alpha, X) = \log_\alpha^{\partial}(1+X)\,\mathcal{L}_p^{\partial}(\epsilon, X) + \log_\alpha^{\nu}\mathcal{L}_p^{\nu}(\epsilon, X),$$

where $\begin{pmatrix} \log_\alpha^{\partial}(1+X) & \log_{\bar\alpha}^{\partial}(1+X) \\ \log_\alpha^{\nu}(1+X) & \log_{\bar\alpha}^{\nu}(1+X) \end{pmatrix} = \mathcal{H}(X) \begin{pmatrix} 1 & 1 \\ -\alpha^{-1} & -\bar\alpha^{-1} \end{pmatrix}$,

$$\mathcal{H}(X) = \begin{pmatrix} 0 & 1 \\ -1 & -a_p \end{pmatrix} \lim_{n\to\infty} \begin{pmatrix} a_p & \phi_p(1+X) \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a_p & \phi_{p^2}(1+X) \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_p & \phi_{p^n}(1+X) \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a_p & p \\ -1 & 0 \end{pmatrix}^N, \quad N = \begin{cases} n+1 & p \text{ odd} \\ n+2 & p = 2 \end{cases}.$$

(if $a_p = 0$, then $\mathcal{L}_p^{\partial} = \mathcal{L}_p^{+}$, $\mathcal{L}_p^{\nu} = \mathcal{L}_p^{-}$, $\log_\alpha^{\partial} = \log_p^{+}$, $\log_\alpha^{\nu} = \alpha \log_p^{-}$ if p is odd, and $\mathcal{L}_2^{\partial} = -\mathcal{L}_2^{-}$, $\mathcal{L}_2^{\nu} = \mathcal{L}_2^{+}$, $\log_\alpha^{\partial} = -\frac{1}{2}\log_2^{+}\alpha$, $\log_\alpha^{\nu} = \log_2^{-}$.)

The proof is algebraic:

Thm (–, 2009) Let $p \mid a_p$. Then $\exists\ \mathrm{Col}^{\partial}, \mathrm{Col}^{\nu}$ s.t.

$$\begin{array}{ccc} H^1(T) & \xrightarrow{\mathrm{Col}^{\partial/\nu}} & \Lambda \\ \Psi & & \Psi \\ z & \longmapsto & \mathcal{L}_p^{\partial/\nu} \end{array}$$

, ie. $\mathrm{Col}^{\partial/\nu}$ allow us to find the desired $\mathcal{L}_p^{\partial/\nu}$ and their construction leads to $\log_\alpha^{\partial}, \log_\alpha^{\nu}$ as well.

From the kernels $\ker \mathrm{Col}^{\vartheta/\upsilon}$, we can (formally) construct $\mathcal{X}^{\vartheta/\upsilon}$ analogously and have

Main Conjecture Let $p \nmid a_p$ and p be odd. Then

$$(\mathcal{L}_p^{\vartheta}) = \mathrm{Char}(\mathcal{X}^{\vartheta}) \lhd \Lambda, \quad (\mathcal{L}_p^{\upsilon}) = \mathrm{Char}(\mathcal{X}^{\upsilon}) \lhd \Lambda$$

$\subset$ (again by Kato's results) $\subset$

§3 How do we construct Col^{ϑ} and Col^{υ}?

(We are still assuming $p \nmid a_p$). Well, how did Kobayashi construct $\mathrm{Col}^{\pm}$?
Let $\mathfrak{m}_n \lhd\lhd \mathcal{O}_{\mathbb{Q}_p(\zeta_{p^n})}$ be the maximal ideal.

Proposition (Kobayashi) The formal group $\hat{E}(\mathfrak{m}_n)$ is generated by δ_n^1 and δ_n^0 as a Λ-module.

Also, there is a bilinear map

$$P_x : H_n^1 \longrightarrow \Lambda_n := \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)] \cong \frac{\Lambda}{(1+X)^{p^n}-1}, \quad x \in \hat{E}(\mathfrak{m}_n)$$

(bilinear in $H_n^1 = H^1(\mathbb{Q}_p(\zeta_{p^n}), T)$ and $\hat{E}(\mathfrak{m}_n)$).

Lemma (Kobayashi) $P_{\delta_n^0}(H_n^1) \subset \Phi_{p^n}(1+X)\Lambda_n$.

Also,

$$\begin{array}{ccc} H_n^1 & \xrightarrow{P_x} & \Lambda_n \\ \mathrm{cor}\downarrow & & \downarrow \mathrm{proj.} \\ H_{n-1}^1 & \xrightarrow{P_{\mathrm{Tr}\,x}} & \Lambda_{n-1} \end{array} \quad \text{commutes.}$$

Note that $\mathrm{Tr}\,\delta_n^0 = p\delta_{n-1}^1$, $\mathrm{Tr}\,\delta_n^1 = a_p\delta_{n-1}^1 - \delta_{n-1}^0$.

Kobayashi's idea: Since $a_p = 0$, $\mathrm{Tr}\,\delta_n^1 = -\delta_{n-1}^0$, so we can find the zeroes:

$$\begin{array}{ccc} H_n^1 & \xrightarrow{\frac{1}{p^2}P_{\delta_n^0}} & \frac{\Phi_n}{p}\frac{\Phi_{n-2}}{p}\Lambda_n \\ \mathrm{cor}\downarrow & & \downarrow \\ H_{n-1}^1 & \xrightarrow{\frac{1}{p}P_{\delta_{n-1}^1}} & \frac{\Phi_{n-2}}{p}\Lambda_{n-1} \\ \mathrm{cor}\downarrow & & \downarrow \\ H_{n-2}^1 & \xrightarrow{-\frac{1}{p}P_{\delta_{n-2}^0}} & \frac{\Phi_{n-2}}{p}\Lambda_{n-2} \\ \mathrm{cor}\downarrow & & \downarrow \\ H_{n-3}^1 & \xrightarrow{-P_{\delta_{n-3}^1}} & \Lambda_{n-3} \end{array}$$

$$H_n^1 \xrightarrow{\mathrm{Col}_n^{\pm}} \Lambda_n \xrightarrow{\varprojlim_n} Ш^1(T) \xrightarrow{\mathrm{Col}^{\pm}} \Lambda.$$

$$P_n^{\pm} = P_{\delta_n^0} \text{ or } P_{\delta_n^1} \quad (\text{parity of } n), \qquad \mathrm{Col}_n^{\pm} = P_n^{\pm} \times \omega_n^{\pm}$$

Let's generalize this to $a_p \neq 0$.

Idea 1 Think of vectors instead of elements, e.g.

$$\mathrm{Tr}\,(\delta_n^1, \delta_n^0) = (\delta_{n-1}^1, \delta_{n-1}^0)\,A \quad , \quad A = \begin{pmatrix} a_p & p \\ -1 & 0 \end{pmatrix}.$$

Idea 2
$$\begin{array}{ccc} H_n^1 & \xrightarrow{(P_{\delta_n^1}, P_{\delta_n^0})} & \Lambda_n^{\oplus 2} \\ \text{m corestr.}\downarrow & \circlearrowright & \downarrow \\ H_{n-m}^1 & \xrightarrow{(P_{\delta_{n-m}^1}, P_{\delta_{n-m}^0})A^m} & \Lambda_{n-m}^{\oplus 2} \end{array}$$
, so we get a factor of $\Phi_{p^{n-m}}$ somewhere, since $P_{\delta_{n-m}^0}(H_{n-m}^1) \subset \phi_{p^{n-m}}\Lambda_{n-m}$.

Let $z \in H_n^1$. By abuse of notation, write $(P_{\delta_n^1}, P_{\delta_n^0})$ instead of $(P_{\delta_n^1}(z), P_{\delta_n^0}(z))$.
Let's find the zeroes (ie. factors Φ_{p^i}) we should find! $\Lambda_n^{\oplus 2} \ni$

→ First zero: $(P_{\delta_n^1}, P_{\delta_n^0}) = (P_{\delta_n^1}, x)\begin{pmatrix} 1 & 0 \\ 0 & \phi_{p^n} \end{pmatrix} = (x, y)\begin{pmatrix} a_p & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \phi_{p^n} \end{pmatrix}$. This is cheap!

→ Second zero: Choose δ_n^{-1} so that $\mathrm{Tr}\,\delta_n^{-1} = \delta_{n-1}^0$.

$$\begin{array}{ccc} H_n^1 & \xrightarrow{P_{\delta_n^{-1}}} & \phi_{p^n}\Lambda_n \\ \downarrow & & \downarrow \\ H_{n-1}^1 & \xrightarrow{P_{\delta_{n-1}^0}} & \phi_{p^{n-1}}\Lambda_{n-1} \end{array}$$

Thus have $(P_{\delta_n^1}, P_{\delta_n^0})\begin{pmatrix} 0 & -1 \\ 1 & \frac{a_p}{p} \end{pmatrix} = \left(P_{\delta_n^0}, P_{\delta_n^{-1}}\right)$, with $\Phi_{p^{n-1}}$ dividing this!

Lemma $\Phi_{p^n}(\zeta_{p^{n-1}}) = p$.

So at $\zeta_{p^{n-1}}$, $(x,y)\underbrace{\begin{pmatrix} a_p & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & \frac{a_p}{p} \end{pmatrix}}_{= \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}} = (P_{\delta_n^0}, 0)$.

$$\Rightarrow (x,y) = (x,y')\begin{pmatrix} 1 & 0 \\ 0 & \phi_{p^{n-1}} \end{pmatrix} = (y',x')\begin{pmatrix} a_p & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \phi_{p^{n-1}} \end{pmatrix}.$$

Thus, $(P_{\delta_n^1}, P_{\delta_n^0}) = (y',x')\underbrace{\begin{pmatrix} a_p & \phi_{p^{n-1}} \\ -1 & 0 \end{pmatrix}}_{\text{second zero}}\underbrace{\begin{pmatrix} a_p & \phi_{p^n} \\ -1 & 0 \end{pmatrix}}_{\text{first zero}}$.

§ 4 Outlook

- Are there analytic methods to produce $\mathcal{L}_p^{\mathcal{U}}$, $\mathcal{L}_p^{\mathcal{V}}$?
- What about the modular form case? → Pollack has constructed $\mathcal{L}_p^{\pm}$ under the assumption $a_p = 0$, which A. Dei has put into a main conjecture. What about the case $a_p \neq 0$ there?