CIMPA-ICTP research school on

Artin L-functions, Artin's primitive roots conjecture and applications

Nesin Mathematics Village, Şirince, Turkey

May 29^{th} - June 9^{th} 2017

Iwasawa Theory for Elliptic Curves

Enis KAYA, Koç University

June 8^{th} 2017

To Eda

• What is Iwasawa theory?

$\begin{pmatrix} \text{algebraic} \\ \text{world} \end{pmatrix}$ Iwas. Thy "p-adic" objects $\begin{pmatrix} \text{analytic} \\ \text{world} \end{pmatrix}$

Iwasawa Theory and Generalization, Kato

↳ "Main conjectures" of Iwasawa Thy:

"Selmer groups" "=" "p-adic L-functions"

"p-adic analogue" of L-functions

the kernels of "global-to-local" maps

• $\mathbb{Q}_\infty$: the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$

$$\mathbb{Q}(\mu_{p^n}) \,/\, \mathbb{Q} \quad \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$$

↳ $$\mathbb{Q}(\mu_{p^\infty}) := \bigcup_n \mathbb{Q}(\mu_{p^n}) \Rightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p$$

↳ By the Galois correspondence, $\exists\, \mathbb{Q}_\infty$ s.t.

- $\mathbb{Q}(\mu_{p^\infty}) \,—\, \mathbb{Q}_\infty \,—\, \mathbb{Q}$
- $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$

Γ

Rk: This is the unique $\mathbb{Z}_p$-ext. of $\mathbb{Q}$.

• Λ : Iwasawa Algebra

M : $\mathbb{Z}$-module

$\rightsquigarrow M_p := M[p^\infty]$: $\mathbb{Z}_p$-module

$\rightsquigarrow$ If Γ acts on M_p, M_p : $\mathbb{Z}_p[\Gamma]$-module

$\rightsquigarrow$ If Γ acts continuosly, M_p : $\mathbb{Z}_p[[\Gamma]]$-module $= \varprojlim_{\Gamma' \trianglelefteq \Gamma} \mathbb{Z}_p[\Gamma/\Gamma']$

$\mathbb{Z}_p[[\Gamma]] = \Lambda$: completed group algebra of Γ over $\mathbb{Z}_p$

$\hookrightarrow$ Fact: $\Lambda \simeq \mathbb{Z}_p[[T]]$; $\gamma \mapsto 1+T$ where $\overline{\langle \gamma \rangle} = \Gamma$!

$\simeq$: topological isomorphism

$\mathbb{Z}_p[[T]]$: a complete Noetherian local ring of Krull dim 2.

• The Structure of Λ-modules

Thm (Serre) : M : fin. gen. torsion Λ-module

$$\Rightarrow M \sim \left(\bigoplus_{i=1}^{s} \Lambda/(p)^{n_i} \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T))^{m_j} \right)$$

$\sim$: pseudo-isomorphic

$s, t \in \mathbb{Z}^{\geq 0}$, $n_i, m_j \in \mathbb{Z}^{>0}$, $f_j(T) \in \mathbb{Z}_p[T]$ irreducible with $f_j(T) \equiv T^{\deg f_j} \pmod p$.

$\rightsquigarrow \mathrm{Char}_\Lambda(M) := \left(p^{\sum_{i=1}^{s} n_i} \prod_{j=1}^{t} f_j(T)^{m_j} \right)$: the characteristic ideal of M.

- Elliptic Curves

$E : y^2 = x^3 + ax + b, \ a, b \in \mathbb{Z}$

p : a prime of good reduction

$a_p := p + 1 - \# E(\mathbb{F}_q)$

assume p is ordinary; that is $p \nmid a_p$.

$\rightsquigarrow L(E,s)$: L-function of E $= \sum_{n=1}^{\infty} \frac{a_n}{n^s}$

- $\mathrm{Sel}_p(E/\mathbb{Q}_\infty)$

L : any number field $\rightsquigarrow \mathrm{Sel}^n(E/L)$: n-Selmer group of E/L

$n \in \mathbb{Z}$

Fact: $E(L)/_{nE(L)} \hookrightarrow \mathrm{Sel}^n(E/L)$

$\rightsquigarrow \mathrm{Sel}_p(E/L) := \varinjlim_m \mathrm{Sel}^{p^m}(E/L)$: pro-p Selmer group of E/L

Fact: $E(L) \otimes \mathbb{Q}_p/_{\mathbb{Z}_p} \hookrightarrow \mathrm{Sel}_p(E/L)$

$\rightsquigarrow \mathrm{Sel}_p(E/\mathbb{Q}_\infty) := \varinjlim_n \mathrm{Sel}_p(E/\mathbb{Q}_n)$: Iwasawa theoretic Selmer Group

where

$$\begin{array}{l} \mathbb{Q}(\mu_{p^{n+1}}) \\ \quad | \\ \quad \mathbb{Q}_n \\ \quad | \\ \quad \mathbb{Q} \end{array} \quad \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/_{p^n\mathbb{Z}}, \quad \mathbb{Q}_\infty = \bigcup_n \mathbb{Q}_n$$

- $\mathcal{L}_p(E,s)$

Thm (Mazur-Tate-Teitelbaum): $\exists$ a "p-adic measure" μ_E on $\mathbb{Z}_p^\times$ characterized by the following "interpolation" formula:

$$\int_{\mathbb{Z}_p^\times} \mu_E = (1-\alpha^{-1})^2 \frac{L(E,1)}{\Omega_E^+}$$

$$\frac{L(E,1)}{\Omega_E^+} \in \mathbb{Q}$$

- α : the unit root of $X^2 - a_p X + p$
- Ω_E^+ : the real period $\in \mathbb{R}^+$

$\mathcal{L}_p(E,s) :=$ "the p-adic Mellin transform of μ_E" $= \int_{\mathbb{Z}_p^\times} \langle t \rangle^{s-1} d\mu_E$

$s \in \mathbb{Z}_p$

$\rightsquigarrow \forall \alpha \in \mathbb{Z}_p^\times$,

$\alpha = \omega(\alpha)\langle\alpha\rangle$

- $\langle\alpha\rangle \in 1+p\mathbb{Z}_p$
- $\omega(\alpha) \in (\mathbb{Z}/p\mathbb{Z})^\times$

$$\Rightarrow \mathcal{L}_p(E,1) = (1-\alpha^{-1})^2 \frac{L(E,1)}{\Omega_E^+}$$

[- Modular symbols
- Modular integrals
- distributions $\rightsquigarrow$ measures
- p-adic L-functions]

Regulators, L-functions and rational points, Bertolini

Mazur's construction of the Kubota-Leopoldt p-adic L-functions, Gutiert

- Main Conjecture of Iwasawa Theory for Elliptic Curves

(In Our Setting)

$$\begin{tikzcd}[column sep=small]
 & (E,p) \arrow[dl, squiggly] \arrow[dr, squiggly] & \\
\text{an alg. obj.} : \mathrm{Sel}_p(E/\mathbb{Q}_\infty)^\vee \arrow[d, squiggly] & & \mathcal{L}_p(E,S) \arrow[d, squiggly] : \text{an anal. obj.} \\
\mathrm{char}_\Lambda\left(\mathrm{Sel}_p(E/\mathbb{Q}_\infty)^\vee\right) \arrow[rr, equal, "\text{M.C.}", "?"'] & & \left(\mathcal{L}_p(E,S)\right)
\end{tikzcd}$$

$\mathrm{Sel}_p(E/\mathbb{Q}_\infty)^\vee$: f.g. torsion Λ-module

$\mathcal{L}_p(E,S) \in \Lambda$

$\mathrm{char}_\Lambda\left(\mathrm{Sel}_p(E/\mathbb{Q}_\infty)^\vee\right) \subset \Lambda$, $\quad \left(\mathcal{L}_p(E,S)\right) \subset \Lambda$

$A^\vee = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ the Pontryagin dual

↳ This conjecture is mostly proved.

Thm (Kato, Skinner-Urban, Rubin).

If E verifies "mild technical hypotheses", then MC is true.

Cor: In our setting,

$$\text{analytic rank} = 0 \iff \text{algebraic rank} = 0$$

as predicted by BSD.

p-adic variation in Arithmetic Geometry: A Survey, [illegible]