Why Iwasawa theorists need p-adic L-functions

christian wuthrich

February 23

Artin-Tate's analogue of BSD in postitive characteristic

Artin-Tate's analogue of BSD in postitive characteristic

- k a finite field with q elements

Artin-Tate's analogue of BSD in postitive characteristic

- k a finite field with q elements
- K a global field with constants k

Artin-Tate's analogue of BSD in postitive characteristic

- k a finite field with q elements
- K a global field with constants k
- E/K an elliptic curve with $j(E) \notin k$

Artin-Tate's analogue of BSD in postitive characteristic

- k a finite field with q elements
- K a global field with constants k
- E/K an elliptic curve with $j(E) \notin k$
- $L(E/K, s) = f_E(T)$ with $T = q^{-s}$ and $f_E(T) \in \mathbb{Z}[T]$

Artin-Tate's analogue of BSD in postitive characteristic

- k a finite field with q elements
- K a global field with constants k
- E/K an elliptic curve with $j(E) \notin k$
- $L(E/K,s) = f_E(T)$ with $T = q^{-s}$ and $f_E(T) \in \mathbb{Z}[T]$

Birch and Swinnerton-Dyer conjecture

- $\mathrm{ord}_{s=1} L(E/K,s) = \mathrm{ord}_{(1-qT)} f_E(T) = \mathrm{rk}\, E(K)$.

Artin-Tate's analogue of BSD in postitive characteristic

- k a finite field with q elements
- K a global field with constants k
- E/K an elliptic curve with $j(E) \notin k$
- $L(E/K, s) = f_E(T)$ with $T = q^{-s}$ and $f_E(T) \in \mathbb{Z}[T]$

Birch and Swinnerton-Dyer conjecture

- $\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{ord}_{(1-qT)} f_E(T) = \mathrm{rk}\, E(K)$.
- The leading term is  $\cdot \mathrm{Reg}(E/K) \cdot \#Ш(E/K)$.

Artin-Tate's analogue of BSD in postitive characteristic

- k a finite field with q elements
- K a global field with constants k
- E/K an elliptic curve with $j(E) \notin k$
- $L(E/K, s) = f_E(T)$ with $T = q^{-s}$ and $f_E(T) \in \mathbb{Z}[T]$

Birch and Swinnerton-Dyer conjecture

- $\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{ord}_{(1-qT)} f_E(T) = \mathrm{rk}\, E(K)$.
- The leading term is  $\cdot \mathrm{Reg}(E/K) \cdot \#Ш(E/K)$.

Artin-Tate

- $\mathrm{ord}_{(1-qT)} f_E(T) \geqslant \mathrm{rk}\, E(K)$

Artin-Tate's analogue of BSD in postitive characteristic

- k a finite field with q elements
- K a global field with constants k
- E/K an elliptic curve with $j(E) \notin k$
- $L(E/K, s) = f_E(T)$ with $T = q^{-s}$ and $f_E(T) \in \mathbb{Z}[T]$

Birch and Swinnerton-Dyer conjecture

- $\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{ord}_{(1-qT)} f_E(T) = \mathrm{rk}\, E(K)$.
- The leading term is  $\cdot \mathrm{Reg}(E/K) \cdot \#\text{Ш}(E/K)$.

Artin-Tate

- $\mathrm{ord}_{(1-qT)} f_E(T) \geqslant \mathrm{rk}\, E(K)$
- If $\text{Ш}(E/K)(p)$ is finite for one prime p, then BSD holds.

Translation to geometry

$$K \quad \leftrightsquigarrow \quad C/k\text{, a smooth projective curve}$$

Translation to geometry

$$\begin{aligned} K &\quad\leftrightsquigarrow\quad C/k\text{, a smooth projective curve} \\ E/K &\quad\leftrightsquigarrow\quad \mathcal{E} \to C\text{, an elliptic surface} \end{aligned}$$

Translation to geometry

$$
\begin{aligned}
K &\leftrightsquigarrow C/k\text{, a smooth projective curve}\\
E/K &\leftrightsquigarrow \mathcal{E} \to C\text{, an elliptic surface}\\
E(K) &\leftrightsquigarrow \mathrm{NS}(\mathcal{E})
\end{aligned}
$$

Translation to geometry

K	$\leftrightsquigarrow$	C/k, a smooth projective curve
E/K	$\leftrightsquigarrow$	$\mathcal{E} \to C$, an elliptic surface
$E(K)$	$\leftrightsquigarrow$	$\mathrm{NS}(\mathcal{E})$
$\mathrm{Sel}_p(E/K)$	$\leftrightsquigarrow$	$\mathrm{H}^2_{\text{ét}}\big(\mathcal{E}, \mathbb{Z}_p(1)\big)$

Translation to geometry

K	$\leftrightsquigarrow$	C/k, a smooth projective curve
E/K	$\leftrightsquigarrow$	$\mathcal{E} \to C$, an elliptic surface
$E(K)$	$\leftrightsquigarrow$	$\mathrm{NS}(\mathcal{E})$
$\mathrm{Sel}_p(E/K)$	$\leftrightsquigarrow$	$\mathrm{H}^2_{\text{ét}}(\mathcal{E}, \mathbb{Z}_p(1))$
$L(E/K, s) = f_E(T)$	$\leftrightsquigarrow$	$\det(1 - \mathrm{Frob}\ T)$ on $\mathrm{H}^2_{\text{ét}}(\overline{\mathcal{E}}, \mathbb{Z}_p(1))$

Here $\mathrm{Frob} \in G = \mathrm{Gal}(\overline{k}/k)$ and $\overline{\mathcal{E}} = \mathcal{E} \times \overline{k}$

$$
\begin{array}{ccccc}
\mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mathbb{Z}_p(1)\big)^G & \xrightarrow{\ \alpha\ } & \mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mathbb{Z}_p(1)\big)_G & \xrightarrow{\ \cong\ } & \left(\mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mu_{p^\infty}\big)^G\right)^\vee \\
\sim\Big\uparrow & & & & \Big\downarrow\sim \\
\mathrm{H}^2_{\text{ét}}\big(\mathcal{E}, \mathbb{Z}_p(1)\big) & & & & \left(\mathrm{H}^2_{\text{ét}}\big(\mathcal{E}, \mu_{p^\infty}\big)\right)^\vee
\end{array}
$$

$$
\begin{array}{ccccc}
\mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mathbb{Z}_p(1)\big)^G & \xrightarrow{\alpha} & \mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mathbb{Z}_p(1)\big)_G & \xrightarrow{\cong} & \left(\mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mu_{p^\infty}\big)^G\right)^\vee \\
\sim \big\uparrow & & & & \big\downarrow \sim \\
\mathrm{H}^2_{\text{ét}}\big(\mathcal{E}, \mathbb{Z}_p(1)\big) & & & & \left(\mathrm{H}^2_{\text{ét}}\big(\mathcal{E}, \mu_{p^\infty}\big)\right)^\vee \\
\big\uparrow & & & & \big\downarrow \\
\mathrm{NS}(\mathcal{E}) \otimes \mathbb{Z}_p & & & & \left(\mathrm{NS}(\mathcal{E}) \otimes {}^{\mathbb{Q}_p}\!/\!_{\mathbb{Z}_p}\right)^\vee
\end{array}
$$

$$
\begin{array}{ccccc}
\mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mathbb{Z}_p(1)\big)^G & \xrightarrow{\alpha} & \mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mathbb{Z}_p(1)\big)_G & \xrightarrow{\cong} & \left(\mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mu_{p^\infty}\big)^G\right)^\vee \\
\sim \Big\uparrow & & & & \Big\downarrow \sim \\
\mathrm{H}^2_{\text{ét}}\big(\mathcal{E}, \mathbb{Z}_p(1)\big) & & & & \left(\mathrm{H}^2_{\text{ét}}\big(\mathcal{E}, \mu_{p^\infty}\big)\right)^\vee \\
\Big\uparrow & & & & \Big\downarrow \\
\mathrm{NS}(\mathcal{E}) \otimes \mathbb{Z}_p & & \xrightarrow{\text{intersection pairing}} & & \left(\mathrm{NS}(\mathcal{E}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee
\end{array}
$$

$$
\begin{array}{ccccc}
\mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mathbb{Z}_p(1)\big)^G & \xrightarrow{\alpha} & \mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mathbb{Z}_p(1)\big)_G & \xrightarrow{\cong} & \left(\mathrm{H}^2_{\text{ét}}\big(\overline{\mathcal{E}}, \mu_{p^\infty}\big)^G\right)^\vee \\
\uparrow \wr & & & & \downarrow \wr \\
\mathrm{H}^2_{\text{ét}}\big(\mathcal{E}, \mathbb{Z}_p(1)\big) & & & & \left(\mathrm{H}^2_{\text{ét}}\big(\mathcal{E}, \mu_{p^\infty}\big)\right)^\vee \\
\uparrow & & & & \downarrow \\
\mathrm{NS}(\mathcal{E}) \otimes \mathbb{Z}_p & & \xrightarrow{\text{intersection pairing}} & & \left(\mathrm{NS}(\mathcal{E}) \otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}\right)^\vee \\
\uparrow & & & & \downarrow \\
E(K) \otimes \mathbb{Z}_p & & \xrightarrow{\text{Néron-Tate height}} & & \left(E(K) \otimes {}^{\mathbb{Q}_p}/_{\mathbb{Z}_p}\right)^\vee
\end{array}
$$

Lemma

Let be M a $\mathbb{Z}_p$-module of finite type with a G-action and $\alpha\colon M^G \to M \to M_G$.

- Then $\ker(\alpha)$ and $\operatorname{coker}(\alpha)$ are finite if and only if

$$\operatorname{ord}_T \det(T - 1 + \operatorname{Frob} |M) = \operatorname{rk} M^G.$$

- If so, then the leading term is

$$\frac{\# \operatorname{coker}(\alpha)}{\# \ker(\alpha)},$$

  up to a unit in $\mathbb{Z}_p$.

Iwasawa theory for elliptic curves

- K number field

Iwasawa theory for elliptic curves

- K number field
- E/K elliptic curve

Iwasawa theory for elliptic curves

- K number field
- E/K elliptic curve
- $p > 2$ prime

Iwasawa theory for elliptic curves

- K number field
- E/K elliptic curve
- $p > 2$ prime
- K_∞/K a $\mathbb{Z}_p$-extension with group Γ

Iwasawa theory for elliptic curves

- K number field
- E/K elliptic curve
- $p > 2$ prime
- K_∞/K a $\mathbb{Z}_p$-extension with group Γ
- $[K_n : K] = p^n$

Iwasawa theory for elliptic curves

- K number field
- E/K elliptic curve
- $p > 2$ prime
- K_∞/K a $\mathbb{Z}_p$-extension with group Γ
- $[K_n : K] = p^n$
- Σ a finite set of places in K, containing the bad and infinite

Iwasawa theory for elliptic curves

- K number field
- E/K elliptic curve
- $p > 2$ prime
- K_∞/K a $\mathbb{Z}_p$-extension with group Γ
- $[K_n : K] = p^n$
- Σ a finite set of places in K, containing the bad and infinite
- $\mathrm{H}^i_\Sigma(K, \cdot) = \mathrm{H}^i(G_\Sigma(K), \cdot)$

- The fine Selmer group

$$Y_0 \;=\; \ker\Big(\mathrm{H}^2_{\Sigma}(K\;\;, T_pE) \to \bigoplus_{\upsilon\in\Sigma} \mathrm{H}^2(K_\upsilon\;\;, T_pE)\Big)$$

- The fine Selmer group

$$Y_0 = \ker\Big(\mathrm{H}^2_\Sigma(K\ ,T_pE) \to \bigoplus_{\upsilon\in\Sigma} \mathrm{H}^2(K_\upsilon\ ,T_pE)\Big)$$

- Y_0 is dual to

$$\ker\Big(\mathrm{H}^1_\Sigma(K\ ,E_{p^\infty}) \to \bigoplus_{\upsilon\in\Sigma} \mathrm{H}^1(K_\upsilon\ ,E_{p^\infty})\Big)$$

- The fine Selmer group

$$Y_0 = \ker\Big(\mathrm{H}^2_\Sigma(K_\infty, T_pE) \to \bigoplus_{v\in\Sigma} \mathrm{H}^2(K_{\infty,v}, T_pE)\Big)$$

- Y_0 is dual to

$$\ker\Big(\mathrm{H}^1_\Sigma(K_\infty, E_{p^\infty}) \to \bigoplus_{v\in\Sigma} \mathrm{H}^1(K_{\infty,v}, E_{p^\infty})\Big)$$

- $(Y_0)^\vee$ contains the fine Mordell-Weil group

$$\mathcal{M} = \ker\Big(E(K) \otimes {}^{\mathbb{Q}_p}\!/\!_{\mathbb{Z}_p} \to \bigoplus_{v|p} E(K_v) \otimes {}^{\mathbb{Q}_p}\!/\!_{\mathbb{Z}_p}\Big)$$

(probably with finite index)

- The fine Selmer group

$$Y_n \;=\; \ker\Big(\mathrm{H}^2_\Sigma(K_n, T_pE) \to \bigoplus_{\upsilon\in\Sigma} \mathrm{H}^2(K_{n,\upsilon}, T_pE)\Big)$$

- Y_n is dual to

$$\ker\Big(\mathrm{H}^1_\Sigma(K_n, E_{p^\infty}) \to \bigoplus_{\upsilon\in\Sigma} \mathrm{H}^1(K_{n,\upsilon}, E_{p^\infty})\Big)$$

- $(Y_0)^\vee$ contains the fine Mordell-Weil group

$$\mathcal{M} \;=\; \ker\Big(E(K) \otimes {}^{\mathbb{Q}_p}\!/\!_{\mathbb{Z}_p} \;\to\; \bigoplus_{\upsilon|p} E(K_\upsilon) \otimes {}^{\mathbb{Q}_p}\!/\!_{\mathbb{Z}_p}\Big)$$

  (probably with finite index)
- $Y = \varprojlim Y_n$

$$
\begin{array}{ccccc}
\left(\mathrm{H}^1_\Sigma(K_\infty, E_{p^\infty})_\Gamma\right)^\vee & \xrightarrow{\text{duality}} & Y^\Gamma & \xrightarrow{\alpha} & Y_\Gamma \\
\uparrow & & & & \downarrow \\
\left(\mathrm{H}^2_\Sigma(K, E_{p^\infty})\right)^\vee & & & & Y_0
\end{array}
$$

$$\begin{array}{ccccc}
\left(\mathrm{H}^1_\Sigma(K_\infty, E_{p^\infty})_\Gamma\right)^\vee & \xrightarrow{\text{duality}} & Y^\Gamma & \xrightarrow{\alpha} & Y_\Gamma \\
\uparrow & & & & \downarrow \\
\left(\mathrm{H}^2_\Sigma(K, E_{p^\infty})\right)^\vee & & \xrightarrow{p\text{-adic height}} & & Y_0
\end{array}$$

$$
\begin{array}{ccccc}
\left(\mathrm{H}^1_\Sigma(K_\infty, E_{p^\infty})_\Gamma\right)^\vee & \xrightarrow{\text{duality}} & Y^\Gamma & \xrightarrow{\alpha} & Y_\Gamma \\
\Big\uparrow {\scriptstyle \sim ?} & & & & \Big\downarrow {\scriptstyle \sim} \\
\left(\mathrm{H}^2_\Sigma(K, E_{p^\infty})\right)^\vee & & \xrightarrow{p\text{-adic height}} & & Y_0
\end{array}
$$

$$\begin{array}{ccccc}
\left(\mathrm{H}^1_\Sigma(K_\infty, E_{p^\infty})_\Gamma\right)^\vee & \xrightarrow{\text{duality}} & Y^\Gamma & \xrightarrow{\alpha} & Y_\Gamma \\
\uparrow{\scriptstyle \sim ?} & & & & \downarrow{\scriptstyle \sim} \\
\left(\mathrm{H}^2_\Sigma(K, E_{p^\infty})\right)^\vee & & \xrightarrow{p\text{-adic height}} & & Y_0
\end{array}$$

If this p-adic height pairing is non-degenerate, then

$$\begin{array}{ccccc} \left(\mathrm{H}^1_\Sigma(K_\infty, E_{p^\infty})_\Gamma\right)^\vee & \xrightarrow{\text{duality}} & Y^\Gamma & \xrightarrow{\alpha} & Y_\Gamma \\ {\scriptstyle \sim?}\uparrow & & & & \downarrow{\scriptstyle \sim} \\ \left(\mathrm{H}^2_\Sigma(K, E_{p^\infty})\right)^\vee & & \xrightarrow{p\text{-adic height}} & & Y_0 \end{array}$$

If this p-adic height pairing is non-degenerate, then

- Y is Λ-torsion

$$
\begin{array}{ccccc}
\left(\mathrm{H}^1_\Sigma(K_\infty, E_{p^\infty})_\Gamma\right)^\vee & \xrightarrow{\text{duality}} & Y^\Gamma & \xrightarrow{\alpha} & Y_\Gamma \\
\uparrow{\scriptstyle \sim ?} & & & & \downarrow{\scriptstyle \sim} \\
\left(\mathrm{H}^2_\Sigma(K, E_{p^\infty})\right)^\vee & & \xrightarrow{p\text{-adic height}} & & Y_0
\end{array}
$$

If this p-adic height pairing is non-degenerate, then

- Y is Λ-torsion
- $\mathrm{H}^2_\Sigma(K_\infty, E_{p^\infty}) = 0$

$$\begin{array}{ccccc}
\left(\mathrm{H}^1_\Sigma(K_\infty, E_{p^\infty})_\Gamma\right)^\vee & \xrightarrow{\text{duality}} & Y^\Gamma & \xrightarrow{\alpha} & Y_\Gamma \\
\uparrow {\scriptstyle \sim ?} & & & & \downarrow {\scriptstyle \sim} \\
\left(\mathrm{H}^2_\Sigma(K, E_{p^\infty})\right)^\vee & & \xrightarrow{p\text{-adic height}} & & Y_0
\end{array}$$

If this p-adic height pairing is non-degenerate, then

- Y is Λ-torsion
- $\mathrm{H}^2_\Sigma(K_\infty, E_{p^\infty}) = 0$
- "$\sim$?" is "$\sim$".

$$
\begin{array}{ccccc}
\left(\mathrm{H}^1_\Sigma(K_\infty, E_{p^\infty})_\Gamma\right)^\vee & \xrightarrow{\text{duality}} & Y^\Gamma & \xrightarrow{\alpha} & Y_\Gamma \\
\Big\uparrow {\scriptstyle \sim ?} & & & & \Big\downarrow {\scriptstyle \sim} \\
\left(\mathrm{H}^2_\Sigma(K, E_{p^\infty})\right)^\vee & & \xrightarrow{p\text{-adic height}} & & Y_0
\end{array}
$$

If this p-adic height pairing is non-degenerate, then

- Y is Λ-torsion
- $\mathrm{H}^2_\Sigma(K_\infty, E_{p^\infty}) = 0$
- "$\sim$?" is "$\sim$".

Weak Leopoldt conjecture

Lemma

Let be Y a torsion Λ-module and $\alpha\colon Y^\Gamma \to Y_\Gamma$.

- Then $\ker(\alpha)$ and $\operatorname{coker}(\alpha)$ are finite if and only if

$$\operatorname{ord}_T \operatorname{char}_\Lambda(Y) = \operatorname{rk} Y^\Gamma.$$

- If so, then the leading term is

$$\frac{\#\operatorname{coker}(\alpha)}{\#\ker(\alpha)},$$

up to a unit in $\mathbb{Z}_p$.

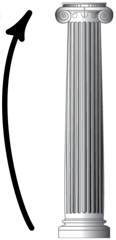
L values

Selmer groups

**p-adic
L-function**

L values

**Selmer
groups**


p-adic L-function
modular symbols
L values
Selmer groups

Suppose $E/\mathbb{Q}$ has good reduction.

Suppose $E/\mathbb{Q}$ has good reduction. Let α be a root of $X^2 - a_p X + p$ with $\mathrm{ord}_p(\alpha) < 1$.

Suppose $E/\mathbb{Q}$ has good reduction. Let α be a root of $X^2 - a_p X + p$ with $\mathrm{ord}_p(\alpha) < 1$.

p-adic L-function

There exists a p-adic L-function $\mathcal{L}_\alpha \in \Lambda \otimes \mathbb{Q}_p$ such that

$$\mathcal{L}_\alpha(\chi) = \chi(\mathcal{L}_\alpha) = \frac{p^n}{\alpha^n} \cdot \frac{L\big(E, \chi^{-1}, 1\big)}{\tau(\chi^{-1}) \cdot \Omega}$$

for all characters $\mathbb{1} \neq \chi$ on Γ of conductor p^n.

- $D_p(E) = \mathbb{Q}_p\omega \oplus \mathbb{Q}_p\eta$, Dieudonné module with $\eta = x\omega$ with φ

- $D_p(E) = \mathbb{Q}_p\omega \oplus \mathbb{Q}_p\eta$, Dieudonné module with $\eta = x\omega$ with φ
- $\Lambda \subset \mathcal{H} \subset \mathbb{Q}_p[\![T]\!]$, logarithmic growth

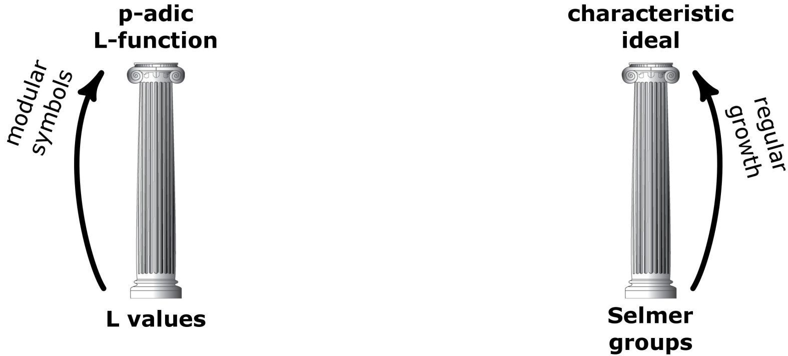
- $D_p(E) = \mathbb{Q}_p\omega \oplus \mathbb{Q}_p\eta$, Dieudonné module with $\eta = x\omega$ with φ
- $\Lambda \subset \mathcal{H} \subset \mathbb{Q}_p[\![T]\!]$, logarithmic growth
- There exists a p-adic L-function $\mathcal{L}_p \in \mathcal{H} \otimes D_p(E)$ such that

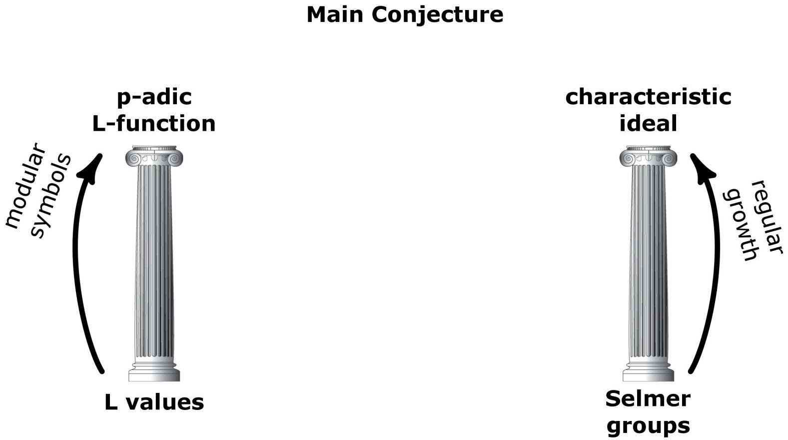
$$(p\varphi)^n \chi(\mathcal{L}_p) = \frac{L_{\{p\}}\left(E, \chi^{-1}, 1\right)}{\tau(\chi^{-1}) \cdot \Omega} \cdot \omega$$

- $D_p(E) = \mathbb{Q}_p\omega \oplus \mathbb{Q}_p\eta$, Dieudonné module with $\eta = x\omega$ with φ
- $\Lambda \subset \mathcal{H} \subset \mathbb{Q}_p[\![T]\!]$, logarithmic growth
- There exists a p-adic L-function $\mathcal{L}_p \in \mathcal{H} \otimes D_p(E)$ such that

$$(p\varphi)^n \chi(\mathcal{L}_p) = \frac{L_{\{p\}}\big(E, \chi^{-1}, 1\big)}{\tau(\chi^{-1}) \cdot \Omega} \cdot \omega$$

- Written in the basis of eigenvectors e_α, e_β such that $e_\alpha + e_\beta = \omega$ on $D_p(E)$, we get $\mathcal{L}_p = \mathcal{L}_\alpha e_\alpha + \mathcal{L}_\beta e_\beta$


p-adic
L-function
modular
symbols
L values
characteristic
ideal
regular
growth
Selmer
groups


Main Conjecture
p-adic
L-function
modular
symbols
L values
characteristic
ideal
regular
growth
Selmer
groups

- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_\Sigma(\mathbb{Q}_n, T_pE) = \mathrm{H}^1_\Sigma(\mathbb{Q}, T_pE \otimes \Lambda)$

- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_\Sigma(\mathbb{Q}_n, T_pE) = \mathrm{H}^1_\Sigma(\mathbb{Q}, T_pE \otimes \Lambda)$
- Coleman map by Perrin-Riou (logarithme élargi)

$$\mathrm{Col}\colon \mathbb{H}^1_{\mathsf{Iw}} \to \mathcal{H} \otimes D_p(E)$$

- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_\Sigma(\mathbb{Q}_n, T_pE) = \mathrm{H}^1_\Sigma(\mathbb{Q}, T_pE \otimes \Lambda)$
- Coleman map by Perrin-Riou (logarithme élargi)

$$\mathrm{Col}\colon \mathbb{H}^1_{\mathsf{Iw}} \to \mathcal{H} \otimes D_p(E)$$

- J the image of Col

- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_\Sigma(\mathbb{Q}_n, T_pE) = \mathrm{H}^1_\Sigma(\mathbb{Q}, T_pE \otimes \Lambda)$
- Coleman map by Perrin-Riou (logarithme élargi)

$$\mathrm{Col}\colon \mathbb{H}^1_{\mathsf{Iw}} \to \mathcal{H} \otimes D_p(E)$$

- J the image of Col
- $I = J \cdot \mathrm{char}_\Lambda(Y)$

- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_\Sigma(\mathbb{Q}_n, T_pE) = \mathrm{H}^1_\Sigma(\mathbb{Q}, T_pE \otimes \Lambda)$
- Coleman map by Perrin-Riou (logarithme élargi)

$$\mathrm{Col}\colon \mathbb{H}^1_{\mathsf{Iw}} \to \mathcal{H} \otimes D_p(E)$$

- J the image of Col
- $I = J \cdot \mathrm{char}_\Lambda(Y)$
- Think of I as the char_Λ of the usual Selmer group

- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_\Sigma(\mathbb{Q}_n, T_pE) = \mathrm{H}^1_\Sigma(\mathbb{Q}, T_pE \otimes \Lambda)$
- Coleman map by Perrin-Riou (logarithme élargi)

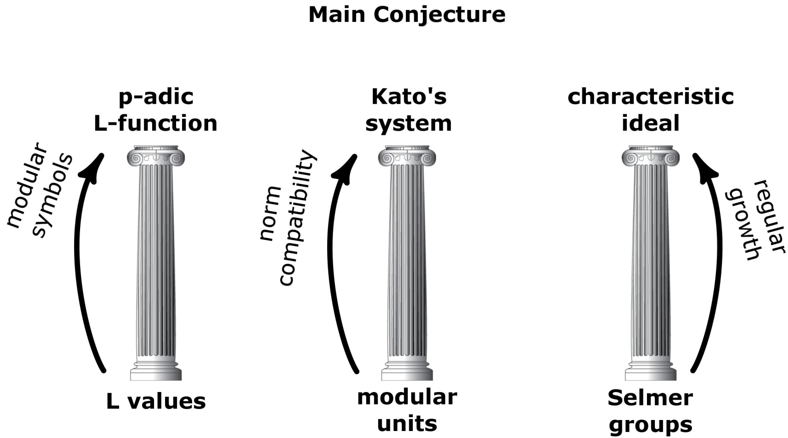
$$\mathrm{Col}\colon \mathbb{H}^1_{\mathsf{Iw}} \to \mathcal{H} \otimes D_p(E)$$

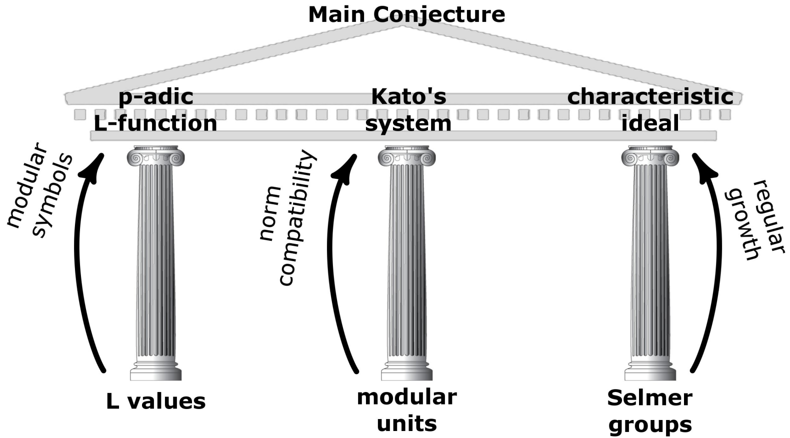
- J the image of Col
- $I = J \cdot \mathrm{char}_\Lambda(Y)$
- Think of I as the char_Λ of the usual Selmer group

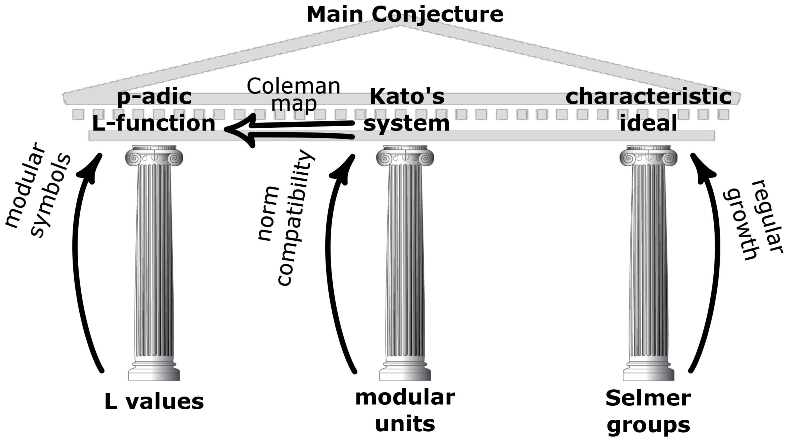
Main conjecture

$$\mathcal{L}_p\,\Lambda = I$$

Main Conjecture


Main Conjecture
p-adic
L-function
Kato's
system
characteristic
ideal
modular
symbols
norm
compatibility
regular
growth
L values
modular
units
Selmer
groups


Main Conjecture
p-adic L-function
Kato's system
characteristic ideal
modular symbols
norm compatibility
regular growth
L values
modular units
Selmer groups


Main Conjecture
p-adic
L-function
Coleman
map
Kato's
system
characteristic
ideal
modular
symbols
norm
compatibility
regular
growth
L values
modular
units
Selmer
groups

- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_{\Sigma}(\mathbb{Q}_n, T_pE)$

- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_\Sigma(\mathbb{Q}_n, T_pE)$
- Kato's Euler system $\mathbf{c} \in \mathbb{H}^1_{\mathsf{Iw}} \otimes \mathbb{Q}_p$

- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_\Sigma(\mathbb{Q}_n, T_pE)$
- Kato's Euler system $\mathbf{c} \in \mathbb{H}^1_{\mathsf{Iw}} \otimes \mathbb{Q}_p$
- Coleman map

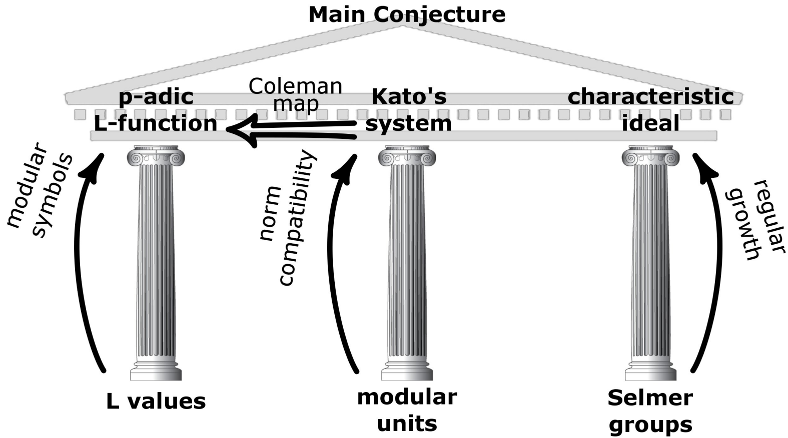
$$\mathrm{Col}\colon \mathbb{H}^1_{\mathsf{Iw}} \to \mathcal{H} \otimes D_p(E)$$

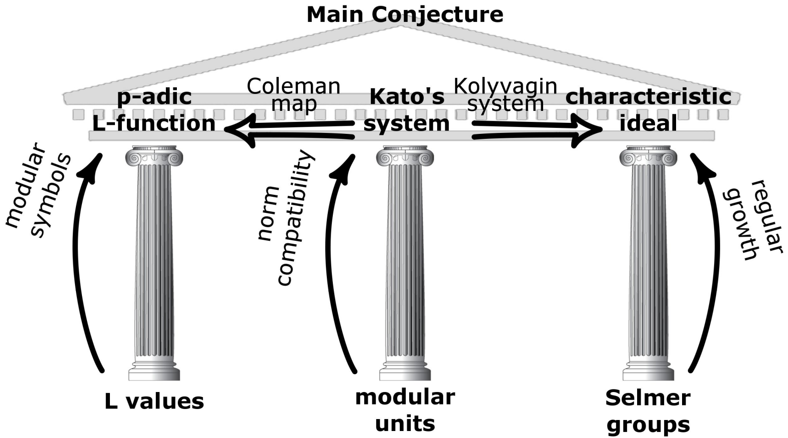
- $\mathbb{H}^1_{\mathsf{Iw}} = \varprojlim \mathrm{H}^1_\Sigma(\mathbb{Q}_n, T_pE)$
- Kato's Euler system $\mathbf{c} \in \mathbb{H}^1_{\mathsf{Iw}} \otimes \mathbb{Q}_p$
- Coleman map

$$\mathrm{Col} \colon \mathbb{H}^1_{\mathsf{Iw}} \to \mathcal{H} \otimes D_p(E)$$

Kato

$$\mathrm{Col}(\mathbf{c}) = \mathcal{L}_p$$


Main Conjecture
p-adic
L-function
Coleman
map
Kato's
system
characteristic
ideal
modular
symbols
norm
compatibility
regular
growth
L values
modular
units
Selmer
groups


Main Conjecture
p-adic L-function
Coleman map
Kato's system
Kolyvagin system
characteristic ideal
modular symbols
norm compatibility
regular growth
L values
modular units
Selmer groups

Kato's Theorem

Suppose $E/\mathbb{Q}$ has good reduction at p and that $\rho_p: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$ is surjective.

Kato's Theorem

Suppose $E/\mathbb{Q}$ has good reduction at p and that $\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$ is surjective.

- Y is Λ-torsion

Kato's Theorem

Suppose $E/\mathbb{Q}$ has good reduction at p and that $\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$ is surjective.

- Y is Λ-torsion
- $\mathcal{L}_p$ belongs to I

p-adic Birch and Swinnerton-Dyer conjecture

$\mathcal{L}_p$ vanishes to the order $\operatorname{rk} E(\mathbb{Q})$

p-adic Birch and Swinnerton-Dyer conjecture

$\mathcal{L}_p$ vanishes to the order $\operatorname{rk} E(\mathbb{Q})$ and the leading term is

 $\cdot \operatorname{Reg}_p(E/\mathbb{Q}) \cdot \#Ш(E/\mathbb{Q})$.

p-adic Birch and Swinnerton-Dyer conjecture

$\mathcal{L}_p$ vanishes to the order $\operatorname{rk} E(\mathbb{Q})$ and the leading term is

 $\cdot \operatorname{Reg}_p(E/\mathbb{Q}) \cdot \#Ш(E/\mathbb{Q})$.

Theorem

- $\operatorname{ord}_T \mathcal{L}_p \geqslant \operatorname{rk} E(\mathbb{Q})$.

p-adic Birch and Swinnerton-Dyer conjecture

$\mathcal{L}_p$ vanishes to the order $\operatorname{rk} E(\mathbb{Q})$ and the leading term is

 $\cdot \operatorname{Reg}_p(E/\mathbb{Q}) \cdot \#Ш(E/\mathbb{Q})$.

Theorem

- $\operatorname{ord}_T \mathcal{L}_p \geqslant \operatorname{rk} E(\mathbb{Q})$.
- If we have equality and the p-adic height is non-degenerate, then leading term gives an upper bound for $\#Ш(E/\mathbb{Q})(p)$.

So, why do we need p-adic L-functions?

- To prove the weak Leopoldt conjecture

So, why do we need p-adic L-functions?

- To prove the weak Leopoldt conjecture
- To have an upper bound on the characteristic series

So, why do we need p-adic L-functions?

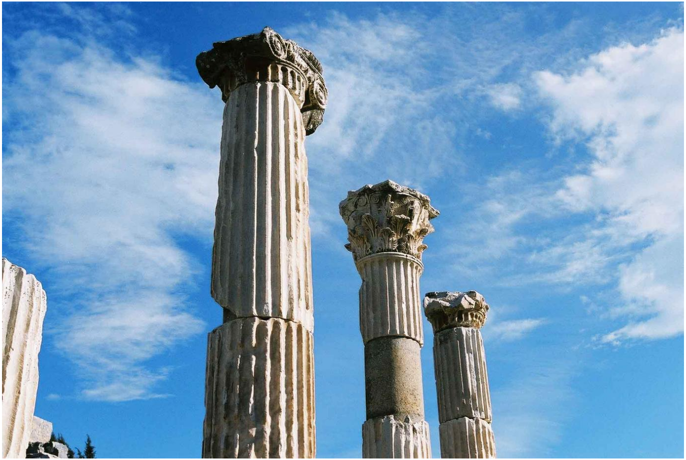
- To prove the weak Leopoldt conjecture
- To have an upper bound on the characteristic series
- Compute Selmer groups of $\mathbb{Q}_\infty$

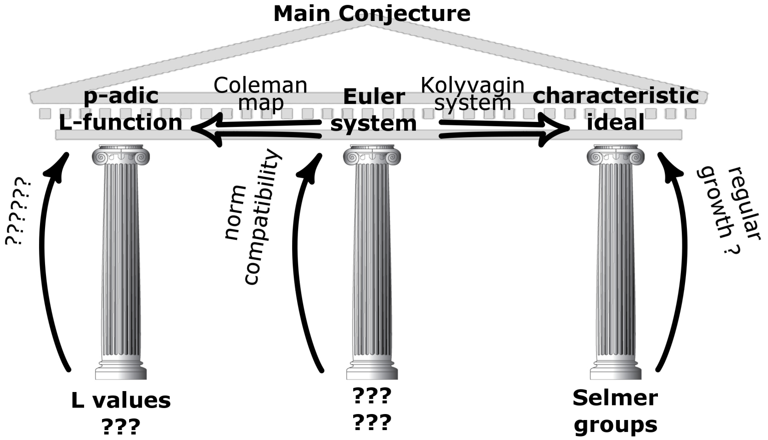
So, why do we need p-adic L-functions?

- To prove the weak Leopoldt conjecture
- To have an upper bound on the characteristic series
- Compute Selmer groups of $\mathbb{Q}_\infty$
- Compute $E(\mathbb{Q}_\infty)$

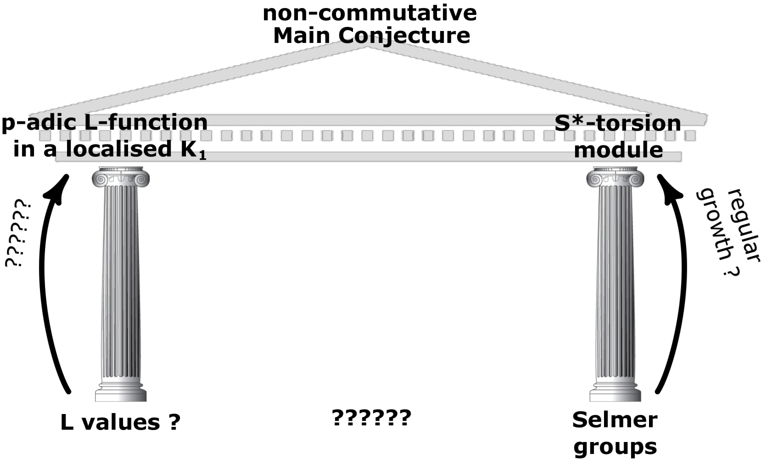
Iwasawa theory for Galois representations

V a finite dimensional vector space with an action by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Suppose V is crystalline.




Main Conjecture
p-adic
L-function
Coleman
map
Euler
system
Kolyvagin
system
characteristic
ideal
??????
norm
compatibility
regular
growth ?
L values
???
???
???
Selmer
groups

Non-commutative Iwasawa theory


non-commutative
Main Conjecture
p-adic L-function
in a localised K₁
S*-torsion
module
??????
regular
growth ?
L values ?
??????
Selmer
groups