MODULAR SYMBOLS AND p-ADIC L-FUNCTIONS

Lecture 1 for sage-days 22 miseri

Fixed for all the lectures we have a elliptic curve

$$E/\mathbb{Q} \; : \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

with $a_i \in \mathbb{Z}$.

N will denote the conductor of E. If $p \neq 2,3$ then

$p \,\|\, N \iff$ mult. red.
$p^2 \,\|\, N \iff$ additive red.
$p \nmid N \iff$ good red.

For each prime p, we define

$$a_p = \begin{cases} p+1-\#\tilde{E}(\mathbb{F}_p) & \text{if } p \text{ good} \\ +1 & \text{split mult} \\ -1 & \text{non-split mult} \\ 0 & \text{additive.} \end{cases}$$

We also set

$p \nmid N \qquad a_{p^{n+1}} = a_p \cdot a_{p^n} - p \cdot a_{p^{n-1}} \quad$ for all $n \geq 1$

and

$$a_{n \cdot m} = a_n \cdot a_m \quad \text{if} \quad (n,m) = 1.$$

Written in one formula we can say that

$$a_{pn} = a_p \cdot a_n - p \cdot a_{n/p} \qquad \forall n \; \forall p \nmid N$$

 if we agree that $a_{\frac{n}{p}} = 0$ whenever $p \nmid n$.

The complex L-function is then defined as

$$L(E,s) = \sum_{n\geq 1} \frac{a_n}{n^s} \quad \text{for } \operatorname{Re}(s) > \frac{3}{2}.$$

The modular form associated to (the isogeny class of) E is

$$f(\tau) = \sum_{n\geq 1} a_n q^n \qquad \text{where } q = e^{2\pi i \tau}$$

for $\tau \in \mathcal{H} = \{ z \in \mathbb{C} \mid \operatorname{Im}(z) > 0 \}$

We will also use the differential form

$$\omega_f = f \cdot \frac{dq}{q} = 2\pi i \, f \, d\tau$$

MODULAR SYMBOLS

We define

$$\lambda(r) = -\int_r^{i\infty} 2\pi i \, f \, d\tau \qquad \text{for } r \in \mathbb{Q}$$

Proposition 1:

$$L(E,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) \, t^s \frac{dt}{t}$$

Proof:

$$\text{rhs} = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty \sum_{n\geq 1} a_n e^{-2\pi n \cdot t} \, t^{s-1} \, dt$$

$$= \sum_{n\geq 1} a_n \frac{(2\pi)^s}{\Gamma(s)} \underbrace{\int_0^\infty e^{-2\pi n t} \, t^{s-1} \, dt}_{\frac{\Gamma(s)}{(2\pi n)^s}} \underset{\operatorname{Re}(s) > \frac{3}{2}}{=} L(E,s)$$

B

Cor 2 : $\lambda(0) = L(E,1)$

$$\lambda(0) = \cancel{2\pi\cdot(-i)}\int_0^\infty f(it)\, d(\cancel{i}t) = L(E,1). \quad \blacksquare$$

Of course we have

$$\lambda(r) = -\int_{e^{2\pi i r}}^{0} f \frac{dq}{q} = \Big[\sum_{n\geq 1} \frac{a_n}{n} q^n \Big]_0^{e^{2\pi i r}}$$

$$= \sum_{n\geq 1} \frac{a_n}{n}\cdot e^{2\pi i n r} \qquad \text{very slowly!}$$

Obviously $\lambda(r+1) = \lambda(r)$

Proposition 3 :

$$a_p \cdot \lambda(r) = \lambda(pr) + \sum_{j=0}^{p-1} \lambda\left(\frac{r+j}{p}\right)$$

for all $p \nmid N$.

Proof : $\text{rhs} = \sum_{m\geq 1} \frac{a_m}{m} e^{2\pi i m p r} + \sum_{j=0}^{p-1} \sum_{m\geq 1} \frac{a_m}{m} e^{2\pi i m \frac{r+j}{p}}$

$$= \quad + \sum_{m\geq 1} \frac{a_m}{m} e^{2\pi i m r/p} \cdot \underbrace{\sum_{j=0}^{p-1} e^{2\pi i m j/p}}_{= \begin{cases} p & \text{if } p\mid m \\ 0 & \text{else}\end{cases}}$$

$n = pm \qquad\qquad np = m$

$$= \sum_{\substack{n\geq 1 \\ p\mid n}} \frac{a_{n/p}}{n/p} e^{2\pi i n r} + \sum_{n\geq 1} \frac{a_{np}}{n\cancel{p}} e^{2\pi i n r}\cdot \cancel{p}$$

$$= \sum_{n\geq 1} \frac{1}{n} \underbrace{\left(p\cdot a_{n/p} + a_{n\cdot p}\right)}_{a_p \cdot a_n} e^{2\pi i n r} = a_p \cdot \lambda(r) \qquad \blacksquare$$

I am hiding Hecke operators here!

C

Modular Parametrisation

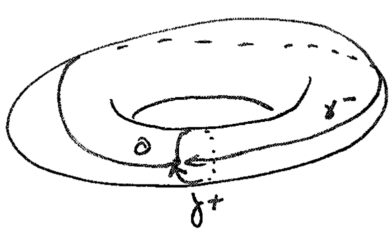
Let ω_E be the invariant differential on E.

Modularity Theorem 4

- ω_f is invariant under $\Gamma_0(N)$
- There is a morphism of curves
$$\varphi : \begin{array}{ccc} X_0(N) & \longrightarrow & E \\ \infty & \longmapsto & 0 \end{array}$$
defined over $\mathbb{Q}$
- There is a constant $c_E \in \mathbb{Z}$ st
$$\omega_f = c_E \cdot \varphi^*(\omega_E)$$

Too hard.

Choose a basis $\{\gamma^+, \gamma^-\}$ of $H_1(E(\mathbb{C}), \mathbb{Z})^{\pm}$



$E(\mathbb{C}) = \mathbb{C}/\Lambda_E$ for a lattice Λ_E

$$\Omega^{\pm} = \int_{\gamma^{\pm}} \omega_E \quad \text{so} \quad \Omega^+ \in \mathbb{R}_{>0}$$
$$\text{and} \quad \Omega^- \in i\mathbb{R}_{>0}$$

There are two cases

$E(\mathbb{R})$ is connected

$\Lambda_E = \mathbb{Z}\Omega^+ + \mathbb{Z}\Omega^-$

$E(\mathbb{R})$ has two components

$\Lambda_E = \mathbb{Z}\Omega^+ + \mathbb{Z}(\Omega^- + \frac{1}{2}\Omega^+)$

Lemma 5: If $M \in \Gamma_0(N)$ and $\tau \in \mathcal{H}$ then
$$\int_{\tau}^{M\tau} \omega_f \in \frac{c_E}{2} \Lambda_E$$

Pf: The path from τ to $M\tau$ maps to a closed path on $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H}$.

So
$$\int_\tau^{M\tau} \omega_f = c_E \cdot \int \omega_E \in c_E(\mathbb{Z}\Omega^+ + \mathbb{Z}\Omega^-) \qquad \blacksquare$$
(some closed path on $E(\mathbb{C})$)

Lemma 6: If $r = \frac{a}{m}$ is a reduced fraction with $(m, N) = 1$, then
$$\lambda(r) - \lambda(0) \in c_E(\mathbb{Z}\Omega^+ + \mathbb{Z}\Omega^-)$$

Pf: $(m, aN) = 1$ gives $x, y \in \mathbb{Z}$ s.t. $m \cdot x - aN \cdot y = 1$

Set $M = \begin{pmatrix} x & a \\ Ny & m \end{pmatrix} \in \Gamma_0(N)$ and $M0 = r$

So
$$\lambda(r) - \lambda(0) = \int_0^r \omega_f \qquad \blacksquare$$

Theorem 7: Let $\ell \nmid N$ and set $N_\ell = \# \tilde{E}(\mathbb{F}_\ell)$. Then
$$\lambda\left(\tfrac{a}{m}\right) \in \frac{c_E}{N_\ell} \cdot (\mathbb{Z}\Omega^+ + \mathbb{Z}\Omega^-) \qquad (m, N) = 1$$

Pf: From Lemma 6, it suffices to show that $N_\ell \cdot \lambda(0) \in \mathbb{Z}\Omega^+ + \mathbb{Z}\Omega^-$.

Prop 3 with $r = 0$ gives
$$N_\ell \cdot \lambda(0) = a_\ell \lambda(0) - (\ell + 1)\lambda(0) = \sum_{j=0}^{\ell-1} \left(\lambda\left(\tfrac{j}{\ell}\right) - \lambda(0)\right) \qquad \blacksquare$$

Cor 8: There is an integer $t \in \mathbb{Z}$ such that
$$\lambda\left(\tfrac{a}{m}\right) \in \frac{1}{t} \cdot (\mathbb{Z}\Omega^+ + \mathbb{Z}\Omega^-)$$

In particular $\lambda(0) \in \frac{1}{t}(\qquad)$.

In fact one can take $t = \dfrac{c_E}{\# E(\mathbb{Q})_{tors}}$

E

For $r = \frac{a}{m}$ with $(m, N) = 1$, we define

$$\lambda(r) = [r]^{+} \underbrace{\Omega^{+}}_{\text{real part}} + [r]^{-} \underbrace{\Omega^{-}}_{\text{imaginary part}}$$

with $[r]^{\pm} \in \frac{1}{t}\mathbb{Z} \subset \mathbb{Q}$.

Lemma 9: $$[r]^{\pm} = \frac{\lambda(r) \pm \lambda(-r)}{2\,\Omega^{\pm}}$$ ∎

In particular $$[0]^{+} = \frac{\lambda(0)}{\Omega^{+}} = \frac{L(E,1)}{\Omega^{+}} \in \mathbb{Q}$$

and $[0]^{-} = 0$.

Congruences

From now on p is a prime $p \nmid N$.

Choose a solution $\alpha \in \mathbb{Z}_p$ of $X^2 - a_p X + p = 0$

So $\beta = \frac{p}{\alpha} = a_p - \alpha$ is the other solution.

Define $$\mu_n^{\pm}(r) = \frac{1}{\alpha^{n+1}}\left[\frac{r}{p^{n+1}}\right]^{\pm} - \frac{1}{\alpha^{n+2}}\left[\frac{r}{p^{n}}\right]^{\pm} \in \mathbb{Q}_p$$

for $n \geq 0$ and $r = \frac{a}{m}$ with $(m, pN) = 1$.

Lemma 10: $$\sum_{j=0}^{p-1} \mu_n^{\pm}(r + jp^n) = \mu_{n-1}^{\pm}(r) \quad \forall\, n \geq 1$$

Pf: $$\text{lhs} = \frac{1}{\alpha^{n+1}} \sum_{j=0}^{p-1}\left[\frac{r\cdot p^{n} + j}{p}\right]^{\pm} - \frac{1}{\alpha^{n+2}} \sum_{j=0}^{p-1}\left[\frac{r}{p^n} + j\right]^{\pm}$$

$$= \frac{1}{\alpha^{n+1}}\left(\cancel{a_p \cdot \left[\frac{r}{p^n}\right]^{\pm}} - \left[p \cdot \frac{r}{p^n}\right]^{\pm}\right) - \frac{1}{\alpha^{n+1}} \cdot \underbrace{\frac{p}{\alpha}}_{(\cancel{a_p} - \alpha)} \cdot \left[\frac{r}{p^n}\right]^{\pm}$$

F

$$= -\frac{1}{\alpha^{n+1}}\left[\frac{r}{p^{n-1}}\right]^{\pm} + \frac{1}{\alpha^{n}}\left[\frac{r}{p^n}\right]^{\pm} = \text{rhs}$$ ∎

Lemma 11: $\displaystyle\sum_{j=1}^{p-1} \mu_0^{\pm}(j) = \left(1-\frac{1}{\alpha}\right)^2 \cdot [0]^{\pm}$

Pf: $\displaystyle \text{lhs} = \frac{1}{\alpha}\sum_{j=0}^{p-1}\left[\frac{j}{p}\right]^{\pm} - \frac{1}{\alpha^2}p\cdot[0]^{\pm} - \frac{1}{\alpha}[0]^{\pm}$

$$= \frac{1}{\alpha}\left(a_p\cdot[0]^{\pm} - [0]^{\pm}\right) - \frac{1}{\alpha}(a_p-\alpha)[0]^{\pm} - \frac{1}{\alpha}[0]^{\pm}$$

$$= \left(1-\frac{2}{\alpha}+\frac{1}{\alpha^2}\right)[0]^{\pm} \qquad \blacksquare$$

THE p-ADIC L-FUNCTION

Suppose now that p is ordinary, too, i.e. $p \nmid a_p$. There is a unique $\alpha \in \mathbb{Z}_p^\times$ solving $X^2 - a_p X + p = 0$.

Let $K_n = \mathbb{Q}(\mu_{p^{n+1}})$ for $n \geq 0$.

and
$$G_n = \mathrm{Gal}(K_n/\mathbb{Q}) \xleftarrow{\cong} (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$$
$$\sigma_a \longleftarrow a$$

Set
$$\lambda_n = \sum_{a\in(\mathbb{Z}/p^{n+1})^\times} \left(\mu_n^+(a) + \mu_n^-(a)\right)\cdot\sigma_a \in \mathbb{Q}_p[G_n]$$

Theorem 12: $\mathcal{L}_p(E) := (\lambda_n)_n \in \varprojlim_n \frac{1}{t}\mathbb{Z}_p[G_n] = \frac{1}{t}\cdot\Lambda$

with the transition maps from $G_n \twoheadrightarrow G_{n-1}$, $\sigma_a \longmapsto \sigma_b$

Proof: λ_n is mapped to if $a = b + p^n j$

$$\sum_{b\in(\mathbb{Z}/p^n)^\times} \underbrace{\sum_{j=0}^{p} (\mu_n^+ + \mu_n^-)(b + j p^n)}_{(\mu_n^+ + \mu_n^-)(b) \text{ by L. 11.}} \cdot \sigma_b$$

Twists

Let $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ be a Dirichlet character modulo $m = \text{conductor}(\chi)$.

We define the twisted L-series by

$$L(E,\chi,s) = \sum_{n \geq 1} \frac{\chi(n) a_n}{n^s} \qquad Re(s) > \frac{3}{2}.$$

and the twisted modular form by

$$f_\chi(\tau) = \sum_{n \geq 1} \chi(n)\, a_n \cdot q^n$$

Lemma 13
$$G(\chi) \cdot f_{\overline{\chi}}(\tau) = \sum_{a \bmod m} \chi(a) \cdot f\left(\tau + \frac{a}{m}\right)$$

where
$$G(\chi) = \sum_{a \bmod m} \chi(a) \cdot e^{2\pi i a/m}$$ is the Gauss sum.

Pf: $$G(\chi)\, f_{\overline{\chi}}(\tau) = \sum_{\substack{b \\ an = b}} \chi(b)\, e^{2\pi i b/m} \sum_{\substack{n \geq 1 \\ (n,m)=1}} a_n\, \overline{\chi}(n)\, e^{2\pi i n \tau}$$

$$= \sum_{\substack{n \geq 1 \\ (n,m)=1}} \sum_{a \bmod m} \chi(an)\, e^{2\pi i\, na/m} \cdot a_n\, \overline{\chi(n)} \cdot e^{2\pi i n \tau}$$

$$= \sum_{a} \chi(a) \sum_{\substack{n \geq 1 \\ \cancel{(n,m)=1}}} a_n\, e^{2\pi i n \left(\tau + \frac{a}{m}\right)} \qquad \blacksquare$$

Recall $|G(\chi)| = \sqrt{m}$ and $G(\overline{\chi}) = \chi(-1) \cdot \overline{G(\chi)}$.

H

Theorem 14 Suppose $(m, N) = 1$.

$$\frac{G(\chi) \cdot L(E, \bar{\chi}, 1)}{\Omega^{\chi(-1)}} = \sum_{a \bmod m} \chi(a) \left[\frac{a}{m}\right]^{\chi(-1)}$$

belongs to $\mathbb{Q}(\chi)$

Proof: $L(E, \bar{\chi}, 1) = -\int_0^{i\infty} 2\pi i f_{\bar{\chi}}\, d\tau$

So

$$G(\chi) \cdot L(E, \bar{\chi}, 1) = -2\pi i \int_0^{i\infty} \sum_{a \bmod m} \chi(a) \cdot f(\underbrace{\tau + \tfrac{a}{m}}_{z})\, d\tau$$

$$= \sum_{a \bmod m} \chi(a) \left(-2\pi i\right) \int_{a/m}^{i\infty} f(z)\, dz$$

$$= \sum_{a \bmod m} \chi(a)\, \lambda\left(\frac{a}{m}\right) = \sum \chi(a) \left[\frac{a}{m}\right]^{+} \Omega^{+} + \sum \chi(a) \left[\frac{a}{m}\right]^{-} \Omega^{-}$$

But

$$\sum \chi(a) \left[\frac{a}{m}\right]^{-\chi(-1)} \Omega^{-\chi(-1)} = \frac{1}{2} \sum \chi(a) \cdot \left[\lambda\left(\frac{a}{m}\right) - \chi(-1)\, \lambda\left(\frac{-a}{m}\right)\right]$$

$$= \frac{1}{2}\left[\sum \chi(a)\, \lambda\left(\frac{a}{m}\right) - \sum \chi(-a)\, \lambda\left(\frac{-a}{m}\right)\right] = 0$$

■

I

A abelian extension $K/\mathbb{Q}$ has a conductor m, ie $K \subset \mathbb{Q}(\zeta_m)$ with m minimal.

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) & \longrightarrow & \mathrm{Gal}(K/\mathbb{Q}) = G \\ \downarrow \cong & & \\ (\mathbb{Z}/m\mathbb{Z})^\times & \bar{a} \longmapsto & \sigma_a \end{array}$$

$\chi : G \longrightarrow \overline{\mathbb{Q}}^\times$ extends to a Dirichlet character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \overline{\mathbb{Q}}^\times$

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^\times & \longrightarrow & \overline{\mathbb{Q}}^\times \\ \uparrow & & \\ \mathbb{Z} & \longrightarrow & \overline{\mathbb{Q}} \end{array}$$

$$L(E/K, s) = \prod_{\chi \in \hat{G}} L(E, \chi, s)$$

STICKELBERGER ELEMENTS

Suppose that K is totally real (just to avoid $-$ part!) $\chi(-1) = +1 \ \forall \chi \in \hat{G}$

$$\Theta = \sum_{a \bmod m} \left[\frac{a}{m}\right]^+ \cdot \sigma_a \in \mathbb{Q}[G]$$

Any $\chi \in \hat{G}$ we get
$$\chi : \mathbb{Q}[G] \longrightarrow \overline{\mathbb{Q}}$$
$$\sum_{g \in G} a_g \cdot g \longmapsto \sum a_g \cdot \chi(g)$$

then
$$\chi(\Theta) = \sum_{a \bmod m} \left[\frac{a}{m}\right]^+ \chi(a) = \frac{G(\chi) \cdot L(E, \bar{\chi}, 1)}{\Omega^+}$$

But Θ does not behave well under maps $G \twoheadrightarrow G'$.
Instead λ_n do.

INTERPOLATION

<u>Theorem 15</u> For any $\chi : G_n = \mathrm{Gal}(K_n/\mathbb{Q}) \longrightarrow \overline{\mathbb{Q}}^\times$ not factoring through G_{n-1}, the induced map $\chi : \Lambda \to \overline{\mathbb{Q}}_p$ sends $\mathcal{L}_p(E)$ to $\dfrac{G(\chi)}{\alpha^{n+1}} \dfrac{L(E, \bar{\chi}, 1)}{\Omega^{\chi(-1)}}$ if $n > 0$

and
$$\mathbb{1}(\mathcal{L}_p(E)) = \left(1 - \frac{1}{\alpha}\right)^2 \cdot \frac{L(E,1)}{\Omega^+}$$

3 Corollary 16: (ROHRLICH) $\mathcal{L}_n \neq 0$ ($L(E, \bar{\chi}, 1) \neq 0$ for some χ).

Pf. By lemma 11

$$\mathbb{1}(\mathcal{L}_p(E)) = \mathbb{1}(\lambda_0) = \sum_{\substack{a \bmod p \\ p \nmid a}} \left(\mu_0^+(a) + \mu_0^-(a)\right) = \left(1 - \frac{1}{\alpha}\right)^2 [0]$$

else

$$\chi(\mathcal{L}_p(E)) = \chi(\lambda_n) = \sum_{\substack{a \bmod p^{n+1} \\ p \nmid a}} \left(\mu_n^+(a) + \mu_n^-(a)\right) \cdot \chi(a)$$

$$= \frac{1}{2} \sum_a \Big(\underbrace{\mu_n^+(a)\chi(a) + \mu_n^+(-a)\chi(-a)}_{\mu_n^+(a)\chi(a)\left(1+\chi(-1)\right)}$$

$$+ \underbrace{\mu_n^-(a)\chi(a) + \mu_n^-(-a)\chi(-a)}_{\mu_n^-(a)\chi(a)\left(1-\chi(-1)\right)} \Big)$$

$$= \sum_a \mu_n^{\chi(-1)}(a) \cdot \chi(a)$$

$$= \underbrace{\frac{1}{\alpha^{n+1}} \sum_a \left[\frac{a}{p^{n+1}}\right]^{\chi(-1)} \chi(a)}_{\text{rhs}} - \frac{1}{\alpha^{n+2}} \underbrace{\sum_a \left[\frac{a}{p^n}\right]^{\chi(-1)} \chi(a)}_{?\ 0}$$

Write $a = b + jp^n$ $\quad \left[\frac{a}{p^n}\right]^{\pm} = \left[\frac{b}{p^n}\right]^{\pm}$

$$\sum_a \left[\frac{a}{p^n}\right]^{\pm} \chi(a) = \sum_{\substack{b \bmod p^n \\ p \nmid b}} \left[\frac{b}{p^n}\right]^{\pm} \cdot \sum_{j=0}^{p-1} \chi(b + jp^n)$$

$$\{\chi(b+jp^n)\}_{j=0}^{p-1} = \{\chi(b(1+p^n)^u)\}_{u=0}^{p-1}$$

?

$$\sum_{j=0}^{p-1} \chi(b + jp^n) = \chi(b) \sum_{u=0}^{p-1} \underbrace{\chi(1+p^n)}^{u} = 0$$

is a primitive p^n-th root of unity by assumption

K

p - ADIC BSD

~~Conjecture 2A~~

Write $\Gamma = \mathrm{Gal}(\bigcup_n \cancel{B}_n / \mathbb{Q})$ and $\chi_{cyc} : \Gamma \xrightarrow{\cong} \mathbb{Z}_p^\times$

st $\zeta^{\chi_{cyc}(\sigma)} = \sigma(\zeta) \quad \forall\, \sigma \in \Gamma$ and $\zeta \in \mu_{p^\infty}$.

$\chi_s = \langle \chi_{cyc} \rangle^s$ for $s \in \mathbb{C}_p$

Define

$$\mathcal{L}_p(E, s) = \chi_s(\mathcal{L}_p(E)) \in \mathbb{C}_p \quad \text{for } s \in \mathbb{C}_p .$$

So $$\mathcal{L}_p(E, 1) = \mathbb{1}(\mathcal{L}_p(E)) = \left(1 - \frac{1}{\alpha}\right)^2 \frac{L(E,1)}{\Omega^+}$$

$$\mathcal{L}_p(E, 1) = 0 \iff L(E,1) = 0 \quad \text{as } \alpha \neq 1 \, !!$$

<u>Conjecture A:</u> $\quad \mathrm{ord}_{s=1} \mathcal{L}_p(E,s) = \mathrm{ord}_{s=1} L(E,s)$

<u>Conjecture B:</u> The leading term at $s=1$ of $\mathcal{L}_p(E,s)$ is

$$\left(1 - \frac{1}{\alpha}\right)^2 \cdot \frac{\prod c_v \cdot \#Ш(E/\mathbb{Q}) \cdot \mathrm{Reg}_p(E/\mathbb{Q})}{(\# E(\mathbb{Q})_{tors})^2}$$

where $\mathrm{Reg}_p(E/\mathbb{Q})$ is the p-adic regulator $\in \mathbb{Q}_p$

<u>Conjecture C:</u> $\quad \mathrm{Reg}_p(E/\mathbb{Q}) \neq 0$.