Modular Symbols:

Aim:

$$\begin{array}{ccc} E & & BSD/K \\ \Big| & & \Big| \, ? \, \Big| \\ E & & BSD/\mathbb{Q} \end{array}$$

Start w/ $E/\mathbb{Q}$ and then go to an extension.

Periods: In general, fix ω some invariant diff on E/F, F a number field.

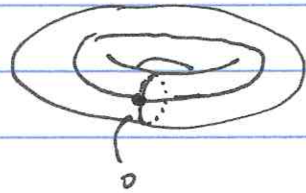
$$\Omega_v = \left| \int_{E(F_v)} \omega \right| \qquad v \text{ real}$$

$$\Omega_v = \left| 2 \int_{E(F_v)} \bar{\omega} \wedge \omega \right| \qquad v \text{ complex.}$$

From now on E is an elliptic curve $/\mathbb{Q}$. Fix a global minimal model (exists b/c $\mathbb{Q}$ has class number one)

Néron differential $\omega = \dfrac{dx}{2y + a_1 x + a_3}$ (this is a generator for $H^1(\mathcal{E}, \Omega^1_{\mathcal{E}/\mathbb{Z}})$.)

$H_1^*(E(\mathbb{C}), \mathbb{Z})$ = group of loops in $E(\mathbb{C})$ based at O / contractible loops



$H_1(E(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^2$
$\uparrow$
as abelian group

Complex conjugation acts on this H_1. There is a fixed space, for example $E^0(\mathbb{R})$ is fixed. Thus the space splits into ± 1 eigenspaces.

Let γ_+ be a generator of $H_1(E(\mathbb{C}),\mathbb{Z})^+$ and γ_- for $H_1(E(\mathbb{C}),\mathbb{Z})^-$.

Define

$$\Omega_+ = \int_{\gamma_+} \omega .$$ Moreover, we can choose γ_+ so that $\Omega_+ > 0$. (Exercise show $\Omega_+ \in \mathbb{R}$).

$$\Omega_- = \int_{\gamma_-} \omega \in \mathbb{R} i$$ and we can choose γ_- so that $\Omega_- \in (\mathbb{R}_{>0}) i$.

<u>Period map:</u>

$$H_1(E(\mathbb{C}),\mathbb{Z}) \longrightarrow \mathbb{C}$$
$$\gamma \longmapsto \int_\gamma \omega .$$

The image is a lattice Λ, called the Néron lattice of E.

From this we have

$$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda . \qquad \omega \longleftrightarrow dz.$$
$$P \longmapsto \int_0^P \omega .$$

<u>Exercise</u>: $\mathbb{Z}\Omega_+ \oplus \mathbb{Z}\Omega_- \subset \Lambda$

Link the index to $c_\infty = \#\left(E(\mathbb{R})/E^\circ(\mathbb{R})\right)$.

<u>Exercise</u>: Express Ω_v in terms of Ω_+, Ω_- and c_∞.

<u>Modularity:</u>

- N conductor of E

$X_0(N)$ = modular curve of level $\Gamma_0(N)$

$X_0(N)(\mathbb{C}) = \Gamma_0(N) \backslash \mathfrak{H}^*$ $\qquad \mathfrak{H}$ = upper half space

$\qquad \mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$.

$X_0(N)/\mathbb{Q}$ is a projective smooth curve

Theorem 1 (Wiles, Taylor, ...): Consequences we need are:

- There is a nonconstant morphism
$$\varphi_E : X_0(N) \longrightarrow E$$
$$i\infty \longmapsto 0$$

- There is a constant $c \in \mathbb{Z}$, called the Manin constant s.t. $\varphi_E^*(\omega) = c\,\omega_X$ where
$$\omega_X = \sum_{n\geq 1} a_n \frac{dq}{q} q^n = 2\pi i \sum_{n\geq 1} a_n e^{2\pi i n \tau} d\tau$$
where $\tau \in \mathfrak{H}$, $q = e^{2\pi i \tau}$ and a_n are given by
$$L(E/\mathbb{Q}, s) = \sum_{n\geq 1} \frac{a_n}{n^s} \qquad Re(s) > 3/2.$$

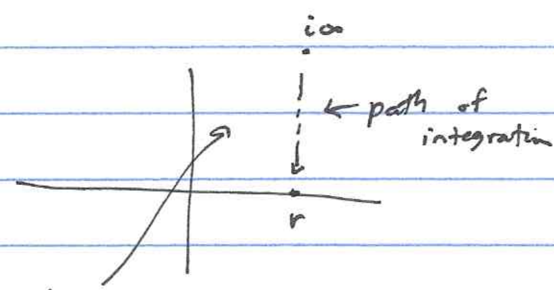
- If χ is a Dirichlet character, then $L(E,\chi,s)$ admit an analytic continuation to $\mathbb{C}$.

For each E there should be an isogenous curve with $c = 1$.
We will always take φ_E to have minimal degree and $c > 0$.
Ex: 11a3 has $c = 5$. ($N = 11$, second number lists different curves of conductor 11)

Modular Symbols:

Aim is to show $\frac{L(E,1)}{\Omega_+} \in \mathbb{Q}$.

For any $r \in \mathbb{Q}$, let $\lambda(r) = \int_{i\infty}^{r} \omega_X$



Let $\{i\infty, r\}$ be the ~~path~~ image of the path in $X_0(N)$.

Then $\lambda(r) = \int_{\{i\infty, r\}} \omega_x$. If $r \sim i\infty \mod \Gamma_0(N)$, then $\{i\infty, r\}$ is a loop.

$H_1(X_0(N)(\mathbb{C}), \mathbb{Z}; \{\text{cusps}\})$ paths going between cusps, where cusps are images of $\mathbb{Q}, \{i\infty\}$ in $X_0(N)(\mathbb{C})$. (finitely many)

So $H_1(X_0(N)(\mathbb{C}), \mathbb{Z}; \{\text{cusps}\}) = \left(\underset{\text{two cusps}}{\text{free abelian groups of paths connecting}}\right) \Big/ \text{homotopy equiv.}$

$$\underset{\otimes \mathbb{Q}_p}{=} H^1_{et}(X_0(N), \mathbb{Q}_p)^\vee.$$

$$\lambda(r) = 2\pi i \sum_{n\geq 1} a_n \int_{i\infty}^{r} e^{2\pi i n z}\, dz$$

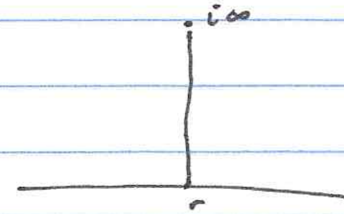
$$= \sum_{n\geq 1} \frac{a_n}{n} e^{2\pi i n r} \qquad \text{(may not converge)}$$

We will often just assume this converges. It actually converges, just very very slowly.

Modular Symbols:

$$\lambda(r) = \sum_{n \geq 1} \frac{a_n}{n} e^{2\pi i n r} \quad \text{where} \quad L(E/\mathbb{Q}, s) = \sum_{n \geq 1} \frac{a_n}{n^s}$$

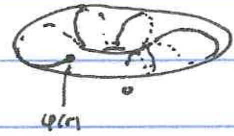
$X_0(N)$



$\mathfrak{h}$

$\downarrow$

E



$$L(E/\mathbb{Q}, s) = \prod_{p \text{ prime}} (1 - a_p p^{-s} + \delta_N(p)\, p\, p^{-2s})^{-1} \quad \text{where}$$

$$\delta_N(p) = \begin{cases} 1 & \text{if } p \nmid N \iff \text{good red.} \\ 0 & \text{if } p \mid N \end{cases}.$$

Exercise: Suppose $\gcd(n,p) = 1$, then show $a_{np} = a_n a_p$ and otherwise $a_{np} = a_n a_p - p\, a_{n/p}$. (assume p is a prime of good reduction.)

Prop. 2: Let p be a prime of good reduction. Then for all $r \in \mathbb{Q}$,
$$a_p \lambda(r) = \lambda(pr) + \sum_{a=0}^{p-1} \lambda\left(\frac{a+r}{p}\right).$$

Exercise 2: • Prove Prop. 2 from previous exercise, ~~im~~ ignoring convergence issues. (Or just use that this is Hecke operator...)

• What if $p \mid N$?

Theorem 3: (Manin, Drinfeld) There is a nonzero integer $t \in \mathbb{Z}$ s.t.

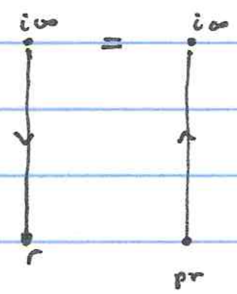
$t \cdot \lambda(r) \in \Lambda$ where Λ is the lattice that is the image of $H_1(E(\mathbb{C}), \mathbb{Z})$ under $\int \omega : H_1(E(\mathbb{C}), \mathbb{Z}) \to \mathbb{C}$.

<u>Lemma 4:</u> Let $r = \frac{u}{v}$ and $r' = \frac{u'}{v'}$ be reduced fractions. Then $r \sim r'$ under $\Gamma_0(N)$ iff $sv' \equiv s'v \pmod{\gcd(vv', N)}$ where s is an inverse of u mod v and s' is an inverse of u' mod v'. ($r \sim r'$ if $\exists \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ s.t. $\frac{ar+b}{cr+d} = r'$.)

<u>Proof:</u> Reference Cremona's book Prop. 2.2.3.
idea: $r \to i\infty \to r'$ via $SL_2(\mathbb{Z})$ and then get conditions for when this matrix is in $\Gamma_0(N)$.

<u>Proof of Thm 3:</u> Let $p \equiv 1 \pmod N$ be a prime. $r = \frac{u}{v}$
Ex: Check $pr \sim r$ under $\Gamma_0(N)$ and $\frac{u+r}{p} \sim r$.
So on $X_0(N)$, the cusps pr and r are equal so a path from pr to r is a loop. By prop. 2:

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



$$\lambda(r) - \lambda(pr) = \int_{\{r, pr\}} \omega_X$$

where $\{r, pr\}$ is the image of a path on the upper half plane from r to pr in $X_0(N)$.

We have seen that $\{r, pr\}$ is a loop.
Recall

$$c\,\omega_X = \varphi^*(\omega),$$

so

$$\int_{\{r,pr\}} \omega_X = \frac{1}{c} \int_{\varphi(\{r,pr\}) \leftarrow \text{Loop on } E(\mathbb{C})} \omega \in \frac{1}{c}\Lambda$$

Chris
6-28-11
PS3

Can do the same thing for each $\lambda(r) - \lambda(\frac{u+r}{p})$. Thus, $(p+1-a_p)\lambda(r) \in \frac{1}{c}\Lambda$. Thus, just set

$$t = c(p+1-a_p)$$

and we have the result, assuming $p+1-a_p \neq 0$. However, $t \neq 0$ b/c $p+1-a_p = \# \tilde{E}(\mathbb{F}_p)$, so it cannot be 0. ∎

<u>Cor. 5:</u> For any $r \in \mathbb{Q}$, ~~then~~ $\varphi_E(r) \in E(\mathbb{C})$ are always torsion points.

$$\begin{tikzcd} \mathfrak{h}^* \arrow[r] \arrow[drr, "\phi"'] & \Gamma_0(N)\backslash \mathfrak{h}^* = X_0(N)(\mathbb{C}) \arrow[d, "\varphi_E"] \\ & \mathbb{C}/\Lambda = E(\mathbb{C}) \end{tikzcd}$$

$$\phi(\tau) = \frac{1}{c}\int_{i\infty}^{\tau} \omega_X$$

The prop. says $\phi(r) = \frac{1}{c}\lambda(r) \in \frac{1}{t}\Lambda$. $\Rightarrow \varphi(r) \in E[ct]$.

<u>Prop. 6:</u> To each elliptic curve E, there is an isogeneous curve s.t. t can be taken coprime to all odd primes of semi-stable reduction. (unpublished work)

<u>Question:</u> What is the power of 2 and of additive primes that divide the best t?

We will be interested in the modular symbols

$$[r] := \frac{\mathrm{Re}(\lambda(r))}{\Omega_+} \in \mathbb{Q}.$$

In fact, $[r] \in \frac{1}{2t}\mathbb{Z}$!

Chris
6-28-11
pg 4

435b1:

a	0	1	2	3	4	5	6	7	8	9	10
$\left[\frac{a}{7}\right]$	1	3	$-5/2$	$-5/2$	$-5/2$	$-5/2$	3				
$\left[\frac{a}{11}\right]$	1	3	3	$-3/2$	$-3/2$	$-3/2$	$-3/2$	$-3/2$	$-7/2$	3	3

11a2:

a	0	1	2	3	4	5	6	7	8	9	10
$\left[\frac{a}{7}\right]$	1	$7/2$	$7/2$	-9	-9	$7/2$	$7/2$				
$\left[\frac{a}{11}\right]$	1	0	5	$5/2$	$-5/2$	-5	-5	$-5/2$	$5/2$	5	0

$[-r] = [r]$

$[r+1] = [r]$

$[r+k] = [r] \quad \forall k \in \mathbb{Z}$

324a1

add. red. at 2 $\quad \left[\frac{1}{9}\right] = \frac{1}{6}$

The lattice is # $\quad c = 1 \quad E(\mathbb{Q}) = \mathbb{Z}/3$.

Winding Number:

Recall $\lambda(r) = \sum \frac{a_n}{n} e^{2\pi i n r}$, $[r] = \frac{Re(\lambda(r))}{\Omega_+}$, and we saw
$Re(\lambda(r)) \in \{Re(x) : x \in \Lambda\} \subseteq \mathbb{Q} \cdot \Omega_+$.

Theorem 7: $\lambda(0) = L(E/\mathbb{Q}, 1)$.

Proof: $\lambda(0) = \sum \frac{a_n}{n} = L(E/\mathbb{Q}, 1)$. ∎
(Do need to look at convergence. Best place to see real proofs is
[Mazur-Tate-Teitelbaum, p-adic BSD])

Cor 8: $[0] = \frac{L(E/\mathbb{Q}, 1)}{\Omega_+} \in \mathbb{Q}$.

$BSD_{\mathbb{Q}}$: $[0] \stackrel{?}{=} \frac{\prod c_v \ \#Ш(E/\mathbb{Q})}{(E(\mathbb{Q})_{tors})^2}$ if $L(E,1) \neq 0$.

Theorem 9 (..., Kato, Urban-Skinner): If $L(E/\mathbb{Q}, 1) \neq 0$ ~~and~~ then $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ are finite, otherwise one of them is infinite.

A lot is also known about $BSD_{\mathbb{Q}}$.

In fact $0 \in X_0(N)(\mathbb{Q})$, so $\varphi(0)$ is in $E(\mathbb{Q})_{tors}$. Thus, the denominator of $[0]$ is a divisor of $c \cdot \# E(\mathbb{Q})_{tors}$.

Example: 11a1 $[0] = 1/5$ $\#E(\mathbb{Q}) = 5$ $c = 1$
$c_{11} = 5$ $\#Ш(E/\mathbb{Q}) = 1$.

66b3: $c_\infty = 2$ $\quad \# E(\mathbb{Q}) = 2$

$[0] = 2$ $\quad c_v = 1 \quad v \nmid \infty.$

$\Rightarrow \# Ш(E/\mathbb{Q}) = 4.$

11a3: $[0] = \frac{1}{25}$ $\quad c = 5$ $\quad \# E(\mathbb{Q}) = 5$

no cancellation in this case.

Abelian Fields:

K number field, $G = Gal(K/\mathbb{Q})$ is abelian.

$E/\mathbb{Q}$. , $K < \mathbb{Q}(\zeta_m)$ by Kronecker-Weber. The minimal such m is called the conductor of K.

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \longrightarrow G$$

$$a \longmapsto (\zeta_m \mapsto \zeta_m^a) \longmapsto \sigma_a|_K$$

Any character $\chi: G \to \mathbb{C}^\times$ can be viewed as a Dirichlet character $\chi: \mathbb{Z} \to \mathbb{C}$, e.g. $\chi(\sigma_a) = \chi(a)$ modulo m of conductor $f_\chi | m$.

H1: (hypothesis 1) No additive place ramifies in $K/\mathbb{Q}$.

H2: K is totally real (this is for convenience)

H3: The degree $d = [K:\mathbb{Q}]$ is coprime to m. (for convenience to exclude Iwasawa theory.)

H3 $\Rightarrow$ m is square-free.

Chris
6-29-11
pg 3

Stickelberger Elements:

Assume H2. Denote by

$$\sum_{a \bmod m^\times} = \sum_{\substack{a \bmod m \\ (a,m)=1}} .$$

$$\Theta = \Theta_{E/K} = \sum_{a \bmod m^\times} \left[\frac{a}{m}\right] \cdot \sigma_a \in \mathbb{Q}[G]$$

Example: 43561 $m=7$ $d=3$

$K = \mathbb{Q}(\zeta_7)^+$ Using the list from last time we get

$\Theta = 3\sigma_1 - 5/2\,\sigma_2 - 5/2\,\sigma_3 - 5/2\,\sigma_4 - 5/2\,\sigma_5 + 3\sigma_6.$

G $g = \sigma_3$ is a generator because 3 is a primitive root mod 7.

$\Theta = 6 \cdot 1 - 5g - 5g^2$

Lemma 10: Let ℓ be a prime $\ell \nmid m$, (H3),

$$\begin{tikzcd}[column sep=small] & L \arrow[dl, dash] \arrow[dd, dash, "\substack{ab \\ \text{cond } m\ell}"] \\ K \arrow[dr, dash, "m"'] & \\ & \mathbb{Q} \end{tikzcd}$$

$$N_{L/K} : \mathbb{Q}[\mathrm{Gal}(L/\mathbb{Q})] \to \mathbb{Q}[\mathrm{Gal}(K/\mathbb{Q})]$$
$$\sigma_a|_L \longmapsto \sigma_a|_K .$$

Then $N_{L/K}(\Theta_{E/L}) = -\sigma_\ell^{-1}|_K \left(\sigma_\ell|_K - a_\ell + \delta_N(\ell)\,\sigma_\ell^{-1}|_K\right) \Theta_{E/K}$

where

$$\delta_N(\ell) = \begin{cases} 1 & \text{if } \ell \nmid N \text{ good red.} \\ 0 & \text{o/w.} \end{cases}$$

and $N =$ conductor of E.

Proof: Chinese Remainder Theorem gives $a \bmod (m\ell)^\times$ can be written as $a = bm + c\ell$ with $b \bmod \ell^\times$ and

$c \bmod m^\times$. Then

$$N_{L/K}(\Theta_L) = \sum_{a \bmod (ml)^\times} \left[\frac{a}{ml}\right] \sigma_a$$

$$= \sum_{c \bmod m^\times} \sum_{b \bmod l^\times} \left[\frac{b + cl/m}{l}\right] \sigma_a$$

$$\cancel{\sum_{b \bmod l}} \qquad (\sigma_a = \sigma_c)$$

$$\left(\sum_{b \bmod l} \left[\frac{b+r}{l}\right] = a_l[r] - \delta_N(l)[lr] \qquad \text{(Hecke op. from last time)} \right)$$

Thus,

from $b=0$.

$$N_{L/K}(\Theta_L) = \sum_{c \bmod m^\times} \left(\left[\frac{cl}{m}\right] - \delta_N(l)\left[\frac{cl^2}{m}\right] - \left[\frac{c}{m}\right] \right)\sigma_c$$

$$= a_l \sum_{c \bmod m^\times} \left[\frac{cl}{m}\right]\sigma_c - \delta_N(l) \sum_{c \bmod m^\times} \left[\frac{cl^2}{m}\right]\sigma_c - \sum_{c \bmod m^\times} \left[\frac{c}{m}\right]\sigma_c$$

$(e = cl)$

$$= a_l \sum_{e \bmod m^\times} \left[\frac{e}{m}\right]\sigma_e \sigma_l^{-1} - \delta_N(l) \sum_{e \bmod m^\times} \left[\frac{e}{m}\right]\sigma_e \sigma_l^{-1} - \Theta_K$$

Now just rearrange terms to get the result. ■

<u>Exercise:</u> What if $l \mid m$?

Chris
6-29-11
pg5

Twists:

$\chi : G \to \mathbb{C}^\times$, in fact, $\chi : G \to \mathbb{Q}(\zeta_d)^\times$, $\chi : \mathbb{Z} \to \mathbb{Q}(\zeta_d)$

f_χ conductor, $f_\chi \mid m$ $\qquad d = [K : \mathbb{Q}]$

Gauss sum $\quad \mathcal{G}(\chi) = \sum_{a \bmod m} \chi(a) e^{2\pi i a/m} \in \overline{\mathbb{Q}}$

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

Theorem 1: If χ is primitive ($f_\chi = m$), then

$$\mathcal{G}(\chi) L(E, \bar{\chi}, 1) = \sum_{a \bmod m} \chi(a) \lambda\left(\tfrac{a}{m}\right)$$

Proof: $\displaystyle \sum_{a \bmod m} \chi(a) \lambda\left(\tfrac{a}{m}\right) = \sum_{a \bmod m} \chi(a) \sum_{n \geq 1} \frac{a_n}{n} e^{2\pi i n a/m}$

$$= \sum_{n \geq 1} \frac{a_n}{n} \sum_{a \bmod m} \chi(a) e^{2\pi i n a/m}$$

If $(n,m) = 1$, then $\chi(na) = \chi(n)\chi(a)$ and na will run through all classes mod m so in this case

$$\sum_{n \geq 1} \frac{a_n}{n} \sum_{a (\bmod m)} \chi(na) \bar{\chi}(n) e^{2\pi i a n/m}$$

$$\sum \chi(\cancel{na}) e^{2\pi i n a/m} = \mathcal{G}(\chi).$$

Exercise: If χ is primitive and $\gcd(n,m) > 1$, then

$$\sum_{a \bmod m} \chi(a) e^{2\pi i n a/m} = 0.$$

$= \bar{\chi}(n) \mathcal{G}(\chi)$

Chris
6-29-4
pg 6

Using this exercise one easily completes the proof, ignoring any convergence issues. ■

Now suppose K is totally real (H2).

$\chi(-a) = \chi(a)$

$\lambda(-a) = \overline{\lambda(a)}$

$$\sum_{a \bmod m} \chi(a)\lambda(\tfrac{a}{m}) = \frac{1}{2}\left(\sum_{a \bmod m} \chi(a)\lambda(\tfrac{a}{m}) + \sum_{a \bmod m} \chi(-a)\lambda(\tfrac{-a}{m})\right)$$

$$= \sum_{a \bmod m} \chi(a)\,\frac{\lambda(\frac{a}{m}) + \overline{\lambda(\frac{a}{m})}}{2}$$

$$= \sum_{a \bmod m} \chi(a)\,\mathrm{Re}(\lambda(\tfrac{a}{m}))$$

Cor 13: $\chi(\Theta) = \sum_{a \bmod m^\times} [\frac{a}{m}]\chi(a) = \dfrac{L(E,\bar{\chi},1)\,\mathcal{G}(\chi)}{\Omega_+}$.

($\chi : \mathbb{Q}[G] \to \mathbb{Q}(\zeta_d)$ by extending linearly)

We immediately see that $\dfrac{L(E,\bar{\chi},1)\,\mathcal{G}(\chi)}{\Omega_+} \in \mathbb{Q}(\zeta_d)$.

There are formulas for non-primitive χ

$$\chi(\Theta) = \underbrace{(\sim)}_{\text{some Euler factors.}}\ \frac{L(E,\bar{\chi},1)\,\mathcal{G}(\chi)}{\Omega_+}$$

Lemma 14 (Artin formalism): Assume (H1).

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

Theorem 15: Assume (H1) – (H3). Then

$$\frac{L(E/K,1)\sqrt{\Delta_K}}{\Omega_+^d} \in \mathbb{Q}$$

$$= \frac{\prod_v c_v(w)\ \#Ш(E/K)}{(\#E(K)_{tors})^2} \quad \text{if it is nonzero.}$$

from Vlad's lecture

Sketch of Proof: Take the product over χ of Cor 13:

$$\frac{\prod_\chi L(E,\bar{\chi},1)\underbrace{\left(\prod_\chi g(\chi)\right)}_{=\sqrt{\Delta_K}}}{\Omega_+^d} \in \mathbb{Q}(\zeta_d)$$

(and some fudge factors from non-primitive χ.)
Now use that the Galois group will actually fix this element to see it is in $\mathbb{Q}$.

Chris
[illegible]
6-30-11
pg #1

Recall: $[r] \in \mathbb{Q}$, $\Theta \in \mathbb{Q}[G]$.

Correction: $N_{L/K}(\Theta_L) = -(\sigma_\ell - a_\ell + \delta_N(\ell)\sigma_\ell^{-1})\,\Theta_{E/K}$.

In the proof $\sigma_a|_K \neq \sigma_c$

$a = bm + c\ell$ $\quad \sigma_a|_K = \sigma_{c\ell} = \sigma_c \sigma_\ell$, so the σ_ℓ^{-1} in the Norm given last lecture is cancelled out.

$K/\mathbb{Q}$ abelian degree d conductor m

- no additive place ramifies
- totally real
- $\gcd(d,m) = 1$.

$$\chi(\Theta) = \frac{L(E,\bar{\chi},1)\,\mathcal{G}(\chi)}{\Omega_+} \in \mathbb{Q}(\zeta_d). \quad \text{if } \chi \text{ is primitive}$$

Theorem (Kato): If $L(E,\chi,1) \neq 0$ then $(E(K) \otimes \mathbb{C})^\chi = 0$.

If $L(E/K,1) \neq 0$, then $E(K)$ is finite and Ш(E/K) is finite.

From now on assume $L(E/K,1) \neq 0$.

If d is an odd prime, G is cyclic:

$$\frac{L(E/K,1)\sqrt{\Delta_K}}{\Omega_+^d} = [0] \cdot \prod_{\chi \neq \mathbb{1}} \chi(\Theta)$$

(Fix one primitive χ.)

$$= [0]\, N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\chi(\Theta)).$$

Chris
6-30-11
PS 2

Example: 435b1 $/\mathbb{Q}$; $\prod_v c_v = 1$, $E(\mathbb{Q}) = 0 = Ш(E/\mathbb{Q})$.

All ρ_p are surjective. $\Rightarrow E(K)_{tors} = 0 \quad \forall\ K/\mathbb{Q}$ abelian.

$m = 7 \quad d = 3, \quad \prod \tau_v(E, \omega_v) = 1$

$\Theta = 6 - 5g - 5g^2$

$\chi(\Theta) = 6 - 5\zeta_3 - 5(1 - \zeta_3) = 11.$

Thus,

$$BSD_K \Leftrightarrow \# Ш(E/K) = 11^2.$$

Exercise: Do the same for $m = 11$, $d = 5$.

Functional Equation:

Assume $(N, m) = 1$, i.e., no bad place ramifies.

$$\chi(\Theta) = W(E/\mathbb{Q})\, \bar{\chi}(N)\, \overline{\chi(\Theta)}$$

(Doesn't know elementary proof, use Atkin-Lehner ...)

$\Rightarrow$ if $d = 3$ and $W(E/\mathbb{Q}) = +1$, then $\chi(\Theta) \in \chi(N)\mathbb{Q}$.

In the example $N \equiv 1 \pmod 7 \Rightarrow \chi(\Theta) \in \mathbb{Q}$.

Equivariant Conjecture:

What is $\chi(\Theta)$?

b/c L-value non-zero by assump.

View $Ш[E/K]$ as a $\mathbb{Z}[G]$-module. Set $T = E(K)_{tors}$ $(= E(K))$.

$T^\vee$ = dual of T

$C = \bigoplus_{\substack{v \text{ place} \\ \text{in } \mathbb{Q}}} \Phi_v$ where

$$\Phi_\infty = \begin{cases} \mathbb{Z}/2\mathbb{Z}[G] & \text{if } c_\infty = 2 \\ 0 & \text{if } c_\infty = 1 \quad (\text{tot. real}) \end{cases}$$

Chris
6-30-11
PS 3

If $w | v$ is a finite place of K

$$\Phi_w = E(K_w) / E^\circ(K_w)$$

(H1) $\Rightarrow$ the global min. model does not change when $K/\mathbb{Q}$.

$$\Phi_v = \bigoplus_{w|v} \Phi_w \quad \text{is a } \mathbb{Z}[G]\text{-module.}$$

Let p be a prime. Assume $p \nmid d$. Fix a primitive char. $\chi : \mathbb{Z}[G] \to \mathbb{Z}[\zeta_d]$. Pick a prime ideal $\mathfrak{p}$ above p in $\mathbb{Q}(\zeta_d)$

Define

$$\mathrm{len}_\mathfrak{p}(M) = \text{lengths of } M_\mathfrak{p} \quad \text{for } M \text{ a finite } \mathbb{Z}[G]\text{-module.}$$

(We can view $\mathfrak{p}$ as a maximal ideal in $\mathbb{Z}[G]$ via χ.)

Let ~~$\mathcal{O}_\mathfrak{p}$ ring of integers~~ $F_\mathfrak{p}$ = Frac (completion of localization $\mathbb{Z}[\zeta_d]_\mathfrak{p}$) and $\mathcal{O}_\mathfrak{p}$ its ring of integers.

Any $\mathcal{O}_\mathfrak{p}$-module is $\bigoplus \mathcal{O}_\mathfrak{p}/\mathfrak{p}^{k_i}$, and then $\mathrm{len}_\mathfrak{p}$ is $\sum k_i$.

$$\#(M_\mathfrak{p}) = \left(\# \mathcal{O}_\mathfrak{p}/\mathfrak{p}\right)^{\mathrm{len}_\mathfrak{p}(M)}.$$

Conjecture: If $L(E, \bar{\chi}, 1) \neq 0$, then

$$\mathrm{ord}_\mathfrak{p}(\chi(\Theta)) = \mathrm{len}_\mathfrak{p}(Ш(E/K)) + \mathrm{len}_\mathfrak{p}(C) - \mathrm{len}_\mathfrak{p}(T) - \mathrm{len}_\mathfrak{p}(T^\vee).$$

Exercise: Check that if d is prime & $BSD_\mathbb{Q}$ implies BSD_K at least for the non-d part.

This conjecture is believed to ~~Hekess~~ be equivalent to the Equivariant Tamagawa Number Conjecture in this case.

$(\mathcal{M} = h^1(E_K)(1), \quad \mathcal{A} = \mathbb{Z}_p[G])$

Reformulation:

Conjecture (Mazur-Tate): $\Theta \in \mathrm{Fitt}^0(\mathrm{Sel}_{\mathbb{Z}}(E/K))$ $\quad p \nmid tc$.

$(\Rightarrow \ \leq)$

Reformulation: $\chi(\Theta) \in \mathbb{F}_p^\times = K_1(\mathbb{F}_p)$

$$\partial : K_1(\mathbb{F}_p) \longrightarrow K_0\left(\substack{\text{fin. gen.} \\ \text{torsion } \mathcal{O}_p\text{-module}}\right) = K_0(\mathcal{O}_p, \mathbb{F}_p).$$

send

$$\chi(\Theta) \longmapsto [Ш] + [c] - [T] - [T^\vee]$$

Recall: χ primitive character mod m of order d

$\mathfrak{p}$ maximal ideal of $\mathbb{Z}[\zeta_d]$ above $p \nmid d$.

Conj: $$\mathrm{ord}_{\mathfrak{p}}(\chi(\circledast)) = \mathrm{len}_{\mathfrak{p}}(Ш(E/K)) + \mathrm{len}_{\mathfrak{p}}(C) - \mathrm{len}_{\mathfrak{p}}(T) - \mathrm{len}_{\mathfrak{p}}(T^{\vee})$$

where we assumed $L(E/K, 1) \neq 0$.

We will concentrate on $Ш(E/K)[p]$. This is a $\mathbb{F}_p[G]$-module, $\mathbb{F}_p[G]$ decomposes as irred. $\mathbb{F}_p[G]$-modules.

$d=3$: $p \equiv 1 \pmod 3$	$p \equiv 2 \pmod 3$
$\Leftrightarrow$ $p = \mathfrak{p}_1 \mathfrak{p}_2$ in $\mathbb{Q}(\zeta_3)$	(p) is prime in $\mathbb{Q}(\zeta_3)$.
$\Leftrightarrow$ $\zeta_3 \in \mathbb{F}_p$	$\zeta_3 \notin \mathbb{F}_p$
$\Leftrightarrow$ $\mathbb{F}_p[G] = \mathbb{F}_p \oplus \mathbb{F}_p\chi \oplus \mathbb{F}_p\bar{\chi}$	$\Leftrightarrow$ $\mathbb{F}_p[G] = \mathbb{F}_p \oplus \underset{\mathbb{F}_{p^2}}{\underset{\shortparallel}{\text{2-dim thing}}} = V$.

If $p \equiv 2 \pmod 3$, then $Ш(E/K)[p] = \underset{(Ш(E/K)[p])^G}{\underset{\shortparallel}{Ш(E/\mathbb{Q})[p]}} \oplus V^n$

In this case $BSD_{\mathbb{Q}}$ and BSD_K implies the conjecture.

If $p \equiv 1 \pmod 3$; the Cassels-Tate pairing is G-equivariant, non-degenerate, so if if

$$Ш(E/K)[p] = Ш(E/\mathbb{Q})[p] \oplus (\mathbb{F}_p\chi)^{n_\chi} \oplus (\mathbb{F}_p\bar{\chi})^{n_{\bar{\chi}}}$$

we get $n_\chi = n_{\bar{\chi}}$ and so $BSD_{\mathbb{Q}}$ & BSD_K imply the conj.

$d=5$: $p \equiv 1 \pmod 5$ $\quad (p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$

$p \equiv -1 \pmod 5$ $\quad (p) = \mathfrak{p}_1\mathfrak{p}_2$

$p \equiv 2, 3 \pmod 5$ $\quad (p)$ is prime.

Chris

7-1-11

PS 2

$\mathbb{F}_p[G] = \mathbb{F}_p \oplus \left(\begin{smallmatrix} d-1 \text{ dim} \\ \text{irred} \end{smallmatrix}\right)$ for $p \equiv 2,3 \pmod 5$

The situation here will be exactly as in $d=3$ case.

$p \equiv 1 \pmod 5$, $\zeta_5 \in \mathbb{F}_p$ (see upcoming example)

Both $p \equiv 1 \pmod 5$ and $p \equiv -1 \pmod 5$ give interesting statement.

$p = d$: Eigenvalues of $g \in G$ are always 1.

$Ш(E/K)[p]^G \neq Ш(E/\mathbb{Q})[p]$ i.e., there might be capitulation.

E.T.N.C says something different in this case.

<u>67a1:</u> $y^2 + y = x^3 + x^2 - 12x - 21$

$E(\mathbb{R})$ is connected, $c_{67} = 1$, $\rho_p : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_p)$ are all surj., $E(\mathbb{Q}) = 0.$, $Ш(E/\mathbb{Q}) = 0.$

$m = 71 \quad d = 7$

$K: x^7 + x^6 - 30x^5 + 3x^4 + 254x^3 - 246x^2 - 245x + 137$

$\Delta_E = 71^6$

$$\frac{L(E/K,1)\sqrt{\Delta_K}}{\Omega_+^7} = 6355441.0000 \underset{\text{mod sym}}{=} 2521^2.$$

Since the Galois reps are all surj, $E(K) = 0$.

(67) is still prime so $C_{(67)} = 1$.

$$BSD_K \Leftrightarrow \# Ш(E/K) = 2521^2.$$

$\Theta = -12 - 12g - 12g^2 + 2g^3 + 15g^4 + 15g^5 + 2g^6$ w/ $g = \sigma_7$, $\zeta = \zeta_7$

$\chi(\Theta) = (-\zeta^3 - 2\cdot\zeta^3 - 2\cdot\zeta - 1)(\zeta^5 + 2\cdot\zeta^4 + 4\cdot\zeta^3 + 2\cdot\zeta + 1)$

unit $\cdot (\zeta^5 + 2\cdot\zeta^4 + \zeta^3 + 2\cdot\zeta - 2)$ generators of some p_i when

$(2521) = p_1 p_2 \cdots p_6$

Conj. $\Rightarrow$ Ш(E/K) [non-7-part]

$$= \frac{\mathbb{Z}[\zeta_7]}{(\zeta^5+2\zeta^4+4\zeta^3+2\zeta+1)} \oplus \frac{\mathbb{Z}[\zeta_7]}{(\zeta^5+2\zeta^4+\zeta^3+2\zeta-2)}$$

as a $\mathbb{Z}[G]$-module.

$\cong \mathbb{F}_p e_1 \oplus \mathbb{F}_p e_2 \qquad p = 2521$

$g(e_1) = 1312\, e_1$

$g(e_2) = 1028\, e_2$.

What does Θ say about $E(\mathbb{Q})$, Ш$(E/\mathbb{Q})$?

Let $I = \ker(\mathbb{Z}[G] \xrightarrow{1} \mathbb{Z})$ be the augmentation ideal.

Conj.: $\Theta \in I^r$ where $r = \mathrm{rk}\, E(\mathbb{Q})$.

One can formulate a BSD-like conjecture

$$\operatorname*{ord}_{s=1} L(E/\mathbb{Q}, s) \overset{?}{\leadsto} \operatorname{ord}_I(\Theta) = \cdots$$

$\operatorname{Ord}_I(\Theta)$ is linked to the $\operatorname*{ord}_{s=1} \mathcal{L}_p(E, s)$ (p-adic L-function)

What is the image of Θ in $I^r/I^{r+1} \simeq \mathbb{Z}$?

But the regulator is a p-adic regulator ... $\leadsto$ p-adic BSD by Mazur-Tate-Teitelbaum.

Tomorrow will discuss Kurihara's recent results on Ш$(E/\mathbb{Q})$ and frequency of vanishing of $L(E/K, 1)$ as K varies.