Lecture 1

Friday, August 5, 2022 7:29 AM

$E: y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Q}$, $4A^3 + 27B^2 \neq 0$,
elliptic curve of conductor N.

Def $r_{alg}(E) := \operatorname{rank} E(\mathbb{Q}) \in \mathbb{Z}_{\geq 0}$.

Greatest Mystery: Given $E/\mathbb{Q}$, determine $r_{alg}(E)$.
(e.g. we don't each know what values $r_{alg}(E)$ can take)

Ex. $E^{(n)}: y^2 = x^3 - n^2 x$.
(Rogers)

$r_{alg}(E^{(n)})$	n
0	1
1	5
2	34
3	1254
4	29274
5	4827223
6	661171986
7	79750754375
8	?

Understanding $r_{alg}(E)$: BSD conjecture

§1. L-function of elliptic curves

Analogous to the Riemann zeta function

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}.$$

$$\sum_{n\geq 1} \frac{\quad}{n^s} = \prod_p \quad .$$

define the L-function of E

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

Here $$L_p(E,s) = \begin{cases} (1 - a_p \cdot p^{-s} + p^{1-2s})^{-1} & p \text{ good} \\ (1 - a_p p^{-s})^{-1} & p \text{ bad} \end{cases}$$

Here $a_p = \begin{cases} p+1 - \#E(\mathbb{F}_p) & p \text{ good.} \\ +1 & p \text{ split multiplicative} \\ -1 & p \text{ nonsplit multiplicative.} \\ 0 & p \text{ additive} \end{cases}$

more computable !

(a uniform way : define $\chi(p) = \begin{cases} 1 & p \text{ good} \\ 0 & p \text{ bad} \end{cases}$

then $$L_p(E,s) = (1 - a_p p^{-s} + \chi(p) \cdot p \cdot p^{-2s})^{-1}$$

Easy consequence :

(1) $a_1 = 1$

(2) $a_{mn} = a_m a_n$ if $(m,n) = 1$

(3) $$a_{p^r} = a_p a_{p^{r-1}} - \chi(p) \cdot p \cdot a_{p^{r-2}} .$$

(this mate the relation of Hecke operators in the theory of modular forms.) .

Rem: $L(E,s)$ is an example of a motivic L-function, namely associated to Galois representations coming from geometry. Consider the 2-dim'l Galois rep on the ℓ-adic Tate module $V_\ell E = T_\ell E \otimes \mathbb{Q}_\ell$.

$$\rho_E : G_{\mathbb{Q}} \to GL(V_\ell E)$$

Then
$$L_p(E,s) = \det\left(1 - p^{-s}\cdot \rho_E(\mathrm{Fr}_p) \,\middle|\, (V_\ell E)^{I_p}\right)^{-1}$$

where $I_p \subseteq G_{\mathbb{Q}_p} \subseteq G_{\mathbb{Q}}$ is the inertia subgp at p.

Notice $\dim (V_\ell E)^{I_p} = \begin{cases} 2 & p \nmid N \\ 1 & p \| N \\ 0 & p^2 \mid N. \end{cases}$

and
$$a_p = \mathrm{tr}\left(\rho_E(\mathrm{Fr}_p) \mid (V_\ell E)^{I_p}\right).$$
("trace of Frobenius").
$$= \begin{cases} p+1-|E(\mathbb{F}_p)| & p \nmid N. \\ \pm 1 & p \| N \\ 0 & p^2 \mid N \end{cases}$$

Exercise $L(E,s)$ converges absolutely when $\mathrm{Re}\, s > \frac{3}{2}$

Philosophy about L-functions: should look like $\zeta(s)$:

① $L(E,s)$ should have Euler product

② $L(E,s)$ should have analytic continuation

② $L(E,s)$ should have analytic continuation

③ $L(E,s)$ should satisfy a functional equation

For motivic L-functions ① is by construction.

② and ③ are hard and becomes one of the motivation for the Langlands program.

$$\text{motives} \quad \longleftrightarrow \quad \text{automorphic forms}$$

$$L(E,s) \quad = \quad L(f_E, s).$$

For automorphic L-functions, ② and ③ are easier.

§2. L-functions of modular forms.

Let $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \pmod N \right\} \leq SL_2(\mathbb{Z})$.

and let $S_k(N)$ = the space of cusp forms of level $\Gamma_0(N)$ and weight k.

Recall: $f \in S_k(N)$ means:

(1) $f : \mathcal{H} \to \mathbb{C}$ holomorphic

(2) $f(\gamma\tau) = (c\tau+d)^k f(\tau)$ $\quad \gamma \in \Gamma_0(N)$, $\tau \in \mathcal{H}$.

(3) f is holomorphic and vanishes at all cusps.

Def. Let $f = \sum_{n \geq 1} a_n q^n$ be the q-expansion at the cusp ∞. We define its L-functi

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

The starting point is that $L(f,s)$ has an explicit integral representation as a Mellin transform.

Def. The Mellin transform of f is defined to be

$$g(s) = \int_0^\infty f(it)\, t^s \frac{dt}{t}.$$

Prop. $g(s) = (2\pi)^{-s}\,\Gamma(s)\,L(f,s)$. $\left(\mathrm{Re}\, s > \frac{k}{2}+1\right)$

Def. The complete L-function is

$$\Lambda(f,s) := N^{\frac{s}{2}} \underbrace{(2\pi)^{-s}\,\Gamma(s)\,L(f,s)}_{g(s)}.$$

Def. Define an operator $W_N : S_k(N) \to S_k(N)$ by

$$(W_N f)(\tau) = \left(\frac{i}{\sqrt{N}\tau}\right)^k f\left(-\frac{1}{N\tau}\right).$$

Then $W_N^2 = 1$. Known as Atkin-Lehner involution.

Thm (Hecke) Let $f \in S_k(N)$. Assume $W_N f = \varepsilon f$. $\varepsilon \in \{\pm 1\}$.

(1) $\Lambda(f,s)$ has analytic continuation to all of $\mathbb{C}$.

(2). $\Lambda(f,s)$ satisfies a functional equation.

↙ sign of functional equation

$\Lambda(f,s) = \varepsilon \cdot \Lambda(f, k-s)$. ← sign of functional equation

§ 3. Modularity of elliptic curves

Modularity Thm (Wiles, Taylor, BCDT).

There exists a weight 2 cusp eigenform $f_E \in S_2(N)$ with q-expansion $f_E(z) = \sum_{n \geq 1} a_n q^n$.

In particular. $L(E,s) = L(f_E, s)$

has analytic continuation to $\mathbb{C}$.

and satisfies a function equation relating $s \leftrightarrow 2-s$.

Ex. $E: y^2 = x^3 - x$ $\quad N = 32$.

p	2	3	5	7	11	13	17	19	23	29	31
a_p	0	0	-2	0	0	6	2	0	0	-10	0.

(Note $a_p \neq 0 \Leftrightarrow p \equiv 1 \pmod 4$).

On the other hand there is a modular form $\in S_2(32)$!

$$f = q \prod_{n \geq 1} (1-q^{4n})^2 (1-q^{8n})^2$$

$$= q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29} \cdots$$

Analytic continuation allows us to define

Def $r_{an}(E) := \operatorname{ord}_{s=1} L(E,s)$ (order of 0 at $s=1$)

Cor (Geometric modularity)

Cor (Geometric modularity)

There exists a nontrivial map of curves over $\mathbb{Q}$:

$$\varphi: X_0(N) \to E$$

$$\| \quad \text{(up to } \mathbb{C}^*\text{)}$$

$$\Gamma_0(N) \backslash \mathcal{H}^*$$

Moreover, $\varphi^* \omega_E = c \cdot f_E(q) \frac{dq}{q}$ for some $c \in \mathbb{Q}^\times$

[Idea: Eichler-Shimura: $\mathrm{Jac}(X_0(N)) \sim \prod_{f \in S_2(N)} A_f$

with $L(A_f, s) = L(f, s)$

Faltings isogeny thm: $L(A_{f_E}, s) = L(E, s)$

$\Rightarrow A_{f_E} \sim E$.

Compose: $X_0(N) \hookrightarrow \mathrm{Jac}(X_0(N)) \to \prod A_f \to A_{f_E} \to E$]

§4. BSD Conjecture

Q How is $r_{an}(E)$ related to $r_{alg}(E)$?

Let us naively evaluate $L(E, s) = \prod_p L_p(E, s)$

at $s = 1$ (although the product doesn't converge)

$$L_p(E, 1) = \left(1 - a_p \cdot p^{-1} + \chi(p) \cdot p^{-1}\right)^{-1}$$

$$= \left(\frac{p - a_p + \chi(p)}{p}\right)^{-1}$$

$$= \frac{p}{p - a_p + \chi(p)} = \frac{p}{|\tilde{E}(\mathbb{F}_p)|}$$

$$= \begin{cases} \dfrac{p}{1+p-a_p} & p \text{ good.} \\ \dfrac{p}{p+1} & p \text{ multiplicative} \\ \dfrac{p}{p} & p \text{ additive.} \end{cases}$$

where $\tilde{E}/\mathbb{F}_p$ = smooth part of $E/\mathbb{F}_p$.

So $L(E,1)$ "=" $\prod_p \dfrac{p}{|\tilde{E}(\mathbb{F}_p)|}$

↑ "more zeros" ↑ "$=$" "$|\tilde{E}(\mathbb{F}_p)|$ larger" for all p.

$r_{an}(E)$ "larger" $\longleftrightarrow$ $r_{alg}(E)$ "larger"

In fact, Birch and Swinnerton-Dyer did numerical computation for the quantity

$$\prod_{p<X} \frac{|\tilde{E}(\mathbb{F}_p)|}{p}.$$

for the family of curves $\{y^2 = x^3 - n^2 x\}$ in 1958 using EDSAC 2, and they were successful in predicting $r_{alg}(E)$ by merely looking at the growth when $X \to \infty$.

$$\prod_{p<X} \frac{|\tilde{E}(\mathbb{F}_p)|}{p} \sim C \cdot (\log X)^{r_{alg}(E)}.$$

This leads to their celebrated conjecture

BSD Conj (rank part)

$$r_{alg}(E) = r_{an}(E).$$

$r_{alg}(E) = r_{an}(E)$.

Rem BSD $\Rightarrow$ an algorithm (though not practical) to compute $r_{alg}(E)$: search for points in $E(\mathbb{Q})$ finding r-points $\to$ check $L^{(r)}(E,1) \neq 0$

Rem (parity conj)

$$\operatorname{ord}_{s=1} \Lambda(E,s) = \begin{cases} \text{even} & \varepsilon = +1 \\ \text{odd} & \varepsilon = -1. \end{cases}$$

Since $L(E,s) = \dfrac{(2\pi)^s}{N^{\frac{s}{2}}\Gamma(s)} \Lambda(E,s)$ has the same order of vanishing as $\Lambda(E,s)$, we know

$$r_{an}(E) = \begin{cases} \text{even} & \varepsilon = +1 \\ \text{odd} & \varepsilon = -1 \end{cases}$$

So BSD predicts :

$$r_{alg}(E) = \begin{cases} \text{even} & \varepsilon = +1 \\ \text{odd} & \varepsilon = -1 \end{cases}$$

Ex 1) N = square-free $\Rightarrow$ $\varepsilon = (-1)^{s+1}$

where $s = \#\{p \mid N : E \text{ split multiplicative at } p\}$

$\overset{BSD}{\Rightarrow}$ $r_{alg} \overset{?}{\equiv} s+1 \pmod 2$

2) $\varepsilon(E^{(n)} : y^2 = x^3 - n^2x) = \begin{cases} -1 & n \equiv 5, 6, 7 \pmod 8 \\ +1 & n \equiv 1, 2, 3 \pmod 8 \end{cases}$

$\overset{BSD}{\Rightarrow}$ $r_{alg}(E^{(n)}) > 0$ if $n \equiv 5, 6, 7 \pmod 8$

Thm (Gross-Zagier, Kolyvagin)

(1) $r_{an}(E) = 0 \Rightarrow r_{alg}(E) = 0$

(2) $r_{an}(E) = 1 \Rightarrow r_{alg}(E) = 1.$

(little is known if $r_{an}(E) > 1$).

Pf of Thm combines two inequalities:

① Gross-Zagier formula:

$$r_{an}(E) = 1 \Rightarrow r_{alg}(E) \geq 1$$

($L'(E,1) \neq 0 \Rightarrow$ Heegner pt is non-torsion)

② Kolyvagin's Euler system of Heegner pts:

$$r_{an}(E) \leq 1 \Rightarrow r_{alg}(E) \leq r_{an}(E)$$

(bound Selmer rank of E from above)

§5. Computing $L^{(n)}(E,s)$

Exercise For $f \in S_k(N)$, $w_N f = \varepsilon f$, $\varepsilon \in \{\pm 1\}$.

$$\Lambda(f,s) = \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)\left(t^s + \varepsilon\, t^{k-s}\right)\frac{dt}{t}.$$

Apply this to $f \in S_2(N) \leftrightarrow E/\mathbb{Q}$ elliptic curve.

① $\varepsilon = +1$. we obtain a formula for the central value

$$\Lambda(f,1) = 2\int_1^\infty f\left(\frac{it}{\sqrt{N}}\right) dt.$$

$$= 2\int_1^\infty \sum_{n\geq 1} a_n e^{\frac{-2\pi nt}{\sqrt{N}}}\, dt$$

$$= 2 \sum_{n\geq 1} \cdot \frac{\sqrt{N}}{2\pi} \cdot \frac{a_n}{n} e^{-\frac{2\pi n}{\sqrt{N}}}$$

(use $\int_1^\infty e^{-ct}\, dt = \frac{1}{c} e^{-c}$.).

By $L(f,1) = \frac{2\pi}{\sqrt{N}} \Lambda(f,1)$, we obtain:

$$\boxed{L(f,1) = 2 \cdot \sum_{n\geq 1} \frac{a_n}{n} e^{-\frac{2\pi n}{\sqrt{N}}}}$$

② $\varepsilon = -1$.

$$\Lambda'(f,1) = 2\int_1^\infty f\left(\frac{it}{\sqrt{N}}\right)(\log t)\, dt$$

$$= 2\int_1^\infty \sum_{n\geq 1} a_n e^{-\frac{2\pi n t}{\sqrt{N}}} \log t\, dt.$$

$$= 2 \sum_{n\geq 1} \frac{\sqrt{N}}{2\pi} \cdot \frac{a_n}{n} \cdot \int_1^\infty e^{-\frac{2\pi n t}{\sqrt{N}}} \frac{dt}{t}.$$

(Use integrate by part. exponential integral

$$\int_1^\infty e^{-ct} \log t\, dt = \frac{1}{c} \int_1^\infty e^{-ct} \frac{dt}{t}.$$)

Use $L'(f,1) = \frac{2\pi}{\sqrt{N}} \Lambda'(f,1)$, we obtain

$$\boxed{L'(f,1) = 2 \sum_{n\geq 1} \frac{a_n}{n} \int_1^\infty e^{-\frac{2\pi n t}{\sqrt{N}}} \frac{dt}{t}.}$$

Rem. More generally, for $r \geq 1$ define

$$E_r(x) := \frac{1}{(r-1)!} \int_1^\infty e^{-xt} (\log t)^{r-1} \frac{dt}{t}.$$

Then $L^{(r)}(f,1) = \frac{2\pi}{\sqrt{N}} \Lambda^{(r)}(f,1)$

Then $$L^{(r)}(f,1) = \frac{2\pi}{\sqrt{N}}\,\Lambda^{(r)}(f,1)$$

$$\boxed{L^{(r)}(f,1) = 2r!\sum_{n\geq 1}\frac{a_n}{n}\,E_r\left(\frac{2\pi n}{\sqrt{N}}\right).}$$

Rem. One can view $L^{(r)}(f,1)$ as a weighted version of "$\sum_{n\geq 1}\frac{a_n}{n}$".

§6. The value $L(E,1)$: periods

Ex. $E: y^2 = x^3 - x$. $N = 32$.

$$f = q\prod_{n\geq 1}(1-q^{4n})^2(1-q^{8n})^2 \qquad (a_p \neq 0 \Leftrightarrow p \equiv 1 \pmod 4)$$

$$= q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29}\ldots$$

$$L(E,1) = \sum_{n\geq 1}\frac{a_n}{n}\,e^{-\frac{2\pi n}{\sqrt{32}}}$$

$$= 0.655514388\ldots$$

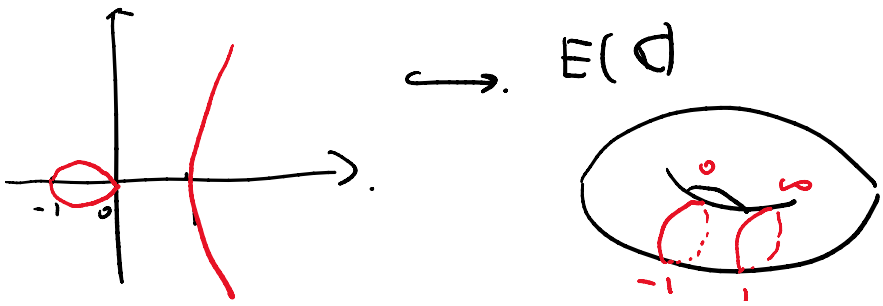
Def The Néron period is defined to be

$$\Omega(E) := \int_{E(\mathbb{R})}\omega_E \in \mathbb{R}.$$

Ex. $E: y^2 = x^3 - x$.

$$\omega_E = \frac{dx}{2y} = \frac{dx}{2\sqrt{x^3-x}}.$$

$E(\mathbb{R})$ ⟶ $E(\mathbb{C})$





$$\Omega(E) = \int_{E(\mathbb{R})} \omega_E = \int_{-1}^{0} \omega_E + \int_{1}^{\infty} \omega_E$$

$$= 2 \int_{1}^{\infty} \omega_E$$

$$= 4 \int_1^\infty \frac{dx}{2\sqrt{x^3 - x}} = 2 \int_1^\infty \frac{dx}{\sqrt{x^3 - x}}$$

$$= 5.2991151058\ldots.$$

Notice $\dfrac{L(E,1)}{\Omega(E)} \approx \dfrac{1}{8} \in \mathbb{Q}$!

§7. The leading term $L^{(r)}(E,1)$: heights

Ex. $E: y^2 = x^3 - 25x$. $N = 25 \cdot 32 = 800$.

$r = 1$. $E(\mathbb{Q}) = \mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}/2$

$(-4,6)$ $(0,0)$ $(5,0)$.

$$f = q - 3q^9 - 6q^{13} - 2q^{17} + \cdots \quad \left(a_p = \chi_5(p) \cdot a_p(X_0(32))\right)$$

$$L'(E,1) = 2 \sum_{n \geq 1} \frac{a_n}{n} E_1\left(\frac{2\pi n}{\sqrt{800}}\right)$$

$$= 2.2273703795\ldots$$

$$\Omega(E) = 2\int_5^\infty \frac{1}{\sqrt{x^3 - 25x}} = 2.3452395729\ldots$$

Then $\dfrac{L'(E,1)}{\Omega(E)} = 0.9491410826\ldots \notin \mathbb{Q}$.

Then $\frac{L'(E,1)}{\Omega(E)} = 0.9417\ldots \notin \mathbb{Q}$.

In fact we can no longer interpret $L'(E,1)$ as a period due to extra "log t" factor.

Ex. $P = (-1, 6)$. $\quad \hat{h}(P) = 1.5567\ldots$

$2P = \left(\frac{1681}{144}, \ldots\right)$ $\quad \frac{\hat{h}(2P)}{4} = 1.5775\ldots$

$4P = \left(\frac{111834\ldots}{22341\ldots}, \ldots\right)$ $\quad \frac{\hat{h}(4P)}{16} = 1.5996\ldots$

$\hat{h}(P) = 1.5996\ldots$

Then $\frac{L'(E,1)}{\Omega(E)\hat{h}(P)} \approx \frac{1}{2} \in \mathbb{Q}$!

Def. The regulator of E is defined to be

$$R(E) := \det\left(\langle P_i, P_j\rangle_{i,j=1\ldots r}\right)$$

where $P_1 \ldots P_r$ is a basis of $\frac{E(\mathbb{Q})}{E(\mathbb{Q})_{tor}}$.

Notice $R(E) \neq 0$.

Ex $\quad r=0 \quad R(E) = 1$

$r=1 \quad R(E) = \hat{h}(P)$. P generates $\frac{E(\mathbb{Q})}{E(\mathbb{Q})_{tor}}$.

Conj. $\frac{L^{(r)}(E,1)}{\Omega(E)\,R(E)} \in \mathbb{Q}^\times$.

Rem

$r = 0$ Follow from modularity (Birch)

$r = 1$ Conj follows from $r=0$ + Gross-Zagier

$r \geq 2$ Not a single example is proved.

(but numerical data is highly supportive)

§8. Full BSD Conj.

Analogy with class number formula:

for $K/\mathbb{Q}$ a number field

$$\operatorname{Res}_{s=1} \zeta_K(s) = \underbrace{\frac{2^{r_1}(2\pi)^{r_2}}{|d_K|^{\frac{1}{2}}}}_{\text{period}} \cdot \underbrace{\frac{R(K)}{|\mathcal{O}_{K,\text{tor}}^\times|}}_{\text{regulator}} \cdot \underbrace{h(K)}_{\substack{\text{class} \\ \text{number.}}}$$

BSD Conjecture

(1) (rank part) $r_{an}(E) = r_{alg}(E)$

(2) (BSD formula) let $r = r_{an}(E)$. then

$$\frac{L^{(r)}(E,1)}{r!} = \underbrace{\Omega(E) \cdot \prod_p c_p}_{\text{period}} \cdot \underbrace{\frac{R(E)}{|E(\mathbb{Q})_{\text{tor}}|^2}}_{\text{regulator}} \cdot \underbrace{|Ш(E)|}_{\text{= class number}}.$$

Rem Full BSD has been proved for many (but not all) $E/\mathbb{Q}$ with $r_{an}(E) \le 1$. due to work of many people using e.g. deep methods from Iwasawa theory.

[Def. The local Tamagawa number is defined to be

$$c_p(E) := [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)].$$

Notice $c_p(E) = 1$ for $p \nmid N$.

Rem. $c_p(E) = \Phi(\mathbb{F}_p)$, where $\Phi = \mathcal{E}/\mathcal{E}^0$

is the gp scheme of components of Néron model at p.

Tate's algorithm gives a way to compute $c_p(E)$

[the gp scheme of components of Néron model at p.
Tate's algorithm gives a way to compute $c_p(E)$
given a Weierstrass equation of E.]

Ex.

E	N	r	$\frac{L(E,1)}{\Omega(E)R(E)}$	$\prod c_p(E)$	ratio	$E(\mathbb{Q})_{tor}$.
$y^2 = x^3 - x$	32	0	$\frac{1}{8}$	$c_2 = 2$.	$\frac{1}{16}$	$\mathbb{Z}/2 \times \mathbb{Z}/2$
$y^2 = x^3 - 25x$	800	1	$\frac{1}{2}$	$c_2 \cdot c_5 = 2 \cdot 4 = 8$	$\frac{1}{16}$.	$\mathbb{Z}/2 \times \mathbb{Z}/2$.

Exercise Numerically verify BSD for

1) $y^2 = x^3 + 1$

2) $y^2 + y = x^3 - x$

(or check out http://www.lmfdb.org/EllipticCurve/Q/)