E_8: $[0,0,1,-1,0]$ $p=5$

$N=37a1$ rank $\underline{1}$ tors $=1$ $c_{37}=1$. Ш $=1$

$N_5 = 8$

rank $E(\infty\mathbb{Q}) = 1$ Ш finite

$f_E = T$

$E_9 = E_8$ $p = 53$

$N_{53} = \underline{53}$

but still rank $\underline{=1}$ Ш finite

$f_E = T$ (Reg cancels with N_p)

$E_{10} = E_8$ $p = 13$

$N_{13} = 16$

but rank $=1$ $b_n = \underline{2n}$ $\left(\mathcal{O}_7/\mathbb{Z}_7\right)^2$

$f_E = T \cdot (T+p)\Lambda^\times$

E_{11} : $[0,1,0,-18,25]$ $p=3$

$N = 5692 = 4 \cdot 1423$ rank $=2$ tors $=0$

$C_2 = 3$ $c_{1423} = 1$ Ш $\overset{?}{=} 1$

$N_3 = 6$

rank $E(\infty\mathbb{Q}) = 6$ $b_n = O(1)$

$$f_E = T^2 \left(\frac{(1+T)^3 - 1}{T}\right)^2 \cdot \Lambda^\times$$

Ш$(E/\mathbb{Q})[3]$ is trivial.

E_5 : $[1\ -1, 1, -3, 3]$ and $p = 7$

$N = 2 \cdot 13$ b1 rank $= 0$ tors $= \mathbb{Z}/7\mathbb{Z}$,

$c_2 = 7$ $c_{13} = 1$ Ш $= 1$ $N_7 = 7$

rank $E(\infty\mathbb{Q}) = 0$ Ш $= (\mathbb{Q}_7/\mathbb{Z}_7)^4$ (up to finite)

$f =$ degree 4 polynomial $b_n = \underline{4n + O(1)}$

-> not cyclotomic

E_6 : $[0; 1, 0, 4, 4]$ and $p = 3$

$N = 2^2 \cdot 5$ .a1 rank $= 0$ tors $= \mathbb{Z}/6\mathbb{Z}$

$c_2 = 3$ $c_5 = 2$ Ш $= 1$ $N_3 = 6$

rank $E(\infty\mathbb{Q}) = \boxed{2}$ $b_n = O(1)$

Ш is finite

$$f_E = \frac{(1+T)^3 - 1}{T} = T^2 + 3T + 3$$

so rank $E({}_1\mathbb{Q}) = 2$

$${}_1\mathbb{Q} = \mathbb{Q}(\theta)/(\theta^3 - 3\theta + 1)$$

and $x = 4\theta^2 + 4\theta$, $y = -20\theta^2 - 2\theta + 14$ is in $E({}_1\mathbb{Q})$ of infinite order

---

E_7 : $[1, 0, 0, -15663, -755809]$ and $p = 3$

$N = 182b3$ rank 0 tors 0 $c_v = 1$

$\#$Ш$(E/\mathbb{Q}) = 9$ $N_3 = 3$

rank $E(\infty\mathbb{Q}) = 2$ $b_n = p^{2n} + 8n + O(1)$

Ш $\sim (\mathbb{Q}_3/\mathbb{Z}_3)^8 \oplus (\mathbb{Z}/p\mathbb{Z})^\infty$

f_E degree 10

$p^2 \,\|\, f_E$ and $(1+T)^3 - 1 \,\|\, f_E$.

EXAMPLES

$_\infty\mathbb{Q}/\mathbb{Q}$ the cyclotomic $\mathbb{Z}_p$-extension $p \geq 2$.

E_1 : $[0, -1, 1, -10, 20]$ and $p = 3$

$N = 11$ a1 rank $= 0$ tors $= \mathbb{Z}/5\mathbb{Z}$ Ш $= 1$

$N_3 = 5$ $c_5 = 5$

rank $E(_\infty\mathbb{Q}) = 0$ and Ш$(E/_\infty\mathbb{Q})[3^\infty]$ is finite.

$f_E \in \Lambda^\times$ $b_n = \mathrm{ord}_p\left(\#Ш(E/_n\mathbb{Q})[p^\infty]\right) = O(1)$

E_2 : $[1, 0, 1, -1, 0]$ and $p = 3$

$N = 14$ a4 rank $= 0$ tors $= \mathbb{Z}/6\mathbb{Z}$ Ш $= 1$

$c_2 = 2$ $c_7 = 1$

$N_3 = 6$

rank $E(_\infty\mathbb{Q}) = 0$ Ш$(_\infty\mathbb{Q})[p^\infty]$ is finite

$f_E \in \Lambda^\times$ $b_n = O(1)$

E_3 : $= E_1$ but $p = 5$

$N_5 = 5$

rank $E(_\infty\mathbb{Q}) = 0$ and Ш$(E/_\infty\mathbb{Q})[5^\infty] = (\mathbb{Z}/5\mathbb{Z})^\infty$

$f_E = p$. $b_n = 5^n$

E_4 : $= E_1$ but $p = 19$

$N_{19} = 20 \equiv 1 \pmod{19} \to$ supersingular

rank $E(_\infty\mathbb{Q}) = 0$ Ш $= (\mathbb{Q}_5/\mathbb{Z}_5)^\infty$

but $b_n \sim p^{n/2}$

Examples

In sage type

L = E. padic_ lseries(p)

L. series(3)

it gives a p-adic power series. in T

where

~~1) 11a1~~ $T = (1+p)^{s-1} - 1$

rather than looking at $s=1$, we consider $T=0$

In fact this gives a non-canonical isomorphism

$$\Lambda \cong \mathbb{Z}_p[\Delta][\![T]\!]$$

(1) $11a1$ $p = 3$

$$\mathcal{L}_p(E,T) = 2+3+3^2+\cdots + (1+3+\cdots)\cdot T + \cdots$$

$$\begin{tikzcd}[column sep=small] & K_\infty \arrow[dl, dash, "\Delta"'] \arrow[d, dash] \\ \mathbb{Q}_\infty \arrow[d, dash, "r"'] & \mathbb{Q}(\zeta_p) \arrow[dl, dash, "\Delta"] \\ \mathbb{Q} & \end{tikzcd}$$

is a unit in Λ.

So $E(\mathbb{Q})$ is finite and $Ш(E/\mathbb{Q})[3^\infty]$ is trivial

More is true, $E(\mathbb{Q}_\infty)$ is finite and so is $Ш(E/\mathbb{Q}_\infty)[3^\infty]$

(2) Same curve but $p=5$.

$$\mathcal{L}_p(E,T) = 5 + 4\cdot 5^2 + \cdots + (4\cdot 5 + \cdots)T = 5\cdot\text{unit}.$$

In fact $5 \mid$ this

$$5+4\cdot 5^2+\cdots = \left(1-\frac{1}{\alpha}\right)^2 \frac{\prod c_v \cdot \# Ш}{\mathrm{tors}^2} = (5^2+4\cdot 5^3\ldots)\frac{5\cdot ?}{5^2} \Rightarrow Ш(E/\mathbb{Q})[5]=0$$

$\mathrm{rk}\, E(\mathbb{Q}_\infty) = 0$ but $\# Ш(E/{}_n\mathbb{Q})[p^\infty] = p^{p^n + O(1)}$

Looking at thm 2, we should believe that more is true. According to BSD the values

$$G(\chi) \cdot \frac{L(E, \bar{\chi}, 1)}{\Omega^{+(-1)}} \quad \text{for } \chi \text{ of conductor } p^{n+1}$$

know about $rk(E(\mathbb{Q}(\zeta_{p^{n+1}})))$. and, at least if they do not vanish about Ш$(E/\mathbb{Q}(\zeta_{p^{n+1}}))$ for all n !!

So $\mathcal{L}_p(E)$ should know about the growth ~~and~~ of the rank and of Ш in the cyclotomic tower.

It is some sort of a generating function for these — at least conjecturally.

that is what Iwasawa theory does.

Kato's theorem 5

- $\text{ord}_{s=1} \mathcal{L}_p(E, s) \geqslant \text{rank } E(\mathbb{Q})$ $\quad *$

$\Bigg($ If $K/\mathbb{Q}$ is abelian ...
but $E/\mathbb{Q}$ then
$\text{ord}_{s=1} \mathcal{L}_p(E/K, s) \geqslant \text{rank } E(K)$ $\Bigg)$

- If $L(E/K, 1) \neq 0$ then Ш$(E/K)[p^\infty]$ is finite $\forall$ good ord p.

- If ρ_p is surjective and we have equality in $*$ then
  - Ш$(E/\mathbb{Q})[p^\infty]$ is finite and $\text{Reg}_p \neq 0$
  - the leading term has valuation $\geqslant$ what it should be.

So for $s=1$, we appy $\chi_0 = \mathbb{1}$. Hence

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

Cor 4 $\quad \mathcal{L}_p(E,1) = 0 \iff L(E,1) = 0$

Good reduction is crucial here!!
$\alpha \neq 1$

Conjecture ★ : $\quad \mathrm{ord}_{s=1} \mathcal{L}_p(E,s) = \mathrm{ord}_{s=1} L(E,s)$

or in other terms we can formulate the

p-adic BSD conjecture

- $\mathrm{ord}_{s=1} \mathcal{L}_p(E,s) = \mathrm{rank}\ E(\mathbb{Q})$
- the leading term of $\mathcal{L}_p(E,s)$ at $s=1$ is

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

where $\mathrm{Reg}_p(E/\mathbb{Q})$ is the determinant of the (cyclotomic) p-adic height

Conjecture $\quad \mathrm{Reg}_p(E/\mathbb{Q}) \neq 0$

Theorem 2. Let $\chi : G_n \longrightarrow \bar{\mathbb{Q}}^\times$ be a Dirichlet character that does not factor thru G_{n-1}. The induced map $\chi : \Lambda \longrightarrow \bar{\mathbb{Q}}_p$

sends $\mathcal{L}_p(E)$ to $\dfrac{1}{\alpha^{n+1}} \cdot \dfrac{G(\chi)\, L(E, \bar{\chi}, 1)}{\Omega^{\chi(-1)}}$ if $n>0$

and $\mathbb{1}$ maps it to

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

Follows from thm 12, which comes from lemma 10, and lemma 11. e.g.

$$\sum_{j=1}^{p-1} \mu_0^+(j) = \left(1 - \frac{1}{\alpha}\right)^2 [0]^+$$

Just like the p-adic ζ-function interpolates the ζ-values (with an Euler-factor removed).

Cor 3 (ROHRLICH) $\mathcal{L}_p(E) \neq 0$

He shows that $L(E, \bar{\chi}, 1) \neq 0$ for some χ.

This describes $\mathcal{L}_p(E)$ on Artin character. Now, let

$\chi_s(\sigma_a) = \langle a \rangle^s$ for $a \in \mathbb{Z}_p^\times \longleftrightarrow \sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$

and $s \in \mathbb{C}_p$. $\langle a \rangle \cdot \omega(a) = a$ with $\omega(a) \in \mu_{p-1}$.
and $\langle a \rangle \in 1 + p\mathbb{Z}_p$

$\langle a \rangle^s = \exp(s \cdot \log_p \langle a \rangle)$

Define

$$\mathcal{L}_p(E, s) = \chi_{s-1}(\mathcal{L}_p(E)) \in \mathbb{C}_p$$

Recall :

$E/\mathbb{Q}$ elliptic curve

N its conductor

Assume good ordinary $p \nmid a_p \cdot N$

For each $\frac{a}{m} \in \mathbb{Q}$ with $(m,N)=1$, we have a modular symbol $\left[\frac{a}{m}\right]^{\pm} \in \mathbb{Q}$

with $[0]^+ = \frac{L(E,1)}{\Omega^+}$

If $p \nmid a_p$ there is a unique $\alpha \in \mathbb{Z}_p^\times$ st $\alpha^2 - a_p \alpha + p = 0$

we used it to define $\mu_n^{\pm}(a) \in \mathbb{Q}_p^\times$ involving $\left[\frac{a}{p^{n+1}}\right]^+$.

and $\lambda_n \in \mathbb{Q}_p[G_n]$

We saw that $\mathcal{L}_p(E) = (\lambda_n)_n \in \varprojlim \mathbb{Q}_p[G_n]$

where $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$

INTERPOLATION

For $\chi \in \mathbb{Z} \longrightarrow \mathbb{C}$ a Dirichlet character of conductor m, we define

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

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

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

is algebraic in $\mathbb{Q}(\chi)$.

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