Tamagawa Numbers, Serre's Conjecture, & Visibility

William Stein ①

1. Modular forms, modular abelian varieties, and the BSD Conjecture

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}$$

$$S_2(\Gamma_0(N)) = \left\{ \begin{matrix} f: h^* \to \mathbb{C} \\ \text{holomorphic} \end{matrix} ; \begin{matrix} f(\mathbb{Q}\cup\{\infty\}) = 0 \\ f(\gamma z)d(\gamma z) = f(z)dz \ \forall \gamma \in \Gamma_0(N) \end{matrix} \right\}$$

$$\cong H^0(X_0(N), \Omega^1)$$

$$X_0(N) \cong \Gamma_0(N) \backslash h^*$$

$f = \sum_{n=1}^{\infty} a_n q^n$

newform: $a_1 = 1$, $T_n(f) = a_n \cdot f$, not old.

$$\mathbb{T} = \mathbb{Z}[T_1, T_2, \ldots] \quad \text{Hecke algebra}$$

$$J_0(N) = \mathrm{Jac}(X_0(N)) = \mathrm{Pic}^0(X_0(N))$$

$$A_f = J_0(N)[I_f]^0$$

- abelian variety $/\mathbb{Q}$
- $\dim = [\mathbb{Q}(\ldots a_n \ldots) : \mathbb{Q}]$
- simple
- $\mathbb{Z}[\ldots a_n \ldots] \subseteq \mathrm{End}(A_f)$.

$$L(A_f, s) = \prod L(f^\sigma, s) = \prod\left(\sum a_n^\sigma / n^s\right)$$

Conjecture (Birch & Swinnerton-Dyer):

rank: $r = \mathrm{rank}\, A(\mathbb{Q}) = \mathrm{ord}_{s=1} L(A_f, s)$.

|| Thm (Kolyvagin): True if $\mathrm{ord}_{s=1} L(f,s) \le 1$.

formula:

Tamagawa #'s; $\int_{A(\mathbb{R})^0} |\omega|$; regulator

$$\frac{L^{(r)}(A,1)}{r!} = \frac{\left(\prod_{p \mid N\cdot\infty} c_{A,p}\right) \cdot \Omega_A^0 \cdot \mathrm{Reg}_A \cdot \#Ш(A)}{\#A(\mathbb{Q})_{tor} \cdot \# A^\vee(\mathbb{Q})_{tor}}$$

II. Visibility of Galois Cohomology Classes

Defn: $A \subset B$ inclusion of ab vars

$$\mathrm{Vis}_B H^1(\mathbb{Q},A) = \ker\left(H^1(\mathbb{Q},A) \longrightarrow H^1(\mathbb{Q},B)\right)$$

Why "visible"?

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

$$X = \pi^{-1}(x) \in WC(A) \longleftrightarrow c \in \mathrm{Vis}_B H^1(\mathbb{Q},A)$$

$$X \subseteq B$$

$$B \longrightarrow x$$

$$\mathrm{Vis}_B H^1(\mathbb{Q},A) \subseteq H^1(\mathbb{Q},A)$$

$$0 \to A(\mathbb{Q}) \longrightarrow B(\mathbb{Q}) \longrightarrow C(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q},A) \longrightarrow H^1(\mathbb{Q},B)$$

Fact: Everything is visible somewhere (restriction of scalars)

Theorem (Agashe–Stein): "Visibility Construction" in J.N.T.

$$\begin{tikzcd} B[\ell] \arrow[r, hook] \arrow[d, hook] & B \arrow[d, hook] \\ A \arrow[r, hook] & D \end{tikzcd}$$

- assume rank $A = 0$.

If $\ell \nmid 2 \cdot N_D \cdot \#(D/B)(\mathbb{Q})_{tor} \cdot \#B(\mathbb{Q})_{tor} \cdot \prod_{p \mid N_D} c_{B,p}$

then $B(\mathbb{Q})/\ell B(\mathbb{Q}) \hookrightarrow \mathrm{Vis}_D H^1_{ur}(\mathbb{Q},A)$

$$\mathrm{Vis}_D H^1_{ur}(\mathbb{Q},A) \supseteq Ш$$

if $\ell \nmid \prod c_{A,p}$

where

$$H^1_{ur}(\mathbb{Q},A) = \ker\left(H^1(\mathbb{Q},A) \longrightarrow \bigoplus_p H^1(\mathbb{Q}_p^{ur},A)\right).$$

$$H^1_{ur}(\mathbb{Q},A) \supseteq Ш(A)$$

III. Tamagawa Numbers and Unramified Cohomology

Component Group: $\Phi_{E,p} = \mathcal{E}_{\mathbb{F}_p} / \mathcal{E}^{\circ}_{\mathbb{F}_p}$, where $\mathcal{E}/\mathbb{Z}$ = Néron model of E.

For primes $p \leq \infty$,

$$H^1(\mathbb{Q}_p^{ur}/\mathbb{Q}_p, E(\mathbb{Q}_p^{ur})) = \begin{cases} H^1(\overline{\mathbb{F}}_p/\mathbb{F}_p, \Phi_{E,p}(\overline{\mathbb{F}}_p)) & \leftarrow \# = c_{E,p} \quad \text{for } p<\infty \\ H^1(\mathbb{C}/\mathbb{R}, E(\mathbb{C})) & \leftarrow \# \, E(\mathbb{R})/E(\mathbb{R})^{\circ} = c_{E,\infty} \end{cases}$$

$(\mathbb{R}^{ur} = \mathbb{C})$

$$\underset{\left(\frac{H^1_{ur}(\mathbb{Q},E)}{Ш(E)}\right)}{\overset{\text{image}(H^1_{ur}(\mathbb{Q},E))}{\|}} \subseteq \underbrace{\bigoplus_{p\leq\infty} H^1(\mathbb{Q}_p^{ur}/\mathbb{Q}_p, E)}_{\# = \prod_{p \mid N\cdot\infty} c_{E,p}}$$

this all contributes to the $c_{E,p}$.

Visible Tamagawa Number: $E \hookrightarrow J_0(N)$ (say)

$$c_{E,p}^{vis} = \# \, \text{image}\left(\text{Vis}_{J_0(N)} H^1_{ur}(\mathbb{Q},E)\right) \subseteq H^1(\mathbb{Q}_p^{ur}/\mathbb{Q}_p, E)$$

IV. A Conjecture

Suppose

$E/\mathbb{Q}$ elliptic curve, conductor N

prime $\ell \mid c_{E,p}$, $\rho_{E,\ell}$ absolutely irreducible, $\ell \geq 5$, $\ell \neq p$.

Analytic Conjecture: $\ell \mid \frac{L(E,1)}{\Omega_E}$

Visibility Conjecture: $\ell \mid c^{vis}_{E,p} = \#\left(\frac{\mathrm{Vis}_{J_0(N)} H^1_{ur}(\mathbb{Q},E)}{\mathrm{Vis}_{J_0(N)} Ш(E/\mathbb{Q})}\right)$

[Same for $A_f \subset J_0(N)$]

Evidence: (1) Grigor Grigorov claims that the analytic conjecture follows from deep work of Kato, Mazur and Rubin on Euler systems.

Ack: Grigor!

(2) BSD: $\frac{L(E,1)}{\Omega_E} = \frac{(\prod c_{E,p}) \cdot \# Ш(E)}{\# E(\mathbb{Q})_{tor}^2}$

so $\rho_{E,\ell}$ irreducible & BSD $\Rightarrow \ell \mid \frac{L(E,1)}{\Omega_E}$

(3) Ribet: Component group $\Phi_{J_0(N),p}$ is Eisenstein, so

$$\ell \mid \ker(\Phi_{E,p} \longrightarrow \Phi_{J_0(N),p})$$

which makes the visibility Conjecture very plausible.

(4) Visibility conjecture can be false if $\rho_{E,\ell}$ reducible, since can have $\Phi_{E,p} \hookrightarrow \Phi_{J_0(N),p}$.

V. Examples

(1) $E: 114C1$, $114 = 2 \times 3 \times 19$ $E(\mathbb{Q}) \approx \mathbb{Z}/4\mathbb{Z}$

$\ell = 5$ $c_{E,2} = 20$, $c_{E,3} = c_{E,19} = 1$.

$F: 57A1$, $c_{F,3} = 2$, $c_{F,19} = 1$ $F(\mathbb{Q}) \approx \mathbb{Z}$.

do just this

$f_E \equiv' f_F \pmod 5$

$$\begin{array}{ccc} E[5] & \hookrightarrow & B = \alpha_1(F) \\ \downarrow & & \downarrow \\ E & \longrightarrow & D \subset J_0(114) \end{array}$$

visibility construction $\mathbb{Z}/5\mathbb{Z} \cong F(\mathbb{Q})/5F(\mathbb{Q}) \hookrightarrow \mathrm{Vis}_J H^1_{ur}(\mathbb{Q}, E)$.

(2) $E: 1506F1$, $y^2 + xy = x^3 + 703x + 12681$, isolated in isogeny class & semistable so all $\rho_{E,\ell}$ are surjective.

$\ell = 11$, $E(\mathbb{Q}) \approx \mathbb{Z}$

$N = 1506$ $c_{E,2} = c_{E,3} = 11$, $c_{E,251} = 1$.

At level $502 = 2 \cdot 251 = N/3$ find no elliptic curves, but Find (using zope MFD) a newform $g \in S_2(\Gamma_0(502))^{new}$ with $[\mathbb{Q}(\ldots a_n(g) \ldots) : \mathbb{Q}] = 6$ (determines) and there's $\lambda \mid 11$ s.t. $g \equiv' f_E \pmod \lambda$

Also $\mathrm{rank}(A_g) = 0$ (in fact $A_g(\mathbb{Q}) = \mathbb{Z}/7\mathbb{Z}$).

dim 6

$c_{A_g,2} = 2^3 \cdot 7 \cdot 11^2$. and $\frac{L(A_g,1)}{\Omega_{A_g}} = \frac{2^3 \cdot 11^2}{7} \cdot 2^?$.

So can lower level again,

Find $h \in S_2(\Gamma_0(251))$ with $h \equiv' g \equiv' f_E \pmod \lambda$

$[\mathbb{Q}(\ldots a_n(h) \ldots) : \mathbb{Q}] = 4$

$\mathrm{ord}_{s=1} L(h,s) \geq 1$ (prob. $=$) so (probably) $11^2 \mid c^{vis}_{A_g,2}$.

and $c_{A_h,251} = 1$

tors

VI. Strategy of Idea to Prove Conjectures Using Congruences Between Modular Forms (Serre's Conj)

$E/\mathbb{Q}$ elliptic curve, conductor N

$\ell \geq 5$ prime,

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[\ell])$$

absolutely irreducible with

$$\ell \,\|\, \prod_{p|N} c_{E,p}, \quad \text{say } \ell | c_{E,p} \text{ and } \underline{\ell \neq p}.$$

(0) $L(E,1) \neq 0$, else trivial) simplifying, but remove using Diamond-Taylor

(1) Kraus & Serre: $N(\rho_{E,\ell}) = \frac{N}{p}$, $k(\rho)=2$ (Serre) since $\ell | \mathrm{ord}_p(\Delta)$, and reduction is mult. at p.
Note that $p \| N$.

(2) Ribet (Report...): Since $\ell \neq p$, there is a

$$g \in S_2(\Gamma_0(N/p))^{new}$$

such that

$$g \equiv f_E \pmod{\lambda}, \quad \lambda | \ell.$$

(3) Multiplicity one (e.g. Edixhoven):

$$\begin{array}{ccc} & \overset{\alpha}{E[\ell]} \subseteq E \\ & \cap\!\!| \quad\quad \cap\!\!| \\ & B=\alpha_1(A_g)+\alpha_p(A_g) \quad \cap\!\!| \\ A_g \subseteq J_0(N/p) & \overset{\alpha_1}{\underset{\alpha_p}{\rightrightarrows}} & J_0(N) \end{array}$$

(4) Functional Equation:

eigenvalue of Atkin-Lehner

$$L(E,1) \neq 0, \text{ so } \varepsilon_E = 1 = -\prod_{q|N} w_q^N(E),$$

For $q \| N/p$, we have

$$\alpha_d \circ W_q^{N/p} = W_q^N \circ \alpha_d, \text{ so}$$

$$w_q^{N/p}(g) = w_q^N(B) \equiv_\ell w_q^N(E) \in \{\pm 1\}, \text{ hence}$$

$$\varepsilon_g = -\prod_{q|N/p} w_q^{N/p}(g) = \varepsilon_f / w_p^N(f) = -\varepsilon_f = -1$$

since $c_{E,p} > 2 \Rightarrow w_p^N(f) = -\mathrm{Frob}_p = -1$.

so $L(B,1) = 0$.

(5) Modular Symbols Congruence: $L(B,1)=0 \Rightarrow \frac{L(E,1)}{\Omega_E} \equiv 0 \pmod{\ell}$. || or Heegner points

+ Manin constant bound of mazur