Abelian Varieties with Big Monodromy

David Zureick-Brown (Emory University)
David Zywina (IAS)

Slides available at `http://www.mathcs.emory.edu/~dzb/slides/`

2013 Joint Math Meetings
Special Session on Number Theory and Geometry
San Diego, CA

January 9, 2013

Background - Galois Representations

$$\begin{aligned}
\rho_{E,n}\colon \quad G_K \to \operatorname{Aut} E[n] \quad &\cong \quad \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\
\rho_{E,\ell^\infty}\colon \quad G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell) \quad &= \quad \varprojlim_n \mathrm{GL}_2\left(\mathbb{Z}/\ell^n\mathbb{Z}\right) \\
\rho_E\colon \quad G_K \to \mathrm{GL}_2(\widehat{\mathbb{Z}}) \quad &= \quad \varprojlim_n \mathrm{GL}_2\left(\mathbb{Z}/n\mathbb{Z}\right)
\end{aligned}$$

Background - Galois Representations

$$\rho_{E,n}\colon G_K \twoheadrightarrow G_n \hookrightarrow \operatorname{Aut} E[n] \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

$$G_n \cong \mathrm{Gal}(K\left(E[n]\right)/K)$$

Example - torsion

If E has a K-rational torsion point $P \in E(K)[n]$ (of exact order n), then the image is constrained:

$$G_n \subset \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

since for $\sigma \in G_K$ and $Q \in E(\overline{K})[n]$ such that $E(\overline{K})[n] \cong \langle P, Q \rangle$,

$$\begin{aligned} \sigma(P) &= \quad P \\ \sigma(Q) &= \quad a_\sigma P \quad + \quad b_\sigma Q \end{aligned}$$

Example - Isogenies

If E has a K-rational, cyclic isogeny $\phi\colon E \to E'$ with $\ker\phi = \langle P \rangle$, then the image is constrained

$$G_n \subset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

since for $\sigma \in G_K$ and $Q \in E(\overline{K})[n]$ such that $E(\overline{K})[n] \cong \langle P, Q \rangle$,

$$\begin{aligned} \sigma(P) &= a_\sigma P \\ \sigma(Q) &= b_\sigma P + c_\sigma Q \end{aligned}$$

Example - other maximal subgroups

Normalizer of a split Cartan:

$$N_{\mathrm{sp}} = \left\langle \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$$

$G_n \subset N_{\mathrm{sp}}$ iff there exists an unordered pair $\{\phi_1, \phi_2\}$ of cyclic isogenies, neither of which is defined over K, but which are both defined over some quadratic extension of K and which are Galois conjugate.

Classification of Images - Mazur's Theorem

Theorem

Let E be an elliptic curve over $\mathbb{Q}$. Then for $\ell > 11$, $E(\mathbb{Q})[\ell] = \{\infty\}$.

In other words, for $\ell > 11$ the mod ℓ image is not contained in a subgroup conjugate to

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

Classification of Images - Mazur; Bilu, Parent

Theorem (Mazur)

Let E be an elliptic curve over $\mathbb{Q}$ without CM. Then for $\ell > 37$ the mod ℓ image is not contained in a subgroup conjugate to

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Theorem (Bilu, Parent)

Let E be an elliptic curve over $\mathbb{Q}$ without CM. Then for $\ell > 13$ the mod ℓ image is not contained in a subgroup conjugate to

$$\left\langle \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$$

Main conjecture

Conjecture

Let E be an elliptic curve over $\mathbb{Q}$ without CM. Then for $\ell > 37$, $\rho_{E,\ell}$ is surjective.

Serre's Open Image Theorem

Theorem (Serre, 1972)

Let E be an elliptic curve over K without CM. The image of ρ_E

$$\rho_E(G_K) \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

is open.

Note:

$$\mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$$

Sample Consequences of Serre's Theorem

Surjectivity

For large ℓ, $\rho_{E,\ell}$ is surjective.

Lang-Trotter

Density of supersingular primes is 0.

Index 2

Fact

Serre also observed that for an elliptic curve over $\mathbb{Q}$, the index is always divisible by 2.

$$
\begin{tikzcd}
\mathbb{Q}(E[2]) \arrow[ddr, dash] & & \mathbb{Q}(E[n]) \arrow[d, dash] \\
& & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \\
& \mathbb{Q}(\sqrt{\Delta_E}) \arrow[d, dash] & \\
& \mathbb{Q} &
\end{tikzcd}
$$

A surjective example

Theorem (Greicius 2008)

Let α be a real root of $x^3 + x + 1$ and let E be the elliptic curve $y^2 + 2xy + \alpha y = x^3 - x^2$. Then ρ_E is surjective.

Random curves

1. (Duke) For a random $E/\mathbb{Q}$, $\rho_{E,\ell}$ is surjective for all ℓ.
2. (Jones) For a random $E/\mathbb{Q}$, $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] = 2$.
3. (Cojocaru and Hall) Variants over $\mathbb{Q}$.
4. (Zywina) For a random E/K, $\rho_E(G_K)$ is **maximal**.
5. (Wallace) Variant for genus 2.

Zywina's Theorem - I

Let $E_{(a,b)}: y^2 = x^3 + ax + b$.

Theorem (Zywina, 2008)

Let K be a number field such that

1. $K \cap \mathbb{Q}^{cyc} = \mathbb{Q}$,
2. $K \neq \mathbb{Q}$.

Let

$$B_K(x) = \{(a,b) \in \mathcal{O}_K^2 : \Delta_{a,b} \neq 0, \ \|(a,b)\| \leq x\}.$$

Then

$$\lim_{x \to \infty} \frac{|\{(a,b) \in B_K(x) : \rho_{E_{(a,b)}}(G_K) = \mathrm{GL}_2(\widehat{\mathbb{Z}})\}|}{|B_K(x)|} = 1.$$

Other families

$$\mathcal{E}\colon y^2 = x(x-a)(x-b)$$

$$\begin{tikzcd} \mathcal{E}_\eta \arrow[d] \\ \eta = \operatorname{Spec} K(a,b) \end{tikzcd} \qquad \begin{tikzcd} \mathcal{E} \arrow[r, hook] \arrow[dr] & \mathbb{A}^4 \arrow[d] & \mathcal{E}_{(a,b)} \arrow[l, hook'] \arrow[d] \\ & \mathbb{A}^2 & \ni \quad (a,b) \end{tikzcd}$$

1. Define $H_\eta = \{M \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \mid M \equiv I \mod 2\}$
2. $\rho_{\mathcal{E}_{(a,b)}}(G_K) \subset H_\eta$
3. $\rho_{\mathcal{E}_\eta}(G_{K(a,b)}) = H_\eta$

Zywina's Theorem - II

Theorem (Zywina, 2010)

Let K be a number field, let U be a non-empty open subset of $\mathbb{P}_K^N$ and let $\mathcal{E} \to U$ be a family of elliptic curves. Let η be the generic point of U and let $H_\eta = \rho_{\mathcal{E}_\eta}(G_{K(\eta)})$.

Then a random fiber has maximal image of Galois; i.e.,

$$\lim_{N\to\infty} \frac{|\{u \in B_K(N) : \rho_{\mathcal{E}_u}(G_K) = H_\eta\}|}{|B_K(N)|} = 1$$

where

$$B_K(N) = \{u \in U(K) : \Delta_{\mathcal{E}_u} \neq 0, \|u\| \leq N\}.$$

Main Theorem

Definition

We say that a principally polarized abelian variety A over a field K has **big monodromy** if the image of ρ_A is open in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$.

Theorem (ZB-Zywina)

Let U be a non-empty open subset of $\mathbb{P}^N_K$ and let $\mathscr{A} \to U$ be a family of principally polarized abelian varieties. Let η be the generic point of U and suppose moreover that $\mathscr{A}_\eta/K(\eta)$ has big monodromy. Let H_η be the image of $\rho_{\mathscr{A}_\eta}$.

Then a random fiber has maximal monodromy.

Outline of proof - 1 dimensional case

1. (Analytic) Zywina's refinement of Hilbert's irreducibility theorem.
2. (Transcendental) Masser-Wüstholz:

$$\text{for } \ell \gg \log \|u\|, \rho_{\mathcal{E}_u}(G_K) \text{ is irreducible.}$$

3. (Geometric) Tate curve – $\rho_{\mathcal{E}_u,\ell}(G_K)$ contains a transvection if

$$v_p(j(\mathcal{E}_u)) < 0 \text{ and } \ell \nmid v_p(j(\mathcal{E}_u)).$$

4. (Group Theory) 'irreducible + transvection' $\Rightarrow$ surjective.
5. (Arithmetic) For fixed ℓ, for most u, there exists p such that

$$v_p(j(\mathcal{E}_u)) < 0 \text{ and } \ell \nmid v_p(j(\mathcal{E}_u)).$$

Higher dimensional curve ball

1. Analytic, Transcendental, Geometric, and Group Theory steps all work for $g > 1$.
2. The condition
$$v_p(j(\mathcal{E}_u)) < 0 \text{ and } \ell \nmid v_p(j(\mathcal{E}_u))$$
is a statement about variation of the component group of the Néron model of $\mathcal{E}_u$.
3. The analogue of this statement for a general family of abelian varieties fails, and new ideas are needed.

Uniform Semistable Approximation

1. Let $\ell > 4g$.
2. $\rho_{\mathcal{E}_u,\ell}(G_K) =: G_\ell \subset \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.
3. (Nori, '87) Approximate G_ℓ by $G(\mathbb{F}_\ell)$ for some reductive group G.
4. Idea – use classification of reductive groups and independence of ℓ.

Uniform Semistable Approximation

$$\rho_{\mathcal{E}_u,l}(G_K) =: G_\ell \subset \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$$

Definition

1. Define $G_\ell^+ := \langle \text{unipotent elements of } G_\ell \rangle$
2. For $M \in G_\ell^+$, define $\phi_M \colon \mathbb{G}_{a,\mathbb{F}_\ell} \to \mathrm{GSp}_{2g,\mathbb{F}_\ell}$.
3. $\mathbb{G}_\ell^+ := \langle \operatorname{im} \phi_M : M \in G_\ell^+ \rangle$.
4. $\mathbb{H}_\ell := \mathbb{G}_{m,\mathbb{F}_\ell} \cdot \mathbb{G}_\ell^+$

Main Theorem

Theorem (ZB-Zywina)

1. $\mathbb{H}_\ell$ *is reductive for* $\ell > c\,(\log \|u\|)^\gamma$.
2. $H_\ell := G_\ell \cap \mathbb{H}_\ell(\mathbb{F}_\ell)$ *has uniformly bounded index in* G_ℓ *and* $\mathbb{H}_\ell(\mathbb{F}_\ell)$.
3. *For fixed* ℓ, *for most* u, $\mathbb{H}_\ell = \mathrm{GSp}_{2g,\mathbb{F}_\ell}$