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

$$ho_{E,n} \colon G_K o \operatorname{Aut} E[n] \cong \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

$$ho_{E,\ell^{\infty}} \colon G_K o \operatorname{GL}_2(\mathbb{Z}_{\ell}) = \varprojlim_n \operatorname{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$$

$$ho_E \colon G_K o \operatorname{GL}_2(\widehat{\mathbb{Z}}) = \varprojlim_n \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

Background - Galois Representations

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

$$G_n \cong \operatorname{Gal}(K(E[n])/K)$$

Example - torsion

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

$$G_n \subset \left(egin{array}{cc} 1 & * \ 0 & * \end{array}
ight)$$

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

$$\sigma(P) = P$$
 $\sigma(Q) = a_{\sigma}P + b_{\sigma}Q$

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

$$G_n \subset \left(\begin{array}{cc} * & * \\ 0 & * \end{array} \right)$$

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

$$\sigma(P) = a_{\sigma}P$$

$$\sigma(Q) = b_{\sigma}P + c_{\sigma}Q$$

Example - other maximal subgroups

Normalizer of a split Cartan:

$$\mathcal{N}_{\mathsf{sp}} = \left\langle \left(egin{array}{cc} * & 0 \\ 0 & * \end{array}
ight), \left(egin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}
ight)
ight
angle$$

 $G_n \subset N_{\mathrm{sp}}$ 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

$$\left(\begin{array}{cc} 1 & * \\ 0 & * \end{array}\right).$$

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

$$\left(\begin{array}{cc} * & * \\ 0 & * \end{array}\right).$$

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

$$\left\langle \left(\begin{array}{cc} * & 0 \\ 0 & * \end{array}\right), \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}\right) \right\rangle.$$

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}

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

is open.

Note:

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

Sample Consequences of Serre's Theorem

Surjectivity

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

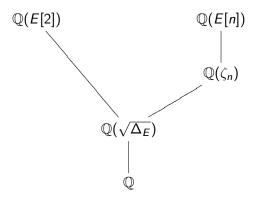
Lang-Trotter

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.



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} , $[\operatorname{GL}_2(\widehat{\mathbb{Z}}): \rho_E(G_{\mathbb{Q}})] = 2$.
- ullet (Cojocaru and Hall) Variants over $\mathbb Q$.
- **4** (Zywina) For a random E/K, $\rho_E(G_K)$ is **maximal**.
- (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

Let

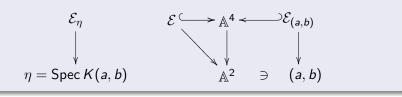
$$B_K(x) = \{(a,b) \in \mathcal{O}_K^2 : \Delta_{a,b} \neq 0, \|(a,b)\| \leq x\}.$$

Then

$$\lim_{x\to\infty}\frac{|\{(a,b)\in B_{\mathcal{K}}(x): \rho_{E_{(a,b)}}(G_{\mathcal{K}})=\mathsf{GL}_2(\widehat{\mathbb{Z}})\}|}{|B_{\mathcal{K}}(x)|}=1.$$

Other families

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



- **1** Define $H_{\eta} = \{ M \in \operatorname{GL}_2(\widehat{\mathbb{Z}}) \mid M \equiv I \mod 2 \}$

Zywina's Theorem - II

Theorem (Zywina, 2010)

Let K be a number field, let U be a non-empty open subset of \mathbb{P}^N_K 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

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

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 $\mathsf{GSp}_{2g}(\widehat{\mathbb{Z}})$.

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

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

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

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

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

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

$$v_p(j(\mathcal{E}_u)) < 0$$
 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.
- The condition

$$v_p(j(\mathcal{E}_u)) < 0$$
 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 .

The analogue of this statement for a general family of abelian varieties fails, and new ideas are needed.

Uniform Semistable Approximation

- **1** Let $\ell > 4g$.
- **1** (Nori, '87) Approximate G_{ℓ} by $G(\mathbb{F}_{\ell})$ for some reductive group G.
- lacktriangle Idea use classification of reductive groups and independence of ℓ .

Uniform Semistable Approximation

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

Definition

- **①** Define $G_{\ell}^+ := \langle \text{unipotent elements of } G_{\ell} \rangle$
- ullet For $M \in G_{\ell}^+$, define $\phi_M \colon \mathbb{G}_{\mathbf{a}, \mathbb{F}_{\ell}} \to \mathsf{GSp}_{2g, \mathbb{F}_{\ell}}$.

Main Theorem

Theorem (ZB-Zywina)

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