Computing the image of Galois representations attached to an elliptic curve

Andrew V. Sutherland (MIT)

December 1, 2009

joint work with Nicholas Katz (Princeton)

Definitions

For an elliptic curve E/K and a prime $\ell \neq \mathrm{char}(K)$, the group $\mathrm{Gal}(\bar{K}/K)$ acts on the ℓ-adic Tate module

$$T_\ell(E) = \varprojlim_n E[\ell^n].$$

This yields a group representation

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}\big(T_\ell(E)\big) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

For this talk $K = \mathbb{Q}$.

Surjectivity of $\rho_{E,\ell}$

For E without complex multiplication, $\rho_{E,\ell}$ is usually surjective.

Theorem (Serre)

Let K be a number field and assume E/K does not have CM.

1. *The image of $\rho_{E,\ell}$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all ℓ.*
2. *There exists ℓ_0 such that $\operatorname{im}\rho_{E,\ell} = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all $\ell > \ell_0$.*

Conjecturally, there is an ℓ_0 that depends only on K.

For $K = \mathbb{Q}$, it is believed that $\ell_0 = 37$.

For this talk E does not have CM.

Reduction modulo ℓ

We will restrict our attention to $\bar{\rho}_{E,\ell} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Theorem (Serre)

For $K = \mathbb{Q}$ and $\ell > 3$, the map $\rho_{E,\ell}$ is surjective iff $\bar{\rho}_{E,\ell}$ is.

Conjecturally, $\operatorname{im} \bar{\rho}_{E,\ell}$ determines $\operatorname{im} \rho_{E,\ell}$ for all $\ell > 3$.

The theorem fails for $\ell = 2$ and $\ell = 3$ [Elkies], but it then suffices to consider $\rho_{E,\ell}$ mod ℓ^k for small k (empirically $k \leq 3$).

When is $\bar{\rho}_{E,\ell}$ non-surjective?

If $E[\ell](\mathbb{Q})$ is non-trivial, then $\bar{\rho}_{E,\ell}$ cannot be surjective.
This occurs for $\ell \le 7$ (and no others [Mazur]).

If $E/\mathbb{Q}$ admits a rational ℓ-isogeny then $\bar{\rho}_{E,\ell}$ is not surjective.
This occurs for $\ell \le 17$ and $\ell = 37$ (and no others, without CM).

However, $\bar{\rho}_{E,\ell}$ may be non-surjective even when $E/\mathbb{Q}$ has no rational ℓ-isogenies, and $\operatorname{im} \bar{\rho}_{E,\ell}$ may vary in any case.

When is $\bar{\rho}_{E,\ell}$ non-surjective?

If $E[\ell](\mathbb{Q})$ is non-trivial, then $\bar{\rho}_{E,\ell}$ cannot be surjective.
This occurs for $\ell \le 7$ (and no others [Mazur]).

If $E/\mathbb{Q}$ admits a rational ℓ-isogeny then $\bar{\rho}_{E,\ell}$ is not surjective.
This occurs for $\ell \le 17$ and $\ell = 37$ (and no others, without CM).

However, $\bar{\rho}_{E,\ell}$ may be non-surjective even when $E/\mathbb{Q}$ has no rational ℓ-isogenies, and $\operatorname{im}\bar{\rho}_{E,\ell}$ may vary in any case.

Classifying the possibilities for $\operatorname{im}\bar{\rho}_{E,\ell} \subseteq \mathrm{GL}_2[\mathbb{Z}/\ell\mathbb{Z}]$ may be viewed as a generalization of Mazur's Theorem.

Distribution of Frobenius traces

For primes p of good reduction, let $a_p = p + 1 - \#E(\mathbb{F}_p)$.

The Čebotarev density theorem implies that for $c \in \mathbb{Z}/\ell\mathbb{Z}$,

$$\operatorname{dens}(a_p \equiv c \bmod \ell) = \frac{\#\{A : \operatorname{tr} A = c, A \in \operatorname{im} \bar{\rho}_{E,\ell}\}}{\# \operatorname{im} \bar{\rho}_{E,\ell}}.$$

When $\operatorname{im} \bar{\rho}_{E,\ell}$ is small, these densities can become highly non-uniform (even zero).

The constants appearing in both the Lang-Trotter conjecture and Koblitz' conjecture depend on $\operatorname{dens}(a_p \equiv c \bmod m)$.

Main results

An algorithm to compute im $\bar{\rho}_{E,\ell}$ for small ℓ (up to isomorphism).

If $\bar{\rho}_{E,\ell}$ is surjective, the algorithm proves this unconditionally.
Otherwise its output is heuristically correct with high probability (in principle, this can also be made unconditional).

Main results

An algorithm to compute im $\bar{\rho}_{E,\ell}$ for small ℓ (up to isomorphism).

If $\bar{\rho}_{E,\ell}$ is surjective, the algorithm proves this unconditionally.
Otherwise its output is heuristically correct with high probability (in principle, this can also be made unconditional).

- Very fast, usually well under a millisecond per curve.
- We have computed $\bar{\rho}_{E,\ell}$ for every E in the Stein-Watkins database (over 100 million curves), for primes $\ell < 60$.

Main results

An algorithm to compute im $\bar{\rho}_{E,\ell}$ for small ℓ (up to isomorphism).

If $\bar{\rho}_{E,\ell}$ is surjective, the algorithm proves this unconditionally. Otherwise its output is heuristically correct with high probability (in principle, this can also be made unconditional).

- Very fast, usually well under a millisecond per curve.
- We have computed $\bar{\rho}_{E,\ell}$ for every E in the Stein-Watkins database (over 100 million curves), for primes $\ell < 60$.

Previous work addressed curves of conductor up to 200 [Reverter-Vila], with partial results up to 30000 [Stein].

A probabilistic approach

The action of the Frobenius endomorphism on $E[\ell](\overline{\mathbb{F}}_p)$ corresponds to a matrix $A_p \in \operatorname{im}\bar{\rho}_\ell \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

We have $\operatorname{tr} A_p = a_p \bmod \ell$ and $\det A_p = p \bmod \ell$, hence we know the characteristic polynomial $\lambda^2 - a_p\lambda + p \bmod \ell$.

By varying p, we can "randomly" sample $\operatorname{im}\bar{\rho}_{E,\ell}$.
The Čebotarev density theorem implies equidistribution.

A probabilistic approach

The action of the Frobenius endomorphism on $E[\ell](\overline{\mathbb{F}}_p)$ corresponds to a matrix $A_p \in \operatorname{im}\bar{\rho}_\ell \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

We have $\operatorname{tr} A_p = a_p \bmod \ell$ and $\det A_p = p \bmod \ell$, hence we know the characteristic polynomial $\lambda^2 - a_p\lambda + p \bmod \ell$.

By varying p, we can "randomly" sample $\operatorname{im}\bar{\rho}_{E,\ell}$.
The Čebotarev density theorem implies equidistribution.

Unfortunately, this does not give enough information.

The case $\ell = 2$

$GL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$ has 6 subgroups in 4 conjugacy classes.

For $H \subseteq GL_2(\mathbb{Z}/2\mathbb{Z})$, let $t_i(H) = \#\{A \in H : \operatorname{tr} A = i\}$.
We consider the possible vectors $t(H) = (t_0(H), t_1(H))$.

1. For $H = GL_2(\mathbb{Z}/2\mathbb{Z})$ we have $t(H) = (4, 2)$.
2. The subgroup $H \cong \mathbb{Z}/3\mathbb{Z}$ has $t(H) = (1, 2)$.
3. Three conjugate $H \cong \mathbb{Z}/2\mathbb{Z}$ have $t(H) = (2, 0)$
4. The trivial H has $t(H) = (1, 0)$.

1-2 are distinguished from 3-4 by a trace 1 element (easy).
We can distinguish 1 from 2 by comparing frequencies (harder).
We can't distinguish 3 from 4 (impossible).

Using the fixspace of A_p

The Frobenius endomorphism fixes $E(\mathbb{F}_p)[\ell]$, hence we have

$$\operatorname{cok}(A_p - I) \cong E(\mathbb{F}_p)[\ell],$$

when viewed as submodules of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

We can easily compute $E(\mathbb{F}_p)[\ell]$, and this yields additional information about A_p that cannot be derived from a_p.

We can now easily distinguish all 4 subgroups when $\ell = 2$. This generalizes nicely.

Signatures in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

For each subgroup H of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we define the *extended signature* of H as the multiset

$$S_H = \left\{ \left(\det A, \operatorname{tr} A, \operatorname{cok}(A - I)\right) : A \in H \right\}.$$

The *signature* s_H is simply the set S_H, ignoring multiplicities. Note that s_H and S_H are invariant under conjugation.

Signatures in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

For each subgroup H of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we define the *extended signature* of H as the multiset

$$S_H = \left\{ \left(\det A, \operatorname{tr} A, \operatorname{cok}(A - I)\right) : A \in H \right\}.$$

The *signature* s_H is simply the set S_H, ignoring multiplicities. Note that s_H and S_H are invariant under conjugation.

Lemma

Let $\ell < 60$ be prime and let G and H be subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for which the determinant map is surjective.

1. $s_G = s_H \quad \Longleftrightarrow \quad S_G = S_H$
2. $S_G = S_H \quad \Longrightarrow \quad G \cong H.$

The lattice of conjugacy classes in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

Up to conjugacy, we may determine im $\bar\rho_{E,\ell}$ identifying its location in the lattice of conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

We may restrict our attention to the (upwardly closed) subset of classes $\mathcal{C}_\ell$ for which the determinant map is surjective.

For any signature set s and $H \in \mathcal{C}_\ell$, we say s_H *minimally covers* s if $s \subset s_H$ and for each $G \in \mathcal{C}_\ell$ we have $s \subset s_G \Longrightarrow s_H \subset s_G$.

Note that if s minimally covered by s_G and s_H, then $s_G = s_H$ and therefore $G \cong H$ (by the lemma).

The algorithm

Given an elliptic curve $E/\mathbb{Q}$, a prime ℓ, and $\epsilon > 0$,
set $s \leftarrow \emptyset, k \leftarrow 0$ and for each good prime $p \neq \ell$:

1. Compute $E(\mathbb{F}_p)$ to obtain a_p and $V_p = E(\mathbb{F}_p)[\ell]$.
2. Set $s \leftarrow s \cup (p \bmod \ell, a_p \bmod \ell, V_p)$, and increment k.
3. If s is minimally covered by s_H for some $H \in \mathcal{C}_\ell$ and we have $\delta_H^k < \epsilon$, then output H and terminate.

The algorithm

Given an elliptic curve $E/\mathbb{Q}$, a prime ℓ, and $\epsilon > 0$,
set $s \leftarrow \emptyset, k \leftarrow 0$ and for each good prime $p \neq \ell$:

1. Compute $E(\mathbb{F}_p)$ to obtain a_p and $V_p = E(\mathbb{F}_p)[\ell]$.
2. Set $s \leftarrow s \cup (p \bmod \ell, a_p \bmod \ell, V_p)$, and increment k.
3. If s is minimally covered by s_H for some $H \in \mathcal{C}_\ell$ and we have $\delta_H^k < \epsilon$, then output H and terminate.

Here δ_H is the maximum over $G \supsetneq H$ of the probability that the signature of a random element of G lies in s_H, which we take to be zero when $H = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

The values of s_H and δ_H for all $H \in \mathcal{C}_\ell$ are precomputed.

Efficient implementation

If $\bar{\rho}_{E,\ell}$ is surjective, we expect the algorithm to terminate in $O(\log \ell)$ iterations (around ten). Otherwise, for $\epsilon = 2^{-n}$, we typically need $O(n)$ iterations (a few hundred).

Efficient implementation

If $\bar{\rho}_{E,\ell}$ is surjective, we expect the algorithm to terminate in $O(\log \ell)$ iterations (around ten). Otherwise, for $\epsilon = 2^{-n}$, we typically need $O(n)$ iterations (a few hundred).

For small p we can quickly compute $\#E(\mathbb{F}_p)$ and determine the structure of $E(\mathbb{F}_p)$ using generic group algorithms.

This is much faster than an ℓ-adic approach for $\ell > 2$, and allows us to treat many ℓ simultaneously at almost no cost.

Efficient implementation

If $\bar{\rho}_{E,\ell}$ is surjective, we expect the algorithm to terminate in $O(\log \ell)$ iterations (around ten). Otherwise, for $\epsilon = 2^{-n}$, we typically need $O(n)$ iterations (a few hundred).

For small p we can quickly compute $\#E(\mathbb{F}_p)$ and determine the structure of $E(\mathbb{F}_p)$ using generic group algorithms.

This is much faster than an ℓ-adic approach for $\ell > 2$, and allows us to treat many ℓ simultaneously at almost no cost.

Precomputing the s_H and δ_H is non-trivial, but this only needs to be done once for each ℓ.

Computational results for the Stein-Watkins database

Testing 136,663,068 curves $E/\mathbb{Q}$ without CM for all $\ell < 60$ took 12 CPU-hours, using $\epsilon = 2^{-100}$, or about 307 μs per curve.

Approximately 1 in 4 curves had non-surjective $\bar{\rho}_{E,\ell}$ for some ℓ, about 1 in 600 for some $\ell > 3$.

In the surjective cases, an average of 9.2 primes p were used, versus 168.5 primes in the non-surjective case.

The most primes used for any one curve was 2061.

mod ℓ images of Galois for $E/\mathbb{Q}$ without CM

ℓ	$\#H$	δ_H	abelian	all traces	all n	torsion/isogeny	SW curves
2	1	0.500	yes	no	no	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	1673058
	2	0.500	yes	no	no	$\mathbb{Z}/2\mathbb{Z}$	33352376
	3	0.333	yes	yes	yes	none	128670
3	2	0.250	yes	no	no	$\mathbb{Z}/3\mathbb{Z}$	3519
	4	0.167	yes	yes	no	3-isogeny	74933
	6	0.250	no	no	no	$\mathbb{Z}/3\mathbb{Z}$	354246
	8	0.250	no	yes	yes	none	18642
	12	0.375	no	yes	no	3-isogeny	3165972
	16	0.167	no	yes	yes	none	53202
5	4	0.200	yes	no	no	$\mathbb{Z}/5\mathbb{Z}$	4
	4	0.200	yes	no	no	5-isogeny	4
	8	0.100	yes	yes	no	5-isogeny	3120
	16	0.050	yes	yes	yes	5-isogeny	500
	16	0.250	no	yes	yes	none	512
	20	0.375	no	no	no	$\mathbb{Z}/5\mathbb{Z}$	504
*	20	0.375	no	no	no	5-isogeny	520
	32	0.333	no	yes	yes	none	3480
	40	0.250	no	yes	no	5-isogeny	109970
	48	0.300	no	yes	yes	none	3090
	80	0.417	no	yes	yes	5-isogeny	44272
	96	0.217	no	yes	yes	none	15246

ℓ	$\#H$	δ_H	abelian	all traces	all n	torsion/isogeny	SW curves
7	18	0.250	no	yes	no	7-isogeny	2
	36	0.333	no	yes	no	7-isogeny	414
	42	0.250	no	no	no	7-isogeny	8
	42	0.417	no	no	no	$\mathbb{Z}/7\mathbb{Z}$	24
*	42	0.417	no	no	no	7-isogeny	24
	72	0.399	no	yes	yes	none	52
	84	0.667	no	yes	no	7-isogeny	1194
	84	0.444	no	yes	no	7-isogeny	12172
	96	0.357	no	yes	yes	none	112
	126	0.250	no	yes	yes	7-isogeny	1042
	252	0.438	no	yes	yes	7-isogeny	28922
11	110	0.450	no	no	no	11-isogeny	2
*	110	0.450	no	no	no	11-isogeny	2
	220	0.640	no	no	no	11-isogeny	2044
	240	0.409	no	yes	yes	none	0
13	288	0.250	no	yes	yes	none	108
	468	0.375	no	yes	yes	13-isogeny	14
*	468	0.375	no	yes	yes	13-isogeny	12
	624	0.667	no	yes	no	13-isogeny	184
	624	0.444	no	yes	yes	13-isogeny	580
	936	0.250	no	yes	yes	13-isogeny	3194
	1872	0.464	no	yes	yes	13-isogeny	3352
17	1088	0.375	no	yes	yes	17-isogeny	368
37	15984	0.444	no	yes	yes	37-isogeny	1024

Future work

This is a work in progress, with much still to be done:

1. Test more curves, analyze the results.
2. Compute mod ℓ^k and mod m Galois images.
3. Consider curves over number fields other than $\mathbb{Q}$.
4. Look at genus 2 Galois images in $\mathrm{GSp}(4, \mathbb{Z}/\ell\mathbb{Z})$.

Computing the image of Galois representations attached to an elliptic curve

Andrew V. Sutherland (MIT)

December 1, 2009

joint work with Nicholas Katz (Princeton)