Computing the image of Galois representations attached to elliptic curves

Andrew V. Sutherland

Massachusetts Institute of Technology

April 6, 2013

Definitions

Let E be an elliptic curve over a number field K.

Let $L = K(E[\ell])$ be the Galois extension of K obtained by adjoining the coordinates of the ℓ-torsion points of $E(\bar{K})$ to K.

The Galois group $\mathrm{Gal}(L/K)$ acts linearly on the ℓ-torsion points

$$E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z},$$

yielding a group representation

$$\rho_{E,\ell}\colon\ \mathrm{Gal}(L/K) \longrightarrow \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

This is the *mod-ℓ Galois representation* attached to E.
This works for any integer $\ell > 1$, but we shall assume ℓ is prime.

Surjectivity

For E without complex multiplication, $\rho_{E,\ell}$ is usually surjective.
Conversely, if E has CM then $\rho_{E,\ell}$ is never surjective for $\ell > 2$.

Theorem (Serre)

Let K be a number field and assume E/K does not have CM. Then $\operatorname{im} \rho_{E,\ell} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *for all sufficiently large primes ℓ.*

Conjecture

For each number field K there is a uniform bound $\ell_{\max}$ such that $\operatorname{im} \rho_{E,\ell} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *for all E/K and all primes $\ell > \ell_{\max}$.*

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

Non-surjectivity

If E has a rational point of order ℓ, then $\rho_{E,\ell}$ is not surjective.
For $E/\mathbb{Q}$ this occurs for $\ell \le 7$ (Mazur).

If E admits a rational ℓ-isogeny, then $\rho_{E,\ell}$ is not surjective.
For $E/\mathbb{Q}$ without CM, this occurs for $\ell \le 17$ and $\ell = 37$ (Mazur).

But $\rho_{E,\ell}$ may be non-surjective even when E does not admit a rational ℓ-isogeny. Even when E has a rational ℓ-torsion point, this does not determine the image of $\rho_{E,\ell}$.

Classifying the possible images of $\rho_{E,\ell}$ that arise over $\mathbb{Q}$ may be viewed as a refinement of Mazur's theorems.

One can consider the same question for any number field K, but we will focus on $K = \mathbb{Q}$.

Applications

There are many practical and theoretical reasons for wanting to compute the image of $\rho_{E,\ell}$, and for searching for elliptic curves with a particular mod-ℓ or mod-m Galois image:

- Explicit BSD computations.
- Modularity lifting.
- Computing Lang-Trotter constants.
- The Koblitz-Zywina conjecture.
- Optimizing the elliptic curve factorization method (ECM).
- Local-global questions.

Computing the image of Galois the hard way

In principle, there is a very simple algorithm to compute the image of $\rho_{E,\ell}$ in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (up to conjugacy):

1. Construct the field $L = K(E[\ell])$ as an (at most quadratic) extension of the splitting field of E's ℓth division polynomial.
2. Pick a basis (P, Q) for $E[\ell]$ and determine the action of each element of $\mathrm{Gal}(L/K)$ on P and Q.

In practice this is computationally feasible only for very small ℓ (say $\ell \le 7$); the degree of L is typically on the order of ℓ^4.

Indeed, this is substantially more difficult than "just" computing the Galois group, which is already a hard problem.

We need something faster, especially if we want to compute *lots* of Galois images (which we do!).

Main results

A very fast algorithm to compute im $\rho_{E,\ell}$ up to isomorphism, (and usually up to conjugacy), for elliptic curves over number fields of low degree and moderate values of ℓ (say $\ell < 200$).

If $\rho_{E,\ell}$ is surjective, the algorithm proves this unconditionally. If not, its output is heuristically correct with very high probability (in principle, this can also be made unconditional).

The current implementation handles elliptic curves over $\mathbb{Q}$ and quadratic number fields, and all primes $\ell < 80$.

The algorithm can also compute $\rho_{E,m}$ for composite m (current work in progress), and generalizes to abelian varieties of low dimension (but the precomputation may be hard).

Main results

We have used the algorithm to compute the mod-ℓ Galois image of every elliptic curve in the Cremona and Stein-Watkins databases for all primes $\ell < 80$.

This includes some 139 million curves, including all curves of conductor $\leq 300,000$. The results are currently being incorporated into Cremona's tables and the LMFDB.

We also analyzed more than 10^{10} curves in various families.

The result is a conjecturally complete classification of 63 non-surjective mod-ℓ Galois images that can arise for an elliptic curve $E/\mathbb{Q}$ without CM.

A probabilistic approach

Let E_p denote the reduction of E modulo a good prime $p \neq \ell$.

The action of the Frobenius endomorphism on $E_p[\ell]$ is given by (the conjugacy class of) an element $A_{p,\ell} \in \operatorname{im} \rho_{E,\ell}$ with

$$\operatorname{tr} A_{p,\ell} \equiv a_p \bmod \ell \qquad \text{and} \qquad \det A_{p,\ell} \equiv p \bmod \ell,$$

where $a_p = p + 1 - \#E_p(\mathbb{F}_p)$ is the trace of Frobenius.

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

Example: $\ell = 2$

$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$ has 6 subgroups in 4 conjugacy classes.
For $H \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, let $t_a(H) = \#\{A \in H : \operatorname{tr} A = a\}$.
Consider the trace frequencies $t(H) = (t_0(H), t_1(H))$:

1. For $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ we have $t(H) = (4, 2)$.
2. The subgroup of order 3 has $t(H) = (1, 2)$.
3. The 3 conjugate subgroups of order 2 have $t(H) = (2, 0)$
4. The trivial subgroup 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 cannot distinguish 3 from 4 at all (impossible).

Sampling traces does not give enough information!

Using the fixed space of A_p

The ℓ-torsion points fixed by the Frobenius endomorphism form the $\mathbb{F}_p$-rational subgroup $E_p[\ell](\mathbb{F}_p)$ of $E_p[\ell]$. Thus

$$\operatorname{fix} A_p = \ker(A_p - I) = E_p[\ell](\mathbb{F}_p) = E_p(\mathbb{F}_p)[\ell]$$

It is easy to compute $E_p(\mathbb{F}_p)[\ell]$, and this gives us information that cannot be derived from a_p alone.

We can now easily distinguish the subgroups of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ by looking at pairs (a_p, r_p), where r_p is the ℓ-rank of $\operatorname{fix} A_p$.

There are three possible pairs, $(0,2)$, $(0,1)$, and $(1,0)$.
The subgroups of order 2 contain $(0,2)$ and $(0,1)$.
The subgroup of order 3 contains $(0,2)$ and $(1,0)$.
The trivial subgroup contains $(0,2)$.

Subgroup signatures

The *signature* of a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is defined by

$$s_H = \{(\det A, \operatorname{tr} A, \operatorname{rk} \operatorname{fix} A) : A \in H\}.$$

Note that s_H is invariant under conjugation.
Remarkably, s_H determines the isomorphism class of H.

Theorem

Let ℓ be a prime and let G and H be subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with surjective determinant maps. If $s_G = s_H$ then $G \simeq H$.

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

Our strategy is to determine $\operatorname{im}\rho_{E,\ell}$ by identifying its location in the lattice of (conjugacy classes of) subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

For any subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we say that a set of triples s is *minimally covered* by s_H if we have $s \subset s_H$, and also $s \subset s_G \implies s_H \subset s_G$ for all subgroups $G \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

If s is minimally covered by both s_G and s_H, then $G \simeq H$.

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 $a_p = p + 1 - \#E(\mathbb{F}_p)$ and $r_p = \mathrm{rk}(E(\mathbb{F}_p)[\ell])$.
2. Set $s \leftarrow s \cup (p \bmod \ell, a_p \bmod \ell, r_p)$ and increment k.
3. If s is minimally covered by s_H, for some $H \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and if $\delta_H^k < \epsilon$, then output H and terminate.

Here δ_H is the maximum over $G \supsetneq H$ of the probability that the triple of a random $A \in G$ lies in s_H (zero if $H = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$).

The values of s_H and δ_H are precomputed all H.

Efficient implementation

If $\rho_{E,\ell}$ is surjective, we expect the algorithm to terminate in $O(\log \ell)$ iterations, typically less than 10 for $\ell < 80$.

Otherwise, if $\epsilon = 2^{-n}$ we expect to need $O(\log \ell + n)$ iterations, typically less than $2n$ (we use $n = 256$).

By precomputing the values a_p and r_p for *every* elliptic curve $E/\mathbb{F}_p$ for all primes p up to, say, 2^{16}, the algorithm is essentially just a sequence of table-lookups, which makes it *very fast*.

It takes just *two minutes* to analyze all 1,887,909 curves in Cremona's tables for all $\ell < 80$ (on a single core).

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

Distinguishing conjugacy classes

Among the non-surjective Galois images that arise with $\ell < 80$ for elliptic curves over $\mathbb{Q}$ without CM and conductor ≤ 300000, there are 45 distinct signatures.

These correspond to 63 possible conjugacy classes.

How can we determine which of these actually occur?

Example: $\ell = 3$

In $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ both of the subgroups

$$H_1 = \langle \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)\rangle \qquad \text{and} \qquad H_2 = \langle \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)\rangle$$

have signature $\{(1,2,1),(2,0,1),(1,2,2)\}$, isomorphic to S_3.

Every element of H_1 and H_2 has 1 as an eigenvalue.
In H_1 the 1-eigenspaces all coincide, but in H_2 they do not.

H_1 corresponds to an elliptic curve with a rational point of order 3, whereas H_2 corresponds to an elliptic curve that has a rational point of order 3 locally everywhere, but not globally.

Distinguishing conjugacy classes

Let d_H denote the least index of a subgroup of H that fixes a nonzero vector in $(\mathbb{Z}/\ell\mathbb{Z})^2$. Then $d_{H_1} = 1$, but $d_{H_2} = 2$.

For $H = \operatorname{im}\rho_{E,\ell}$, the quantity d_H is the degree of the minimal extension L/K over which E has an L-rational point of order ℓ. This can be determined using the ℓ-division polynomial.

Using d_H and s_H we can determine the conjugacy class of $H = \operatorname{im}\rho_{E,\ell}$ in all but one case that arises among the 45 signatures we have found. In this one case, we compute $\operatorname{im}\rho_{E,\ell}$ the hard way (for just a few curves).

It turns out that all 63 of the identified conjugacy classes do arise as the Galois image of an elliptic curve over $\mathbb{Q}$.

Non-surjective Galois images for $E/\mathbb{Q}$ w/o CM and conductor ≤ 300000.

ℓ	gap id	index	d_H	δ_H	$\twoheadrightarrow a_p$	$\twoheadrightarrow N_p$	type	-1	$\#\{E\}$	$\#\{j(E)\}$
2	1.1	6	1	.50	no	no	C_s	yes	67231	21584
	2.1	3	1	.50	no	no	B	yes	772463	292366
	3.1	2	3	.33	yes	yes	C_{ns}	yes	3652	706
3	2.1	24	1	.25	no	no	$\subset C_s$	no	1772	1183
	4.2	12	2	.17	yes	no	C_s	yes	3468	420
	6.1	8	1	.25	no	no	$\subset B$	no	38202	38202
	6.1	8	2	.25	no	no	$\subset B$	no	38202	38202
	8.3	6	4	.25	yes	yes	$N(C_s)$	yes	1394	222
	12.4	4	2	.38	yes	no	B	yes	91594	19758
	16.8	3	8	.17	yes	yes	$N(C_{ns})$	yes	3178	431
5	4.1	120	1	.20	no	no	$\subset C_s$	no	7	7
	4.1	120	2	.20	no	no	$\subset C_s$	no	4	4
	8.2	60	2	.10	yes	no	$\subset C_s$	yes	174	4
	16.2	30	4	.05	yes	yes	C_s	yes	26	6
	16.6	30	8	.25	yes	yes	$\subset N(C_s)$	yes	40	4
	20.3	24	4	.38	no	no	$\subset B$	no	1158	1158
	20.3	24	1	.38	no	no	$\subset B$	no	1158	1158
	20.3	24	4	.38	no	no	$\subset B$	no	455	455
	20.3	24	2	.38	no	no	$\subset B$	no	455	455
	32.11	15	8	.33	yes	yes	$N(C_s)$	yes	288	27
	40.12	12	4	.25	yes	no	$\subset B$	yes	3657	511
	40.12	12	2	.25	yes	no	$\subset B$	yes	3657	511
	48.5	10	24	.33	yes	yes	$N(C_{ns})$	yes	266	38

Non-surjective Galois images for $E/\mathbb{Q}$ w/o CM and conductor ≤ 300000.

ℓ	gap id	index	d_H	δ_H	$\twoheadrightarrow a_p$	$\twoheadrightarrow N_p$	type	-1	$\#\{E\}$	$\#\{j(E)\}$
5	80.30	6	4	.42	yes	yes	B	yes	2352	344
	96.67	5	24	.22	yes	yes	$\twoheadrightarrow S_4$	yes	844	80
7	18.3	112	6	.25	yes	no	$\subset N(C_s)$	no	2	1
	36.12	56	12	.33	yes	no	$\subset N(C_s)$	yes	26	1
	42.4	48	3	.25	no	no	$\subset B$	no	18	18
	42.4	48	6	.25	no	no	$\subset B$	no	18	18
	42.1	48	1	.42	no	no	$\subset B$	no	66	66
	42.1	48	6	.42	no	no	$\subset B$	no	66	66
	42.1	48	2	.42	no	no	$\subset B$	no	29	29
	42.1	48	3	.42	no	no	$\subset B$	no	29	29
	72.30	28	12	.40	yes	yes	$N(C_s)$	yes	32	6
	84.12	24	6	.67	yes	no	$\subset B$	yes	76	6
	84.7	24	2	.44	yes	no	$\subset B$	yes	495	43
	84.7	24	6	.44	yes	no	$\subset B$	yes	495	43
	96.62	21	48	.36	yes	yes	$N(C_{ns})$	yes	36	6
	126.7	16	3	.25	yes	yes	$\subset B$	no	143	143
	126.7	16	6	.25	yes	yes	$\subset B$	no	143	143
	252.28	8	6	.44	yes	yes	B	yes	495	218
11	110.1	120	10	.45	no	no	$\subset B$	no	1	1
	110.1	120	5	.45	no	no	$\subset B$	no	1	1
	110.1	120	10	.45	no	no	$\subset B$	no	1	1
	110.1	120	5	.45	no	no	$\subset B$	no	1	1
	220.7	60	10	.64	no	no	$\subset B$	yes	54	1

Non-surjective Galois images for $E/\mathbb{Q}$ w/o CM and conductor $\leq$ 300000.

ℓ	gap id	index	d_H	δ_H	$\twoheadrightarrow a_p$	$\twoheadrightarrow N_p$	type	-1	$\#\{E\}$	$\#\{j(E)\}$
	220.7	60	10	.64	no	no	$\subset B$	yes	54	1
	240.51	55	120	.41	yes	yes	$N(C_{ns})$	yes	4	1
13	288.400	91	72	.25	yes	yes	$\twoheadrightarrow S_4$	yes	20	2
	468.29	56	12	.38	yes	yes	$\subset B$	no	4	4
	468.29	56	3	.38	yes	yes	$\subset B$	no	4	4
	468.29	56	12	.38	yes	yes	$\subset B$	no	1	1
	468.29	56	6	.38	yes	yes	$\subset B$	no	1	1
	624.155	42	12	.67	yes	no	$\subset B$	yes	16	2
	624.119	42	4	.44	yes	yes	$\subset B$	yes	20	1
	624.119	42	12	.44	yes	yes	$\subset B$	yes	20	1
	936.171	28	12	.25	yes	yes	$\subset B$	yes	85	4
	936.171	28	6	.25	yes	yes	$\subset B$	yes	85	4
	1872.576	14	12	.46	yes	yes	B	yes	192	16
17	1088.1674	72	8	.38	yes	yes	$\subset B$	yes	12	1
	1088.1674	72	16	.38	yes	yes	$\subset B$	yes	12	1
37	15984	114	36	.44	yes	yes	$\subset B$	yes	32	1
	15984	114	12	.44	yes	yes	$\subset B$	yes	32	1