Computing the image of Galois representations attached to elliptic curves

Andrew V. Sutherland
Massachusetts Institute of Technology

May 18, 2015

http://arxiv.org/abs/1504.07618

The action of Galois

Let $y^2 = x^3 + Ax + B$ be an elliptic curve over a number field K.

Let $K(E[m])$ be the extension of K obtained by adjoining the coordinates of all the m-torsion points of $E(\overline{K})$.

This is a Galois extension, and $\mathrm{Gal}(K(E[m])/K)$ acts on

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

via its action on points, $\sigma\colon (x : y : z) \mapsto (x^\sigma : y^\sigma : z^\sigma)$.

This induces a group representation

$$\mathrm{Gal}(K(E[m])/K) \to \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m).$$

Galois representations

The action of $\mathrm{Gal}(K(E[m])/K)$ extends to $G_K := \mathrm{Gal}(\overline{K}/K)$:

$$\rho_{E,m}\colon\ G_K \longrightarrow \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m),$$

The $\rho_{E,m}$ are compatible; they determine a representation

$$\rho_E\colon\ G_K \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}})$$

satisfying $\rho_{E,m} = \pi_m \circ \rho_E$ (here $\pi_m\colon\ \mathrm{GL}_2(\hat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/m)$).

Theorem (Serre's open image theorem)
For E/K without CM, the index of $\rho_E(G_K)$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is finite.

Thus for any E/K without CM there is a minimal $m_E \in \mathbb{Z}$ such that $\rho_E(G_K) = \pi_{m_E}^{-1}(\rho_{E,m_E}(G_K))$.

Mod-ℓ representations

A first step toward computing m_E and $\rho_E(G_K)$ is to determine the primes ℓ and groups $\rho_{E,\ell}(G_K)$ where $\rho_{E,\ell}$ is non-surjective.[1]

By Serre's theorem, if E does not have CM, this is a finite list (henceforth E does not have CM).

Under the GRH, the largest such ℓ is quasi-linear in the bit-size of E (this follows from the conductor bound in [LV 14]). If we put

$$\|E\| := \max(|N_{K/\mathbb{Q}}(A)|, |N_{K/\mathbb{Q}}(B)|).$$

then ℓ is bounded by $(\log \|E\|)^{1+o(1)}$. Conjecturally this bound depends only on K; for $K = \mathbb{Q}$ we expect $\ell \leq 37$.

[1] This does not determine m_E, not even when m_E is squarefree.

Non-surjectivity

Generically, $\rho_{E,\ell}$ (and ρ_{E,ℓ^∞}) is surjective for every prime ℓ.
But the exceptions are interesting.

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, and 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 can arise may be viewed as a refinement of Mazur's theorems.

Applications

There are many practical and theoretical reasons for wanting to compute the images 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 completely straight-forward algorithm to compute $\rho_{E,\ell}(G_K)$ up to conjugacy in $\mathrm{GL}_2(\mathbb{Z}/\ell)$:

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.

The complexity can be bounded by $\tilde{O}(\ell^{18}[K:\mathbb{Q}]^9)$.
It is only practical for very small cases (say $\ell \le 7$ when $K = \mathbb{Q}$).

We need something faster, especially if we want to compute $\rho_{E,\ell}(G_K)$ for many E and ℓ (which we do!).

Main results

- (GRH) Las-Vegas algorithm to compute $\rho_{E,\ell}(G_K)$ up to local conjugacy for all primes ℓ in expected time
$$(\log \|E\|)^{11+o(1)}.$$
- (GRH) Monte-Carlo algorithm to compute $\rho_{E,\ell}(G_K)$ up to local conjugacy for all primes ℓ in time
$$(\log \|E\|)^{1+o(1)}.$$
- Complete classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell)$ up to conjugacy and an algorithm to recognize or enumerate them (with generators) in quasi-linear time.

Locally conjugate groups

Definition

Subgroups H_1 and H_2 of $\mathrm{GL}_2(\mathbb{Z}/\ell)$ are *locally conjugate* if there is a bijection between them preserving conjugacy classes.

Theorem

For every subgroup H_1 of $\mathrm{GL}_2(\mathbb{Z}/\ell)$ there is at most one locally conjugate H_2 that is not conjugate to H_1. The groups H_1 and H_2 are isomorphic and have the same semisimplification.

Theorem

If $\rho_{E_1,\ell}(G_K) = H_1$ is locally conjugate but not conjugate to H_2 then there is an ℓ^n-isogenous E_2 such that $\rho_{E_2,\ell}(G_K) = H_2$. The curve E_2 is defined over K and unique up to isomorphism.

Computations

We have computed all the mod-ℓ Galois images of every elliptic curve in the Cremona and Stein-Watkins databases.

This includes about 140 million curves of conductor up to 10^{10}, including all curves of conductor $\leq 350,000$. The results have been incorporated into the LMFDB (`http://lmfdb.org`).

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 (as expected, they all occur for $\ell \leq 37$).

We have also run the algorithm on all of the elliptic curves defined over quadratic fields that are listed in the LMFDB.

A probabilistic approach

Let $E_{\mathfrak{p}}$ be the reduction of E modulo a good prime $\mathfrak{p}$ of K that does not divide ℓ, and let $p := N\mathfrak{p}$ (wlog we assume p is prime).

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

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

where $a_{\mathfrak{p}} := p + 1 - \#E_{\mathfrak{p}}(\mathbb{F}_p)$ is the trace of Frobenius.

By varying $\mathfrak{p}$, we can "randomly" sample $\rho_{E,\ell}(G_K)$.

The Čebotarev density theorem implies equidistribution, and under the GRH we can assume $\log p = O(\log \ell)$.

This implies $\log p = O(\log\log ||E||)$, so computations with complexity subexponential in $\log p$ are negligible.

Example: $\ell = 2$

$GL_2(\mathbb{Z}/2) \simeq S_3$ has 6 subgroups in 4 conjugacy classes.
For $H \subseteq GL_2(\mathbb{Z}/2)$, 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 $GL_2(\mathbb{Z}/2)$ 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 1-eigenspsace space of $A_\mathfrak{p}$

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

$$\operatorname{fix} A_\mathfrak{p} := \ker(A_\mathfrak{p} - I) = E_\mathfrak{p}[\ell](\mathbb{F}_q) = E_\mathfrak{p}(\mathbb{F}_p)[\ell]$$

Equivalently, $\operatorname{fix} A_\mathfrak{p}$ is the 1-eigenspace of $A_\mathfrak{p}$.
It is easy to compute $E_\mathfrak{p}(\mathbb{F}_p)[\ell]$ (use the Weil pairing), and this gives us information that cannot be derived from $a_\mathfrak{p}$ alone.

We can now easily distinguish the subgroups of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ by looking at pairs $(a_\mathfrak{p}, r_\mathfrak{p})$, where $r_\mathfrak{p}$ is the rank of $\operatorname{fix} A_\mathfrak{p}$ (0, 1, or 2).

There are three possible pairs, $(0,2)$, $(0,1)$, and $(1,0)$.
The subgroups of order 2 contain $(0,2)$ and $(0,1)$ but not $(1,0)$.
The subgroup of order 3 contains $(0,2)$ and $(1,0)$ but not $(0,1)$.
The trivial subgroup contains only $(0,2)$.

Identifying subgroups by their signatures

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

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

We also define the trace-zero ratio of H,

$$z_H := \#\{A : \operatorname{tr} A = 0\}/\#H.$$

Given s_H there are at most two possibilities for z_H.
There exist $O(1)$ elements that determine s_H.
$O(\ell)$ random elements determine s_H, z_H with high probability.

Theorem

If H_1 and H_2 are subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell)$ for which $s_{H_1} = s_{H_2}$ and $z_{H_1} = z_{H_2}$ then H_1 and H_2 are locally conjugate.

Efficient implementation

Asymptotic optimization

There is an integer matrix $A_{\mathfrak{p}}$ for which $A_{\mathfrak{p},\ell} \equiv A_{\mathfrak{p}} \bmod \ell$ for all primes ℓ. The matrix $A_{\mathfrak{p}}$ is determined by $\mathrm{End}(E)$, and under the GRH it can be computed in time subexponential in $\log p$, which is asymptotically negligible [DT02, B11, BS11].

Practical optimization

By precomputing the values $a_{\mathfrak{p}}$ and $r_{\mathfrak{p}}$ for *every* elliptic curve over $\mathbb{F}_p$, say for all primes p up to 2^{18}, the algorithm reduces to a sequence of table-lookups. This makes it extremely fast.

It takes less than a minute to analyze all 1,887,909 curves in Cremona's tables (typically ≤ 10 table lookups per curve).

Distinguishing locally-conjugate non-conjugate groups

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

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

both have signature $\{(1,2,1),(2,0,1),(1,2,2)\}$,
and are 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 locally-conjugate non-conjugate groups

Let $d_1(H)$ denote the least index of a subgroup of H that fixes a nonzero vector in $(\mathbb{Z}/\ell)^2$. Then $d_1(H_1) = 1$, but $d_1(H_2) = 2$.

For $H = \rho_{E,\ell}(G_K)$, the quantity $d_1(H)$ 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 (in fact, using $X_0(\ell)$, since these cases all lie in a Borel).

Using $d_1(H)$ we can distinguish locally conjugate but non-conjugate $\rho_{E,\ell}(G_\mathbb{Q})$ in all but one case that arises over $\mathbb{Q}$. In this one case, we computed $\rho_{E,\ell}(G_\mathbb{Q})$ the hard way.[2]

[2] Using the modular curves in [Z15], this can now be done more efficiently.

Non-surjective mod-ℓ images for $E/\mathbb{Q}$ without CM of conductor $\leq 350,000$.

subgroup	index	generators	-1	d_0	d_1	d	curve
2Cs	6	-	yes	1	1	1	15.a.1
2B	3	$[1,1,0,1]$	yes	1	1	2	14.a.1
2Cn	2	$[0,1,1,1]$	yes	3	3	3	196.a.1
3Cs.1.1	24	$[1,0,0,2]$	no	1	1	2	14.a.1
3Cs	12	$[2,0,0,1],\ [1,0,0,2]$	yes	1	2	4	98.a.3
3B.1.1	8	$[1,0,0,2],\ [1,1,0,1]$	no	1	1	6	14.a.4
3B.1.2	8	$[2,0,0,1],\ [1,1,0,1]$	no	1	2	6	14.a.3
3Ns	6	$[1,0,0,2],\ [2,0,0,1],\ [0,1,1,0]$	yes	2	4	8	338.d.1
3B	4	$[1,0,0,2],\ [2,0,0,1],\ [1,1,0,1]$	yes	1	2	12	50.b.1
3Nn	3	$[1,2,1,1],\ [1,0,0,2]$	yes	4	8	16	245.a.1
5Cs.1.1	120	$[1,0,0,2]$	no	1	1	4	11.a.1
5Cs.1.3	120	$[3,0,0,4]$	no	1	2	4	275.b.2
5Cs.4.1	60	$[4,0,0,4],\ [1,0,0,2]$	yes	1	2	8	99.d.2
5Ns.2.1	30	$[2,0,0,3],\ [0,1,3,0]$	yes	2	8	16	6975.a.1
5Cs	30	$[1,0,0,2],\ [2,0,0,1]$	yes	1	4	16	18176.b.2
5B.1.1	24	$[1,0,0,2],\ [1,1,0,1]$	no	1	1	20	11.a.3
5B.1.2	24	$[2,0,0,1],\ [1,1,0,1]$	no	1	4	20	11.a.2
5B.1.3	24	$[3,0,0,4],\ [1,1,0,1]$	no	1	4	20	50.a.1
5B.1.4	24	$[4,0,0,3],\ [1,1,0,1]$	no	1	2	20	50.a.3
5Ns	15	$[1,0,0,2],\ [2,0,0,1],\ [0,1,1,0]$	yes	2	8	32	608.b.1
5B.4.1	12	$[4,0,0,4],\ [1,0,0,2],\ [1,1,0,1]$	yes	1	2	40	99.d.1
5B.4.2	12	$[4,0,0,4],\ [2,0,0,1],\ [1,1,0,1]$	yes	1	4	40	99.d.3
5Nn	10	$[1,4,2,1],\ [1,0,0,4]$	yes	6	24	48	675.b.1
5B	6	$[1,0,0,2],\ [2,0,0,1],\ [1,1,0,1]$	yes	1	4	80	338.d.1
5S4	5	$[1,4,1,1],\ [1,0,0,2]$	yes	6	24	96	324.b.1

Non-surjective mod-ℓ images for $E/\mathbb{Q}$ without CM of conductor $\leq 350,000$.

subgroup	index	generators	-1	d_0	d_1	d	curve
7Ns.2.1	112	$[2,0,0,4],\ [0,1,4,0]$	no	2	6	18	2450.ba.1
7Ns.3.1	56	$[3,0,0,5],\ [0,1,4,0]$	yes	2	12	36	2450.a.1
7B.1.1	48	$[1,0,0,3],\ [1,1,0,1]$	no	1	1	42	26.b.1
7B.1.2	48	$[2,0,0,5],\ [1,1,0,1]$	no	1	3	42	637.a.1
7B.1.5	48	$[5,0,0,2],\ [1,1,0,1]$	no	1	6	42	637.a.2
7B.1.3	48	$[3,0,0,1],\ [1,1,0,1]$	no	1	6	42	26.b.2
7B.1.4	48	$[4,0,0,6],\ [1,1,0,1]$	no	1	3	42	294.a.1
7B.1.6	48	$[6,0,0,4],\ [1,1,0,1]$	no	1	2	42	294.a.2
7Ns	28	$[1,0,0,3],\ [3,0,0,1],\ [0,1,1,0]$	yes	2	12	72	9225.a.1
7B.6.1	24	$[6,0,0,6],\ [1,0,0,3],\ [1,1,0,1]$	yes	1	2	84	208.d.1
7B.6.2	24	$[6,0,0,6],\ [2,0,0,5],\ [1,1,0,1]$	yes	1	6	84	5733.d.1
7B.6.3	24	$[6,0,0,6],\ [3,0,0,1],\ [1,1,0,1]$	yes	1	6	84	208.d.2
7Nn	21	$[1,3,1,1],\ [1,0,0,6]$	yes	8	48	96	15341.a.1
7B.2.1	16	$[2,0,0,4],\ [1,0,0,3],\ [1,1,0,1]$	no	1	3	126	162.b.1
7B.2.3	16	$[2,0,0,4],\ [3,0,0,1],\ [1,1,0,1]$	no	1	6	126	162.b.3
7B	8	$[3,0,0,1],\ [1,0,0,3],\ [1,1,0,1]$	yes	1	6	252	162.c.1
11B.1.4	120	$[4,0,0,6],\ [1,1,0,1]$	no	1	5	110	121.a.2
11B.1.6	120	$[6,0,0,4],\ [1,1,0,1]$	no	1	10	110	121.a.1
11B.1.5	120	$[5,0,0,7],\ [1,1,0,1]$	no	1	5	110	121.c.2
11B.1.7	120	$[7,0,0,5],\ [1,1,0,1]$	no	1	10	110	121.c.1
11B.10.4	60	$[10,0,0,10],\ [4,0,0,6],\ [1,1,0,1]$	yes	1	10	220	1089.f.2
11B.10.5	60	$[10,0,0,10],\ [5,0,0,7],\ [1,1,0,1]$	yes	1	10	220	1089.f.1
11Nn	55	$[2,2,1,2],\ [1,0,0,10]$	yes	12	120	240	232544.f.1

Non-surjective mod-ℓ images for $E/\mathbb{Q}$ without CM of conductor $\leq 350,000$.

subgroup	index	generators	-1	d_0	d_1	d	curve
13S4	91	$[1,12,1,1],\ [1,0,0,8]$	yes	6	72	288	152100.g.1
13B.3.1	56	$[3,0,0,9],\ [1,0,0,2],\ [1,1,0,1]$	no	1	3	468	147.b.1
13B.3.2	56	$[3,0,0,9],\ [2,0,0,1],\ [1,1,0,1]$	no	1	12	468	147.b.2
13B.3.4	56	$[3,0,0,9],\ [4,0,0,7],\ [1,1,0,1]$	no	1	6	468	24843.o.1
13B.3.7	56	$[3,0,0,9],\ [7,0,0,4],\ [1,1,0,1]$	no	1	12	468	24843.o.2
13B.5.1	42	$[5,0,0,8],\ [1,0,0,2],\ [1,1,0,1]$	yes	1	4	624	2890.d.1
13B.5.2	42	$[5,0,0,8],\ [2,0,0,1],\ [1,1,0,1]$	yes	1	12	624	2890.d.2
13B.5.4	42	$[5,0,0,8],\ [4,0,0,7],\ [1,1,0,1]$	yes	1	12	624	216320.i.1
13B.4.1	28	$[4,0,0,10],\ [1,0,0,2],\ [1,1,0,1]$	yes	1	6	936	147.c.1
13B.4.2	28	$[4,0,0,10],\ [2,0,0,1],\ [1,1,0,1]$	yes	1	12	936	147.c.2
13B	14	$[1,0,0,2],\ [2,0,0,1],\ [1,1,0,1]$	yes	1	12	1872	2450.l.1
17B.4.2	72	$[4,0,0,13],\ [2,0,0,10],\ [1,1,0,1]$	yes	1	8	1088	14450.n.1
17B.4.6	72	$[4,0,0,13],\ [6,0,0,9],\ [1,1,0,1]$	yes	1	16	1088	14450.n.2
37B.8.1	114	$[8,0,0,14],\ [1,0,0,2],\ [1,1,0,1]$	yes	1	12	15984	1225.e.1
37B.8.2	114	$[8,0,0,14],\ [2,0,0,1],\ [1,1,0,1]$	yes	1	36	15984	1225.e.2

References

[B11] G. Bisson, *Computing endomorphism rings of elliptic curves under the GRH*, Journal of Mathematical Cryptology **5** (2011), 101–113.

[BS11] G. Bisson and A.V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, Journal of Number Theory **131** (2011), 815–831.

[DT02] W. Duke and A. Toth, *The splitting of primes in division fields of elliptic curves*, Experimental Mathematics **11** (2002), 555–565.

[LV14] E. Larson and D. Vaintrob, *On the surjectivity of Galois representations associated to elliptic curves over number fields*, Bulletin of the London Mathematical Society **46** (2014) 197–209.

[S68] Jean-Pierre Serre, *Abelian ℓ-adic representations and elliptic curves* (revised reprint of 1968 original), A.K. Peters, Wellesley MA, 1998.

[Z15] D. Zywina, *The possible images of the mod-ℓ representations associated to elliptic curves over $\mathbb{Q}$*, preprint (2015).