# Computing exceptional primes associated to Galois representations of abelian surfaces

Barinder Singh Banwait, Armand Brumer, Hyun Jong Kim, Zev Klagsbrun, Jacob Mayle, Padmavathi Srinivasan, Isabel Vogt

VANTAGE
December 8th, 2020

# Outline

# Galois actions: Why study them?

| Source | $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-set | Some geometric information in $G_{\mathbb{Q}}$-action |
|---|---|---|
| $f(x) \in \mathbb{Q}[x]$ | Roots of $f$ in $\overline{\mathbb{Q}}$ | |
| $A/\mathbb{Q}$ abelian variety | $\ell$-torsion of $A(\overline{\mathbb{Q}})$ | |
| $X/\mathbb{Q}$ nice variety | $\pi_1^{\acute{e}t}(X_{\overline{\mathbb{Q}}}), \mathrm{H}^1_{\acute{e}t}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ | |

# Galois actions: Why study them?

| Source | $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-set | Some geometric information in $G_{\mathbb{Q}}$-action |
|---|---|---|
| $f(x) \in \mathbb{Q}[x]$ | Roots of $f$ in $\overline{\mathbb{Q}}$ | |
| $A/\mathbb{Q}$ abelian variety | $\ell$-torsion of $A(\overline{\mathbb{Q}})$ | Knows about reduction type of $A \mod \ell$ |
| $X/\mathbb{Q}$ nice variety | $\pi_1^{\acute{e}t}(X_{\overline{\mathbb{Q}}}), \mathrm{H}^1_{\acute{e}t}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ | Controls location of rational/torsion points on $X$ |

# Galois actions: Size?

Common Belief:

$$\mathrm{Im}(G_{\mathbb{Q}}) \text{ should be as large as possible,}$$

Common Belief:

$\mathrm{Im}(G_{\mathbb{Q}})$ should be as large as possible,
*unless there is a good reason not to be.*

Restriction:

Common Belief:

$\mathrm{Im}(G_{\mathbb{Q}})$ should be as large as possible,
*unless there is a good reason not to be.*

Restriction:

A finite index subgroup of $G_{\mathbb{Q}}$ commutes with $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$-action.

Common Belief:

$\mathrm{Im}(G_{\mathbb{Q}})$ should be as large as possible,
*unless there is a good reason not to be.*

Restriction:

A finite index subgroup of $G_{\mathbb{Q}}$ commutes with $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$-action.
*Larger* $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \Longrightarrow$ *smaller* $\mathrm{Im}(G_{\mathbb{Q}})$.

Common Belief:

$\mathrm{Im}(G_{\mathbb{Q}})$ should be as large as possible,
*unless there is a good reason not to be.*

Restriction:

A finite index subgroup of $G_{\mathbb{Q}}$ commutes with $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$-action.
*Larger* $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \Longrightarrow$ *smaller* $\mathrm{Im}(G_{\mathbb{Q}})$.

Question:

If $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$, is $\mathrm{Im}(G_{\mathbb{Q}})$ large?

**Theorem (Serre, 1972, $\dim A = 1$)**

*If $E/\mathbb{Q}$ is an elliptic curve, $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$, then*

$$\rho_E \colon G_{\mathbb{Q}} \to \mathrm{Aut}(\varprojlim E[m]) = \mathrm{GL}_2(\hat{\mathbb{Z}})$$

*has open image.*

Remarks:

- Also true when $\dim A$ is $2, 6$ or odd. (Serre, 1986 letter)
- False when $\dim A = 4$. Mumford gave a counterexample. ($G_{\mathbb{Q}}$-action has to preserve additional symmetries for some $A$.)
- Also holds for abelian varieties over number fields.

**Theorem (Serre, 1972, $\dim A = 1$)**

*If $E/\mathbb{Q}$ is an elliptic curve, $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$, then*

$$\rho_E \colon G_{\mathbb{Q}} \to \mathrm{Aut}(\varprojlim E[m]) = \mathrm{GL}_2(\hat{\mathbb{Z}})$$

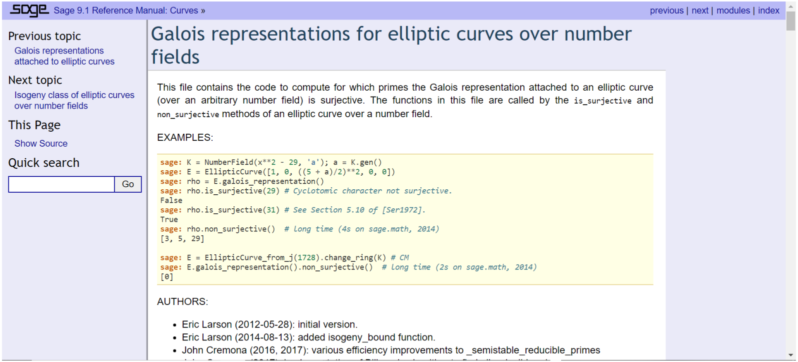
*has open image. In particular, $\rho_{E,\ell}$ is surjective for almost all $\ell$.*

Remarks:

- Also true when $\dim A$ is $2, 6$ or odd. (Serre, 1986 letter)
- False when $\dim A = 4$. Mumford gave a counterexample. ($G_{\mathbb{Q}}$-action has to preserve additional symmetries for some $A$.)
- Also holds for abelian varieties over number fields.

1. Given $E$, can you effectively compute all the *exceptional* $\ell$ where $\rho_{E,\ell}$ is nonsurjective?

1. Given $E$, can you effectively compute all the *exceptional* $\ell$ where $\rho_{E,\ell}$ is nonsurjective? Yes!


Sage 9.1 Reference Manual: Curves »

previous | next | modules | index

Previous topic

Galois representations attached to elliptic curves

Next topic

Isogeny class of elliptic curves over number fields

This Page

Show Source

Quick search

Go

# Galois representations for elliptic curves over number fields

This file contains the code to compute for which primes the Galois representation attached to an elliptic curve (over an arbitrary number field) is surjective. The functions in this file are called by the `is_surjective` and `non_surjective` methods of an elliptic curve over a number field.

EXAMPLES:

```
sage: K = NumberField(x**2 - 29, 'a'); a = K.gen()
sage: E = EllipticCurve([1, 0, ((5 + a)/2)**2, 0, 0])
sage: rho = E.galois_representation()
sage: rho.is_surjective(29) # Cyclotomic character not surjective.
False
sage: rho.is_surjective(31) # See Section 5.10 of [Ser1972].
True
sage: rho.non_surjective()  # long time (4s on sage.math, 2014)
[3, 5, 29]

sage: E = EllipticCurve_from_j(1728).change_ring(K) # CM
sage: E.galois_representation().non_surjective()  # long time (2s on sage.math, 2014)
[0]
```

AUTHORS:

- Eric Larson (2012-05-28): initial version.
- Eric Larson (2014-08-13): added isogeny_bound function.
- John Cremona (2016, 2017): various efficiency improvements to _semistable_reducible_primes

In 2015, Sutherland computes $\rho_{E,\ell}(G_{\mathbb{Q}})$!

# Some related open problems for elliptic curves

2. Serre's uniformity question
   Is there an upper bound $N$ on the largest nonsurjective prime for all $E$ with $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$? Conjectured $N = 37$.

3. Mazur's Program B
   For each subgroup $H$ of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, can you find all the $E/\mathbb{Q}$ such that $\mathrm{Im}\,\rho_E$ is contained in $H$?

INPUT

*$C/\mathbb{Q}$ is a genus 2 curve with affine equation $y^2 = f(x)$,*
*$A = \mathrm{Jac}(C)$ with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$.*

$$\rho_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(A[\ell], \langle \cdot, \cdot \rangle) = \mathrm{GSp}_4(\mathbb{F}_\ell)$$

Serre: $\rho_{A,\ell}$ is surjective for all but finitely many primes $\ell$.

OUTPUT

*The complete list of primes $\ell$ for which $\rho_{A,\ell}$ is nonsurjective.*

# Available now on LMFDB's Olive Branch

We would welcome your feedback and suggestions!

## Galois representations

The mod $\ell$ Galois representation has maximal image $\mathrm{GSp}(4,\mathbb{F}_\ell)$ for all primes $\ell$ except those listed.

| prime | Image type | Witnesses | Is Torsion prime? |
|---|---|---|---|
| 2 | ? | [-1] | no |
| 13 | nss.2p2 | [0, 3] | no |

see it live at The Olive Branch olive.lmfdb.xyz

https://olive.lmfdb.xyz/Genus2Curve/Q/8450/a/8450/1

# Outline

1. Generate $\ell$: Produce a finite list that contains all primes $\ell$ for which $\rho_{A,\ell}$ is nonsurjective.

2. Weed out $\ell$: Given a prime $\ell$, determine if $\rho_{A,\ell}$ is nonsurjective.

# Method

1. Generate $\ell$: Produce a finite list that contains all primes $\ell$ for which $\rho_{A,\ell}$ is nonsurjective.
2. Weed out $\ell$: Given a prime $\ell$, determine if $\rho_{A,\ell}$ is nonsurjective.

Ingredients:

- Mitchell's 1914 classification of maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$.
- Dieulefait's 2002 criteria for $\rho_{A,\ell}(G_{\mathbb{Q}})$ to be contained in each of these subgroups.
- Characteristic polynomials of Frobenius at various auxiliary primes.

# Classification of maximal subgroups of $\mathsf{GSp}_4(\mathbb{F}_\ell)$

1. Stabilizers of linear subspaces.
2. Stabilizer of a hyperbolic or elliptic congruence.
3. Stabilizer of a quadric.
4. Stabilizer of a twisted cubic.
5. Exceptional maximal subgroups.

Key Fact:
$\rho_{A,\ell}$ is nonsurjective $\Leftrightarrow$ $\mathrm{Im}(\rho_{A,\ell})$ is contained in one of these subgroups.

# Notation

| | |
|---|---|
| $N$: | conductor of $A$ |
| $p$: | prime of good reduction for $A$ |
| $\mathrm{Frob}_p$: | a Frobenius element at $p$ |
| $L_{p,A}(T)$: | integral characteristic polynomial for $\mathrm{Frob}_p$ |
| $S_2(\Gamma_0(d))$: | space of weight 2 cusp forms of level $d$ |
| $a_p(f)$: | $p^{\text{th}}$ Fourier coefficient of a cusp form $f$ |

# Step 1: Producing a finite list of primes

Borel Example The $2 + 2$ self-dual summands case, i.e.

- $\ell$ is a prime of good reduction for $A$,
- $\overline{\rho}_{A,\ell} \cong \pi_1 \oplus \pi_2$, with,
- $\dim(\pi_1) = \dim(\pi_2) = 2$ and $\det(\pi_1) = \det(\pi_2) = \mathrm{cyc}_\ell$.

# Step 1: Producing a finite list of primes

Borel Example The $2+2$ self-dual summands case, i.e.

- $\ell$ is a prime of good reduction for $A$,
- $\overline{\rho}_{A,\ell} \cong \pi_1 \oplus \pi_2$, with,
- $\dim(\pi_1) = \dim(\pi_2) = 2$ and $\det(\pi_1) = \det(\pi_2) = \mathrm{cyc}_\ell$.

Serre's conjecture (Khare–Wintenberger theorem):
Modularity of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$-Galois representations $\Longrightarrow$

$$\exists \quad \text{weight 2 cusp forms} \quad f_1, f_2 \quad \text{such that} \quad \pi_i \cong \rho_{f_i,\ell}.$$

Furthermore, we can control the levels of $f_1$ and $f_2$. More precisely,

the product of the levels of $f_1$ and $f_2$ divides the conductor $N$ of $A$.

# Test for $\ell$ in the $2+2$ self dual summands case

Khare-Wintenberger theorem $\Rightarrow \overline{\rho}_{A,\ell} \cong \rho_{f_1,\ell} \oplus \rho_{f_2,\ell}$.

Observation:

Test for finding $\ell$:

$\ell$ divides

# Test for $\ell$ in the $2+2$ self dual summands case

Khare-Wintenberger theorem $\Rightarrow \overline{\rho}_{A,\ell} \cong \rho_{f_1,\ell} \oplus \rho_{f_2,\ell}$.

Observation: If $p$ is a prime of good reduction for $A$, then

$$L_{p,A}(T) = (T^2 - a_p(f_1)T + p)(T^2 - a_p(f_2)T + p) \mod \ell.$$

Test for finding $\ell$:

$\ell$ divides

# Test for $\ell$ in the $2+2$ self dual summands case

Khare-Wintenberger theorem $\Rightarrow \overline{\rho}_{A,\ell} \cong \rho_{f_1,\ell} \oplus \rho_{f_2,\ell}$.

Observation: If $p$ is a prime of good reduction for $A$, then

$$L_{p,A}(T) = (T^2 - a_p(f_1)T + p)(T^2 - a_p(f_2)T + p) \mod \ell.$$

Test for finding $\ell$:

By control of level, there is some $d$ dividing $N$, $d \leqslant \sqrt{N}$, and some $f \in S_2(\Gamma_0(d))$, such that

$$\ell \text{ divides } p\mathrm{Res}\left(L_{p,A}(T), T^2 - a_p(f)T + p\right).$$

# Step 2: Eliminating surjective primes by sampling $Frob_p$

For $\ell > 7$, we employ the following purely group theoretical proposition, which is a consequence of Mitchell's classification.

### Proposition

*For a non-exceptional subgroup $G \subseteq \mathrm{GSp}_4(\mathbb{F}_\ell)$ with surjective similitude character, we have that $G = \mathrm{GSp}_4(\mathbb{F}_\ell)$ if and only if there exists matrices $M, N \in G$ with*

- $\mathrm{charpoly}(M)$ *is irreducible, and*
- $\mathrm{trace}\, N \neq 0$ *and* $\mathrm{charpoly}(N)$ *has a linear factor with multiplicity* $1$.

For primes $\ell \leqslant 7$, we also take into account exceptional subgroups.

# Nonsurjectivity at $\ell = 2$

$$C\colon y^2 = f(x), \quad \deg(f) = 6.$$

Observe:

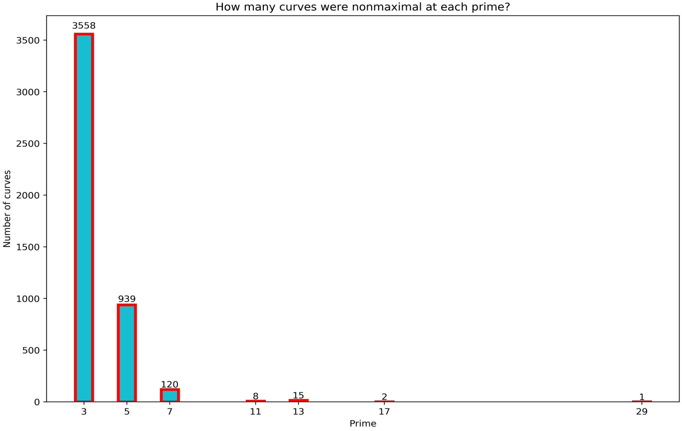
$\rho_{A,2}\colon G_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{F}_2) \cong S_6$ is exactly $G_{\mathbb{Q}} \circlearrowright$ Roots of $f(x)$.

Results:

- $63,107$ curves in LMFDB with $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}(C)) = \mathbb{Z}$.
- $42,230$ curves were nonsurjective at 2.

# Which odd primes $\ell$ were nonsurjective?

Sample space = 63,107 curves in LMFDB with $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}(C)) = \mathbb{Z}$.



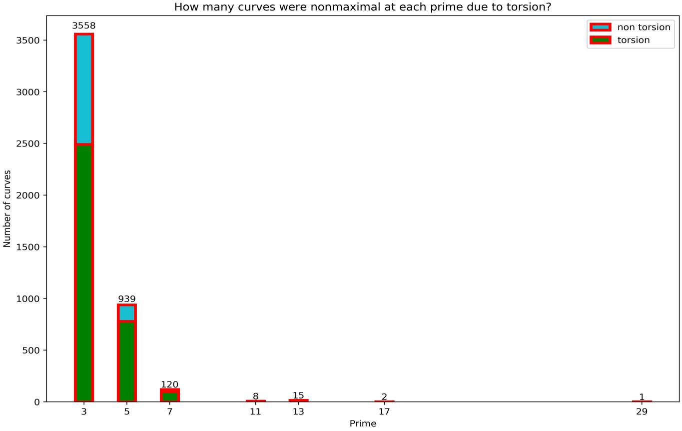
# Possible reasons for nonsurjectivity

# Possible reasons for nonsurjectivity

- Jac($C$) has rational $\ell$-torsion.
- Jac($C$) is isogenous to the Jacobian of a curve with rational $\ell$-torsion.
- ??

# Nonsurjectivity explained by torsion

Sample space = 63,107 curves in LMFDB with $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}(C)) = \mathbb{Z}$.



# An interesting example not explained by torsion

- Running our code on the curve below with LMFDB label 8450.a.8450.1 took 4.8 seconds.

$$y^2 + (x+1)y = x^5 + x^4 - 9x^3 - 5x^2 + 21x.$$

- The list of possibly nonsurjective primes generated by Step 1 is

$$2, 3, 5, 7, 13.$$

- Running Step 2 by testing $\mathrm{Frob}_p$ for all $p < 10,000$, we narrowed this list to

$$2, 13.$$

- Interesting because the Jacobian has no rational torsion!

# Further questions

- Are there effective upper bounds on how Frobenius elements to sample before we hit every conjugacy class in $\rho_{A,\ell}(G_{\mathbb{Q}})$?
- Can we compute $\rho_{A,\ell}(G_{\mathbb{Q}})$ when $\ell$ is not surjective?
- $\dim(A) > 2$?
- Other number fields?