Computing nonsurjective primes associated to Galois representations of genus 2 curves

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

7/11/2023

The mod-ℓ Galois representation of a curve over $\mathbb{Q}$

- Let
  - $C/\mathbb{Q}$ be a smooth, projective, geometrically integral curve of genus g,
  - $A = \mathrm{Jac}(C)$.
- For each prime ℓ, there is the *mod-ℓ Galois representation*

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(A[\ell]) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$$

Question

For what ℓ is $\rho_{A,\ell}$ surjective?

Serre's Open Image Theorem addresses this question almost entirely

Theorem (Serre, 2000)

If A is typical, i.e. $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$, *and if* $\dim A$ *is* 2, 6, *or odd, then* $\rho_{A,\ell}$ *is surjective for all but finitely many* ℓ.

Problem

Given a typical genus 2 *curve* $C/\mathbb{Q}$, *can we compute the finitely many nonsurjective primes* ℓ?

- The analogous problem for elliptic curves with an algorithm implemented in Sage.
- Sutherland (2015) devised an algorithm to compute $\mathrm{Im}\,\rho_{E,\ell}$.

We have an algorithm to find exactly the nonsurjective ℓ.

- "Part 1 algorithm (Dieulefait, 2002 + small improvements)":
  - Given $C/\mathbb{Q}$, generate a finite list PossiblyNonsurjectivePrimes(C) that provably contains all nonsurjective primes ℓ
- "Part 2 algorithm":
  - Given $C/\mathbb{Q}$ and $B > 0$, obtain a sublist LikelyNonsurjectivePrimes(C; B).
  - If B is big enough, then this sublist consists precisely of the nonsurjective primes.

A quick example of these ideas

Running our code on 8450.a.8450.1 from LMFDB:

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

Part 1 gives us

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

as the only possibly non-surjective primes.

Running Part 2 by sampling Frob_p for all $p < 1,000$

```
Conclusions            Frobenius witnesses for each maximal subgroup
--------------------   ----------------------------------------------
Not surjective at 2    [3, 7, 7, 0, 3]
Surjective at 3        [11, 11, 29, 11, 11, 11]
Surjective at 5        [7, 3, 11, 3, 3, 3, 3, 11, 3]
Surjective at 7        [29, 29, 3, 11]
Not surjective at 13   [0, 0, 3]
```

The two parts share overarching ideas

1. Use Mitchell's 1914 classification of maximal (proper) subgroups of $\mathrm{PSp}_4(\mathbb{F}_\ell)$
2. Sample characteristic polynomials $P_p(t)$ of Frobenius elements $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acting on $A[\ell]$.

Remark

- *We classify maximal subgroups of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *with surjective similitude character.*
- $\rho_{A,\ell}$ *is surjective* $\Leftrightarrow$ $\mathrm{Im}\,\rho_{A,\ell}$ *is not contained in one of these maximal subgroups.*
- $P_p(t)$ *can be computed by counting* $C(\mathbb{F}_p)$ *and* $C(\mathbb{F}_{p^2})$.

$\mathrm{GSp}_4(\mathbb{F}_\ell)$ has a few types of maximal subgroups

Write (V, ω) for the 4-dimensional symplectic bilinear form space.

- Reducible maximal subgroups
  - Stabilizer of a 1-dimensional isotropic subspace for ω
  - Stabilizer of a 2-dimensional isotropic subspace for ω
- Irreducible subgroups; normalizer of stabilizer subgroup of V_1 and V_2 where $V = V_1 \oplus V_2$, $\dim V_i = 2$, and V_1 and V_2 are jointly defined over $\mathbb{F}_\ell$ and either
  - V_i are both nondegenerate for ω or
  - V_i are both isotropic for ω
- Stabilizer of a twisted cubic
- Exceptional maximal subgroups

Not all maximal subgroups generally occur as Im $\rho_{A,\ell}$

Write ω for the symplectic bilinear form.

- Reducible maximal subgroups
  - Stabilizer of a 1-dimensional isotropic subspace for ω
  - Stabilizer of a 2-dimensional isotropic subspace for ω
- Irreducible subgroups; normalizer of stabilizer subgroup of V_1 and V_2 where $V = V_1 \oplus V_2$, dim $V_i = 2$, and V_1 and V_2 are jointed defined over $\mathbb{F}_\ell$ and either
  - V_i are both nondegenerate for ω or
  - V_i are both isotropic for ω
- ~~Stabilizer of a twisted cubic~~ (unless $\ell \leq 7$ or ℓ is not semistable)
- ~~Exceptional maximal subgroups~~ (unless $\ell \leq 7$ or ℓ is not semistable)

One subalgorithm for part 1 uses modularity.

Suppose that ℓ is nonsurjective good prime by virtue of:

- $\rho_{A,\ell}^{\text{semisimplification}} \cong_{\overline{\mathbb{F}}_\ell} \pi_1 \oplus \pi_2$ where
- $\dim(\pi_i) = 2$, $\det(\pi_i) = \mathrm{cyc}_\ell$.

By Khare-Wintenberger's theorem (2006, 2009), previously Serre's conjecture, there exist modular forms f_i such that $\pi_i \cong \rho_{f_i,\ell}$.

- In fact, $f_i \in S_2^{\text{new}}(\Gamma_0(N_i))$.
- Thus, for any good prime $p \neq \ell N$,

$$P_p(t) \equiv (t^2 - a_p(f_1)t + p)(t^2 - a_p(t_2)t + p) \pmod{\ell}.$$
$$\ell \mid \mathrm{Res}(P_p(t), t^2 - a_p(f_i)t + p)$$

Part 2 removes surjective primes by sampling Frob_p

- $\rho_{A,\ell}$ is not surjective $\Leftrightarrow$ $\mathrm{Im}\,\rho_{A,\ell}$ is contained in some maximal subgroup.
- There are criteria for $P_p(t)$ to satisfy for $\mathrm{Im}\,\rho_{A,\ell}$ to be contained in the various types/conjugacy classes of maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$.
- Given C and $B > 0$, and for each ℓ, we sample $P_p(t)$ for $p < B$ and remove ℓ if all of these criteria are violated for some (combination of) $P_p(t)$.

Remark

$\rho_{A,2}$ is surjective if and only if the Galois group of the splitting field of the discriminant of C is $\mathrm{Sym}(6)$.

The general criteria is purely group theoretic

Proposition

Let $\ell > 7$ be a prime and let $G \subseteq \mathrm{GSp}_4(\mathbb{F}_\ell)$. Then, $G = \mathrm{GSp}_4(\mathbb{F}_\ell)$ if and only if there exist $X, Y \in G$ such that

- $\mathrm{charpoly}(X)$ *is irreducible*
- $\mathrm{trace}(Y) \neq 0$ *and* $\mathrm{charpoly}(Y)$ *has a linear factor with multiplicity one.*

Part 2 gives exactly the nonsurjective ℓ if enough Frobenii are considered

Theorem

Given a typical genus 2 curve $C/\mathbb{Q}$, if B is sufficiently large, then $\mathrm{LikelyNonsurjectivePrimes}(C, B)$ *consists exactly of the nonsurjective primes of A.*

Question

What is "sufficiently large" here?

Chebotarev bounds give sufficiently large B

Theorem

Let q be the largest non-surjective prime for C. Assuming GRH, any B such that

$$B \geq \left(4\left[(2q^{11}-1)\log \mathrm{rad}(2qN_A) + 22q^{11}\log(2q)\right] + 5q^{11} + 5\right)^2$$

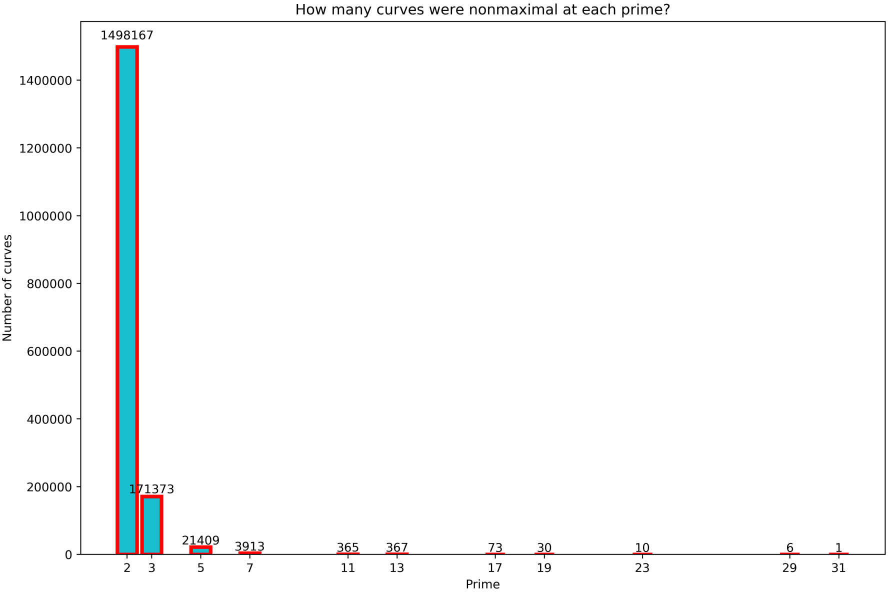
is "sufficiently large".

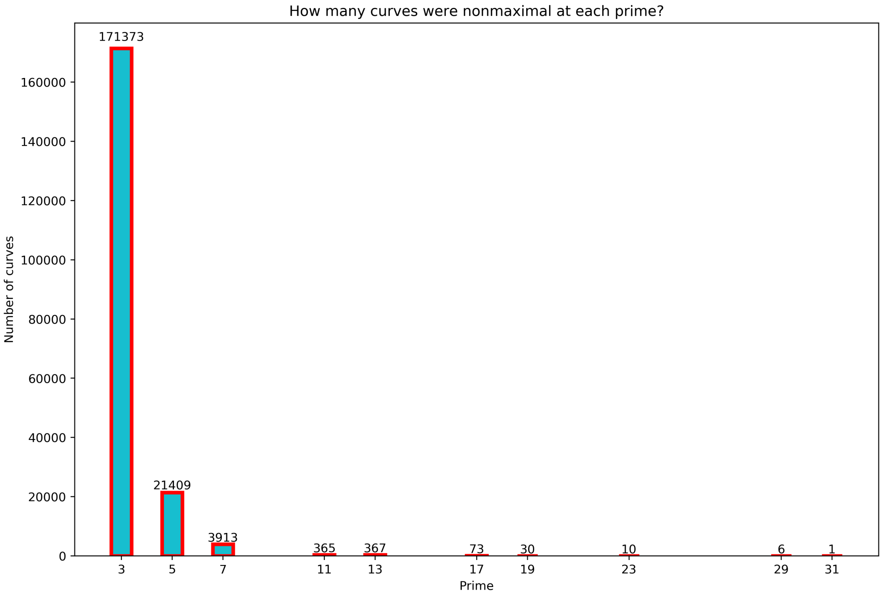
Theorem

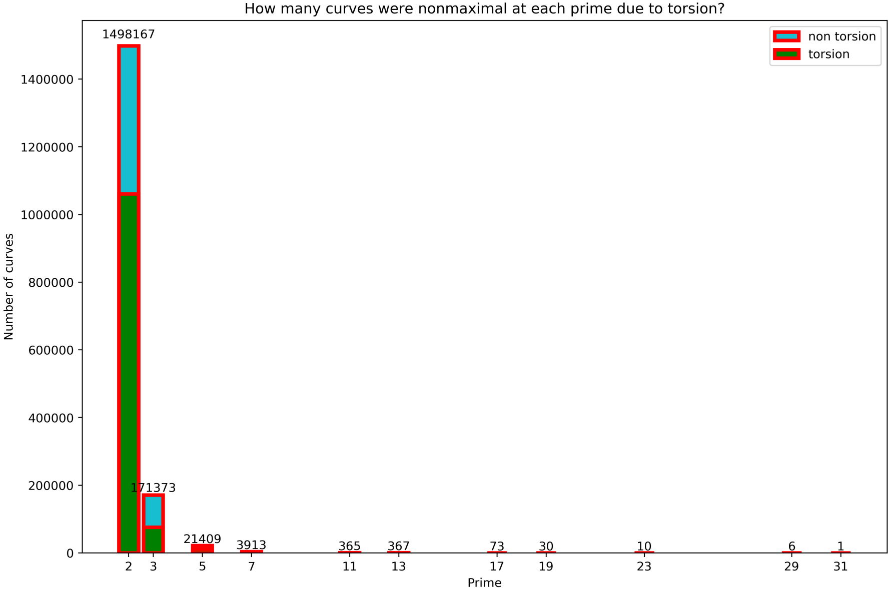
Assuming that $\rho_{A,\ell}$ is surjective, there is an effective bound B_0 such that, for any $B > B_0$, if we sample $P_p(t)$ for n primes $p \in [B, 2B]$ uniformly and independently at random, then the Part 2 algorithm fails to remove ℓ with a probability $< 3 \cdot \left(\frac{9}{10}\right)^n$.

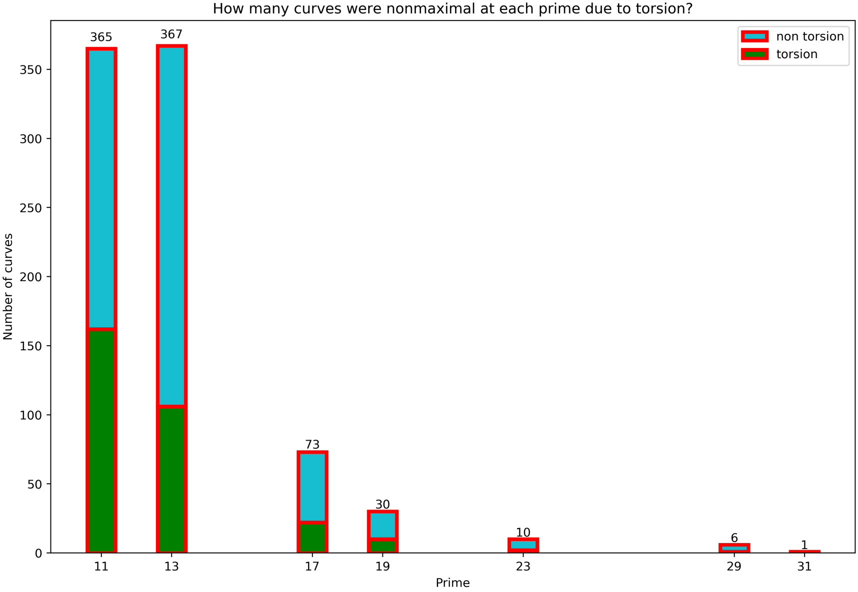
We ran our algorithm on $1,743,737$ typical genus 2 curves

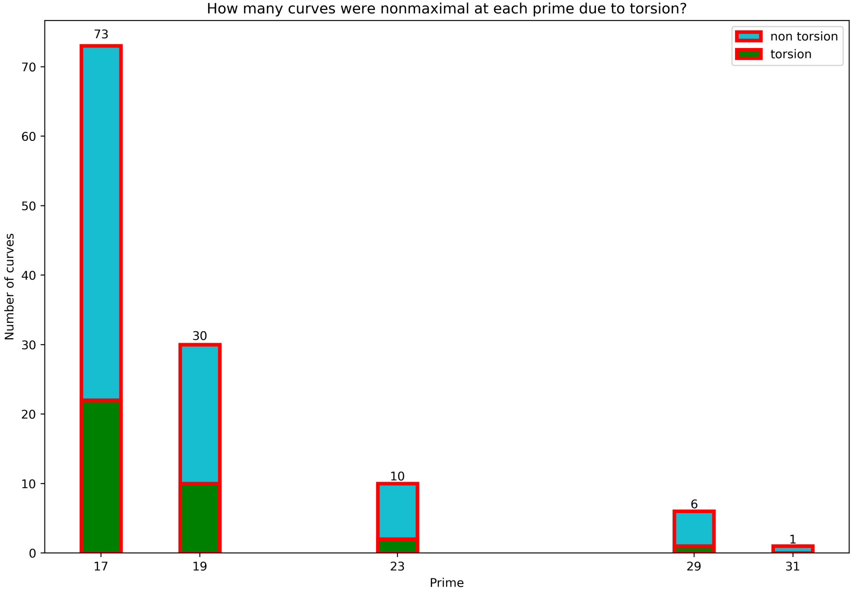
- All of conductor bounded by 2^{20}.
- The curves are being prepared for addition into the LMFDB.
- Let $B = 1,000$ in the part 2 algorithm.
- Took about 35 hours on MIT's Lovelace computer.

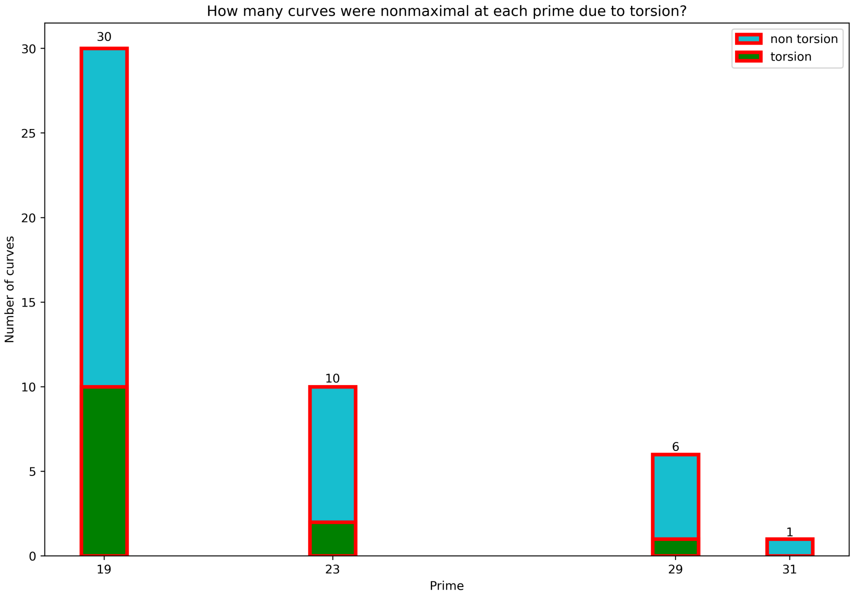

How many curves were nonmaximal at each prime?
Number of curves
Prime
1498167
171373
21409
3913
365
367
73
30
10
6
1
0
200000
400000
600000
800000
1000000
1200000
1400000
2
3
5
7
11
13
17
19
23
29
31


How many curves were nonmaximal at each prime?
Number of curves
Prime
0
20000
40000
60000
80000
100000
120000
140000
160000
3
5
7
11
13
17
19
23
29
31
171373
21409
3913
365
367
73
30
10
6
1


How many curves were nonmaximal at each prime due to torsion?
non torsion
torsion
Number of curves
Prime
1498167
171373
21409
3913
365
367
73
30
10
6
1
0
200000
400000
600000
800000
1000000
1200000
1400000
2
3
5
7
11
13
17
19
23
29
31


How many curves were nonmaximal at each prime due to torsion?
non torsion
torsion
Number of curves
Prime
365
367
73
30
10
6
1
0
50
100
150
200
250
300
350
11
13
17
19
23
29
31


How many curves were nonmaximal at each prime due to torsion?
non torsion
torsion
Number of curves
Prime
0
10
20
30
40
50
60
70
17
19
23
29
31
73
30
10
6
1


How many curves were nonmaximal at each prime due to torsion?
non torsion
torsion
Number of curves
Prime
30
10
6
1
0
5
10
15
20
25
30
19
23
29
31

Find our computational results on the LMFDB!

- We had also run our code all 63,107 typical genus 2 curves in the LMFDB
- `https://www.lmfdb.org/`
- `https://www.lmfdb.org/Genus2Curve/Q/439587/d/439587/1`

Further questions

- Can we compute $\operatorname{Im} \rho_{A,\ell}$ when ℓ is not surjective?
- $\dim(A) > 2$?
- Other number fields?
- Bounds on the index of Galois image?

Acknowledgements

On behalf of my collaborators, I would like to thank

- Noam Elkies for providing interesting examples of genus 2 curves in the literature
- Davide Lombardo for helpful discussions about computing geometric endomorphism rings
- Drew Sutherland for providing us with a dataset of Hecke characteristic polynomials and with the dataset of the $1,743,737$ typical genus 2 curves
- The *Workshop on Arithmetic Geometry, Number Theory, and Computation* at ICERM in 2020 via Simons Foundation Grant 546235
- Collaborate@ICERM in 2022 via NSF Grant No. DMS-1929284
- (Isabel Vogt, partially): NSF grants DMS-1902743 and DMS-2200655
- The LuCaNT Organizers

Bibliography

- Dieulefait, Luis V. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$, *Experimental Mathematics*, 11(4):503-512, 2002.
- Mitchell, Howard H. The subgroups of the quaternary abelian linear group, *Transactions of the American Mathematical Society*, 15(4):379-396, 1914.
- Serre, Jean-Pierre. Oeuvres. *Springer-Verlag*, 4:1-55, 2000.
- Sutherland, Andrew V. Computing Images of Galois Representations Attached to Elliptic Curves, *Forum of Mathematics, Sigma*, 4, 2016.