Hensel-lifting torsion points on Jacobians and Galois representations from higher étale cohomology spaces

Nicolas Mascot

Trinity College Dublin

p-adic Langlands correspondence
IRMAR, Rennes
September 5th 2019

Goal

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_d(\mathbb{F}_\ell)$ be a Galois representation.

Goal

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_d(\mathbb{F}_\ell)$ be a Galois representation.

Goal: compute ρ explicitly.

Goal

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_d(\mathbb{F}_\ell)$ be a Galois representation.

Goal: compute ρ explicitly.

This means:

1. Find $F(x) \in \mathbb{Q}[x]$ and an indexation of its roots by ${\mathbb{F}_\ell}^d$ such that the Galois action on these roots represents ρ,
2. Have an efficient method to determine $\rho(\mathrm{Frob}_p)$, even for huge p.

The case of curves

Suppose we know a curve $C/\mathbb{Q}$ such that ρ is afforded by an $\mathbb{F}_\ell$-subspace $T \subseteq J[\ell]$, where $J = \mathrm{Jac}(C)$.

The case of curves

Suppose we know a curve $C/\mathbb{Q}$ such that ρ is afforded by an $\mathbb{F}_\ell$-subspace $T \subseteq J[\ell]$, where $J = \mathrm{Jac}(C)$.

To isolate $T \subset J[\ell]$, we assume that for one good prime $p \neq \ell$, we know

$$\chi_\rho(x) = \det\left(x - \mathrm{Frob}_p\,|_T\right) \in \mathbb{F}_\ell[x]$$

and

$$L(x) = \det\left(x - \mathrm{Frob}_p\,|_J\right) \in \mathbb{Z}[x],$$

and that

$$\gcd(\chi_\rho, L/\chi_\rho) = 1 \in \mathbb{F}_\ell[x].$$

Strategy

1. Find $q = p^a$ such that $T \subseteq J(\mathbb{F}_q)[\ell]$,
2. Generate $\mathbb{F}_q$-points of T until we get an $\mathbb{F}_\ell$-basis,
3. Lift these points from $J(\mathbb{F}_q)$ to $J(\mathbb{Z}_q/p^e)$, $e \gg 1$,
4. Form all linear combinations of these points in $T \subseteq J(\mathbb{Z}_q/p^e)[\ell]$,
5. $F(x) = \prod_{t \in T} \big(x - \alpha(t)\big)$, where $\alpha : J \dashrightarrow \mathbb{A}^1$,
6. Identify $F(x) \in \mathbb{Q}[x]$.

Getting a basis of T

Idea: $J(\mathbb{F}_q) \twoheadrightarrow J(\mathbb{F}_q)[\ell^\infty] \twoheadrightarrow J(\mathbb{F}_q)[\ell] \twoheadrightarrow T$.

- $\#J(\mathbb{F}_q) = \mathrm{Res}\left(L(x), x^a - 1\right) = \ell^b M.$

$$\rightsquigarrow \forall t \in J(\mathbb{F}_q),\ M \cdot t \in J(\mathbb{F}_q)[\ell^\infty].$$

Getting a basis of T

Idea: $J(\mathbb{F}_q) \longrightarrow\!\!\!\!\!\rightarrow J(\mathbb{F}_q)[\ell^\infty] \longrightarrow\!\!\!\!\!\rightarrow J(\mathbb{F}_q)[\ell] \longrightarrow\!\!\!\!\!\rightarrow T$.

- $\#J(\mathbb{F}_q) = \mathrm{Res}\left(L(x), x^a - 1\right) = \ell^b M.$

  $$\rightsquigarrow \forall t \in J(\mathbb{F}_q),\ M \cdot t \in J(\mathbb{F}_q)[\ell^\infty].$$

- $L(x) = \chi_\rho(x)\psi(x) \in \mathbb{F}_\ell[x]$

  $$\rightsquigarrow \forall t \in J(\mathbb{F}_q)[\ell],\ \psi(\mathrm{Frob}_p) \cdot t \in T.$$

Getting a basis of T

Idea: $J(\mathbb{F}_q) \longrightarrow\!\!\!\!\!\rightarrow J(\mathbb{F}_q)[\ell^\infty] \longrightarrow\!\!\!\!\!\rightarrow J(\mathbb{F}_q)[\ell] \longrightarrow\!\!\!\!\!\rightarrow T$.

- $\#J(\mathbb{F}_q) = \mathrm{Res}\left(L(x), x^a - 1\right) = \ell^b M.$

  $$\rightsquigarrow \forall t \in J(\mathbb{F}_q),\ M \cdot t \in J(\mathbb{F}_q)[\ell^\infty].$$

- $L(x) = \chi_\rho(x)\psi(x) \in \mathbb{F}_\ell[x]$

  $$\rightsquigarrow \forall t \in J(\mathbb{F}_q)[\ell],\ \psi(\mathrm{Frob}_p) \cdot t \in T.$$


Not uniformly distributed!

Gaussian elimination by pairings

Example

Suppose $J(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $T = J[\ell]$.

Gaussian elimination by pairings

Example

Suppose $J(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $T = J[\ell]$.
$x_1 = (a_1, b_1) \in J(\mathbb{F}_q)[\ell^\infty]$

Gaussian elimination by pairings

Example

Suppose $J(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $T = J[\ell]$.
$x_1 = (a_1, b_1) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_1 := \ell x_1 = (\ell a_1, 0) \in J(\mathbb{F}_q)[\ell]$

Gaussian elimination by pairings

Example

Suppose $J(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $T = J[\ell]$.
$x_1 = (a_1, b_1) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_1 := \ell x_1 = (\ell a_1, 0) \in J(\mathbb{F}_q)[\ell]$
$x_2 = (a_2, b_2) \in J(\mathbb{F}_q)[\ell^\infty]$

Gaussian elimination by pairings

Example

Suppose $J(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $T = J[\ell]$.

$x_1 = (a_1, b_1) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_1 := \ell x_1 = (\ell a_1, 0) \in J(\mathbb{F}_q)[\ell]$

$x_2 = (a_2, b_2) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_2 := \ell x_2 = (\ell a_2, 0) \in J(\mathbb{F}_q)[\ell]$

Gaussian elimination by pairings

Example

Suppose $J(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $T = J[\ell]$.
$x_1 = (a_1, b_1) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_1 := \ell x_1 = (\ell a_1, 0) \in J(\mathbb{F}_q)[\ell]$
$x_2 = (a_2, b_2) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_2 := \ell x_2 = (\ell a_2, 0) \in J(\mathbb{F}_q)[\ell]$

Use the Frey-Rück pairing

$$[\,\cdot\,,\,\cdot\,]_\ell : J(\mathbb{F}_q)[\ell] \times J(\mathbb{F}_q)/\ell J(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^\times/\mathbb{F}_q^{\times\ell}$$

to detect linear dependency in $J(\mathbb{F}_q)[\ell]$, and obtain a generating set of T.

Gaussian elimination by pairings

Example

Suppose $J(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $T = J[\ell]$.
$x_1 = (a_1, b_1) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_1 := \ell x_1 = (\ell a_1, 0) \in J(\mathbb{F}_q)[\ell]$
$x_2 = (a_2, b_2) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_2 := \ell x_2 = (\ell a_2, 0) \in J(\mathbb{F}_q)[\ell]$

Use the Frey-Rück pairing

$$[\,\cdot\,,\,\cdot\,]_\ell : J(\mathbb{F}_q)[\ell] \times J(\mathbb{F}_q)/\ell J(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^\times/\mathbb{F}_q^{\times\ell}$$

to detect linear dependency in $J(\mathbb{F}_q)[\ell]$, and obtain a generating set of T.

Example (continued)

Take $y \in J(\mathbb{F}_q)$, find $\lambda, \mu \in \mathbb{Z} :\ \lambda[t_1, y]_\ell + \mu[t_2, y]_\ell = 0 \in \mathbb{F}_\ell$.
Then probably $\lambda t_1 + \mu t_2 = 0$

Gaussian elimination by pairings

Example

Suppose $J(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $T = J[\ell]$.
$x_1 = (a_1, b_1) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_1 := \ell x_1 = (\ell a_1, 0) \in J(\mathbb{F}_q)[\ell]$
$x_2 = (a_2, b_2) \in J(\mathbb{F}_q)[\ell^\infty] \rightsquigarrow t_2 := \ell x_2 = (\ell a_2, 0) \in J(\mathbb{F}_q)[\ell]$

Use the Frey-Rück pairing

$$[\,\cdot\,,\,\cdot\,]_\ell : J(\mathbb{F}_q)[\ell] \times J(\mathbb{F}_q)/\ell J(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^\times/\mathbb{F}_q^{\times\ell}$$

to detect linear dependency in $J(\mathbb{F}_q)[\ell]$, and obtain a generating set of T.

Example (continued)

Take $y \in J(\mathbb{F}_q)$, find $\lambda, \mu \in \mathbb{Z} : \lambda[t_1, y]_\ell + \mu[t_2, y]_\ell = 0 \in \mathbb{F}_\ell$.
Then probably $\lambda t_1 + \mu t_2 = 0 \rightsquigarrow t_3 := \lambda x_1 + \mu x_2 \in J(\mathbb{F}_q)[\ell]$.

Jacobians

☠ Computing with Jacobians is *not* straightforward.

Example (duplication in genus 2)

Let us temporarily assume that our curve has the form $\mathcal{C}^g$ of equation (8). Then the following is the matrix W^g (Lemma 2.1) which gives the addition of a rational point, $\mathbf{b}^g$, of order 2.

$$W^g_{11} = -g_2^2h_0 + g_0g_2h_2 + g_0^2h_4$$
$$W^g_{12} = -g_1g_2h_0 + g_0g_2h_1$$
$$W^g_{13} = -g_1^2h_0 + 2g_0g_2h_0 + g_0g_1h_1$$
$$W^g_{14} = g_0$$
$$W^g_{21} = g_2^2h_1 - g_1g_2h_2 - g_0g_2h_3$$
$$W^g_{22} = g_2^2h_0 - g_0g_2h_2 + g_0^2h_4$$
$$W^g_{23} = -g_0g_2h_1 - g_0g_1h_2 + g_0^2h_3$$
$$W^g_{24} = -g_1$$
$$W^g_{31} = g_1g_2h_3 - g_1^2h_4 + 2g_0g_2h_4$$
$$W^g_{32} = g_0g_2h_3 - g_0g_1h_4$$
$$W^g_{33} = g_2^2h_0 + g_0g_2h_2 - g_0^2h_4$$
$$W^g_{34} = g_2$$
$$W^g_{41} = -g_0g_2^2h_1h_3 - g_0g_1g_2h_2h_3 + g_0g_1g_2h_1h_4 + g_0g_1^2h_2h_4 + g_0^2g_2h_3^2 - 4g_0^2g_2h_2h_4 - g_0^2g_1h_3h_4$$
$$W^g_{42} = g_1^2g_2h_0h_3 - g_1^3h_0h_4 - 2g_0g_2^2h_0h_3 - g_0g_1g_2h_1h_3 + 4g_0g_1g_2h_0h_4 + g_0g_1^2h_1h_4 - 2g_0^2g_2h_1h_4$$
$$W^g_{43} = -g_1g_2^2h_0h_1 + g_1^2g_2h_0h_2 + g_0g_2^2h_1^2 - 4g_0g_2^2h_0h_2 - g_0g_1g_2h_1h_2 + g_0g_1g_2h_0h_3 - g_0^2g_2h_1h_3$$
$$W^g_{44} = -g_2^2h_0 - g_0g_2h_2 - g_0^2h_4$$

Appendix B. Bilinear Forms on the Jacobian

The file www.maths.ox.ac.uk/~flynn/genus2/jac/bilforms contains the bilinear forms $\phi_{ij}(\mathbf{a},\mathbf{b})$ described in Theorem 3.2, satisfying $(\phi_{ij}(\mathbf{a},\mathbf{b})) = (k_i(\mathbf{a}-\mathbf{b})k_j(\mathbf{a}+\mathbf{b}))$. The terms of each form are arranged in paragraphs; the initial part (free of $f_0,\ldots,f_6$) is given first, and subsequent paragraphs are in order of increasing degree in $f_0,\ldots,f_6$.

Appendix C. The Duplication Law

Let $\mathbf{k} \in \mathcal{K}(\mathcal{C})$. Then the following are the quartic forms $\delta_i(\mathbf{k})$ described in Corollary 3.8, which satisfy $2\mathbf{k} = (\delta_1(\mathbf{k}),\delta_2(\mathbf{k}),\delta_3(\mathbf{k}),\delta_4(\mathbf{k}))$. These are in the file www.maths.ox.ac.uk/~flynn/genus2/kummer/dupl

$$\delta_1(\mathbf{k}) = 4k_1k_4^3 + 4k_4^2(k_1^2f_2 - k_2k_3f_5 - 3k_3^2f_6) + \ldots$$

25

26

REFERENCES

[1] Adleman, L. M. and Huang, M. A. *Recognising Primes in Random Polynomial Time.* Proceedings of the Nineteenth Annual Symposium on Theory of Computing (1987), Association for Computing Machinery, 462-469.

[2] Bost, J. B. and Mestre, J.-F. *Moyenne arithmético-géometrique et périodes des courbes de genre 1 et 2.* Gaz. Math. Soc. France, **38** (1988), 36-64.

[3] Cantor, D. G. *Computing in the Jacobian of a Hyperelliptic Curve.* Mathematics of Computation, **48** (1987), 95-101.

[4] Cantor, D. G. *On the Analogue of the Division Polynomials for Hyperelliptic Curves I.* (preprint, U.C.L.A., 1991).

[5] Cassels, J. W. S. *Diophantine Equations with Special Reference to Elliptic Curves.* J. London Math. Soc. **41** (1966), 193-291.

27

Makdisi's algorithms

- Fix $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ (where $n \gg_g 1$), and a divisor $D_0 \gg_g 0$. Let $V = \mathcal{L}(2D_0)$.

Makdisi's algorithms

- Fix $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ (where $n \gg_g 1$), and a divisor $D_0 \gg_g 0$. Let $V = \mathcal{L}(2D_0)$.

- A basis $v_1, v_2, \cdots$ of V can be represented by the matrix

$$\begin{pmatrix} v_1(P_1) & v_2(P_1) & \cdots \\ \vdots & \vdots & \\ v_1(P_n) & v_2(P_n) & \cdots \end{pmatrix}.$$

Makdisi's algorithms

- Fix $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ (where $n \gg_g 1$), and a divisor $D_0 \gg_g 0$. Let $V = \mathcal{L}(2D_0)$.

- A point $[D - D_0] \in J$ is represented by the subspace

$$W = \mathcal{L}(2D_0 - D) \subset V,$$

  i.e. by the matrix

$$\begin{pmatrix} w_1(P_1) & w_2(P_1) & \cdots \\ \vdots & \vdots & \\ w_1(P_n) & w_2(P_n) & \cdots \end{pmatrix},$$

  where $w_1, w_2, \cdots$ is a basis of W.

Group law

Let $a = [A - D_0]$, $b = [B - D_0] \in J$ represented by $\mathcal{L}(2D_0 - A)$, $\mathcal{L}(2D_0 - B)$.

Algorithm (Makdisi, 2004)

1. $\mathcal{L}(2D_0 - A) \otimes \mathcal{L}(2D_0 - B) \twoheadrightarrow \mathcal{L}(4D_0 - A - B)$.
2. $\mathcal{L}(3D_0 - A - B) = \{v \in \mathcal{L}(3D_0) \mid v\mathcal{L}(D_0) \subset \mathcal{L}(4D_0 - A - B)\}$
3. Take $f \in \mathcal{L}(3D_0 - A - B)$.
   Observation: $(f) = -3D_0 + A + B + C$
   $\rightsquigarrow c := [C - D_0] = -(a + b) \in J$.
4. $\mathcal{L}(2D_0 - C) = \{v \in V \mid v\mathcal{L}(3D_0 - A - B) \subset f\mathcal{L}(2D_0)\}$.

Approximate p-adic linear algebra

Theorem (Page + M., 2018)

Let $A \in M_{m,n}(\mathbb{Z}_q)$ such that $\mathrm{rk}_{\mathbb{Q}_q}(A) = \mathrm{rk}_{\mathbb{F}_q}(A \bmod p)$. (GR)
Fix $e \in \mathbb{N}$, and let H be the Howell normal form of the kernel of $(A \bmod p^e)$.
Then the elements of H that are nonzero mod p form a reduction mod p^e of a $\mathbb{Z}_q$-basis of $\ker(A)$, and are linearly independent mod p.

Example

Take $A = (p \;\; 1)$, $e = 2$. Then

$$H = \left\{ \begin{pmatrix} p \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ p \end{pmatrix} \right\}.$$

Membership test

Algorithm (Makdisi, 2004)

Let W be a matrix as above.

1. $w \leftarrow 1^{\text{st}}$ column of W
2. $W' \leftarrow \{v \in V \mid vW \subset wV\}$
3. $n \leftarrow \dim W'$
4. Return True if $n = \#W$, False if $n < \#W$.

Proof.

$W' = \mathcal{L}(2D_0 - D')$, where $(w) = -2D_0 + D + D'$ and D is the largest divisor such that $W \subset \mathcal{L}(2D_0 - D)$. □

Differentiation of linear algebra

Let ${}_rA_n$ have rank r.

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \left(\frac{{}_rA_n}{{}_{n-r}S_n} \right)$,

where $S = \texttt{supplement}(A)$ so that $\widetilde{A}$ is invertible

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \begin{pmatrix} {}_rA_n \\ \hline {}_{n-r}S_n \end{pmatrix}$,

where $S = \texttt{supplement}(A)$ so that $\widetilde{A}$ is invertible, and split $\widetilde{A}^{-1} = ({}_nL_r \mid {}_nK_{n-r})$.

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \left(\begin{array}{c} {}_rA_n \\ \hline {}_{n-r}S_n \end{array}\right)$,

where $S = \texttt{supplement}(A)$ so that $\widetilde{A}$ is invertible, and split $\widetilde{A}^{-1} = ({}_nL_r \mid {}_nK_{n-r})$. Then

$$I_n = \widetilde{A}\widetilde{A}^{-1} = \left(\begin{array}{c|c} {}_rAL_r & {}_rAK_{n-r} \\ \hline {}_{n-r}SL_r & {}_{n-r}SK_{n-r} \end{array}\right)$$

so $K \stackrel{\text{def}}{=} \text{Ker}(A)$.

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \left(\begin{array}{c} {}_rA_n \\ \hline {}_{n-r}S_n \end{array}\right)$,

where $S = \texttt{supplement}(A)$ so that $\widetilde{A}$ is invertible, and split $\widetilde{A}^{-1} = ({}_nL_r \mid {}_nK_{n-r})$. Then

$$I_n = \widetilde{A}\widetilde{A}^{-1} = \left(\begin{array}{c|c} {}_rAL_r & {}_rAK_{n-r} \\ \hline {}_{n-r}SL_r & {}_{n-r}SK_{n-r} \end{array}\right)$$

so $K \overset{\text{def}}{=} \text{Ker}(A)$.

For ${}_rH_n$ with coefficients in $p^e\mathbb{Z}_q$, $\widetilde{A+H} = \widetilde{A} + \left(\begin{array}{c} H \\ \hline 0 \end{array}\right)$, so

$$\widetilde{A+H}^{-1} = \widetilde{A}^{-1} - \widetilde{A}^{-1}\left(\begin{array}{c} H \\ \hline 0 \end{array}\right)\widetilde{A}^{-1} + O(p^{2e})$$

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \left(\begin{array}{c} {}_rA_n \\ \hline {}_{n-r}S_n \end{array}\right)$,

where $S = \texttt{supplement}(A)$ so that $\widetilde{A}$ is invertible, and split $\widetilde{A}^{-1} = ({}_nL_r \mid {}_nK_{n-r})$. Then

$$I_n = \widetilde{A}\widetilde{A}^{-1} = \left(\begin{array}{c|c} {}_rAL_r & {}_rAK_{n-r} \\ \hline {}_{n-r}SL_r & {}_{n-r}SK_{n-r} \end{array}\right)$$

so $K \overset{\text{def}}{=} \operatorname{Ker}(A)$.

For ${}_rH_n$ with coefficients in $p^e\mathbb{Z}_q$, $\widetilde{A+H} = \widetilde{A} + \left(\begin{array}{c} H \\ \hline 0 \end{array}\right)$, so

$$\widetilde{A+H}^{-1} = \widetilde{A}^{-1} - \widetilde{A}^{-1}\left(\begin{array}{c} H \\ \hline 0 \end{array}\right)\widetilde{A}^{-1} + O(p^{2e})$$

$$\rightsquigarrow \operatorname{Ker}(A+H) = \operatorname{Ker}(A) - LH\operatorname{Ker}(A) + O(p^{2e}).$$

Differentiation of linear algebra

$$\rightsquigarrow \mathrm{Ker}(A+H) = \mathrm{Ker}(A) - LH\,\mathrm{Ker}(A) + O(p^{2e}).$$

Let ${}_rP_r$ have rank r. Then

$$\left(\begin{array}{c|c} {}_rP_r & {}_rQ_n \\ \hline {}_mR_r & {}_mS_n \end{array}\right) \text{ has rank } r \iff S - RP^{-1}Q = 0.$$

Example: A modular Galois representation

Let

$$f = q + (\zeta_3 - 1)q^2 + (-2\zeta_3 - 2)q^3 + \cdots \in \mathcal{S}_2\big(\Gamma_1(13)\big)$$

be the newform of weight 2 and level 13.

Let

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_7)$$

be the representation attached to f mod the prime above $\ell = 7$ such that $\zeta_3 \equiv 2$.

We know that ρ occurs in the 7-torsion of the Jacobian of

$$C := X_1(13) : y^2 + (x^3 + x + 1)y = x^5 + x^4.$$

Take $p = 17$: the charpoly. of $\rho(\mathrm{Frob}_{17})$ is $x^2 - x - 2 \in \mathbb{F}_7[x]$.

Representations from higher étale cohomology

So we can compute $\rho \subset \mathrm{H}^1_{\text{ét}}(\mathrm{Curve}, \mathbb{Z}/\ell\mathbb{Z})$.

Representations from higher étale cohomology

So we can compute $\rho \subset \mathrm{H}^1_{\text{ét}}(\text{Curve}, \mathbb{Z}/\ell\mathbb{Z})$.

What if $\rho \subset \mathrm{H}^2_{\text{ét}}(\text{Surface}, \mathbb{Z}/\ell\mathbb{Z})$?

Representations from higher étale cohomology

So we can compute $\rho \subset \mathrm{H}^1_{\text{ét}}(\text{Curve}, \mathbb{Z}/\ell\mathbb{Z})$.

What if $\rho \subset \mathrm{H}^2_{\text{ét}}(\text{Surface}, \mathbb{Z}/\ell\mathbb{Z})$?

Solution: *dévissage* by Leray's spectral sequence

$$\text{“}\mathrm{H}^p(\mathrm{H}^q) \Rightarrow \mathrm{H}^{p+q}\text{”}.$$

Representations from higher étale cohomology

So we can compute $\rho \subset \mathrm{H}^1_{\text{ét}}(\text{Curve}, \mathbb{Z}/\ell\mathbb{Z})$.

What if $\rho \subset \mathrm{H}^2_{\text{ét}}(\text{Surface}, \mathbb{Z}/\ell\mathbb{Z})$?

Solution: *dévissage* by Leray's spectral sequence

$$\text{“}\mathrm{H}^p(\mathrm{H}^q) \Rightarrow \mathrm{H}^{p+q}\text{”}.$$

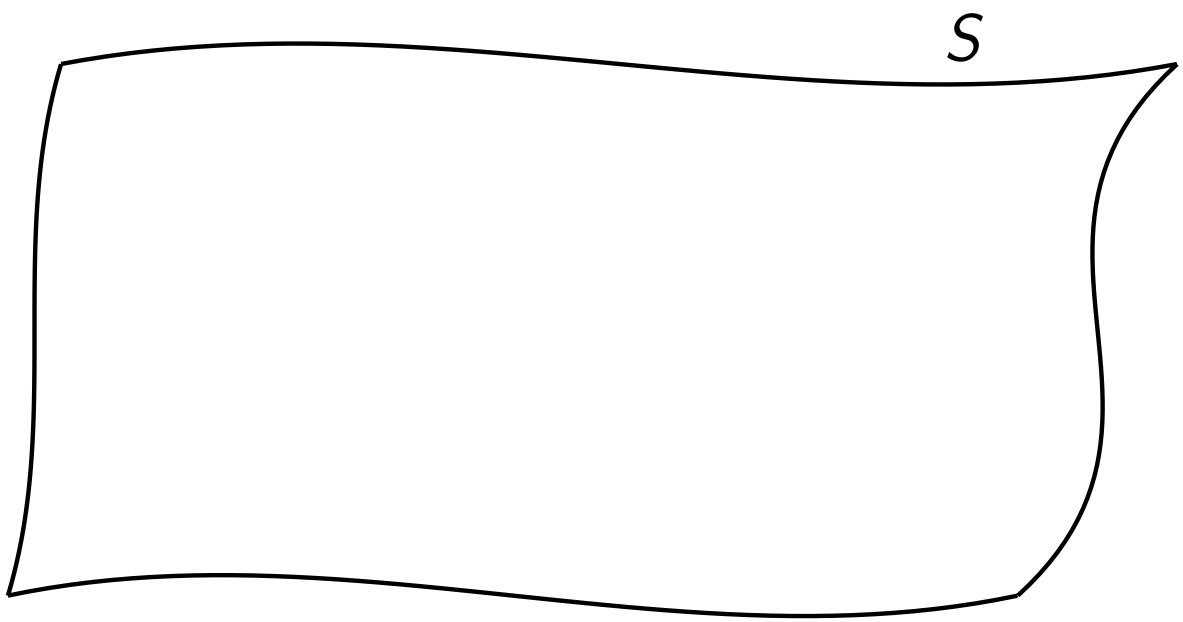
Theorem (M., 2019)

Let $S/\mathbb{Q}$ be a regular surface. For every $\rho \subset \mathrm{H}^2_{\text{ét}}(S, \mathbb{Z}/\ell\mathbb{Z})$, one can construct a curve $C/\mathbb{Q}$ such that $\rho \subset \mathrm{Jac}(C)[\ell]$ (up to twist by the cyclotomic character).

Representations from higher étale cohomology

Theorem (M., 2019)

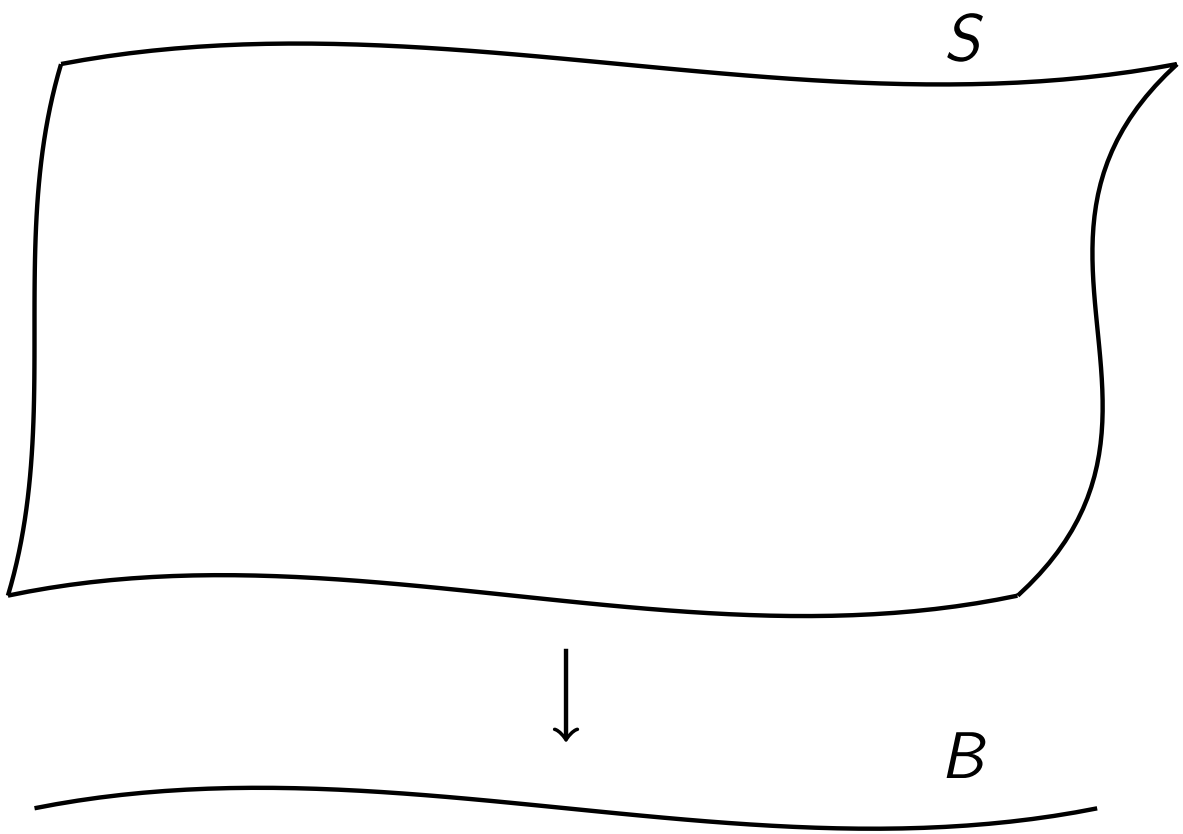
Let $S/\mathbb{Q}$ be a regular surface. For every $\rho \subset \mathrm{H}^2_{\text{ét}}(S, \mathbb{Z}/\ell\mathbb{Z})$, one can construct a curve $C/\mathbb{Q}$ such that $\rho \subset \mathrm{Jac}(C)[\ell]$.



Representations from higher étale cohomology

Theorem (M., 2019)

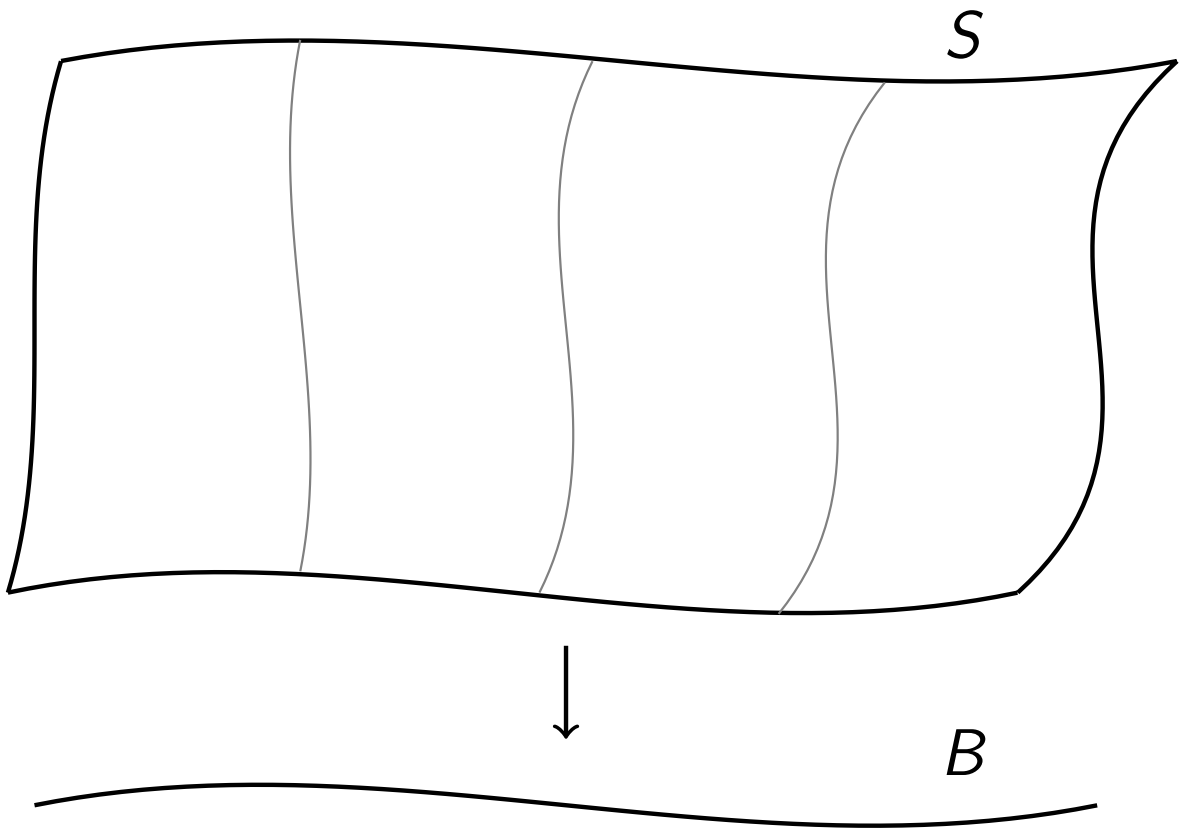
Let $S/\mathbb{Q}$ be a regular surface. For every $\rho \subset \mathrm{H}^2_{\text{ét}}(S, \mathbb{Z}/\ell\mathbb{Z})$, one can construct a curve $C/\mathbb{Q}$ such that $\rho \subset \mathrm{Jac}(C)[\ell]$.



Representations from higher étale cohomology

Theorem (M., 2019)

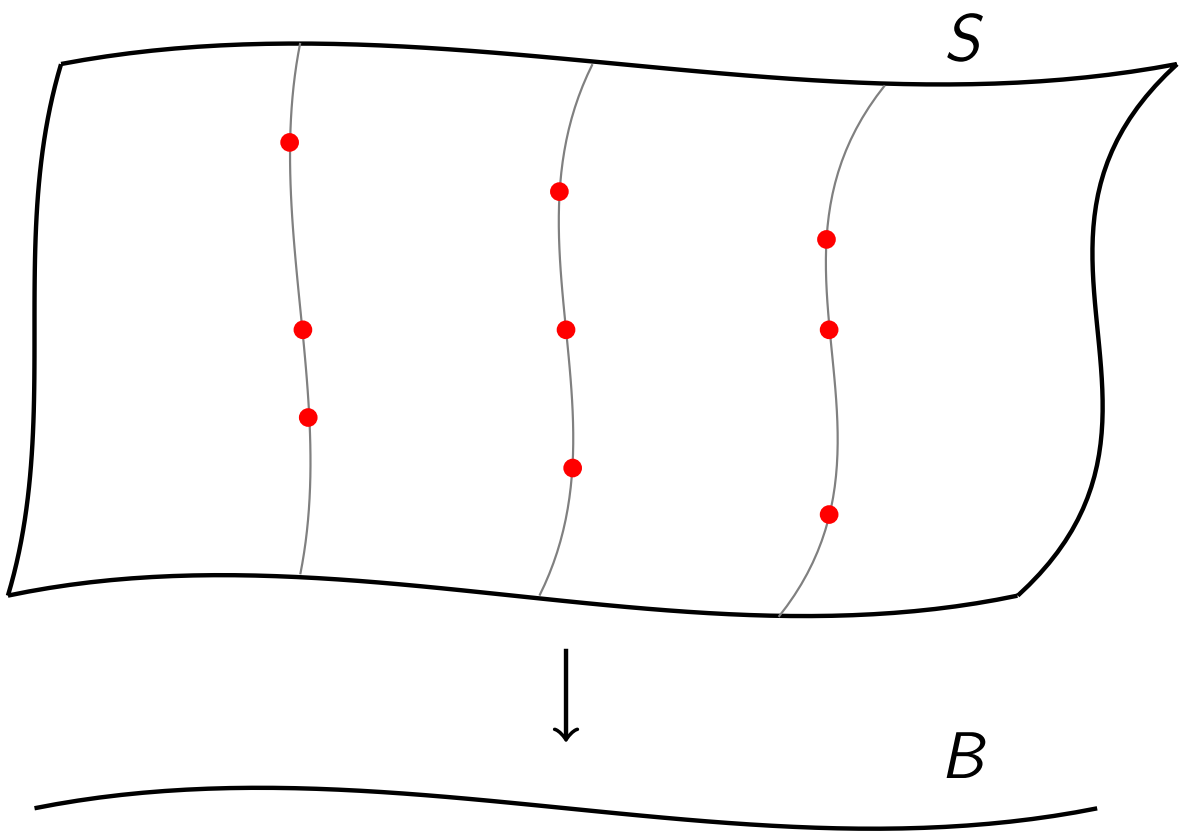
Let $S/\mathbb{Q}$ be a regular surface. For every $\rho \subset \mathrm{H}^2_{\text{ét}}(S, \mathbb{Z}/\ell\mathbb{Z})$, one can construct a curve $C/\mathbb{Q}$ such that $\rho \subset \mathrm{Jac}(C)[\ell]$.



Representations from higher étale cohomology

Theorem (M., 2019)

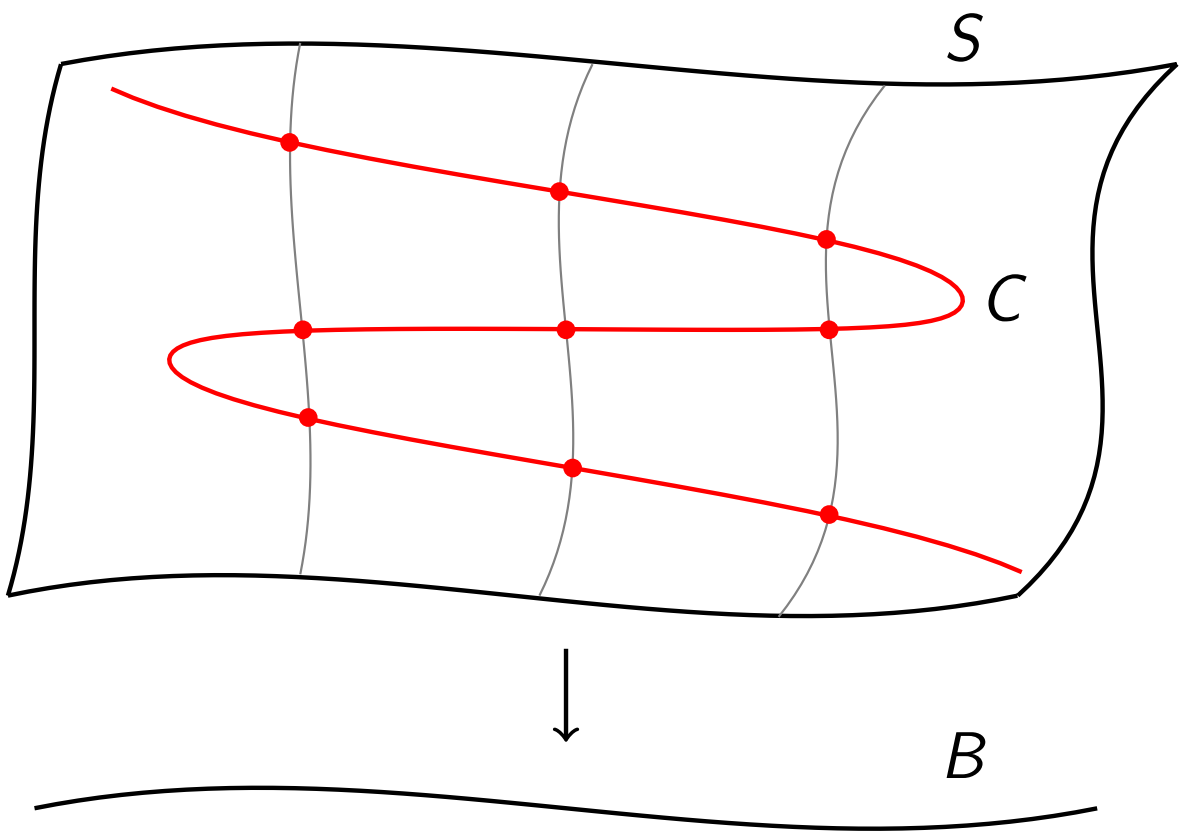
Let $S/\mathbb{Q}$ be a regular surface. For every $\rho \subset \mathrm{H}^2_{\text{ét}}(S, \mathbb{Z}/\ell\mathbb{Z})$, one can construct a curve $C/\mathbb{Q}$ such that $\rho \subset \mathrm{Jac}(C)[\ell]$.



Representations from higher étale cohomology

Theorem (M., 2019)

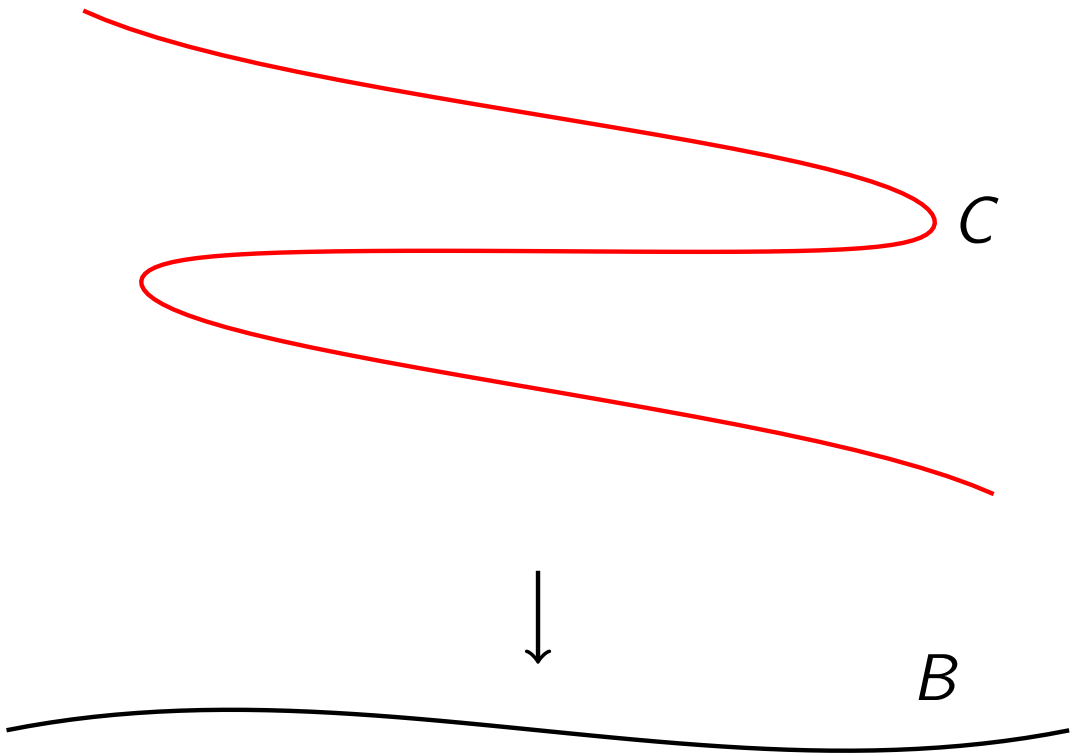
Let $S/\mathbb{Q}$ be a regular surface. For every $\rho \subset \mathrm{H}^2_{\text{ét}}(S, \mathbb{Z}/\ell\mathbb{Z})$, one can construct a curve $C/\mathbb{Q}$ such that $\rho \subset \mathrm{Jac}(C)[\ell]$.



Representations from higher étale cohomology

Theorem (M., 2019)

Let $S/\mathbb{Q}$ be a regular surface. For every $\rho \subset \mathrm{H}^2_{\text{ét}}(S, \mathbb{Z}/\ell\mathbb{Z})$, one can construct a curve $C/\mathbb{Q}$ such that $\rho \subset \mathrm{Jac}(C)[\ell]$.



Application (1/4): An eigenform/ SL(3)

Let S be the minimal regular model of the surface / $\mathbb{Q}$

$$y^2 = xz(x^2 - 1)(z^2 - 1)(x^2 - 2xz - z^2).$$

Application (1/4): An eigenform / SL(3)

Let S be the minimal regular model of the surface / $\mathbb{Q}$

$$y^2 = xz(x^2 - 1)(z^2 - 1)(x^2 - 2xz - z^2).$$

Van Geemen & Top observed that there exists an eigenform u of level 2^7 over SL(3) such that $\forall \ell \in \mathbb{N}$, a twist of

$$\widetilde{\rho}_{u,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3\big(\mathbb{Q}_\ell(\sqrt{-1})\big)$$

is contained in $\mathrm{H}^2_{\text{ét}}(S, \mathbb{Q}_\ell)$.

For $p \notin \{2, \ell\}$, the characteristic polynomial of $\widetilde{\rho}_{u,\ell}$ is

$$x^3 - a_p x^2 + p\overline{a_p} x - p^3\chi(p)$$

for some $\chi : (\mathbb{Z}/2^3\mathbb{Z})^\times \longrightarrow \mathbb{Q}(\sqrt{-1})^\times$, where $a_p \in \mathbb{Z}[2\sqrt{-1}]$.

Application (2/4): Geometry

The fibres of

$$\begin{array}{rccc} \pi & : & S & \longrightarrow & \mathbb{P}^1_t \\ & & (x,y,z) & \longmapsto & t = x/z \end{array}$$

are elliptic curves:

$$y^2 = (t^3 - 2t^2 - t)(x - 2t)(x + 2t)(x + t^2 + 1)$$

Application (2/4): Geometry

The fibres of

$$\begin{array}{rccc} \pi & : & S & \longrightarrow & \mathbb{P}^1_t \\ & & (x,y,z) & \longmapsto & t = x/z \end{array}$$

are elliptic curves:

$$y^2 = (t^3 - 2t^2 - t)(x - 2t)(x + 2t)(x + t^2 + 1)$$

$\rightsquigarrow$ for each ℓ, we can find a curve $C_\ell \,/\, \mathbb{Q}$ whose Jacobian contains

$$\rho_{u,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3\big(\mathbb{F}_\ell(\sqrt{-1})\big).$$

Application (2/4): Geometry

The fibres of

$$\begin{array}{rccc} \pi \ : & S & \longrightarrow & \mathbb{P}^1_t \\ & (x,y,z) & \longmapsto & t = x/z \end{array}$$

are elliptic curves:

$$y^2 = (t^3 - 2t^2 - t)(x - 2t)(x + 2t)(x + t^2 + 1)$$

$\rightsquigarrow$ for each ℓ, we can find a curve $C_\ell \ / \ \mathbb{Q}$ whose Jacobian contains

$$\rho_{u,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3\big(\mathbb{F}_\ell(\sqrt{-1})\big).$$

Remark: $\mathrm{genus}(C_\ell) = \frac{3\ell^2 - 6\ell + 5}{2}$.

Application (2/4): Geometry

$\rightsquigarrow$ for each ℓ, we can find a curve C_ℓ / $\mathbb{Q}$ whose Jacobian contains

$$\rho_{u,\ell} : \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathsf{GL}_3\big(\mathbb{F}_\ell(\sqrt{-1})\big).$$

Remark: $\mathsf{genus}(C_\ell) = \frac{3\ell^2-6\ell+5}{2}$.

For $\ell = 3$, C_3 has genus $g = 7$:

Application (2/4): Geometry

$\rightsquigarrow$ for each ℓ, we can find a curve C_ℓ / $\mathbb{Q}$ whose Jacobian contains

$$\rho_{u,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3\big(\mathbb{F}_\ell(\sqrt{-1})\big).$$

Remark: $\mathrm{genus}(C_\ell) = \frac{3\ell^2-6\ell+5}{2}$.

For $\ell = 3$, C_3 has genus $g = 7$:

$$\begin{aligned}
&-256t^{56}+6144t^{55}-62464t^{54}+333824t^{53}-859648t^{52}-120832t^{51}+7252992t^{50}-16046080t^{49}-9891072t^{48}+90136576t^{47}\\
&-73076736t^{46}-237805568t^{45}+420485120t^{44}+341843968t^{43}-1165840384t^{42}-192667648t^{41}+2178936320t^{40}-238563328t^{39}\\
&-3063240704t^{38}+639488000t^{37}+3412593664t^{36}-639488000t^{35}-3063240704t^{34}+238563328t^{33}+2178936320t^{32}+192667648t^{31}\\
&-1165840384t^{30}-341843968t^{29}+(-288y^4+420485120)t^{28}+(3456y^4+237805568)t^{27}+(-14400y^4-73076736)t^{26}\\
&+(14976y^4-90136576)t^{25}+(56160y^4-9891072)t^{24}+(-142848y^4+16046080)t^{23}+(-52992y^4+7252992)t^{22}+(400896y^4+120832)t^{21}\\
&+(-55872y^4-859648)t^{20}+(-624384y^4-333824)t^{19}+(134784y^4-62464)t^{18}+(624384y^4-6144)t^{17}+(-55872y^4-256)t^{16}\\
&+(16y^6-400896y^4)t^{15}+(-96y^6-52992y^4)t^{14}+(-384y^6+142848y^4)t^{13}+(3232y^6+56160y^4)t^{12}+(-5424y^6-14976y^4)t^{11}\\
&+(960y^6-14400y^4)t^{10}-3456y^4t^9+(960y^6-288y^4)t^8+5424y^6t^7+3232y^6t^6+384y^6t^5-96y^6t^4-16y^6t^3+27y^8 = 0.
\end{aligned}$$

Application (2/4): Geometry

$\rightsquigarrow$ for each ℓ, we can find a curve C_ℓ / $\mathbb{Q}$ whose Jacobian contains

$$\rho_{u,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3\big(\mathbb{F}_\ell(\sqrt{-1})\big).$$

Remark: $\mathrm{genus}(C_\ell) = \frac{3\ell^2-6\ell+5}{2}$.

For $\ell = 3$, C_3 has genus $g = 7$:

$$(3Y^5-6Y^3+3Y)X^4+(2Y^8-8Y^7+4Y^6+12Y^5+12Y^3-4Y^2-8Y-2)X^2$$
$$+(9Y^9-36Y^8-36Y^7+36Y^6+18Y^5-36Y^4-36Y^3+36Y^2+9Y) = 0.$$

Application (3/4): Computation

Pick a prime $p \notin \{2, 3\}$, and compute the representation afforded by the piece $T \subset \mathrm{Jac}(C_3)[3]$ where Frob_p acts with charpoly

$$x^3 - a_p x^2 + p\overline{a_p} x - p^3 \chi(p) \in \mathbb{F}_3(\sqrt{-1})[x].$$

Application (3/4): Computation

Pick a prime $p \notin \{2, 3\}$, and compute the representation afforded by the piece $T \subset \mathrm{Jac}(C_3)[3]$ where Frob_p acts with charpoly

$$\mathrm{Norm}_{\mathbb{F}_3(\sqrt{-1})[x]/\mathbb{F}_3[x]} \left(x^3 - a_p x^2 + p\overline{a_p} x - p^3 \chi(p)\right) \in \mathbb{F}_3[x].$$

Application (3/4): Computation

Pick a prime $p \notin \{2, 3\}$, and compute the representation afforded by the piece $T \subset \mathrm{Jac}(C_3)[3]$ where Frob_p acts with charpoly

$$\mathrm{Norm}_{\mathbb{F}_3(\sqrt{-1})[x]/\mathbb{F}_3[x]} \left(x^3 - a_p x^2 + p\overline{a_p} x - p^3\chi(p)\right) \in \mathbb{F}_3[x].$$

We find that the twist of

$$\rho_{u,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3(\mathbb{F}_9)$$

by $\left(\frac{6}{\cdot}\right)$ cuts off the splitting field of

$$x^{28} - 12x^{27} + 60x^{26} - 132x^{25} - 30x^{24} + 624x^{23} + 420x^{22} - 7704x^{21} + 17118x^{20} - 9504x^{19} - 14424x^{18}$$
$$+ 10824x^{17} + 36492x^{16} - 64992x^{15} + 19488x^{14} + 56064x^{13} - 89604x^{12} + 109296x^{11} - 88368x^{10}$$
$$- 11472x^9 + 58488x^8 - 130176x^7 + 34224x^6 - 58272x^5 - 39960x^4 + 32256x^3 + 24480x^2 - 352x - 1776$$

Application (3/4): Computation

Pick a prime $p \notin \{2, 3\}$, and compute the representation afforded by the piece $T \subset \mathrm{Jac}(C_3)[3]$ where Frob_p acts with charpoly

$$\mathrm{Norm}_{\mathbb{F}_3(\sqrt{-1})[x]/\mathbb{F}_3[x]} \left(x^3 - a_p x^2 + p\overline{a_p} x - p^3\chi(p)\right) \in \mathbb{F}_3[x].$$

We find that the twist of

$$\rho_{u,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3(\mathbb{F}_9)$$

by $\left(\frac{6}{\cdot}\right)$ cuts off the splitting field of

$$x^{28} - 12x^{27} + 60x^{26} - 132x^{25} - 30x^{24} + 624x^{23} + 420x^{22} - 7704x^{21} + 17118x^{20} - 9504x^{19} - 14424x^{18}$$
$$+ 10824x^{17} + 36492x^{16} - 64992x^{15} + 19488x^{14} + 56064x^{13} - 89604x^{12} + 109296x^{11} - 88368x^{10}$$
$$- 11472x^9 + 58488x^8 - 130176x^7 + 34224x^6 - 58272x^5 - 39960x^4 + 32256x^3 + 24480x^2 - 352x - 1776$$

and has thus image $\mathrm{SU}_3(\mathbb{F}_9)$.

Application (4/4): Image of Frobenius elements

p	$\rho_{u,3}(\mathrm{Frob}_p)$	$a_p(u) \bmod 3\mathbb{Z}[i]$
$10^{1000}+453$	$+\begin{pmatrix} 1 & 0 & 0 \\ 0 & i-1 & i-1 \\ 0 & i+1 & -i-1 \end{pmatrix}$	-1
$10^{1000}+1357$	$-\begin{pmatrix} 0 & 0 & i \\ 0 & i & 0 \\ 1 & 0 & 0 \end{pmatrix}$	$-i$
$10^{1000}+2713$	$-\begin{pmatrix} 0 & 0 & -i \\ 0 & -i & 0 \\ 1 & 0 & 0 \end{pmatrix}$	i
$10^{1000}+4351$	$-\begin{pmatrix} 0 & i+1 & -i-1 \\ 0 & -i+1 & -i+1 \\ 1 & 0 & 0 \end{pmatrix}$	$i-1$
$10^{1000}+5733$	$+\begin{pmatrix} 0 & i+1 & -i+1 \\ 0 & -i-1 & -i+1 \\ 1 & 0 & 0 \end{pmatrix}$	$-i-1$

Any questions ?

Thank you !