Modular Galois representations p-adically using Makdisi's moduli-friendly forms

Nicolas Mascot

Trinity College Dublin

LFANT seminar
IMB
September 22nd 2020

Goal: Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(N), \varepsilon\big)$, $k \geqslant 2$, be a newform with coefficient field $K_f = \mathbb{Q}(a_n, n \geqslant 2)$.

Pick a prime $\mathfrak{l}$ of K_f above some $\ell \in \mathbb{N}$.

Goal: Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(N), \varepsilon\big)$, $k \geqslant 2$, be a newform with coefficient field $K_f = \mathbb{Q}(a_n, n \geqslant 2)$.

Pick a prime $\mathfrak{l}$ of K_f above some $\ell \in \mathbb{N}$.

Theorem (Deligne, Serre)

There exists a Galois representation

$$\rho_{f,\mathfrak{l}} \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}}),$$

which is unramified outside ℓN, and such that the image of any Frobenius element at $p \nmid \ell N$ has characteristic polynomial

$$x^2 - a_p x + \varepsilon(p) p^{k-1} \in \mathbb{F}_{\mathfrak{l}}[x].$$

Goal: Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(N), \varepsilon\big)$, $k \geqslant 2$, be a newform with coefficient field $K_f = \mathbb{Q}(a_n, n \geqslant 2)$.

Pick a prime $\mathfrak{l}$ of K_f above some $\ell \in \mathbb{N}$.

Theorem (Deligne, Serre)

There exists a Galois representation

$$\rho_{f,\mathfrak{l}} \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}}),$$

which is unramified outside ℓN, and such that the image of any Frobenius element at $p \nmid \ell N$ has characteristic polynomial

$$x^2 - a_p x + \varepsilon(p) p^{k-1} \in \mathbb{F}_{\mathfrak{l}}[x].$$

Goal : compute $\rho_{f,\mathfrak{l}}$.

Modular Galois representations in Jacobians

Under reasonable hypotheses, $\rho_{f,\mathfrak{l}}$ is afforded by a Galois-stable piece $T \subseteq J[\ell]$, where J is the Jacobian of the modular curve $X_1(N')$,

$$N' = \begin{cases} N & \text{if } k = 2, \\ \ell N & \text{if } k > 2. \end{cases}$$

More general case

Suppose we know a "nice" curve $C/\mathbb{Q}$ such that some Galois-stable $\mathbb{F}_\ell$-subspace $T \subseteq J[\ell]$ affords some interesting Galois representation ρ, where $J = \operatorname{Jac}(C)$.

More general case

Suppose we know a "nice" curve $C/\mathbb{Q}$ such that some Galois-stable $\mathbb{F}_\ell$-subspace $T \subseteq J[\ell]$ affords some interesting Galois representation ρ, where $J = \operatorname{Jac}(C)$.

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

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

and

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

and that

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

A p-adic 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 this basis 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. $F(x) = \prod_{t \in T} \left(x - \theta(t)\right)$, where $\theta : J \dashrightarrow \mathbb{A}^1$,
6. Identify $F(x) \in \mathbb{Q}[x]$.

Getting a basis of T

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

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

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

Getting a basis of T

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

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

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

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

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

Reminder: line bundles

Let $\mathcal{O}_C$ = regular functions on C.

Definition

A line bundle on C is a locally free $\mathcal{O}_C$-module.

Reminder: line bundles

Let $\mathcal{O}_C =$ regular functions on C.

Definition

A line bundle on C is a locally free $\mathcal{O}_C$-module.

Example 1

Differential forms: for all $P \in C$, there exists ω such that the other differential forms are of the form $f\omega$ near P for some function f on C which is regular near P.

Reminder: line bundles

Let $\mathcal{O}_C$ = regular functions on C.

Definition

A line bundle on C is a locally free $\mathcal{O}_C$-module.

Example 1

Differential forms: for all $P \in C$, there exists ω such that the other differential forms are of the form $f\omega$ near P for some function f on C which is regular near P.

Example 2

If C is a modular curve, then for all $k \in \mathbb{N}$, modular forms of weight k form a line bundle over C.

Makdisi's algorithms

- Fix a line bundle $\mathcal{L}$ on C of degree $d_0 \gg_g 1$, and $n \gg_{d_0} 1$ points $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ along with local trivialisations of $\mathcal{L}$ at the P_i.

Makdisi's algorithms

- Fix a line bundle $\mathcal{L}$ on C of degree $d_0 \gg_g 1$, and $n \gg_{d_0} 1$ points $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ along with local trivialisations of $\mathcal{L}$ at the P_i.
- A basis $v_1, v_2, \cdots$ of the global section space $H^0(\mathcal{L})$ can be represented by the matrix

$$\begin{pmatrix} s_1(P_1) & s_2(P_1) & \cdots \\ \vdots & \vdots & \\ s_1(P_n) & s_2(P_n) & \cdots \end{pmatrix}.$$

Makdisi's algorithms

- Fix a line bundle $\mathcal{L}$ on C of degree $d_0 \gg_g 1$, and $n \gg_{d_0} 1$ points $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ along with local trivialisations of $\mathcal{L}$ at the P_i.

- A basis $v_1, v_2, \cdots$ of the global section space $H^0(\mathcal{L})$ can be represented by the matrix

$$\begin{pmatrix} s_1(P_1) & s_2(P_1) & \cdots \\ \vdots & \vdots & \\ s_1(P_n) & s_2(P_n) & \cdots \end{pmatrix}.$$

We can deduce a matrix representing $H^0(\mathcal{L}^{\otimes 2})$, because Riemann-Roch & our assumptions ensure that the multiplication map

$$H^0(\mathcal{L}) \otimes H^0(\mathcal{L}) \longmapsto H^0(\mathcal{L}^{\otimes 2})$$

is surjective.

Makdisi's algorithms

- Fix a line bundle $\mathcal{L}$ on C of degree $d_0 \gg_g 1$, and $n \gg_{d_0} 1$ points $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ along with local trivialisations of $\mathcal{L}$ at the P_i.

- A point $[D] - [\mathcal{L}] \in J$ is represented by the subspace

$$W = H^0\big(\mathcal{L}^{\otimes 2}(-D)\big) \subset H^0\big(\mathcal{L}^{\otimes 2}\big),$$

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 $a = [A] - [\mathcal{L}]$, $b = [B] - [\mathcal{L}] \in J$ represented by $H^0\big(\mathcal{L}^{\otimes 2}(-A)\big)$, $H^0\big(\mathcal{L}^{\otimes 2}(-B)\big)$.

Algorithm (Makdisi, 2004)

1. $H^0\big(\mathcal{L}^{\otimes 2}(-A)\big) \otimes H^0\big(\mathcal{L}^{\otimes 2}(-B)\big) \twoheadrightarrow H^0\big(\mathcal{L}^{\otimes 4}(-A-B)\big)$.
2. $H^0\big(\mathcal{L}^{\otimes 3}(-A-B)\big)$
   $= \big\{ s \in H^0\big(\mathcal{L}^{\otimes 3}\big) \mid s \cdot H^0\big(\mathcal{L}\big) \subset H^0\big(\mathcal{L}^{\otimes 4}(-A-B)\big) \big\}$
3. Take $f \in H^0\big(\mathcal{L}^{\otimes 3}(-A-B)\big)$.
   Observation: given any section s of $\mathcal{L}^{\otimes 3}$, f/s is a function whose divisor is $A + B + C - 3[\mathcal{L}]$
   $\rightsquigarrow c := [C] - [\mathcal{L}] = [A] + [B] - 2[\mathcal{L}] = -(a+b) \in J$.
4. $H^0\big(\mathcal{L}^{\otimes 2}(-C)\big)$
   $= \big\{ s \in H^0\big(\mathcal{L}^{\otimes 2}\big) \mid s \cdot H^0\big(\mathcal{L}^{\otimes 3}(-A-B)\big) \subset f \cdot H^0\big(\mathcal{L}^{\otimes 2}\big) \big\}$

Modular curves

$$\begin{array}{cc}
\text{Curves} & \text{Points} \\
& \text{Pairs } (E, \alpha) \\
X(N) & \text{where } \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq E[N] \\
\Big\downarrow & \text{and } e_N(\alpha(1,0), \alpha(0,1)) = \zeta_N \\
& \text{Pairs } (E, P) \\
X_1(N) & \text{where } P \in E \\
\Big\downarrow & \text{has exact order } N \\
X(1) & \text{Elliptic curves } E
\end{array}$$

where ζ_N is a fixed primitive N-th root of 1.

Makdisi for $X(N)$

Need line bundle $\mathcal{L}$:
Pick $\mathcal{L}$ whose sections are modular forms of weight 2.

Need points $P_1, \cdots, P_n$ to evaluate forms at:
Fix (E, α), take the

$$(E, \alpha \circ \gamma)$$

for $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$.

Still need to "evaluate" a basis of the pace of forms of weight 2 at the P_i...

Algebraic modular forms

Let $k \in \mathbb{N}$, and R a commutative ring such that $6N \in R^\times$.

Algebraic modular forms

Let $k \in \mathbb{N}$, and R a commutative ring such that $6N \in R^\times$.

Definition

An <u>algebraic modular form</u> of weight k for $X(N)$ over R is a rule f assigning a value to isomorphism classes of triples $(E/R, \alpha, \omega)$ where ω generates the differential forms on E/R

Algebraic modular forms

Let $k \in \mathbb{N}$, and R a commutative ring such that $6N \in R^\times$.

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to isomorphism classes of triples $(E/R, \alpha, \omega)$ where ω generates the differential forms on E/R, and such that

$$f(E, \alpha, u\omega) = u^{-k} f(E, \alpha, \omega)$$

for all $u \in R^\times$.

Algebraic modular forms

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to triples $(E/R, \alpha, \omega)$, such that

$$f(E, \alpha, u\omega) = u^{-k} f(E, \alpha, \omega)$$

for all $u \in R^\times$.

Algebraic modular forms

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to triples $(E/R, \alpha, \omega)$, such that

$$f(E, \alpha, u\omega) = u^{-k} f(E, \alpha, \omega)$$

for all $u \in R^\times$.

Short Weierstrass

$$(\mathcal{E}) \ : \ y^2 = x^3 + Ax + B$$

$$\rightsquigarrow \omega = dx/2y.$$

Algebraic modular forms

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to triples $(E/R, \alpha, \omega)$, such that

$$f(E, \alpha, u\omega) = u^{-k} f(E, \alpha, \omega)$$

for all $u \in R^\times$.

Short Weierstrass

$$(\mathcal{E}) \ : \ y^2 = x^3 + Ax + B$$

$$\rightsquigarrow \omega = dx/2y.$$

Isomorphic to

$$(\mathcal{E}') \ : \ y^2 = x^3 + A'x + B'$$

by $(x, y) \mapsto (u^2 x, u^3 y)$, $A' = u^4 A$, $B' = u^6 B$, $\omega' = u^{-1}\omega$.

Algebraic modular forms

Definition

An algebraic modular form of weight k for $X(N)$ over R is a rule f assigning a value to pairs $(\mathcal{E}/R, \alpha)$, such that

$$f(\mathcal{E}', \alpha) = u^k f(\mathcal{E}, \alpha)$$

for all $u \in R^\times$.

Short Weierstrass

$$(\mathcal{E}) \ : \ y^2 = x^3 + Ax + B$$

$$\rightsquigarrow \omega = dx/2y.$$

Isomorphic to

$$(\mathcal{E}') \ : \ y^2 = x^3 + A'x + B'$$

by $(x, y) \mapsto (u^2 x, u^3 y)$, $A' = u^4 A$, $B' = u^6 B$, $\omega' = u^{-1}\omega$.

Algebraic modular forms

Definition

An <u>algebraic modular form</u> of weight k for $X(N)$ over R is a rule f assigning a value to pairs $(\mathcal{E}/R, \alpha)$, such that

$$f(\mathcal{E}', \alpha) = u^k f(\mathcal{E}, \alpha)$$

for all $u \in R^\times$.

Examples

$\mathcal{E} \mapsto A$ is a modular form of weight 4.

$\mathcal{E} \mapsto \Delta := -64A^3 - 432B^2$ is a modular form of weight 12.

by $(x, y) \mapsto (u^2 x, u^3 y)$, $A' = u^4 A$, $B' = u^6 B$, $\omega' = u^{-1}\omega$.

Makdisi's moduli-friendly forms

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq \mathcal{E}[N]$$

For $v, w \in (\mathbb{Z}/N\mathbb{Z})^2$ such that $v, w, v+w$ are all nonzero, let

$$\lambda_{v,w} : (\mathcal{E}, \alpha) \longmapsto \text{slope of line joining } \alpha(v) \text{ to } \alpha(w).$$

Makdisi's moduli-friendly forms

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq \mathcal{E}[N]$$

For $v, w \in (\mathbb{Z}/N\mathbb{Z})^2$ such that $v, w, v+w$ are all nonzero, let

$$\lambda_{v,w} : (\mathcal{E}, \alpha) \longmapsto \text{slope of line joining } \alpha(v) \text{ to } \alpha(w).$$

Theorem (Makdisi, 2011)

1. *$\lambda_{v,w}$ is a modular form of weight 1 for $X(N)$.*

Makdisi's moduli-friendly forms

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq \mathcal{E}[N]$$

For $v, w \in (\mathbb{Z}/N\mathbb{Z})^2$ such that $v, w, v+w$ are all nonzero, let

$$\lambda_{v,w} : (\mathcal{E}, \alpha) \longmapsto \text{slope of line joining } \alpha(v) \text{ to } \alpha(w).$$

Theorem (Makdisi, 2011)

1. *$\lambda_{v,w}$ is a modular form of weight 1 for $X(N)$.*
2. *The R-algebra generated by the $\lambda_{v,w}$ contains all modular forms for $X(N)$, except cuspforms of weight 1.*

Makdisi's moduli-friendly forms

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \simeq \mathcal{E}[N]$$

For $v, w \in (\mathbb{Z}/N\mathbb{Z})^2$ such that $v, w, v+w$ are all nonzero, let

$$\lambda_{v,w} : (\mathcal{E}, \alpha) \longmapsto \text{slope of line joining } \alpha(v) \text{ to } \alpha(w).$$

Theorem (Makdisi, 2011)

1. *$\lambda_{v,w}$ is a modular form of weight 1 for $X(N)$.*
2. *The R-algebra generated by the $\lambda_{v,w}$ contains all modular forms for $X(N)$, except cuspforms of weight 1.*
3. *The $\lambda_{v,w}$ are moduli-friendly!*

Construction of a p-adic model of Jac $\left(X(N)\right)$

1. Pick $p \nmid 6\ell N$ and $A, B \in \mathbb{Z}$ such that

$$a = \operatorname{lcm}\left([\mathbb{F}_p(\mathcal{E}[N]), \mathbb{F}_p]\ ,\ \operatorname{ord} \rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)\right)$$

is small, where $(\mathcal{E})\ :\ y^2 = x^3 + Ax + B$.

Construction of a p-adic model of Jac $\left(X(N)\right)$

1. Pick $p \nmid 6\ell N$ and $A, B \in \mathbb{Z}$ such that
$$a = \operatorname{lcm}\left([\mathbb{F}_p(\mathcal{E}[N]), \mathbb{F}_p]\ ,\ \operatorname{ord} \rho_{f,\mathfrak{l}}(\operatorname{Frob}_p)\right)$$
is small, where $(\mathcal{E})\ :\ y^2 = x^3 + Ax + B$.
2. Let $N = \prod_i l_i^{v_i}$.

Construction of a p-adic model of Jac $\left(X(N)\right)$

1. Pick $p \nmid 6\ell N$ and $A, B \in \mathbb{Z}$ such that

$$a = \operatorname{lcm}\left([\mathbb{F}_p(\mathcal{E}[N]), \mathbb{F}_p]\ ,\ \operatorname{ord} \rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)\right)$$

   is small, where $(\mathcal{E})\ :\ y^2 = x^3 + Ax + B$.

2. Let $N = \prod_i l_i^{v_i}$. For each i, find a basis

$$\langle Q_i, R_i \rangle = \mathcal{E}[l_i^{v_i}]/\mathbb{F}_q,$$

Construction of a p-adic model of $\operatorname{Jac}(X(N))$

1. Pick $p \nmid 6\ell N$ and $A, B \in \mathbb{Z}$ such that

$$a = \operatorname{lcm}\left([\mathbb{F}_p(\mathcal{E}[N]), \mathbb{F}_p] \ , \ \operatorname{ord} \rho_{f,\mathfrak{l}}(\operatorname{Frob}_p) \right)$$

   is small, where $(\mathcal{E}) \ : \ y^2 = x^3 + Ax + B$.

2. Let $N = \prod_i l_i^{v_i}$. For each i, find a basis

$$\langle Q_i, R_i \rangle = \mathcal{E}[l_i^{v_i}]/\mathbb{F}_q,$$

   then lift it to $\mathbb{Z}_q$ using $\psi_{l_i^{v_i}}(x) \in \mathbb{Q}[x]$.

Construction of a p-adic model of $\operatorname{Jac}(X(N))$

1. Pick $p \nmid 6\ell N$ and $A, B \in \mathbb{Z}$ such that
$$a = \operatorname{lcm}\left([\mathbb{F}_p(\mathcal{E}[N]), \mathbb{F}_p]\ ,\ \operatorname{ord} \rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)\right)$$
is small, where $(\mathcal{E})\ :\ y^2 = x^3 + Ax + B$.
2. Let $N = \prod_i l_i^{v_i}$. For each i, find a basis
$$\langle Q_i, R_i \rangle = \mathcal{E}[l_i^{v_i}]/\mathbb{F}_q,$$
then lift it to $\mathbb{Z}_q$ using $\psi_{l_i^{v_i}}(x) \in \mathbb{Q}[x]$.
Let $Q = \sum_i Q_i$, $R = \sum_i R_i \rightsquigarrow (\mathcal{E}, \alpha)/\mathbb{Z}_q$.

Construction of a p-adic model of $\mathrm{Jac}\left(X(N)\right)$

1. Pick $p \nmid 6\ell N$ and $A, B \in \mathbb{Z}$ such that

$$a = \operatorname{lcm}\left([\mathbb{F}_p(\mathcal{E}[N]), \mathbb{F}_p]\ ,\ \operatorname{ord} \rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)\right)$$

   is small, where $(\mathcal{E}) : y^2 = x^3 + Ax + B$.

2. Let $N = \prod_i l_i^{v_i}$. For each i, find a basis

$$\langle Q_i, R_i \rangle = \mathcal{E}[l_i^{v_i}]/\mathbb{F}_q,$$

   then lift it to $\mathbb{Z}_q$ using $\psi_{l_i^{v_i}}(x) \in \mathbb{Q}[x]$.
   Let $Q = \sum_i Q_i$, $R = \sum_i R_i \rightsquigarrow (\mathcal{E}, \alpha)/\mathbb{Z}_q$.

3. Let $P_\gamma = (\mathcal{E}, \alpha \circ \gamma) \in X(N)$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$.

Construction of a p-adic model of $\operatorname{Jac}(X(N))$

1. Pick $p \nmid 6\ell N$ and $A, B \in \mathbb{Z}$ such that
$$a = \operatorname{lcm}\left([\mathbb{F}_p(\mathcal{E}[N]), \mathbb{F}_p]\ ,\ \operatorname{ord} \rho_{f,\mathfrak{l}}(\operatorname{Frob}_p)\right)$$
is small, where $(\mathcal{E})\ :\ y^2 = x^3 + Ax + B$.
2. Let $N = \prod_i l_i^{v_i}$. For each i, find a basis
$$\langle Q_i, R_i \rangle = \mathcal{E}[l_i^{v_i}]/\mathbb{F}_q,$$
then lift it to $\mathbb{Z}_q$ using $\psi_{l_i^{v_i}}(x) \in \mathbb{Q}[x]$.
Let $Q = \sum_i Q_i$, $R = \sum_i R_i \rightsquigarrow (\mathcal{E}, \alpha)/\mathbb{Z}_q$.
3. Let $P_\gamma = (\mathcal{E}, \alpha \circ \gamma) \in X(N)$ for $\gamma \in \operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$.
4. Form the matrix $\left(\lambda_{v,w}(P_\gamma)\right)_{\{P_\gamma\} \times \{(v,w)\}}$.

Construction of a p-adic model of $\mathrm{Jac}\left(X(N)\right)$

1. Pick $p \nmid 6\ell N$ and $A, B \in \mathbb{Z}$ such that
$$a = \mathrm{lcm}\left([\mathbb{F}_p(\mathcal{E}[N]), \mathbb{F}_p]\ ,\ \mathrm{ord}\, \rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)\right)$$
is small, where $(\mathcal{E})\ :\ y^2 = x^3 + Ax + B$.
2. Let $N = \prod_i l_i^{v_i}$. For each i, find a basis
$$\langle Q_i, R_i \rangle = \mathcal{E}[l_i^{v_i}]/\mathbb{F}_q,$$
then lift it to $\mathbb{Z}_q$ using $\psi_{l_i^{v_i}}(x) \in \mathbb{Q}[x]$.
Let $Q = \sum_i Q_i$, $R = \sum_i R_i \rightsquigarrow (\mathcal{E}, \alpha)/\mathbb{Z}_q$.
3. Let $P_\gamma = (\mathcal{E}, \alpha \circ \gamma) \in X(N)$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$.
4. Form the matrix $\left(\lambda_{v,w}(P_\gamma)\right)_{\{P_\gamma\} \times \{(v,w)\}}$.

$\rightsquigarrow$ We can compute in the Jacobian of $X(N)/R$ just by looking at one E/R!

Example 1

Let

$$f = q + (-i-1)q^2 + (i-1)q^3 + O(q^4) \in S_2\big(\Gamma_1(16)\big)$$

and

$$\mathfrak{l} = (5, i-2).$$

We choose $p = 43$, because $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{43})$ has order only 4.

We catch $\rho_{f,\mathfrak{l}}$ in the 5-torsion of the Jacobian of $X_1(16)$ (genus 2).

Example 2

Let

$$f = \Delta = q - 24q^2 + 252q^3 + O(q^4) \in S_{12}\big(\Gamma_1(1)\big)$$

and

$$\mathfrak{l} = 17.$$

We choose $p = 47$, because $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{47})$ has order only 4.

We catch $\rho_{f,\mathfrak{l}}$ in the 17-torsion of the Jacobian of $X_1(17)$ (genus 5).

Optimisation

We do not have to evaluate the forms at all the P_γ.

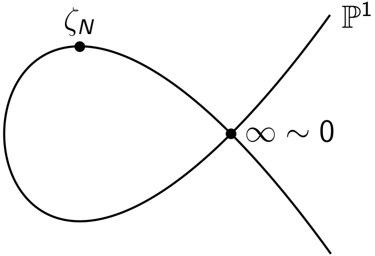
We can replace $\mathcal{L}$, which gives all modular forms of weight 2, by modular forms of weight 2 that vanish at some cusps.

The Galois action on cusps

Moduli interpretation of cusps of $X_1(N)$: a point of order N on a Néron polygon.

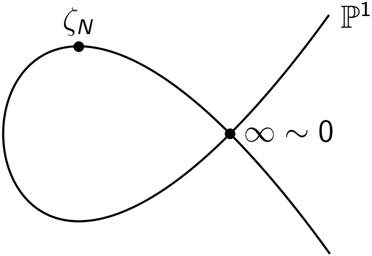
The Galois action on cusps

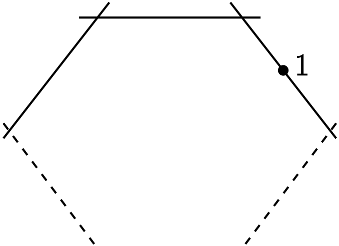
Moduli interpretation of cusps of $X_1(N)$: a point of order N on a Néron polygon.



The Galois action on cusps

Moduli interpretation of cusps of $X_1(N)$: a point of order N on a Néron polygon.





Example 2

Let

$$f = \Delta = q - 24q^2 + 252q^3 + O(q^4) \in S_{12}\big(\Gamma_1(1)\big)$$

and

$$\mathfrak{l} = 17.$$

We choose $p = 47$, because $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{47})$ has order only 4.

We catch $\rho_{f,\mathfrak{l}}$ in the 17-torsion of the Jacobian of $X_1(17)$ (genus 5).

The complex-analytic method

$$\begin{tikzcd} \begin{array}{r}\text{Algebraic model:}\\ \text{Divisors on}\\ \text{modular curves}\end{array} \arrow[r, bend left, "\text{Abel-Jacobi}", "\int"'] & \begin{array}{l}\text{Analytic model:}\\ \text{Jacobian} = \mathbb{C}^g/\Lambda\\ \text{Easy torsion}\end{array} \arrow[l, bend left, dashed] \end{tikzcd}$$

Modular forms represented by q-expansions.

Comparison with the complex-analytic method

Genus	p-adic	Complex
2	3s on 4 cores	5m on 64 cores
13	11m on 64 cores	12h on 64 cores
26	11h on 64 cores	3d on $\approx$100 cores

Comparison with the complex-analytic method

$\rho_{f,\mathfrak{l}}$ is afforded by

$$\bigcap_{n \in \mathbb{N}} \ker(T_n - a_n(f) \bmod \mathfrak{l}) \subset \mathrm{Jac}[\ell].$$

However, the p-adic method carves it out by using the characteristic polynomial of Frob_p, which cannot do better than

$$\bigcap_{n \in \mathbb{N}} \ker(T_n - a_n(f) \bmod \mathfrak{l})^\infty \subset \mathrm{Jac}[\ell].$$

Future work

- Implement Hecke action
- Improve random generation of points on the Jacobian
- Generalise to Shimura curves and Hilbert modular forms

Future work

- Implement Hecke action
- Improve random generation of points on the Jacobian
- Generalise to Shimura curves and Hilbert modular forms
  Missing ingredient: analogue of Makdisi's $\lambda_{v,w}$.

Any questions ?

Thank you !