Computing modular Galois representations

Nicolas Mascot

University of Warwick

CLap-CLap seminar
February 9$^{\text{th}}$ 2017

The modular curve $X_1(N)$

For $N \in \mathbb{N}$, let

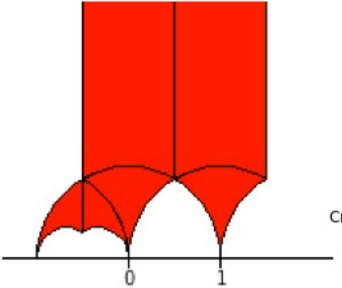
$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right] \bmod N \right\}.$$

The modular curve $X_1(N)$

For $N \in \mathbb{N}$, let

$$\Gamma_1(N) = \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv \left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right] \bmod N\}.$$

Let $\mathcal{H}^\bullet = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Then $\Gamma_1(N)\backslash\mathcal{H}^\bullet$ is a compact Riemann surface.



Credit: Helena Verrill

The modular curve $X_1(N)$

For $N \in \mathbb{N}$, let

$$\Gamma_1(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right] \bmod N\}.$$

Let $\mathcal{H}^\bullet = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Then $\Gamma_1(N)\backslash\mathcal{H}^\bullet$ is a compact Riemann surface, which is the set of $\mathbb{C}$-points of a nonsingular, complete algebraic curve $X_1(N)$ defined over $\mathbb{Q}$ and which has good reduction away from N.

We call its Jacobian $J_1(N)$.

Hecke operators

Let $\alpha = \left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right]$ where $p \in \mathbb{N}$ is prime, and $\Gamma = \Gamma_1(N)$. The correspondence

$$\begin{tikzcd}
(\Gamma \cap \alpha^{-1}\Gamma\alpha)\backslash\mathcal{H}^\bullet \arrow[r, "\sim", "\alpha"'] \arrow[d] & (\alpha\Gamma\alpha^{-1} \cap \Gamma)\backslash\mathcal{H}^\bullet \arrow[d] \\
X_1(N) \arrow[r, Rrightarrow, "T_p"'] & X_1(N)
\end{tikzcd}$$

extends to an operator on $J_1(N)$. We let $\mathbb{T}$ be the ring generated by these operators for $p \in \mathbb{N}$ prime.

Hecke operators

Let $\alpha = \left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right]$ where $p \in \mathbb{N}$ is prime, and $\Gamma = \Gamma_1(N)$. The correspondence

$$\begin{tikzcd}
(\Gamma \cap \alpha^{-1}\Gamma\alpha)\backslash\mathcal{H}^\bullet \arrow[rr, "\sim", "\alpha"'] \arrow[d] & & (\alpha\Gamma\alpha^{-1} \cap \Gamma)\backslash\mathcal{H}^\bullet \arrow[d] \\
X_1(N) \arrow[rr, Rrightarrow, "T_p"'] & & X_1(N)
\end{tikzcd}$$

extends to an operator on $J_1(N)$. We let $\mathbb{T}$ be the ring generated by these operators for $p \in \mathbb{N}$ prime.

Besides, let $\Gamma_0(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right] \bmod N\}$. Then $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^*$ by $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mapsto d \bmod N$, whence operators $\langle d \rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^*$. Actually $\langle d \rangle \in \mathbb{T}$.

Newforms

Let $\mathcal{N}_k\big(\Gamma_1(N)\big) \subset \mathcal{S}_k\big(\Gamma_1(N)\big)$ be the finite set of newforms.

Newforms

Let $\mathcal{N}_k\big(\Gamma_1(N)\big) \subset \mathcal{S}_k\big(\Gamma_1(N)\big)$ be the finite set of newforms.

Whenever $M \mid N$, we have

$$\begin{array}{ccc} \mathcal{N}_k\big(\Gamma_1(M)\big) & \begin{array}{c}\hookrightarrow\\ \hookrightarrow\\ \hookrightarrow\end{array} & \mathcal{S}_k\big(\Gamma_1(N)\big) \\ f(\tau) & \longmapsto & f(t\tau) \qquad \left(t \mid \frac{N}{M}\right). \end{array}$$

Newforms

Let $\mathcal{N}_k\big(\Gamma_1(N)\big) \subset \mathcal{S}_k\big(\Gamma_1(N)\big)$ be the finite set of newforms.

For all $f = q + \sum_{n \geqslant 2} a_n q^n \in \mathcal{N}_k\big(\Gamma_1(N)\big)$,

$$\forall p \in \mathbb{N}, \quad T_p f = a_p f,$$

so that

$$K_f = \mathbb{Q}(a_2, a_3, \cdots)$$

is actually a number field. Also, there exists

$$\varepsilon_f : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow K_f^*$$

such that

$$\langle d \rangle f = \varepsilon_f(d) f.$$

Newforms

Let $\mathcal{N}_k\big(\Gamma_1(N)\big) \subset \mathcal{S}_k\big(\Gamma_1(N)\big)$ be the finite set of newforms.

For all $f = q + \sum_{n\geqslant 2} a_n q^n \in \mathcal{N}_k\big(\Gamma_1(N)\big)$,

$$K_f = \mathbb{Q}(a_2, a_3, \cdots)$$

is actually a number field. Also, there exists

$$\varepsilon_f : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow K_f^*$$

such that

$$\langle d \rangle f = \varepsilon_f(d) f.$$

For all $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$,

$$f^\sigma = q + \sum_{n\geqslant 2} \sigma(a_n) q^n \in \mathcal{N}_k\big(\Gamma_1(N)\big)$$

and $K_{f^\sigma} = K_f^\sigma$, $\varepsilon_{f^\sigma} = \sigma \circ \varepsilon_f$.

Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in \mathcal{N}_k\big(\Gamma_1(N)\big)$, $k \geqslant 2$.

Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in \mathcal{N}_k\big(\Gamma_1(N)\big)$, $k \geqslant 2$.

Pick a prime $\mathfrak{l}$ of K_f lying over $\ell \in \mathbb{N}$, and let $K_{f,\mathfrak{l}}$ be the $\mathfrak{l}$-adic completion of K_f.

Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in \mathcal{N}_k(\Gamma_1(N))$, $k \geqslant 2$.

Pick a prime $\mathfrak{l}$ of K_f lying over $\ell \in \mathbb{N}$, and let $K_{f,\mathfrak{l}}$ be the $\mathfrak{l}$-adic completion of K_f.

Theorem (Deligne, Serre, Shimura, 1971)

There exists a unique continuous Galois representation

$$R_{f,\mathfrak{l}} \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(K_{f,\mathfrak{l}}),$$

which is unramified outside ℓN, and such that for all $p \nmid \ell N$, $R_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ has characteristic polynomial

$$X^2 - a_p X + \varepsilon_f(p) p^{k-1} \in K_{f,\mathfrak{l}}[X].$$

Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in \mathcal{N}_k\big(\Gamma_1(N)\big)$, $k \geqslant 2$.

Pick a prime $\mathfrak{l}$ of K_f lying over $\ell \in \mathbb{N}$, and let $\mathbb{F}_\mathfrak{l}$ be its residual field.

Theorem (Deligne, Serre, Shimura, 1971)

There exists a unique continuous Galois representation

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

which is unramified outside ℓN, and such that for all $p \nmid \ell N$, $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ has characteristic polynomial

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

Modular Galois representations

Theorem (Deligne, Serre, Shimura, 1971)

There exists a unique continuous Galois representation

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

which is unramified outside ℓN, and such that for all $p \nmid \ell N$, $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ has characteristic polynomial

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

Application (Couveignes, Edixhoven, 2006)

$\rho_{f,\mathfrak{l}}$ can be computed in time polynomial in ℓ, and $a_p \bmod \mathfrak{l}$ in time polynomial in $\log p$.

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

Motivation

- The Galois representation itself,

Motivation

- The Galois representation itself,
- The field $L = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}}$ is a Galois number field, with Galois group (almost) $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$, whose ramification behaviour is well-understood
$\rightsquigarrow$ Inverse Galois problem for GL_2 and PGL_2, Gross's problem, construction of very lightly ramified fields,

Motivation

- The Galois representation itself,
- The field $L = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}}$ is a Galois number field, with Galois group (almost) $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$, whose ramification behaviour is well-understood
$\rightsquigarrow$ Inverse Galois problem for GL_2 and PGL_2, Gross's problem, construction of very lightly ramified fields,
- Fast computation of Fourier coefficients: computation of $a_p \bmod \mathfrak{l} = \operatorname{Tr} \rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ in time $(\log p)^{2+\varepsilon(p)}$.

Example 1

Theorem (M.)

- The field cut out by $\rho_{\Delta,31}$ is the field generated by the 31^{st} roots of unity and by the roots of

$$
\begin{aligned}
&x^{64} - 21\,x^{63} + 118\,x^{62} + 527\,x^{61} - 8587\,x^{60} + 18383\,x^{59} + 263035\,x^{58} - 2095879\,x^{57} + 2416016\,x^{56} + 44283128\,x^{55} - 240474192\,x^{54}\\
&+84687350\,x^{53} + 3638349286\,x^{52} - 12617823980\,x^{51} - 10297265505\,x^{50} + 155175311479\,x^{49} - 196432825560\,x^{48} - 771645455342\,x^{47}\\
&+1482783472303\,x^{46} + 2641351695834\,x^{45} + 4650870173875\,x^{44} - 45480241563019\,x^{43} - 54597672402738\,x^{42} + 501026042999912\,x^{41}\\
&-496541492329624\,x^{40} - 712343608491160\,x^{39} + 5302741451178477\,x^{38} - 30548025690548139\,x^{37} + 34878663423629056\,x^{36}\\
&+288784532405339724\,x^{35} - 874206875792459963\,x^{34} - 825384106177640249\,x^{33} + 6958723996166230970\,x^{32}\\
&-4535708640900181166\,x^{31} - 30017821501048367756\,x^{30} + 56583574288118086410\,x^{29} + 60507682456797414358\,x^{28}\\
&-278043951776326798765\,x^{27} + 87013091280485835964\,x^{26} + 765685764124853689529\,x^{25} - 1039521490897195574873\,x^{24}\\
&-857609563094973739451\,x^{23} + 3508677503532089909529\,x^{22} - 2261986657658172377618\,x^{21} - 5701736296366236274465\,x^{20}\\
&+13022859322612898456054\,x^{19} - 6410034736367305328 62\,x^{18} - 29939230256003209147601\,x^{17} + 25447129369769267020402\,x^{16}\\
&+36125137963345226955671\,x^{15} - 55314588133331740131989\,x^{14} - 18703775559594899286772\,x^{13} + 43941206930666596631797\,x^{12}\\
&+17651378415866112635127\,x^{11} + 10928239966752626190216\,x^{10} - 81873964056071560411072\,x^{9} - 14246438965830190561265\,x^{8}\\
&+128298548281018972743749\,x^{7} - 50060167623901195766317\,x^{6} - 45764538130200829948820\,x^{5} + 18800719945150143916844\,x^{4}\\
&-81794726341377172440 72\,x^{3} + 62290435026572905701979\,x^{2} - 71710139962834196823306\,x + 25842211492123062583556.
\end{aligned}
$$

(several CPU years).

Example 1

Theorem (M.)

- The field cut out by $\rho_{\Delta,31}$ is the field generated by the 31^{st} roots of unity and by the roots of $x^{64} - 21\,x^{63} + \cdots$.
- We have the following values:

p	$\rho_{\Delta,31}(\mathrm{Frob}_p)$ similar to	$\tau(p)$ mod 31
$10^{1000} + 453$	$\begin{bmatrix} 30 & 0 \\ 0 & 20 \end{bmatrix}$	19
$10^{1000} + 1357$	$\begin{bmatrix} 0 & 2 \\ 1 & 13 \end{bmatrix}$	13
$10^{1000} + 4351$	$\begin{bmatrix} 4 & 1 \\ 0 & 4 \end{bmatrix}$	8

(30s of CPU time per p).

Example 2

Theorem (M.)

Let $f = q + 2q^2 - 4q^3 + O(q^4) \in \mathcal{N}_6\big(\Gamma_0(5)\big)$.
The field cut out by the projective representation attached to f mod 13 is the field generated by the roots of

$$x^{14} - x^{13} - 26x^{11} + 39x^{10} + 104x^9 - 299x^8 - 195x^7 + 676x^6 + 481x^5 - 156x^4 - 39x^3 + 65x^2 - 14x + 1.$$

Example 2

Theorem (M.)

Let $f = q + 2q^2 - 4q^3 + O(q^4) \in \mathcal{N}_6\big(\Gamma_0(5)\big)$.
The field cut out by the projective representation attached to f mod 13 is the field generated by the roots of

$$x^{14} - x^{13} - 26x^{11} + 39x^{10} + 104x^9 - 299x^8 - 195x^7 + 676x^6 + 481x^5 - 156x^4 - 39x^3 + 65x^2 - 14x + 1.$$

This polynomial and this field were not known before. Its root discriminant is $47.816\cdots$, whereas the next best known example has root discriminant $69.939\cdots$.

Conjecture (Roberts, M.)

This field is the one that has the smallest discriminant among all the Galois number fields with Galois group $\mathrm{PGL}_2(\mathbb{F}_{13})$.

Explicit construction of the representation

The Tate module of $J_1(N)$

When A is an Abelian variety over $\mathbb{Q}$ of dimension g, define

$$\operatorname{Ta}_\ell A = \varprojlim_{n \in \mathbb{N}} A[\ell^n],$$

a free $\mathbb{Z}_\ell$-module of rank $2g$, and

$$V_\ell A = \operatorname{Ta}_\ell A \otimes_{\mathbb{Z}} \mathbb{Q} = \operatorname{Ta}_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

The Tate module of $J_1(N)$

When A is an Abelian variety over $\mathbb{Q}$ of dimension g, define

$$\operatorname{Ta}_\ell A = \varprojlim_{n \in \mathbb{N}} A[\ell^n],$$

a free $\mathbb{Z}_\ell$-module of rank $2g$, and

$$V_\ell A = \operatorname{Ta}_\ell A \otimes_{\mathbb{Z}} \mathbb{Q} = \operatorname{Ta}_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

The action of Galois yields a representation

$$R_{A,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$$

which is unramified away from ℓ and the primes of bad reduction of A.

The Tate module of $J_1(N)$

The action of Galois yields a representation

$$R_{A,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$$

which is unramified away from ℓ and the primes of bad reduction of A.

Take now $A = J_1(N)$. Then $V_\ell J_1(N)$ is actually a free $(\mathbb{T} \otimes \mathbb{Q}_\ell)$-module of rank 2, whence

$$R_{J_1(N),\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{T} \otimes \mathbb{Q}_\ell)$$

unramified away from ℓN.

The Tate module of $J_1(N)$

The action of Galois yields a representation

$$R_{A,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$$

which is unramified away from ℓ and the primes of bad reduction of A.

Take now $A = J_1(N)$. Then $V_\ell J_1(N)$ is actually a free $(\mathbb{T} \otimes \mathbb{Q}_\ell)$-module of rank 2, whence

$$R_{J_1(N),\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{T} \otimes \mathbb{Q}_\ell)$$

unramified away from ℓN.

For $p \nmid \ell N$, the characteristic polynomial of the image of Frob_p is

$$X_2 - T_p X + p\langle p \rangle \in (\mathbb{T} \otimes \mathbb{Q}_\ell)[X].$$

Modular Abelian varieties

For $f \in \mathcal{N}_2(\Gamma_1(N))$, let

$$I_f = \{ T \in \mathbb{T} \mid Tf = 0 \},$$

and define

$$A_f = J_1(N)/I_f J_1(N).$$

Modular Abelian varieties

For $f \in \mathcal{N}_2(\Gamma_1(N))$, let

$$I_f = \{T \in \mathbb{T} \mid Tf = 0\},$$

and define

$$A_f = J_1(N)/I_f J_1(N).$$

Properties

- $I_{f^\sigma} = I_f$, so $A_{f^\sigma} = A_f$.
- A_f is a simple Abelian variety defined over $\mathbb{Q}$.
- $\dim A_f = [K_f : \mathbb{Q}]$.
- $K_f \hookrightarrow \operatorname{End}(A_f) \otimes \mathbb{Q}$ via $a_p \mapsto T_p$, $\varepsilon_f(d) \mapsto \langle d \rangle$. Indeed, $K_f \simeq (\mathbb{T}/I_f) \otimes \mathbb{Q}$.
- $L(A_f, s) = \prod_\sigma L(f^\sigma, s) \overset{\text{def}}{=} \prod_\sigma \sum_{n \geqslant 1} \frac{\sigma(a_n)}{n^s}$.

The decomposition of $J_1(N)$

Over $\mathbb{Q}$, $J_1(N)$ is isogenous to

$$\prod_{M \mid N} \prod_{f \in G_{\mathbb{Q}} \backslash \mathcal{N}_2\left(\Gamma_1(M)\right)} A_f^{\sigma_0(N/M)}.$$

So

$$V_\ell J_1(N) \simeq \prod_{M \mid N} \prod_{f \in G_{\mathbb{Q}} \backslash \mathcal{N}_2\left(\Gamma_1(M)\right)} (V_\ell A_f)^{\sigma_0(N/M)}$$

as $G_{\mathbb{Q}}$-modules.

The decomposition of $J_1(N)$

Example: $N = 22$

$\mathcal{S}_2\big(\Gamma_1(1)\big) = \mathcal{S}_2\big(\Gamma_1(2)\big) = 0.$

At level 11, we have one rational newform

$$f_{11} = q - 2q^2 - q^3 + O(q^4).$$

At level 22, the newforms are

$$f_{22} = q + \zeta_5 q^2 + (\zeta_5^3 - \zeta_5 - 1)q^3 + O(q^4)$$

and its Galois conjugates.

$$\rightsquigarrow \mathcal{S}_2\big(\Gamma_1(22)\big) = \underbrace{\langle f_{11}(\tau), f_{11}(2\tau)\rangle}_{\text{Old}} \oplus \underbrace{\langle \text{Galois conjugates of } f_{22}\rangle}_{\text{New}},$$

$$J_1(22) \sim A_{f_{11}}^2 \times A_{f_{22}}.$$

$A_{f_{11}}$ is the elliptic curve of conductor 11; $A_{f_{22}}$ is a simple Abelian variety of dimension 4.

So $\text{genus}\big(X_1(22)\big) = 6$.

Recovering the modular representations

$V_\ell A_f$ is a $\mathbb{Q}_\ell$-vector space of dimension $2[K_f : \mathbb{Q}]$, and actually a free $K_f \otimes \mathbb{Q}_\ell$-module of rank 2.

Recovering the modular representations

$V_\ell A_f$ is a $\mathbb{Q}_\ell$-vector space of dimension $2[K_f : \mathbb{Q}]$, and actually a free $K_f \otimes \mathbb{Q}_\ell$-module of rank 2.

As $K_f \otimes \mathbb{Q}_\ell \simeq \prod_{\mathfrak{l} \mid \ell} K_{f,\mathfrak{l}}$, we recover the representations

$$R_{f,\mathfrak{l}} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(K_{f,\mathfrak{l}})$$

inside $V_\ell A_f \subset V_\ell J_1(N)$.

Recovering the modular representations

$V_\ell A_f$ is a $\mathbb{Q}_\ell$-vector space of dimension $2[K_f : \mathbb{Q}]$, and actually a free $K_f \otimes \mathbb{Q}_\ell$-module of rank 2.

As $K_f \otimes \mathbb{Q}_\ell \simeq \prod_{\mathfrak{l} \mid \ell} K_{f,\mathfrak{l}}$, we recover the representations

$$R_{f,\mathfrak{l}} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(K_{f,\mathfrak{l}})$$

inside $V_\ell A_f \subset V_\ell J_1(N)$.

In particular, if $\mathfrak{l}$ is of degree 1, $\rho_{f,\mathfrak{l}}$ is afforded by

$$V_{f,\mathfrak{l}} = \bigcap_p \mathrm{Ker}\left(T_p|_{J_1(N)[\ell]} - a_p(f) \bmod \mathfrak{l} \right) \subset J_1(N)[\ell].$$

Weight lowering

Weight-lowering theorem

Suppose $\ell \geqslant 5$ and $\ell \nmid N$, and let $f \in \mathcal{N}_{k}(\Gamma_1(N))$ be a newform of weight $3 \leqslant k \leqslant \ell$. There exists a newform $f_2 \in \mathcal{N}_{2}(\Gamma_1(\ell N))$ of weight 2 and a prime $\mathfrak{l}_2 \mid \ell$ of K_{f_2} such that

$$f \bmod \mathfrak{l} = f_2 \bmod \mathfrak{l}_2.$$

Weight lowering

Weight-lowering theorem

Suppose $\ell \geqslant 5$ and $\ell \nmid N$, and let $f \in \mathcal{N}_k(\Gamma_1(N))$ be a newform of weight $3 \leqslant k \leqslant \ell$. There exists a newform $f_2 \in \mathcal{N}_2(\Gamma_1(\ell N))$ of weight 2 and a prime $\mathfrak{l}_2 \mid \ell$ of K_{f_2} such that

$$f \bmod \mathfrak{l} = f_2 \bmod \mathfrak{l}_2.$$

Thus $\rho_{f_2,\mathfrak{l}_2} \simeq \rho_{f,\mathfrak{l}}$, so that we can use the same geometric construction again. We now find $\rho_{f,\mathfrak{l}}$ in $J_1(\ell N)[\ell]$.

Weight lowering

Thus $\rho_{f_2,\mathfrak{l}_2} \simeq \rho_{f,\mathfrak{l}}$, so that we can use the same geometric construction again. We now find $\rho_{f,\mathfrak{l}}$ in $J_1(\ell N)[\ell]$.

Example

Take $f = \Delta \in \mathcal{N}_{12}\big(\Gamma_1(1)\big)$. If $\ell \geqslant 13$, there exists

$$f_2 \in \mathcal{N}_2\big(\Gamma_1(\ell)\big), \qquad \mathfrak{l}_2 \subset K_{f_2}$$

such that

$$f_2 \bmod \mathfrak{l}_2 = \Delta \bmod \ell \text{ in } \mathbb{F}_\ell[[q]],$$

so that $\rho_{\Delta,\ell}$ is afforded in $J_1(\ell)[\ell]$.

The modular curve $X_H(\ell N)$

The condition

$$f \bmod \mathfrak{l} = f_2 \bmod \mathfrak{l}_2$$

implies that

$$\forall x,\ \varepsilon_{f_2}(x) \bmod \mathfrak{l}_2 = x^{k-2}\varepsilon_f(x).$$

$\rho_{f,\mathfrak{l}}$ actually occurs in the Jacobian of the modular curve $X_H(\ell N)$ attached to

$$\Gamma_H(\ell N) = \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(\ell N) \ \middle|\ d \in H \right\}$$

where $H = \operatorname{Ker}(\varepsilon_{f_2} \bmod \mathfrak{l}_2) \leqslant (\mathbb{Z}/\ell N\mathbb{Z})^*$.

The genus of this curve is sometimes much smaller than that of $X_1(\ell N)$.

Computing in the modular Jacobian

Divisors on curves

Let X be a proper, nonsingular, absolutely integral curve of genus g over a field K.

A *divisor* on X is a formal $\mathbb{Z}$-linear combination of points of X.

The *degree* of $\sum_{P \in X} n_P P$ is $\sum_{P \in X} n_P \in \mathbb{Z}$.

Divisors of degree 0 form a subgroup $\operatorname{Div}^0(X)$ of the group $\operatorname{Div}(X)$ of divisors on X.

A divisor is *principal* if it is the divisor (f) of a function $f \in K(X)^*$. Principal divisors form a subgroup $\operatorname{Ppal}(X)$ of $\operatorname{Div}^0(X)$.

We define $\operatorname{Pic}^0(X) = \operatorname{Div}^0(X) / \operatorname{Ppal}(X)$.

Divisors on curves

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
1 \arrow[r] & K^* \arrow[r] & K(X)^* \arrow[r] & \mathrm{Ppal}(X) \arrow[r] \arrow[d] & 0 \\
 & & & \mathrm{Div}^0(X) \arrow[d] & \\
 & & & \mathrm{Pic}^0(X) \arrow[d] & \\
 & & & 0 &
\end{tikzcd}$$

Divisors on curves

Divisors of degree 0 form a subgroup $\mathrm{Div}^0(X)$ of the group $\mathrm{Div}(X)$ of divisors on X.

A divisor is *principal* if it is the divisor (f) of a function $f \in K(X)^*$. Principal divisors form a subgroup $\mathrm{Ppal}(X)$ of $\mathrm{Div}^0(X)$.

We define $\mathrm{Pic}^0(X) = \mathrm{Div}^0(X) / \mathrm{Ppal}(X)$.

We have

$$\mathrm{Pic}^0(X)(L) \simeq \mathrm{Jac}(X)(L)$$

for all extensions L of K.

Assume that $K = \mathbb{C}$, and let $\omega_1, \cdots, \omega_g$ be a basis of holomorphic differentials on X.

The Abel-Jacobi map

Assume that $K = \mathbb{C}$, and let $\omega_1, \cdots, \omega_g$ be a basis of holomorphic differentials on X.

A *period* is a vector

$$\lambda = \int_\gamma (\omega_i)_{i=1\cdots g} \in \mathbb{C}^g$$

where γ is a loop on X.
Peridods forms a lattice $\Lambda \in \mathbb{C}^g$, and $\mathrm{Jac}(X)(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$.

The Abel-Jacobi map

Assume that $K = \mathbb{C}$, and let $\omega_1, \cdots, \omega_g$ be a basis of holomorphic differentials on X.

A *period* is a vector

$$\lambda = \int_\gamma (\omega_i)_{i=1\cdots g} \in \mathbb{C}^g$$

where γ is a loop on X.
Peridods forms a lattice $\Lambda \in \mathbb{C}^g$, and $\mathrm{Jac}(X)(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$.

If we fix $O \in X$, we can define

$$\begin{array}{rcl} \jmath_O : X & \longrightarrow & \mathbb{C}^g/\Lambda \\ P & \longmapsto & \displaystyle\int_O^P (\omega_i)_{i=1\cdots g}, \end{array}$$

The Abel-Jacobi map

A *period* is a vector
$$\lambda = \int_\gamma (\omega_i)_{i=1\cdots g} \in \mathbb{C}^g$$
where γ is a loop on X.
Peridods forms a lattice $\Lambda \in \mathbb{C}^g$, and $\operatorname{Jac}(X)(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$.

If we fix $O \in X$, we can define
$$\begin{array}{rcl} \jmath_O : X & \longrightarrow & \mathbb{C}^g/\Lambda \\ P & \longmapsto & \displaystyle\int_O^P (\omega_i)_{i=1\cdots g}, \end{array}$$
extend it additively to $\operatorname{Div}(X)$, and restrict it to
$$\begin{array}{rcl} \jmath : \operatorname{Div}^0(X) & \longrightarrow & \mathbb{C}^g/\Lambda \\ \displaystyle\sum_n (P_n' - P_n) & \longmapsto & \displaystyle\sum_n \int_{P_n}^{P_n'} (\omega_i)_{i=1\cdots g} \end{array}$$

The Abel-Jacobi map

If we fix $O \in X$, we can define

$$\begin{array}{rcl} \jmath_O : X & \longrightarrow & \mathbb{C}^g/\Lambda \\ P & \longmapsto & \displaystyle\int_O^P (\omega_i)_{i=1\cdots g}, \end{array}$$

extend it additively to $\mathrm{Div}(X)$, and restrict it to

$$\begin{array}{rcl} \jmath : \mathrm{Div}^0(X) & \longrightarrow & \mathbb{C}^g/\Lambda \\ \displaystyle\sum_n (P'_n - P_n) & \longmapsto & \displaystyle\sum_n \int_{P_n}^{P'_n} (\omega_i)_{i=1\cdots g} \end{array}$$

which no longer depends on O and whose kernel is exactly $\mathrm{Ppal}(X)$, whence

$$\jmath : \mathrm{Pic}^0(X) \xrightarrow{\sim} \mathbb{C}^g/\Lambda = \mathrm{Jac}(X).$$

Makdisi's algorithms: basic blocks

When $D \in Div(X)$, write

$$H^0(D) = \{f \in K(X)^* \mid (f) + D \geqslant 0\} \cup \{0\}.$$

Lemma (Basic blocks)

- If $\deg D_1, \deg D_2 \geqslant 2g + 1$, then the multiplication map

$$H^0(D_1) \otimes H^0(D_2) \longrightarrow H^0(D_1 + D_2)$$

  is surjective.
- $f \cdot H^0(D) = H^0\big(D - (f)\big)$.
- If $\deg D_1 \geqslant 2g$, then

$$H^0(D_2 - D_1) = \{f \in K(X) \mid f \cdot H^0(D_1) \subset H^0(D_2)\}.$$

Makdisi's algorithms: representation of elements

Fix a divisor D_0 on X of degree $d_0 \geqslant 2g+1$, and let

$$V = H^0(3D_0), \quad V_2 = H^0(6D_0),$$

whose elements are represented by multipoint evaluation, or Taylor series (or both !)

Makdisi's algorithms: representation of elements

Fix a divisor D_0 on X of degree $d_0 \geqslant 2g+1$, and let

$$V = H^0(3D_0), \quad V_2 = H^0(6D_0),$$

whose elements are represented by multipoint evaluation, or Taylor series (or both !)

A point $x \in \mathrm{Jac}(X) = \mathrm{Pic}^0(X) \leftrightarrow$ the subspace

$$W_{D_x} = V(-D_x) = H^0(3D_0 - D_x) \subset V,$$

where $D_x \geqslant 0$ is a divisor of degree d_0 such that

$$[D_x - D_0] = x.$$

D_x is not unique !

Makdisi's algorithms: group law

Let W_{D_1}, W_{D_2} represent two points $x_1, x_2 \in \mathrm{Jac}(X)$.

Makdisi's algorithms: group law

Let W_{D_1}, W_{D_2} represent two points $x_1, x_2 \in \mathrm{Jac}(X)$.

1. Compute $H^0(6D_0 - D_1 - D_2) = W_{D_1} \cdot W_{D_2}$.

Makdisi's algorithms: group law

Let W_{D_1}, W_{D_2} represent two points $x_1, x_2 \in \text{Jac}(X)$.

1. Compute $H^0(6D_0 - D_1 - D_2) = W_{D_1} \cdot W_{D_2}$.
2. Compute
$H^0(3D_0 - D_1 - D_2) = \{f \in V \mid f \cdot V \subset H^0(6D_0 - D_1 - D_2)\}$.

Makdisi's algorithms: group law

Let W_{D_1}, W_{D_2} represent two points $x_1, x_2 \in \operatorname{Jac}(X)$.

1. Compute $H^0(6D_0 - D_1 - D_2) = W_{D_1} \cdot W_{D_2}$.
2. Compute $H^0(3D_0 - D_1 - D_2) = \{f \in V \mid f \cdot V \subset H^0(6D_0 - D_1 - D_2)\}$.
3. Take $s \in H^0(3D_0 - D_1 - D_2)$, so that
$$(s) = -3D_0 + D_1 + D_2 + D_3, \quad \text{some } D_3 \geqslant 0.$$
Compute $H_0(6D_0 - D_1 - D_2 - D_3) = s \cdot V$.

Makdisi's algorithms: group law

Let W_{D_1}, W_{D_2} represent two points $x_1, x_2 \in \mathrm{Jac}(X)$.

1. Compute $H^0(6D_0 - D_1 - D_2) = W_{D_1} \cdot W_{D_2}$.
2. Compute $H^0(3D_0 - D_1 - D_2) = \{f \in V \mid f \cdot V \subset H^0(6D_0 - D_1 - D_2)\}$.
3. Take $s \in H^0(3D_0 - D_1 - D_2)$, so that
$$(s) = -3D_0 + D_1 + D_2 + D_3, \quad \text{some } D_3 \geqslant 0.$$
Compute $H_0(6D_0 - D_1 - D_2 - D_3) = s \cdot V$.
4. Compute $W_{D_3} = H^0(3D_0 - D_3)$
$= \{f \in V \mid f \cdot H^0(3D_0 - D_1 - D_2) \subset H_0(6D_0 - D_1 - D_2 - D_3)\}$.

Makdisi's algorithms: group law

Let W_{D_1}, W_{D_2} represent two points $x_1, x_2 \in \mathrm{Jac}(X)$.

1. Compute $H^0(6D_0 - D_1 - D_2) = W_{D_1} \cdot W_{D_2}$.
2. Compute $H^0(3D_0 - D_1 - D_2) = \{f \in V \mid f \cdot V \subset H^0(6D_0 - D_1 - D_2)\}$.
3. Take $s \in H^0(3D_0 - D_1 - D_2)$, so that
$$(s) = -3D_0 + D_1 + D_2 + D_3, \quad \text{some } D_3 \geqslant 0.$$
Compute $H_0(6D_0 - D_1 - D_2 - D_3) = s \cdot V$.
4. Compute $W_{D_3} = H^0(3D_0 - D_3)$
$= \{f \in V \mid f \cdot H^0(3D_0 - D_1 - D_2) \subset H_0(6D_0 - D_1 - D_2 - D_3)\}$.

Then W_{D_3} represents $x_3 \in \mathrm{Jac}(X)$ such that $x_1 + x_2 + x_3 = 0$.

Makdisi's algorithms on the modular curve

Let $f_0 \in \mathcal{S}_2\big(\Gamma_1(\ell N)\big)$ be defined over $\mathbb{Q}$.

We take $D_0 = (f_0) + c_1 + c_2 + c_3$, where the c_i are cusps such that $\sum c_i$ is defined over $\mathbb{Q}$.

$$\rightsquigarrow H^0(D_0) \simeq \mathcal{S}_2\big(\Gamma_1(\ell N)\big) \oplus \langle E_{1,2}, E_{1,3} \rangle \subset \mathcal{M}_2\big(\Gamma_1(\ell N)\big),$$

where $E_{1,i}$ is an Eisenstein series of weight 2 that vanishes at all the cusps except c_1 and c_i.

Makdisi's algorithms on the modular curve

Let $f_0 \in \mathcal{S}_2\big(\Gamma_1(\ell N)\big)$ be defined over $\mathbb{Q}$.

We take $D_0 = (f_0) + c_1 + c_2 + c_3$, where the c_i are cusps such that $\sum c_i$ is defined over $\mathbb{Q}$.

$$\rightsquigarrow H^0(D_0) \simeq \mathcal{S}_2\big(\Gamma_1(\ell N)\big) \oplus \langle E_{1,2}, E_{1,3} \rangle \subset \mathcal{M}_2\big(\Gamma_1(\ell N)\big),$$

where $E_{1,i}$ is an Eisenstein series of weight 2 that vanishes at all the cusps except c_1 and c_i.

We represent these forms by their q-expansion at all cusps.

Let $f_0 \in \mathcal{S}_2\big(\Gamma_1(\ell N)\big)$ be defined over $\mathbb{Q}$.

We take $D_0 = (f_0) + c_1 + c_2 + c_3$, where the c_i are cusps such that $\sum c_i$ is defined over $\mathbb{Q}$.

$$\rightsquigarrow H^0(D_0) \simeq \mathcal{S}_2\big(\Gamma_1(\ell N)\big) \oplus \langle E_{1,2}, E_{1,3} \rangle \subset \mathcal{M}_2\big(\Gamma_1(\ell N)\big),$$

where $E_{1,i}$ is an Eisenstein series of weight 2 that vanishes at all the cusps except c_1 and c_i.

We represent these forms by their q-expansion at all cusps.

We then compute $V = H^0(3D_0) \subset \mathcal{M}_6\big(\Gamma_1(\ell N)\big)$ by multiplication.

Computation of the representation

Assumptions

From now on, we assume that $f \in \mathcal{N}_k\big(\Gamma_1(N)\big)$ and $\mathfrak{l} \subset K_f$ are such that

- $\deg \mathfrak{l} = 1$,
- $\ell \nmid N$ and $k \leqslant \ell$,
- $\operatorname{Im} \rho_{f,\mathfrak{l}} \supset \mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$.

How does one compute such a representation ?

In order to compute $\rho_{f,\mathfrak{l}}$, we first compute the number field

$$L = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}} = \mathbb{Q}(x, x \in V_{f,\mathfrak{l}})$$

that it cuts out, and then the image of the Frobenius elements.

How does one compute such a representation ?

In order to compute $\rho_{f,\mathfrak{l}}$, we first compute the number field

$$L = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}} = \mathbb{Q}(x, x \in V_{f,\mathfrak{l}})$$

that it cuts out, and then the image of the Frobenius elements.

- If we were dealing with an elliptic curve, we could simply compute the division polynomial $\Phi_\ell \in \mathbb{Q}[X]$.

How does one compute such a representation ?

In order to compute $\rho_{f,\mathfrak{l}}$, we first compute the number field

$$L = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}} = \mathbb{Q}(x, x \in V_{f,\mathfrak{l}})$$

that it cuts out, and then the image of the Frobenius elements.

- If we were dealing with an elliptic curve, we could simply compute the division polynomial $\Phi_\ell \in \mathbb{Q}[X]$.
- But we are dealing with the Jacobian $J_1(\ell)$, so this approach is intractable.

The analytic model comes in handy

In the elliptic curve case:

$$
\begin{tikzcd}[column sep=huge]
\begin{array}{c}\text{Algebraic model}\\ y^2 = x^3 + ax + b\\ \text{(Weierstrass)}\end{array}
\arrow[r, bend left, "\text{Abel-Jacobi } \jmath", "P \mapsto \int_\infty^P \frac{dx}{y}"']
&
\begin{array}{c}\text{Analytic model}\\ \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)\\ \text{Easy torsion}\end{array}
\arrow[l, bend left, "(\wp_\tau ; \wp'_\tau)"]
\end{tikzcd}
$$

The analytic model comes in handy

In the elliptic curve case:

$$\begin{tikzcd}[column sep=huge] \begin{array}{c}\text{Algebraic model}\\ y^2 = x^3 + ax + b\\ \text{(Weierstrass)}\end{array} \arrow[r, bend left, "\text{Abel-Jacobi } \jmath", "P \mapsto \int_\infty^P \frac{dx}{y}"'] & \begin{array}{c}\text{Analytic model}\\ \mathbb{C}/(\mathbb{Z}\oplus\mathbb{Z}\tau)\\ \text{Easy torsion}\end{array} \arrow[l, bend left, "(\wp_\tau ; \wp'_\tau)"] \end{tikzcd}$$

In the modular case, we work with divisors instead of points.

$$\begin{tikzcd}[column sep=huge] \begin{array}{c}\text{Algebraic model}\\ \mathrm{Div}^0\left(X_1(\ell N)\right)\\ \text{Easy to evaluate}\end{array} \arrow[r, bend left, "\text{Abel-Jacobi } \jmath"] & \begin{array}{c}\text{Analytic model}\\ J_1(\ell N)(\mathbb{C}) = \mathbb{C}^g/\Lambda\\ \text{Easy torsion}\end{array} \arrow[l, bend left, dashed] \end{tikzcd}$$

$$\left[\sum_{i=1}^g P_i - gO\right] \mapsto \sum_{i=1}^g \xi(P_i)$$

There is no $\wp$, so we must invert $\jmath$ "by hand".

Strategy

Goal: compute $V_{f,\mathfrak{l}} \subset J_1(\ell N)[\ell]$.

1. Period lattice Λ of $X_1(\ell N)$
   High accuracy q-expansions, term-by-term integration

   $\rightsquigarrow$ analytic model of $J_1(\ell N)$
2. Approximation over $\mathbb{C}$ of the ℓ-torsion

   Computation of divisors $D_1,\ D_2 \in \mathrm{Div}^0\left(X_1(\ell N)\right)$ representing a basis of

   $V_{f,\mathfrak{l}} \subset J_1(\ell N)[\ell]$
3. Evaluation of the ℓ-torsion
   Choice of a "well-behaved" function $\alpha\colon V_{f,\mathfrak{l}} \longrightarrow \overline{\mathbb{Q}}$

   $\rightsquigarrow$ number field L cut out by $\rho_{f,\mathfrak{l}}$
4. Frobenius elements

   Recipe to compute the image of the Frobenius at p, given $p \nmid \ell N$

Step 1

- Period lattice Λ of $X_1(\ell N)$
  High accuracy q-expansions, term-by-term integration

  $\rightsquigarrow$ analytic model of $J_1(\ell N)$

  Approximation over $\mathbb{C}$ of the ℓ-torsion

  Computation of divisors $D_1, D_2 \in \operatorname{Div}^0\left(X_1(\ell N)\right)$ representing a basis of $V_{f,\mathfrak{l}} \subset J_1(\ell N)[\ell]$

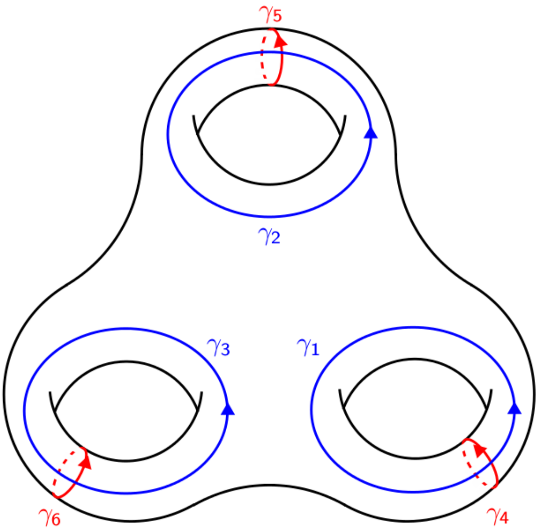
  Evaluation of the ℓ-torsion
  Choice of a "well-behaved" function $\alpha\colon V_{f,\mathfrak{l}} \longrightarrow \overline{\mathbb{Q}}$

  $\rightsquigarrow$ number field L cut out by $\rho_{f,\mathfrak{l}}$

  Frobenius elements

  Recipe to compute the image of the Frobenius at p, given $p \nmid \ell N$

Periods of the modular curve $X_1(\ell N)$



Periods of the modular curve $X_1(\ell N)$

Analytic model of $J_1(\ell N)$

Let $\omega_1, \cdots, \omega_g$ be a basis of $\Omega^1\big(X_1(\ell N)\big) \simeq S_2\big(\Gamma_1(\ell N)\big)$. Integrate the differentials $\omega_i(\tau)d\tau$ along the curves γ_j. This yields a lattice $\Lambda = \left\langle \left(\int_{\gamma_j} \omega_i\right)_{1 \leqslant i \leqslant g} \right\rangle_{1 \leqslant j \leqslant 2g} \subset \mathbb{C}^g$, and $J_1(\ell) = \mathbb{C}^g/\Lambda$.

Periods of the modular curve $X_1(\ell N)$

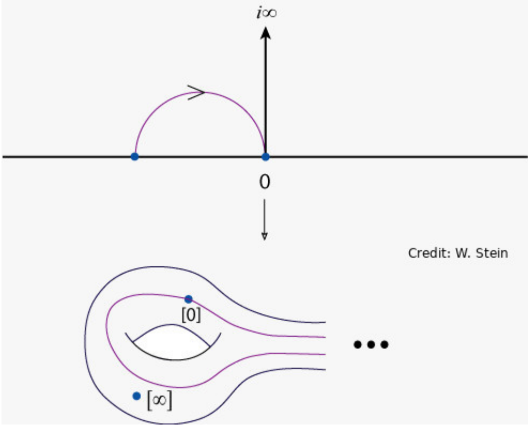
Analytic model of $J_1(\ell N)$

Let $\omega_1, \cdots, \omega_g$ be a basis of $\Omega^1\big(X_1(\ell N)\big) \simeq S_2\big(\Gamma_1(\ell N)\big)$. Integrate the differentials $\omega_i(\tau)d\tau$ along the curves γ_j. This yields a lattice $\Lambda = \left\langle \left(\int_{\gamma_j} \omega_i\right)_{1 \leqslant i \leqslant g} \right\rangle_{1 \leqslant j \leqslant 2g} \subset \mathbb{C}^g$, and $J_1(\ell) = \mathbb{C}^g/\Lambda$.

These curves can be represented by *modular symbols* $\mathbb{S}_2\big(\Gamma_1(\ell N)\big) \subset \mathbb{M}_2\big(\Gamma_1(\ell N)\big)$.

Periods of the modular curve $X_1(\ell N)$

These curves can be represented by *modular symbols* $\mathbb{S}_2(\Gamma_1(\ell N)) \subset \mathbb{M}_2(\Gamma_1(\ell N))$.



Explicit integration

Split the integration path, move the endpoints to ∞.
$\rightsquigarrow$ integrals of the form

$$\int_{\infty}^{z} \left(\sum_{n=1}^{+\infty} \omega_n e^{2\pi i n \tau} \right) d\tau = \frac{1}{2\pi i} \sum_{n=1}^{+\infty} \frac{\omega_n}{n} e^{2\pi i n z},$$

which converge best for $\operatorname{Im} z \gg 0$.

Using the Hecke-module structure

$\mathbb{T}$ also acts on modular symols, and integration is equivariant:

$$\int_{Tw} \omega = \int_{w} T\omega.$$

So, if we have a $\mathbb{T}$-generating family of symbols (w_i) which are easy to integrate along, we can compute the periods:

$$\gamma_j = \sum_i T_{j,i} w_i, \quad T_{j,i} \in \mathbb{T},$$

$$\int_{\gamma_j} \omega = \int_{\sum_i T_{j,i} w_i} \omega = \sum_i \int_{w_i} T_{j,i}\omega = \sum_i \lambda(T_{j,i}, \omega) \int_{w_i} \omega.$$

High precision q-expansions

Let $\omega = \sum_{n=0}^{+\infty} \omega_n q^n \in S_2\big(\Gamma_1(\ell N)\big)$, and let $B \in \mathbb{N}$.

High precision q-expansions

Let $\omega = \sum_{n=0}^{+\infty} \omega_n q^n \in S_2\big(\Gamma_1(\ell N)\big)$, and let $B \in \mathbb{N}$.

Theorem (Manin, 1972)

Using modular symbols, the ω_n can be computed for $n \leqslant B$ in a number of bit operations which is polynomial (but at least quadratic) in B.

High precision q-expansions

Let $\omega = \sum_{n=0}^{+\infty} \omega_n q^n \in S_2\big(\Gamma_1(\ell N)\big)$, and let $B \in \mathbb{N}$.

Theorem (Manin, 1972)

Using modular symbols, the ω_n can be computed for $n \leqslant B$ in a number of bit operations which is polynomial (but at least quadratic) in B.

Theorem (M., 2013)

The ω_n can be computed for $n \leqslant B$ in $\widetilde{O}(B)$ bit operations.

High precision q-expansions

Let $\omega = \sum_{n=0}^{+\infty} \omega_n q^n \in S_2\big(\Gamma_1(\ell N)\big)$, and let $B \in \mathbb{N}$.

1. Bounds are known on the ω_n $\rightsquigarrow$ we compute $\omega_n \bmod \mathfrak{p}$, with $p \mid \mathfrak{p}$ a large enough prime.

High precision q-expansions

Let $\omega = \sum_{n=0}^{+\infty} \omega_n q^n \in S_2\big(\Gamma_1(\ell N)\big)$, and let $B \in \mathbb{N}$.

1. Bounds are known on the ω_n $\rightsquigarrow$ we compute $\omega_n \bmod \mathfrak{p}$, with $p \mid \mathfrak{p}$ a large enough prime.
2. We use $u = \frac{1}{j} = \frac{E_4^3 - E_6^2}{1728\ E_4^3} = \sum_{n=1}^{+\infty} u_n q^n$, the u_n are easy to compute mod p.

High precision q-expansions

Let $\omega = \sum_{n=0}^{+\infty} \omega_n q^n \in S_2\big(\Gamma_1(\ell N)\big)$, and let $B \in \mathbb{N}$.

1. Bounds are known on the $\omega_n \rightsquigarrow$ we compute $\omega_n \bmod \mathfrak{p}$, with $p \mid \mathfrak{p}$ a large enough prime.
2. We use $u = \frac{1}{j} = \frac{E_4^3 - E_6^2}{1728\ E_4^3} = \sum_{n=1}^{+\infty} u_n q^n$, the u_n are easy to compute mod p.
3. There is an equation $\Phi(X, Y) \in \mathbb{F}_{\mathfrak{p}}[X, Y]$ with known degrees such that $\Phi(u, \omega/du) = 0$.

High precision q-expansions

Let $\omega = \sum_{n=0}^{+\infty} \omega_n q^n \in S_2\big(\Gamma_1(\ell N)\big)$, and let $B \in \mathbb{N}$.

1. Bounds are known on the $\omega_n \rightsquigarrow$ we compute $\omega_n \bmod \mathfrak{p}$, with $p \mid \mathfrak{p}$ a large enough prime.
2. We use $u = \frac{1}{j} = \frac{E_4^3 - E_6^2}{1728\ E_4^3} = \sum_{n=1}^{+\infty} u_n q^n$, the u_n are easy to compute mod p.
3. There is an equation $\Phi(X, Y) \in \mathbb{F}_\mathfrak{p}[X, Y]$ with known degrees such that $\Phi(u, \omega/du) = 0$.
4. We compute Φ by identification in $\mathbb{F}_\mathfrak{p}[[q]]$.

High precision q-expansions

Let $\omega = \sum_{n=0}^{+\infty} \omega_n q^n \in S_2\big(\Gamma_1(\ell N)\big)$, and let $B \in \mathbb{N}$.

1. Bounds are known on the $\omega_n \rightsquigarrow$ we compute $\omega_n \bmod \mathfrak{p}$, with $p \mid \mathfrak{p}$ a large enough prime.
2. We use $u = \frac{1}{j} = \frac{E_4^3 - E_6^2}{1728\ E_4^3} = \sum_{n=1}^{+\infty} u_n q^n$, the u_n are easy to compute mod p.
3. There is an equation $\Phi(X, Y) \in \mathbb{F}_\mathfrak{p}[X, Y]$ with known degrees such that $\Phi(u, \omega/du) = 0$.
4. We compute Φ by identification in $\mathbb{F}_\mathfrak{p}[[q]]$.
5. From precomputed u_n for $n \leqslant B$, we compute ω by Newton-iterating on $\Phi(u, \omega/du) = 0$.

Step 2

✓ Period lattice Λ of $X_1(\ell N)$
High accuracy q-expansions, term-by-term integration

$\rightsquigarrow$ analytic model of $J_1(\ell N)$

▶ Approximation over $\mathbb{C}$ of the ℓ-torsion

Computation of divisors $D_1,\ D_2 \in \operatorname{Div}^0\left(X_1(\ell N)\right)$ representing a basis of $V_{f,\mathfrak{l}} \subset J_1(\ell N)$

Evaluation of the ℓ-torsion
Choice of a "well-behaved" function $\alpha\colon V_{f,\mathfrak{l}} \longrightarrow \overline{\mathbb{Q}}$

$\rightsquigarrow$ number field L cut out by $\rho_{f,\mathfrak{l}}$

Frobenius elements

Recipe to compute the image of the Frobenius at p, given $p \nmid \ell N$

The setup

$$V_{f,\mathfrak{l}} \overset{\text{def}}{=} \bigcap_{p \text{ prime}} \operatorname{Ker}\left(T_p - a_p\right)\Big|_{J_1(\ell N)[\ell]}$$
$$= \bigcap_{p \leqslant B} \operatorname{Ker}\left(T_p - a_p\right)\Big|_{J_1(\ell N)[\ell]}$$

for B large enough.

The matrices of $T_p \circlearrowleft J_1(\ell N)[\ell]$ allow us to find

$$x_1, x_2 \in J_1(\ell N)[\ell](\mathbb{C}) = (\mathbb{C}^g/\Lambda)[\ell] = \frac{1}{\ell}\Lambda/\Lambda$$

which form a basis of $V_{f,\mathfrak{l}} \subset J_1(\ell N)[\ell]$.

Goal: compute $D_1,\ D_2 \in \operatorname{Div}^0\left(X_1(\ell N)(\mathbb{C})\right)$ such that

$$[D_k] = x_k.$$

Abel-Jacobi and Newton

We have a target $x \in \mathbb{C}^g/\Lambda$, we want

$$\jmath\left(\sum_n (P_n' - P_n)\right) \overset{\text{def}}{=} \sum_n \left(\int_{P_n}^{P_n'} \omega_i\right)_{1 \leqslant i \leqslant g} = x.$$

Abel-Jacobi and Newton

We have a target $x \in \mathbb{C}^g/\Lambda$, we want

$$\jmath\left(\sum_{n=1}^{g}(P'_n - P_n)\right) \overset{\text{def}}{=} \sum_{n=1}^{g}\left(\int_{P_n}^{P'_n}\omega_i\right)_{1\leqslant i\leqslant g} = x$$

Fix g points $P_1, \cdots, P_g \in X_1(\ell N)(\mathbb{C})$, and solve for $P'_1, \cdots, P'_g$ by Newton iteration in $\mathbb{C}^g$.

Abel-Jacobi and Newton

We have a target $x \in \mathbb{C}^g/\Lambda$, we want

$$\jmath\left(\sum_{n=1}^{g}(P'_n - P_n)\right) \stackrel{\text{def}}{=} \sum_{n=1}^{g}\left(\int_{P_n}^{P'_n}\omega_i\right)_{1\leqslant i\leqslant g} = x$$

Fix g points $P_1, \cdots, P_g \in X_1(\ell N)(\mathbb{C})$, and solve for $P'_1, \cdots, P'_g$ by Newton iteration in $\mathbb{C}^g$.

Poor precision, and likely to diverge...

Abel-Jacobi and Newton

We have a target $x \in \mathbb{C}^g/\Lambda$, we want

$$\jmath\left(\sum_{n=1}^{g}\left({P'}_n^{(m)} - P_n^{(m)}\right)\right) \overset{\text{def}}{=} \sum_{n=1}^{g}\left(\int_{P_n^{(m)}}^{{P'}_n^{(m)}} \omega_i\right)_{1 \leqslant i \leqslant g} = \frac{x}{2^m}$$

Fix g points $P_1^{(m)}, \cdots, P_g^{(m)} \in X_1(\ell N)(\mathbb{C})$, and solve for ${P'}_1^{(m)}, \cdots, {P'}_g^{(m)}$ by Newton iteration in $\mathbb{C}^g$.

Abel-Jacobi and Newton

We have a target $x \in \mathbb{C}^g/\Lambda$, we want

$$\jmath\left(\sum_{n=1}^{g}\left(P'^{(m)}_n - P^{(m)}_n\right)\right) \overset{\text{def}}{=} \sum_{n=1}^{g}\left(\int_{P^{(m)}_n}^{P'^{(m)}_n}\omega_i\right)_{1\leqslant i\leqslant g} = \frac{x}{2^m}$$

Fix g points $P^{(m)}_1, \cdots, P^{(m)}_g \in X_1(\ell N)(\mathbb{C})$, and solve for $P'^{(m)}_1, \cdots, P'^{(m)}_g$ by Newton iteration in $\mathbb{C}^g$.

Proposition (Inverse function theorem)

If $m \gg 0$, then for generic $P^{(m)}_1, \cdots, P^{(m)}_1$, then Newton converges to a solution with $P'^{(m)}_i$ close to $P^{(m)}_i$, $1 \leqslant i \leqslant g$.

Recovering ℓ-torsion divisors

$$[D] = 2^m[D^{(m)}] = \left[\sum_{n=1}^{g} 2^m\left(P'_n - P_n\right)\right] \in J_1(\ell N)[\ell].$$

$\rightsquigarrow$ Use Makdisi's algorithms to double $[D^{(m)}]$ repeatedly.

Step 3

- ✓ Period lattice Λ of $X_1(\ell N)$
  High accuracy q-expansions, term-by-term integration
  $\rightsquigarrow$ analytic model of $J_1(\ell N)$
- ✓ Approximation over $\mathbb{C}$ of the ℓ-torsion
  Computation of divisors D_1, $D_2 \in \mathrm{Div}^0\left(X_1(\ell N)\right)$ representing a basis of $V_{f,\mathfrak{l}} \subset J_1(\ell N)$
- ▶ Evaluation of the ℓ-torsion
  Choice of a "well-behaved" function $\alpha \colon V_{f,\mathfrak{l}} \longrightarrow \overline{\mathbb{Q}}$
  $\rightsquigarrow$ number field L cut out by $\rho_{f,\mathfrak{l}}$
- Frobenius elements
  Recipe to compute the image of the Frobenius at p, given $p \nmid \ell N$

Evaluating the ℓ-torsion

We have computed divisors D_1 and D_2 representing a basis of $V_{f,\mathfrak{l}} \subset J_1(\ell N)[\ell]$.

Evaluating the ℓ-torsion

We have computed divisors D_1 and D_2 representing a basis of $V_{f,\mathfrak{l}} \subset J_1(\ell N)[\ell]$.

Thanks to Makdisi's algorithms, we compute $\mathbb{F}_\ell$-linear combinations of D_1 and D_2
$\rightsquigarrow$ divisors representing all the ℓ^2 points of $V_{f,\mathfrak{l}}$.

Evaluating the ℓ-torsion

We have computed divisors D_1 and D_2 representing a basis of $V_{f,\mathfrak{l}} \subset J_1(\ell N)[\ell]$.

Thanks to Makdisi's algorithms, we compute $\mathbb{F}_\ell$-linear combinations of D_1 and D_2
$\rightsquigarrow$ divisors representing all the ℓ^2 points of $V_{f,\mathfrak{l}}$.

Proposition

Let $\alpha \in \mathbb{Q}\big(J_1(\ell N)\big)$, and let

$$F(x) = \prod_{\substack{D \in V_{f,\mathfrak{l}} \\ D \neq 0}} \big(x - \alpha(D)\big).$$

Then $F(x) \in \mathbb{Q}[x]$.

For generic α, $F(x)$ is irreducible, and its decomposition field is

$$L = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}}.$$

Classical choice of $\alpha \in \mathbb{Q}\big(J_1(\ell N)\big)$

Pick $\xi \in \mathbb{Q}\big(X_1(\ell N)\big)$, and extend it to $J_1(\ell N)$ by

$$\begin{array}{cccc} \alpha : & J_1(\ell N) & \dashrightarrow & \mathbb{C} \\ & \displaystyle\sum_{i=1}^{g} P_i - gO & \longmapsto & \displaystyle\sum_{i=1}^{g} \xi(P_i) \end{array}.$$

Classical choice of $\alpha \in \mathbb{Q}(J_1(\ell N))$

Pick $\xi \in \mathbb{Q}(X_1(\ell N))$, and extend it to $J_1(\ell N)$ by

$$\begin{array}{cccc} \alpha: & J_1(\ell N) & \dashrightarrow & \mathbb{C} \\ & \displaystyle\sum_{i=1}^{g} P_i - gO & \longmapsto & \displaystyle\sum_{i=1}^{g} \xi(P_i) \end{array}.$$

The divisor of poles of α is

$$(\alpha)_\infty = \sum_{Q \text{ pole of } \xi} \tau^*_{[Q-O]}\Theta,$$

so ξ must be chosen with degree as small as possible.

Classical choice of $\alpha \in \mathbb{Q}(J_1(\ell N))$

Pick $\xi \in \mathbb{Q}(X_1(\ell N))$, and extend it to $J_1(\ell N)$ by

$$\begin{array}{cccc} \alpha : & J_1(\ell N) & \dashrightarrow & \mathbb{C} \\ & \sum_{i=1}^{g} P_i - gO & \longmapsto & \sum_{i=1}^{g} \xi(P_i) \end{array}.$$

The divisor of poles of α is

$$(\alpha)_\infty = \sum_{Q \text{ pole of } \xi} \tau^*_{[Q-O]} \Theta,$$

so ξ must be chosen with degree as small as possible.
Unfortunately,

Theorem (Abramovich, 1996)

$$\deg \xi \gtrsim g.$$

Better choice of $\alpha \in \mathbb{Q}\big(J_1(\ell N)\big)$

Points on $J_1(\ell N)$ can be written $E - gO$, $E \geqslant 0$ of degree g. Fix an effective divisor B of degree $2g$. Then

$$H^0(B - E) = \mathbb{C}\phi_E.$$

We can thus define

$$\begin{array}{rccc} \alpha : & J_1(\ell N) & \dashrightarrow & \mathbb{C} \\ & E - gO & \longmapsto & \dfrac{\phi_E(P)}{\phi_E(Q)} \end{array}$$

where $P,\ Q \in X_1(\ell N)(\mathbb{Q})$ are fixed.

Better choice of $\alpha \in \mathbb{Q}\big(J_1(\ell N)\big)$

$$H^0(B - E) = \mathbb{C}\phi_E.$$

We can thus define

$$\begin{array}{rccc} \alpha : & J_1(\ell N) & \dashrightarrow & \mathbb{C} \\ & E - gO & \longmapsto & \dfrac{\phi_E(P)}{\phi_E(Q)} \end{array}$$

where $P,\ Q \in X_1(\ell N)(\mathbb{Q})$ are fixed.

Proposition (M., 2012)

The divisor of poles of α is the sum of only 2 translates of Θ.

Step 4

- ✓ Period lattice Λ of $X_1(\ell N)$

  High accuracy q-expansions, term-by-term integration

  $\rightsquigarrow$ analytic model of $J_1(\ell N)$

- ✓ Approximation over $\mathbb{C}$ of the ℓ-torsion

  Computation of divisors $D_1,\ D_2 \in \operatorname{Div}^0\left(X_1(\ell N)\right)$ representing a basis of $V_{f,\mathfrak{l}} \subset J_1(\ell N)$

- ✓ Evaluation of the ℓ-torsion

  Choice of a "well-behaved" function $\alpha\colon V_{f,\mathfrak{l}} \longrightarrow \overline{\mathbb{Q}}$

  $\rightsquigarrow$ number field L cut out by $\rho_{f,\mathfrak{l}}$

- ▶ Frobenius elements

  Recipe to compute the image of the Frobenius at p, given $p \nmid \ell N$

Summary

We have computed $F(x) \in \mathbb{Q}[x]$ with decomposition field $L = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}}$. We know the roots of $F(x)$ in $\mathbb{C}$ with high accuracy, and the permutation action of $\operatorname{Gal}(L/\mathbb{Q}) \subseteq \operatorname{GL}_2(\mathbb{F}_\ell)$ on them as well.

Summary

We have computed $F(x) \in \mathbb{Q}[x]$ with decomposition field $L = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}}$. We know the roots of $F(x)$ in $\mathbb{C}$ with high accuracy, and the permutation action of $\operatorname{Gal}(L/\mathbb{Q}) \subseteq \operatorname{GL}_2(\mathbb{F}_\ell)$ on them as well.

We must now compute

$$\rho_{f,\mathfrak{l}}(\operatorname{Frob}_p)$$

for prime $p \in \mathbb{N}$.

Summary

We have computed $F(x) \in \mathbb{Q}[x]$ with decomposition field $L = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}}$. We know the roots of $F(x)$ in $\mathbb{C}$ with high accuracy, and the permutation action of $\operatorname{Gal}(L/\mathbb{Q}) \subseteq \operatorname{GL}_2(\mathbb{F}_\ell)$ on them as well.

We must now compute

$$\rho_{f,\mathfrak{l}}(\operatorname{Frob}_p)$$

for prime $p \in \mathbb{N}$.

$$f = q + \sum_{n \geqslant 2} a_n q^n, \qquad \operatorname{Tr} \rho_{f,\mathfrak{l}}(\operatorname{Frob}_p) = a_p \bmod \mathfrak{l}.$$

The Dokchitsers' resolvents

Theorem (T. & V. Dokchitser, 2010)

Let $F(x) \in \mathbb{Q}[x]$ be irreducible, $n = \deg F(x)$, $L \subset \mathbb{C}$ its decomposition field, and $a_i \in \mathbb{C}$ its roots.

The Dokchitsers' resolvents

Theorem (T. & V. Dokchitser, 2010)

Let $F(x) \in \mathbb{Q}[x]$ be irreducible, $n = \deg F(x)$, $L \subset \mathbb{C}$ its decomposition field, and $a_i \in \mathbb{C}$ its roots.

For almost all $h(x) \in \mathbb{Z}[x]_{n-1}$, the resolvents

$$\Gamma_C(x) = \prod_{\sigma \in C} \left(x - \sum_{i=1}^{n} h(a_i)\sigma(a_i) \right) \in \mathbb{Q}[x],$$

C conjugacy class of $\operatorname{Gal}(L/\mathbb{Q})$, are pairwise coprime.

The Dokchitsers' resolvents

Theorem (T. & V. Dokchitser, 2010)

For almost all $h(x) \in \mathbb{Z}[x]_{n-1}$, the resolvents

$$\Gamma_C(x) = \prod_{\sigma \in C} \left(x - \sum_{i=1}^{n} h(a_i)\sigma(a_i) \right) \in \mathbb{Q}[x],$$

C conjugacy class of $\mathrm{Gal}(L/\mathbb{Q})$, are pairwise coprime.

For each prime $p \in \mathbb{N}$ such that $F(x)$ is defined and squarefree mod p, let

$$\mathbb{F}_p[a] = \mathbb{F}_p[x] / \big(F(x) \bmod p \big), \quad u = \mathrm{Tr}_{\mathbb{F}_p[a]/\mathbb{F}_p} h(a) a^p \in \mathbb{F}_p.$$

The Dokchitsers' resolvents

Theorem (T. & V. Dokchitser, 2010)

For almost all $h(x) \in \mathbb{Z}[x]_{n-1}$, the resolvents

$$\Gamma_C(x) = \prod_{\sigma \in C} \left(x - \sum_{i=1}^{n} h(a_i)\sigma(a_i) \right) \in \mathbb{Q}[x],$$

C conjugacy class of $\mathrm{Gal}(L/\mathbb{Q})$, are pairwise coprime.

For each prime $p \in \mathbb{N}$ such that $F(x)$ is defined and squarefree mod p, let

$$\mathbb{F}_p[a] = \mathbb{F}_p[x]/\big(F(x) \bmod p\big), \quad u = \mathrm{Tr}_{\mathbb{F}_p[a]/\mathbb{F}_p} h(a)a^p \in \mathbb{F}_p.$$

$$\text{Then } \mathrm{Frob}_p \in C \Longrightarrow \Gamma_C(u) = 0 \bmod p.$$

$F(x)$ is HUGE

Problem

The degree of $F(x)$ is large ($\approx \ell^2$), and its coefficients are huge, so the coefficients of $\Gamma_C(x)$ are huge$^{\ell^2}$.

There are algorithms to reduce a polynomial, that is to say compute another polynomial defining the same number field. But $F(x)$ is simply too big for them.

The projective representation

Instead, we could consider the projective representation

$$\rho^{\text{proj}} \colon \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell).$$

The projective representation

Instead, we could consider the projective representation

$$\rho^{\text{proj}} \colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \operatorname{GL}_2(\mathbb{F}_\ell) \longrightarrow \operatorname{PGL}_2(\mathbb{F}_\ell).$$

This corresponds to

$$F^{\text{proj}}(x) = \prod_{w \in \mathbb{P}^1\mathbb{F}_\ell} \left(x - \sum_{\substack{D \in w \\ D \neq 0}} \alpha(D) \right) \in \mathbb{Q}[X],$$

which is of degree $\ell + 1$ only, and can thus be reduced.

Quotient representations

More generally, for $S \leqslant \mathbb{F}_\ell^*$ embedded diagonally into $\mathrm{GL}_2(\mathbb{F}_\ell)$, we can consider

$$\rho^S : \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S.$$

Quotient representations

More generally, for $S \leqslant \mathbb{F}_\ell^*$ embedded diagonally into $\mathrm{GL}_2(\mathbb{F}_\ell)$, we can consider

$$\rho^S\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S.$$

Fact

Let $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that we know its image in $\mathrm{GL}_2(\mathbb{F}_\ell)/S$ and $\det A$. If $-1 \notin S$, we can recover A.

Quotient representations

More generally, for $S \leqslant \mathbb{F}_\ell^*$ embedded diagonally into $\mathrm{GL}_2(\mathbb{F}_\ell)$, we can consider

$$\rho^S : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S.$$

Fact

Let $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that we know its image in $\mathrm{GL}_2(\mathbb{F}_\ell)/S$ and $\det A$. If $-1 \notin S$, we can recover A.

As $\det \rho_{f,\mathfrak{l}} = \varepsilon \chi_\ell^{k-1}$ is known, we consider

$$\mathbb{F}_\ell^* = S_0 \underset{2}{>} S_1 \underset{2}{>} \cdots \underset{2}{>} S_r \not\ni -1,$$

where $r = \mathrm{ord}_2(\ell - 1)$, and the associated $F_i(x) := F^{S_i}(x)$.

Quotient representations

More generally, for $S \leqslant \mathbb{F}_\ell^*$ embedded diagonally into $\mathrm{GL}_2(\mathbb{F}_\ell)$, we can consider

$$\rho^S : \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S.$$

Fact

Let $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that we know its image in $\mathrm{GL}_2(\mathbb{F}_\ell)/S$ and $\det A$. If $-1 \notin S$, we can recover A.

As $\det \rho_{f,\mathfrak{l}} = \varepsilon \chi_\ell^{k-1}$ is known, we consider

$$\mathbb{F}_\ell^* = S_0 \underset{2}{>} S_1 \underset{2}{>} \cdots \underset{2}{>} S_r \not\ni -1,$$

where $r = \mathrm{ord}_2(\ell - 1)$, and the associated $F_i(x) := F^{S_i}(x)$.

We now focus on $F_r(x)$ instead of $F(x)$.

Reduction of the polynomials

First, we can reduce $F_0(x)$, whose degree is only $\ell + 1$.

Reduction of the polynomials

First, we can reduce $F_0(x)$, whose degree is only $\ell + 1$.

Then, we write $K_i = \mathbb{Q}[x]/F_i(x)$, so that

$$K_{i+1} = K_i(\sqrt{\Delta_i}), \quad \Delta_i \in K_i.$$

We can inductively reduce the $F_i(x)$, by writing $\Delta_i = A_i^2 \delta_i$ in K_i with δ_i small.

The fields

The filtration

$$\mathbb{F}_\ell^* = S_0 \underset{2}{\supsetneq} S_1 \underset{2}{\supsetneq} \cdots \underset{2}{\supsetneq} S_r = S \not\ni -1$$

yields a tower of quadratic extensions

$$L_0 \underset{2}{\subsetneq} L_1 \underset{2}{\subsetneq} \cdots \underset{2}{\subsetneq} L_r,$$

where $L_i = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}^{S_i}}$.

The fields

The filtration

$$\mathbb{F}_\ell^* = S_0 \underset{2}{\supsetneq} S_1 \underset{2}{\supsetneq} \cdots \underset{2}{\supsetneq} S_r = S \not\ni -1$$

yields a tower of quadratic extensions

$$L_0 \underset{2}{\subsetneq} L_1 \underset{2}{\subsetneq} \cdots \underset{2}{\subsetneq} L_r,$$

where $L_i = \overline{\mathbb{Q}}^{\operatorname{Ker} \rho_{f,\mathfrak{l}}^{S_i}}$.

Proposition

$$L = L_r \underbrace{L_{\det \rho_{f,\mathfrak{l}}}}_{\subseteq \mathbb{Q}(\zeta_M)}.$$

Certification of the output

Certification

We have identified the coefficients of

$$F(x) = \prod_{\substack{D \in V_{f,\mathfrak{l}} \\ D \neq 0}} \big(x - \alpha(D)\big) \in \mathbb{Q}[x],$$

beyond reasonable doubt, but this is not rigorous.

Certification

We have identified the coefficients of

$$F(x) = \prod_{\substack{D \in V_{f,\mathfrak{l}} \\ D \neq 0}} \left(x - \alpha(D)\right) \in \mathbb{Q}[x],$$

beyond reasonable doubt, but this is not rigorous.

Question

How do we certify that $F(x)$ defines $\rho_{f,\mathfrak{l}}$?

Certification

We have identified the coefficients of

$$F(x) = \prod_{\substack{D \in V_{f,\mathfrak{l}} \\ D \neq 0}} \big(x - \alpha(D)\big) \in \mathbb{Q}[x],$$

beyond reasonable doubt, but this is not rigorous.

Question

How do we certify that $F(x)$ defines $\rho_{f,\mathfrak{l}}$?

For simplicity, we will assume that f and $\mathfrak{l}$ are such that $\ell \geqslant 5$, $N = 1$, and that $\operatorname{Im} \rho_{f,\mathfrak{l}} = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Certification

We have identified the coefficients of

$$F(x) = \prod_{\substack{D \in V_{f,\mathfrak{l}} \\ D \neq 0}} \big(x - \alpha(D)\big) \in \mathbb{Q}[x],$$

beyond reasonable doubt, but this is not rigorous.

Question

How do we certify that $F(x)$ defines $\rho_{f,\mathfrak{l}}$?

For simplicity, we will assume that f and $\mathfrak{l}$ are such that $\ell \geqslant 5$, $N = 1$, and that $\operatorname{Im} \rho_{f,\mathfrak{l}} = \mathrm{GL}_2(\mathbb{F}_\ell)$.

We must prove that

1. $\mathrm{Gal}_{\mathbb{Q}}(F) \circlearrowleft \{\alpha(D)\}$ is permutation-isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell) \circlearrowleft {\mathbb{F}_\ell}^2 - \{0\}$,
2. the corresponding Galois representation ϱ is $\rho_{f,\mathfrak{l}}$.

Certification

We have identified the coefficients of

$$F(x) = \prod_{\substack{D \in V_{f,\mathfrak{l}} \\ D \neq 0}} \left(x - \alpha(D) \right) \in \mathbb{Q}[x],$$

beyond reasonable doubt, but this is not rigorous.

Question

How do we certify that $F(x)$ defines $\rho_{f,\mathfrak{l}}$?

For simplicity, we will assume that f and $\mathfrak{l}$ are such that $\ell \geqslant 5$, $N = 1$, and that $\operatorname{Im} \rho_{f,\mathfrak{l}} = \mathrm{GL}_2(\mathbb{F}_\ell)$.

We must prove that

1. $\mathrm{Gal}_{\mathbb{Q}}(F) \circlearrowleft \{\alpha(D)\}$ is permutation-isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell) \circlearrowleft {\mathbb{F}_\ell}^2 - \{0\}$
   $\rightsquigarrow$ compute $\mathrm{Gal}_{\mathbb{Q}}(F)$ with Magma,
2. the corresponding Galois representation ϱ is $\rho_{f,\mathfrak{l}}$.

Certification

We have identified the coefficients of

$$F(x) = \prod_{\substack{D \in V_{f,\mathfrak{l}} \\ D \neq 0}} \left(x - \alpha(D)\right) \in \mathbb{Q}[x],$$

beyond reasonable doubt, but this is not rigorous.

Question

How do we certify that $F(x)$ defines $\rho_{f,\mathfrak{l}}$?

For simplicity, we will assume that f and $\mathfrak{l}$ are such that $\ell \geqslant 5$, $N = 1$, and that $\operatorname{Im} \rho_{f,\mathfrak{l}} = \mathrm{GL}_2(\mathbb{F}_\ell)$.

We must prove that

1. $\mathrm{Gal}_{\mathbb{Q}}(F) \circlearrowleft \{\alpha(D)\}$ is permutation-isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell) \circlearrowleft {\mathbb{F}_\ell}^2 - \{0\}$
   $\rightsquigarrow$ compute $\mathrm{Gal}_{\mathbb{Q}}(F)$ with Magma,
2. the corresponding Galois representation ϱ is $\rho_{f,\mathfrak{l}}$
   $\rightsquigarrow$ use Serre's modularity conjecture.

Serre's modularity conjecture

Theorem (Khare+Wintenberger, 2009)

Let $c \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the complex conjugation, and let

$$\rho\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{GL}_2(\mathbb{F}_\ell)$$

be an irreducible Galois representation such that $\det \rho(c) = -1$. Then there exists a newform $f \in S_{k_\rho}\big(\Gamma_1(N_\rho), \varepsilon_\rho\big)$ and a prime $\mathfrak{l} | \ell$ such that

$$\rho \sim \rho_{f,\mathfrak{l}}.$$

Moreover, there are explicit recipes to compute N_ρ, k_ρ and ε_ρ.

Proof of the projective Galois group

Let $x, y, z, t \in \mathbb{P}^1\mathbb{F}_\ell$ be pairwise distinct. Their cross-ratio is by definition $\gamma(t)$, where $\gamma \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ is the only element sending (x, y, z) to $(\infty, 0, 1)$.

Proof of the projective Galois group

Let $x, y, z, t \in \mathbb{P}^1\mathbb{F}_\ell$ be pairwise distinct. Their cross-ratio is by definition $\gamma(t)$, where $\gamma \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ is the only element sending (x, y, z) to $(\infty, 0, 1)$.

Proposition

Let γ be a permutation of $\mathbb{P}^1\mathbb{F}_\ell$. Then

$$\gamma \text{ preserves cross-ratios} \iff \gamma \in \mathrm{PGL}_2(\mathbb{F}_\ell).$$

Proof of the projective Galois group

Proposition

Let γ be a permutation of $\mathbb{P}^1\mathbb{F}_\ell$. Then

$$\gamma \text{ preserves cross-ratios} \iff \gamma \in \mathrm{PGL}_2(\mathbb{F}_\ell).$$

Let $\left(\beta_w = \sum_{0\neq D\in w} \alpha(D)\right)_{w\in\mathbb{P}^1\mathbb{F}_\ell}$ be the roots of $F^{\text{proj}}(x)$, and let $\lambda_1, \cdots, \lambda_4$ be distinct integers. We compute

$$R_4(x) = \prod_{\substack{w_1,\cdots,w_4 \\ \text{distinct}}} \left(x - \sum_{m=1}^{4} \lambda_m \beta_{w_m} \right) \in \mathbb{Z}[x].$$

If $R_4(x)$ is squarefree and factors along cross-ratios, this proves that $\mathrm{Gal}_{\mathbb{Q}}(F^{\text{proj}}) \leqslant \mathrm{PGL}_2(\mathbb{F}_\ell)$.

Proof of the projective Galois group

We can define the *unordered cross-ratio* map

$$u \colon \begin{array}{ccc} \binom{\mathbb{P}^1(\mathbb{F}_\ell)}{4} & \longrightarrow & \mathbb{F}_\ell \\ \{x,y,z,t\} & \longmapsto & j([x,y,z,t]) \end{array},$$

where $j(\lambda) = 256\frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}$.

Proof of the projective Galois group

We can define the *unordered cross-ratio* map

$$u : \begin{array}{ccc} \binom{\mathbb{P}^1(\mathbb{F}_\ell)}{4} & \longrightarrow & \mathbb{F}_\ell \\ \{x,y,z,t\} & \longmapsto & j([x,y,z,t]) \end{array},$$

where $j(\lambda) = 256\frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}$.

Theorem (M., 2016)

1. $\forall \ell \geqslant 5$, $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is a maximal subgroup of $\mathfrak{S}_{\mathbb{P}^1(\mathbb{F}_\ell)}$.
2. $\forall \ell \neq 5$, $\gamma \circlearrowleft \mathbb{P}^1(\mathbb{F}_\ell)$ preserves $u \iff \gamma \in \mathrm{PGL}_2(\mathbb{F}_\ell)$.

Proof of the projective Galois group

Theorem (M., 2016)

1. $\forall \ell \geqslant 5$, $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is a maximal subgroup of $\mathfrak{S}_{\mathbb{P}^1(\mathbb{F}_\ell)}$.
2. $\forall \ell \neq 5$, $\gamma \circlearrowleft \mathbb{P}^1(\mathbb{F}_\ell)$ preserves $u \iff \gamma \in \mathrm{PGL}_2(\mathbb{F}_\ell)$.

Instead of

$$R_4(x) = \prod_{\substack{w_1, \cdots, w_4 \\ \text{distinct}}} \left(x - \sum_{m=1}^{4} \nu_m \beta_{w_m} \right) \in \mathbb{Z}[x],$$

for $\ell \neq 5$ we may use

$$R_{4,\mathrm{sym}}(x) = \prod_{W \in \binom{\mathbb{P}^1(\mathbb{F}_\ell)}{4}} \left(x - \sum_{w \in W} \beta_w \right) \in \mathbb{Z}[X]$$

whose degree is 24 times smaller.

Proof of the projective representation

Theorem(Projective Serre) (Moon+Taguchi 2003, Bosman 2007)

Let $\pi\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{PGL}_2(\mathbb{F}_\ell)$ be an irreducible projective Galois representation such that $\pi(c)$ fixes exactly two points of $\mathbb{P}^1\mathbb{F}_\ell$. If the discriminant of the field corresponding to $\pi^{-1}\left(\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\right)$ is of the form $\pm\ell^{\ell+k-2}$ for some $k \geqslant 3$, then there exists a newform $f \in S_k(1)$ and a prime $\mathfrak{l}|\ell$ such that $\pi \sim \rho_{f,\mathfrak{l}}^{\text{proj}}$.

Proof of the projective representation

Theorem(Projective Serre) (Moon+Taguchi 2003, Bosman 2007)

Let $\pi\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{PGL}_2(\mathbb{F}_\ell)$ be an irreducible projective Galois representation such that $\pi(c)$ fixes exactly two points of $\mathbb{P}^1\mathbb{F}_\ell$. If the discriminant of the field corresponding to $\pi^{-1}\left(\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]\right)$ is of the form $\pm\ell^{\ell+k-2}$ for some $k \geqslant 3$, then there exists a newform $f \in S_k(1)$ and a prime $\mathfrak{l} | \ell$ such that $\pi \sim \rho_{f,\mathfrak{l}}^{\text{proj}}$.

To make sure we have the right f, we use the fact that for prime $v \nmid \operatorname{Disc}\left(F^{\text{proj}}(x)\right)$,

$$\begin{aligned} a_v(f) \equiv 0 \bmod \mathfrak{l} \quad &\Longleftrightarrow \quad \rho_{f,\mathfrak{l}}(\operatorname{Frob}_v) \text{ is of order } 2 \\ &\Longleftrightarrow \quad F^{\text{proj}}(x) \bmod v \text{ splits into linear or quadratic factors, and is not completely split.} \end{aligned}$$

Switching to p-adics

Later on, we will need to work on p-adic numbers instead of complex ones.

Switching to p-adics

Later on, we will need to work on p-adic numbers instead of complex ones.

We fix a large prime $p \in \mathbb{N}$ such that the $F_i(x)$ are irreducible mod p, and we will work with the roots of the $F_i(x)$ in $\overline{\mathbb{Q}_p}$ from now on.

Switching to p-adics

Later on, we will need to work on p-adic numbers instead of complex ones.

We fix a large prime $p \in \mathbb{N}$ such that the $F_i(x)$ are irreducible mod p, and we will work with the roots of the $F_i(x)$ in $\overline{\mathbb{Q}_p}$ from now on.

Unfortunately, we have thus thrown away the indexation of the roots. We will have to recover it at some point.

The higher Galois groups

For each $i \leqslant r$, let

- $K_i = \mathbb{Q}[x]/F_i(x)$ the root field of $F_i(x)$,
- L_i be the splitting field of $F_i(x)$,
- Z_i the set of p-adic roots of $F_i(x)$,
- and write $V_i = ({\mathbb{F}_\ell}^2 - \{0\})/S_i$.

The higher Galois groups

For each $i \leqslant r$, let

- $K_i = \mathbb{Q}[x]/F_i(x)$ the root field of $F_i(x)$,
- L_i be the splitting field of $F_i(x)$,
- Z_i the set of p-adic roots of $F_i(x)$,
- and write $V_i = ({\mathbb{F}_\ell}^2 - \{0\})/S_i$.

We want to find a compatible system of isomorphisms $Z_i \simeq V_i$ and $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$.

The higher Galois groups

For each $i \leqslant r$, let

- $K_i = \mathbb{Q}[x]/F_i(x)$ the root field of $F_i(x)$,
- L_i be the splitting field of $F_i(x)$,
- Z_i the set of p-adic roots of $F_i(x)$,
- and write $V_i = ({\mathbb{F}_\ell}^2 - \{0\})/S_i$.

We want to find a compatible system of isomorphisms $Z_i \simeq V_i$ and $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$.

For now, all we know is that

$$\mathrm{Gal}(L_0/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell) \circlearrowright \mathbb{P}^1\mathbb{F}_\ell.$$

The Galois closures are not too big

We know that $K_{i+1} = K_i(\sqrt{\delta_i})$ is quadratic over K_i, and that L_i is the Galois closure of K_i.

The Galois closures are not too big

We know that $K_{i+1} = K_i(\sqrt{\delta_i})$ is quadratic over K_i, and that L_i is the Galois closure of K_i.

It is reasonable to assume that $K_i = \mathbb{Q}(\delta_i) \simeq \mathbb{Q}[x]/d_i(x)$.

The Galois closures are not too big

We know that $K_{i+1} = K_i(\sqrt{\delta_i})$ is quadratic over K_i, and that L_i is the Galois closure of K_i.

It is reasonable to assume that $K_i = \mathbb{Q}(\delta_i) \simeq \mathbb{Q}[x]/d_i(x)$.

- We can check that L_{i+1}/L_i is at most quadratic, by studying how

$$\operatorname{Res}_y \left(d_i(x^2 y), d_i(y) \right) = \text{Cst.} \prod_{\sigma(\delta_i) \neq \tau(\delta_i)} \left(x^2 - \frac{\sigma(\delta_i)}{\tau(\delta_i)} \right)$$

factors over subfields of $\mathbb{Q}(\mu_\ell)$.

The Galois closures are not too big

We know that $K_{i+1} = K_i(\sqrt{\delta_i})$ is quadratic over K_i, and that L_i is the Galois closure of K_i.

It is reasonable to assume that $K_i = \mathbb{Q}(\delta_i) \simeq \mathbb{Q}[x]/d_i(x)$.

- We can check that L_{i+1}/L_i is at most quadratic, by studying how

$$\operatorname{Res}_y \left(d_i(x^2 y), d_i(y)\right) = \text{Cst.} \prod_{\sigma(\delta_i) \neq \tau(\delta_i)} \left(x^2 - \frac{\sigma(\delta_i)}{\tau(\delta_i)}\right)$$

  factors over subfields of $\mathbb{Q}(\mu_\ell)$.
- We can check that $L_{i+1} \neq L_i$ by finding a prime $v \in \mathbb{N}$ such that $F_i(x)$ splits completely mod v but $F_{i+1}(x)$ does not.

A classification theorem

Theorem (Quer, 1995)

Let $i \in \mathbb{N}$.

1. $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big) \simeq C_2 \times C_2$, so there are 4 central extensions
$$1 \longrightarrow C_{2^i} \longrightarrow \tilde{G} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1.$$
Write the corresponding normalised cocycles as $\beta_1 = 1$, $\beta_{\det}$, β_+ and β_-, and the corresponding central extensions as $C_{2^i} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$.

A classification theorem

Theorem (Quer, 1995)

Let $i \in \mathbb{N}$.

1. $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big) \simeq C_2 \times C_2$, so there are 4 central extensions
$$1 \longrightarrow C_{2^i} \longrightarrow \tilde{G} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1.$$
Write the corresponding normalised cocycles as $\beta_1 = 1$, $\beta_{\det}$, β_+ and β_-, and the corresponding central extensions as $C_{2^i} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$.
2. If $i = 1$, then for all $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ of order exactly 2,
   - $\beta_1(g, g) = 1$,
   - $\beta_{\det}(g, g) = 1 \iff g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$,
   - $\beta_+(g, g) = 1 \iff g \notin \mathrm{PSL}_2(\mathbb{F}_\ell)$,
   - $\beta_-(g, g) = -1$.

A classification theorem

Theorem (Quer, 1995)

Let $i \in \mathbb{N}$.

1. $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big) \simeq C_2 \times C_2$.
2. If $i = 1$, then for all $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ of order exactly 2,
   - $\beta_1(g,g) = 1$,
   - $\beta_{\det}(g,g) = 1 \iff g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$,
   - $\beta_+(g,g) = 1 \iff g \notin \mathrm{PSL}_2(\mathbb{F}_\ell)$,
   - $\beta_-(g,g) = -1$.
3. If $i \geqslant 2$,
   - $\big(C_{2^i} \times \mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^i} \times C_2$,
   - $\big(2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^{i+1}}$,
   - $\big(2^i_{+}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^i}$,
   - $\big(2^i_{-}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^{i-1}} \times C_2$.

A classification theorem

Theorem (Quer, 1995)

Let $i \in \mathbb{N}$.

1. $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big) \simeq C_2 \times C_2$, so there are 4 central extensions
$$1 \longrightarrow C_{2^i} \longrightarrow \tilde{G} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1.$$
Write the corresponding normalised cocycles as $\beta_1 = 1$, $\beta_{\det}$, β_+ and β_-, and the corresponding central extensions as $C_{2^i} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$.

A classification theorem

Theorem (Quer, 1995)

Let $i \in \mathbb{N}$.

1. $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big) \simeq C_2 \times C_2$, so there are 4 central extensions
$$1 \longrightarrow C_{2^i} \longrightarrow \tilde{G} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1.$$
Write the corresponding normalised cocycles as $\beta_1 = 1$, $\beta_{\det}$, β_+ and β_-, and the corresponding central extensions as $C_{2^i} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$.
2. If $i = 1$, then for all $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ of order exactly 2,
   - $\beta_1(g, g) = 1$,
   - $\beta_{\det}(g, g) = 1 \iff g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$,
   - $\beta_+(g, g) = 1 \iff g \notin \mathrm{PSL}_2(\mathbb{F}_\ell)$,
   - $\beta_-(g, g) = -1$.

A classification theorem

Theorem (Quer, 1995)

Let $i \in \mathbb{N}$.

1. $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), C_{2^i}\big) \simeq C_2 \times C_2$.
2. If $i = 1$, then for all $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ of order exactly 2,
   - $\beta_1(g,g) = 1$,
   - $\beta_{\mathrm{det}}(g,g) = 1 \iff g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$,
   - $\beta_+(g,g) = 1 \iff g \notin \mathrm{PSL}_2(\mathbb{F}_\ell)$,
   - $\beta_-(g,g) = -1$.
3. If $i \geqslant 2$,
   - $\big(C_{2^i} \times \mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^i} \times C_2$,
   - $\big(2^i_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^{i+1}}$,
   - $\big(2^i_{+}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^i}$,
   - $\big(2^i_{-}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq C_{2^{i-1}} \times C_2$.

$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$

Lemma

Let $1 \longrightarrow C_2 \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$ be an extension with normalised cocycle $\beta \in H^2(G, C_2)$, and let $g \in G$ of order 2. Then the lifts of g have order 2 if $\beta(g, g) = 1$, and order 4 else.

$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$

Lemma

Let $1 \longrightarrow C_2 \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$ be an extension with normalised cocycle $\beta \in H^2(G, C_2)$, and let $g \in G$ of order 2. Then the lifts of g have order 2 if $\beta(g, g) = 1$, and order 4 else.

Thanks to the complex conjugation, we deduce that

$$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \begin{cases} 2_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell), & \ell \equiv 1 \bmod 4, \\ 2_{+}\mathrm{PGL}_2(\mathbb{F}_\ell), & \ell \equiv -1 \bmod 4, \end{cases}$$

$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$

Lemma

Let $1 \longrightarrow C_2 \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$ be an extension with normalised cocycle $\beta \in H^2(G, C_2)$, and let $g \in G$ of order 2. Then the lifts of g have order 2 if $\beta(g,g) = 1$, and order 4 else.

Thanks to the complex conjugation, we deduce that

$$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \begin{cases} 2_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell), & \ell \equiv 1 \bmod 4, \\ 2_{+}\mathrm{PGL}_2(\mathbb{F}_\ell), & \ell \equiv -1 \bmod 4, \end{cases}$$

and that the same goes for $\mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$.

$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$

Lemma

Let $1 \longrightarrow C_2 \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$ be an extension with normalised cocycle $\beta \in H^2(G, C_2)$, and let $g \in G$ of order 2. Then the lifts of g have order 2 if $\beta(g, g) = 1$, and order 4 else.

$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$

Lemma

Let $1 \longrightarrow C_2 \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$ be an extension with normalised cocycle $\beta \in H^2(G, C_2)$, and let $g \in G$ of order 2. Then the lifts of g have order 2 if $\beta(g,g) = 1$, and order 4 else.

Thanks to the complex conjugation, we deduce that

$$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \begin{cases} 2_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell), & \ell \equiv 1 \bmod 4, \\ 2_{+}\mathrm{PGL}_2(\mathbb{F}_\ell), & \ell \equiv -1 \bmod 4, \end{cases}$$

$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$

Lemma

Let $1 \longrightarrow C_2 \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$ be an extension with normalised cocycle $\beta \in H^2(G, C_2)$, and let $g \in G$ of order 2. Then the lifts of g have order 2 if $\beta(g,g) = 1$, and order 4 else.

Thanks to the complex conjugation, we deduce that

$$\mathrm{Gal}(L_1/\mathbb{Q}) \simeq \begin{cases} 2_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell), & \ell \equiv 1 \bmod 4, \\ 2_{+}\mathrm{PGL}_2(\mathbb{F}_\ell), & \ell \equiv -1 \bmod 4, \end{cases}$$

and that the same goes for $\mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$.

Going up and down

Since $r = 1$ when $\ell \equiv -1 \bmod 4$, we now assume $\ell \equiv 1 \bmod 4$.

Going up and down

Since $r = 1$ when $\ell \equiv -1 \bmod 4$, we now assume $\ell \equiv 1 \bmod 4$.

$\mathrm{Gal}(L_i/\mathbb{Q})$ is an extension of $\mathrm{Gal}(L_{i-1}/\mathbb{Q})$ by C_2. We prove by induction on i that it is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by C_{2^i}, and that this extension is central.

Going up and down

Since $r = 1$ when $\ell \equiv -1 \bmod 4$, we now assume $\ell \equiv 1 \bmod 4$.

$\mathrm{Gal}(L_i/\mathbb{Q})$ is an extension of $\mathrm{Gal}(L_{i-1}/\mathbb{Q})$ by C_2. We prove by induction on i that it is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by C_{2^i}, and that this extension is central.

We deduce from the abelianisations that

$$\mathrm{Gal}(L_r/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_r.$$

Going up and down

Since $r = 1$ when $\ell \equiv -1 \bmod 4$, we now assume $\ell \equiv 1 \bmod 4$.

$\mathrm{Gal}(L_i/\mathbb{Q})$ is an extension of $\mathrm{Gal}(L_{i-1}/\mathbb{Q})$ by C_2. We prove by induction on i that it is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by C_{2^i}, and that this extension is central.

We deduce from the abelianisations that

$$\mathrm{Gal}(L_r/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_r.$$

More generally, we see that

$$\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i \simeq \begin{cases} \mathrm{PGL}_2(\mathbb{F}_\ell), & i = 0, \\ 2^i_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell), & 0 < i < r, \\ 2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell), & i = r. \end{cases}$$

The action of Galois

We now know that $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ as an abstract group, so we get Galois representations ϱ_i.

But is its action on the roots of $F_i(x)$ equivalent to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i \circlearrowleft V_i$?

The action of Galois

We now know that $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ as an abstract group, so we get Galois representations ϱ_i.

But is its action on the roots of $F_i(x)$ equivalent to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i \circlearrowleft V_i$?

By construction, the image of the stabilizer of a root of $F_1(x)$ is conjugate to a subgroup of index 2 of $\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right] < \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$.

The action of Galois

We now know that $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ as an abstract group, so we get Galois representations ϱ_i.

But is its action on the roots of $F_i(x)$ equivalent to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i \circlearrowleft V_i$?

By construction, the image of the stabilizer of a root of $F_1(x)$ is conjugate to a subgroup of index 2 of $\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right] < \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$.

So it must be either

- $H_\uparrow = \left\{ \left[\begin{smallmatrix} x & * \\ 0 & * \end{smallmatrix}\right] \mid x \in \mathbb{F}_\ell^{*2} \right\}$, or
- $H_\downarrow = \left\{ \left[\begin{smallmatrix} * & * \\ 0 & y \end{smallmatrix}\right] \mid y \in \mathbb{F}_\ell^{*2} \right\}$, or
- $H_\updownarrow = \left\{ \left[\begin{smallmatrix} x & * \\ 0 & y \end{smallmatrix}\right] \mid xy \in \mathbb{F}_\ell^{*2} \right\}$.

The action of Galois

By construction, the image of the stabilizer of a root of $F_1(x)$ is conjugate to a subgroup of index 2 of $\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right] < \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$.

So it must be either

- $H_\uparrow = \left\{ \left[\begin{smallmatrix} x & * \\ 0 & * \end{smallmatrix}\right] \mid x \in \mathbb{F}_\ell^{*2} \right\}$, or
- $H_\downarrow = \left\{ \left[\begin{smallmatrix} * & * \\ 0 & y \end{smallmatrix}\right] \mid y \in \mathbb{F}_\ell^{*2} \right\}$, or
- $H_\updownarrow = \left\{ \left[\begin{smallmatrix} x & * \\ 0 & y \end{smallmatrix}\right] \mid xy \in \mathbb{F}_\ell^{*2} \right\}$.

But

$$\bigcap_g g H_\updownarrow g^{-1} \ni \left[\begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon \end{smallmatrix}\right] \neq 1$$

for $\epsilon \notin \mathbb{F}_\ell^{*2}$, so $H_\updownarrow$ corresponds to a non-faithful action of $\mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$.

The action of Galois

By construction, the image of the stabilizer of a root of $F_1(x)$ is conjugate to a subgroup of index 2 of $\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right] < \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$.

So it must be either

- $H_\uparrow = \left\{ \left[\begin{smallmatrix} x & * \\ 0 & * \end{smallmatrix}\right] \mid x \in \mathbb{F}_\ell^{*2} \right\}$, or
- $H_\downarrow = \left\{ \left[\begin{smallmatrix} * & * \\ 0 & y \end{smallmatrix}\right] \mid y \in \mathbb{F}_\ell^{*2} \right\}$, or
- $H_\updownarrow = \left\{ \left[\begin{smallmatrix} x & * \\ 0 & y \end{smallmatrix}\right] \mid xy \in \mathbb{F}_\ell^{*2} \right\}$.

$H_\updownarrow$ corresponds to a non-faithful action of $\mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^{*2}$.

After twisting by the automorphism $A \mapsto \frac{1}{\det A} A$ which swaps $H_\uparrow$ and $H_\downarrow$, we can suppose that the stabilizer is $H_\uparrow$.

Are the representations correct ?

Now we know that

$$\mathrm{Gal}(F_i) = \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$$

in a compatible way, we get a compatible collection of representations

$$\varrho_i : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S_i.$$

We want to show that

$$\rho_r \sim \rho_{f,\mathfrak{l}}^{S_r}.$$

Recovering the indexation of the roots

We can index the p-adic roots of $F_0(x)$ by $\mathbb{P}^1\mathbb{F}_\ell$ thanks to our Galois group computation, and then compute

$$\varrho_0(\mathrm{Frob}_p) = \overline{\Phi} \in \mathrm{PGL}_2(\mathbb{F}_\ell)$$

by looking at Frob_p acting on them.

Recovering the indexation of the roots

We can index the p-adic roots of $F_0(x)$ by $\mathbb{P}^1\mathbb{F}_\ell$ thanks to our Galois group computation, and then compute

$$\varrho_0(\mathrm{Frob}_p) = \overline{\Phi} \in \mathrm{PGL}_2(\mathbb{F}_\ell)$$

by looking at Frob_p acting on them.

So $\varrho_r(\mathrm{Frob}_p) = \lambda\Phi \in \mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ for some unknown $\lambda \in \mathbb{F}_\ell^*/S_r$.

Recovering the indexation of the roots

We can index the p-adic roots of $F_0(x)$ by $\mathbb{P}^1\mathbb{F}_\ell$ thanks to our Galois group computation, and then compute

$$\varrho_0(\mathrm{Frob}_p) = \overline{\Phi} \in \mathrm{PGL}_2(\mathbb{F}_\ell)$$

by looking at Frob_p acting on them.

So $\varrho_r(\mathrm{Frob}_p) = \lambda\Phi \in \mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ for some unknown $\lambda \in \mathbb{F}_\ell^*/S_r$.

Let $z \in Z_r$ be a root of $F_r(x)$. We find the corresponding root of $F_0(x)$, then the line $w \in \mathbb{P}^1\mathbb{F}_\ell$ that indexes it, and we index z by a vector $v \in w$.

Recovering the indexation of the roots

We can index the p-adic roots of $F_0(x)$ by $\mathbb{P}^1\mathbb{F}_\ell$ thanks to our Galois group computation, and then compute

$$\varrho_0(\mathrm{Frob}_p) = \overline{\Phi} \in \mathrm{PGL}_2(\mathbb{F}_\ell)$$

by looking at Frob_p acting on them.

So $\varrho_r(\mathrm{Frob}_p) = \lambda\Phi \in \mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ for some unknown $\lambda \in \mathbb{F}_\ell^*/S_r$.

Let $z \in Z_r$ be a root of $F_r(x)$. We find the corresponding root of $F_0(x)$, then the line $w \in \mathbb{P}^1\mathbb{F}_\ell$ that indexes it, and we index z by a vector $v \in w$.

Then for each λ, we get a candidate indexation of Z_r by V_r:

$$\mathrm{Frob}_p^n z \leftrightarrow (\lambda\Phi)^n v.$$

Recovering the indexation of the roots

We can index the p-adic roots of $F_0(x)$ by $\mathbb{P}^1\mathbb{F}_\ell$ thanks to our Galois group computation, and then compute

$$\varrho_0(\mathrm{Frob}_p) = \overline{\Phi} \in \mathrm{PGL}_2(\mathbb{F}_\ell)$$

by looking at Frob_p acting on them.

So $\varrho_r(\mathrm{Frob}_p) = \lambda\Phi \in \mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ for some unknown $\lambda \in \mathbb{F}_\ell^*/S_r$.

Let $z \in Z_r$ be a root of $F_r(x)$. We find the corresponding root of $F_0(x)$, then the line $w \in \mathbb{P}^1\mathbb{F}_\ell$ that indexes it, and we index z by a vector $v \in w$.

Then for each λ, we get a candidate indexation of Z_r by V_r:

$$\mathrm{Frob}_p^n z \leftrightarrow (\lambda\Phi)^n v.$$

For each of these, we compute one coefficient of one resolvent $\Gamma_C(x)$. All but one clash with archimedian bounds.

$\varrho_r \sim \rho_{f,\mathfrak{l}}^{S_r}$

Since $\varrho_0 \sim \rho_{f,\mathfrak{l}}$, there exists a Galois character $\psi\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell^*/S_r$ such that

$$\varrho_r \sim \psi \otimes \rho_{f,\mathfrak{l}}^{S_r}.$$

Since $\varrho_0 \sim \rho_{f,\mathfrak{l}}$, there exists a Galois character $\psi\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell^*/S_r$ such that

$$\varrho_r \sim \psi \otimes \rho_{f,\mathfrak{l}}^{S_r}.$$

Because of the ramification, ψ must be a power of the cyclotomic character mod ℓ.

$\varrho_r \sim \rho_{f,\mathfrak{l}}^{S_r}$

Since $\varrho_0 \sim \rho_{f,\mathfrak{l}}$, there exists a Galois character $\psi\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell^*/S_r$ such that

$$\varrho_r \sim \psi \otimes \rho_{f,\mathfrak{l}}^{S_r}.$$

Because of the ramification, ψ must be a power of the cyclotomic character mod ℓ.

We check that

$$\operatorname{Tr} \varrho_r(\operatorname{Frob}_v) \in \big(a_v(f) \bmod \mathfrak{l}\big) S_r$$

for some small $v \in \mathbb{N}$ such that $\langle v \rangle = \mathbb{F}_\ell^*$ and $a_v(f) \not\equiv 0 \bmod \mathfrak{l}$.

Examples of results

Example: $\rho_{\Delta,29}$ (genus $g = 22$)

p	$\rho_{\Delta,29}(\mathrm{Frob}_p)$ similar to	$\tau(p) \bmod 29$
$10^{1000} + 453$	$\begin{bmatrix} 0 & 5 \\ 1 & 21 \end{bmatrix}$	21
$10^{1000} + 1357$	$\begin{bmatrix} 0 & 28 \\ 1 & 8 \end{bmatrix}$	8
$10^{1000} + 2713$	$\begin{bmatrix} 0 & 9 \\ 1 & 11 \end{bmatrix}$	11
$10^{1000} + 4351$	$\begin{bmatrix} 0 & 26 \\ 1 & 0 \end{bmatrix}$	0
$10^{1000} + 5733$	$\begin{bmatrix} 20 & 0 \\ 0 & 2 \end{bmatrix}$	22
$10^{1000} + 7383$	$\begin{bmatrix} 19 & 0 \\ 0 & 10 \end{bmatrix}$	0
$10^{1000} + 10401$	$\begin{bmatrix} 7 & 0 \\ 0 & 2 \end{bmatrix}$	9

Example: Lehmer's conjecture

Conjecture (Lehmer, 1947)

For all $n \geqslant 1$, $\tau(n) \neq 0$.

Example: Lehmer's conjecture

Conjecture (Lehmer, 1947)

For all $n \geqslant 1$, $\tau(n) \neq 0$.

Improvement of previous results (Bosman 2007):

p	$\rho_{\Delta,29}(\mathrm{Frob}_p)$ similar to	$\tau(p)$ mod 29
22798241520242687999	$\begin{bmatrix} 0 & 26 \\ 1 & 3 \end{bmatrix}$	3
60707199950936063999	$\begin{bmatrix} 0 & 19 \\ 1 & 9 \end{bmatrix}$	9
93433753964906495999	$\begin{bmatrix} 0 & 14 \\ 1 & 4 \end{bmatrix}$	4
102797608484376575999	$\begin{bmatrix} 0 & 23 \\ 1 & 4 \end{bmatrix}$	4

Example: $\rho_{f_{24},31}$ (genus $g = 26$)

$$f_{24} = \sum_{n=1}^{\infty} \tau_{24}(n) q^n \in \mathcal{S}_{24}(1),$$

$$\tau_{24}(n) \in K_{f_{24}} = \mathbb{Q}(\alpha), \quad \alpha = \frac{1+\sqrt{144169}}{2}.$$

Example: $\rho_{f_{24},31}$ (genus $g = 26$)

p	$\rho_{f_{24},\mathfrak{l}_5}(\mathrm{Frob}_p)$	$\rho_{f_{24},\mathfrak{l}_{27}}(\mathrm{Frob}_p)$	$\tau_{24}(p) \bmod 31\mathbb{Z}[\alpha]$
$10^{1000}+453$	$\begin{bmatrix} 0 & 10 \\ 1 & 5 \end{bmatrix}$	$\begin{bmatrix} 20 & 0 \\ 0 & 15 \end{bmatrix}$	$1+7\alpha$
$10^{1000}+1357$	$\begin{bmatrix} 18 & 0 \\ 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 25 & 0 \\ 0 & 22 \end{bmatrix}$	$1+4\alpha$
$10^{1000}+2713$	$\begin{bmatrix} 24 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 29 & 0 \\ 0 & 7 \end{bmatrix}$	$4+23\alpha$
$10^{1000}+4351$	$\begin{bmatrix} 17 & 0 \\ 0 & 13 \end{bmatrix}$	$\begin{bmatrix} 11 & 0 \\ 0 & 6 \end{bmatrix}$	$9+29\alpha$
$10^{1000}+5733$	$\begin{bmatrix} 19 & 0 \\ 0 & 12 \end{bmatrix}$	$\begin{bmatrix} 15 & 0 \\ 0 & 9 \end{bmatrix}$	$3+18\alpha$
$10^{1000}+7383$	$\begin{bmatrix} 0 & 17 \\ 1 & 27 \end{bmatrix}$	$\begin{bmatrix} 7 & 0 \\ 0 & 2 \end{bmatrix}$	$17+2\alpha$
$10^{1000}+10401$	$\begin{bmatrix} 22 & 0 \\ 0 & 5 \end{bmatrix}$	$\begin{bmatrix} 0 & 14 \\ 1 & 7 \end{bmatrix}$	$9+16\alpha$

Thank you !