Computing modular Galois representations and lightly ramified PGL_2-fields

Nicolas Mascot

University of Warwick

Arithmetic Geometry and Computer Algebra workshop
Oldenburg
July 1st 2017

Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in \mathcal{N}_k(N, \varepsilon)$ be a newform of weight $k \geqslant 2$.

Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in \mathcal{N}_k(N, \varepsilon)$ be a newform of weight $k \geqslant 2$.

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

Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in \mathcal{N}_k(N, \varepsilon)$ be a newform of weight $k \geqslant 2$.

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

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

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

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

Modular Galois representations

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in \mathcal{N}_k(N, \varepsilon)$ be a newform of weight $k \geqslant 2$.

Theorem (Deligne, Serre, Shimura, 1971)

There exists a unique continuous Galois representation

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

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

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

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

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: $f = \Delta \bmod \mathfrak{l} = 31$

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

$$\begin{aligned}
&x^{64} - 21\,x^{63} + 118\,x^{62} + 527\,x^{61} - 8587\,x^{60} + 18383\,x^{59} + 263035\,x^{58} - 2095879\,x^{57} + 2416016\,x^{56} + 44283128\,x^{55} - 240474192\,x^{54}\\
&+84687350\,x^{53} + 3638349286\,x^{52} - 12617823980\,x^{51} - 10297265505\,x^{50} + 155175311479\,x^{49} - 196432825560\,x^{48} - 771645455342\,x^{47}\\
&+1482783472303\,x^{46} + 2641351695834\,x^{45} + 4650870173875\,x^{44} - 45480241563019\,x^{43} - 54597672402738\,x^{42} + 501026042999912\,x^{41}\\
&-496541492329624\,x^{40} - 712343608491160\,x^{39} + 5302741451178477\,x^{38} - 30548025690548139\,x^{37} + 34878663423629056\,x^{36}\\
&+288784532405339724\,x^{35} - 874206875792459963\,x^{34} - 825384106177640249\,x^{33} + 6958723996166230970\,x^{32}\\
&-4535708640900181166\,x^{31} - 30017821501048367756\,x^{30} + 56583574288118086410\,x^{29} + 60507682456797414358\,x^{28}\\
&-278043951776326798765\,x^{27} + 87013091280485835964\,x^{26} + 765685764124853689529\,x^{25} - 1039521490897195574873\,x^{24}\\
&-857609563094973739451\,x^{23} + 3508677503532089909529\,x^{22} - 2261986657658172377618\,x^{21} - 5701736296366236274465\,x^{20}\\
&+13022859322612898456054\,x^{19} - 6410034736367305328 62\,x^{18} - 29939230256003209147601\,x^{17} + 25447129369769267020402\,x^{16}\\
&+36125137963345226955671\,x^{15} - 55314588133331740131989\,x^{14} - 18703775559594899286772\,x^{13} + 43941206930666596631797\,x^{12}\\
&+17651378415866112635127\,x^{11} + 10928239966752626190216\,x^{10} - 81873964056071560411072\,x^{9} - 14246438965830190561265\,x^{8}\\
&+12829854828101897274374 9\,x^{7} - 50060167623901195766317\,x^{6} - 45764538130200829948820\,x^{5} + 18800719945150143916844\,x^{4}\\
&-8179472634137717244072\,x^{3} + 6229043502657290570197 9\,x^{2} - 7171013996283419682330 6\,x + 258422114921230625835 56.
\end{aligned}$$

(several CPU years).

Example: $f = \Delta \bmod \mathfrak{l} = 31$

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	$\tau(p) \bmod 31$
$10^{1000} + 453$	$\begin{bmatrix} 30 & 0 \\ 0 & 20 \end{bmatrix}$	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

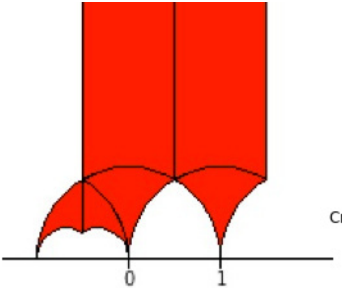
(30s of CPU time per p).

The modular curve $X_1(N)$

For $N \in \mathbb{N}$, let $X_1(N)$ be the modular curve $\Gamma_1(N) \backslash \mathcal{H}^\bullet$.

The modular curve $X_1(N)$

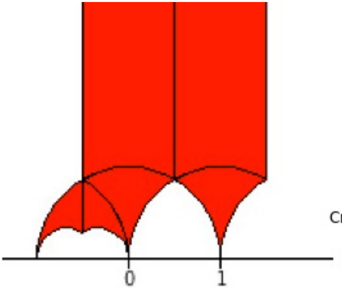
For $N \in \mathbb{N}$, let $X_1(N)$ be the modular curve $\Gamma_1(N) \backslash \mathcal{H}^\bullet$.



Credit: Helena Verrill

The modular curve $X_1(N)$

For $N \in \mathbb{N}$, let $X_1(N)$ be the modular curve $\Gamma_1(N)\backslash\mathcal{H}^\bullet$.



Credit: Helena Verrill

The ℓ-torsion of its Jacobian $J_1(N)$ contains the mod ℓ representations attached to the newforms of weight $k = 2$ and level $\Gamma_1(N)$.

Weight lowering

Weight-lowering theorem

Suppose $\ell \geqslant 5$ and $\ell \nmid N$, and let $f \in \mathcal{N}_{k}\big(\Gamma_1(N)\big)$ be a newform of weight $3 \leqslant k \leqslant \ell$. There exists a newform $f_2 \in \mathcal{N}_{2}\big(\Gamma_1(\ell N)\big)$ 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 $f \in \mathcal{N}_k\big(\Gamma_1(N)\big)$ be a newform of weight $3 \leqslant k \leqslant \ell$. There exists a newform $f_2 \in \mathcal{N}_2\big(\Gamma_1(\ell N)\big)$ 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 $\rho_{f,\mathfrak{l}} \simeq \rho_{f_2,\mathfrak{l}_2}$ shows up as

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

Weight lowering

Thus $\rho_{f,\mathfrak{l}} \simeq \rho_{f_2,\mathfrak{l}_2}$ shows up as

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

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 genus of $X_1(\ell N)$ get quickly large with ℓN.

The modular curve $X_H(\ell N)$

The genus of $X_1(\ell N)$ get quickly large with ℓN.

However, the condition

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

implies that

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

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

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

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

The modular curve $X_H(\ell N)$

☠ The genus of $X_1(\ell N)$ get quickly large with ℓN.

However, the condition

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

implies that

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

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

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

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

When H is large, the genus of this curve is much smaller than that of $X_1(\ell N)$.

Khuri-Makdisi's algorithms

Let C be a "nice" curve of genus g.
Fix a divisor D_0 on C of degree $d_0 \geqslant 2g+1$, and compute a basis of

$$V = H^0(C, 3D_0),$$

the elements being represented by multipoint evaluation, or Taylor series (or both !)

Khuri-Makdisi's algorithms

Let C be a "nice" curve of genus g.
Fix a divisor D_0 on C of degree $d_0 \geqslant 2g+1$, and compute a basis of

$$V = H^0(C, 3D_0),$$

the elements being represented by multipoint evaluation, or Taylor series (or both !)

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

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

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

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

Khuri-Makdisi's algorithms

Let C be a "nice" curve of genus g.
Fix a divisor D_0 on C of degree $d_0 \geqslant 2g+1$, and compute a basis of

$$V = H^0(C, 3D_0),$$

the elements being represented by multipoint evaluation, or Taylor series (or both !)

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

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

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

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

Arithmetic in $\mathrm{Pic}^0(C)$ is then performed by linear algebra on the subspaces of V.

Khuri-Makdisi's algorithms on the modular curve

Let $f_0 \in \mathcal{S}_2\big(\Gamma_H(\ell N)\big)$ 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 $\mathbb{Q}$.

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

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

Khuri-Makdisi's algorithms on the modular curve

Let $f_0 \in \mathcal{S}_2\big(\Gamma_H(\ell N)\big)$ 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 $\mathbb{Q}$.

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

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 the cusps.

Khuri-Makdisi's algorithms on the modular curve

Let $f_0 \in \mathcal{S}_2\big(\Gamma_H(\ell N)\big)$ 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 $\mathbb{Q}$.

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

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 the cusps.

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

An analytic point of view

In the elliptic curve case:

Algebraic model | Analytic model

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

(Weierstrass) | Easy torsion

An analytic point of view

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.

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

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

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

Strategy

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

1. Period lattice Λ of $X_H(\ell N)$
   High accuracy q-expansions and term-by-term integration of weight 2 cuspforms

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

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

   Locally invert Abel-Jacobi near 0 by Newton. Use periods to compute $2^m\ell$-torsion divisor classes, $m \gg 1$. Use Khuri-Makdisi's algorithms to double these classes m times.

3. Evaluation of the ℓ-torsion
   Construct of a function $\alpha \in \mathbb{Q}\big(J_H(\ell N)\big)$, evaluate it at the points of $V_{f,\mathfrak{l}} \subset J_H(\ell N)[\ell]$.

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

4. Compute $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$

   thanks to the Dokchitsers' algorithm.

Evaluating the ℓ-torsion

Proposition

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

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

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

If α is injective on $V_{f,\mathfrak{l}}$, then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes the roots of $F(x)$ as it permutes the points of $V_{f,\mathfrak{l}}$. In particular, $F(x)$ is then irreducible, and its decomposition field is

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

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

Let E_0 be an effective divisor defined over $\mathbb{Q}$ and of degree g. Pick $\xi \in \mathbb{Q}\big(X_H(\ell N)\big)$, and extend it to $J_H(\ell N)$ by

$$\begin{array}{rccc} \alpha: & J_H(\ell N) & \dashrightarrow & \mathbb{C} \\ & \left[\sum_{i=1}^{g} P_i - E_0\right] & \longmapsto & \sum_{i=1}^{g} \xi(P_i) \end{array}.$$

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

Let E_0 be an effective divisor defined over $\mathbb{Q}$ and of degree g. Pick $\xi \in \mathbb{Q}\big(X_H(\ell N)\big)$, and extend it to $J_H(\ell N)$ by

$$\begin{array}{cccc} \alpha : & J_H(\ell N) & \dashrightarrow & \mathbb{C} \\ & \left[\sum_{i=1}^{g} P_i - E_0 \right] & \longmapsto & \sum_{i=1}^{g} \xi(P_i) \end{array} .$$

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.

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

Let E_0 be an effective divisor defined over $\mathbb{Q}$ and of degree g. Pick $\xi \in \mathbb{Q}\big(X_H(\ell N)\big)$, and extend it to $J_H(\ell N)$ by

$$\begin{array}{cccc} \alpha : & J_H(\ell N) & \dashrightarrow & \mathbb{C} \\ & \left[\sum_{i=1}^{g} P_i - E_0\right] & \longmapsto & \sum_{i=1}^{g} \xi(P_i) \end{array}.$$

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)

$$\deg \xi \gtrapprox g.$$

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

Let E_0 be an effective divisor defined over $\mathbb{Q}$ and of degree g. Points on $J_H(\ell N)$ can be written $[E - E_0]$, E effective of degree g. Fix an effective divisor B of degree $2g$. Then

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

We can thus define

$$\begin{array}{cccc} \alpha: & J_H(\ell N) & \dashrightarrow & \mathbb{C} \\ & [E - E_0] & \longmapsto & \dfrac{\phi_E(P)}{\phi_E(Q)} \end{array}$$

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

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

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

We can thus define

$$\begin{array}{rccc} \alpha: & J_H(\ell N) & \dashrightarrow & \mathbb{C} \\ & [E - E_0] & \longmapsto & \dfrac{\phi_E(P)}{\phi_E(Q)} \end{array}$$

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

Theorem (M.)

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

Companion forms and tame ramification

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

- unramified outside ℓN,
- (at most) tamely ramified at every $p \neq \ell$ s.t. $p \| N$,
- and usually wildly ramified at ℓ,

Companion forms and tame ramification

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

- unramified outside ℓN,
- (at most) tamely ramified at every $p \neq \ell$ s.t. $p \| N$,
- and usually wildly ramified at ℓ, except
  - if f is *supersingular* mod $\mathfrak{l}$, i.e. $a_\ell(f) \equiv 0 \bmod \mathfrak{l}$,
  - or if f admits a *companion form* mod $\mathfrak{l}$, i.e.

$$\exists g \in \mathcal{S}_{\ell+1-k}\big(\Gamma_1(N)\big) \text{ s.t. } \sum_n n a_n(f) q^n \equiv \sum_n n^k a_n(g) q^n.$$

Companion forms and tame ramification

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

- unramified outside ℓN,
- (at most) tamely ramified at every $p \neq \ell$ s.t. $p \| N$,
- and usually wildly ramified at ℓ, except
  - if f is *supersingular* mod $\mathfrak{l}$, i.e. $a_\ell(f) \equiv 0$ mod $\mathfrak{l}$,
  - or if f admits a *companion form* mod $\mathfrak{l}$, i.e.

$$\exists g \in \mathcal{S}_{\ell+1-k}\big(\Gamma_1(N)\big) \text{ s.t. } \sum_n n a_n(f) q^n \equiv \sum_n n^k a_n(g) q^n.$$

We can use these exceptional cases to discover number fields with Galois group $\leqslant \mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ and very small discriminant.

Companion forms and tame ramification

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

- unramified outside ℓN,
- (at most) tamely ramified at every $p \neq \ell$ s.t. $p \| N$,
- and usually wildly ramified at ℓ, except
  - if f is *supersingular* mod $\mathfrak{l}$, i.e. $a_\ell(f) \equiv 0 \bmod \mathfrak{l}$,
  - or if f admits a *companion form* mod $\mathfrak{l}$, i.e.

$$\exists g \in \mathcal{S}_{\ell+1-k}\big(\Gamma_1(N)\big) \text{ s.t. } \sum_n n a_n(f) q^n \equiv \sum_n n^k a_n(g) q^n.$$

We can use these exceptional cases to discover number fields with Galois group $\leqslant \mathrm{PGL}_2(\mathbb{F}_\mathfrak{l})$ and very small discriminant, by considering the *projective* representation

$$\pi_{f,\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\mathfrak{l}) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_\mathfrak{l}).$$

Prediction of the discriminants

Let $f \in \mathcal{N}_k(N, \varepsilon)$ with N squarefree and coprime to ℓ and $\mathfrak{l} \mid \ell$ of degree m. Let

$$\pi_{f,\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_{\mathfrak{l}})$$

be the projective representation attached to f mod $\mathfrak{l}$, and consider the Galois number field L that it cuts out, and let $K \subset L$ correspond to the stabiliser of a point of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{l}})$. Let d_K, d_L be their respective root discriminants.

Prediction of the discriminants

Theorem (M.)

Assume that $\pi_{f,\mathfrak{l}}$ acts transitively on $\mathbb{P}^1(\mathbb{F}_\mathfrak{l})$. Let $M = \operatorname{cond}(\varepsilon \bmod \mathfrak{l})$ and $N' = \prod\{p \neq \ell \mid \rho_{f,\mathfrak{l}} \text{ ramif. at } p\}$, so $M \mid N' \mid N$, and define $r_p = \operatorname{ord}(\varepsilon_p \bmod \mathfrak{l})$ for $p \mid M$. Then

$$d_K = \ell^\alpha \left(\frac{N'}{M}\right)^{\frac{1-1/\ell}{1+1/\ell^m}} \left(\prod_{p \mid M} p^{1-1/r_p}\right)^{\frac{\ell^m-1}{\ell^m+1}}, \quad d_L = \ell^\beta \left(\frac{N'}{M}\right)^{1-1/\ell} \prod_{p \mid M} p^{1-1/r_p}$$

where

$$\beta = 1 - \frac{\gcd(k-1, \ell-1)}{\ell - 1}, \quad \alpha = \frac{\ell^m - 1}{\ell^m + 1}\beta$$

if f admits a companion form mod $\mathfrak{l}$, and

$$\beta = 1 - \frac{\gcd(k-1, \ell+1)}{\ell + 1}, \quad \alpha = \begin{cases} \beta & \text{if } m \text{ is odd,} \\ \frac{\ell^m-1}{\ell^m+1}\beta & \text{if } m \text{ is even} \end{cases}$$

if f is supersingular mod $\mathfrak{l}$.

Example 1

$f = q + 2q^2 - 4q^3 + O(q^4) \in \mathcal{N}_6\big(\Gamma_0(5)\big)$ is supersingular mod $\mathfrak{l} = 13$.

$\operatorname{Im} \pi_{f,\mathfrak{l}} = \mathrm{PGL}_2(\mathbb{F}_{13})$, and $X_H(5 \cdot 13)$ has genus $g = 13$.

Theorem (M.)

K is the root field and L is the splitting field of

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

We have $d_K = 43.002\cdots$, $d_L = 47.816\cdots$
(cf. $8\pi e^\gamma = 44.763\cdots$).

Conjecture (Roberts, M.)

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

Example 2

$f = q - 6q^2 - 42q^3 + O(q^4) \in \mathcal{N}_8\big(\Gamma_0(7)\big)$ admits a companion mod $\mathfrak{l} = 13$.

$\operatorname{Im} \pi_{f,\mathfrak{l}} = \mathrm{PGL}_2(\mathbb{F}_{13})$, and $X_H(7 \cdot 13)$ has genus $g = 13$ (again).

Theorem (M.)

K is the root field and L is the splitting field of
$x^{14} - 52x^7 + 91x^6 + 273x^5 - 364x^4 - 1456x^3 - 455x^2 + 1568x + 1495.$
We have $d_K = 39.775\cdots$, $d_L = 63.271\cdots$.

Example 3

$f = q + 1728q^2 - 59049q^3 + O(q^4) \in \mathcal{N}_{22}\big(\Gamma_0(3)\big)$ admits a companion mod $\mathfrak{l} = 41$.

$\operatorname{Im} \pi_{f,\mathfrak{l}} = \mathrm{PGL}_2(\mathbb{F}_{41})$, and this time $X_H(3 \cdot 41)$ has genus $g = 25$.

Theorem (M.)

K is the root field and L is the splitting field of

$$
\begin{aligned}
&x^{42} - 13x^{41} + 70x^{40} - 209x^{39} + 395x^{38} - 1235x^{37} + 8745x^{36} - 32673x^{35} + 41466x^{34} + 23047x^{33} + 117494x^{32} - 1473749x^{31} \\
&+3432505x^{30} + 2534861x^{29} - 8121350x^{28} - 46053615x^{27} + 55119882x^{26} + 3771513x^{25} + 926108685x^{24} + 222895020x^{23} - 7775139729x^{22} \\
&-13813042275x^{21} + 57369301467x^{20} + 104177173023x^{19} - 235503859068x^{18} - 631349403945x^{17} + 789220697001x^{16} + 2415426085387x^{15} \\
&-1368495524968x^{14} - 7976148397256x^{13} + 2486419230610x^{12} + 18312969605213x^{11} - 3490664476058x^{10} - 33337073689065x^{9} \\
&+9634206834816x^{8} + 38121337992357x^{7} - 8827768624685x^{6} - 35949940921273x^{5} + 19912312531x^{4} + 24698337243313x^{3} \\
&+7457815492250x^{2} - 8123634511724x - 4296658258197.
\end{aligned}
$$

We have $d_K = 89.533\cdots$, $d_L = 109.131\cdots$.

Example 4

$f = q + 18\sqrt{-26}q^2 - (54\sqrt{-26} + 675)q^3 + O(q^4) \in \mathcal{N}_{13}(3, (\frac{-3}{\bullet}))$ is supersingular mod both primes above 37.

We have $\operatorname{Im} \pi_{f,\mathfrak{l}} = \mathrm{PSL}_2(\mathbb{F}_{37})$, $d_K = 51.483\cdots$, and $d_L = 52.993\cdots$.

Unfortunately, the genus of $X_H(3 \cdot 37)$ is $g = 385$.

Thank you !