Residual modular Galois representations: an algorithmic approach

Samuele Anni

University of Warwick

Algebra and Number Theory Seminar
University College Dublin
22nd September 2014

Let us fix a positive integer $n \in \mathbb{Z}_{>0}$.

Definition

The **congruence subgroup** $\Gamma_1(n)$ of $\mathrm{SL}_2(\mathbb{Z})$ is the subgroup given by

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : n \mid a-1 \,,\, n \mid c \right\}.$$

The integer n is called **level** of the congruence subgroup.

Over the upper half plane:

$$\mathbb{H} = \{z \in \mathbb{C} | \, \mathrm{Im}(z) > 0\}$$

we can define an action of $\Gamma_1(n)$ via **fractional transformations**:

$$\begin{array}{rcl} \Gamma_1(n) \times \mathbb{H} & \to & \mathbb{H} \\ (\gamma, z) & \mapsto & \gamma(z) = \dfrac{az+b}{cz+d} \end{array}$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Moreover, if $n \geq 4$ then $\Gamma_1(n)$ acts freely on $\mathbb{H}$.

Escher, Reducing Lizards Tessellation

Definition

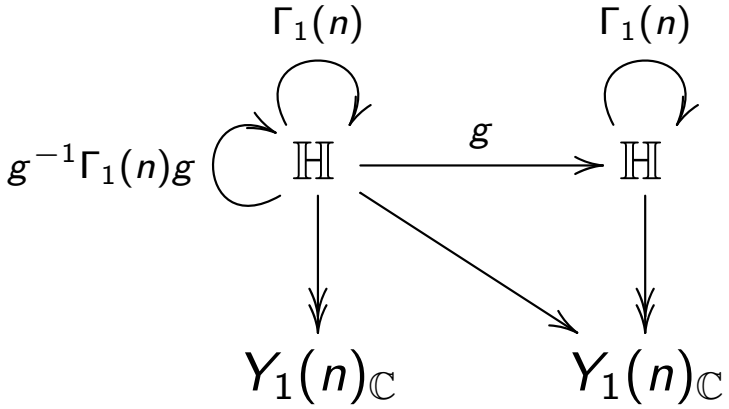
We define the **modular curve** $Y_1(n)_{\mathbb{C}}$ to be the non-compact Riemann surface obtained giving on $\Gamma_1(n)\backslash\mathbb{H}$ the complex structure induced by the quotient map. Let $X_1(n)_{\mathbb{C}}$ be the compactification of $Y_1(n)_{\mathbb{C}}$.

Fact: $Y_1(n)_{\mathbb{C}}$ can be defined algebraically over $\mathbb{Q}$ (in fact over $\mathbb{Z}[1/n]$).

The group $GL_2^+(\mathbb{Q})$ acts on $\mathbb{H}$ via fractional transformation, and its action has a particular behaviour with respect to $\Gamma_1(n)$.

Proposition

For every $g \in GL_2^+(\mathbb{Q})$, the discrete groups $g\Gamma_1(n)g^{-1}$ and $\Gamma_1(n)$ are commensurable



We define operators on $Y_1(n)$ through the correspondences given before:

- the **Hecke operators** T_p for every prime p, using $g = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in GL_2^+(\mathbb{Q})$;
- the **diamond operators** $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$, using $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(n)$, where $\Gamma_0(n)$ is the set of matrices in $\mathrm{SL}_2(\mathbb{Z})$ which are upper triangular modulo n.

For $n \geq 5$ and k positive integers, let ℓ be a prime not dividing n. Following Katz, we define the space of mod ℓ cusp forms as

mod ℓ cusp forms

$$S(n,k)_{\overline{\mathbb{F}}_\ell} = \mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell}, \omega^{\otimes k}(-\mathrm{Cusps})).$$

$S(n,k)_{\overline{\mathbb{F}}_\ell}$ is a finite dimensional $\overline{\mathbb{F}}_\ell$-vector space, equipped with Hecke operators T_n $(n \geq 1)$ and diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$.

Analogous definition in characteristic zero and over any ring where n is invertible.

One may think that mod ℓ modular forms come from reduction of characteristic zero modular forms mod ℓ:

$$S(n,k)_{\mathbb{Z}[1/n]} \to S(n,k)_{\mathbb{F}_\ell}.$$

Unfortunately, this map is **not surjective** for $k = 1$.

Even worse: let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character, whose image is contained in $\mathcal{O}_K$, ring of integers of the number field K, then the map

$$S(n,k,\epsilon)_{\mathcal{O}_K} \to S(n,k,\overline{\epsilon})_{\mathbb{F}}$$

is **not** always **surjective** even if $k > 1$, where $\mathbb{F}$ is the residue field at ℓ and $\overline{\epsilon}$ is the reduction of ϵ.

$$S(n,k,\epsilon)_{\mathcal{O}_K} := \{f \in S(n,k)_{\mathcal{O}_K} \mid \forall d \in (\mathbb{Z}/n\mathbb{Z})^*, \langle d\rangle f = \epsilon(d) f\}$$

Definition

The **Hecke algebra** $\mathbb{T}(n,k)$ of $S(n,k)_{\mathbb{C}}$ is the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S(\Gamma_1(n),k)_{\mathbb{C}})$ generated by Hecke operators T_p for every prime p and by diamond operators $\langle d\rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$.

Fact:

$\mathbb{T}(n,k)$ is finitely generated as $\mathbb{Z}$-module.

Given a character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$, we associate a Hecke algebra $\mathbb{T}_\epsilon(n,k)$ to each $S(n,k,\epsilon)_{\mathbb{C}}$:

$$S(n,k,\epsilon)_{\mathbb{C}} = \{f \in S(n,k)_{\mathbb{C}} | \forall d \in (\mathbb{Z}/n\mathbb{Z})^*, \langle d\rangle f = \epsilon(d) f\}.$$

Theorem (Deligne, Shimura)

Let n and k be positive integers. Let $\mathbb{F}$ be a finite field of characteristic ℓ, with ℓ not dividing n, and $f : \mathbb{T}(n,k) \twoheadrightarrow \mathbb{F}$ a surjective morphism of rings. Then there is a continuous semi-simple representation:

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}),$$

unramified outside $n\ell$, such that for all p not dividing $n\ell$ we have:

$$\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = f(T_p) \text{ and } \det(\rho_f(\mathrm{Frob}_p)) = f(\langle p \rangle)p^{k-1} \text{ in } \mathbb{F}.$$

Such a ρ_f is unique up to isomorphism.

Computing ρ_f is "difficult", but theoretically it **can be done in polynomial time** in $n, k, \#\mathbb{F}$:

Edixhoven, Couveignes, de Jong, Merkl, Bruin, Bosman ($\#\mathbb{F} \leq 32$).

For example: $n = 1$, $k = 22$ and $\ell = 23$ then the number field corresponding to $\mathbb{P}\rho_f$ is given by:

$$\begin{aligned} & x^{24} - 2x^{23} + 115x^{22} + 23x^{21} + 1909x^{20} + 22218x^{19} + 9223x^{18} + 121141x^{17} \\ & + 1837654x^{16} - 800032x^{15} + 9856374x^{14} + 52362168x^{13} - 32040725x^{12} \\ & + 279370098x^{11} + 1464085056x^{10} + 1129229689x^{9} + 3299556862x^{8} \\ & + 14586202192x^{7} + 29414918270x^{6} + 45332850431x^{5} - 6437110763x^{4} \\ & - 111429920358x^{3} - 12449542097x^{2} + 93960798341x - 31890957224 \end{aligned}$$

Mascot, Zeng, Tian ($\#\mathbb{F} \leq 41$).

Question

Can we compute the image of a residual modular Galois representation without computing the representation?

Why one should be interested in this?

- To obtain explicit answer to question proposed by Serre, Ribet... for example, uniform bounds for surjectivity of residual representations for elliptic curves and abelian varieties.
- The inverse Galois problem.
- Diophantine equations.
- In lifting theorems for representations and chain of congruences techniques one of the hypothesis is big residual image.

Main ingredients:

Theorem (Dickson)

Let ℓ be an odd prime and H a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. Then a conjugate of H is one of the following groups:

- a finite subgroup of the upper triangular matrices;
- $\mathrm{SL}_2(\mathbb{F}_{\ell^r})/\{\pm 1\}$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ for $r \in \mathbb{Z}_{>0}$;
- a dihedral group D_{2n} with $n \in \mathbb{Z}_{>1}$, $(\ell, n) = 1$;
- or it is isomorphic to A_4, S_4 or A_5.

Definition

If $G := \rho_f(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ has order prime to ℓ we call the image **exceptional**.

Theorem (Khare, Wintenberger, Dieulefait, Kisin), Serre's Conjecture

Let ℓ be a prime number and let $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd, absolutely irreducible, continuous representation. Then ρ is **modular** of level $N(\rho)$, weight $k(\rho)$ and character $\epsilon(\rho)$.

- $N(\rho)$ (the level) is the Artin conductor away from ℓ.
- $k(\rho)$ (the weight) is given by a recipe in terms of $\rho|_{I_\ell}$.
- $\epsilon(\rho)\colon (\mathbb{Z}/N(\rho)\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ is given by:

$$\det \rho = \epsilon(\rho)\chi^{k(\rho)-1}.$$

Theorem (A.)

There is a polynomial time algorithm which takes as input:

- *n and k be positive integers;*
- *ℓ be a prime number not dividing n, such that $2 \leq k \leq \ell + 1$;*
- *a character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$;*
- *a morphism of ring $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$, and in particular the images of all diamond operators and of the T_p operators up to a bound B,*

and gives as output the image of the associated Galois representation ρ_f, up to conjugacy as subgroup of $\mathsf{GL}_2(\overline{\mathbb{F}}_\ell)$ without computing ρ_f.

In almost all cases, the bound B is the Sturm Bound for $\Gamma_0(n)$ and weight k:

$$\frac{k}{12} \cdot n \cdot \prod_{p|n \text{ prime}} \left(1 + \frac{1}{p}\right) \ll \frac{k}{12} \cdot n \log\log n$$

In the cases when this bound is not enough, then the Sturm Bound for $\Gamma_0(nq^2)$ and weight k, where q is the smallest odd prime not dividing n, is the required bound.

Problems

- ρ_f can arise from lower level or weight, i.e. there exists $g \in S(m,j)_{\overline{\mathbb{F}}_\ell}$ with $m \leq n$ or $j \leq k$ such that $\rho_g \cong \rho_f$.
- ρ_f can arise as twist of a representation of lower conductor, i.e. there exist $g \in S(m,j)_{\overline{\mathbb{F}}_\ell}$ with $m \leq n$ or $j \leq k$ and a Dirichlet character χ such that $\rho_g \otimes \chi \cong \rho_f$.

Algorithm

- **Step 1** Iteration "down to top"
- **Step 2** Determine minimality with respect to level and weight.
- **Step 3** Determine whether reducible or irreducible.
- **Step 4** Determine minimality up to twisting.
- **Step 5** Compute the projective image
- **Step 6** Compute the image

Remarks

- Reducibility is checked by comparing with systems of eigenvalues coming from specific Eisenstein series.
- The projective image is determined by excluding cases. Each exceptional case is related to a particular equality of mod ℓ modular forms or a particular construction.

Setting $(*)$

- n and k be positive integers;
- ℓ be a prime number not dividing n, such that $2 \leq k \leq \ell + 1$;
- $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character;
- $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings;
- $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the unique, up to isomorphism, continuous semi-simple representation attached to f;
- $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Let p be a prime dividing $n\ell$. Let us denote by

- $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset G_{\mathbb{Q}}$ the decomposition subgroup at p;
- I_p the inertia subgroup, I_t the tame inertia subgroup;

Given a residual representation ρ, we will denote as $\mathrm{N}_p(\rho)$ the valuation at p of the Artin conductor of ρ.

Theorem (Gross-Vignéras-Fontaine, Serre: Conjecture 3.2.6$_?$)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ be a continuous, odd, irreducible representation of the absolute Galois group over $\mathbb{Q}$ to a 2-dimensional $\overline{\mathbb{F}}_\ell$-vector space V.
Let $f \in S(\mathrm{N}(\rho), k(\rho))_{\overline{\mathbb{F}}_\ell}$ be an eigenform such that $\rho_f \cong \rho$.
Let p be a prime divisor of ℓn.

(1) *If $f(T_p) \neq 0$, then there exists a stable line $D \subset V$ for the action of G_p, such that I_p acts trivially on V/D. Moreover, $f(T_p)$ is equal to the eigenvalue of Frob_p which acts on V/D.*

(2) *If $f(T_p) = 0$, then there exists no stable line $D \subset V$ as in (1).*

Proposition (A.)

Assume setting $(*)$ and that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n such that $f(T_p) \neq 0$.
Then $\rho_f|_{G_p}$ is decomposable if and only if $\rho_f|_{I_p}$ is decomposable.

Proposition (A.)

Assume setting $(*)$ and that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n, such that $f(T_p) \neq 0$. Then:

(A) *$\rho_f|_{I_p}$ is decomposable if and only if $\mathrm{N}_p(\rho_f) = \mathrm{N}_p(\overline{\epsilon})$;*

(B) *$\rho_f|_{I_p}$ is indecomposable if and only if $\mathrm{N}_p(\rho_f) = 1 + \mathrm{N}_p(\overline{\epsilon})$.*

Assume setting $(*)$ and that ρ_f is irreducible and it does not arise from lower level or weight.

Then ρ_f can still arise as twist of a representation of lower conductor or weight, i.e. there exist $g \in S(m,j)_{\overline{\mathbb{F}}_\ell}$ with $m \leq n$ or $j \leq k$ and a Dirichlet character χ such that $\rho_g \otimes \chi \cong \rho_f$.

Question

Can we fill in the database for arbitrary twists?
Equivalently, what is the relation between the conductors, the weights and the eigenvalue systems corresponding to a representation and its twist by a character?

Let n be a positive integer. Any Dirichlet character of conductor n can be decomposed into local characters, one for each prime divisor of n.

For this talk, we limit ourselves to study twists of modular Galois representations with Dirichlet characters with prime power conductor and unramified at ℓ.

Question

What is the conductor of the twist?

Shimura gave an upper bound:

$$\mathrm{lcm}(\mathrm{cond}(\chi)^2, n)$$

where n is the level of the form and χ is the character used for twisting.

Proposition (A.)

Assume setting $(*)$. Let p be a prime **not** *dividing $n\ell$. Let $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, for $i > 0$, be a non-trivial character. Then*

$$\mathrm{N}_p(\rho_f \otimes \chi) = 2\mathrm{N}_p(\chi).$$

Proposition (A.)

Assume setting $(*)$ and that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n and suppose that $f(T_p) \neq 0$. Let $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, for $i > 0$, be a non-trivial character. Then

$$\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\chi\bar{\epsilon}) + \mathrm{N}_p(\chi).$$

It is also possible to know what is the system of eigenvalues associated to the twist:

Proposition (A.)

Assume setting $(*)$. Suppose that ρ_f is irreducible and that $\mathrm{N}(\rho_f) = n$. Let p be a prime dividing n and suppose that $f(T_p) \neq 0$. Let χ from $(\mathbb{Z}/p^i\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$, with $i > 0$, be a non-trivial character. Then

(A) *if $\rho_f|_{I_p}$ is decomposable then the representation $\rho_f \otimes \chi$, restricted to G_p, admits a stable line with unramified quotient if and only if $\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\rho_f)$;*

(B) *if $\rho_f|_{I_p}$ is indecomposable then the representation $\rho_f \otimes \chi$, restricted to G_p, does not admit any stable line with unramified quotient.*

Proposition (A.)

Assume setting $(*)$. Suppose that ρ_f is irreducible and that $\mathrm{N}(\rho_f) = n$. Let p be a prime dividing n and suppose that $f(T_p) = 0$. Then:

(A) *if $\rho_f|_{G_p}$ is reducible then there exists a mod ℓ modular form g of weight k and level at most np and a non-trivial character $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ with $i > 0$ such that $g(T_p) \neq 0$ and $\rho_g \cong \rho_f \otimes \chi$;*

(B) *if $\rho_f|_{G_p}$ is irreducible then for any non-trivial character $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ with $i > 0$ the representation $\rho_f \otimes \chi$ restricted to G_p does not admit any stable line with unramified quotient.*

Example 1

Let $n = 135 = 3^3 5$. Let ϵ be the Dirichlet character modulo 135 of conductor 5 mapping $56 \to 1$, $82 \to \zeta_{36}^{9}$.

$S(135, 3, \epsilon)_{\mathbb{C}}^{\mathrm{new}}$ two Galois orbits: the two Hecke eigenvalue fields are:
$\mathbb{Q}\left(x^{16} + 217x^{12} + 9264x^8 + 59497x^4 + 28561\right)$ and
$\mathbb{Q}\left(x^{16} + 286x^{12} + 16269x^8 + 85684x^4 + 62500\right)$.

In the first one, applying the reduction map for all prime ideals above 7, we obtain the following eigenvalue systems defined over
$\mathbb{F}_{7^2} \cong \mathbb{F}_7[x]/[x^2 + 6x + 4] \cong \mathbb{F}_7[\alpha]$:

p	$f_1(T_p)$	$f_2(T_p)$	$f_3(T_p)$
2	α	6α	$\alpha+6$
3	0	0	0
5	$5\alpha+4$	$2\alpha+3$	$5\alpha+5$
7	0	0	0
11	$\alpha+3$	$6\alpha+4$	$\alpha+3$
13	6α	6α	$\alpha+6$
17	6α	α	$6\alpha+1$
19	$6\alpha+4$	$6\alpha+4$	$\alpha+3$
23	$3\alpha+4$	$4\alpha+3$	3α

f_1, f_2 and f_3 are mod 7 modular forms of level 135 and weight 3.

It is easy to verify that the corresponding representations are of minimal level and weight.

Let us focus on f_1.

Since 5 divides the level and $f_1(T_5) \neq 0$:

$$\rho_{f_1}|_{G_5} \cong \begin{pmatrix} \epsilon_1 \chi_7^2 & * \\ 0 & \epsilon_2 \end{pmatrix} \cong \begin{pmatrix} \epsilon_2^{-1} \epsilon_{f_1} \chi_7^2 & 0 \\ 0 & \epsilon_2 \end{pmatrix}$$

The character of f_1 has conductor 5 hence the representation is reducible and decomposable, so $* = 0$. Moreover $\epsilon_2(5) = f_1(T_5) = 5\alpha + 4$.

If we twist by $\epsilon_{f_1}^{-1}$ then we have:

$$(\rho_{f_1} \otimes \epsilon_{f_1}^{-1})|_{G_5} \cong \begin{pmatrix} \epsilon_2^{-1} \chi_7^2 & 0 \\ 0 & \epsilon_2 \epsilon_{f_1}^{-1} \end{pmatrix}$$

The conductor of the twist is 135 and the eigenvalue at 5 is

$$(\epsilon_2^{-1} \chi_7^2)(5) = 4\epsilon_2^{-1}(5) = 5\alpha + 5.$$

p	$f_1(T_p)$	$f_2(T_p)$	$f_3(T_p)$	$\rho_{f_1} \otimes \epsilon_{f_1}^{-1}$
2	α	6α	$\alpha+6$	$\alpha+6$
3	0	0	0	0
5	$5\alpha+4$	$2\alpha+3$	$5\alpha+5$	$5\alpha+5$
7	0	0	0	0
11	$\alpha+3$	$6\alpha+4$	$\alpha+3$	$\alpha+3$
13	6α	6α	$\alpha+6$	$\alpha+6$
17	6α	α	$6\alpha+1$	$6\alpha+1$
19	$6\alpha+4$	$6\alpha+4$	$\alpha+3$	$\alpha+3$
23	$3\alpha+4$	$4\alpha+3$	3α	3α
29	2	5	5	5
31	4	4	4	4
37	$\alpha+6$	$\alpha+6$	6α	6α
41	$5\alpha+1$	$2\alpha+6$	$5\alpha+1$	$5\alpha+1$
43	α	α	$6\alpha+1$	$6\alpha+1$
47	2α	5α	$2\alpha+5$	$2\alpha+5$

The level is also divisible by 3. But $f_1(T_3) = 0$.

The local representation at 3 is irreducible: to prove this claim we have to check all lover levels and possible twist.
In this case it is easy, since the newforms space is empty in most cases.
The argument is similar for all levels, let us what happens for level 15.

p	$f_1(T_p)$	$g_1(T_p)$	$g_2(T_p)$	$g_3(T_p)$	$g_4(T_p)$
2	α	$6\alpha+6$	$\alpha+5$	$4\alpha+1$	$3\alpha+5$
3	0	6α	$\alpha+6$	α	$6\alpha+1$
5	$5\alpha+4$	$3\alpha+5$	$4\alpha+1$	$2\alpha+1$	$5\alpha+3$
7	0	$4\alpha+5$	$3\alpha+2$	2	2
11	$\alpha+3$	$6\alpha+1$	α	α	$6\alpha+1$
13	6α	$4\alpha+5$	$3\alpha+2$	5	5

It is possible to show that the image of the Galois representation up to conjugation is

$$\rho_{f_1}(G_{\mathbb{Q}}) \cong < \alpha > \mathsf{SL}_2(\mathbb{F}_7) \subset \mathsf{GL}_2(\mathbb{F}_{7^2})$$

Example 2

Let us consider $S(40, 2, \tau)^{\text{new}}_{\mathbb{C}}$ where τ is the quadratic character conductor 40 mapping 31 $\to$ 1,21 $\to -1$, 17 $\to -1$.

As before, by reduction get mod 7 eigenvalue systems, for example f_i for $i = 1, 2, 3, 4$:

p	$f_1(T_p)$	$f_2(T_p)$	$f_3(T_p)$	$f_4(T_p)$
2	6	1	5	2
3	3	4	3	4
5	2	1	6	5
7	6	1	1	6
11	4	4	3	3
13	0	0	0	0
17	2	5	5	2
19	3	3	4	4
23	1	6	6	1

Let χ be the character over $\mathbb{F}_7$ of conductor 8 such that $\chi\epsilon_{f_1}$ has conductor 4. Since $f_1(T_2) \neq 0$, then we have that:

$$\mathrm{N}_2(\rho_f \otimes \chi) = \mathrm{N}_2(\chi\epsilon_{f_1}) + \mathrm{N}_2(\chi) = 2 + 3 = 5 \neq 6.$$

Hence, let us check the twist and the eigenvalue systems at level 160: $\mathrm{N}_2(\rho_f \otimes \chi) = 2^5 5 = 160$:

p	$g_1(T_p)$	$g_2(T_p)$	$g_3(T_p)$	$g_4(T_p)$	$\rho_{f_1} \otimes \chi$	$\rho_{f_2} \otimes \chi$	$\rho_{f_3} \otimes \chi$	$\rho_{f_4} \otimes \chi$
2	0	0	0	0	0	0	0	0
3	4	3	4	3	3	4	3	4
5	6	5	2	1	5	6	1	2
7	6	1	1	6	1	6	6	1
11	4	4	3	3	4	4	3	3
13	0	0	0	0	0	0	0	0
17	5	2	2	5	2	5	5	2
19	3	3	4	4	3	3	4	4
23	1	6	6	1	6	1	1	6

All the systems given by g_i are reduction of the same form.

Also in this case it is possible to prove that the image of the Galois representation is big: in this case, it is isomorphic to $\mathrm{GL}_2(\mathbb{F}_7)$, up to conjugation.

Example 3

$S(7,3)^{\text{new}}_{\mathbb{C}}$, $S(49,3)^{\text{new}}_{\mathbb{C}}$

The Hecke eigenvalue fields in newformspace at level 49 are given by:

- $\mathbb{Q}\left(x^2 - 3x + 9\right)$
- $\mathbb{Q}\left(x^4 - 4x^3 + 22x^2 - 44x + 167\right)$
- $\mathbb{Q}\left(x^8 + 4x^7 - 6x^6 - 96x^5 + 225x^4 + 1336x^3 - 514x^2 - 5948x + 7399\right)$
- Number Field with defining polynomial $x^{54} + 5x^{53} + 43x^{52} + 169x^{51} + \cdots + 248413945171829320x^{16} + \cdots + 34860578859420261 9x^8 + \cdots + 10909749546081$
- Number Field with defining polynomial $x^{96} + 13x^{95} + 69x^{94} + 174x^{93} + 16x^{92} - 1672x^{91} + \ldots$

while in level 7 . . . the Hecke eigenvalue field is $\mathbb{Q}$.

Let $\mathbb{F}_{5^2} \cong \mathbb{F}_5[x]/[x^2+2x+4] \cong \mathbb{F}_5[\beta]$.

Let χ be Dirichlet character over $\mathbb{F}_{5^2}$ modulo 49 of conductor 7 mapping $3 \to 3\beta$.

p	$f(T_p)$	$g(T_p)$	$\rho_f \otimes \chi$
2	2	β	β
3	0	0	0
5	0	0	0
7	3	0	0
11	4	$3\beta+1$	$3\beta+1$
13	0	0	0
17	0	0	0
19	0	0	0
23	3	4β	4β
29	1	1	1

In this case we have that $\mathbb{P}\rho_f \cong A_4$ and $\rho_f(G_{\mathbb{Q}}) \cong \mathbb{F}_5^* \tilde{A}_4$.

In the cases where the projective image is isomorphic to S_4, A_4 or A_5, in the algorithm we proceed using characteristic switching technique.

Example: projective image S_4 in characteristic 3.

Ideas:

- a modular representation which has S_4 as projective image in characteristic 3 has "big" projective image i.e. $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$;
- from mod 3 modular forms with projective image S_4, we want to construct characteristic 0 forms;
- use these forms to decide about projective image S_4 in characteristic larger than 3.

Input:

- n positive integer, $(n, 3) = 1$;
- $k \in \{2, 3, 4\}$;
- a character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$;
- a morphism of rings $f : \mathbb{T}(n, k, \epsilon) \to \overline{\mathbb{F}}_3$.

Suppose the algorithm has certified that ρ_f is absolutely irreducible and that $\mathbb{P}\rho_f \cong S_4$. Suppose also that f is minimal with respect to weight, level and twisting. What else do we know?

- Field of definition of the representation: $\mathbb{F}$;
- Field of definition of the projective representation: $\mathbb{F}_3$;
- Data on the local components;
- Image of the representation: $\rho_f(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq \mathbb{F}^* \cdot \mathrm{GL}_2(\mathbb{F}_3)$.

Let $\beta : \mathbb{F}^* \cdot \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathcal{O}_K)$ be a 2-dimensional representation, where $\mathcal{O}_K$ is the ring of integers of a number field.

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow[\rho_f]{} \mathbb{F}^* \mathrm{GL}_2(\mathbb{F}_3) \xrightarrow[\beta]{} \mathrm{GL}_2(\mathcal{O}_K), \qquad \rho_{f_\beta}$$

There exists f_β of weight 1 such that $\rho_{f_\beta} \cong \beta \circ \rho_f$.

Can we determine the level of f_β?

Yes, studying the local representation at primes dividing n and at 3.

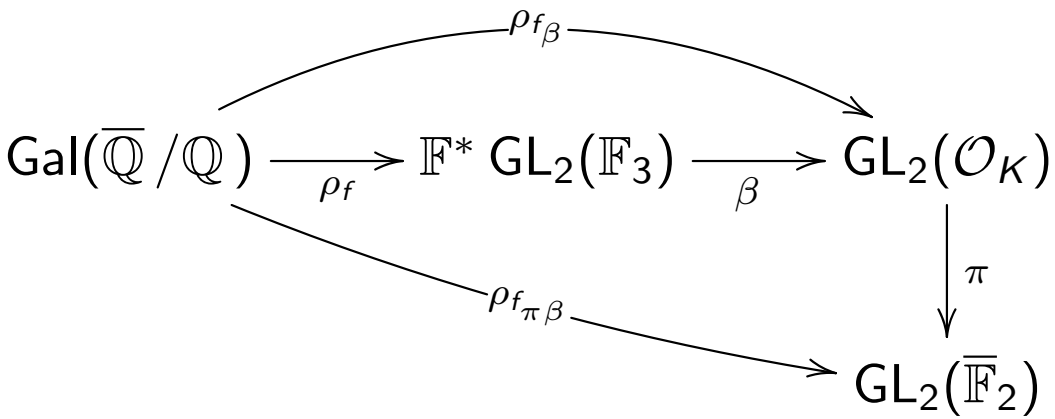
Can we determine $f_\beta(T_p)$, $f_\beta(\langle p \rangle)$ for all p?

Yes for the primes dividing the level and 3

No for the unramified primes! Problem: distinguish elements in $\mathrm{GL}_2(\mathbb{F}_3)$ using only traces and determinants is not possible.

Solution:

check in characteristic 2 and 5.



$$\rho_{f_{\pi\beta}}(\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq \mathbb{F}'^* \times \mathsf{GL}_2(\mathbb{F}_2)$$

$$\mathbb{P}\rho_{f_{\pi\beta}}(\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \cong S_3$$

There exists a mod 2 modular form $f_{\pi\beta}$ such that $\rho_{f_{\pi\beta}} \cong \pi \circ \beta \circ \rho_f$.

Can we determine the level of $f_{\pi\beta}$?

Yes, we can bound it.

Can we determine $f_\beta(T_p)$, $f_\beta(\langle p \rangle)$ using $f_{\pi\beta}(T_p)$, $f_{\pi\beta}(\langle p \rangle)$ for all p?

Yes for the primes dividing the level and 3.

For the unramified primes there is still a problem but we have candidates i.e. a finite list of mod 2 modular forms with prescribed properties.

How can we solve this problem?

For each candidate we have a power series in characteristic 0. All power series are defined over the same ring of integers so we can reduce them modulo 5 and check if the list we obtain does occur as eigenvalue system or not. Claim: only one power series is a modular form. If this method does not work use Schaeffer's Algorithm.

Residual modular Galois representations: an algorithmic approach

Samuele Anni

University of Warwick

Algebra and Number Theory Seminar
University College Dublin
22nd September 2014

Thanks!