Image of big Galois representations and modular forms mod p

Notes by Tony Feng
for a talk by Joel Bellaiche

June 14, 2016

1 Introduction

This will be a talk about modular forms mod p, specifically:

- the coefficients,
- Hecke algebra, an attached Galois representation, and the image of the Galois representation.

Fix a prime $p > 2$ and let $\mathbb{F}$ be a finite extension of $\mathbb{F}_p$. Let $N \geq 1$ and $k \in \mathbb{Z}/(p-1)\mathbb{Z}$. Let $\mathcal{M} = \mathcal{M}_{\Gamma_0(N),k}(\mathbb{F})$ be the space of modular forms with coefficients in $\mathbb{F}$, e.g. in the sense of Katz. This is a subspace of $\mathbb{F}[[q]]$. Let

$$\mathcal{M}_0 := \{f = \sum_n a_n q^n \in \mathcal{M} \colon a_n \neq 0 \implies (n, Np) = 1\} = \bigcap_{\ell \mid Np} \ker(U_\ell \colon \mathcal{M} \to \mathcal{M}).$$

Proposition 1.1. *For $f = \sum a_n q^n \in \mathcal{M}_0$,*

$$\#\{\ell \leq x, a_\ell \neq 0\} \sim \delta(f) \frac{x}{\log x}.$$

If $f \neq 0$ then $\delta(f) > 0$.

Corollary 1.2. *If $f = \sum a_n q^n$ and $g = \sum b_n q^n \in \mathcal{M}_0$, and $a_\ell = b_\ell$ for almost all ℓ, then $f = g$.*

This would be trivial if f, g were eigenforms, but we want to stay away from that assumption.

We would like to understand how $\delta(f)$ changes as f varies over the space of modular forms. We will focus on a special class of modular forms.

2 Cyclotomic forms

Definition 2.1. We say that $f \in \mathcal{M}_0$ is cyclotomic if there exists q such that a_ℓ depends only on $\ell \mod q$.

It is true but nontrivial that $T_\ell f$ depends on $\ell \mod N$. The converse is immediate, so the two notions are in fact equivalent.

Fact. There exists a sequence of cyclotomic forms $f_n \in \mathcal{M}_0$ such that $\delta(f_n) \to 0$. So we cannot hope for any uniform control of $\delta(f)$ if we allow sequences of cyclotomic forms.

Remark 2.2. The name comes from analogy with *dihedral forms*, which have analogous definition with target being a dihedral group instead.

Let A be a closed subalgebra generated by the T_ℓ in $\mathrm{End}_{\mathbb{F}}(\mathcal{M}_0)$. Then A is a semi-local ring. If $\mathbb{F}$ is large enough, then

$$A = \prod_{\overline{\rho} \in \mathcal{R}} A_{\overline{\rho}}$$

where each $A_{\overline{\rho}}$ is a local ring and the index set $\mathcal{R}$ is a finite set of semi-simple Galois representations $G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\mathbb{F})$. This induces a decomposition

$$\mathcal{M}_0 = \bigoplus_{\rho \in R} \mathcal{M}_{\overline{\rho}}$$

where $\mathcal{M}_{\overline{\rho}} = A_{\overline{\rho}} \mathcal{M}_0$ is the set of generalized eigenforms f for the T_ℓ with eigenvalue $\mathrm{Tr}\,\overline{\rho}(\mathrm{Frob}_\ell)$.

We have a pairing

$$A \times \mathcal{M}_0 \to \mathbb{F}$$

sending $(t, f) \mapsto a_1(tf)$, and it is perfect.

We will shortly define a subspace $\mathcal{M}_{\overline{\rho},\text{special}} \subset \mathcal{M}_{\overline{\rho}}$. The punchline is that

Theorem 2.3. *For all $\overline{\rho}$, there exists $c > 0$ such that for all $f \in \mathcal{M}_{\overline{\rho}} - \mathcal{M}_{\overline{\rho},special}$, we have $\delta(f) > c$.*

Theorem 2.4. *$\mathcal{M}_{\overline{\rho},special}$ is of infinite codimension in $\mathcal{M}_{\overline{\rho}}$.*

Classification of $\overline{\rho}$ according to the projective image. Recall that the projectivization of the image can be

- cyclic,
- dihedral,
- *(exceptional image)* A_4, S_4, A_5,
- *(large image)* $\mathrm{PGL}_2(\mathbb{F}_q), \mathrm{PSL}_2(\mathbb{F}_q)$ for $\mathbb{F}_q \subset \mathbb{F}$.

The representation $\overline{\rho}$ is irreducible except in the cyclic case.

Theorem 2.5. *If $\overline{\rho}$ has exceptional or large image, then $\mathcal{M}_{\overline{\rho},special}$ is of finite dimension. If $\overline{\rho}$ is reducible and the projectivization of $\operatorname{Im}\overline{\rho} \neq \mathbb{Z}/2$, then $\mathcal{M}_{\overline{\rho},special}$ consists of the cyclotomic forms.*

The goal for the rest of the talk is to explain the definition of a special modular form.

3 Pseudorepresentations

Recall that a *pseudorepresentation* of a group G on an algebra A consists of the data of

- $t\colon G \to A$,
- $d\colon G \to A^*$
- $t(1) = 2$
- $t(xy) = t(yx)$
- $t(xy) + d(y)t(xy^{-1}) = t(x)t(y)$.

Proposition 3.1. *There exists a unique pseudo-representation*

$$t, d\colon G_{\mathbb{Q},Np} \to A_{\overline{\rho}}$$

such that $t(\mathrm{Frob}_\ell) = T_\ell \in A_{\overline{\rho}}$ and $d = \det\overline{\rho}$ (meaning that d takes image in $\mathbb{F} \subset A_{\overline{\rho}}$).

Moreover, this is a deformation of $\overline{\rho}$ in the sense that

$$t \mod \mathfrak{m}_{A,\overline{\rho}} = \operatorname{Tr}\overline{\rho}$$
$$d \mod \mathfrak{m}_{A,\overline{\rho}} = \det\overline{\rho}$$

Proposition 3.2. *$A_{\overline{\rho}}$ is generated as a closed vector space by the T_ℓ.*

This implies the first Proposition I stated that $\delta(f) > 0$.

4 Generalized Matrix Algebras (GMA)

Let B, C be A-modules (in this talk they will be finite), with a multiplication

$$m\colon B \otimes C \to A$$

satisfying some properties. Then we can form

$$R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$$

and the properties are rigged to make R an associative algebra.

We say that R is *faithful* if m is a perfect pairing. There are maps

$$\mathrm{Tr}\colon R \to A$$
$$\det\colon R \to A$$

with the same formulas as usual.

Theorem 4.1. *There exists a faithful GMA R and morphism $\rho\colon G_{\mathbb{Q},Np} \to R^*$ such that $\mathrm{Tr}\,\rho = t$ and $\det\rho = d$. It can be assumed that $\rho(G_{\mathbb{Q},Np})$ generates R as an A-module, in which case (ρ, R) is unique.*

5 Pink's theory

Let $\mathcal{A}$ be a local complete ring with residue field $\mathbb{F}$ finite of characteristic $p > 2$. Let R be a GMA; we will be interested in $R = M_2(A)$ or $\begin{pmatrix} A & B \\ C & A \end{pmatrix}$ with $BC \subset \mathfrak{m}_A$.

Definition 5.1. Define $SR^1 = \{x \in R^*, \det x = 1, x \equiv \mathrm{Id} \mod \mathfrak{m}_R\}$. This is a pro-$p$ group.

Define $(\mathrm{rad}\,R)^0 = \{y \in \mathrm{rad}\,R, \mathrm{tr}(y) = 0\}$. This is the Lie algebra of SR^1.

Pink defined a logarithm

$$\theta\colon SR^1 \to (\mathrm{rad}\,R)^0$$

sending $x \mapsto x - \frac{\mathrm{tr}\,\rho(x)}{2}$. This is a homeomorphism with inverse

$$\theta^{-1}(y) = y + \sqrt{1 + \frac{\mathrm{Tr}(y^2)}{2}}\,\mathrm{Id}\,.$$

Theorem 5.2. *Let Γ be a closed subgroup of SR^1. Let L be the closed additive subgroup of $(\mathrm{rad}\,R)^0$ generated by $\theta(\Gamma)$. Then L is a Lie subring of $(\mathrm{rad}\,R)^0$. (This means a subgroup stable by Lie bracket.)*

Proof. Check that

$$\theta(x)\theta(y) - \theta(y)\theta(x) = \theta(xy) - \theta(yx).$$

□

We have $\Gamma \subset \theta^{-1}(L)$, but this is not always an equality.

Theorem 5.3. *If $L_2 = \overline{[L, L]}$ and $\Gamma_2 = \overline{(\Gamma, \Gamma)}$ then $\Gamma_2 = \theta^{-1}(L_2)$.*

6 Large image

Let $\overline{\rho}\colon G_{\mathbb{Q},Np} \to R^*$ and G be the image. Let $\Gamma = G \cap SR^1$. We have an exact sequence (using constancy of the determinant)

$$1 \to \Gamma \to G \to \mathrm{Im}\,\overline{\rho} \to 1.$$

Let L be the assocsiated Pink algebra.

Theorem 6.1. *Suppose $\overline{\rho}$ is exceptional or large image. Then there exists a closed subgroup I of $A_{\overline{\rho}}$ with $I^2 \subset I$, such that $\mathbb{F}I = \mathfrak{m}_{A,\overline{\rho}}$ and*

$$\mathbb{F}_{p^2}L = \begin{pmatrix} I & I \\ I & I \end{pmatrix}^0$$

and $\Gamma = \theta^{-1}(L)$.

Theorem 6.2. *Suppose $\overline{\rho}$ is reducible, $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$. Then there exists a subgroup $I \subset A$ with $I^3 \subset I$ and $BC \subset I$ such that*

$$\mathbb{F}L = \begin{pmatrix} I & B \\ C & I \end{pmatrix}^0 .$$

We can finally explain what a special form is.

Definition 6.3. f is *special* if for all $g \in G$ with $g^2 = 1$, f is orthogonal to $\mathrm{Tr}(gL_2) \subset A$.