Counting modular forms with a Galois representation mod p and the Atkin-Lehner eigenvalue at p fixed simultaneously

Samuele Anni

Novenas Jornadas de Teoría de Números 2022

Universidad de la Rioja

Aix-Marseille université

INSTITUT DE MATHÉMATIQUES de MARSEILLE

Introduction

Modular forms

Let n be a positive integer, the congruence subgroup $\Gamma_0(n)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ given by

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : n \mid c \right\}.$$

Given a pair of positive integers n (level) and k (weight), a **modular form** f for $\Gamma_0(n)$ is an holomorphic function on the complex upper half-plane $\mathbb{H}$ satisfying

$$f(\gamma z) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad \forall \gamma \in \Gamma_0(n), z \in \mathbb{H}$$

and a growth condition for the coefficients of its power series expansion

$$f(z) = \sum_{0}^{\infty} a_m q^m, \qquad \text{where} \qquad q = e^{2\pi i z}.$$

Newforms

There are families of operators acting on the space of modular forms. In particular, the **Hecke operators** T_p for every prime p. These operators describe the interplay between different group actions on the complex upper half-plane.

We will consider only cuspidal **newforms**: cuspidal modular forms ($a_0 = 0$), normalized ($a_1 = 1$), which are eigenforms for the Hecke operators and arise from level n.

We will denote by $S_k(n, \mathbb{C})$ the space of cuspforms and by $S_k(n, \mathbb{C})^{new}$ the subspace of newforms.

Hecke eigenvalue field

Definition

Let f be a newform, $f = \sum a_m q^m$. Then $\mathbb{Q}_f = \mathbb{Q}(\{a_m\})$ is a number field, called the **Hecke eigenvalue field** *of f.*

The set $\{a_m\}$ is a **Hecke eigenvalue system**.

Hecke eigenvalue field

Definition

Let f be a newform, $f = \sum a_m q^m$. Then $\mathbb{Q}_f = \mathbb{Q}(\{a_m\})$ is a number field, called the **Hecke eigenvalue field** *of f.*
The set $\{a_m\}$ is a **Hecke eigenvalue system**.

Example: $S_2(77, \mathbb{C})^{new}$

$f_0(q) = q - 3q^3 - 2q^4 - q^5 - q^7 + 6q^9 - q^{11} + 6q^{12} - 4q^{13} + 3q^{15} + \dots$
$f_1(q) = q + q^3 - 2q^4 + 3q^5 + q^7 - 2q^9 - q^{11} - 2q^{12} - 4q^{13} + 3q^{15} + \dots$
$f_2(q) = q + q^2 + 2q^3 - q^4 - 2q^5 + 2q^6 - q^7 - 3q^8 + q^9 - 2q^{10} + q^{11} + \dots$
$f_{3,4}(q) = q + \alpha q^2 + (-\alpha + 1)\, q^3 + 3q^4 - 2q^5 + (\alpha - 5)\, q^6 + q^7 + \dots$
where α satisfies $x^2 - 5 = 0$.
The Hecke eigenvalue fields are $\mathbb{Q}$ for f_0, f_1, f_2 and $\mathbb{Q}(\sqrt{5})$ for $f_{3,4}$.

Hecke algebra

Definition

*The **Hecke algebra** $\mathbb{T}(n,k)$ is the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S_k(n,\mathbb{C}))$ generated by Hecke operators T_p for every prime p.*

Newforms can be seen as ring homomorphisms $f : \mathbb{T}(n,k) \to \overline{\mathbb{Q}}$.

Residual modular Galois representations

Theorem (Deligne, Serre, Shimura)

Let n and k be positive integers. Let $\mathbb{F}$ be a finite field of characteristic ℓ, with $\ell \nmid n$, and $f : \mathbb{T}(n,k) \twoheadrightarrow \mathbb{F}$ a surjective ring homomorphism. Then there is a (unique) continuous semi-simple representation:

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

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

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

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

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

Example: for $n = 1$, $k = 22$ and $\ell = 23$, the number field corresponding to $\mathbb{P}\bar{\rho}_f$ (Galois group isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{23})$) 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 ($\#\mathbb{F} \leq 53$).

p-new forms

Fix $p \geq 5$ a prime, N a level prime to p, and let $k \geq 2$ be a weight.

Let $S_k := S_k(\Gamma_0(Np), \overline{\mathbb{Q}}_p)$ be the space of p-new (i.e., not coming from level N) cuspidal modular forms of level Np and weight k with coefficients in $\overline{\mathbb{Q}}_p$.

The Atkin-Lehner involution

The Atkin-Lehner involution

Fix $p \geq 5$ a prime and N a level prime to p, there exist $x, y, z, t \in \mathbb{Z}$ for which the matrix

$$W_p = \begin{pmatrix} px & y \\ Npz & pt \end{pmatrix}$$

has determinant p.

The matrix W_p normalizes the group $\Gamma_0(Np)$, and for any weight k it induces a linear operator w_p on the space of cusp forms S_k that commutes with the Hecke operators T_q for all $q \nmid n$ and acts as its own inverse.

The Atkin-Lehner involution

The linear operator w_p does not depend on the choice of x, y, z, t and is called the **Atkin-Lehner involution** of S_k.

Any cusp form f in S_k which is an eigenform for all T_q with $q \nmid N$ is also an eigenform for w_p, with eigenvalue ± 1.

The matrix W_p induces an automorphism of the modular curve $X_0(Np)$ that is also denoted w_p.

The Atkin-Lehner involution w_p acts on S_k and splits it into a direct sum of plus/minus eigenspaces:

$$S_k = S_k^+ \oplus S_k^-.$$

Since we have dimension formulas for $s_k := \dim S_k$, in order to understand the dimensions $s_k^\pm = \dim S_k^\pm$ of the Atkin-Lehner eigenspaces, it suffices to understand the difference

$$d_k := s_k^+ - s_k^-.$$

$s_k^{\pm} = \dim S_k(p)^{\pm}$

$p = 5$

k	s_k^+	s_k^-
2	0	0
4	1	0
6	0	1
8	2	1
10	1	2
12	3	2
14	2	3
16	4	3
18	3	4
20	5	4
22	4	5
24	6	5
26	5	6
28	7	6
30	6	7

$d_k = \pm 1$

$p = 11$

k	s_k^+	s_k^-
2	0	1
4	2	0
6	1	3
8	4	2
10	3	5
12	6	4
14	5	7
16	8	6
18	7	9
20	10	8
22	9	11
24	12	10
26	11	13
28	14	12
30	13	15

$d_k = \pm 2$

$p = 59$

k	s_k^+	s_k^-
2	0	5
4	10	4
6	9	15
8	20	14
10	19	25
12	30	24
14	29	35
16	40	34
18	39	45
20	50	44
22	49	55
24	60	54
26	59	65
28	70	64
30	69	75

$d_k = \pm 6$

$p = 101$

k	s_k^+	s_k^-
2	1	7
4	16	9
6	17	24
8	33	26
10	34	41
12	50	43
14	51	58
16	67	60
18	68	75
20	84	77
22	85	92
24	101	94
26	102	109
28	118	111
30	119	126

$d_k = \pm 7$

Classical result that d_k is constant in absolute value and alternates in sign, modulo a correction for the "missing" E_2 in weight 2: Let

$$d_k^* := \begin{cases} d_k - 1 & \text{if } k = 2; \\ d_k, & \text{if } k \geq 4 \text{ even.} \end{cases}$$

Theorem (Fricke, Yamauchi, Momose, Ogg, Wakatsuki, Helfgott, Martin et al.)

We have

$$d_k^* = (-1)^{\frac{k}{2}} \frac{\#FP}{2},$$

where $\#FP$ *is the number of fixed points of the Atkin-Lehner involution* w_p *on* $X_0(Np)$.

Theorem (Fricke, Yamauchi, Momose, Ogg, Wakatsuki, Helfgott, Martin et al.)

We have

$$d_k^* = (-1)^{\frac{k}{2}} \frac{\#FP}{2},$$

where $\#FP$ is the number of fixed points of the Atkin-Lehner involution w_p on $X_0(Np)$.

The fixed points of w_p on $X_0(Np)$ correspond to elliptic curves with level structure and CM by $\sqrt{-p}$, in fact the d_k are closely related to class numbers.

Theorem (Fricke, Yamauchi, Momose, Ogg, Wakatsuki, Helfgott, Martin et al.)

We have

$$d_k^* = (-1)^{\frac{k}{2}} \frac{\#FP}{2},$$

where $\#FP$ is the number of fixed points of the Atkin-Lehner involution w_p on $X_0(Np)$.

The fixed points of w_p on $X_0(Np)$ correspond to elliptic curves with level structure and CM by $\sqrt{-p}$, in fact the d_k are closely related to class numbers.

$$\#\mathrm{FP} = c_p \cdot h(\sqrt{-p}) \cdot \prod_{q|N,\ \text{prime}} \left(1 + \left(\frac{-4p}{q}\right)\right).$$

A refinement - Main theorem

Our aim - joint work with A. Ghitza (University of Melbourne) and A. Medvedovsky (Boston University)

Systems of mod-p prime-to-Np Hecke eigenvalues correspond to continuous semisimple Galois representations $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ which are odd and unramified outside Np.

Our aim - joint work with A. Ghitza (University of Melbourne) and A. Medvedovsky (Boston University)

Systems of mod-p prime-to-Np Hecke eigenvalues correspond to continuous semisimple Galois representations $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ which are odd and unramified outside Np.

We can decompose

$$S_k = \bigoplus_{\bar{\rho}} S_{k,\bar{\rho}},$$

where $S_{k,\bar{\rho}}$ is the span of eigenforms with mod-p eigensystems corresponding to $\bar{\rho}$.

Since w_p commutes with prime-to-Np Hecke operators, $S_{k,\bar{\rho}}$ also splits into Atkin-Lehner eigenspaces:

$$S_{k,\bar{\rho}} = S^+_{k,\bar{\rho}} \oplus S^-_{k,\bar{\rho}},$$

once again let $s^\pm_{k,\bar{\rho}}$ denote $\dim S^\pm_{k,\bar{\rho}}$.

The behavior of dimensions $s_{k,\bar{\rho}} := \dim S_{k,\bar{\rho}}$ have been studied by Jochnowitz ($N = 1$) and Bergdall-Pollack, so once again we focus on the dimension difference $d_{k,\bar{\rho}} := s^{+}_{k,\bar{\rho}} - s^{-}_{k,\bar{\rho}}$.

As before, $k = 2$ and $\bar{\rho}$ forces us to make an adjustment, so let

$$d^{*}_{k,\bar{\rho}} := \begin{cases} d_{k,\bar{\rho}} - 1, & \text{if } k = 2 \text{ and } \bar{\rho} = 1 \oplus \omega \\ d_{k,\bar{\rho}}, & \text{otherwise,} \end{cases}$$

where ω is the mod p cyclotomic character.

Theorem (Anni, Ghitza, Medvedovsky)

For $k \geq 2$ and any $\Gamma_0(Np)$-modular $\bar{\rho}$ we have

$$d^*_{k+2,\bar{\rho}[1]} = -d^*_{k,\bar{\rho}}.$$

Here $\bar{\rho}[1]$ is a Tate twist: on the Galois side it corresponds to tensoring $\bar{\rho}$ by the mod-p cyclotomic character ω; on the Hecke side by having T_ℓ act by ℓT_ℓ.

From this result and related formulations we recover both the classical alternation statement $d^*_{k+2} = -d^*_k$ and the Bergdall-Pollack dimension formulas, but with very different techniques.

Example: $p = 5,\ N = 23$

k	(s_k^+, s_k^-)
2	$(5, 6)$
4	$(18, 16)$
6	$(28, 30)$
8	$(42, 40)$
10	$(52, 54)$
12	$(66, 64)$
14	$(76, 78)$
16	$(90, 88)$
18	$(100, 102)$
20	$(114, 112)$

$$d_k = \pm 2$$

Example: $p = 5,\ N = 23$

In weight k for $\bar{\rho}$ the entry is $\left(s^{+}_{k,\tau}, s^{-}_{k,\tau}\right)$ for $\tau = \bar{\rho}[\frac{k-2}{2}]$.

Two twists of $\bar{\rho}$ can appear in any given weight: $\bar{\rho}$ and its quadratic twist $\bar{\rho}' = \bar{\rho}[2] = \bar{\rho} \otimes \omega^2$.

- e is the Eisenstein thread: $e = 1 \oplus \omega$ in weight 2;
- p is a peu ramifié form, appearing in weight 2;
- t is a très ramifié form, here appearing in weight 2;
- s is an $\mathbb{F}_{5^4}$-Galois orbit of 4 très ramifié forms appearing in weight 2;
- f, g, h are locally reducible, globally irreducible forms; h is an $\mathbb{F}_{5^3}$-orbit of 3 forms.

Example: $p = 5,\ N = 23$

$k \backslash \bar{\rho}$	e	e'	p	p'	t	t'	$s \times 4$	$s' \times 4$	$f, f'; g, g'; h, h' \times 3$	Total
2	$(0,0)$	$(0,0)$	$(3,2)$	$(0,0)$	$(2,0)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,0)$	$(5,6)$
4	$(2,1)$	$(0,0)$	$(2,3)$	$(0,0)$	$(0,2)$	$(0,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(18,16)$
6	$(1,2)$	$(1,1)$	$(3,2)$	$(5,5)$	$(2,0)$	$(2,2)$	$(0,1)$	$(1,1)$	$(1,1)$	$(28,30)$
8	$(2,1)$	$(3,3)$	$(2,3)$	$(5,5)$	$(0,2)$	$(2,2)$	$(1,0)$	$(1,1)$	$(2,2)$	$(42,40)$
10	$(2,3)$	$(3,3)$	$(8,7)$	$(5,5)$	$(4,2)$	$(2,2)$	$(1,2)$	$(1,1)$	$(2,2)$	$(52,54)$
12	$(5,4)$	$(3,3)$	$(7,8)$	$(5,5)$	$(2,4)$	$(2,2)$	$(2,1)$	$(1,1)$	$(3,3)$	$(66,64)$
14	$(4,5)$	$(4,4)$	$(8,7)$	$(10,10)$	$(4,2)$	$(4,4)$	$(1,2)$	$(2,2)$	$(3,3)$	$(76,78)$
16	$(5,4)$	$(6,6)$	$(7,8)$	$(10,10)$	$(2,4)$	$(4,4)$	$(2,1)$	$(2,2)$	$(4,4)$	$(90,88)$
18	$(5,6)$	$(6,6)$	$(13,12)$	$(10,10)$	$(6,4)$	$(4,4)$	$(2,3)$	$(2,2)$	$(4,4)$	$(100,102)$
20	$(8,7)$	$(6,6)$	$(12,13)$	$(10,10)$	$(4,6)$	$(4,4)$	$(3,2)$	$(2,2)$	$(5,5)$	$(114,112)$

Bergdall and Pollack use Ash-Stevens, a fundamentally characteristic p technique for filtering cohomology of modular symbols, to derive their dimension formulas. But Ash-Stevens has nothing to say about Atkin-Lehner, in part because the Atkin-Lehner operator requires inverting p.

On the other hand, the classical complex methods - trace formulae, Gauss-Bonnet, Riemann-Hurwitz - do not know anything about $\bar{\rho}$.

Idea

Combining the **trace formula** (Zagier - Cohen - Osterlé - Cohen - Strömberg and Skoruppa - Zagier - Popa) with an **algebra theorem**, a refinement of Brauer-Nesbitt.

An algebra theorem, and the method of proof for the main theorem

The basic question

Let M be a finite free $\mathbb{Z}_p$-module with an action of a linear operator T.

Question

How much information does one need to know about the traces of $\mathbb{Z}_p[T]$ acting on M in order to know the structure of $M \otimes \mathbb{F}_p$ as an $\mathbb{F}_p[T]$-module, at least up to semisimplification?

Knowing $\mathrm{Tr}(T^n|M)$ for enough n as an element of $\mathbb{Z}_p$ is plenty:

Theorem (Brauer-Nesbitt)

Let k be a field and V a $k[T]$-module that is finite-dimensional as a k-vector space. If k has characteristic zero or if $\mathrm{char}\, k > \dim_k V$, then V is determined up to semisimplification by $\mathrm{Tr}(T^n|V)$ for all n with $1 \leq n \leq \dim_k V$.

But this very precise characteristic-zero information is much more than we need: we merely want to understand M modulo p.

On the other hand, knowing all the $\mathrm{Tr}(T^n|M)$ modulo p is not enough to determine $M \otimes \mathbb{F}_p$.

Example

If M has rank p and T acts on M as multiplication by a scalar α in $\mathbb{Z}_p$ then $\mathrm{Tr}(T^n|M) = p\alpha^n$ for all $n \geq 0$. Thus $\mathrm{Tr}(T^n|M) \equiv 0 \mod p$ for all n, and we cannot recover $\alpha \mod p$ from this trace data.

Since knowing $\mathrm{Tr}(T^n|M)$ in $\mathbb{Z}_p$ is too much and knowing $\mathrm{Tr}(T^n|M)$ modulo p is not enough, one can ask for some kind of in-between criterion depending on $\mathrm{Tr}(T^n|M)$ modulo *powers* of p.

Theorem (Anni, Ghitza, Medvedovsky + Gessel)

Let M and N be two finite free $\mathbb{Z}_p$-modules of the same rank d, each with an action of an operator T. Then $\bar{M}^{\mathrm{ss}} \cong \bar{N}^{\mathrm{ss}}$ as $\mathbb{F}_p[T]$-modules if and only if for every n with $1 \leq n \leq d$ we have

$$\mathrm{Tr}(T^n|M) \equiv \mathrm{Tr}(T^n|N) \mod pn.$$

Here $\bar{M}$ and $\bar{N}$ are the $\mathbb{F}_p[T]$-modules $M \otimes \mathbb{F}_p$ and $N \otimes \mathbb{F}_p$, respectively, and $\bar{M}^{\mathrm{ss}}$ and $\bar{N}^{\mathrm{ss}}$ refers to their semisimplification.

Remarks

Remarks

- Since every prime except p is invertible, congruence modulo pn is the same as congruence modulo $p^{1+v_p(n)}$, where $v_p : \mathbb{Z}_p \to \mathbb{Z}_{\geq 0}$ is the normalized p-adic valuation.

Remarks

- Since every prime except p is invertible, congruence modulo pn is the same as congruence modulo $p^{1+v_p(n)}$, where $v_p : \mathbb{Z}_p \to \mathbb{Z}_{\geq 0}$ is the normalized p-adic valuation.
- This completely resolves our example with $T = \alpha$ acting on $M = \mathbb{Z}_p^{\oplus p}$: knowing $\mathrm{Tr}(T^p|M) = p\alpha^p$ modulo p^2 is knowing α^p modulo p, which in turn determines α modulo p uniquely. Yet this is not enough to pin down α in $\mathbb{Z}_p$.

Remarks

- Since every prime except p is invertible, congruence modulo pn is the same as congruence modulo $p^{1+v_p(n)}$, where $v_p : \mathbb{Z}_p \to \mathbb{Z}_{\geq 0}$ is the normalized p-adic valuation.
- This completely resolves our example with $T = \alpha$ acting on $M = \mathbb{Z}_p^{\oplus p}$: knowing $\mathrm{Tr}(T^p|M) = p\alpha^p$ modulo p^2 is knowing α^p modulo p, which in turn determines α modulo p uniquely. Yet this is not enough to pin down α in $\mathbb{Z}_p$.
- The "only if" direction is trivial when all the eigenvalues of M, N are in $\mathbb{Z}_p$. Thus the heart is the "if" direction.

Remarks

- Since every prime except p is invertible, congruence modulo pn is the same as congruence modulo $p^{1+v_p(n)}$, where $v_p : \mathbb{Z}_p \to \mathbb{Z}_{\geq 0}$ is the normalized p-adic valuation.
- This completely resolves our example with $T = \alpha$ acting on $M = \mathbb{Z}_p^{\oplus p}$: knowing $\mathrm{Tr}(T^p|M) = p\alpha^p$ modulo p^2 is knowing α^p modulo p, which in turn determines α modulo p uniquely. Yet this is not enough to pin down α in $\mathbb{Z}_p$.
- The "only if" direction is trivial when all the eigenvalues of M, N are in $\mathbb{Z}_p$. Thus the heart is the "if" direction.
- The result generalizes to p-adic fields that are not too ramified.

The result is a combinatorial statement about deep congruences between power-sum symmetric functions implying simple congruences between corresponding elementary symmetric functions.

Let A be a torsion-free $\mathbb{Z}_{(p)}$-algebra and assume that A is a domain.

Theorem (Anni, Ghitza, Medvedovsky)

Let P, Q be monic polynomials in $A[X]$. Then

$$\bar{P} \equiv \bar{Q} \quad \text{in } A/\mathfrak{a}[X]$$

if and only if

$$\mathfrak{p}_n(P) \equiv \mathfrak{p}_n(Q) \mod n\mathfrak{a}$$

for all $1 \leq n \leq \max\{\deg P, \deg Q\}$.

In particular here we do not require P and Q to be of the same degree; nor do we require $\mathfrak{a}$ to be prime (nor indeed A to be a domain).

The proof uses combinatorial theory of symmetric functions, specifically, formulas that express elementary symmetric functions in terms of power-sum functions and vice versa.

A generalization to virtual modules

Corollary

Let M_1, M_2, N_1, N_2 be free $\mathbb{Z}_p$-modules of finite rank, each with an action of an operator T. Suppose we have fixed T-equivariant embeddings $\iota_1 : \bar{N}_1 \hookrightarrow \bar{M}_1$ and $\iota_2 : \bar{N}_2 \hookrightarrow \bar{M}_2$ and consider the quotients $W_1 := \bar{M}_1/\iota_1(\bar{N}_1)$ and $W_2 := \bar{M}_2/\iota_2(\bar{N}_2)$. Then

$$W_1^{\mathrm{ss}} \cong W_2^{\mathrm{ss}}$$

as $\mathbb{F}_p[T]$-modules if and only if for every $n \geq 0$ we have

$$v_p\big(\mathrm{Tr}(T^n|M_1) - \mathrm{Tr}(T^n|N_1) - \mathrm{Tr}(T^n|M_2) + \mathrm{Tr}(T^n|N_2)\big) \geq 1 + v_p(n).$$

The essential point is that we do not assume that there are embeddings $N_i \hookrightarrow M_i$ over $\mathbb{Z}_p$, but only after base change to $\mathbb{F}_p$.

Back to the main theorem

For N prime to p and $k \geq 2$, write $M_k(Np, \mathbb{Z}_p)$ for the space of classical modular forms of weight k and level Np, viewed via the q-expansion map as a subspace of a finite free $\mathbb{Z}_p$-module.
Let $M_k(Np, \mathbb{F}_p)$ denote the image of $M_k(Np, \mathbb{Z}_p)$ in $\mathbb{F}_p[\![q]\!]$.

For $k \geq 4$, multiplication by the level-p and weight-2 Eisenstein form $E_{2,p}$, normalized to be in $1 + p\mathbb{Z}_p[\![q]\!]$, induces an embedding

$$M_{k-2}(Np, \mathbb{F}_p) \hookrightarrow M_k(Np, \mathbb{F}_p);$$

let

$$W_k(Np) := M_k(Np, \mathbb{F}_p)/M_{k-2}(Np, \mathbb{F}_p)$$

denote the quotient.

The tame case - level N

Let $p \geq 5$, there is a Hecke-equivariant embedding

$$M_{k-p+1}(N, \mathbb{F}_p) \hookrightarrow M_k(N, \mathbb{F}_p)$$

induced by by multiplication by the form E_{p-1}, the Hasse invariant.
The quotient module $W_k(N)$ has been carefully studied.
If $k \geq p+1$ we have:

- $W_k(N) \cong W_{k+p^2-1}(N)$, Serre 1987
- $W_k(N)[1] \cong W_{k+p+1}(N)$, Robert 1980 for $N = 1$, Jochnowitz
- $W_k(N) \cong W_{pk}(N)$, Serre 1996

Let $W_k^0(N) := S_k(N, \mathbb{F}_p)/E_{p-1}S_{k-p+1}(N, \mathbb{F}_p)$, for $k \geq p+3$, we have

$$W_k(N) \cong W_k^0(N).$$

The wild case - level Np

None of the previous statements hold in level Np, but we have observed (and proved) some patterns:

- $W_{k+p^2-p}(Np) \cong W_k(Np)$, the same for $W_k^0(Np)$;
- $W_k(Np)[1]^{ss} \cong W_{k+2}(Np)^{ss}$;
- $W_k(Np)[\frac{p-1}{2}]^{ss} \cong W_k(Np)^{ss}$.

The proofs do not follow the previous techniques, all use the trace formula.

We use the trace formula to establish the required congruences.

The trace formula

Fix a natural number N and a prime number ℓ, then for all $n \geq 0$ and all even $k \geq 4$ we have

$$\mathrm{Tr}\left(T_{\ell^n} \mid S_k(N)\right) = t_{n,k} = A_1(\ell^n, k) - A_2(\ell^n, k) - A_3(\ell^n, k).$$

A_1 is the parabolic term, A_2 is the elliptic term, and A_3 the hyperbolic term.

Let us introduce the following notation to present the linear combination of traces appearing in the following : for any pair of integers n and k, and any weight k as above let

$$\delta^{m}_{n,k} := \ell^{m(k+p-2)} t_{n,k+p-1} - \ell^{m(k-1)} t_{n,k}.$$

Let p be a prime, $p > 2$. Let $k \geq 2$, $h \geq 2$ be integers, $a \in \mathbb{Z}/(p-1)\mathbb{Z}$ such that $k + 2a \equiv h \mod p-1$.

Fix a level M that may or may not be divisible by p.

Set for $n \geq 0$

$$B(n,k,h,a) = \ell^{na}\delta^0_{n,k} - \delta^0_{n,h}$$

and for $n \geq 2$

$$C(n-2,k,h,a) = \ell^{na}\delta^1_{n-2,k} - \delta^1_{n-2,h}.$$

Theorem (Anni, Ghitza, Medvedovsky)

Suppose that for all but finitely many primes ℓ we have

1. *for $n = 0$:*
$$B(0, k, h, a) = 0;$$
2. *for $n = 1$:*
$$B(1, k, h, a) \equiv 0 \pmod{p};$$
3. *for all $n \geq 2$:*
$$B(n, k, h, a) \equiv C(n-2, k, h, a) \pmod{p^{1+v_p(n)}}.$$

Then

$$W_{k+p-1}(M)[a]^{\mathrm{ss}} = W_{h+p-1}(M)^{\mathrm{ss}}.$$

Using the previous corollary, we deduce statements about dimensions.

Generalisations with $\bar{\rho}$ fixed and/or fixed Atkin-Lehner.

Let $M_k(Np, \mathbb{Z}_p)$ be the lattice of forms in $M_k(Np, \mathbb{Q}_p)$ with integral q-expansions at infinity, and let

$$M_k(Np, \mathbb{Z}_p)^{\pm} := M_k(Np, \mathbb{Z}_p) \cap M_k(Np, \mathbb{Q}_p)^{\pm}.$$

Then $M_k(Np, \mathbb{Z}_p)^{\pm}$ are integral lattices inside the Atkin-Lehner eigenspaces, and may be reduced modulo p: let

$$M_k(Np, \mathbb{F}_p)^{\pm} := M_k(Np, \mathbb{Z}_p)^{\pm} \otimes \mathbb{F}_p.$$

Let

$$E^{\pm}_{p-1}(z) := E_{p-1}(z) \pm p^{(p-1)/2} E_{p-1}(pz)$$

one can check that $E^{\pm}_{p-1}$ is a form of level p with w_p eigenvalue ± 1 and mod-p q-expansion congruent to 1. Therefore for any signs $\epsilon, \eta \in \{\pm 1\}$ multiplication by $E^{\epsilon/\eta}_{p-1}$ gives embeddings

$$M_{k-p+1}(Np, \mathbb{F}_p)^{\eta} \hookrightarrow M_k(Np, \mathbb{F}_p)^{\epsilon}.$$

Let $W^{\epsilon,\eta}_k(Np)$ be the quotient, a Hecke module

Theorem (Anni, Ghitza, Medvedovsky)

For any signs ϵ, η and any $k \geq 2$ we have

$$W_{k+2}^{-\epsilon,-\eta}(Np)^{\mathrm{ss}} \cong W_k^{\epsilon,\eta}(Np)[1]^{\mathrm{ss}}.$$

Proof of the main theorem

For cusp forms:

$$W_k(Np)^{0,\epsilon\eta} := S_k(Np,\mathbb{F}_p)^\epsilon / S_{k-p+1}(Np,\mathbb{F}_p)^\eta$$

and

$$W_k(Np)^{0,\epsilon\eta}[1]^{\mathrm{ss}} = W_{k+2}(Np)^{0,-\epsilon-\eta,\mathrm{ss}},$$

so

$$\dim W_k(Np)^{0,\epsilon\eta}[1] = \dim W_{k+2}(Np)^{0,-\epsilon-\eta}$$

Denoting by $s_k^\bullet = \dim S_k(Np)^\bullet$, we have

$$s_k^\epsilon - s_{k-p+1}^\eta = s_{k+2}^{-\epsilon} - s_{k+2-(p-1)}^{-\eta}.$$

Proof of the main theorem

On the other hand

$$W_k(Np)^{0,-\epsilon\eta}[1]^{\mathrm{ss}} = W_{k+2}(Np)^{0,\epsilon-\eta,\mathrm{ss}}$$

so

$$s_k^{-\epsilon} - s_{k-p+1}^{\eta} = s_{k+2}^{\epsilon} - s_{k+2-(p-1)}^{-\eta}.$$

Combining with $s_k^{\epsilon} - s_{k-p+1}^{\eta} = s_{k+2}^{-\epsilon} - s_{k+2-(p-1)}^{-\eta}$ we have

$$-d_k^* = d_{k+2}^*.$$

Example: $p = 5,\ N = 23$

$k \backslash \bar{\rho}$	e	e'	p	p'	t	t'	$s \times 4$	$s' \times 4$	$f, f'; g, g';$ $h, h' \times 3$	Total
2	$(0,0)$	$(0,0)$	$(3,2)$	$(0,0)$	$(2,0)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,0)$	$(5,6)$
4	$(2,1)$	$(0,0)$	$(2,3)$	$(0,0)$	$(0,2)$	$(0,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(18,16)$
6	$(1,2)$	$(1,1)$	$(3,2)$	$(5,5)$	$(2,0)$	$(2,2)$	$(0,1)$	$(1,1)$	$(1,1)$	$(28,30)$
8	$(2,1)$	$(3,3)$	$(2,3)$	$(5,5)$	$(0,2)$	$(2,2)$	$(1,0)$	$(1,1)$	$(2,2)$	$(42,40)$
10	$(2,3)$	$(3,3)$	$(8,7)$	$(5,5)$	$(4,2)$	$(2,2)$	$(1,2)$	$(1,1)$	$(2,2)$	$(52,54)$
12	$(5,4)$	$(3,3)$	$(7,8)$	$(5,5)$	$(2,4)$	$(2,2)$	$(2,1)$	$(1,1)$	$(3,3)$	$(66,64)$
14	$(4,5)$	$(4,4)$	$(8,7)$	$(10,10)$	$(4,2)$	$(4,4)$	$(1,2)$	$(2,2)$	$(3,3)$	$(76,78)$
16	$(5,4)$	$(6,6)$	$(7,8)$	$(10,10)$	$(2,4)$	$(4,4)$	$(2,1)$	$(2,2)$	$(4,4)$	$(90,88)$
18	$(5,6)$	$(6,6)$	$(13,12)$	$(10,10)$	$(6,4)$	$(4,4)$	$(2,3)$	$(2,2)$	$(4,4)$	$(100,102)$
20	$(8,7)$	$(6,6)$	$(12,13)$	$(10,10)$	$(4,6)$	$(4,4)$	$(3,2)$	$(2,2)$	$(5,5)$	$(114,112)$

Counting modular forms with a Galois representation mod p and the Atkin-Lehner eigenvalue at p fixed simultaneously

Samuele Anni

Novenas Jornadas de Teoría de Números 2022

Thank you!

Aix Marseille université

INSTITUT DE MATHÉMATIQUES de MARSEILLE