Higher congruences between modular forms

Ian Kiming, Univ. of Copenhagen

Primarily discuss work by myself, I. Chen, P. Tsaknias, G. Wiese + students J. B. Rasmussen, N. Rustom

Other related work by: R. Adibhatla, T. Berger, S. R. Dahmen + S. Yazdani, L. Dieulefait + X. Taixes i Ventosa, N. Dummigan, B. Naskrecki

Motivations:

- Refined Serre conjectures mod p^m?
- Diophantine applications?
- Understand forms mod p^m better $\rightsquigarrow$ understand p-adic reprs. attached to eigenforms better (G. Wiese)
- Simple curiosity

p prime, $p \nmid N \in \mathbb{N}$

$f = \sum_{n=1}^{\infty} a_n(f) q^n \in S_k(\Gamma_1(N))$ normalized cuspidal eigenform for all Hecke operators T_n

Galois representation

$$\rho_{f,\Lambda,p} : G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_K),$$

with $\mathcal{O}_K$ is the ring of integers of a finite extension K of $\mathbb{Q}_p$ (may depend on choice of $\mathcal{O}_K$-lattice $\Lambda \subseteq K^2$).
Reduce $\rho_{f,\Lambda,p}$ mod power of $\mathfrak{p} = \mathfrak{p}_K$: Maximal ideal of $\mathcal{O}_K$.

Define $\gamma_K(m) := (m-1)e_{K/\mathbb{Q}_p} + 1$, with $e_{K/\mathbb{Q}_p}$ the ramification index of $K/\mathbb{Q}_p$. Get ring injection:

$$\mathbb{Z}/p^m \hookrightarrow \mathcal{O}_K/\mathfrak{p}_K^{\gamma_K(m)}$$

Define ring

$$\overline{\mathbb{Z}/p^m\mathbb{Z}} := \lim_{\substack{\rightarrow \\ K}} \mathcal{O}_K/\mathfrak{p}_K^{\gamma_K(m)}$$

Get representation 'mod p^m' attached to f:

$$\rho_{f,\Lambda,p,m} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Z}/p^m\mathbb{Z}})$$

Does not depend on Λ if residual representation absolutely irreducible by Thm. of Carayol.

Different versions of the notion of a mod p^m eigenform:

- Strong eigenforms mod p^m
- Weak eigenforms mod p^m
- dc-weak eigenforms mod p^m ('dc' $=$ 'divided congruence')

Strong $\Rightarrow$ weak $\Rightarrow$ dc-weak

Consider spaces $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$ or $S = S_k(\Gamma_1(M))$
The q-expansion map $S \to \mathbb{C}[[q]]$ is *injective*

We have an action of Hecke operators T_n on S by letting them act diagonally.

The space S has an integral structure in the sense that it contains a full lattice stable under the Hecke operators T_n.

$\mathbb{T}(S) := \langle T_n \in \mathrm{End}_{\mathbb{C}}(S) | n \geq 1 \rangle_{\mathbb{Z}-\mathrm{algebra}} \subseteq \mathrm{End}_{\mathbb{C}}(S)$
Define $S(A) := \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}(S), A)$ ($\mathbb{Z}$-linear homomorphisms) for any commutative ring A
Cusp forms in S with coefficients in A.
We can talk about eigenforms in $S(A)$ (typically for all T_n with n coprime to some fixed integer).

Eigenforms mod p^m: Eigenforms in $S(\overline{\mathbb{Z}/p^m\mathbb{Z}})$:

- Weak eigenforms of level M: $S = S_k(\Gamma_1(M))$ some k
- dc-weak eigenforms of level M: $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$ some b
- Strong eigenforms of level M: Reduction mod p^m of classical eigenform in some $S_k(\Gamma_1(M))$

Why introduce all these notions of an eigenform?

When $m = 1$ the three notions of eigenform mod p^m coincide:

Lemma (I. Chen, IK, G. Wiese)

Let $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$. Let $f \in S(\overline{\mathbb{F}}_p)$ be a dc-weak eigenform of level M; say, it is an eigenform for all T_n for n coprime to some $D \in \mathbb{N}$.
Then there is a normalized holomorphic eigenform g of level M and some weight k such that $a_n(g) \equiv a_n(f) \pmod{p}$ for all n coprime with D (i.e., f is in fact a strong eigenform mod p of level (dividing) M.)

This is a version of the Deligne–Serre lifting lemma.

Theorem (I. Chen, IK, G. Wiese, adaptation of arguments by H. Carayol)

Let f be a normalized dc-weak eigenform of level M over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$. Assume that the residual representation $\rho_{f,p,1}$ is absolutely irreducible. Then there is a continuous Galois representation

$$\rho_{f,p,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Z}/p^m\mathbb{Z}})$$

unramified outside Mp such that for primes $\ell \nmid Mp$ we have

$$\mathrm{tr}(\rho_{f,p,m}(\mathrm{Frob}_\ell)) = a_\ell(f)$$

Theorem (I. Chen, IK, G. Wiese, adaptation of results by H. Hida)

Let f be a dc-weak eigenform of level Np^r over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$. Assume that the residual representation $\rho_{f,p,1}$ is absolutely irreducible. Also assume $p \geq 5$.
Then the representation $\rho_{f,p,m}$ dc-weakly arises from $\Gamma_1(N)$, i.e., is attached to a dc-weak eigenform mod p^m of level N.

Our reinterpretation of a theorem of Hatada:

Theorem (Hatada)

Let f be an eigenform of level Np^r and weight k over $\overline{\mathbb{Z}}_p$ such that $\langle \ell \rangle f = \chi(\ell) f$, where χ has no non-trivial component of p-power conductor and order.

Then the representation $\rho_{f,p,m}$ weakly arises from $\Gamma_1(N)$, i.e., is attached to a weak eigenform mod p^m of level N.

However, we can show that when the nebentypus has a non-trivial component of p-power conductor and order, the representations $\rho_{f,p,m}$ can not in general be attached to a weak eigenform mod p^m of level N if $m \geq 2$.

I.e.: weak $\neq$ dc-weak in general (at a fixed level N prime to p).

Weight bounds:

Is there a function $b = b(N, p, m)$ such that any mod p^m representation attached to a dc-weak eigenform mod p^m of level N is necessarily attached to a dc-weak eigenform in $S(\overline{\mathbb{Z}/p^m\mathbb{Z}})$ where:

$$S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(N)) \quad ?$$

In other words: Is the number of such eigensystems finite once we fix N, p, and m?

Of course, when $m = 1$ the answer is 'Yes' (with a non-trivial proof).
When $m \geq 2$ the question seems to be much harder.

Let us ask a simpler question: Is the number of mod p^m representations attached to classical eigenforms of level N (and some weight) finite? If so, can one give explicit weight bounds? Again: As is well-known, when $m = 1$ the answer to both questions is 'Yes'.

Should one conjecture an affirmative answer to the finiteness question in the general case $m \geq 2$?

Personally, I'm undecided at this point as I see indications in both directions.

Buzzard's question: Look at eigenforms at a fixed level N, but all weights. Is it true that the degree over $\mathbb{Q}_p$ of the fields of coefficients is bounded across all weights?

If the answer is affirmative then, for any $m \in \mathbb{N}$, there are only finitely many mod p^m representations arising from a classical eigenform of level N.

Reason: The size of the image of any such representation is bounded and there are restrictions on the ramification.

Using a result by D. Wan (1998), one can show the following:

Let α be a non-negative rational number. Restrict attention to classical eigenforms of level N and p-slope α, allowing a priori all weights.

Then any mod p^m representation arising from one of these eigenforms will arise from one of weight $\leq A\alpha^2 + B\alpha + C$ with (in principle explicit) constants A, B, and C depending only on N, p, and m.

In particular, the number of such representations is finite.

For $\alpha = 0$ (i.e., the ordinary case) one can also deduce the above from a lemma by Hida (and get an explicit constant C).

Study θ operator in the mod p^m setting, for now just on spaces $S_k(\Gamma_1(N))(\mathbb{Z}/p^m)$ (recall: $p \nmid N$).

Classical θ operator acts on q-expansions via

$$\theta\left(\sum a_n q^n\right) := \sum n a_n q^n.$$

Get derivation ∂ on $M(\mathbb{Z}_p) := \oplus_k M_k(\mathbb{Z}_p)$ where $M_k := M_k(\Gamma_1(N))$:

$$\frac{1}{12}\partial f := \theta f - \frac{k}{12} E_2 \cdot f = \theta f + 2kG_2 \cdot f$$

∂ maps M_k to M_{k+2}. For $k \in \mathbb{N}$, k even and ≥ 2:

$$G_k := -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

Why study the θ operator mod p^m?

Applying θ to a strong eigenform corresponds to twisting the attached Galois representation by cyclotomic character

Important to understand more about the properties of this operation, cf. for instance the refined Serre conjectures in the mod p setting

Secondly: In the mod p theory, the θ operator plays a crucial role in Jochnowitz' proof of finiteness of the set of mod p eigensystems coming from $\Gamma_1(N)$. In fact, in the mod p theory, the study of the θ operator is one way of obtaining 'weight bounds'.

There is some interest in studying how far Jochnowitz' arguments can be pushed for eigensystems modulo powers of p.

Recall $M_k := M_k(\Gamma_1(N))$. Recall from Serre/Katz/Jochnowitz arguments the notion of filtration $w_p(f)$ of a non-zero element $f \in M_k(\mathbb{Z}/p)$:

$w_p(f) := \kappa$ if κ is smallest possible such that $f \in M_\kappa(\mathbb{Z}/p)$.

Theorem (Katz)

Suppose that $w_p(f) = k$ and that $p \nmid k$. Then ($\theta f \neq 0$ and)

$$w_p(\theta f) = k + p + 1 = k + 2 + p^{1-1}(p-1)$$

Among other things, this is the starting point for the theory of (mod p) 'θ cycles'

Results on θ mod p^m ($m \geq 2$):

Theorem (I. Chen, IK)

The classical theta operator θ induces an operator

$$\theta : M_k(\mathbb{Z}/p^m) \to M_{k+k(m)}(\mathbb{Z}/p^m),$$

where $k(m) = 2 + 2p^{m-1}(p-1)$.
Its effect on q-expansions is $\theta\left(\sum a_n q^n\right) = \sum n a_n q^n$ and satisfies

$$T_\ell \circ \theta = \ell \cdot \theta \circ T_\ell$$

for primes $\ell \nmid Np$.

Define $w_{p^m}(f)$ for $0 \neq f \in M_k(\Gamma_1(N))(\mathbb{Z}/p^m)$ in the obvious way.

Theorem (I. Chen, IK, + contributions by N. Rustom)

Suppose that $m \geq 2$.
If $f \in M_k(\Gamma_1(N))(\mathbb{Z}/p^m)$ with $f \not\equiv 0 \ (p)$ and $w_p(f) = k \not\equiv 0 \ (p)$ then

$$w_{p^m}(\theta f) = k + 2 + 2p^{m-1}(p-1).$$

Compare with Thm of Katz for the mod p situation.

In the paper by I. Chen and me, we study $w_{p^2}(\theta f)$ in much greater detail, but only at level 1. Conclusion so far: Things become much more complicated in the mod p^m setting when $m \geq 2$ as compared with the mod p situation.

About the proofs of the θ results:

When $k > 2$ the function G_k is in fact a true modular form of weight k, but not when $k = 2$.

However, one knows the following: For any $k \geq 2$, if we choose a sequence of even integers k_i such that $k_i \to \infty$ in the usual, real metric, but $k_i \to k$ in the p-adic metric, then the sequence G_{k_i} has a p-adic limit denoted by G_k^*. It does not depend on the choice of the sequence k_i.

G_k^* is a p-adic modular form in the sense of Serre. This fact is the basis of developing a theory of θ modulo powers of p ($p \geq 5$):

$$\theta f = \frac{1}{12}\partial f - 2kG_2 \cdot f$$

Recall that G_k^* is p-adic limit of G_{k_i} where $k_i \to \infty$ in real and $\to k$ in p-adic metric. One has (Serre):

$$G_k = G_k^* + p^{k-1}\left(G_k^* \mid V\right) + \ldots + p^{t(k-1)}\left(G_k^* \mid V^t\right) + \ldots$$

with V the usual V-operator: $(f \mid V)(q) = f(q^p)$.

Lemma

Suppose k even and ≥ 2 with $p-1 \nmid k$. Then for $t \in \mathbb{N}$:

$$G_k^* \equiv G_{k+p^{t-1}(p-1)} \quad (p^t)$$

Corollary

We have

$$G_2 \equiv \sum_{j=0}^{m-1} p^j \cdot \left(G_{2+p^{m-j-1}(p-1)} \mid V^j \right) \pmod{p^m}$$

If f is on $\mathrm{SL}_2(\mathbb{Z})$ then $f \mid V$ is on $\Gamma_0(p)$. But then (Serre) $f \mid V$ is p-adically on $\mathrm{SL}_2(\mathbb{Z})$.

One can use Serre's theory of p-adic modular forms to work out explicitly a weight such that $f \mid V$ is congruent mod p^t to something on $\mathrm{SL}_2(\mathbb{Z})$ at that weight.

Proposition

Let $m \in \mathbb{N}$. Define the positive even integers $k_0, \ldots, k_{m-1}$ as follows: If $m \geq 2$, define:

$$k_j := 2 + p^{m-j-1}(p^{j+1} - 1) \quad \textit{for } j = 0, \ldots, m-2$$

and

$$k_{m-1} := p^{m-1}(p+1)$$

and define just $k_0 := p + 1$ if $m = 1$.
Then $k_0 < \ldots < k_{m-1}$ and there are modular forms $f_0, \ldots, f_{m-1}$, depending only on p and m, of weights $k_0, \ldots, k_{m-1}$, respectively, that have rational q-expansions, satisfy $v_p(f_j) = 0$ for all j, and are such that

$$G_2 \equiv \sum_{j=0}^{m-1} p^j f_j \pmod{p^m}$$

Explicitly for $m = 2$ (but more complicated when $m > 2$):

$$G_2 \equiv f_0 + p \cdot f_1 \pmod{p^2}$$

with modular forms f_0 and f_1 of weights $2 + p(p-1)$ and $p(p+1)$, respectively, explicitly:

$$G_2 \equiv G_{2+p(p-1)} + p \cdot G_{p+1}^{p} \pmod{p^2}.$$

Corollary

For $p \neq 2, 3$, we have the following congruence of Bernoulli numbers,

$$\frac{B_2}{2} \equiv \frac{B_{p(p-1)+2}}{p(p-1)+2} + p\frac{B_{p+1}}{p+1} \pmod{p^2}.$$

We get the θ operator as a linear map:

$$\theta : M_k(\mathbb{Z}/p^m) \longrightarrow M_{k+2}(\mathbb{Z}/p^m) \oplus \bigoplus_{j=0}^{m-1} p^j M_{k+k_j}(\mathbb{Z}/p^m)$$

$k_j := 2 + p^{m-j-1}(p^{j+1} - 1)$ for $j \leq m-2$, and
$k_{m-1} := p^{m-1}(p+1)$. If we put:

$$k(m) := 2 + 2p^{m-1}(p-1)$$

then $k(m) - k_j$ is a multiple of $p^{m-j-1}(p-1)$ so that we have a natural inclusion

$$p^j M_{k+k_j}(\mathbb{Z}/p^m) \hookrightarrow p^j M_{k+k(m)}(\mathbb{Z}/p^m)$$

via multiplication with a power $E_{p-1}^{p^{m-j-1}}$.

Recall:

Theorem

Suppose that $m \geq 2$.
If $f \in M_k(\Gamma_1(N))(\mathbb{Z}/p^m)$ with $f \not\equiv 0 \pmod{p}$ and $w_p(f) = k \not\equiv 0 \pmod{p}$ then

$$w_{p^m}(\theta f) = k + 2 + 2p^{m-1}(p-1).$$

Main inputs in proof:
E_{p-1} mod p (Hasse invariant) has only simple zeros
E_{p-1} and E_{p+1} mod p have no common zeros (Katz)

Lemma

If $f \in M_k(\Gamma_1(N), \mathbb{Z}/p)$, $f \neq 0$, then $w_p(E_{p+1}f) = p + 1 + w_p(f)$.

My student N. Rustom computed a number of 'θ cycles mod p^2' for cusp forms (with integral coefficients) on $\mathrm{SL}_2(\mathbb{Z})$ and for various primes p.

By 'θ cycle mod p^2' we mean the sequence of weights:

$$w_{p^2}(\theta^2 f), \ldots, w_{p^2}(\theta^{p(p-1)+1} f)$$

Recall that in the mod p setting, for p is sufficiently large there is a universal classification (i.e., not depending on p) of the possible shapes of a θ cycle mod p:

$$w_p(\theta f), \ldots, w_p(\theta^{p-1} f)$$

In particular, the number of 'drops' in filtration, i.e., the number of instances where

$$w_p(\theta^{i+1} f) < w_p(\theta^i f)$$

is either 0 or 1.

From the data, it seems very unlikely that there is such a classification of θ cycles mod p^2, i.e., one that is independent of p for p sufficiently large.

Data for θ cycle mod p^2 and $f = \Delta$:

p	Total drops	Length of cycle $= p(p-1)$
5	7	20
7	8	42
11	18	110
13	22	156
17	25	272
19	28	342
23	30	506
29	44	812
31	47	930
37	54	1332
41	61	1640
43	66	1806

A (very) little about the computations: To compute in high weights, we first determine generators for the whole algebra of modular forms at the given level (and coefficients in $\mathbb{Z}[1/N]$).

Then, to compute some $w_{p^m}(\theta^i f)$, one first represents $\theta^i f \bmod p^m$ in terms of the algebra generators at the (high) weight in question. After that, it is a question of polynomial algebra to determine $w_{p^m}(\theta^i f)$.

Theorem

(N. Rustom) Let $N \geq 5$. Then $M(\Gamma_1(N), \mathbb{Z}[1/N]) = \oplus_k M_k(\Gamma_1(N), \mathbb{Z}[1/N])$ is generated in weight at most 3.

In fact, $\oplus_{k\geq 2} M_k(\Gamma_1(N), \mathbb{Z}[1/N])$ will be generated by forms in weight 2 and 3. Similar results for $\Gamma_0(N)$ under certain conditions (no ellitic elements); in this case, one potentially needs to go to weight 6 to get generators.

Let N, k_1, k_2 be natural numbers, and let f and g be cusp forms of level N and weights k_1 and k_2, respectively, and coefficients in some number field K with ring of integers O.
Suppose that f and g are eigenforms outside Np, i.e., eigenforms for T_ℓ for all primes $\ell \nmid Np$.
How can we determine by a finite amount of computation whether we have

$$a_\ell(f) \equiv a_\ell(g) \pmod{\mathfrak{p}^m}$$

for all primes $\ell \nmid Np$?
The interest being that this condition is equivalent to the attached mod $\mathfrak{p}^m$ representations being isomorphic, – at least if (say) $\bar{\rho}_{f,p}$ is absolutely irreducible.

If the weights of the given forms are equal we have the following easy generalization of a well-known theorem of Sturm:

Proposition

Suppose that N is arbitrary, but that f and g are forms on $\Gamma_1(N)$ of the same weight $k = k_1 = k_2$ and coefficients in O.

Then $\mathrm{ord}_{\mathfrak{p}^m}(f - g) > k\mu/12$ implies $f \equiv g \ (\mathfrak{p}^m)$.

Here,

$$\mathrm{ord}_{\mathfrak{p}^m} h = \inf \left\{ n \mid \ \mathfrak{p}^m \nmid c_n \right\},$$

if $h = \sum c_n q^n$.

In fact, given Sturm's theorem, the proof is by a simple induction on m.

Theorem (I. Chen, IK, J. B. Rasmussen)

Suppose that $p \nmid N$ and that f and g are forms on $\Gamma_1(N)$ of weights k_1 and k_2 and with nebentypus characters ψ_1 and ψ_2, respectively. Suppose that f and g are eigenforms outside Np and have coefficients in O, and that the mod $\mathfrak{p}$ Galois representation attached to f is absolutely irreducible.
Suppose finally that the character $(\psi_1\psi_2^{-1} \bmod \mathfrak{p}^m)$ is unramified at p when viewed as a character on $G_{\mathbb{Q}}$.

Then we have $a_\ell(f) \equiv a_\ell(g) \pmod{\mathfrak{p}^m}$ for all primes with $\ell \nmid Np$ if and only if

$$k_1 \equiv k_2 \begin{cases} \pmod{p^{\lceil \frac{m}{e} \rceil - 1}(p-1)} & \textit{if } p \textit{ is odd} \\ \pmod{2^{\lceil \frac{m}{e} \rceil}} & \textit{if } p = 2 \end{cases}$$

and $a_\ell(f) \equiv a_\ell(g) \pmod{\mathfrak{p}^m}$ for all primes $\ell \leq k\mu'/12$ with $\ell \nmid Np$.