Ian Kiming, Univ. of Copenhagen

Modular mod p^m representations.

2 papers:

1. Joint with Imin Chen on level-lowering for modular mod p^m Galois representations,

2. Joint with Imin Chen and Jonas B. Rasmussen (Copenhagen) on detecting congruences mod p^m between eigenforms (of possibly different weights).

p prime,
K finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$ with integers O,
$\mathfrak{p}$ a prime over p,
$e := e(\mathfrak{p}/p)$.
Consider a representation: $\rho : \ G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(O/\mathfrak{p}^m)$.
Attached residual repr. is $\bar{\rho} : \ G_{\mathbb{Q}} \to \mathrm{GL}_n(O/\mathfrak{p})$ obtained via reduction mod $\mathfrak{p}$.
Easy to see: The quantity $a := \lceil \frac{m}{e} \rceil$ is independent on choice of K etc.
We could call ρ a 'mod p^a' Galois representation. Alternatively, if K etc. are fixed, call ρ a 'mod $\mathfrak{p}^m$ Galois representation.

Given an eigenform f of weight k on some $\Gamma_1(N)$ and coefficients in K we can attach to it a p-adic representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(O)$. Reducing this mod $\mathfrak{p}^m$ we obtain a mod p^a representation $(a = \lceil \frac{m}{e} \rceil)$:

$$\rho_{f,p,a} : \; G_{\mathbb{Q}} \to \mathrm{GL}_2(O/\mathfrak{p}^m)$$

with attached residual representation $\bar{\rho}_{f,p} : \; G_{\mathbb{Q}} \to \mathrm{GL}_2(O/\mathfrak{p})$.

By construction we have:

$$(*) \qquad \operatorname{tr} \rho_{f,p,a}(\mathrm{Frob}_\ell) \equiv a_\ell(f) \pmod{\mathfrak{p}^m}$$

for almost all primes ℓ.
If $\bar{\rho}_{f,p}$ is absolutely irreducible, Chebotarev + the following theorem of Carayol show that the property $(*)$ completely fixes the isomorphism class of $\rho_{f,p,a}$.
In particular, this isomorphism class does not depend on the choice of lattice when making the p-adic representation integral.

Theorem

(Carayol, 'Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet' (1994)).
Let A be a local ring with maximal ideal $\mathfrak{m}$, let R an A-algebra, and suppose ρ and ρ' are two representations of R of the same dimension n over A.

Assume that the residual representation

$$\overline{\rho} : R \longrightarrow \mathrm{GL}_n(A/\mathfrak{m})$$

obtained by reduction modulo $\mathfrak{m}$ is absolutely irreducible.

If for all $r \in R$, $\operatorname{tr}\rho(r) = \operatorname{tr}\rho'(r)$, then ρ and ρ' are isomorphic as representations of R over A.

Applying the theorem to $R = A[G]$ for a group G we obtain:

Corollary

Let $\rho, \rho' : G \to \mathrm{GL}_2(A)$ be representations of a group G over a local ring A such that the residual representation $\overline{\rho}$ is absolutely irreducible.

Suppose $\operatorname{tr}\rho(g) = \operatorname{tr}\rho'(g)$ for all $g \in G$. Then ρ and ρ' are isomorphic as representations of G over A.

Given a mod p^a Galois representation

$$\rho: \; G_{\mathbb{Q}} \to \mathrm{GL}_2(O/\mathfrak{p}^m)$$

we say that ρ is *strongly* resp. *weakly modular* of level $N \in \mathbb{N}$ if there is a modular form f of some weight on $\Gamma_1(N)$ that is an eigenform for all Hecke operators T_ℓ, for primes $\ell \nmid Np$, with corresponding eigenvalues $a_\ell(f)$, respectively is just an eigenform mod $\mathfrak{p}^m$ with eigenvalues $(a_\ell(f) \mod \mathfrak{p}^m)$, such that

$$\operatorname{tr} \rho(\mathrm{Frob}_\ell) = (a_\ell(f) \mod \mathfrak{p}^m)$$

for all primes $\ell \nmid Np$.

Theorem

(I. Chen + IK). Suppose that $p \geq 5$, that $N \in \mathbb{N}$ with $p \nmid N$, and that

$$\rho : \ G_{\mathbb{Q}} \to \mathrm{GL}_2(O/\mathfrak{p}^m)$$

is a given representation.

If ρ is (weakly or strongly) modular of level $N \cdot p^u$ for some u then ρ is weakly modular of level N.

Question: Does 'weakly modular of level N' imply 'strongly modular of level N'?

We don't know, but believe so. Results of Hida seem to show this if the form in question is ordinary, but the general case appears problematic.

The trouble is that the Deligne-Serre lifting lemma does not generalize in any naive or formal way to the mod $\mathfrak{p}^m$ setting, so a much more complicated argument is probably needed.

It seems very probable that in going from 'weakly modular' to 'strongly modular' one may very well need to change the weight, and at this point we don't have any good ideas about how to deal with that.

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.

Setup: Will assume $3 \mid N$ if $p = 2$, $2 \mid N$ if $p = 3$. Put:

$$N' := \begin{cases} N \cdot \prod_{q|N} q \ , & \text{if } p \mid N \\ N \cdot p^2 \cdot \prod_{q|N} q \ , & \text{if } p \nmid N \end{cases}$$

where the products are over prime divisors q of N, and put:

$$\mu := [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] \ , \quad \mu' := [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N')] \ ,$$

and fix the following notation:

k	$:=$	$\max\{k_1, k_2\}$,
$\mathfrak{p}$	:	a fixed prime of K over p,
e	$:=$	$e(\mathfrak{p}/p)$, the ramification index of $\mathfrak{p}$ over p,
L	:	Galois closure of $K/\mathbb{Q}$,
$e(L,p)$	:	the ramification index of L relative to p in $\mathbb{Q}$,
r	:	largest integer such that p^r divides the ramification index $e(L,p)$.

For a non-negative integer a and a modular form $h = \sum c_n q^n$ on some $\Gamma_1(M)$ and coefficients c_n in O we define:

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

with the convention that $\operatorname{ord}_{\mathfrak{p}^a} h = \infty$ if $\mathfrak{p}^a \mid c_n$ for all n.

So, $f \equiv g \ (\mathfrak{p}^m)$ means (by definition) that $\operatorname{ord}_{\mathfrak{p}^m}(f - g) = \infty$.

Our starting point is the following observation:

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* $f \equiv g \pmod{\mathfrak{p}^m}$.

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

The real trouble begins when the weights k_1 and k_2 are not equal.

We do not have a complete solution, but 2 theorems that apply in different cases.

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

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

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

When we allow p to divide the level N (as we would want to allow), we do not have clean, necessary and sufficient, computationally verifiable conditions for

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

to hold for all primes $\ell \nmid Np$, but at least we have a sufficient condition.

To motivate the sufficient condition, consider first the following theorem.

Theorem

(I. Chen, IK, J. B. Rasmussen). Let the weights k_1 and k_2 of f and g be arbitrary, but assume that $p \nmid N$ and that f and g are normalized forms on $\Gamma_1(N) \cap \Gamma_0(p)$ with coefficients in O.

Then if $f \equiv g \ (\mathfrak{p}^m)$ we have $k_1 \equiv k_2 \ (p^s(p-1))$.

Here, the non-negative integer s is defined as follows:

$$s := \begin{cases} \max\{0, \lceil \frac{m}{e} \rceil - 1 - r\} \ , & \text{if } p \geq 3 \\ \max\{0, \alpha(\lceil \frac{m}{e} \rceil - r)\} \ , & \text{if } p = 2 \end{cases}$$

with $\alpha(u)$ defined for $u \in \mathbb{Z}$ as follows:

$$\alpha(u) := \begin{cases} u - 1 \ , & \text{if } u \leq 2 \\ u - 2 \ , & \text{if } u \geq 3 \ . \end{cases}$$

Recall that r is defined so that p^r is the highest power of p dividing $e(L, p)$, the ramification index of the Galois closure L of K, relative to p.

Theorem

(I. Chen, IK, J. B. Rasmussen). Let N be arbitrary and f and g normalized forms of weights k_1 and k_2, respectively, on $\Gamma_1(N)$ that are eigenforms outside Np and have coefficients in O.

Assume that $k_1 \equiv k_2 \pmod{p^s(p-1)}$ and that $a_\ell(f) \equiv a_\ell(g) \pmod{\mathfrak{p}^m}$ for all primes $\ell \leq k\mu'/12$ with $\ell \nmid Np$.

If $p > 2$ and $r = 0$ we then have

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

for all primes $\ell \nmid Np$, and this conclusion also holds if $p = 2$, $r = 0$, but $m \leq 2e$.

If $r > 0$ and $m \geq e$ we have at least the weaker congruence $a_\ell(f) \equiv a_\ell(g) \pmod{\mathfrak{p}^{e\cdot(s+1)}}$ for all primes $\ell \nmid Np$.

An example: We start with $f = q - 8q^4 + 20q^7 + \cdots$, the (normalized) cusp form on $\Gamma_0(9)$ of weight 4 with integral coefficients, and look for congruences of the coefficients of f and g modulo powers of a prime above 5, for a form g of weight k_2 satisfying $k_2 \equiv 4 \ (5 \cdot (5-1))$.
The smallest possible choice of weight for g is $k_2 = 24$. There is a newform g on $\Gamma_0(9)$ of weight 24 with coefficients in the number field $K = \mathbb{Q}(\alpha)$ with α a root of $x^4 - 29258x^2 + 97377280$. The prime 5 is ramified in K and has the decomposition $5 \cdot O = \mathfrak{p}^2\mathfrak{p}_2$.
We have $k = 24$, $N = 9$, $N' = 675$ and $\mu' = 1080$, and we find that $a_\ell \equiv b_\ell \ (\mathfrak{p}^3)$ for primes $\ell \leq k\mu'/12 = 2160$ with $\ell \neq 3, 5$.
Since $[K : \mathbb{Q}] = 4$, the Galois closure L of K satisfies $[L : \mathbb{Q}] \mid 24$ (in fact $[L : \mathbb{Q}] = 8$ in this case). This shows that $5 \nmid e(L, 5)$, i.e., $r = 0$. Since we also have $m = 3$ and $e = e(\mathfrak{p}/5) = 2$, we get $s = 1$ as desired. By one of the theorems above we conclude that $a_\ell(f) \equiv a_\ell(g) \ (\mathfrak{p}^3)$ for all primes $\ell \neq 3, 5$.

Numerical experiments:
Suppose that f is a normalized eigenform of weight k_1 on $\Gamma_1(N \cdot p^u)$ where $p \nmid N$, coefficients in K with ring of integers O, $\mathfrak{p}$ a prime over p as before.
We believe that f is strongly modular mod $\mathfrak{p}^m$ of level N, i.e., that there is an eigenform g on $\Gamma_1(N)$ of some other weight k_2 such that the mod $\mathfrak{p}^m$ representation attached to g is isomorphic to the one coming from f. So far we can only prove this in the weaker sense discussed earlier.
But the theorems I discussed allows us under appropriate conditions ('$r = 0$', p odd, for instance) to check this conjecture in a strong sense, i.e., by *proving* the existence of such a g given a concrete form f. So far, we have found a form g for all examples that we have looked at (and they are plenty).

We are interested in the following question: Assuming the above conjecture, i.e., the existence of g on $\Gamma_1(N)$ what is the minimal weight k_2 of such a g?

Certainly, k_2 depends on obvious things such as the weight k_1 of the original form f as well as m (in mod $\mathfrak{p}^m$). But what other properties of, say, the mod $\mathfrak{p}^m$ representation attached to f do also have to do with the minimal k_2?

We are launching a larger experimental study of this by taking elliptic curves of conductors Np^u, ‘stripping p^u mod $\mathfrak{p}^m$ from the level’ of the corresponding eigenforms for as many m as we can, and then tabulating the minimal weights where this level reduction mod $\mathfrak{p}^m$ occurs.

So far, the results look complicated ...

E	Cond	N	p	m	k_2	red.type
$[1,0,0,-4,-1]$	21	7	3	2	$8 = 2 + p \cdot (p-1)$	spl.mult.
–	–	–	–	3	$20 = 2 + p^2 \cdot (p-1)$	–
$[0,0,0,6,-7]$	72	8	3	2	$20 = 2 + p^2 \cdot (p-1)$	add
–	–	–	–	3	$20 = 2 + p^2 \cdot (p-1)$	–
$[0,0,0,-3,-34]$	216	8	3	2	$8 = 2 + p \cdot (p-1)$	add
$[1,1,1,-10,-10]$	15	3	5	2	$22 = 2 + p \cdot (p-1)$	spl.mult.
$[1,0,1,4,-6]$	14	2	7	2	$44 = 2 + p \cdot (p-1)$	spl.mult.
$\vdots$						