

ON CONGRUENCES MOD \mathfrak{p}^m BETWEEN EIGENFORMS AND THEIR ATTACHED GALOIS REPRESENTATIONS.

IMIN CHEN, IAN KIMING AND JONAS B. RASMUSSEN

ABSTRACT. Given a prime p and cusp forms f_1 and f_2 on some $\Gamma_1(N)$ that are eigenforms outside Np and have coefficients in the ring of integers of some number field K , we consider the problem of deciding whether f_1 and f_2 have the same eigenvalues mod \mathfrak{p}^m (where \mathfrak{p} is a fixed prime of K over p) for Hecke operators T_ℓ at all primes $\ell \nmid Np$.

When the weights of the forms are equal the problem is easily solved via an easy generalization of a theorem of Sturm. Thus, the main challenge in the analysis is the case where the forms have different weights. Here, we prove a number of necessary and sufficient conditions for the existence congruences mod \mathfrak{p}^m in the above sense.

The prime motivation for this study is the connection to modular mod \mathfrak{p}^m Galois representations, and we also explain this connection.

1. INTRODUCTION

Let $N \in \mathbb{N}$ and let p be a fixed prime number.

Suppose that we are given cusp forms $f_1 = \sum a_n(f_1)q^n$ and $f_2 = \sum a_n(f_2)q^n$ (where $q := e^{2\pi iz}$) on $\Gamma_1(N)$ of weights k_1 and k_2 , respectively, and with coefficients in \mathcal{O}_K where K is some number field. We will assume in all that follows that f_1 and f_2 are normalized, i.e., that $a_1(f_1) = a_1(f_2) = 1$.

We say that f_1 and f_2 are *eigenforms outside Np* if they are (normalized) eigenforms for all Hecke operators T_ℓ for primes ℓ with $\ell \nmid Np$. The corresponding eigenvalues for such T_ℓ acting on f_i are then exactly the coefficients $a_\ell(f_i)$.

Now fix a prime \mathfrak{p} of K over p . If f_i is an eigenform outside Np , and if $m \in \mathbb{N}$, there is attached to f_i a ‘mod \mathfrak{p}^m ’ Galois representation:

$$\rho_{f_i, \mathfrak{p}^m} : G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathcal{O}_K/\mathfrak{p}^m)$$

obtained by making the p -adic representation attached to f_i integral with coefficients in \mathcal{O}_K and then reducing modulo \mathfrak{p}^m . The representation $\rho_{f_i, \mathfrak{p}^m}$ is unramified outside Np and we have:

$$(*) \quad \text{tr } \rho_{f_i, \mathfrak{p}^m}(\text{Frob}_\ell) = (a_\ell(f_i) \bmod \mathfrak{p}^m)$$

for primes $\ell \nmid Np$.

By a theorem of Carayol, cf. Théorème 1 of [2], combined with the Chebotarev density theorem, one has that the representation $\rho_{f_i, \mathfrak{p}^m}$ is determined up to isomorphism by the property (*) for primes $\ell \nmid Np$ if we additionally suppose that the mod \mathfrak{p} representation $\rho_{f_i, \mathfrak{p}}$ is absolutely irreducible.

Imin Chen and Ian Kiming are launching a study of the arithmetic properties of ‘modular mod \mathfrak{p}^m Galois representations’ as above, cf. [3]. In this connection we found it natural to prepare the ground for numerical experimentation with

these representations. As is obvious from the above, the key to this is to obtain a computationally decidable criterion for when we have $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$ for all primes $\ell \nmid Np$, if f_1 and f_2 as above are given cusp forms that are eigenforms outside Np .

Now, for the case $m = 1$, and if the weights k_1 and k_2 are equal, there is a well-known theorem of Sturm that gives a necessary and sufficient condition for the forms to be congruent mod \mathfrak{p} in the sense that all their Fourier coefficients are congruent mod \mathfrak{p} . It turns out to be very easy to generalize Sturm's theorem to the cases $m > 1$ provided that we still have $k_1 = k_2$. Then, still under the assumption that the weights are equal, a simple twisting argument allows us to discuss the case of eigenforms outside Np .

For various reasons we are interested in also considering cases where the weights are distinct and this turns out to present a genuinely new challenge.

We study two distinct approaches to this challenge. Under favorable circumstances these approaches both result in computable necessary and sufficient conditions for the forms to be 'congruent mod \mathfrak{p}^m outside Np ' in the above sense.

The first approach is to generalize a theorem of Serre-Katz on p -adic modular forms, cf. Cor. 4.4.2 of [5] which – under certain restrictions on the levels of the forms – gives a necessary congruence between the weights for the forms to be congruent mod \mathfrak{p}^m . In the Serre-Katz theorem one needs to assume that the prime \mathfrak{p} of the field K of coefficients is unramified relative to p in \mathbb{Q} . We are able to generalize this theorem to cases where \mathfrak{p} is ramified over p .

Under certain technical restrictions, in particular that the ramification index relative to p of the Galois closure of the field K of coefficients is not divisible by p , and that p is odd, our Theorem 1 results in the desired computable necessary and sufficient conditions. See Corollary 1 below.

The second approach is via a study of the determinants of the attached mod \mathfrak{p}^m representations. Again under certain technical restrictions, here notably a restriction on the nebentypus characters of the forms, our Theorem 2 leads to the desired computable necessary and sufficient conditions. Cf. Corollary 2 below.

It is remarkable that these two rather distinct approaches result – under the technical restrictions alluded to above – in necessary and sufficient conditions that are close to being equivalent.

We illustrate the results by a few numerical examples.

1.1. Notation. To formulate our results, let us introduce the following notation:

Define

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

where the products are over prime divisors q of N . 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:

m	:	a natural number,
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 power of p dividing the ramification index $e(L, p)$,
ℓ	:	a (not fixed) prime number.

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 \mathcal{O}_K we define:

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

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

We say that f_1 and f_2 are congruent modulo \mathfrak{p}^a if $\text{ord}_{\mathfrak{p}^a}(f_1 - f_2) = \infty$, and we denote this by $f_1 \equiv f_2 \pmod{\mathfrak{p}^a}$.

1.2. Results. The following proposition is the first, basic observation, and is an easy generalization of a well-known theorem of Sturm, cf. [9].

Proposition 1. *Suppose that N is arbitrary, but that f_1 and f_2 are forms on $\Gamma_1(N)$ of the same weight $k = k_1 = k_2$ and coefficients in \mathcal{O}_K .*

Then $\text{ord}_{\mathfrak{p}^m}(f_1 - f_2) > k\mu/12$ implies $f_1 \equiv f_2 \pmod{\mathfrak{p}^m}$.

Part (i) of the following theorem is a slight generalization of theorems of Serre and Katz, cf. [8], Théorème 1, [5], Corollary 4.4.2.

Theorem 1. *Suppose that f_1 and f_2 are normalized cusp forms on $\Gamma_1(N)$ of weights k_1 and k_2 , respectively, and with coefficients in \mathcal{O}_K .*

(i) *Assume additionally that $p \nmid N$ and that f_1 and f_2 are forms on $\Gamma_1(N) \cap \Gamma_0(p)$.*

Then if $f_1 \equiv f_2 \pmod{\mathfrak{p}^m}$ we have $k_1 \equiv k_2 \pmod{p^s(p-1)}$ with the non-negative integer s 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:

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

(ii) *Let N be arbitrary, but assume $3 \mid N$ if $p = 2$, and $2 \mid N$ if $p = 3$.*

Suppose that $k_1 \equiv k_2 \pmod{p^s(p-1)}$.

Then, if $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$ for all primes $\ell \leq k\mu'/12$ with $\ell \nmid Np$, the following holds:

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

$$a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$$

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:

$$a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^{e \cdot (s+1)}}$$

for all primes $\ell \nmid Np$.

The following corollary is an immediate consequence of Theorem 1.

Corollary 1. *Retain the setup and notation of Theorem 1, and assume that p is odd, $r = 0$, that N is prime to p , that $3 \mid N$ if $p = 2$, and $2 \mid N$ if $p = 3$, and that f_1 and f_2 are forms on $\Gamma_1(N) \cap \Gamma_0(p)$.*

Then we have $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$ for all primes $\ell \nmid Np$ if and only if this congruence holds for all primes $\ell \leq k\mu'/12$ with $\ell \nmid Np$ and we have the congruence

$$k_1 \equiv k_2 \pmod{p^s(p-1)}$$

between the weights.

Theorem 2. *Suppose that N is arbitrary, but assume that p is odd and that f_1 and f_2 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_1 and f_2 are eigenforms outside Np and have coefficients in \mathcal{O}_K , and that the mod \mathfrak{p} Galois representation attached to f_1 is absolutely irreducible.

View the nebentypus characters ψ_i as finite order characters on $G_{\mathbb{Q}}$, and let the order of the character

$$(\psi_2\psi_1^{-1} \bmod \mathfrak{p}^m)_{|I_p}$$

where I_p is an inertia group at p , be $p^\delta \cdot d$ with d a divisor of $p-1$.

(i) If we have $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$ for all primes with $\ell \nmid Np$ then $\delta \leq \lceil \frac{m}{e} \rceil - 1$ and we have:

$$k_1 \equiv k_2 \pmod{p^{\lceil \frac{m}{e} \rceil - 1 - \delta} \cdot (p-1)/d}$$

so that in particular, $k_1 \equiv k_2 \pmod{p^{\lceil \frac{m}{e} \rceil - 1} \cdot (p-1)/d}$ if $\delta = 0$.

(ii) Suppose that

$$k_1 \equiv k_2 \pmod{p^{\lceil \frac{m}{e} \rceil - 1} \cdot (p-1)/d}.$$

Then, if $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$ for all primes $\ell \leq k\mu'/12$ with $\ell \nmid Np$ we have this congruence for all primes $\ell \nmid Np$.

The following corollary follows immediately from Theorem 2.

Corollary 2. *Retain the setup and notation of Theorem 2, and assume that $\delta = 0$.*

Then we have $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$ for all primes $\ell \nmid Np$ if and only if this congruence holds for all primes $\ell \leq k\mu'/12$ with $\ell \nmid Np$ and we have the congruence

$$k_1 \equiv k_2 \pmod{p^{\lceil \frac{m}{e} \rceil} (p-1)/d}$$

between the weights.

Remark: Obtaining results like those in the corollaries, but in more general situations, for instance with r and δ not necessarily 0, are obvious problems for future work. It seems fairly clear to us that such questions lead to rather hard problems that will require some new ideas.

2. PROOFS

Let us first prove Proposition 1 that turns out to be an easy generalization of a theorem by Sturm, cf. [9].

Proof of Proposition 1: We prove this by induction on m . The case $m = 1$ is a theorem of Sturm, cf. Theorem 1 of [9].

Assume that $m > 1$, and that the theorem is true for powers \mathfrak{p}^a of \mathfrak{p} with $a < m$. Let $\varphi = f_1 - f_2$. By assumption we have $\text{ord}_{\mathfrak{p}^m} \varphi > k\mu/12$, and therefore also $\text{ord}_{\mathfrak{p}^{m-1}} \varphi > k\mu/12$, and hence the induction hypothesis gives $\text{ord}_{\mathfrak{p}^{m-1}} \varphi = \infty$. This means there is a cusp form ψ on $\Gamma_1(N)$ of weight k with coefficients in \mathcal{O}_K such that $\varphi \in \mathfrak{p}^{m-1}\psi$.

Now, since $\text{ord}_{\mathfrak{p}^m} \varphi > k\mu/12$, we must have $\text{ord}_{\mathfrak{p}} \psi > k\mu/12$, so that $\text{ord}_{\mathfrak{p}} \psi = \infty$ by the induction hypothesis for $m = 1$ (i.e., the theorem of Sturm). From this we conclude that $\text{ord}_{\mathfrak{p}^m} \varphi = \infty$, as desired. \square

In the following arguments we occasionally need the following simple and probably well-known lemma.

Lemma 1. *Let F'/F be a finite extension of number fields. Let \mathfrak{q} be a prime ideal of F and let \mathfrak{Q} be a prime ideal of F' over \mathfrak{q} of ramification index ϵ . Let b be a positive integer.*

Then

$$\mathfrak{Q}^b \cap F = \mathfrak{q}^{\lceil \frac{b}{\epsilon} \rceil}.$$

Proof. There is a non-negative integer a such that $a\epsilon < b \leq (a+1)\epsilon$, and then we have

$$\mathfrak{Q}^{(a+1)\epsilon} \subseteq \mathfrak{Q}^b \subseteq \mathfrak{Q}^{a\epsilon}.$$

From this we get that

$$\mathfrak{q}^{a+1} = \mathfrak{Q}^{(a+1)\epsilon} \cap F \subseteq \mathfrak{Q}^b \cap F \subseteq \mathfrak{Q}^{a\epsilon} \cap F = \mathfrak{q}^a,$$

and so $\mathfrak{Q}^b \cap F$ is either \mathfrak{q}^a or \mathfrak{q}^{a+1} .

Assume that $\mathfrak{Q}^b \cap F = \mathfrak{q}^a$. Then $\mathfrak{q}^a \subseteq \mathfrak{Q}^b$, i.e., $\mathfrak{Q}^{a\epsilon} \subseteq \mathfrak{Q}^b$, and so $a\epsilon \geq b$, a contradiction. We conclude that $\mathfrak{Q}^b \cap F = \mathfrak{q}^{a+1}$, and since $a+1 = \lceil \frac{b}{\epsilon} \rceil$ by the definition of a , we are done. \square

Part (i) of Theorem 1 can be seen as a generalization of a theorem of Serre and Katz, cf. Cor. 4.4.2 of [5], and Katz' theorem is also the main point of the proof.

Proof of part (i) of Theorem 1: Recall that L denotes the Galois closure of K . Let us fix a prime \mathfrak{P} over \mathfrak{p} in the Galois closure L of K . Thus, the ramification index $e(L, p)$ is the ramification index of $e(\mathfrak{P}/p)$ of \mathfrak{P} relative to p in \mathbb{Q} . Recall that we denote the ramification index $e(\mathfrak{p}/p)$ by e .

Let L_0 be the subfield of L corresponding to the inertia group $I(\mathfrak{P}/p)$. Let \mathfrak{p}_0 be the prime of L_0 under \mathfrak{P} .

We now let $I(\mathfrak{P}/p)$ act on the f_i by acting on their Fourier coefficients. Since $f_1 \equiv f_2 \pmod{\mathfrak{p}^m}$ we have $\sigma(f_1) \equiv \sigma(f_2) \pmod{\mathfrak{P}^{m \cdot e(\mathfrak{P}/p)}}$ for all $\sigma \in I(\mathfrak{P}/p)$. Letting

$$F_1 = \sum_{\sigma} \sigma(f_1) \quad \text{and} \quad F_2 = \sum_{\sigma} \sigma(f_2)$$

with the sums taken over all $\sigma \in I(\mathfrak{P}/p)$, we therefore obtain

$$F_1 \equiv F_2 \pmod{\mathfrak{P}^{m \cdot e(\mathfrak{P}/p)}}.$$

Now, since F_1 and F_2 are invariant under the action of $I(\mathfrak{P}/p)$ they actually have coefficients in L_0 , and we therefore have

$$F_1 \equiv F_2 \pmod{\mathfrak{p}_0^{\lceil \frac{m}{e} \rceil}}$$

since $\mathfrak{P}^b \cap L_0 = \mathfrak{p}_0^{\lceil \frac{b}{e(L,p)} \rceil}$ for non-negative integers b , cf. Lemma 1, and because

$$e(L, p) = e(\mathfrak{p}/p)e(\mathfrak{P}/\mathfrak{p}) = e \cdot e(\mathfrak{P}/\mathfrak{p}) .$$

Now, the extension $(L_0)_{\mathfrak{p}_0}/\mathbb{Q}_p$ of local fields is unramified, and so $(L_0)_{\mathfrak{p}_0}$ is the field of fractions of the ring $W = W(\mathbb{F}_{p^f})$ of Witt vectors over \mathbb{F}_{p^f} for some f . Since the F_i have integral coefficients in L_0 , we can view them as having coefficients in W .

Now let a be the largest non-negative integer such that all Fourier coefficients of F_1 and F_2 are divisible by p^a . Then the forms $p^{-a}F_1$ and $p^{-a}F_2$ are cusp forms on $\Gamma_1(N) \cap \Gamma_0(p)$ of weights k_1 and k_2 , respectively, and with coefficients in W . At least one of these forms has a q -expansion that does not reduce to 0 identically modulo p . Their q -expansions are congruent modulo

$$\mathfrak{p}_0^{\max\{0, \lceil \frac{m}{e} \rceil - a\}}$$

and hence also modulo

$$\mathfrak{p}_0^{\max\{0, \lceil \frac{m}{e} \rceil - r\}}$$

since certainly $a \leq r$ because the coefficients of q for both forms F_i equals $\#I(\mathfrak{P}/p)$ which is just $e(L, p)$.

By a theorem of Katz, cf. Cor. 4.4.2 of [5] we then deduce that

$$k_1 \equiv k_2 \pmod{(p^s(p-1))}$$

where s is given as in the theorem. □

To prepare for the proof of part (ii) of Theorem 1 we need the following lemma.

Let us say that a cusp form $h = \sum c_n q^n$ on $\Gamma_1(N)$ and coefficients in \mathcal{O}_K is an *eigenform mod \mathfrak{p}^m outside Np* if it is normalized and we have $T_\ell h \equiv \lambda_\ell h \pmod{\mathfrak{p}^m}$ for all primes $\ell \nmid Np$ with certain $\lambda_\ell \in \mathcal{O}_K$. The same argument as in characteristic 0 shows that in that case, the mod \mathfrak{p}^m eigenvalues λ_ℓ are congruent mod \mathfrak{p}^m to the Fourier coefficients c_ℓ .

Lemma 2. *Let N be arbitrary and let f_1 and f_2 be normalized forms of the same weight k on $\Gamma_1(N)$ and with coefficients in \mathcal{O}_K .*

Suppose that f_1 and f_2 are eigenforms mod \mathfrak{p}^m outside Np such that

$$a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$$

for all primes $\ell \leq k\mu'/12$ with $\ell \nmid Np$.

Then $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$ for all primes $\ell \nmid Np$.

Proof. We first apply Lemma 4.6.5 of Miyake [6]: By that lemma we obtain from the f_i forms f'_i of weight k on $\Gamma_1(N')$ by putting:

$$f'_i := \sum_{\gcd(n, Np)=1} a_n(f_i) \cdot q^n .$$

Here, N' is as defined in the notation section. The forms f'_i obviously still have coefficients in \mathcal{O}_K .

Now, since the f_i are eigenforms mod \mathfrak{p}^m outside Np , the forms f'_i are also eigenforms mod \mathfrak{p}^m outside Np , with the same eigenvalues ($a_\ell(f_i) \bmod \mathfrak{p}^m$).

On the other hand, all Fourier coefficient of the forms f'_i at any index n not prime to Np vanishes. By our hypotheses we can thus conclude that

$$\text{ord}_{\mathfrak{p}^m}(f'_1 - f'_2) > k\mu'/12$$

and by Proposition 1 this implies $f'_1 \equiv f'_2 \pmod{\mathfrak{p}^m}$.

But then $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$ for all primes $\ell \nmid Np$. \square

Proof of part (ii) of Theorem 1. Assume without loss of generality that $k_2 \geq k_1$. We can then write:

$$k_2 = k_1 + t \cdot p^s(p-1)$$

where t is a non-negative integer.

Now, we have an Eisenstein series E of weight $p-1$ on $\Gamma_1(N)$ with coefficients in \mathbb{Z} and such that $E \equiv 1 \pmod{p}$: If $p \geq 5$ we can take $E := E_{p-1}$ the standard Eisenstein series of weight $p-1$ on $\text{SL}_2(\mathbb{Z})$. If $p = 2$ there is, cf. [4] chap. 4.8 for instance, an Eisenstein series of weight 1 on $\Gamma_1(3)$:

$$E := 1 - \frac{2}{B_{1,\psi}} \cdot \sum_{n=1}^{\infty} \left(\sum_{d|n} \psi(d) \right) \cdot q^n ;$$

here, ψ is the primitive Dirichlet character of conductor 3, and $B_{1,\psi}$ is the first Bernoulli number of ψ . One computes $B_{1,\psi} = -\frac{1}{3}$, so that in fact E has coefficients in \mathbb{Z} and reduces to 1 modulo 2. Also, E is a modular form on $\Gamma_1(N)$ as we have assumed $3 \mid N$ if $p = 2$.

If $p = 3$ we choose

$$E := 1 + 24 \cdot \sum_{n=1}^{\infty} \left(\sum_{d|n} d \right) \cdot q^n ;$$

this is a modular form of weight 2 on $\Gamma_1(2)$ and hence also on $\Gamma_1(N)$ as we have $2 \mid N$ if $p = 3$. Again, cf. for instance [4], chap. 4.6.

With the above choice of E we have in all cases that E is a modular form of weight $p-1$ on $\Gamma_1(N)$ with coefficients in \mathbb{Z} that reduces to 1 modulo p . By induction on j we see that $E^{p^j} \equiv 1 \pmod{p^{j+1}}$ for all non-negative integers j , and hence also:

$$E^{t \cdot p^s} \equiv 1 \pmod{p^{s+1}}$$

that we write as $E^{t \cdot p^s} \equiv 1 \pmod{\mathfrak{p}^{e \cdot (s+1)}}$. Consequently, the form

$$\tilde{f} := E^{t \cdot p^s} \cdot f_1$$

satisfies $\tilde{f} \equiv f_1 \pmod{\mathfrak{p}^{e \cdot (s+1)}}$. If we call \tilde{a}_n the Fourier coefficients of \tilde{f} we have then

$$\tilde{a}_n \equiv a_n(f_1) \pmod{\mathfrak{p}^{e \cdot (s+1)}}$$

and thus consequently:

$$\tilde{a}_\ell \equiv a_\ell(f_2) \pmod{\mathfrak{p}^{e \cdot (s+1)}}$$

for all primes $\ell \leq k\mu'/12$ with $\ell \nmid Np$, because of our hypothesis.

Now, \tilde{f} and f_2 are both forms on $\Gamma_1(N)$ of weight $k = k_2$.

Using the definition of s one checks that if $r > 0$ and $m \geq e$ then $e \cdot (s+1) \leq m$ in all cases.

Also, $e \cdot (s+1) \geq m$ if either $p > 2$ and $r = 0$, or if $p = 2$, $r = 0$, but $m \leq 2e$.

As f_1 is an eigenform mod \mathfrak{p}^m outside Np , we can then conclude that \tilde{f} and f_2 are both eigenforms mod $\mathfrak{p}^{e \cdot (s+1)}$ outside Np , if $r > 0$ and $m \geq e$. In this case, Lemma 2 then implies that

$$\tilde{a}_\ell \equiv a_\ell(f_2) \pmod{\mathfrak{p}^{e \cdot (s+1)}}$$

and hence also

$$a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^{e \cdot (s+1)}}$$

for all primes $\ell \nmid Np$.

If either $p > 2$ and $r = 0$, or if $p = 2$, $r = 0$, but $m \leq 2e$, we have that \tilde{f} and f_2 are both eigenforms mod \mathfrak{p}^m outside Np , and then Lemma 2 gives us that

$$\tilde{a}_\ell \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$$

and hence also

$$a_\ell(f_1) \equiv a_\ell(f_2)$$

for all primes $\ell \nmid Np$. □

Proof of Theorem 2: Proof of part (i): Consider the representations $\rho_{f_i, \mathfrak{p}^m}$ attached to the forms f_i .

Since $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^m}$ for all primes $\ell \nmid Np$ we can conclude by Chebotarev's density theorem that the representations $\rho_{f_1, \mathfrak{p}^m}$ and $\rho_{f_2, \mathfrak{p}^m}$ have the same traces. As $\rho_{f_1, \mathfrak{p}}$ is assumed absolutely irreducible, Théorème 1 of Carayol [2] then implies that $\rho_{f_1, \mathfrak{p}^m}$ and $\rho_{f_2, \mathfrak{p}^m}$ are isomorphic. Hence, the determinants of these representations are also isomorphic. These determinants are:

$$\det \rho_{f_i, \mathfrak{p}^m} = (\psi_i \cdot \chi^{k_i-1} \pmod{\mathfrak{p}^m})$$

where χ denotes the p -adic cyclotomic character $\chi : G_{\mathbb{Q}} \rightarrow \mathbb{Z}_p^\times$, and the nebentypus characters ψ_i are now seen as finite order characters on $G_{\mathbb{Q}}$. Observe that the characters ψ_i take values in \mathcal{O}_K so that it makes sense to reduce them mod \mathfrak{p}^m . Also, reducing χ mod \mathfrak{p}^m is to be taken in the obvious sense.

We can now deduce that

$$(\psi_2 \psi_1^{-1} \pmod{\mathfrak{p}^m})|_{I_p} = (\chi \pmod{\mathfrak{p}^m})|_{I_p}^{k_1 - k_2}.$$

Now let us view via local class field theory the character $(\chi \pmod{\mathfrak{p}^m})|_{I_p}$ as a character on \mathbb{Z}_p^\times . As such it factors through $(\mathbb{Z}/\mathbb{Z}p^{\lceil \frac{m}{e} \rceil})^\times$ and has order

$$p^{\lceil \frac{m}{e} \rceil - 1} \cdot (p-1);$$

cf. Lemma 1. By definition, the character $(\psi_2 \psi_1^{-1} \pmod{\mathfrak{p}^m})|_{I_p}$ has order $p^\delta \cdot d$ with d a divisor of $p-1$. Hence, first we see that $p^\delta \cdot d$ is a divisor of $p^{\lceil \frac{m}{e} \rceil - 1} \cdot (p-1)$ which implies that $\delta \leq \lceil \frac{m}{e} \rceil - 1$. Secondly, we then conclude that $k_1 - k_2$ is divisible by $p^{\lceil \frac{m}{e} \rceil - 1 - \delta} \cdot (p-1)/d$ as desired.

Proof of part (ii): Observe first the following. If $p \nmid N$ then upon replacing N by Np and then calculating μ' we end up with the same number μ' as had we calculated it from N . And of course our forms are also forms on $\Gamma_1(Np)$.

This means that we may well assume that N is divisible by p , – our hypotheses remain unchanged when N is replaced by Np if N is not divisible by p .

In particular, we may assume that the group $\Gamma_1(N)$ is contained in $\Gamma_1(p)$.

Now assume without loss of generality that $k_2 \geq k_1$. Our hypotheses imply that we can then write:

$$k_2 = k_1 + t \cdot p^{\lceil \frac{m}{e} \rceil - 1} \cdot (p-1)/d$$

with t a non-negative integer.

Since p is odd there is a certain Eisenstein series E on $\Gamma_1(p)$ of weight

$$\kappa := (p-1)/d$$

and \mathfrak{p}' -adically integral coefficients in the field $\mathbb{Q}(\mu_{p-1})$ of $(p-1)$ 'st roots of unity with \mathfrak{p}' a prime of $\mathbb{Q}(\mu_{p-1})$ over p , and which reduces to 1 modulo \mathfrak{p}' : E is the form derived from

$$G := L(1 - \kappa, \omega^{-\kappa})/2 + \sum_{n=1}^{\infty} \left(\sum_{d|n} \omega^{-\kappa}(d) \cdot d^{\kappa-1} \right)$$

by scaling so that the constant term is 1. Here, ω is the character that becomes the Teichmüller character when viewed as taking values in \mathbb{Z}_p^\times . Cf. Serre, [8], Lemme 10, and Ribet, [7], §2.

Now view E as having coefficients in the compositum M of K and $\mathbb{Q}(\mu_{p-1})$. Pick a prime \mathfrak{p}_1 of M over \mathfrak{p} . Then the ramification index of \mathfrak{p}_1 relative to p is e . We deduce that

$$E^{p^{\lceil \frac{m}{e} \rceil - 1} \cdot t} \equiv 1 \pmod{\mathfrak{p}_1^m}$$

and so $\tilde{f} := f_1 \cdot E^{p^{\lceil \frac{m}{e} \rceil - 1} \cdot t} \equiv f_1 \pmod{\mathfrak{p}_1^m}$. As now \tilde{f} is a form on $\Gamma_1(N)$ (as N is divisible by p and E is on $\Gamma_1(p)$) of weight

$$k_1 + p^{\lceil \frac{m}{e} \rceil - 1} \cdot t \cdot \kappa = k_2$$

we can finish the argument in the same way as in the proof of part (ii) of Theorem 1. \square

3. EXAMPLES

We used the mathematics software program MAGMA [1] to find examples illustrating Theorem 1. We looked for examples of higher congruences and where p is ramified in the field of coefficients. In the notation of this paper, what we are looking for are situations where $e > 1$ and $s \geq 1$. Here are 2 such examples.

We start with

$$f_1 = q - 8q^4 + 20q^7 + \dots,$$

the (normalized) cusp form on $\Gamma_0(9)$ of weight 4 with integral coefficients, and look for congruences of the coefficients of f_1 and f_2 modulo powers of a prime above 5, for a form f_2 of weight k_2 satisfying $k_2 \equiv 4 \pmod{5 \cdot (5-1)}$.

The smallest possible choice of weight for f_2 is $k_2 = 24$. There is a newform f_2 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 $5\mathcal{O}_K = \mathfrak{p}^2\mathfrak{p}_2$.

We have $k = 24$, $N = 9$, $N' = 675$ and $\mu' = 1080$, and we find that $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^3}$ 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 Theorem 1 we conclude that $a_\ell(f_1) \equiv a_\ell(f_2) \pmod{\mathfrak{p}^3}$ for all primes $\ell \neq 3, 5$.

Similarly we find a newform f_3 on $\Gamma_0(9)$ of weight $k_3 = 44$ with coefficients in a number field $K' = \mathbb{Q}(\beta)$ with β a root of

$$x^8 - 438896x^6 + 60873718294x^4 - 2968020622607040x^2 + 40426030666768772025.$$

As before 5 is ramified in K' and has the decomposition $5\mathcal{O}_{K'} = \mathfrak{p}^4\mathfrak{p}_2^2\mathfrak{p}_3^2$, and thus $e = 4$. One finds that $a_\ell(f_1) \equiv a_\ell(f_3) \pmod{\mathfrak{p}^5}$ for primes $\ell \leq k_2\mu'/12 = 3960$ with $\ell \neq 3, 5$. The Galois closure L' of K' satisfies $[L' : \mathbb{Q}] = 384 \not\equiv 0 \pmod{5}$, which again implies $r = 0$. With $m = 5$ we have $s = 1$ and conclude by Theorem 1 that $a_\ell(f_1) \equiv a_\ell(f_3) \pmod{\mathfrak{p}^5}$ for all primes $\ell \neq 3, 5$.

We are developing a larger database of similar examples. This will be reported on elsewhere.

REFERENCES

- [1] W. Bosma, J. Cannon, C. Playoust: ‘The Magma algebra system. I. The user language’, *J. Symbolic Comput.* **24** (1997), 235–265.
- [2] H. Carayal: ‘Formes Modulaires et Représentations Galoisiennes à valeurs dans un Anneau Local complet’, in *p -adic Monodromy and the Birch and Swinnerton-Dyer Conjecture* (Boston, MA, 1991), *Contemp. Math.* **165** (1994), Amer. Math. Soc., 213–237.
- [3] I. Chen, I. Kiming: ‘On modular mod \mathfrak{p}^m Galois representations’, in preparation.
- [4] F. Diamond, J. Shurman: ‘A first course in modular forms’, *Graduate texts in Mathematics* **228**, Springer, 2005.
- [5] N. M. Katz: ‘ p -adic properties of modular schemes and modular forms’, in *Modular Functions of One Variable III*, *Lecture Notes in Math.* **350** (1973), 69–190.
- [6] T. Miyake: ‘Modular Forms’, Springer-Verlag, 1989.
- [7] K. Ribet: ‘Report on mod ℓ representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ’, *Motives, Proc. Sympos. Pure Math.*, 55, Part 2, 639–676, Amer. Math. Soc., 1994.
- [8] J.-P. Serre: ‘Formes modulaires et fonctions zêta p -adiques’, *Modular functions of one variable*, III, pp. 191–268. *Lecture Notes in Math.* **350**, Springer, 1973.
- [9] J. Sturm: ‘On the Congruence of Modular Forms’, in *Number Theory, Lecture Notes in Math.* **1240** (1987), 275–280.

(Imin Chen) DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, 8888 UNIVERSITY DRIVE, BURNABY, B.C., V5A 1S6, CANADA

E-mail address: ichen@math.sfu.ca

(Ian Kiming, Jonas B. Rasmussen) DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF COPENHAGEN, UNIVERSITETSPARKEN 5, 2100 COPENHAGEN Ø, DENMARK

E-mail address: kiming@math.ku.dk

E-mail address: jonas@math.ku.dk