On modular Galois representations modulo prime powers

Chen, Imin; Kiming, Ian; Wiese, Gabor

World Scientific
www.worldscientific.com

ON MODULAR GALOIS REPRESENTATIONS
MODULO PRIME POWERS

IMIN CHEN

Department of Mathematics, Simon Fraser University
8888 University Drive, Burnaby, BC, V5A 1S6, Canada
ichen@math.sfu.ca

IAN KIMING

Department of Mathematics, University of Copenhagen
Universitetsparken 5, DK-2100 Copenhagen Ø, Denmark
kiming@math.ku.dk

GABOR WIESE

Faculté des Sciences
de la Technologie et de la Communication
Université du Luxembourg
6, rue Richard Coudenhove-Kalergi
L-1359 Luxembourg, Luxembourg
gabor.wiese@uni.lu

We study modular Galois representations mod p^m. We show that there are three progressively weaker notions of modularity for a Galois representation mod p^m: We have named these "strongly", "weakly", and "dc-weakly" modular. Here, "dc" stands for "divided congruence" in the sense of Katz and Hida. These notions of modularity are relative to a fixed level M. Using results of Hida we display a level-lowering result ("stripping-of-powers of p away from the level"): A mod p^m strongly modular representation of some level Np^r is always dc-weakly modular of level N (here, N is a natural number not divisible by p). We also study eigenforms mod p^m corresponding to the above three notions. Assuming residual irreducibility, we utilize a theorem of Carayol to show that one can attach a Galois representation mod p^m to any "dc-weak" eigenform, and hence to any eigenform mod p^m in any of the three senses. We show that the three notions of modularity coincide when $m = 1$ (as well as in other particular cases), but not in general.

Keywords: Galois representations; Hida theory; higher congruences of modular forms; level lowering.

Mathematics Subject Classification 2010: 11F80, 11F33, 11F11

1. Introduction

Let p be a prime number, which remains fixed throughout the article. Let N be a natural number not divisible by p. All number fields in the article are taken inside some fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and we fix once and for all field embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, as well as a compatible isomorphism $\mathbb{C} \cong \overline{\mathbb{Q}}_p$. Here, $\overline{\mathbb{Q}}_p$ is a fixed algebraic closure of $\mathbb{Q}_p$. We also denote by $\overline{\mathbb{Z}}_p$ the ring of integers of $\overline{\mathbb{Q}}_p$.

Let $f = \sum_{n=1}^{\infty} a_n(f) q^n \in S_k(\Gamma_1(Np^r))$ be a normalized cuspidal eigenform for all Hecke operators T_n with $n \geq 1$ (normalized means $a_1(f) = 1$). By Shimura, Deligne, and Serre, there is a continuous Galois representation

$$\rho = \rho_{f,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$$

attached to f, which is unramified outside Np, and which satisfies

$$\mathrm{tr}\,\rho(\mathrm{Frob}_\ell) = a_\ell(f) \quad \text{and} \quad \det\rho(\mathrm{Frob}_\ell) = \ell^{k-1}\chi(\ell),$$

for primes $\ell \nmid Np$, where χ is the nebentypus of f.

By continuity and compactness, the Galois representation descends to a representation

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

where $\mathcal{O}_K$ is the ring of integers of a finite extension K of $\mathbb{Q}_p$. This representation depends in general on a choice of $\mathcal{O}_K$-lattice Λ in K^2. Let $\mathfrak{p} = \mathfrak{p}_K$ be the maximal ideal of $\mathcal{O}_K$. We wish to consider the reduction mod $\mathfrak{p}^m$ of $\rho_{f,\Lambda,p}$. However, because of ramification, the exponent m is not invariant under base extension.

For this reason, it is useful, following [17], to define $\gamma_K(m) := (m-1)e_{K/\mathbb{Q}_p} + 1$, with $e_{K/\mathbb{Q}_p}$ the ramification index of $K/\mathbb{Q}_p$. This definition is made precisely so that the natural maps below yield injections of rings, i.e. ring extensions of $\mathbb{Z}/p^m\mathbb{Z}$,

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

for any finite extension L/K (with $\mathfrak{P}_L$ the prime of L over $\mathfrak{p}_K$ in K). We can thus form the ring

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

which we also consider as a topological ring with the discrete topology. When we speak of $\alpha \pmod{p^m}$ for $\alpha \in \overline{\mathbb{Z}}_p$, we mean its image in $\overline{\mathbb{Z}/p^m\mathbb{Z}}$. In particular, for $\alpha, \beta \in \overline{\mathbb{Z}}_p$, we define $\alpha \equiv \beta \pmod{p^m}$ as an equality in $\overline{\mathbb{Z}/p^m\mathbb{Z}}$, or equivalently, by $\alpha - \beta \in \mathfrak{p}_K^{\gamma_K(m)}$, where $K/\mathbb{Q}_p$ is any finite extension containing α and β.

In this spirit, we define the reductions

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

for any $m \in \mathbb{N}$. The representation $\rho_{f,\Lambda,p,m}$ has the property:

$$\mathrm{tr}\,\rho_{f,\Lambda,p,m}(\mathrm{Frob}_\ell) = (a_\ell(f) \mod p^m) \tag{$*$}$$

for all primes $\ell \nmid Np$.

From [2, Théorème 1] and the Chebotarev density theorem, a continuous Galois representation $\rho_{p,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$ is determined uniquely up to isomorphism by $\mathrm{tr}\,\rho_{p,m}(\mathrm{Frob}_\ell)$ for almost all (i.e. all but finitely many) primes ℓ, assuming the residual representation is absolutely irreducible. It follows that if there is one choice of $\mathcal{O}_K$-lattice Λ as above such that $\rho_{f,\Lambda,p,1}$ is absolutely irreducible, then $\rho_{f,p,m} = \rho_{f,\Lambda,p,m}$ is determined uniquely up to isomorphism. In such a case, we say $\rho_{f,p,m}$ is the mod p^m Galois representation attached to f.

Let $M \in \mathbb{N}$. The $\mathbb{C}$-vector spaces $S = S_k(\Gamma_1(M))$ and $S = S^b(\Gamma_1(M)) := \bigoplus_{i=1}^b S_i(\Gamma_1(M))$ have integral structures, so it is possible to define (arithmetically) the A-module of cusp forms in S with coefficients in a ring A, which we denote by $S(A)$ (cf. Sec. 2.3). The spaces $S(A)$ have actions by the Hecke operators T_n for all $n \geq 1$. We point out that every $f \in S(\mathbb{Z}/p^m\mathbb{Z})$ can be obtained as the reduction of some $\tilde{f} \in S(\mathcal{O}_K)$ for some number field (or p-adic field) K. However, for $m > 1$, if f is an eigenform for the Hecke operators T_n over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$ (for all $n \geq 1$ coprime to some fixed positive integer D), the lift $\tilde{f}$ cannot be chosen as an eigenform (for the same Hecke operators), in general.

We introduce the following three progressively weaker notions of eigenforms mod p^m.

Definition 1.

- We say that $f \in S_k(\Gamma_1(M))(\overline{\mathbb{Z}/p^m\mathbb{Z}})$ is a *strong Hecke eigenform* (*of level M and weight k over* $\overline{\mathbb{Z}/p^m\mathbb{Z}}$) if there is an element $\tilde{f} \in S_k(\Gamma_1(M))(\overline{\mathbb{Z}}_p)$ that reduces to f and a positive integer D such that

$$T_n\tilde{f} = a_n(\tilde{f}) \cdot \tilde{f} \quad \text{and} \quad a_1(\tilde{f}) = 1$$

for all $n \geq 1$ coprime with D, where $a_n(\tilde{f})$ is the nth coefficient in the q-expansion of $\tilde{f}$ at ∞.

- We say $f \in S_k(\Gamma_1(M))(\overline{\mathbb{Z}/p^m\mathbb{Z}})$ is a *weak Hecke eigenform* (*of level M and weight k over* $\overline{\mathbb{Z}/p^m\mathbb{Z}}$) if

$$T_nf = f(T_n) \cdot f \quad \text{and} \quad f(T_1) = 1$$

for all $n \geq 1$ coprime to some positive integer D. The piece of notation $f(T_n)$ is defined in Sec. 2.3 and represents the nth coefficient of the formal q-expansion of f.

- We say $f \in S^b(\Gamma_1(M))(\overline{\mathbb{Z}/p^m\mathbb{Z}})$ is a *dc-weak Hecke eigenform* (*of level M and in weights $\leq b$ over* $\overline{\mathbb{Z}/p^m\mathbb{Z}}$) if

$$T_nf = f(T_n) \cdot f \quad \text{and} \quad f(T_1) = 1$$

for all $n \geq 1$ coprime to some positive integer D. Here, dc stands for "divided congruence" for reasons that will be explained in detail below.

We point out that above (and also in Definition 10), we define eigenforms as "eigenforms away from finitely many primes" because this extra flexibility is very

useful in our applications. We will specify this implicit parameter D when necessary. In that case, we will speak of an *eigenform away from D*.

There are natural maps

$$S_k(\Gamma_1(M))(\overline{\mathbb{Z}}_p) \to S_k(\Gamma_1(M))(\overline{\mathbb{Z}/p^m\mathbb{Z}}),$$

$$S_k(\Gamma_1(M))(\overline{\mathbb{Z}/p^m\mathbb{Z}}) \hookrightarrow S^b(\Gamma_1(M))(\overline{\mathbb{Z}/p^m\mathbb{Z}}), \quad k \leq b,$$

$$S^b(\Gamma_1(M))(\overline{\mathbb{Z}/p^m\mathbb{Z}}) \hookrightarrow \varinjlim_{c \geq 1} S^c(\Gamma_1(M))(\overline{\mathbb{Z}/p^m\mathbb{Z}}).$$

It follows that a strong eigenform of level M and some weight is a weak eigenform of the same level and weight, and that a weak eigenform of level M and some weight gives rise to a dc-weak eigenform of the same level. Furthermore, if we regard our eigenforms inside the last direct limit, we can make sense of when two eigenforms (of the various kinds) are the same.

We derive in this article from Katz–Hida theory ([10–12]) that a dc-weak form of some level Np^r is dc-weak of level N (recall $p \nmid N$), under some mild technical restrictions. More precisely, we prove the following proposition.

Proposition 2. *Suppose that $p \geq 5$. Let $f \in S^b(\Gamma_1(Np^r))(\overline{\mathbb{Z}/p^m\mathbb{Z}})$. Then there is $c \in \mathbb{N}$ and an element $g \in S^c(\Gamma_1(N))(\overline{\mathbb{Z}/p^m\mathbb{Z}})$ such that*

$$f(q) = g(q) \in \overline{\mathbb{Z}/p^m\mathbb{Z}}[[q]],$$

where $f(q)$ and $g(q)$ denote the q-expansions of f and g.

As we show in Lemma 16, when $m = 1$, a dc-weak f eigenform over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$ is in fact a strong eigenform. This means that we have a mod p Galois representation $\rho_{f,p,1}$ attached to f. Using results of Carayol [2], we show more generally that it is possible to attach mod p^m Galois representations to dc-weak eigenforms of level M over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$, whenever the residual representation is absolutely irreducible. More general results involving infinite-dimensional completed Hecke algebras are due to Mazur, Gouvêa (see specifically [8, Corollary III.5.8]), Hida, and Wiles, but we provide a self-contained proof based on [2].

Theorem 3. *Let f be a 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 almost all primes $\ell \nmid Mp$ we have

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

where $f(T_\ell) \in \overline{\mathbb{Z}/p^m\mathbb{Z}}$ is the eigenvalue of the operator T_ℓ (see Sec. 2).

One can be more precise: If the normalized dc-weak eigenform in the theorem is an eigenform for all T_n with n coprime to the positive integer D, then the final equality holds for all primes $\ell \nmid DMp$.

Having Galois representations attached to dc-weak eigenforms (and hence also to weak eigenforms), we can consider modularity questions. Towards this aim, we introduce further terminology corresponding to the above three notions of "eigenform mod p^m".

Definition 4. Given a Galois representation

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

which we assume to be residually absolutely irreducible, we say that $\rho_{p,m}$

- strongly arises from $\Gamma_1(M)$ if $\rho_{p,m}$ is isomorphic to $\rho_{f,p,m}$ for some strong Hecke eigenform f. As discussed above, this is equivalent to

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

  almost all primes $\ell \nmid Mp$, where $\tilde{f}$ is a normalized eigenform over $\overline{\mathbb{Z}}_p$ lifting f.
- We say $\rho_{p,m}$ *weakly arises from* $\Gamma_1(M)$ if $\rho_{p,m}$ is isomorphic to $\rho_{f,p,m}$ for some weak Hecke eigenform of level M and some weight k over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$.
- We say that $\rho_{p,m}$ *dc-weakly arises from* $\Gamma_1(M)$ if $\rho_{p,m}$ is isomorphic to $\rho_{f,p,m}$ for some dc-weak Hecke eigenform of level M over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$.

One of the motivations behind the present work is building a framework for understanding such mod p^m representations. We consider it conceptually very important to establish a precise link between mod p^m Galois representations, especially those that arise as reductions of p-adic ones, and modular forms mod p^m. Such a link would have many important consequences of a theoretical and computational nature.

Results about mod p Galois representations and their modularity have proven very useful in applications to Diophantine equations — such as in the proof of Fermat's Last Theorem, and many other families of generalized Fermat equations. In [4], a Ribet-type level lowering result for mod p^m Galois representations is proven and applied to resolve some new cases of generalized Fermat equations.

In the present paper we treat the question of "stripping powers of p away from the level".

Question. If $\rho_{p,m}$ strongly arises from $\Gamma_1(Np^r)$, does it strongly arise from $\Gamma_1(N)$?

As is well-known, mod p Galois representations $\rho_{f,p,1}$ always strongly arise from $\Gamma_1(N)$, cf. [15, Theorem 2.1] for $p \geq 3$, and [9, Theorem 2] for $p \geq 2$. However, when the nebentypus has a non-trivial component of p-power conductor and order, the representations $\rho_{f,p,m}$ do not in general even weakly arise from $\Gamma_1(N)$ if $m \geq 2$, as we show in Sec. 5.

Let us remark that in the deduction that mod p Galois representations in level Np^r always strongly arise from level N (rather than just weakly arise or dc-weakly arise) one uses two facts: the validity of the Deligne–Serre lifting lemma for mod p representations, and the absence of constraints on the determinant of mod p Galois

representations arising from strong Hecke eigenforms. Neither of these facts are true in general for mod p^m representations.

However, we derive from Katz–Hida theory, via Proposition 2, the following weaker version mod p^m of the above level-lowering result.

Theorem 5. *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 $\Gamma_1(N)$.

Proof. This follows by a combination of Proposition 2 and Theorem 3: By definition the form f is a normalized eigenform for all T_n with $(n, D) = 1$. Pick a form g at level N according to Proposition 2. Enlarging D if necessary so as to have $p|D$, we can be sure that g is also a normalized eigenform for all T_n with $(n, D) = 1$. As the Galois representation attached to g by Theorem 3 is isomorphic to $\rho_{f,p,m}$, the desired follows.   □

We stress the following particular consequence of the theorem. If $f \in S_k(\Gamma_1(Np^r))$ is a normalized eigenform, then there exist a number field K and a $g \in S^b(N)(\mathcal{O}_K)$ (which cannot be taken to be an eigenform, in general) such that $g \pmod{p^m}$ is a dc-weak eigenform and its attached Galois representation $\rho_{g,p,m}$ is isomorphic to $\rho_{f,p,m}$. We do not treat in this paper the more difficult question of weight information concerning such a g.

We note that a result of Hatada [9, Theorem 1] has a consequence that can be interpreted as the following statement, showing that the need for divided congruence forms only appears when the nebentypus has a non-trivial component of p-power conductor and order.

Theorem 6 (Hatada). *Let f be a strong eigenform of level Np^r and weight k over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$ 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 $\Gamma_1(N)$.*

The paper is organized as follows. In Sec. 2 we provide background information on integral structures on spaces of modular forms, Hecke algebras, and divided congruence forms. In Sec. 3 we construct Galois representations attached to dc-weak eigenforms. In Sec. 4 we give a proof of our level-lowering result in the mod p^m setting. Finally, in Sec. 5 we make a number of observations on the relations between the three notions "strong", "weak", and "dc-weak" of eigenforms mod p^m.

2. Modular Forms and Hecke Algebras

All material in this section is well-known. We present it here in a concise form.

2.1. *q-expansions*

Let $\mathcal{S} = \bigoplus_{k \in \mathbb{N}} S_k(\Gamma_1(M))$ be the $\mathbb{C}$-vector space of all cusp forms of any positive weight at a fixed level M. Let each Hecke operator T_n act on $\mathcal{S}$ via the diagonal

action. We will be considering finite-dimensional subspaces $S \subseteq \mathcal{S}$ of the following type:

$$S = S^b(\Gamma_1(M)) := \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$$

for any $b \in \mathbb{N}$, $M \geq 1$. Such a subspace S is stabilized by T_n for all $n \geq 1$.

For $f \in \mathcal{S}$, let $f(q) \in \mathbb{C}[[q]]$ denote its q-expansion. We denote the *q-expansion map* on $S \subset \mathcal{S}$ by

$$\Phi_S : S \to \mathbb{C}[[q]], \quad f \mapsto f(q) = \sum_{n \geq 1} a_n(f)q^n.$$

Proposition 7. *Fix $M \in \mathbb{N}$ and $b \in \mathbb{N}$. Let $S := S^b(\Gamma_1(M))$. Then Φ_S is injective.*

Proof. Let $f_k \in S_k(\Gamma_1(M))$, for $k = 1, \ldots, b$, be such that $\sum_{k=1}^{b} f_k(q) = 0$. The function $\sum_{k=1}^{b} f_k$ is holomorphic and 1-periodic and hence uniquely determined by its Fourier series. Hence, $\sum_{k=1}^{b} f_k = 0$ and it then follows from [14, Lemma 2.1.1] that we have $f_k = 0$ for each k. □

2.2. *Hecke algebras*

Let R be a subring of $\mathbb{C}$. Let

$$\mathbb{T}_R(S) \subseteq \mathrm{End}_{\mathbb{C}}(S)$$

be the *R-Hecke algebra* associated to $S \subset \mathcal{S}$, defined as the R-algebra generated by Hecke operators T_n, $n \geq 1$.

Lemma 8. *Let $S := S^b(\Gamma_1(M))$.*

(a) *Let $f \in S$. Then $a_1(T_n f) = a_n(f)$ for all $n \geq 1$.*
(b) *Let $R \subseteq \mathbb{C}$ be a subring. Then the pairing of R-modules*

$$\mathbb{T}_R(S) \times S \to \mathbb{C}, \quad (T, f) \mapsto a_1(Tf)$$

is non-degenerate.

Proof. Part (a) follows, since the equation $a_1(T_n f) = a_n(f)$ is true on every summand of S, hence also in the sum.

(b) Let first $f \in S$ be given. If $a_1(Tf) = 0$ for all $T \in \mathbb{T}_R(S)$, then, in particular, $a_1(T_n f) = a_n(f) = 0$ for all n, whence f is zero by the injectivity of the q-expansion map. Let now $T \in \mathbb{T}_R(S)$ be given. If $a_1(Tf) = 0$ for all $f \in S$, then, in particular, $0 = a_1(T(T_n f)) = a_n(Tf)$ for all f and all n. Thus, as before we conclude that Tf is zero for all f, which by definition means $T = 0$. □

2.3. *Integral structures and cusp forms with coefficients in rings*

As is well-known, the spaces $S_k(\Gamma_1(M))$ have integral structures in the sense that $S_k(\Gamma_1(M))$ contains a full lattice which is stable under the Hecke operators T_n for

all $n \geq 1$ (cf., for instance, [5, Proposition 2.7]). It follows that the space $S = S^b(\Gamma_1(M)) := \bigoplus_{k=1}^b S_k(\Gamma_1(M))$ also contains a full lattice stable under the Hecke operators T_n for all $n \geq 1$.

Thus, $\mathbb{T}_{\mathbb{Z}}(S)$ sits inside an integer matrix ring, and $\mathbb{T}_{\mathbb{C}}(S)$ sits inside the corresponding complex matrix ring. This implies that $\mathbb{T}_{\mathbb{Z}}(S)$ is free and finite over $\mathbb{Z}$. Furthermore, the natural homomorphism $\mathbb{T}_{\mathbb{Z}}(S) \otimes \mathbb{C} \to \mathbb{T}_{\mathbb{C}}(S)$ is injective, so as $T_n \otimes 1$ is sent to T_n and these generate $\mathbb{T}_{\mathbb{C}}(S)$ over $\mathbb{C}$, this is an isomorphism

$$\mathbb{T}_{\mathbb{Z}}(S) \otimes \mathbb{C} \cong \mathbb{T}_{\mathbb{C}}(S).$$

Hence we also see that the map

$$\alpha : \operatorname{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}(S), \mathbb{C}) \to \operatorname{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{Z}}(S) \otimes \mathbb{C}, \mathbb{C}) \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S), \mathbb{C})$$

coming from $\mathbb{T}_{\mathbb{Z}}(S) \to \mathbb{T}_{\mathbb{Z}}(S) \otimes \mathbb{C} \to \mathbb{T}_{\mathbb{C}}(S)$ is an isomorphism (the last arrow is always an isomorphism).

Now, $S \cong \operatorname{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}(S), \mathbb{C})$ as we have a non-degenerate pairing between these two complex vector spaces, cf. Lemma 8. Explicitly, we obtain an isomorphism

$$\beta : \operatorname{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}(S), \mathbb{C}) \to S$$

by mapping $\phi \in \operatorname{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}(S), \mathbb{C})$ to $\sum_n \phi(T_n) q^n$ ($q = e^{2\pi i z}$). By the above isomorphisms, it follows that the map

$$\Psi_S := \beta \circ \alpha^{-1} : \operatorname{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S), \mathbb{C}) \to S,$$

which satisfies

$$\Psi_S(\phi) = \sum_n \phi(T_n) q^n,$$

is well defined and is an isomorphism.

Definition 9. Let A be any commutative ring A. We let

$$S(A) := \operatorname{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S), A) \quad (\mathbb{Z}\text{-}linear\ homomorphisms),$$

which we call the *cusp forms in S with coefficients in A*.

The A-module $S(A)$ is equipped with a natural action of $\mathbb{T}_{\mathbb{Z}}(S)$ given by

$$(T.f)(T') = f(TT').$$

Note that $S(\mathbb{C}) \cong S$. We remark that for any ring A and any $1 \leq k \leq b$, the map

$$S_k(\Gamma_1(M))(A) \to S^b(\Gamma_1(M))(A), \quad f \mapsto f \circ \pi,$$

is an injective A-module homomorphism, where π is the surjective ring homomorphism

$$\mathbb{T}_{\mathbb{Z}}(S^b(\Gamma_1(M))) \to \mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(M)))$$

defined by restricting Hecke operators.

We mention that for $k \geq 2$ and $M \geq 5$ invertible in A, $S_k(\Gamma_1(M))(A)$ coincides with the corresponding A-module of Katz modular forms (see e.g., [6, Theorem 12.3.2]).

Definition 10. We say that a cusp form $f \in S(A)$ is a *normalized Hecke eigenform* if there is a positive integer D such that

$$T_n f = f(T_n) \cdot f \quad \text{and} \quad f(T_1) = 1$$

for all integers n coprime to D.

The above notion of normalized Hecke eigenform is consistent with Definition 1. As before, if the parameter D is specified, then we will speak of an *eigenform away from D*.

The chosen isomorphism $\mathbb{C} \cong \overline{\mathbb{Q}}_p$ identifies $S \cong S(\mathbb{C})$ with $S(\overline{\mathbb{Q}}_p)$. Hence, via the isomorphism $S(\mathbb{C}) \cong S$ normalized holomorphic eigenforms in S (in the usual sense, for almost all Hecke operators) are precisely the normalized eigenforms in $S(\overline{\mathbb{Q}}_p)$. In the following we will identify forms in S with elements in either of the two spaces $S(\mathbb{C})$ and $S(\overline{\mathbb{Q}}_p)$.

Let $R \subseteq \mathbb{C}$ be a subring. For a positive integer D, let $\mathbb{T}_R^{(D)}(S)$ be the R-subalgebra of $\mathbb{T}_R(S)$ generated by those Hecke operators T_n for which n and D are coprime.

Lemma 11. *Let A be a ring, $f \in S(A)$ be a normalized Hecke eigenform and D be as in Definition* 10.

Then the restriction of f to $\mathbb{T}_\mathbb{Z}^{(D)}$ is a ring homomorphism.

Proof. The claim immediately follows from the equation

$$f(TT') = (T \cdot f)(T') = f(T)f(T')$$

with $T, T' \in \mathbb{T}_\mathbb{Z}^{(D)}(S)$. □

2.4. *Integral structures for Hecke algebras, base change and lifting*

Using the integral structure on S we can also equip Hecke algebras with an integral structure in the following sense.

Lemma 12. *Fix $M, b \in \mathbb{N}$ and let $S := \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$. Let $R \subseteq \mathbb{C}$ be a subring.*

(a) *The R-Hecke algebra $\mathbb{T}_R(S)$ is free as an R-module of rank equal to $\dim_\mathbb{C} S$, in particular, $\mathbb{T}_\mathbb{Z}(S)$ is a free $\mathbb{Z}$-module of that rank.*
(b) *$\mathbb{T}_R(S) \cong \mathbb{T}_\mathbb{Z}(S) \otimes_\mathbb{Z} R$.*

Proof. We know that the natural map $\mathbb{T}_\mathbb{Z}(S) \otimes \mathbb{C} \to \mathbb{T}_\mathbb{C}(S)$ is an isomorphism and that $\mathbb{T}_\mathbb{Z}(S)$ is free and finite over $\mathbb{Z}$. It follows that $\mathbb{T}_\mathbb{Z}(S)$ is a lattice of full rank in $\mathbb{T}_\mathbb{C}(S)$. That rank is the $\mathbb{C}$-dimension of $\mathbb{T}_\mathbb{C}(S)$, i.e. of $\mathrm{Hom}_\mathbb{C}(\mathbb{T}_\mathbb{C}(S), \mathbb{C}) \cong S$. Hence we have (a) for $R = \mathbb{Z}$.

It follows immediately that $\mathbb{T}_{\mathbb{Z}}(S) \otimes_{\mathbb{Z}} R$ is a free R-module of the same rank, which surjects onto $\mathbb{T}_R(S)$. Now, $\mathbb{T}_{\mathbb{Z}}(S)$ has a $\mathbb{Z}$-basis which remains linearly independent over $\mathbb{C}$. Thus, it also remains linearly independent over R, and its R-span is by definition $\mathbb{T}_R(S)$, which is thus a free R-module of the same rank and is isomorphic to $\mathbb{T}_{\mathbb{Z}}(S) \otimes_{\mathbb{Z}} R$. $\qquad\square$

We further obtain that cusp forms in S with coefficients behave well with respect to arbitrary base change.

Lemma 13. *Fix $M, b \in \mathbb{N}$ and let $S := \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$. Let $A \to B$ be a ring homomorphism. Then $S(A) \otimes_A B \cong S(B)$.*

Proof. By Lemma 12 we know that $\mathbb{T}_{\mathbb{Z}}(S)$ is a free $\mathbb{Z}$-module of some finite rank d. Hence, $S(A) \otimes_A B = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S), A) \otimes_A B \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^d, A) \otimes_A B \cong A^d \otimes_A B \cong B^d \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^d, B) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S), B) = S(B)$. $\qquad\square$

For the sake of completeness we also record the following simple lifting property.

Lemma 14. *Fix $M, b \in \mathbb{N}$ and let $S := \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$.*

Let $f \in S(\overline{\mathbb{Z}/p^m\mathbb{Z}})$. Then there is a number field (and hence there is also a p-adic field) K and $\tilde{f} \in S(\mathcal{O}_K)$ such that $\tilde{f} \equiv f \pmod{p^m}$, in the sense that $\tilde{f}(T_n) \equiv f(T_n) \pmod{p^m}$ for all $n \in \mathbb{N}$.

Proof. As $\mathbb{T}_{\mathbb{Z}}(S)$ is a free $\mathbb{Z}$-module of finite rank (Lemma 12), it is a projective $\mathbb{Z}$-module. Moreover, the image of the homomorphism (of abelian groups) $f : \mathbb{T}_{\mathbb{Z}}(S) \to \overline{\mathbb{Z}/p^m\mathbb{Z}}$ lies in $\mathcal{O}_K/\mathfrak{p}_K^{\gamma_K(m)}$ for some number field (or, p-adic field) K. The projectivity implies by definition that f lifts to a homomorphism $\tilde{f} : \mathbb{T}_{\mathbb{Z}}(S) \to \mathcal{O}_K$. $\qquad\square$

We stress again that eigenforms mod p^m cannot, in general, be lifted to eigenforms if $m > 1$, but see Lemma 16.

2.5. *Divided congruences*

In the next lemma we will show that when the coefficients are over a $\mathbb{Q}$-algebra K one can split $S(K)$ into a direct sum according to weights. This does not hold true, in general, for arbitrary rings and leads to divided congruences.

Lemma 15. *Fix $M, b \in \mathbb{N}$ and let $S := \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$. Put $S_k := S_k(\Gamma_1(M))$ for each k.*

If K is any $\mathbb{Q}$-algebra, then one has $S(K) = \bigoplus_{k=1}^{b} S_k(K)$. Moreover, if K is a field extension of $\mathbb{Q}$ and $f \in S(K)$ is a normalized eigenform (say, it is an eigenform away from D), then there is k and a normalized eigenform $\tilde{f} \in S_k(L)$ for some finite extension L/K such that $f(T_n) = \tilde{f}(T_n)$ for all n coprime with D.

Proof. For each $1 \leq k \leq b$, we have a natural homomorphism $\mathbb{T}_{\mathbb{Q}}(S) \to \mathbb{T}_{\mathbb{Q}}(S_k)$ given by restriction, and hence taking the product of these, we obtain an injective homomorphism $\mathbb{T}_{\mathbb{Q}}(S) \to \prod_{k=1}^{b} \mathbb{T}_{\mathbb{Q}}(S_k)$ of $\mathbb{Q}$-algebras. By Lemma 12, we have that

$$\dim_{\mathbb{Q}} \mathbb{T}_{\mathbb{Q}}(S) = \dim_{\mathbb{C}} S = \sum_{k=1}^{b} \dim_{\mathbb{C}} S_k = \sum_{k=1}^{b} \dim_{\mathbb{Q}} \mathbb{T}_{\mathbb{Q}}(S_k),$$

showing that $\mathbb{T}_{\mathbb{Q}}(S) \cong \prod_{k=1}^{b} \mathbb{T}_{\mathbb{Q}}(S_k)$. Now, we see that

$$S(K) = \operatorname{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S), K) \cong \operatorname{Hom}_{\mathbb{Q}}(\mathbb{T}_{\mathbb{Z}}(S) \otimes_{\mathbb{Z}} \mathbb{Q}, K) \cong \operatorname{Hom}_{\mathbb{Q}}(\mathbb{T}_{\mathbb{Q}}(S), K)$$

$$\cong \operatorname{Hom}_{\mathbb{Q}}\left(\prod_{k=1}^{b} \mathbb{T}_{\mathbb{Q}}(S_k), K\right) \cong \bigoplus_{k=1}^{b} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S_k), K) = \bigoplus_{k=1}^{b} S_k(K).$$

Now assume that K is a field extension of $\mathbb{Q}$ and that $f \in S(K)$ is a normalized eigenform. By definition and Lemma 11 this means that there is a positive integer D such that the restriction of f to $\mathbb{T}_{\mathbb{Q}}^{(D)}(S)$ is a ring homomorphism $\mathbb{T}_{\mathbb{Q}}^{(D)}(S) \to K$. It can be extended to a ring homomorphism $\tilde{f} \colon \mathbb{T}_{\mathbb{Q}}(S) \to L$ for some finite extension L/K, since in the integral extension of rings $\mathbb{T}_{\mathbb{Q}}^{(D)}(S) \hookrightarrow \mathbb{T}_{\mathbb{Q}}^{(1)}(S) = \mathbb{T}_{\mathbb{Q}}(S)$ we need only to choose a prime ideal of $\mathbb{T}_{\mathbb{Q}}(S)$ lying over the prime ideal $\ker(f) \lhd \mathbb{T}_{\mathbb{Q}}^{(D)}(S)$ ("going up", see [7, Proposition 4.15]). We need to make this extension in order to apply the results of the preceding paragraph, which we only proved for the full Hecke algebra.

To conclude, it suffices to note that every ring homomorphism $\mathbb{T}_{\mathbb{Q}}(S) \to L$ factors through a unique $\mathbb{T}_{\mathbb{Q}}(S_k)$. In order to see this, one can consider a complete set of orthogonal idempotents $e_1, \ldots, e_n$ of $\mathbb{T}_{\mathbb{Q}}(S)$, i.e. $e_i^2 = e_i$, $e_i e_j = 0$ for $i \neq j$ and $1 = e_1 + \cdots + e_n$. As L is a field and idempotents are mapped to idempotents, each e_i is either mapped to 0 or 1, and as 0 maps to 0 and 1 maps to 1, there is precisely one idempotent that is mapped to 1, the others to 0. This establishes the final assertion. $\qquad\square$

We explicitly point out the following easy consequence of Lemma 15. We let $\mathcal{O}$ be the ring of integers of K, where K is a number field or a finite extension of $\mathbb{Q}_p$. Consider again a space S of the form $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$. By definition, it follows that we have

$$S(\mathcal{O}) = \{f \in S(K) | f(T_n) \in \mathcal{O} \, \forall n\} = \left\{ f \in \bigoplus_{k=1}^{b} S_k(K) | f(T_n) \in \mathcal{O} \, \forall n \right\}.$$

Hence, our spaces $S^b(\Gamma_1(Np^r))(K)$ and $S^b(\Gamma_1(Np^r))(\mathcal{O})$ are precisely the ones denoted $S^b(\Gamma_1(Np^r); K)$ and $S^b(\Gamma_1(Np^r); \mathcal{O})$ in [10, p. 550].

Explicitly, $f \in S(\mathcal{O})$ is of the form $f = \sum_k f_k$ with $f_k \in S_k(K)$, and although none of the f_k need to be in $S_k(\mathcal{O})$, the sum has all its coefficients in $\mathcal{O}$. This is the origin of the name "divided congruence" for such an f: Suppose for example that we have forms $g_k \in S(\mathcal{O})$ for various weights k and that $\sum_k g_k \equiv 0 \, (\pi^m)$ for

some m where π is a uniformizer of $\mathcal{O}$. Putting $f_k := g_k/\pi^m$ for each k we then have $f_k \in S_k(K)$ for all k as well as $f := \sum_k f_k \in S(\mathcal{O})$. Conversely, any element of $S(\mathcal{O})$ arises in this way by "dividing a congruence".

We now turn our attention to the case $m = 1$ (recall $\overline{\mathbb{Z}/p\mathbb{Z}} = \overline{\mathbb{F}}_p$) and give a short proof of the Deligne–Serre lifting lemma (see [5, Lemme 6.11]) in terms of our setup. It implies that "dc-weak", "weak", and "strong" are equivalent notions for $m = 1$.

Lemma 16 (Deligne–Serre lifting lemma). *Let $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$ be as above. 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 $g(T_n) \equiv f(T_n) \,(\mathrm{mod}\,p)$ for all n coprime with D (i.e. f is in fact a strong eigenform).*

Proof. The kernel of the ring homomorphism $f : \mathbb{T}_{\mathbb{Z}}^{(D)}(S) \to \overline{\mathbb{F}}_p$ is a maximal ideal $\mathfrak{m}$ of $\mathbb{T}_{\mathbb{Z}}^{(D)}(S)$. Recall that $\mathbb{T}_{\mathbb{Z}}^{(D)}(S)$ is free of finite rank as a $\mathbb{Z}$-module (by Lemma 12), whence it is equidimensional of Krull dimension 1, since $\mathbb{Z}_\ell \hookrightarrow \mathbb{T}_{\mathbb{Z}}^{(D)}(S)_\lambda$ is an integral ring extension for any completion at a maximal ideal λ (say, lying above ℓ), and the Krull dimension is invariant under integral extensions (cf. [7, Proposition 9.2], for instance). Consequently, there is a prime ideal $\mathfrak{p} \lhd \mathbb{T}_{\mathbb{Z}}^{(D)}(S)$ such that $\mathfrak{p} \subsetneq \mathfrak{m}$. The quotient $\mathbb{T}_{\mathbb{Z}}^{(D)}(S)/\mathfrak{p}$ is an order in a number field K. Moreover, there is a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ such that the following diagram is commutative:

$$
\begin{array}{ccccccc}
\mathbb{T}_{\mathbb{Z}}^{(D)}(S) & \longrightarrow & \mathbb{T}_{\mathbb{Z}}^{(D)}(S)/\mathfrak{p} & \hookrightarrow & \mathcal{O}_K & \hookrightarrow & \mathbb{C} \\
\| & & \downarrow & & \downarrow & & \\
\mathbb{T}_{\mathbb{Z}}^{(D)}(S) & \longrightarrow & \mathbb{T}_{\mathbb{Z}}^{(D)}(S)/\mathfrak{m} & \hookrightarrow & \mathcal{O}_K/\mathfrak{q} & \hookrightarrow & \overline{\mathbb{F}}_p.
\end{array}
$$

The lower row is the ring homomorphism f, and the upper row is a ring homomorphism that can be extended to a normalized Hecke eigenform g in $S(\mathbb{C}) = S$, which by (the proof of) Lemma 15 lies in $S_k(\Gamma_1(M))$ for some k. The commutativity of the diagram implies the claim on the reduction modulo p. $\square$

3. Galois Representations

In this section we construct a Galois representation attached to a dc-weak eigenform mod p^m. For expressing its determinant, we find it convenient to work with Hida's stroke operator $_{|\ell}$, which we denote by $[\ell]$. We recall its definition from [10, p. 549]. Let us consider again a space of the form $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(M))$ for some b. We now consider specifically a level M written in the form

$$M = Np^r$$

where $p \nmid N$.

Let $Z = \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$, into which we embed $\mathbb{Z}$ diagonally with dense image. We have a natural projection $\pi : Z \to \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/Np^r\mathbb{Z}$. Let first $f \in S$ be of weight k. Hida defines for $z = (z_p, z_0) \in Z$

$$[z]f = z_p^k \langle \pi(z) \rangle f$$

where $\langle \cdot \rangle$ is the diamond operator. We recall that the diamond operator $\langle d \rangle$ for $d \in \mathbb{Z}/Np^r\mathbb{Z}$ is defined as $f_{|_k \sigma_d}$ with $\sigma_d \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma_d \equiv \left(\begin{smallmatrix} d^{-1} & * \\ 0 & d \end{smallmatrix} \right) (\mathrm{mod}\ Np^r)$. Since the diamond operator is multiplicative (it gives a group action of $\mathbb{Z}/Np^r\mathbb{Z}^\times$), so is the stroke operator.

We now show that for $z \in \mathbb{Z}$ the definition of $[z]$ can be made so as not to involve the weight. Let $\ell \nmid Np$ be a prime. Due to the well-known equality

$$\ell^{k-1} \langle \ell \rangle = T_\ell^2 - T_{\ell^2}$$

(cf., for instance, [6, p. 53]), one obtains

$$[\ell] = \ell^k \langle \ell \rangle = \ell(T_\ell^2 - T_{\ell^2}).$$

This first of all implies that $[\ell] \in \mathbb{T}_\mathbb{Z}(S)$, since the right-hand side clearly makes sense on S and is an element of $\mathbb{T}_\mathbb{Z}(S)$. Due to multiplicativity, all $[n]$ lie in $\mathbb{T}_\mathbb{Z}(S)$ for $n \in \mathbb{Z}$. Consequently, $[n]$ acts on $S(A)$ for any ring A by its action via $\mathbb{T}_\mathbb{Z}(S)$. Moreover, if $f \in S(A)$ is an eigenform for all T_n ($n \in \mathbb{N}$), then it is also an eigenfunction for all $[n]$. Strictly speaking it is not necessary for our purposes, but, nevertheless we mention that one can extend the stroke operator to a group action of Z on $S(\mathcal{O})$ for all complete $\mathbb{Z}_p$-algebras $\mathcal{O}$ by continuity (which one must check). Thus, if $f \in S(\mathcal{O})$ is an eigenfunction for all Hecke operators, then it is in particular an eigenfunction for all $[z]$ for $z \in Z$, whence sending $[z]$ to its eigenvalue on f gives rise to a character $\theta : Z \to \mathcal{O}^\times$, which we may also factor as $\theta = \eta\psi$ with $\psi : \mathbb{Z}/N\mathbb{Z}^\times \to \mathcal{O}^\times$ and $\eta : \mathbb{Z}_p^\times \to \mathcal{O}^\times$.

Since it is the starting point and the fundamental input to the sequel, we recall the existence theorem on p-adic Galois representations attached to normalized Hecke eigenforms for $k = 2$ by Shimura, for $k > 2$ by Deligne and for $k = 1$ by Deligne and Serre (see, e.g., [6, p. 120]). By Frob_ℓ we always mean an arithmetic Frobenius element at ℓ.

Theorem 17. *Suppose that $S = S_k(\Gamma_1(Np^r))$ with $k \geq 1$. Suppose $f \in S(\overline{\mathbb{Q}}_p)$ is a normalized eigenform (say, it is an eigenform away from D), so that $\langle \ell \rangle f = \chi(\ell)f$ for a character $\chi : (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ for primes $\ell \nmid DNp$.*

Then there is a continuous odd Galois representation

$$\rho = \rho_{f,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$$

that is unramified outside Np and satisfies

$$\mathrm{tr}(\rho(\mathrm{Frob}_\ell)) = f(T_\ell) \quad and \quad \det(\rho(\mathrm{Frob}_\ell)) = \ell^{k-1}\chi(\ell)$$

for all primes $\ell \nmid DNp$.

Corollary 18. *Suppose that $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(Np^r))$. Suppose $f \in S(\overline{\mathbb{Q}}_p)$ is a normalized eigenform (say, it is an eigenform away from D), so that $[\ell]f = \eta(\ell)\psi(\ell)f$ for some characters $\psi : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \overline{\mathbb{Q}}_p^{\times}$ and $\eta : \mathbb{Z}_p^{\times} \to \overline{\mathbb{Q}}_p^{\times}$ for primes $\ell \nmid DNp$.*

Then there is a continuous Galois representation

$$\rho = \rho_{f,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$$

that is unramified outside Np and satisfies

$$\mathrm{tr}(\rho(\mathrm{Frob}_\ell)) = f(T_\ell) \quad and \quad \det(\rho(\mathrm{Frob}_\ell)) = f(\ell^{-1}[\ell]) = \ell^{-1}\eta(\ell)\psi(\ell)$$

for all primes $\ell \nmid DNp$.

Proof. From Lemma 15 we know that f has a unique weight k, i.e. lies in some $S_k(\Gamma_1(Np^r))(\overline{\mathbb{Q}}_p)$. Thus, f also gives rise to a character $\chi : \mathbb{Z}/Np^r\mathbb{Z}^{\times} \to \overline{\mathbb{Q}}_p^{\times}$ by sending the diamond operator $\langle \ell \rangle$ to its eigenvalue on f. The assertion now follows from the equation $\ell^k \langle \ell \rangle = [\ell]$ and Theorem 17. $\qquad\square$

Corollary 19. *Suppose that $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(Np^r))$. Suppose $\bar{f} \in S(\overline{\mathbb{F}}_p)$ is a normalized eigenform (say, it is an eigenform away from D), so that $[\ell]\bar{f} = \eta(\ell)\psi(\ell)\bar{f}$ for some characters $\psi : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \overline{\mathbb{F}}_p^{\times}$ and $\eta : \mathbb{Z}_p^{\times} \to \overline{\mathbb{F}}_p^{\times}$ for primes $\ell \nmid DNp$.*

Then there is a semisimple continuous Galois representation

$$\rho = \rho_{\bar{f},p,1} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

that is unramified outside Np and satisfies

$$\mathrm{tr}(\rho(\mathrm{Frob}_\ell)) = \bar{f}(T_\ell) \quad and \quad \det(\rho(\mathrm{Frob}_\ell)) = \ell^{-1}\eta(\ell)\psi(\ell)$$

for all primes $\ell \nmid DNp$.

Proof. By Lemma 16, there is an eigenform $f \in S(\overline{\mathbb{Z}}_p)$ whose reduction is $\bar{f}$, whence by Corollary 18 there is an attached Galois representation $\rho_{f,p}$. Due to the compactness of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the continuity, there is a finite extension $K/\mathbb{Q}_p$ such that the representation is isomorphic to one of the form $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_K)$. We define $\rho_{\bar{f},p,1}$ as the semisimplification of the reduction of this representation modulo the maximal ideal of $\mathcal{O}_K$. It inherits the assertions on the characteristic polynomial at Frob_ℓ from $\rho_{f,p}$. $\qquad\square$

Next we construct a Galois representation into the completed Hecke algebra.

Theorem 20. *Suppose that $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(Np^r))$.*

Let D be a positive integer and let $\mathfrak{m}$ be a maximal ideal of $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S) := \mathbb{T}_{\mathbb{Z}}^{(D)}(S) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and denote by $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}}$ the completion of $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)$ at $\mathfrak{m}$. Assume that the residual Galois representation attached to

$$\mathbb{T}_{\mathbb{Z}}^{(D)}(S) \hookrightarrow \hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S) \to \hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}} \to \hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)/\mathfrak{m} \hookrightarrow \overline{\mathbb{F}}_p$$

is absolutely irreducible (*note that this ring homomorphism can be extended to a normalized eigenform in $S(\overline{\mathbb{F}}_p)$ by the argument using "going up" from the proof of Lemma* 15).

Then there is a continuous representation

$$\rho = \rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}}),$$

that is unramified outside Np and satisfies

$$\mathrm{tr}(\rho(\mathrm{Frob}_\ell)) = T_\ell \quad and \quad \det(\rho(\mathrm{Frob}_\ell)) = \ell^{-1}[\ell]$$

for all primes $\ell \nmid DNp$.

Proof. Assume first that all prime divisors of Np also divide D. As the Hecke operators T_n with n coprime to D commute with each other and are diagonalizable (as elements of $\mathrm{End}_{\mathbb{C}}(S)$), there is a $\mathbb{C}$-basis Ω for S consisting of eigenforms for $\mathbb{T}_{\mathbb{Z}}^{(D)}(S)$. As $\mathbb{T}_{\mathbb{Z}}^{(D)}(S)$ is finite over $\mathbb{Z}$, for each $f \in \Omega$, its image onto $\mathbb{T}_{\mathbb{Z}}^{(D)}(\mathbb{C}f)$ is an order in a number field. Here, obviously $\mathbb{T}_{\mathbb{Z}}^{(D)}(\mathbb{C}f)$ denotes the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(\mathbb{C}f)$ generated by the T_n with $(n, D) = 1$.

Consider the natural map $\mathbb{T}_{\mathbb{Z}}^{(D)}(S) \to \prod_{f \in \Omega} \mathbb{T}_{\mathbb{Z}}^{(D)}(\mathbb{C}f)$, which is an injective homomorphism because Ω is a $\mathbb{C}$-basis for S. Letting $R = \mathbb{T}_{\mathbb{Z}}^{(D)}(S) \otimes \mathbb{Q}$, we see that $\prod_{f \in \Omega} \mathbb{T}_{\mathbb{Z}}^{(D)}(\mathbb{C}f) \otimes \mathbb{Q}$ is a semisimple R-module, as each $\mathbb{T}_{\mathbb{Z}}^{(D)}(\mathbb{C}f) \otimes \mathbb{Q}$ is a simple R-module. Thus, the R-submodule $R \subset \prod_{f \in \Omega} \mathbb{T}_{\mathbb{Z}}^{(D)}(\mathbb{C}f) \otimes \mathbb{Q}$ is also a semisimple R-module, and $R = \mathbb{T}_{\mathbb{Z}}^{(D)}(S) \otimes \mathbb{Q}$ is a semisimple ring. It follows that $\mathbb{T}_{\mathbb{Z}}^{(D)}(S) \otimes \mathbb{Q} \cong \prod_i F_i$, where the F_i are a finite collection of number fields. This means that $\mathbb{T}_{\mathbb{Z}}^{(D)}(S) \otimes \mathbb{Q}_p \cong \prod_i K_i$ with the K_i a finite collection of finite extensions of $\mathbb{Q}_p$.

Thus, there is an injective homomorphism $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S) \hookrightarrow \prod_i \mathcal{O}_i$, where $\mathcal{O}_i$ is the ring of integers of K_i. Hence, there is an injective homomorphism $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}} \hookrightarrow \prod_i \mathcal{O}_i$, which is obtained from the previous one by discarding factors where $\mathfrak{m}$ is not sent into the maximal ideal of $\mathcal{O}_i$. Each projection $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}} \to \mathcal{O}_i$ is a map of local rings.

Each ring homomorphism $g_i : \mathbb{T}_{\mathbb{Z}}^{(D)}(S) \to K_i$ lifts to a ring homomorphism $f_i : \mathbb{T}_{\mathbb{Z}}(S) \to E_i$, where E_i is a finite extension of K_i. By Corollary 18, for each i, there is a continuous Galois representation $\rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}'_i)$, where $\mathcal{O}'_i$ is the ring of integers of E_i.

Let $\rho = \prod_i \rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \prod_i \mathrm{GL}_2(\mathcal{O}'_i) = \mathrm{GL}_2(\prod_i \mathcal{O}'_i)$ be the product representation. Under the inclusion $\mathbb{T}_{\mathbb{Z}}^{(D)}(S) \hookrightarrow \prod_i \mathcal{O}'_i$, we see for $\ell \nmid DNp$, that $\mathrm{tr}\,\rho(\mathrm{Frob}_\ell) = T_\ell$ and $\det \rho(\mathrm{Frob}_\ell) = \ell^{-1}[\ell]$. The residual Galois representations $\overline{\rho}_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(k'_i)$, where k'_i is the residue field of $\mathcal{O}'_i$, are all isomorphic to the Galois representation attached to $\mathbb{T}_{\mathbb{Z}}^{(D)}(S) \to \hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)/\mathfrak{m}$, and hence are absolutely irreducible.

We will now apply [2, Théorème 2], the setting of which is as follows. Suppose that A is a local Henselian ring with maximal ideal $\mathfrak{m}$ and residue field $F = A/\mathfrak{m}$. Assume that the Brauer group of F vanishes (this will be the case if F is finite).

Let A' be a semilocal extension of A: $A' = \prod_i A'_i$ with the A'_i local rings with maximal ideals $\mathfrak{m}_i$ and residue fields $F'_i = A'_i/\mathfrak{m}_i$ that are extensions of F. Suppose that we are given an A-algebra R and a representation $\rho' = \prod_i \rho'_i : R \otimes_A A' \to M_n(A') = \prod_i M_n(A'_i)$. Suppose further that $\operatorname{tr} \rho'(r \otimes 1) \in A$ for all $r \in R$, and that the attached residual representations $\bar{\rho}'_i : R \otimes_A F'_i \to M_n(F'_i)$ are all absolutely irreducible. The conclusion of [2, Théorème 2] is then that ρ' is (equivalent to) the base change from A to A' of a representation $\rho : R \to M_n(A)$.

We see that we can apply [2, Théorème 2] with $A = \hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}}$ (which is a complete local ring, hence Henselian), and $A' = \prod_i \mathcal{O}'_i$ (which is a semilocal extension of A), to deduce that the representation ρ descends to a continuous Galois representation

$$\rho_{\mathfrak{m}} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}}),$$

as claimed.

For the general case, when D is not divisible by all prime divisors of Np, one first applies the above with $D' := DNp$ and the maximal ideal $\mathfrak{m}'$ of $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D')}$ given as $\mathfrak{m} \cap \hat{\mathbb{T}}_{\mathbb{Z}}^{(D')}$ to obtain $\rho_{\mathfrak{m}'} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\hat{\mathbb{T}}_{\mathbb{Z}}^{(D')}(S)_{\mathfrak{m}'})$, which can finally be composed with the natural map $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D')}(S)_{\mathfrak{m}'} \to \hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}}$.   □

Corollary 21. *Suppose that $S = \bigoplus_{k=1}^b S_k(\Gamma_1(Np^r))$. Let A be a complete local ring with maximal ideal $\mathfrak{p}$ of residue characteristic p. Suppose $f \in S(A)$ is a normalized eigenform (say, it is an eigenform away from D), so that $[\ell]f = \eta(\ell)\psi(\ell)f$ for some characters $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to A^\times$ and $\eta : \mathbb{Z}_p^\times \to A^\times$, for all $\ell \nmid DNp$.*

Assume the Galois representation attached to the reduction $\bar{f} : \mathbb{T}_{\mathbb{Z}}(S) \to A \to A/\mathfrak{p} \pmod{\mathfrak{p}}$ of f, which defines a normalized eigenform in $S(\overline{\mathbb{F}}_p)$, is absolutely irreducible (cf. Corollary 19).

Then there is a continuous Galois representation

$$\rho = \rho_{f,p} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(A)$$

that is unramified outside Np and satisfies

$$\operatorname{tr}(\rho(\operatorname{Frob}_\ell)) = f(T_\ell) \quad \text{and} \quad \det(\rho(\operatorname{Frob}_\ell)) = \ell^{-1}\eta(\ell)\psi(\ell)$$

for all primes $\ell \nmid DNp$.

Proof. Since $S(A)$ is a normalized eigenform, $f : \mathbb{T}_{\mathbb{Z}}^{(D)}(S) \to A$ is a ring homomorphism, which factors through $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}}$ for some maximal ideal $\mathfrak{m}$, since A is complete and local. (The ideal $\mathfrak{m}$ can be seen as the kernel of $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S) \to A \twoheadrightarrow A/\mathfrak{p}$.) We thus have a ring homomorphism $\hat{\mathbb{T}}_{\mathbb{Z}}^{(D)}(S)_{\mathfrak{m}} \to A$. Composing this with the Galois representation $\rho_{\mathfrak{m}}$ from Theorem 20 yields the desired Galois representation $\rho_{f,p}$.
    □

For our applications, the most important case of Corollary 21 is when $A = \overline{\mathbb{Z}/p^m\mathbb{Z}}$. Note also that one can attach a Galois representation by the above corollary to any ring homomorphism $\mathbb{T}_{\mathbb{Z}}^{(D)}(S) \to A$.

Proof of Theorem 3. It suffices to apply Corollary 21 with $A = \overline{\mathbb{Z}/p^m\mathbb{Z}}$. □

4. Stripping Powers of p from the Level

In this section, we use results of Katz and Hida in order to remove powers of p from the level of cusp forms over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$, at the expense of using divided congruences.

Let M be any positive integer. Let $\mathcal{O}$ be the ring of integers of either a number field or a finite extension of $\mathbb{Q}_p$. Define

$$\mathbb{S}(\Gamma_1(M))(\mathcal{O}) := \varinjlim_{b \geq 1} S^b(\Gamma_1(M))(\mathcal{O}).$$

Specializing $\mathcal{O}$ to $\mathbb{Z}_p$, we complete these spaces, which are of infinite rank, and put

$$\bar{\mathbb{S}}(\Gamma_1(M); \mathbb{Z}_p) := \varprojlim_{m \geq 1} \mathbb{S}(\Gamma_1(M))(\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p^m\mathbb{Z}_p$$

$$\cong \varprojlim_{m \geq 1} \mathbb{S}(\Gamma_1(M))(\mathbb{Z}_p/p^m\mathbb{Z}_p)$$

$$\cong \varprojlim_{m \geq 1} \mathbb{S}(\Gamma_1(M))(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/p^m\mathbb{Z}.$$

For the isomorphisms, we use that the direct limit is exact on modules and

$$S^b(\Gamma_1(M))(\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p^m\mathbb{Z}_p \cong S^b(\Gamma_1(M))(\mathbb{Z}_p/p^m\mathbb{Z}_p)$$

$$\cong S^b(\Gamma_1(M))(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/p^m\mathbb{Z}, \tag{1}$$

which is an application of Lemma 13.

Theorem 22 (Hida). *Assume $p \geq 5$. Let N be a positive integer prime to p and let $r \in \mathbb{N}$.*

Under the q-expansion map, the images of $\bar{\mathbb{S}}(\Gamma_1(N); \mathbb{Z}_p)$ and $\bar{\mathbb{S}}(\Gamma_1(Np^r); \mathbb{Z}_p)$ agree inside $\mathbb{Z}_p[[q]]$.

Proof. This result is stated in [10, (1.3)]. (For the sake of completeness, let us point out that Hida's spaces $\bar{\mathbb{S}}$ result from completing with respect to a natural norm $|f|_p$ whereas our $\bar{\mathbb{S}}$ arise as projective limits. However, it is easy to see that the two points of view are equivalent. Also, the spaces of modular forms that both we and Hida are working with are spaces of "classical forms", cf. Sec. 2.) □

Proposition 23. *Assume $p \geq 5$. Let K be a number field and $\mathcal{O}$ be its ring of integers. Let N be a positive integer prime to p and $r \in \mathbb{N}$. Let $f \in \mathbb{S}(\Gamma_1(Np^r); \mathcal{O})$.*

Then for all $m \in \mathbb{N}$, there are $b_m \geq 1$ and $g_m \in S^{b_m}(\Gamma_1(N))(\mathcal{O}) \hookrightarrow \mathbb{S}(\Gamma_1(N))(\mathcal{O})$ such that $f(q) \equiv g_m(q) \pmod{p^m}$.

Proof. There is a $b \geq 1$ such that $f \in S^b(\Gamma_1(Np^r))(\mathcal{O})$. Since $S^b(\Gamma_1(Np^r))(\mathcal{O}) = S^b(\Gamma_1(Np^r))(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathcal{O}$ by Lemma 13, there are $f_i \in S^b(\Gamma_1(Np^r))(\mathbb{Z})$ and $a_i \in \mathcal{O}$ for $i = 1, \ldots, t$ such that $f = \sum_{i=1}^{t} a_i f_i$.

There is a $b_m \geq 1$ such that the images of f_i under the composition of maps

$$S^b(\Gamma_1(Np^r))(\mathbb{Z}) \hookrightarrow \mathbb{S}(\Gamma_1(Np^r))(\mathbb{Z}) \hookrightarrow \bar{\mathbb{S}}(\Gamma_1(Np^r); \mathbb{Z}_p) \xrightarrow{\sim \text{Theorem 22}} \bar{\mathbb{S}}(\Gamma_1(N); \mathbb{Z}_p)$$

$$\rightarrow \bar{\mathbb{S}}(\Gamma_1(N); \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{S}(\Gamma_1(N))(\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p^m\mathbb{Z}_p$$

all lie in $S^{b_m}(\Gamma_1(N))(\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p^m\mathbb{Z}_p \cong S^{b_m}(\Gamma_1(N))(\mathbb{Z}) \otimes \mathbb{Z}/p^m\mathbb{Z}$. Hence, there are $g_{i,m} \in S^{b_m}(\Gamma_1(N))(\mathbb{Z})$ such that $f_i(q) \equiv g_{i,m}(q) \pmod{p^m}$. Finally, $g_m := \sum_{i=1}^{t} a_i g_{i,m} \in S^{b_m}(\Gamma_1(N))(\mathcal{O})$ is such that $f(q) \equiv g_m(q) \pmod{p^m}$. $\square$

Proof of Proposition 2. By virtue of Lemma 14, we can lift f to an element of $S^b(\Gamma_1(Np^r))(\mathcal{O}_K)$ for some number field K. Hence, Proposition 23 applies, yielding a form g_m, whose reduction mod p^m satisfies the requirements. $\square$

5. On the Relationships Between Strong, Weak, and DC-Weak

In this section we make a number of remarks concerning the notions of a mod p^m Galois representation arising "strongly", "weakly", and "dc-weakly" from $\Gamma_1(M)$, and the accompanying notions of "strong", "weak", and "dc-weak" eigenforms. Notice that Lemma 16 above implies that these are equivalent notions when $m = 1$. We show here that the three notions are not equivalent in general (for fixed level M), but must leave as an open question to classify the conditions under which the three notions coincide.

We also give a few illustrative examples at the end of the section.

5.1. *Nebentypus obstructions*

We show here that in order to strip powers of p from the level of a Galois representation which is strongly modular, it is necessary in general to consider the Galois representations attached to dc-weak eigenforms. The argument uses certain nebentypus obstructions that also — in general — prohibit "weak" eigenforms of level prime-to-p from coinciding with "dc-weak" eigenforms. The argument can also be seen as a demonstration of the fact that the nebentypus restriction in Hatada's theorem (Theorem 6) are in fact necessary.

Assume $p \nmid N$ and let $f_0 \in S_k(\Gamma_1(Np^r))(\overline{\mathbb{Z}/p^m\mathbb{Z}})$ be a strong eigenform. A consequence of Theorem 5 is that the Galois representation $\rho_{f_0,p,m}$ dc-weakly arises from $\Gamma_1(N)$. We show that $\rho_{f_0,p,m}$ does not, in general, weakly arise from $\Gamma_1(N)$.

By the definition of "strong eigenform" there is $f \in S_k(\Gamma_1(Np^r))(\overline{\mathbb{Z}}_p)$ that is normalized and an eigenform outside some positive integer D and that reduces to f_0. Suppose that $\langle \ell \rangle f = \chi(\ell) f$ for primes ℓ with $\ell \nmid DNp$, with a character χ that we decompose as $\chi = \psi \omega^i \eta$ where ψ is a character of conductor dividing N, ω is the Teichmüller lift of the mod p cyclotomic character, and η is a character of conductor dividing p^r and order a power of p. Assume p is odd, $r \geq 2$, $\eta \neq 1$, and $m \geq 2$. Let $\rho_{f,p,m}$ be the mod p^m representation attached to f. Then $\rho_{f,p,m} \cong \rho_{f_0,p,m}$. By the argument below, it is not possible to find a weak eigenform $g \in S_{k'}(\Gamma_1(N))(\overline{\mathbb{Z}/p^m\mathbb{Z}})$ of any weight k' such that $\rho_{g,p,m} \cong \rho_{f,p,m}$.

Let η have order p^s where $1 \leq s \leq r - 1$. Then we may regard η as a character $\eta : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Z}_p[\zeta]^\times$, where ζ is a primitive p^sth root of unity. Assume there exists a weak eigenform g on $\Gamma_1(N)$ such that $\rho_{f,p,m} \cong \rho_{g,p,m}$. As g is an eigenform for $\langle \ell \rangle$ for primes ℓ with $\ell \nmid DNp$, we have that $\langle \ell \rangle g = \psi'(\ell)g$, where

$$\psi' : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Z}/p^m\mathbb{Z}}^\times$$

is a mod p^m character of conductor dividing N. Since $\rho_{f,p,m} \cong \rho_{g,p,m}$, we have that $\det \rho_{g,p,m} = \det \rho_{f,p,m}$. Now, we know that

$$\det \rho_{f,p,m} \equiv \epsilon^{k-1}\psi\omega^i\eta \pmod{p^m},$$

with ϵ the p-adic cyclotomic character. Also, from the construction of the Galois representation attached to g (cf. [2, Théorème 3]), we have that

$$\det \rho_{g,p,m} \equiv \epsilon^{k'-1}\psi' \pmod{p^m}.$$

Hence, after restricting to the inertia group at p, we have that

$$\epsilon^{k'-1} \equiv \eta\epsilon^{k-1} \pmod{p^m}$$

as characters of $\mathbb{Z}_p^\times$, or equivalently $\eta \equiv \epsilon^{k'-k} \pmod{p^m}$.

The cyclotomic character $\epsilon(x) = x$ has values in $\mathbb{Z}_p$, however the image of the character η in $\mathbb{Z}_p[\zeta]$ contains ζ. Since $m \geq 2$, the injection

$$\mathbb{Z}_p/(p^m) \hookrightarrow \mathbb{Z}_p[\zeta]/(1-\zeta)^{(m-1)p^{s-1}(p-1)+1}$$

is not a surjection. Thus, the reduction $\pmod{p^m}$ of $\epsilon^{k'-k}$ has values in $\mathbb{Z}_p/(p^m)$, but the reduction $\pmod{p^m}$ of η does not. This contradicts the equality $\eta \equiv \epsilon^{k'-k} \pmod{p^m}$.

Note for $m = 1$, we always have $\eta \equiv 1 \pmod{p}$ and hence it is possible to have the equality of characters in this situation.

Although the main purpose of this section is to show that there exist $\rho_{f,p,m}$ which arise strongly from $\Gamma_1(Np^r)$ and do not arise weakly from $\Gamma_1(N)$, we note the proof shows there exist dc-weak eigenforms of level N which are not weak eigenforms of level N.

5.2. *On the weights in divided congruences*

In this subsection we show that under *certain* conditions, the weights occurring in a dc-weak eigenform satisfy enough congruence conditions so that one can equalize them using suitable powers of Eisenstein series, a technique which was used in [3]. In fact, Corollary 26 below is a generalization of some of the results in [3], using different methods. We impose here that $p > 2$.

Lemma 24. *Let $\mathcal{O}$ be a local ring with maximal ideal $\mathfrak{p}$, and let M be a finite projective $\mathcal{O}$-module. If $\bar{f}_1, \ldots, \bar{f}_n \in M/\mathfrak{p}M$ are linearly independent over $\mathcal{O}/\mathfrak{p}$, then $f_1, \ldots, f_n \in M/\mathfrak{p}^m M$ are linearly independent over $\mathcal{O}/\mathfrak{p}^m$.*

Proof. By [13, Chapter X, Theorem 4.4], we have that M is isomorphic to $F \oplus \bigoplus_{i=1}^{n} \mathcal{O}f_i$ with F a free $\mathcal{O}$-module, from which the assertion immediately follows. □

Proposition 25. *Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Let $f_i \in S_{k_i}(\Gamma_1(Np^r))(\mathcal{O})$ for $i = 1, \ldots, t$, where the k_i are distinct, and suppose $[\ell]f_i = \ell^{k_i}\psi_i(\ell)\eta_i(\ell)f_i$, for $\ell \nmid DNp$ (for some positive integer D), where $\psi_i : \mathbb{Z}/N\mathbb{Z}^\times \to \mathcal{O}^\times$, $\eta_i : \mathbb{Z}/p^r\mathbb{Z}^\times \to \mathcal{O}^\times$ have finite order. Suppose also that the q-expansions $f_i(q)$ (mod p) are linearly independent over $\overline{\mathbb{Z}/p\mathbb{Z}} = \overline{\mathbb{F}}_p$.*

Put $f := \sum_{i=1}^{t} f_i$ and assume that f is an eigenform for the operators $[\ell]$ (e.g. this is the case if f is a dc-weak eigenform).

Then $k_1 \equiv k_2 \equiv \cdots \equiv k_t \pmod{\varphi(p^m)/h}$, where φ is the Euler-φ-function, and h is the least common multiple of the orders of the η_i (mod p^m).

Proof. Denote by λ and λ_i the $[\ell]$-eigenvalue of f and the f_i, respectively. Then we have $\lambda f \equiv \sum_{i=1}^{t} \lambda_i f_i(q) \pmod{p^m}$, whence $\sum_{i=1}^{t}(\lambda - \lambda_i)f_i(q) \equiv 0 \pmod{p^m}$. Lemma 24 applied with $M = \mathcal{O}[[q]]/(q^L)$ for suitable L large enough (for instance, take L so that the q-expansion map $\bigoplus_{i=1}^{t} S_{k_i}(\Gamma_1(Np^r))(\mathcal{O}) \to \mathcal{O}[[q]]/(q^L)$ is injective) shows that $\lambda \equiv \lambda_i \pmod{p^m}$ for all i. In particular, we have $\lambda_i \equiv \lambda_j \pmod{p^m}$ for all i, j.

We have $\lambda_i = \ell^{k_i}\psi_i(\ell)\eta_i(\ell)$. If $\ell \equiv 1 \pmod{N}$ then $\psi_i(\ell) = 1$. For such ℓ we thus have

$$\ell^{k_i h} = \lambda_i^h \equiv \lambda_j^h = \ell^{k_j h} \pmod{p^m}$$

for all i, j, by the definition of h.

By Chebotarev's density theorem, we can choose ℓ so that in addition to the property $\ell \equiv 1 \pmod{N}$, we have that ℓ is a generator of $(\mathbb{Z}/p^m\mathbb{Z})^\times$ (here we use that p is odd and that $p \nmid N$.) It then follows that $k_1 h \equiv k_2 h \equiv \cdots \equiv k_t h \pmod{\varphi(p^m)}$ as desired. □

The proposition has the following application. Suppose that f is a dc-weak eigenform mod p^m at level N of the form $f = \sum_{i=1}^{t} f_i$ with $f_i \in S_{k_i}(\Gamma_1(N))(\mathcal{O})$ for $i = 1, \ldots, t$, where the k_i are distinct. Suppose that each f_i has a nebentypus and that, crucially, the q-expansions $f_i(q)$ (mod p) are linearly independent over $\overline{\mathbb{F}}_p$.

Then the proposition applies with $h = 1$ and shows that we have $k_1 \equiv \cdots \equiv k_t$ (mod $\varphi(p^m)$). Without loss of generality suppose that k_t is the largest of the weights. When $p \geq 5$, we can use, as in [3], the Eisenstein series $E := E_{p-1}$ of weight $p - 1$ and level 1, normalized in the usual way so that its q-expansion is congruent to 1 (mod p). The form $\tilde{E} := E^{p^{m-1}}$ is of weight $\varphi(p^m) = (p-1)p^{m-1}$, level 1, and is congruent to 1 (mod p^m). Due to the congruence on the weights, we may multiply each f_i for $i = 1, \ldots, t-1$ with a suitable power of $\tilde{E}$ so as to make it into a form of weight k_t with the same q-expansion mod p^m. Consequently, in weight k_t and level N there is a form that is congruent to f (mod p^m), i.e. f is in fact a weak eigenform mod p^m at level N.

We also record the following variant of Proposition 25 as it represents a generalization of some of the results of [3].

Corollary 26. *Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Let $f_i \in S_{k_i}(\Gamma_1(Np^r))(\mathcal{O})$ for $i = 1, \ldots, t$ satisfy $f_1(q) + \cdots + f_t(q) \equiv 0 \,(\mathrm{mod}\, p^m)$, where the k_i are distinct, and suppose $[\ell]f_i = \ell^{k_i}\psi_i(\ell)\eta_i(\ell)f_i$, for $\ell \nmid DNp$ (for some positive integer D), where $\psi_i : \mathbb{Z}/N\mathbb{Z}^\times \to \mathcal{O}^\times$, $\eta_i : \mathbb{Z}/p^r\mathbb{Z}^\times \to \mathcal{O}^\times$ have finite order. Suppose for some i, the q-expansions $f_j(q) \,(\mathrm{mod}\, p)$, $j \neq i$ are linearly independent over $\overline{\mathbb{Z}/p\mathbb{Z}} = \overline{\mathbb{F}}_p$.*

Then $k_1 \equiv k_2 \equiv \cdots \equiv k_t \,(\mathrm{mod}\, \varphi(p^m)/h)$, where φ is the Euler-φ-function, and h is the least common multiple of the orders of the $\eta_j \,(\mathrm{mod}\, p^m)$.

Proof. Without loss of generality, assume $i = 1$. As $-f_1(q) \equiv \sum_{i=2}^t f_i \,(\mathrm{mod}\, p^m)$ the proof of Proposition 25 shows that we have

$$\ell^{k_1}\psi_1(\ell)\eta_1(\ell) \equiv \ell^{k_i}\psi_i(\ell)\eta_i(\ell) \pmod{p^m}$$

for $i = 2, \ldots, t$, and the desired congruences then follow in the same way. □

5.3. *Examples*

We do not know whether the notions "strong" and "weak" at a fixed level prime-to-p coincide in general when the weight is allowed to vary. However, the following examples seem to suggest that they do not. It is of obvious interest to resolve this question, perhaps first by looking for a numerical counterexample. (There would be theoretical problems to consider before one could do that, specifically obtaining a weight bound.)

In [17, Sec. 4.2], one has an example mod 9 in weight 2 for $\Gamma_0(71)$. Note: the notion of strong and weak eigenform in [17] is at a single weight, i.e. the weight is also fixed, which differs from our terminology. The example in [17] shows that there is a cusp form in $S_2(\Gamma_0(71))$ which when reduced mod 9 is an eigenform mod 9, and which does not arise from the reduction mod 9 of an eigenform (for all T_n) on $S_2(\Gamma_0(71))$.

As a general mechanism for producing eigenvalues mod p^2 that do not lift to characteristic 0 (at the same weight), consider the following setup: Let p be an odd prime. Suppose $f, g \in M = \mathbb{Z}_p^2$ and $f \equiv g \not\equiv 0 \,(\mathrm{mod}\, pM)$. Suppose that T is an endomorphism of M, that $Tf = \lambda f$, that $Tg = \mu g$, and that $\{f, g\}$ is a basis for $M \otimes \overline{\mathbb{Q}}_p$. Then $\lambda \equiv \mu \,(\mathrm{mod}\, p)$. Suppose further that $\lambda \not\equiv \mu \,(\mathrm{mod}\, p^2)$. Consider $h = f + g$. Then $Th - \frac{\lambda+\mu}{2}h = \lambda f + \mu g - \frac{\lambda+\mu}{2}h = \frac{\lambda-\mu}{2}(f - g)$, so we have $Th \equiv \frac{\lambda+\mu}{2}h$ $(\mathrm{mod}\, p^2M)$. Thus, $\frac{\lambda+\mu}{2} \in \mathbb{Z}_p/p^2\mathbb{Z}_p$ is an eigenvalue which does not lift to $\overline{\mathbb{Z}}_p$ as an eigenvalue of T acting on $M \otimes \overline{\mathbb{Q}}_p$.

Using MAGMA, cf. [1], we found the following concrete example involving modular forms of the same weight. Let S be the free $\mathbb{Z}_3$-module of rank 5 which is obtained from the image of $S_2(\Gamma_0(52))(\mathbb{Z}_3)$ in $\mathbb{Z}_3[[q]]$ under the q-expansion map.

Consider

```
f = q + 2*q^5 - 2*q^7 - 3*q^9 - 2*q^11 - q^13 + 6*q^17 - 6*q^19
    + O(q^20),
```

```
g = q + q^2 - 3*q^3 + q^4 - q^5 - 3*q^6 + q^7 + q^8 + 6*q^9 - q^10
    - 2*q^11 - 3*q^12 - q^13 + q^14 + 3*q^15 + q^16 - 3*q^17
    + 6*q^18 + 6*q^19 + O(q^20)
```

which are the q-expansions, respectively, of newform 1 in $S_2(\Gamma_0(52))$, and newform 2 in $S_2(\Gamma_0(26))$, in MAGMA's internal labeling system.

By [14, Lemma 4.6.5] the series $\sum_{2\nmid n} a_n(g)$ is the q-expansion of an element $\tilde{g}$ of $S_2(\Gamma_0(52))$. Also, $\tilde{g}$ is an eigenform for all the Hecke operators T_n for all $n \geq 1$ (this can be checked from the explicit formulae of T_n acting on q-expansions for n prime).

We have that $\{f, \tilde{g}\}$ is $\overline{\mathbb{Q}}_3$-linearly independent, and that $a_n(f) \equiv a_n(\tilde{g}) \pmod{3}$ for all n (to see that the congruence holds for all n use the Sturm bound, cf. [16, Theorem 1]. The bound is 14 in this case.)

Let $h = \frac{f + \tilde{g}}{2}$ so that

```
h = q - 3/2*q^3 + 1/2*q^5 - 1/2*q^7 + 3/2*q^9 - 2*q^11
    + 3/2*q^15 + 3/2*q^17 + O(q^20).
```

By the arguments above, $(h \bmod 9)$ is a $\mathbb{Z}_3/9\mathbb{Z}_3$-eigenform for the Hecke operators T_n for all $n \geq 1$. Furthermore, the system of eigenvalues for T_n for all $n \geq 1$ does not arise from the reductions mod 9 of f, nor g, as well as g_1, the other newform in $S_2(\Gamma_0(26))$. Thus, we see finally that the system of eigenvalues $\in \mathbb{Z}_3/9\mathbb{Z}_3$ for the T_n for all $n \geq 1$, acting on h, do not lift to $\overline{\mathbb{Z}}_3$ inside $S \otimes \overline{\mathbb{Q}}_3$.

On the other hand, we make the remark that we have attached a mod 9 Galois representation to h by Corollary 21 (note: the residual mod 3 representation is absolutely irreducible).

Acknowledgments

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997) 235–265.

[2] H. Carayol, Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet, in *p-Adic Monodromy and the Birch and Swinnerton–Dyer Conjecture*, Contemporary Mathematics, Vol. 165 (American Mathematical Society, Providence, RI, 1994), pp. 213–237.

[3] I. Chen, I. Kiming and J. B. Rasmussen, On congruences mod $\mathfrak{p}^m$ between eigenforms and their attached Galois representations, *J. Number Theory* **130** (2010) 608–619.

[4] S. R. Dahmen and S. Yazdani, Level lowering modulo prime powers and twisted Fermat equations, *Canad. J. Math.* **64** (2012) 282–300.

[5] P. Deligne and J.-P. Serre, Formes modulaires de poids 1, *Ann. Sci. École Norm. Sup.* (*4*) **7** (1974) 507–530.

[6] F. Diamond and J. Im, Modular forms and modular curves, in *Seminar on Fermat's Last Theorem*, CMS Conference Proceedings, Vol. 17 (American Mathematical Society, Providence, RI, 1995), pp. 39–133.

[7] D. Eisenbud, *Commutative Algebra With a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, Vol. 150 (Springer, 1995).

[8] F. Gouvêa, *Arithmetic of p-Adic Modular Forms*, Lecture Notes in Mathematics, Vol. 1304 (Springer, Berlin, 1988), viii+121 pp.

[9] K. Hatada, On classical and ℓ-adic modular forms of levels $N\ell^m$ and N, *J. Number Theory* **87** (2001) 1–14.

[10] H. Hida, Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, *Invent. Math.* **85** (1986) 545–613.

[11] ———, Iwasawa modules attached to congruences of cusp forms, *Ann. Sci. École Norm. Sup.* (*4*) **19** (1986) 231–273.

[12] N. M. Katz, Higher congruences between modular forms, *Ann. of Math.* (*2*) **101** (1975) 332–367.

[13] S. Lang, *Algebra*, 3rd edn. (Addison-Wesley, 1993).

[14] T. Miyake, *Modular Forms* (Springer, 1989).

[15] K. A. Ribet, Report on mod ℓ representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, in *Motives* (*Seattle, WA, 1991*), Proceedings of Symposia in Pure Mathematics, Vol. 55 (American Mathematical Society, Providence, RI, 1994), pp. 639–676.

[16] J. Sturm, *On the Congruence of Modular Forms*, Lecture Notes in Mathematics, Vol. 1240 (Springer, 1987).

[17] X. Taixés i Ventosa and G. Wiese, Computing congruences of modular forms and Galois representations modulo prime powers, in *Arithmetic, Geometry, Cryptography and Coding Theory 2009*, eds. D. Kohel and R. Rolland, Contemporary Mathematics, Vol. 521 (American Mathematical Society, Providence, RI, 2010), pp. 145–166.