# Topics on modular Galois representations modulo prime powers

Panagiotis Tsaknias and Gabor Wiese

**Abstract** This article surveys modularity, level raising and level lowering questions for two-dimensional representations modulo prime powers of the absolute Galois group of the rational numbers. It contributes some new results and describes algorithms and a database of modular forms orbits and higher congruences.

**Key words:** Modular forms, Galois representations, modularity higher congruences, level raising, level lowering, database
*Subject Classifications*:11F33, 11F80

## 1 Introduction

The Fontaine-Mazur conjecture relates $\ell$-adic 'geometric' Galois representations with objects from geometry. In the 2-dimensional case over $\mathbb{Q}$ much progress has been achieved ([Eme11, Thm.1.2.4(2)] and [Kis09]):

**Theorem 1 (Emerton, Kisin).** *Let $\ell > 2$, let $E/\mathbb{Q}_\ell$ be a finite extension and let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(E)$ be an irreducible, finitely ramified, odd Galois representation which is de Rham at $\ell$ with distinct Hodge-Tate weights. Assume that the residual representation $\overline{\rho}$ satisfies certain local conditions.*

*Then a twist of $\rho$ is attached to some newform.*

In fact, the level and the weight of the newform can be read off from $\rho$.

The picture for mod $\ell$ representations is even more complete: Serre type modularity conjectures relate 2-dimensional Galois representations with $\overline{\mathbb{F}}_\ell$-coefficients with modular forms over $\overline{\mathbb{F}}_\ell$. Serre's original modularity conjecture has been established by Khare and Wintenberger [KW09]:

Université du Luxembourg, Unité de Recherche en Mathématiques, Maison du nombre, 6, avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg; e-mail: p.tsaknias@gmail.com, e-mail: gabor.wiese@uni.lu

**Theorem 2 (Khare, Wintenberger, Kisin).** *Let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd irreducible Galois representation. Then $\overline{\rho}$ is attached to (the reduction of) some newform.*

Also in this case, the level and the weight of one of the (infinitely many) newforms attached to $\overline{\rho}$ can be read off from $\overline{\rho}$: the level is the prime-to-$\ell$ Artin conductor, and there is a formula for the weight given by Serre. In fact, it had been known for a long time that if $\overline{\rho}$ is attached to *some* newform then it also is to one with a certain predicted weight and level. Since the predicted weight and level are minimal (except for two cases in the weight, see [Edi92]), the process of finding a newform with predicted invariants is called *level lowering* or *weight lowering*. The quest for attached newforms with non-minimal levels is accordingly called *level raising*. These three questions have been completely solved (with a tiny exception when $\ell = 2$ and the minimal weight 1 is concerned).

With the $\ell$-adic and the mod $\ell$ cases of irreducible odd 2-dimensional representations of $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ essentially settled, it is natural to wonder what happens in between, i.e. modulo prime powers. Quite some research has been done, but the picture is far from clear. In fact, very basic questions are still open.

## Modularity modulo prime powers

Let us consider a representation (continuous like all representations in this paper)

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

with $\mathscr{O}$ the valuation ring of a finite extension of $\mathbb{Q}_\ell$ and $\lambda$ its valuation ideal. It turns out that the *modularity* of $\rho$ follows from known results if one supposes that the residual representation $\overline{\rho}$ is absolutely irreducible and odd and satisfies certain technical local conditions. This was surely known to many experts and had been, for instance, discussed on mathoverflow. We make this precise in Section 2.

An important point here is that one needs to use the right notion of *modularity*. This difficulty is not visible when only working $\ell$-adically or modulo $\ell$. The second author together with Chen and Kiming introduced in [CKW13] three notions of modularity modulo prime powers: *strong modularity*, *weak modularity*, *dc-weak modularity*. These three notions stem from three notions of Hecke eigenforms modulo prime powers, also called *strong*, *weak*, and *dc-weak*, which we briefly explain now.

Throughout this article, we understand by a *Hecke eigenform* $f$ with coefficients in a ring $R$ (they are all normalised and almost all cuspidal without this being said explicitly) a ring homomorphism $f : \mathbb{T} \to R$, where $\mathbb{T}$ is a Hecke algebra (to be specified very soon). We often think of $f$ as the $q$-expansion $\sum_{n\geq 1} f(T_n)q^n \in R[[q]]$. Let $\mathbb{T}_k(\Gamma)$ be the full Hecke algebra, generated as a ring by all Hecke operators $T_n$, acting faithfully on the space of holomorphic cusp forms $S_k(\Gamma)$ of weight $k$ and level $\Gamma$.

A *weak* Hecke eigenform of weight $k$ and level $\Gamma$ with coefficients in $R$ is a ring homomorphism $f : \mathbb{T}_k(\Gamma) \to R$. It is called *strong* if there exists an order $\mathscr{O}$ in a number field together with a ring homomorphism $\pi : \mathscr{O} \to R$ such that $f$ factors as $\mathbb{T}_k(\Gamma) \to \mathscr{O} \xrightarrow{\pi} R$. By embedding the order $\mathscr{O}$ into $\mathbb{C}$, the first arrow leads to $\mathbb{T}_k(\Gamma) \to \mathbb{C}$, a holomorphic Hecke eigenform. In simple terms, strong Hecke eigenforms with coefficients in $R$ are those that are obtained by applying $\pi$ to the coefficients of a holomorphic eigenform.

Put $S_{\leq b}(\Gamma) = \bigoplus_{k=1}^{b} S_k(\Gamma)$ and let $\mathbb{T}_{\leq b}(\Gamma)$ be the full Hecke algebra acting faithfully on it. A ring homomorphism $f : \mathbb{T}_{\leq b}(\Gamma) \to R$ is called a *dc-weak eigenform* of level $\Gamma$ (and weights $\leq b$; in fact, $b$ will not play any role as long as it is large enough). A dc-weak eigenform can hence have contributions from many different weights, as is the case for divided congruences, which is what the abbreviation 'dc' stands for. If $R$ is a finite field or $\overline{\mathbb{F}}_\ell$, all three notions coincide by the Deligne-Serre lifting lemma (for a presentation in the setup used here, see [CKW13, Lemma 16]), but they are different in general. An example that strong is stronger than weak modulo $\ell^m$ for $m > 1$, even if one allows the weight to change (but not the level), is given in [KRW16, §2.5].

As rings of coefficients $R$, we take in this article rings of the form $\mathscr{O}/\lambda^m$ where $\mathscr{O}$ is the valuation ring of a finite field extension of $\mathbb{Q}_\ell$, $\lambda$ is its valuation ideal and $m$ a positive integer. Many results can be and are phrased in this way. However, a general difficulty exists: we often need to compare two eigenforms, one with coefficients in $\mathscr{O}_1/\lambda_1^{m_1}$, the other one with coefficients in $\mathscr{O}_2/\lambda_2^{m_2}$. One then needs to find a ring containing both. In order for such a ring to exist, it is necessary that $\lambda_i^{m_i} \cap \mathbb{Z}_\ell$ for $i = 1, 2$ both yield the same power of $\ell$, say $\ell^m$. This led the second author together with Taixés i Ventosa [TiVW10] to introduce the ring

$$\overline{\mathbb{Z}/\ell^m\mathbb{Z}} = \overline{\mathbb{Z}}_\ell/\{x \in \overline{\mathbb{Z}}_\ell \mid v(x) > m-1\},$$

where $v$ denotes the normalised valuation, i.e. $v(\ell) = 1$. We always consider $\overline{\mathbb{Z}/\ell^m\mathbb{Z}}$ with the discrete topology. We have $\overline{\mathbb{Z}/\ell\mathbb{Z}} = \overline{\mathbb{F}}_\ell$ and for the valuation ring $\mathscr{O}$ of any finite extension of $\mathbb{Q}_\ell$ with absolute ramification index $e$ and valuation ideal $\lambda$, the quotient $\mathscr{O}/\lambda^{e(m-1)+1}$ injects into $\overline{\mathbb{Z}/\ell^m\mathbb{Z}}$. This quotient is the smallest one that extends $\mathbb{Z}/\ell^m\mathbb{Z}$. The ring $\overline{\mathbb{Z}/\ell^m\mathbb{Z}}$ is a local $\mathbb{Z}/\ell^m\mathbb{Z}$-algebra of Krull dimension 0 with residue field $\overline{\mathbb{F}}_\ell$ and the ring extension $\mathbb{Z}/\ell^m\mathbb{Z} \subseteq \overline{\mathbb{Z}/\ell^m\mathbb{Z}}$ is integral. Any finitely generated subring $R$ of $\overline{\mathbb{Z}/\ell^m\mathbb{Z}}$ is contained in some ring $\mathscr{O}/\lambda^{e(m-1)+1}$ as above. These are free as $\mathbb{Z}/\ell^m\mathbb{Z}$-modules, but this is not true for all finite subrings of $\overline{\mathbb{Z}/\ell^m\mathbb{Z}}$. A Hecke eigenform with coefficients in $\overline{\mathbb{Z}/\ell^m\mathbb{Z}}$ shall simply be called a *modulo* $\ell^m$ *Hecke eigenform*. Dc-weak (and hence also weak) Hecke eigenforms modulo $\ell^m$ have attached Galois representations, under the condition that the residual representation is absolutely irreducible (see [CKW13, Theorem 3]).

**Weight lowering and finiteness**

Let us recall now that in a fixed prime-to-$\ell$ level, there are only finitely many modular Galois representations with coefficients in $\overline{\mathbb{F}}_\ell$, which can all be realised – up to twist – in weights up to $\ell+1$ and that there is an explicit recipe for the minimal weight.

A natural question is whether there is a recipe for a minimal weight for strong eigenforms modulo $\ell^m$, i.e. whether (almost) all the (prime-indexed) Hecke eigenvalues of a given strong eigenform $f$ modulo $\ell^m$ in weight $k$ and level $N$ (prime to $\ell$) also occur for a strong eigenform $g$ modulo $\ell^m$ in the same level $N$ and a 'low' or 'minimal' weight that can be calculated from the restriction to a decomposition group at $\ell$ of the Galois representation attached to $f$ (under the assumption of residual absolute irreducibilty).

This question seems to be very difficult. One is then led to consider the question, for fixed prime-to $\ell$ level $N$, whether the set

$$\{\sum_{n\geq 1} f(T_n)q^n \in \overline{\mathbb{Z}/\ell^m\mathbb{Z}}[[q]] \mid f \text{ strong eigenform modulo } \ell^m \text{ of level } N, \text{ any weight } \}$$

is finite. It can also be seen as the set of reductions modulo $\ell^m$ of all holomorphic Hecke eigenforms in level $N$ of any weight. The second author together with Kiming and Rustom conjectures that this is the case ([KRW16, Conjecture 1]). As is shown in Theorem 2 of loc. cit., a positive answer to a question of Buzzard [Buz05, Question 4.4] would indeed imply this. As an indication towards finiteness or the potential existence of a weight recipe as alluded to above, [KRW16, Theorem 3], proved with the help of Frank Calegari, shows that for $\ell \geq 5$, there exists a bound $B = B(N,\ell^m)$ such that the $q$-expansion of any *strong* Hecke eigenform modulo $\ell^m$ of level $N$, but any weight, already occurs in weight $k \leq B$ for some *weak* Hecke eigenform modulo $\ell^m$ of level $N$. One should compare this with the level raising and level lowering results below, which also 'only' lead to weak forms.

Some first experimentation has led Kiming, Rustom and the second author to state the formula

$$B(N,\ell^m) = 2\ell^m + \ell^2 + 1$$

for $m \geq 2$. It is consistent with the available computational data, but should not be understood as a conjecture at this point.

**Level raising**

Led by classical level raising results, one can hope that similar statements are true modulo $\ell^m$. It seems that part of the theory indeed carries over from modulo $\ell$ to modulo $\ell^m$ eigenforms. In Section 3 we prove a level raising result for weight 2 eigenforms on $\Gamma_0(N)$. For $\ell > 2$, this result is as general as possible. Only for $\ell = 2$ some rare cases could not be proved.

Let $f : \mathbb{T} \to \overline{\mathbb{Z}/\ell^m\mathbb{Z}}$ be a weak modulo $\ell^m$ Hecke eigenform with Galois representation $\rho$. The main idea is to extend Ribet's 'classical' geometric approach of level raising to our more general situation. For that we need to realise $\rho$ on the Jacobian $J$ of the appropriate modular curve. It is well known that the Hecke algebra acts faithfully on $J$. However, we need that $\mathbb{T}/\ker(f)$, i.e. the image of the weak eigenform, also acts faithfully on a subgroup of the Jacobian. The natural place is $J(\overline{\mathbb{Q}})[\ker(f)]$. It turns out that this faithfulness does not seem to be that clear. In fact, we currently make use of the 'multiplicity one' property for the residual Galois representation on the Jacobian and, equivalently, the Gorenstein property of the residual Hecke algebra. Once this faithfulness is established, the proof proceeds by comparing the new and the old subvarieties in level $Np$ as in Ribet's original work [Rib90b]. One should expect similar limitations when extending level raising modulo $\ell^m$ to higher weights, e.g. the weight will likely have to be less than $\ell$ if one wants complete results in order to remain in the multiplicity one situation, where faithfulness is known and easily obtained from existing results.

**Level lowering and other results**

Another natural domain is that of level lowering modulo $\ell^m$. The principal idea is that one should always be able to find an eigenform giving rise to a given Galois representation when the level is equal to the Artin conductor of the representation. An immediate difficulty is then, of course, to define an Artin conductor for Galois representations modulo $\ell^m$. It does not seem to be immediately clear how to do this because not every module over $\mathbb{Z}/\ell^m\mathbb{Z}$ is free, so that there is no natural analog for the dimension (of, say, inertia invariants) used in the classical Artin conductor. Nevertheless, one can at least ask whether one can always find a modulo $\ell^m$ Hecke eigenform of a level which is only divisible by primes ramifying in the representation. There are, indeed, two such results, one is due to Dummigan, and the other one due to Camporino and Pacetti. We quote both in Section 4. Dummigan's result, similar to our level raising theorem, works geometrically on cohomology, whereas Camporino and Pacetti use the deformation theory of Galois representations. Both approaches currently seem to lead to some restrictions (a congruence condition for Dummigan, and unramified coefficients for Camporino–Pacetti).

Concerning generalisations along the lines of level lowering results modulo $\ell$, which are based on the use of Shimura curves, the mod $\ell^m$ Galois representation must first be realised in the cohomology (or the Jacobian) of the appropriate Shimura curve. This is likely going to lead into faithfulness problems analogous to the one we solved in the level raising result by appealing to the Gorenstein or multiplicity one condition.

As a further instance of level lowering (though of a slightly different nature), we mention the following result from [CKW13, Theorem 5]: Any dc-weak eigenform modulo $\ell^m$ in level $N\ell^r$ already arises from a dc-weak eigenform modulo $\ell^m$ in level $N$, under the hypotheses $\ell \geq 5$ and that the mod $\ell$ reduction has an absolutely

irreducible Galois representation. It is also shown that even if one starts with a strong eigenform modulo $\ell^m$, the one in level $N$ will only be dc-weak, in general.

Another natural direction is to extend companionship results from eigenforms modulo $\ell$ to $\ell^m$. This has been successfully performed by Adibhatla and Manoharmayum in [AM12] for odd $\ell$ and ordinary modular forms with coefficients unramified at $\ell$, under certain conditions. In fact, that work is set in the more general world of Hilbert modular forms. Another companionship result modulo prime powers has been achieved by the first author together with Adibhatla [AT15].

## Computations, algorithm and database

Next to the theoretical and structural motivation for studying modular forms and modularity questions modulo prime powers, there is also a strong computational driving force: realising $\ell$-adic modular forms on a computer is only possible up to a certain precision, i.e. one necessarily realises modular forms modulo $\ell^m$.

This also naturally leads to the questions studied in this article. For instance, if one wants to compute modulo which power of $\ell$ a modular $\ell$-adic Galois representation $\rho$ of conductor $Np$ (with $p$ a prime not dividing $N$) becomes unramified at $p$, one can test whether the system of Hecke eigenvalues modulo $\ell^m$ also occurs in level $N/p$ for $m = 1, 2, \ldots$ until this fails. If it first fails at $m+1$, then $\rho$ modulo $\ell^m$ is known to be unramified at $p$. In cases where level lowering modulo $\ell^m$ is entirely proved, one also gets that $\rho$ modulo $\ell^{m+1}$ does ramify at $p$. The authors know of no other way of obtaining such information of an $\ell$-adic modular Galois representation.

The authors have developed several algorithmic tools for handling modular forms modulo $\ell^m$ and they have set up a database. Section 5 contains a brief exposition of how to compute decompositions of commutative algebras into local factors in situations arising from Hecke algebras, and how to perform weak modularity tests explicitly. Finally, in Section 6 we describe features of the database of modular form orbits and higher congruences that we have developed.

## Acknowledgements

The authors would like to thank Rajender Adibhatla, Sara Arias-de-Reyna, Gebhard Böckle, Frank Calegari, Imin Chen, Shaunak Deo, Frazer Jarvis, Ian Kiming, Ariel Pacetti, Nadim Ruston and many others for various discussions about topics on modular Galois representations modulo prime powers. They also thank Ken Ribet for having pointed out an inaccuracy in a previous version. Thanks are also due to the referee for a careful reading and useful suggestions. The second author thanks Gabi Nebe for having explained the simple algorithmic idempotent lifting (Eq. (4)) to him a long time ago.

This project was supported by the Luxembourg Research Fund (Fonds National de la Recherche Luxembourg) INTER/DFG/12/10/COMFGREP in the framework of the priority program 1489 of the Deutsche Forschungsgemeinschaft.

## 2 Modularity

In this section we prove the following modularity theorem. This theorem has been known to the experts and is a pretty straight forward application of 'bigR=bigT' theorems.

**Theorem 3.** *Let $\ell \geq 5$ be a prime number, let $\Sigma$ be a finite set of primes not containing $\ell$ and let $G_{\mathbb{Q},\Sigma\cup\{\infty,\ell\}}$ be the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside $\Sigma\cup\{\ell,\infty\}$. Consider a continuous Galois representation*

$$\rho : G_{\mathbb{Q},\Sigma\cup\{\infty,\ell\}} \to \mathrm{GL}_2(\overline{\mathbb{Z}/\ell^m\mathbb{Z}})$$

*such that the residual representation $\overline{\rho}$ satisfies:*

- *$\overline{\rho}$ is odd,*
- *$\overline{\rho}|_{G_{\mathbb{Q}(\zeta_p)}}$ is absolutely irreducible,*
- *$\overline{\rho}|_{G_{\mathbb{Q}_\ell}} \not\sim \chi\otimes\begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix}$ and $\overline{\rho}|_{G_{\mathbb{Q}_\ell}} \not\sim \chi\otimes\begin{pmatrix}1 & *\\ 0 & \overline{\varepsilon}\end{pmatrix}$, for any $\overline{\mathbb{F}}_\ell$-valued character $\chi$ of $G_{\mathbb{Q}_\ell}$ and the mod $\ell$ cyclotomic character $\overline{\varepsilon}$ (where $*$ may or may not be zero).*

*Let $N$ be the maximal positive integer divisible only by primes in $\Sigma$ such that there is a newform of level $N$ (and some weight) giving rise to $\overline{\rho}$.*

*Then $\rho$ is dc-weakly modular of level $N$, i.e. $\rho \cong \rho_f$ with $f$ a dc-weak Hecke eigenform modulo $\ell^m$ of level $N$.*

In the exposition of the theory, we essentially follow Deo's paper [Deo17]. Let us assume the notation and the set-up from Theorem 3. Let $\mathscr{O}$ be the valuation ring of a finite extension of $\mathbb{Q}_\ell$ with ramification index $e$, valuation ideal $\lambda$ and residue field $\mathbb{F}$ such that (possibly after conjugation) $\rho$ takes values in $\mathrm{GL}_2(\mathscr{O}/\lambda^w) \subset \mathrm{GL}_2(\overline{\mathbb{Z}/\ell^m\mathbb{Z}})$ with $w = e(m-1)+1$. Let $\mathbb{T}'_{\mathscr{O}}(\Gamma_1(N))$ be defined as the projective limit over $b$ of $\mathscr{O}\otimes\mathbb{T}'_{\leq b}(\Gamma_1(N))$ which are defined precisely like $\mathbb{T}_{\leq b}(\Gamma_1(N))$, but only take Hecke operators $T_n$ with $n$ coprime to $N\ell$ into account. Similarly, like Deo we define the partially full Hecke algebra $\mathbb{T}^{\mathrm{pf}}_{\mathscr{O}}(\Gamma_1(N))$ as the projective limit of $\mathscr{O}\otimes\mathbb{T}^{\mathrm{pf}}_{\leq b}(\Gamma_1(N))$ by using in addition the operators $U_q$ for primes $q \mid N$. If we localise at the system of eigenvalues afforded by $\overline{\rho}$, we denote this by $\overline{\rho}$ in the index. Accordingly, denote by $R_{\overline{\rho}}$ the universal deformation ring of $\overline{\rho}$ for the group $G_{\mathbb{Q},\Sigma\cup\{\infty,\ell\}}$ in the category of local profinite $\mathscr{O}$-algebras with residue field $\mathbb{F}$.

**Theorem 4 (Böckle, Diamond–Flach–Guo, Gouvêa–Mazur, Kisin).** *Assume the set-up of Theorem 3. Then $R_{\overline{\rho}} \cong \mathbb{T}'_{\mathscr{O}}(\Gamma_1(N))_{\overline{\rho}}$.*

This is Theorem 5 from [Deo17]. Note that Deo works with pseudo-representations, but this comes down to the same thing here because we assume $\overline{\rho}$ to be irreducible. In the proof, Deo essentially explains why the results of [DFG04] allow to strengthen the conclusions of [Böc01]. A similar discussion can also be found in [Eme11, §7.3], where the theorem is, however, not stated in the form we need here. Alternatively, one can also invoke [Eme11, Theorem 1.2.3] to an $\ell$-adic lift

of $\rho$, provided such a lift exists. Recent work by Khare and Ramakrishna [KR15] provides a construction in the ordinary case.

We now apply Theorem 4. By assumption, $\rho$ is a deformation of $\overline{\rho}$ with the right ramification set, whence the universality leads to an $\mathscr{O}$-algebra homomorphism $R_{\overline{\rho}} \to \mathscr{O}/\lambda^w$, which we consider as an $\mathscr{O}$-algebra homomorphism

$$f : \mathbb{T}'_{\mathscr{O}}(\Gamma_1(N))_{\overline{\rho}} \to \mathscr{O}/\lambda^w.$$

By construction, the Galois representation associated with $f$ is isomorphic to $\rho$.

In order to finish the proof of Theorem 3, $f$ has to be extended to the full Hecke algebra in order to make it a genuine Hecke eigenform modulo $\ell^m$. Next we use that $\mathbb{T}^{\mathrm{pf}}_{\mathscr{O}}(\Gamma_1(N))_{\overline{\rho}}$ is finite over $\mathbb{T}'_{\mathscr{O}}(\Gamma_1(N))_{\overline{\rho}}$. This is proved in [Deo17, Proposition 6]; one should note that the $\Gamma_1(N)$-new assumption is not necessary for this statement (see the proof of [Deo17, Theorem 3]). This integrality allows us to extend $f$ to an $\mathscr{O}$-algebra homomorphism

$$f : \mathbb{T}^{\mathrm{pf}}_{\mathscr{O}}(\Gamma_1(N))_{\overline{\rho}} \to \tilde{\mathscr{O}}/\tilde{\lambda}^{\tilde{w}}$$

where $\mathscr{O} \subseteq \tilde{\mathscr{O}}$ is the valuation ring of some finite extension of $\mathbb{Q}_\ell$ with valuation ideal $\tilde{\lambda}$ and ramification index $\tilde{e}$ and $\tilde{w} = \tilde{e}(m-1)+1$. One is able to make this extension because one only needs to find one zero in some ring of the form $\tilde{\mathscr{O}}/\tilde{\lambda}^{\tilde{w}}$ for any monic polynomial with coefficients in $\mathscr{O}/\lambda^w$; that this is possible follows, for instance, by choosing any monic lift to $\mathscr{O}$. From the natural degeneracy map, we next get an $\mathscr{O}$-algebra homomorphism $f : \mathbb{T}^{\mathrm{pf}}_{\mathscr{O}}(\Gamma_1(N\ell))_{\overline{\rho}} \to \tilde{\mathscr{O}}/\tilde{\lambda}^{\tilde{w}}$, which after choice of $f(U_\ell)$ leads to the $\mathscr{O}$-algebra homomorphism

$$f : \mathbb{T}^{\mathrm{pf}}_{\mathscr{O}}(\Gamma_1(N\ell))_{\overline{\rho}}[[U_\ell]] \to \tilde{\mathscr{O}}/\tilde{\lambda}^{\tilde{w}}.$$

According to [Deo17, Proposition 5], one can identify $\mathbb{T}^{\mathrm{pf}}_{\mathscr{O}}(\Gamma_1(N\ell))_{\overline{\rho}}[[U_\ell]]$ with a quotient of the full Hecke algebra $\mathbb{T}_{\mathscr{O}}(\Gamma_1(N\ell))$. We obtain thus an $\mathscr{O}$-algebra homomorphism

$$f : \mathbb{T}_{\mathscr{O}}(\Gamma_1(N\ell)) \to \tilde{\mathscr{O}}/\tilde{\lambda}^{\tilde{w}}.$$

As its image is finite, it will factor through $\mathscr{O} \otimes \mathbb{T}_{\leq b}(\Gamma_1(N\ell))$ for a suitable weight bound $b$, so that we finally get a ring homomorphism

$$f : \mathbb{T}_{\leq b}(\Gamma_1(N\ell)) \to \tilde{\mathscr{O}}/\tilde{\lambda}^{\tilde{w}}.$$

This is the dc-weak eigenform that is needed to finish the proof of Theorem 3. Note that one can still remove $\ell$ from the level of the final form because of [CKW13, Theorem 5].

## 3 Level raising via modular curves

Let $p$ be a rational prime. Then one has a natural inclusion map

$$S_k(\Gamma_0(N)) \oplus S_k(\Gamma_0(N)) \to S_k(\Gamma_0(Np)),$$

the image of which is called the *p-old subspace*. This subspace is stable under the action of $\mathbb{T}_k(Np) := \mathbb{T}_k(\Gamma_0(Np))$ and so is its orthogonal complement under the Petersson inner product. This complementary subspace is called the *p-new subspace* and we denote by $\mathbb{T}_k^{p-\text{new}}(Np)$ the quotient of $\mathbb{T}_k(Np)$ that acts faithfully on it. We will call this quotient the *p-new quotient of* $\mathbb{T}_k(Np)$. There is also the *p-old quotient* that is defined in the obvious way.

We can now state the main level raising result of this article.

**Theorem 5.** *Let $R$ be a local topological ring with maximal ideal $\mathfrak{m}_R$. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ be a continuous Galois representation that is modular, associated with a weak eigenform $\theta : \mathbb{T}_2(N) \to R$, and such that the residual representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(R/\mathfrak{m})$ is absolutely irreducible. If the characteristic of $R/\mathfrak{m}$ is 2, assume the* multiplicity one/Gorenstein condition *that $\overline{\rho}$ is not unramified at 2 with scalar Frobenius.*

*Let $p$ be a prime which satisfies the* level raising condition *for $\rho$ by which we mean that $\rho$ is unramified at $p$ and*

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = \pm(p+1).$$

*Then the image of $\theta$ is a finite ring, $R/\mathfrak{m}$ is a finite field and $\rho$ is also associated with a weak eigenform $\theta' : \mathbb{T}_2(Np) \to R$ which is new at $p$, i.e. $\theta'$ factors through $\mathbb{T}_2^{p-new}(Np)$.*

In view of Lemma 8, the following corollary is essentially just an equivalent reformulation. Let $\mathscr{O}$ be the ring of integers of a number field and $\lambda$ a prime in $\mathscr{O}$ above $\ell$.

**Corollary 6.** *Let $m \geq 1$ be an integer and $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathscr{O}/\lambda^m)$ be a continuous (for the discrete topology on $\mathscr{O}/\lambda^m$) Galois representation that is modular, associated with a weak eigenform $\theta : \mathbb{T}_2(N) \to \mathscr{O}/\lambda^m$, and such that the residual representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathscr{O}/\lambda)$ is absolutely irreducible. If $\mathscr{O}/\lambda$ is of characteristic 2, assume the* multiplicity one/Gorenstein condition *that $\overline{\rho}$ is not unramified at 2 with scalar Frobenius.*

*Let $p$ be a prime which satisfies the* level raising condition *for $\rho$, which means here that*

$$(\ell N, p) = 1 \text{ and } \mathrm{Tr}(\rho(\mathrm{Frob}_p)) \equiv \pm(p+1) \mod \lambda^m.$$

*Then $\rho$ is also associated with a weak eigenform $\theta' : \mathbb{T}_2(Np) \to \mathscr{O}/\lambda^m$ which is new at $p$, i.e. $\theta'$ factors through the $\mathbb{T}_2^{p-new}(Np)$.*

We remark that for $m = 1$ this is Theorem 1 of [Rib90b]. Even if $\theta$ is a strong eigenform, there is no guarantee that the weak eigenform of level new at $p$ that one obtains in the end is strong.

**Corollary 7.** *Let $R$ be a local topological ring with maximal ideal $\mathfrak{m}_R$ and let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ be a continuous Galois representation that is modular, has finite image and such that the residual representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(R/\mathfrak{m})$ is absolutely irreducible. If the characteristic of $R/\mathfrak{m}$ is 2, assume the* multiplicity one/Gorenstein condition *that $\overline{\rho}$ is not unramified at 2 with scalar Frobenius.*

*Then there exists a positive set of primes $p$ (coprime to $N$) such that $\rho$ is modular of level $Np$ and new at $p$.*

*Proof.* This is proved as in [Rib90b]. The argument is that complex conjugation, as an involution, has trace 0 and determinant $-1$. By Chebotarev's density theorem, there is a positive density set of primes $p$ such that $-1 = \det(\rho(\mathrm{Frob}_p)) = p$ and $p+1 = 0 = \mathrm{Tr}(\rho(\mathrm{Frob}_p))$ in $R$. □

### Jacobians of modular curves

In what follows we set $\mathbb{T}_N := \mathbb{T}_2(\Gamma_0(N))$ and $\mathbb{T}_{Np} := \mathbb{T}_2(\Gamma_0(Np))$. The approach taken here is adapted from Ribet's original one, i.e. it is based on the geometry of modular curves and their Jacobians. In this section we gather the necessary results from [Rib90b] that we need for the proof of the main result. Let $N$ be a positive integer. Let $X_0(N)$ be the modular curve of level $N$ and $J_0(N) := \mathrm{Pic}^0(X_0(N))$ its Jacobian. There is a well defined action of the Hecke operators $T_n$ on $X_0(N)$ and hence, by functoriality, on $J_0(N)$, too. The dual of $J_0(N)$ carries an action of the Hecke algebra as well and can be identified with $S_2(\Gamma_0(N))$. This implies that one has a faithful action of $\mathbb{T}_N$ on $J_0(N)$.

Let now $p$ be a prime not dividing $N$. In the same way one has an action of Hecke operators on $X_0(Np)$ and its Jacobian $J_0(Np)$ and the latter admits a faithful action of $\mathbb{T}_{Np}$. The moduli interpretation of $X_0(N)$ and $X_0(Np)$ allows us to define the two natural degeneracy maps $\delta_1, \delta_p : X_0(Np) \to X_0(N)$ and their pullbacks $\delta_1^*, \delta_p^* : J_0(N) \to J_0(Np)$. The image of the map

$$\alpha : J_0(N) \times J_0(N) \to J_0(Np), \qquad (x,y) \mapsto \delta_1^*(x) + \delta_p^*(y).$$

is by definition the *p-old subvariety* of $J_0(Np)$. We will denote it by $A$. The map $\alpha$ is *almost* Hecke-equivariant:

$$\alpha \circ T_q = T_q \circ \alpha \text{ for every prime } q \neq p, \tag{1}$$

$$\alpha \circ \begin{pmatrix} T_p & p \\ -1 & 0 \end{pmatrix} = U_p \circ \alpha. \tag{2}$$

For the first equation to make sense one interprets the operator $T_q$ on the left hand side of equation (1) as acting diagonally on $J_0(N) \times J_0(N)$. We also work under the notational convention $T_q = U_q$ for primes $q \mid N$, but we write $U_p$ in level $Np$. Consider also the kernel Sh of the map $J_0(N) \to J_1(N)$ induced by $X_1(N) \to X_0(N)$. If we inject it into $J_0(N) \times J_0(N)$ via $x \mapsto (x, -x)$ then its image, which we will denote by $\Sigma$, is the kernel of $\alpha$ (see Proposition 1 in [Rib90b]).

Let $\Delta$ be the kernel of $\begin{pmatrix} 1+p & T_p \\ T_p & 1+p \end{pmatrix} \in M^{2\times 2}(\mathbb{T}_N)$ acting on $J_0(N)\times J_0(N)$. The group $\Delta$ is finite and comes equipped with a perfect $\mathbb{G}_m$-valued skew-symmetric pairing. Furthermore $\Sigma$ is a subgroup of $\Delta$, self orthogonal, and $\Sigma \subseteq \Sigma^\perp \subseteq \Delta$. One can also see $\Delta/\Sigma$, and therefore its subgroup $\Sigma^\perp/\Sigma$, as a subgroup of $A$.

Let $B$ be the $p$-new subvariety of $J_0(Np)$. It is a complement of $A$, i.e. $A+B = J_0(Np)$ and $A\cap B$ is finite. The Hecke algebra acts faithfully on $B$ through its $p$-new quotient and it turns out (see Theorem 2 in [Rib90b]) that

$$A\cap B \cong \Sigma^\perp/\Sigma. \tag{3}$$

as groups.

Furthermore Sh, and therefore $\Sigma$ and its Cartier dual $\Delta/\Sigma^\perp$, are annihilated by the operators $\eta_r = T_r - (r+1) \in \mathbb{T}_N$ for all primes $r \nmid Np$ (see Proposition 2 in [Rib90b]). In this context, we recall that a maximal ideal $\mathfrak{m}$ of the Hecke algebra $\mathbb{T}_N$ is called *Eisenstein* if $T_r \mod \mathfrak{m}$ equals the Frobenius traces of a two-dimensional reducible Galois representation at almost all primes $r$. This is in particular the case if $\mathfrak{m}$ contains the operator $T_r-(r+1)$ for almost all primes $r$. Consequently, any maximal ideal in the support of the Hecke modules $\Sigma$ and $\Delta/\Sigma^\perp$ is Eisenstein.

**Proof of Theorem 5**

We assume the setting of Theorem 5. In particular, we assume that $\rho$ satisfies the level raising condition at a prime $p \nmid N$, i.e. there is $\varepsilon \in \{\pm 1\}$ such that $\theta(T_p) = \mathrm{Tr}(\rho(\mathrm{Frob}_p)) = \varepsilon(p+1)$. Let $\overline{\theta} : \mathbb{T}_N \to R/\mathfrak{m}_R$ be its reduction modulo $\mathfrak{m}_R$ (which is associated with $\overline{\rho}$, the modulo $\mathfrak{m}_R$ reduction of $\rho$), and let $I$ and $\mathfrak{m}$ be the kernels of $\theta$ and $\overline{\theta}$, respectively. It will be enough to find a weak eigenform $\theta' : \mathbb{T}_{Np} \to R$ (i.e. a ring homomorphism) that agrees with $\theta$ on $T_q$ for all primes $q \neq p$ and factors through $\mathbb{T}_{Np}^{p-\mathrm{new}}$ (hence, new at $p$).

**Lemma 8.** *The ideal $\mathfrak{m}$ is the only maximal ideal of $\mathbb{T}_N$ containing $I$. Moreover, $\mathbb{T}_N/I$ is a finite subring of $R$ of positive characteristic a prime power $\ell^r$.*

*Proof.* Since $\mathbb{T}_N$ is a $\mathbb{Z}$-Hecke algebra acting faithfully on $S_2(N)$ we have that $\mathbb{T}_N$ injects into $M^{d\times d}(\mathbb{Z})$, where $d$ is the dimension of $S_2(N)$. We can therefore see every operator in $\mathbb{T}_N$ as an integral matrix of dimension $d$. We recall that the eigenvalues of the operator $T_n$ will correspond to the coefficients $a_n(f)$ when $f$ runs through the normalised eigenforms in $S_2(N)$.

Let $g(X) \in \mathbb{Z}[X]$ be the characteristic polynomial of $T_p$. The hypothesis $\theta(T_p) = \varepsilon(p+1)$ implies that $T_p - \varepsilon(p+1) \in I$ and therefore $m := g(\varepsilon(p+1)) \in I$. Since $p \nmid N$, the Ramanujan-Petersson bounds guarantee that none of the eigenvalues of $T_p$ is equal to $\varepsilon(p+1)$ and therefore $m$ is non-zero. We thus have that $(m) \subseteq I$. This makes the quotient $\mathbb{T}/I$ finite.

Since $\mathbb{T}/I$ is Artinian, it can be written as a direct product of Artinian local rings indexed by its finitely many maximal ideals. Assume it decomposes as a direct product of $s$ local rings, with $s \geq 1$. The set containing the identity $e_i$ of each component

then forms a complete set (i.e. $\sum_{i=1}^{s} e_i = 1$) of pairwise orthogonal (i.e. $e_i e_j = 0$ for $1 \leq i \neq j \leq s$) non-trivial (i.e. $e_i \neq 0, 1$) idempotents for $\mathbb{T}_N/I$. The set $\{\overline{e_1}, \ldots, \overline{e_s}\}$ of their image through the injection of $\mathbb{T}_N/I$ into $R$ is clearly a complete set of pairwise orthogonal non-trivial idempotents, too. This implies that $R$ is isomorphic to $\prod_{i=1}^{s} \overline{e_i}R$. But this cannot happen unless $s = 1$ since $R$ is local. Since $s = 1$ we get that $\mathbb{T}_N/I$ is local as well. The claims are then immediate. □

By the previous lemma, we have inclusions $(\ell^r) \subseteq I \subseteq \mathfrak{m}$ with some prime power $\ell^r > 1$, giving rise to inclusions

$$V[\ell^r] := J_0(N)(\overline{\mathbb{Q}})[\ell^r] \supseteq V[I] := J_0(N)(\overline{\mathbb{Q}})[I] \supseteq V[\mathfrak{m}] := J_0(N)(\overline{\mathbb{Q}})[\mathfrak{m}].$$

**Lemma 9.** *The support of $V[I]$ is the singleton $\mathfrak{m}$ and is hence non-Eisenstein.*

*Proof.* As $V[I] \supseteq V[\mathfrak{m}]$, the maximal ideal $\mathfrak{m}$ is in the support of $V[I]$. Since the representation $\overline{\rho}$ is irreducible we get that $\mathfrak{m}$ is non-Eisenstein (see for example Theorem 5.2c in [Rib90a]). Finally, Lemma 8 implies that $\mathrm{Supp}(V[I])$ is the singleton $\{\mathfrak{m}\}$. □

**Lemma 10.** *The restriction of $\alpha$ to $V[I]$ is injective and its image $\alpha(V[I])$ is stable under the action of $\mathbb{T}_{Np}$. In particular, $U_p$ acts on $\alpha(V[I])$ by multiplication by $\varepsilon$.*

*Proof.* Consider the image of $V[I]$ (still denoted $V[I]$) under the $\mathbb{T}_N$-equivariant embedding

$$J_0(N) \xrightarrow{x \mapsto (x, -\varepsilon x)} J_0(N) \times J_0(N).$$

Next recall that the kernel $\Sigma$ of $J_0(N) \times J_0(N) \xrightarrow{\alpha} A \subseteq J_0(Np)$ is annihilated by almost all operators $T_r - (r+1)$ with $r$ prime. The fact that the support of $V[I]$ is non-Eisenstein from Lemma 9 shows that the intersection of $\Sigma$ and $V[I]$ is trivial, proving the injectivity of $\alpha|_{V[I]}$.

As $\alpha$ commutes with the action of the Hecke operators $T_n$ with $n$ coprime to $p$ (see Equation (1)), it follows that $\alpha(V[I])$ is stable under those operators. Here the level raising condition enters for proving the stability under $U_p$, as follows by using Equation (2) for $y \in V[I]$:

$$\begin{aligned} U_p(y) = U_p(\alpha(x, -\varepsilon x)) &= \alpha(\begin{pmatrix} T_p & p \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ -\varepsilon x \end{pmatrix}) = \alpha(T_p(x) - \varepsilon p x, -x) \\ &= \alpha(\varepsilon(p+1)x - \varepsilon p x, -x) = \alpha(\varepsilon x, -x) = \varepsilon \alpha(x, -\varepsilon x) = \varepsilon y. \end{aligned}$$

The final claim follows as well. □

The following proposition is a non-trivial input.

**Proposition 11.** *The $\mathbb{T}_N/I$-module $V[I]$ is faithful.*

*Proof.* Due to the assumptions, Theorem 9.2 of [Edi92] implies that $V[\mathfrak{m}]$ is of dimension 2 as $\mathbb{T}_N/\mathfrak{m}$-module. By Nakayama's Lemma, it follows that the localisation at $\mathfrak{m}$ of the $\ell$-adic Tate module is free of rank 2 as $(\mathbb{T}_N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)_{\mathfrak{m}}$-module and that

$\mathrm{Hom}_{\mathbb{Z}_\ell}((\mathbb{T}_N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)_{\mathfrak{m}}, \mathbb{Z}_\ell)$ is free of rank 1 as $(\mathbb{T}_N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)_{\mathfrak{m}}$-module, precisely as on p. 333 of [Til97]. Consequently,

$$V[\ell^r]_{\mathfrak{m}} \cong (\mathbb{T}_N/\ell^r\mathbb{T}_N)^2_{\mathfrak{m}} \cong \mathrm{Hom}_{\mathbb{Z}_\ell}((\mathbb{T}_N/\ell^r\mathbb{T}_N)_{\mathfrak{m}}, \mathbb{Z}/\ell^r\mathbb{Z})^2,$$

which implies by taking the $\bar{I}$-kernel with $\bar{I}$ the ideal such that $\mathbb{T}_N/I \cong (\mathbb{T}_N/\ell^r\mathbb{T}_N)/\bar{I}$ that

$$V[I] \cong \mathrm{Hom}_{\mathbb{Z}}((\mathbb{T}_N/\ell^r\mathbb{T}_N)/\bar{I}, \mathbb{Z}/\ell^r\mathbb{Z})^2 = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_N/I, \mathbb{Z}/\ell^r\mathbb{Z}),$$

showing that $V[I]$ is faithful as $\mathbb{T}_N/I$-module. □

The authors do not know if the 'multiplicity one' or 'Gorenstein' condition is necessary. In the remaining case, the $2^r$-torsion group scheme is ordinary, and hence by arguments as in Corollary 2.3 of [Wie07] admits a nice decomposition as

$$0 \to (\mathbb{T}_N/\ell^r\mathbb{T}_N)_{\mathfrak{m}} \to V[\ell^r]_{\mathfrak{m}} \to \mathrm{Hom}_{\mathbb{Z}}((\mathbb{T}_N/\ell^r\mathbb{T}_N)_{\mathfrak{m}}, \mathbb{Z}/\ell^r\mathbb{Z}) \to 0.$$

However, we do not know if this sequence remains exact after taking the $\bar{I}$-kernel. If this were the case, the additional assumption would be unnecessary.

**Lemma 12.** *The action of $\mathbb{T}_{Np}$ on $\alpha(V[I])$ is given by a ring homomorphism $\theta' : \mathbb{T}_{Np} \to R$ satisfying $\theta'(T_q) = \theta(T_q)$ for all primes $q \neq p$ and $\theta'(U_p) = \varepsilon$. In particular, $\theta$ and $\theta'$ give rise to isomorphic Galois representations.*

*Proof.* The faithfulness of $V[I]$ as $\mathbb{T}/I$-module from Proposition 11 implies that $\theta$ factors through a subring $S$ of $\mathrm{End}(V[I])$, which is also a subring of $R$. By Lemma 10 and Equation (1), the action of $\mathbb{T}_{Np}$ on $\alpha(V[I])$ is also given by elements of $S$, leading to a ring homomorphism $\theta' : \mathbb{T}_{Np} \to S \subseteq R$. □

To finish the proof of Theorem 5, it remains to show that $\theta'$ factors through the $p$-new quotient of $\mathbb{T}_{Np}$. To this end, it is enough to show that $\alpha(V[I])$ is a subgroup of $A \cap B$. We again proceed according to Ribet. By the level raising condition, $V[I]$, when considered as a subgroup of $J_0(N) \times J_0(N)$, is a subgroup of $\Delta$, whence $\alpha(V[I]) \subseteq \Delta/\Sigma$. As $\Delta/\Sigma^\perp$ is Eisenstein but $\alpha(V[I])$ is not, $\alpha(V[I])/\Sigma^\perp = 0$. This implies $\alpha(V[I]) \subseteq \Sigma^\perp/\Sigma = A \cap B$, completing the proof of Theorem 5.

## 4 Level lowering

In this section we give an overview of results about level lowering modulo prime powers. We start by the following simple observation: twisting an eigenform $f$ by a Dirichlet character $\chi$ such that $\chi \equiv 1 \mod \lambda^m$ leads to an eigenform $g = f \otimes \chi$, which is congruent to $f$ modulo $\lambda^m$. This idea leads to the following two level lowering results from the first author's unpublished PhD thesis [Tsa09].

**Proposition 13 (Split ramified case).** *Let $f \in S_k(\Gamma_1(M))$ be a newform such that the restriction to a decomposition group at $p \neq \ell$ of the $\ell$-adic Galois representation*

*attached to $f$ is isomorphic to $\chi_1 \oplus \chi_2$, where both characters ramify. Let $\lambda$ be a prime ideal of a number field containing the coefficients of $f$.*

*If $\chi_1$ is unramified modulo $\lambda^m$, then there exists a normalised eigenform $g \in S_k(\Gamma_1(M/p))$ such that $f \equiv g \mod \lambda^m$.*

*Proof.* We can decompose $\chi_1 = \chi_{1,\mathrm{unr}}\chi_{1,\mathrm{ram}}$ into an unramified and a ramified character of $G_{\mathbb{Q}_p}$. As $p \neq \ell$, the order of $\chi_{1,\mathrm{ram}}$ is finite. By assumption, $\chi_{1,\mathrm{ram}} \equiv 1 \mod \lambda^m$, whence in particular the order of $\chi_{1,\mathrm{ram}}$ is a power of $\ell$ because only roots of unity of $\ell$-power order vanish under reduction modulo $\lambda$. Thus $\chi_{1,\mathrm{ram}}$ is tamely ramified. By the local and the global Kronecker-Weber theorems, $\chi_{1,\mathrm{ram}}$ can be seen as a global Dirichlet character $\tilde{\chi}_{1,\mathrm{ram}}$ of conductor $p$ the restriction of which to $G_{\mathbb{Q}_p}$ equals $\chi_{1,\mathrm{ram}}$.

Let now $g$ be the newform corresponding to the twist $f \otimes \tilde{\chi}_{1,\mathrm{ram}}^{-1}$. Then the restriction to a decomposition group at $p$ of the $\ell$-adic Galois representation attached to $g$ is isomorphic to $\chi_{1,\mathrm{unr}} \oplus \chi_2\chi_{1,\mathrm{ram}}^{-1}$. If $\chi_2$ is tame (i.e. of conductor $p$), then $\chi_2\chi_{1,\mathrm{ram}}^{-1}$ is either tame or unramified, and in any case its conductor divides $p$. If $\chi_2$ is wild, i.e. it factors through $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^rN})/\mathbb{Q}_p)$ with $r \geq 2$ and $p \nmid N$, but not through $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{r-1}N})/\mathbb{Q}_p)$, then also $\chi_2\chi_{1,\mathrm{ram}}^{-1}$ factors through $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^rN})/\mathbb{Q}_p)$ but not through $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{r-1}N})/\mathbb{Q}_p)$, whence the conductor of $\chi_2\chi_{1,\mathrm{ram}}^{-1}$ equals that of $\chi_2$. In both cases we hence find that the conductor of $\chi_2\chi_{1,\mathrm{ram}}^{-1}$ divides the conductor of $\chi_2$. Since the $p$-valuation of $M$ equals the $p$-valuation of the conductor of $\chi_2$ plus 1 (since the conductor of $\chi_1$ is $p$) and the $p$-valuation of the newform level of $g$ is the $p$-valuation of the conductor of $\chi_2\chi_{1,\mathrm{ram}}^{-1}$, it is clear that the newform level of $g$ divides $M/p$. □

**Proposition 14 (Special ramified case).** *Let $f \in S_k(\Gamma_1(M))$ be a newform such that the restriction to a decomposition group at $p \neq \ell$ of the $\ell$-adic Galois representation attached to $f$ is isomorphic to $\chi \otimes \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$, where $\chi$ and $*$ ramify and $\omega$ is the $\ell$-adic cyclotomic character. Let $\lambda$ be a prime ideal of a number field containing the coefficients of $f$.*

*If $\chi$ is unramified modulo $\lambda^m$, then there exists a newform $g \in S_k(\Gamma_1(M/p))$ such that $f \equiv g \mod \lambda^m$.*

*Proof.* The proof is essentially the same as in the split ramified case. Note, however, that the tameness of $\chi$ implies that $p^2$ exactly divides $M$, whence the newform level of $g$ will be exactly $M/p$. □

These propositions may be useful in some situations. We also remark that the only Dirichlet character that is trivial modulo $\ell^2$ in the sense of being equal to $1 \in \overline{\mathbb{Z}/\ell^2\mathbb{Z}}$ is the trivial one. That is just due to the fact that $\lambda := 1 - \zeta_\ell$ is a uniformiser of $\mathbb{Q}_\ell(\zeta_\ell)$, whence $\zeta_\ell \not\equiv 1 \mod (\lambda)^2$. This implies that the level does not lower modulo $\ell^m$ for any $m \geq 2$ at primes $p$ satisfying the hypothesis of one of the preceding propositions. We now quote the main result from [Dum15], including the discussion in the last paragraph of that article.

**Theorem 15 (Dummigan).** *Let $\ell$ be a prime. Let $\ell+2 > k \geq 2$ and let $p$ be a prime not dividing $N \in \mathbb{N}$ such that $p \not\equiv 1 \mod \ell$. Let $f \in S_k(\Gamma_1(Np))$ be an eigenform and let $\lambda$ be a prime of the coefficient field of $f$ above $\ell$. Suppose that the residual Galois representation of $f$ modulo $\lambda$ is irreducible.*

*If for some $m \geq 1$ the Galois representation of $f$ modulo $\lambda^m$ is unramified at $p$, then there is a weak eigenform $g$ of weight $k$ and level $\Gamma_1(N)$ such that $f \mod \lambda^m$ equals $g$ at all coefficients the index of which is coprime to $p$.*

Dummigan also gives an explicit example where the resulting form $g$ cannot be strong. We include another still unpublished result from [CP13] on level lowering, which is proved using the deformation theory of Galois representations.

**Theorem 16 (Pacetti-Camporino).** *Let $\ell \geq 7$ be a prime. Let $2 \leq k \leq \ell - 1$. Let $M$ be a positive integer. Let $f \in S_k(\Gamma_1(M))$ be an eigenform with coefficients in $K_f$. Let $\mathcal{O}_f$ be the ring of integers of $K_f$. Assume that*

- *$\ell$ is unramified in $\mathcal{O}_f$, and*
- *$\mathrm{SL}_2(\mathcal{O}_f/\lambda)$ is a subgroup of the image of the mod $\lambda$ representation attached to $f$.*

*If $p \mid M$ is a prime and $m \geq 1$ is an integer such that the modulo $\lambda^m$ Galois representation associated with $f$ is unramified at $p$, then there is a weak eigenform $g$ of weight $k$ and level $\Gamma_1(M/p)$ such that $f \mod \lambda^m$ equals $g$ at all coefficients the index of which is coprime to $p$.*

This result is proved by first applying techniques of Ramakrishna: by introducing auxiliary primes in order to kill local obstructions, the authors construct an $\ell$-adic lift in which $p$ remains unramified. They then prove and use a modularity lifting theorem to obtain that their lift is associated with some newform. Finally, they apply Theorem 15 to remove the auxiliary primes, which had been chosen in such a way that Dummigan's theorem applies.

## 5 Computational aspects

In this section, we describe various algorithms we have implemented and used in our computational study of higher congruences.

### Some commutative algebra

We start by summarising some well known facts from commutative algebra. Let $R$ be an *Artinian* ring, i.e. a ring in which every descending chain of ideals becomes stationary. In particular, for any ideal $\mathfrak{a}$ of $R$, the sequence $\mathfrak{a}^n$ becomes stationary, i.e. $\mathfrak{a}^n = \mathfrak{a}^{n+1}$ for all $n$ "big enough". We will then use the notation $\mathfrak{a}^\infty$ for $\mathfrak{a}^n$. The following proposition is well known and easy to prove:

**Proposition 17.** *Let $R$ be an Artinian ring. Then every prime ideal of $R$ is maximal and there are only finitely many maximal ideals in $R$. Moreover, the maximal ideal $\mathfrak{m}$ is the only one containing $\mathfrak{m}^\infty$. Furthermore, if $\mathfrak{m} \neq \mathfrak{n}$ are two maximal ideals, then for any $k \in \mathbb{N} \cup \{\infty\}$, the ideals $\mathfrak{m}^k$ and $\mathfrak{n}^k$ are coprime. The Jacobson radical $\bigcap_{\mathfrak{m} \in \mathrm{Spec}(R)} \mathfrak{m}$ is equal to the nilradical and consists of the nilpotent elements, and we have $\bigcap_{\mathfrak{m} \in \mathrm{Spec}(R)} \mathfrak{m}^\infty = (0)$. Moreover, for every maximal ideal $\mathfrak{m}$, the ring $R/\mathfrak{m}^\infty$ is local with maximal ideal $\mathfrak{m}$ and is hence isomorphic to $R_\mathfrak{m}$, the localisation of $R$ at $\mathfrak{m}$. Finally, by virtue of the Chinese Remainder Theorem we have the following isomorphism, referred to as* local decomposition*:*

$$R \xrightarrow{a \mapsto (\ldots, a+\mathfrak{m}^\infty, \ldots)} \prod_{\mathfrak{m} \in \mathrm{Spec}(R)} R/\mathfrak{m}^\infty \cong \prod_{\mathfrak{m} \in \mathrm{Spec}(R)} R_\mathfrak{m}.$$

**Definition 18.** An *idempotent* of a ring $R$ is an element $e$ that satisfies $e^2 = e$. Two idempotents $e$, $f$ are *orthogonal* if $ef = 0$. An idempotent $e$ is *primitive* if it cannot be written as a sum of two idempotents both different from 0. A set of idempotents $\{e_1, \ldots, e_n\}$ is said to be *complete* if $1 = \sum_{i=1}^n e_i$.

In concrete terms, a complete set of primitive pairwise orthogonal idempotents is given by $(1,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (0,\ldots,0,1)$.

**Proposition 19 (Newton method/Hensel lifting – special case).** *Let $R$ be a ring and $I$ be an ideal. Let $f \in R[X]$ be a polynomial. We assume that there exist $a \in R$ and a polynomial $b \in R[X]$ such that $1 = af(X) + b(X)f'(X)$. Let further $a_0 \in R$ be such that $f(a_0) \in I^r$ for some $r \geq 1$. For $n \geq 1$, we make the following recursive definition:*

$$a_n := a_{n-1} - f(a_{n-1})b(a_{n-1}).$$

*Then for all $n \in \mathbb{N}$, we have $f(a_n) \in (I^r)^{2^n}$. In particular, if $\bigcap_{n \geq 1} I^n = 0$ then the sequence $f(a_n)$ converges to 0 exponentially.*

*Proof.* This is a straight forward calculation with Taylor expansions of the polynomial. □

**Corollary 20 (Algorithmic idempotent lifting).** *Let $R$ be a commutative $\mathbb{Z}_\ell$-algebra which is finitely generated as $\mathbb{Z}_\ell$-module. Let $e_0 \in R/\ell R$ be an idempotent. For $n \geq 1$, make the following recursive definition:*

$$e_n := e_{n-1} - (e_{n-1}^2 - e_{n-1})(2e_{n-1} - 1) = 3e_{n-1}^2 - 2e_{n-1}^3. \tag{4}$$

*Then $e_n^2 \equiv e_n \mod \ell^{2^n} R$ for all $n \geq 0$. Moreover, the $e_n$ form a Cauchy sequence in $R$ and thus converge to an idempotent $e \in R$ 'lifting' $e_0$, i.e. the image of $e$ in $R/\ell R$ is $e_0$.*

*Proof.* This is a simple application of the Newton method to the polynomial $f(X) = X^2 - X$. Note that we have $f'(X) = 2X - 1$ and $1 = -4(X^2 - X) + (2X-1)(2X-1)$. □

The corollary thus tells us that any idempotent of $R/\ell R$ lifts to an idempotent of $R$, and it tells us that the lift can be approximated by a simple recursion formula that is easy to implement and converges very rapidly. We shall now apply the preceding considerations to a commutative $\mathbb{Z}_\ell$-algebra $\mathbb{T}$ which is free and finitely generated as a $\mathbb{Z}_\ell$-module. Let $\overline{\mathbb{T}} = \mathbb{T} \otimes \mathbb{F}_\ell$ and $\mathbb{T}_{\mathbb{Q}_\ell} = \mathbb{T} \otimes \mathbb{Q}_\ell$. Note that $\overline{\mathbb{T}}$ and $\mathbb{T}_{\mathbb{Q}_\ell}$ are Artinian rings because they are finite dimensional vector spaces. The following well-known result follows from the above considerations together with some standard commutative algebra.

**Proposition 21.** *The algebra $\mathbb{T}$ is equidimensional (in the sense of Krull dimension) of dimension* 1*, i.e. any maximal ideal $\mathfrak{m}$ strictly contains at least one minimal prime ideal $\lambda$ and there is no prime ideal strictly in between the two. The maximal ideals of $\mathbb{T}$ correspond bijectively under taking pre-images to the maximal ideals of $\overline{\mathbb{T}}$; the same letter will be used to denote them. The minimal primes $\lambda$ of $\mathbb{T}$ are in bijection with the prime ideals of $\mathbb{T}_{\mathbb{Q}_\ell}$ (all of which are maximal) under extension, for which the notation $\lambda^{(e)}$ will be used. Under the correspondences, one has $\overline{\mathbb{T}}_\mathfrak{m} \cong \mathbb{T}_\mathfrak{m} \otimes \mathbb{F}_\ell$ and $\mathbb{T}_\lambda \cong \mathbb{T}_{\mathbb{Q}_\ell, \lambda^{(e)}}$. By virtue of lifts of idempotents and Proposition 17, we have the local decompositions*

$$\mathbb{T} \cong \prod_\mathfrak{m} \mathbb{T}_\mathfrak{m}, \overline{\mathbb{T}} \cong \prod_\mathfrak{m} \overline{\mathbb{T}}_\mathfrak{m} \text{ and } \mathbb{T}_{\mathbb{Q}_\ell} \cong \prod_\lambda \mathbb{T}_{\mathbb{Q}_\ell, \lambda^{(e)}} \cong \prod_\lambda \mathbb{T}_\lambda,$$

*where $\mathfrak{m}$ runs through the maximal ideals of $\mathbb{T}$ (and $\overline{\mathbb{T}}$) and $\lambda$ runs through the minimal primes of $\mathbb{T}$ (or, equivalently, all the prime=maximal ideals of $\mathbb{T}_{\mathbb{Q}_\ell}$).*

### Package for computing $\ell$-adic decompositions

The second author has developed the MAGMA [BCP97] package PADICALGEBRAS (see [Wie14]) for computing the objects appearing in Proposition 21. The package depends on the second author's earlier MAGMA package ARTINALGEBRAS (see [Wie08]).

The main ingredients are standard linear algebra, especially over finite fields, and the algorithmic idempotent lifting from Corollary 20.

### Application of the commutative algebra to modular forms

Let $S(\mathbb{C})$ be a space of modular forms, e.g. $S_k(\Gamma_1(N))$. We only work with spaces that have a basis with coefficients in $\mathbb{Z}$. We denote by $S(R)$ the corresponding space with coefficients in the ring $R$. Here the notion $S(R)$ is the naive one via the standard $q$-expansion: $S(R)$ is the set of $R$-linear combinations of the image of the $\mathbb{Z}$-basis in $R[[q]]$ via the standard $q$-expansion. The space $S(R)$ can also be characterised as follows. The Hecke operators $T_n$ for $n \in \mathbb{N}$ acting on $S(\mathbb{C})$ generate a ring (a $\mathbb{Z}$-algebra), denoted $\mathbb{T}$, and we have the isomorphism

$$S(R) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, R).$$

Concretely, if $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, R)$, then $\sum_{n\geq 1} \varphi(T_n)q^n$ is a cusp form. Thus a $\mathbb{Z}$-basis of $\mathbb{T}$ gives rise to a 'dual basis' of $S(R)$. We also speak of an 'echelonised basis'.

By Proposition 21, we have the decompositions

$$\mathbb{T}_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T} \cong \prod_{[f]} \mathbb{T}_{[f]} \text{ and } S(\mathbb{Q}) \cong \bigoplus_{[f]} S_{[f]}(\mathbb{Q}),$$

where the product and the sum run over $G_{\mathbb{Q}}$-orbits of Hecke eigenforms. If the space $S(\mathbb{C})$ is a newspace, then $S_{[f]}(\mathbb{Q})$ is the set of forms with coefficients in $\mathbb{Q}$ in the $\mathbb{C}$-span of all the $G_{\mathbb{Q}}$-conjugates of $f$. Concretely, $S_{[f]}(\mathbb{Z})$ is the $\mathbb{Z}$-dual of the $\mathbb{Z}$-algebra generated by the Hecke operators $T_n$ in $\mathbb{T}_{[f]}$. All Hecke operators acting on $S_{[f]}(\mathbb{Z})$ are represented as matrices with $\mathbb{Z}$-entries.

We now consider $\mathbb{T}_{\mathbb{Z}_\ell} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathbb{T}$. Then we have $S(\mathbb{Z}_\ell) = \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T}_{\mathbb{Z}_\ell}, \mathbb{Z}_\ell)$. Importantly, again by Proposition 21, we have the decompositions

$$\mathbb{T}_{\mathbb{Z}_\ell} \cong \prod_{[\overline{f}]} \mathbb{T}_{[\overline{f}]} \text{ and } S(\mathbb{Z}_\ell) \cong \bigoplus_{[\overline{f}]} S_{[\overline{f}]}(\mathbb{Z}_\ell),$$

where the sum and the product run over the $G_{\mathbb{F}_\ell}$-orbits of Hecke eigenforms in $S(\overline{\mathbb{F}}_\ell)$. These correspond to the maximal ideals of $\mathbb{T}_{\mathbb{Z}_\ell}$. We refer to the $S_{[\overline{f}]}(\mathbb{Z}_\ell)$ either as $\mathbb{Z}_\ell$-orbits or as $G_{\mathbb{F}_\ell}$-orbits.

We are also interested in $\mathbb{Q}_\ell$-orbits of eigenforms inside a $\mathbb{Z}_\ell$-orbit. By Proposition 21, $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} S(\mathbb{Z}_\ell) = S(\mathbb{Q}_\ell)$ breaks as a direct sum

$$S(\mathbb{Q}_\ell) \cong \bigoplus_{[\tilde{f}]} S_{[\tilde{f}]}(\mathbb{Q}_\ell),$$

where the sum runs over the $\overline{\mathbb{Q}}_\ell$-valued eigenforms up to $G_{\mathbb{Q}_\ell}$-conjugation. The fact that these $G_{\mathbb{Q}_\ell}$-orbits lie in a single $\mathbb{Z}_\ell$-orbit simply means that they are all congruent modulo a uniformiser.

### Testing weak congruences

The second author has developed the MAGMA package WEAKCONG (see [Wie16]), which has the purpose to compute whether Hecke eigenforms over $\overline{\mathbb{Q}}_\ell$ belong to given $\mathbb{Z}_\ell$-orbits of Hecke eigenforms modulo powers of $\ell$ (or uniformisers). Here we briefly describe how it functions.

Let $n_1, \ldots, n_r$ be indices such that $T_{n_1}, \ldots, T_{n_r}$ form a basis of the Hecke algebra $\mathbb{T}_{\mathbb{Z}_\ell}$ (which we may assume to be local by using the MAGMA package PADICALGEBRAS, see above). We speak of *basis indices*. These indices are computed via Nakayama's lemma, i.e. by reducing the matrices to $\mathbb{F}_\ell$.

For any $n$, we have $T_n = \sum_{i=1}^{r} a_{n,i} T_{n_i}$; in particular, $a_{n_j,i} = \delta_{i,j}$. For each $i \in \{1, \ldots, r\}$, we define a cusp form $f_i$ by specifying its coefficients as follows:

$$a_n(f_i) := a_{n,i}.$$

Then $f_1, \ldots, f_r$ form an $R$-basis of $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T}_{\mathbb{Z}_\ell}, R)$ for any $\mathbb{Z}_\ell$-algebra $R$. We call this basis *echelonised* because it is at the coefficients $n_1, \ldots, n_r$. It is the dual basis with respect to the basis $T_{n_1}, \ldots, T_{n_r}$ of $\mathbb{T}_{\mathbb{Z}_\ell}$.

Furthermore, we compute one $\overline{\mathbb{Q}}_\ell$-eigenform for each $\mathbb{Q}_\ell$-orbit inside the given $\mathbb{Z}_\ell$-orbit. This is done via standard linear algebra over local fields, using both the new MAGMA command LocalField and the older implementation. If we find that a system of linear equations which mathematically must have a solution does not seem to have any, then we lower the precision until the desired solution exists. Thus, in this procedure generally some precision is lost.

Let $g = \sum_{n \geq 1} b_n q^n \in S(\overline{\mathbb{Q}}_\ell)$ be an eigenform in some level and weight. Let $\mathscr{O}$ be the valuation ring of some finite extension of $\mathbb{Q}_\ell$ that contains all coefficients $b_n$ of $g$, and let $\lambda$ be a uniformiser of $\mathscr{O}$. The main purpose of this package is to compute the maximum integer $m$ such that $g$ lies in a given $\mathbb{Z}_\ell$-orbit (some level and some weight) modulo $\lambda^m$.

Put $h := g - \sum_{i=1}^r b_{n_i} f_i$. We then have:

$$h \equiv 0 \mod \lambda^m \Leftrightarrow \exists s_1, \ldots, s_r \in \mathscr{O} : g \equiv \sum_{i=1}^r s_i f_i \mod \lambda^m.$$

This equivalence is clear as the basis is echelonised, whence automatically $s_i \equiv b_{n_i} \mod \lambda^m$ for all $i = 1, \ldots, r$. The desired highest exponent $m$ can thus be computed as the minimum of the valuations of the coefficients of $h$ up to the Sturm bound.

## 6 Database of modular form orbits and higher congruences

The first author has created a PostgreSQL database containing data on $\mathbb{Q}$-, $\mathbb{Q}_\ell$- and $\mathbb{Z}_\ell$-orbits, as well as information on congruences modulo powers of $\ell$. We are currently planning to integrate parts of the database into the LMFDB.[1]

### Technical features

In this section we describe the way our database is organised and what kind of data it contains. This will also highlight two important aspects of our approach:

- We do our best to avoid computing again data that are used more than once. This aims to speed up the process of computing the $G_{\mathbb{Q}_\ell}$-orbits. In order to do this we store a lot of useful information, even intermediate results, e.g. congruences with forms other than those that provide an optimal weight or level, even congruence of individual coefficients.

[1] `http://lmfdb.org`

- We try to parallelise as much of the problem as possible. This also aims at speeding up the computation of congruences. This becomes especially handy when the coefficient fields of the forms that are compared become large.

We will come back to both of these features after the description of the database tables. We list them together with a brief description of the data each one holds.

1. **Modular form spaces over** $\mathbb{Q}$: For every level and weight we store some useful information: The dimension of its Eiseinstein subspace, old cuspidal subspace, new cuspidal subspace as well as the number of new Eisenstein $\mathbb{Q}$-Galois orbits and the number of newform $\mathbb{Q}$-Galois orbits.
2. **Bases of modular form spaces over** $\mathbb{Q}$: Here we store the basis in terms of modular symbols for every space in the previous table. This in Magma readable format.
3. **Eigenforms over** $\mathbb{Q}$: For every space over $\mathbb{Q}$, we store an entry for every Eisenstein and newform $\mathbb{Q}$-Galois orbit uniquely determined my its level, weight and orbit number.
4. **Hecke matrices over** $\mathbb{Z}$: For each of the newform orbits in the previous table we store a list (up to a bound that can be increased as needed) of all the Hecke matrices acting on the $\mathbb{Q}$-subspace spanned by this orbit.
5. **Lattices**: For each of the newform orbits in the $\mathbb{Q}$-eigenforms table, we store a list of base change matrices that ensure the matrices in the table above, after base change, are with respect to the same basis.
6. $\ell$**-adic idempotents**: Given a newform from the $\mathbb{Q}$-eigenforms list and a prime number $\ell$, we store a list of idempotents which provide the decomposition of the corresponding $\ell$-adic Hecke algebra into local factors (see Proposition 21), their number and the $\ell$-adic precision that they were computed in.
7. $\mathbb{F}_\ell$**-Galois orbits**: For each entry in the table above (i.e. a list of idempotents), we store an $\mathbb{Z}$-integral basis for each of the components (indexed by the idempotents in this list) that the parent $\mathbb{Q}$-Galois orbit of newforms breaks into.
8. $\mathbb{Q}_\ell$**-Galois orbits of newforms**: For each $\mathbb{Q}$-Galois orbit of newforms and the prime $\ell$, we store the $\mathbb{Q}_\ell$-Galois orbit of newforms it decomposes into, along with the $\ell$-adic precision they were computed in.

These are the tables that provide a hierarchical organisation of the objects involved in the database and we tried to present it in a top to bottom fashion were an entry in one of these table will be associated with many entries in the ones mentioned after it.

There are some auxiliary tables where all the congruence information is stored. We store everything down to congruences of individual pairs of coefficients. These are detailed catalogs of all meaningful congruences when it comes to level or weight lowering, weak or strong.

It is obvious that the comparison of two eigenvalues at a prime $p$ is independent from the comparison of the ones at some other prime $q$. We thus run a multi-threaded application utilising as many CPU cores as possible where all threads compare a specific pair of eigenvalues each simultaneously. Let us stress here that the design of the database and the multi-threaded application is such that it allows us to utilise

more than one server and/or personal computers to compute even more congruences simultaneously. Extra care has been taken to avoid overlapping of threads, i.e. two of those computing the same congruence, but we choose not to elaborate on these technical matters.

The current size of the database is 488GB. It contains 3906 $\mathbb{Q}$-eigenforms, of level and weight up to 361 and 298 respectively (not of all possible combinations of course).

### Accessibility

We have designed a basic web interface[2] for the database which currently allows one to query the database about the following:

1. Given a $G_{\mathbb{Q}}$-orbit $[f]$ and a prime $\ell$, return $G_{\mathbb{Q}_\ell}$-orbits appearing in it.
2. Given a $G_{\mathbb{Q}}$ orbit $[f]$, a prime $\ell$ and a positive integer $n$, return the $G_{\mathbb{Q}_\ell}$-orbits that are congruent to the ones corresponding to $[f]$ and $\ell$ modulo $\ell^n$ and are of the smallest weight possible, i.e. the answer to the strong weight lowering modulo $\ell^n$ problem for $[f]$.
3. Given a $G_{\mathbb{Q}}$-orbit $[f]$ and a prime $\ell$, return a list of downloadable files (one for each $G_{\mathbb{Q}_\ell}$-orbit) containing all the $\ell$-adic, prime-indexed Hecke polynomials (that are stored in the database) for each $G_{\mathbb{Q}_\ell}$-orbit.

### Some remarks on the algorithms used

We now describe how we computed the various orbits. Our algorithm is implemented in the MAGMA computer algebra system [BCP97]. Assume as input a given level $N$, weight $k$ and prime $\ell$.

1. Compute the newsubspace of the cuspidal subspace of the modular symbols of level $N$ and weight $k$. Decompose this subspace into irreducible Hecke modules. These correspond to $G_{\mathbb{Q}}$-orbits. This is done with standard MAGMA commands.
2. For a given irreducible Hecke module of the previous decomposition, compute the matrices for all operators $T_n$ acting on it up to a sufficient bound $B$.
3. Use the package PADICALGEBRAS [Wie14] to factor the completion of the Hecke algebra at $\ell$ into local factors over $\mathbb{Z}_\ell$. Each of these factors corresponds to a $G_{\mathbb{F}_\ell}$-orbit. Project the matrices representing the $T_n$'s onto each of these local factors.
4. After tensoring with $\mathbb{Q}_\ell$, each of these $G_{\mathbb{F}_\ell}$-orbits is the sum of all the $G_{\mathbb{Q}_\ell}$-orbits admitting the same reduction mod $\ell$. For each such orbit, take the collection of projections of the Hecke matrices onto it computed in the previous step and decompose the corresponding $\mathbb{Q}_\ell$-vector space into simultaneous generalised

[2] `http://math.uni.lu/~tsaknias/elladicdatabase_2.php`

eigenspaces by applying each operator successively. The resulting decomposition is the breaking of the corresponding $G_{\mathbb{F}_\ell}$-orbit into the $G_{\mathbb{Q}_\ell}$-ones that coincide mod $\ell$.

## References


AM12. Rajender Adibhatla and Jayanta Manoharmayum. Higher congruence companion forms. *Acta Arith.*, 156(2):159–175, 2012.

AT15. Rajender Adibhatla and Panagiotis Tsaknias. A characterisation of ordinary modular eigenforms with CM. In *Arithmetic and geometry*, volume 420 of *London Math. Soc. Lecture Note Ser.*, pages 24–35. Cambridge Univ. Press, Cambridge, 2015.

BCP97. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

Böc01. Gebhard Böckle. On the density of modular points in universal deformation spaces. *Amer. J. Math.*, 123(5):985–1007, 2001.

Buz05. Kevin Buzzard. Questions about slopes of modular forms. *Astérisque*, (298):1–15, 2005. Automorphic forms. I.

CKW13. Imin Chen, Ian Kiming, and Gabor Wiese. On modular Galois representations modulo prime powers. *Int. J. Number Theory*, 9(1):91–113, 2013.

CP13. Maximiliano Camporino and Ariel Pacetti. Congruences between modular forms modulo prime powers, 2013.

Deo17. Shaunak V. Deo. Structure of Hecke algebras of modular forms modulo $p$. *Algebra Number Theory*, 11(1):1–38, 2017.

DFG04. Fred Diamond, Matthias Flach, and Li Guo. The Tamagawa number conjecture of adjoint motives of modular forms. *Ann. Sci. École Norm. Sup. (4)*, 37(5):663–727, 2004.

Dum15. Neil Dummigan. Level-lowering for higher congruences of modular forms. `http://neil-dummigan.staff.shef.ac.uk/level18.pdf`, 2015.

Edi92. Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

Eme11. Matthew Emerton. Local-global compatibility in the $p$-adic Langlands programme for $\mathrm{GL}_{2/\mathbb{Q}}$. `http://www.math.uchicago.edu/~emerton/pdffiles/lg.pdf`, 2011.

Kis09. Mark Kisin. The Fontaine-Mazur conjecture for $\mathrm{GL}_2$. *J. Amer. Math. Soc.*, 22(3):641–690, 2009.

KR15. Chandrashekhar Khare and Ravi Ramakrishna. Lifting torsion Galois representations. *Forum Math. Sigma*, 3:e14, 37, 2015.

KRW16. Ian Kiming, Nadim Rustom, and Gabor Wiese. On certain finiteness questions in the arithmetic of modular forms. *J. London Math. Soc.*, 94(2):479–502, 2016.

KW09. Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

Rib90a. Kenneth. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

Rib90b. Kenneth A. Ribet. Raising the levels of modular representations. In *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 259–271. Birkhäuser Boston, Boston, MA, 1990.

Til97. Jacques Tilouine. Hecke algebras and the Gorenstein property. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 327–342. Springer, New York, 1997.

TiVW10. Xavier Taixés i Ventosa and Gabor Wiese. Computing congruences of modular forms and Galois representations modulo prime powers. In *Arithmetic, geometry, cryptography and coding theory 2009*, volume 521 of *Contemp. Math.*, pages 145–166. Amer. Math. Soc., Providence, RI, 2010.

Tsa09. Panagiotis Tsaknias. *On higher congruences of modular Galois representations*. PhD thesis, University of Sheffield, 2009.

Wie07. Gabor Wiese. Multiplicities of Galois representations of weight one. *Algebra Number Theory*, 1(1):67–85, 2007. With an appendix by Niko Naumann.

Wie08. Gabor Wiese. *Magma package ArtinAlgebras*. `http://math.uni.lu/~wiese/programs/ArtinAlgebras`, 2008.

Wie14. Gabor Wiese. *Magma package pAdicAlgebras*. `http://math.uni.lu/~wiese/programs/pAdicAlgebras`, 2014.

Wie16. Gabor Wiese. *Magma package WeakCong*. `http://math.uni.lu/~wiese/programs/WeakCong`, 2016.