Overconvergent Modular Forms, Theoretical and Computational Aspects

Alexandre Johnson

A Thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of
Master of Science (Mathematics) at
Concordia University
Montréal, Québec, Canada

August 2022

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: **Alexandre Johnson**
Entitled: **Overconvergent Modular Forms, Theoretical and Computational Aspects**

and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Mathematics)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.
Signed by the Final Examining Committee:

______________________________ Chair
Dr.Carlo Pagano

______________________________ Thesis Supervisor
Dr. Adrian Iovita

______________________________ Thesis Supervisor
Dr. Giovanni Rosso

Approved by ______________________________
Dr.Yogendra P. Chaubey, Graduate program Director
Department of Mathematics and Statistics

____________ 2022 ______________________________
Dr.Pascale Sicotte, Dean of Faculty
Faculty of Mathematics and Statistics

Abstract

Overconvergent Modular Forms, Theoretical and Computational Aspects
Alexandre Johnson

In this thesis, we perform a review of the theory of overconvergent modular forms, then we explore the distribution of the eigenvalues of the Hecke operator T_p by considering their p-adic valuations. We begin by covering algebraic and geometric definitions of modular forms, then expanding these definitions to overconvergent modular forms. We then introduce algortithms, from "Computations with classical and p-adic modular forms" by Alan G. B. Lauder[6], which provide a method for calculating the p-adic valuations of the aforementioned eigenvalues. In order to implement these algorithms, programs were written for the Sagemath computer algebra program to perform the necessary calculations. These programs were used to collect lists of p-adic valuations, for various values of p and for spaces of modular forms of various weights and of various levels. The collected data confirms the fact that the Gouvea-Mazur conjecture is false, but also indicates that it may be a useful approximation of the true behavior at large weights or at large values of p, at least for the first few slopes. It shows the existence of "plateaus" of weights which have the same slopes, up to the precision used, even at low values of p and k. The reason for the existence of these "plateaus" is unknown.

Acknowledgements

I would like to thank my supervisors Dr.Adrian Iovita and Dr.Giovanni Rosso for their help with all elements of the thesis, as well as Dr.Jan Vonk and David Ayotte for significant help with troubleshooting the Sagemath code used.

Contents

List of Figures

List of Tables

Introduction

The purpose of this thesis is to examine the theoretical aspects of overconvergent modular forms, as well as studying the distribution of the eigenvalues of the Hecke operator applied to these forms.

We begin in section 1 by going over the analytical definition of a modular form of weight k as a function $f : \mathbb{H} \to \mathbb{C}$ with certain conditions. After defining the concept of a q-expansion, we extend the definition by introducing congruence subgroups Γ, and in particular the congruence subgroup $\Gamma_1(N)$, to define modular forms of weight k and level Γ. Once these definitions are in place, we go over the definition of Hecke operators, the main subject of this thesis, as well as Hecke eigenvalues and Hecke eigenvectors.

Subsequently, we move on to define a few related concepts which are important to proofs presented later in the thesis. First, we define and prove the Valence formula for weakly modular forms of weight $k \geq 0$. We then use this to derive another theorem, and finally derive the Sturm bound as a corollary of this theorem. The Sturm bound is then used in section 6 for calculating the Hecke eigenvalues of overconvergent modular forms.

In section 2, we present and prove the Spectral Theorem for compact operators acting on Banach spaces, which will allow us to order the eigenvalues of the Hecke operator by their p-adic valuation later in this thesis.

In section 3, we cover an alternate definition of modular forms, in relation to elliptic curves over schemes, following the method of "p-adic properties of modular schemes and modular forms" by Nicholas M. Katz[5]. We begin by covering the basic definition of modular forms of weight k, though the definition of Katz does not include holomorphicity at ∞, as the definition used in section 1 does, so this requirement was added. We then extend the definition to modular forms with level N structure. However, the level N structure described by Katz is different from the one in section 1. This discrepancy is resolved in section 4, as more groundwork must be covered before it is possible to relate the two definitions, but the upshot is that a modular form of level N "à la Katz" is a level $\Gamma(N)$ form in the sense of section 1.

We then define the modular curve M_k and its normalization $\overline{M}_k$, which we use to extend the definition of modular forms to modular forms of weight k and level $\Gamma(N)$ holomorphic at ∞ with coefficients in K, for any $\mathbb{Z}[\frac{1}{n}]$-module K. Once the definition is extended in this way, we present a base change theorem, which required this extension of the definition. This base change is used in the proof of a necessary lemma in section 5.

In section 4, we make the connection between the two definitions of modular forms we have presented, allowing us to use both definitions interchangeably for the remainder of the thesis.

Section 5 covers overconvergent modular forms themselves, which are the subject of this thesis. We begin by defining ordinary and supersingular elliptic curves, as well as their relation to the Hasse invariant. We then move on to defining overconvergent modular forms proper. The rest of the section consists of examining the structure of the space of overconvergent modular forms more closely in preparation for section 6, as we need to have this structure in order to calculate the eigenvalues. In particular, we develop a decomposition $B(R_0, N, k, a)$ of $M(R_0, N, k)$, where $M(R_0, N, k)$ is the space of modular forms over R_0 of level N and weight k and the relation between them is given by an isomorphism $M\big(R_0, N, k+j(p-1)\big) \cong \bigoplus_{a=0}^{j} B(R_0, N, k, a)$, as well as a direct sum decomposition $H^0\big(\overline{M}_N \otimes_{\mathbb{Z}_p} R_0, \underline{\omega}^{\otimes\, k+(j+1)(p-1)}\big) \cong E_{p-1} \cdot H^0\big(\overline{M}_N \otimes_{\mathbb{Z}_p} R_0, \underline{\omega}^{\otimes\, k+j(p-1)}\big) \bigoplus B(R_0, N, k, j+1)$, both of which are essential for the algorithms in section 6.

Section 6 covers the actual algorithms, from "Computations with classical and p-adic modular forms" by Alan G. B. Lauder[6], that we used to calculate the inverse of the eigenvalues of the Hecke operator. A small modification is made to obtain the p-adic valuations, rather than the inverse of the eigenvalues themselves. The algorithm is split into a level $\Gamma_1(1)$ version and a level $\Gamma_1(N)$, $N \geq 2$ version, as the level $\Gamma_1(1)$ version is both simpler to prove and faster to run on a computer. Given a prime number $p \geq 5$, a weight k and a precision m, the level $\Gamma_1(1)$ algorithm returns the valuations of the inverse of the eigenvalues of the Hecke operator T_p modulo p^m on $M(\mathbb{Z}_p, r, 1, k)$, which is then used to calculate the p-adic valuations of these inverted eigenvalues. The level $\Gamma_1(N)$ version takes an extra input in the form of N, and returns the valuations of the inverse of the eigenvalues of T_p modulo p^m on $M(\mathbb{Z}_p, r, N, k)$). A Sagemath program was developed in order to implement this algorithm, which can be found in the appendix.

Our next step is to prove that these algorithms indeed give the result that we desire. In order to do this, we first prove a version of the algorithm which is modified to be easier to prove, and then we prove that removing these modifications does not change the output of the algorithm, thus proving that the original algorithm is indeed valid. Subsequently, we prove the level $\Gamma_1(N)$ algorithm, but to do this we simply need to prove a slightly modified version of a lemma used in the proof of the level $\Gamma_1(1)$ algorithm, and the rest of the proof follows exactly as in the case of $\Gamma_1(1)$.

Section 7 covers our results and observations. As expected, as the Gouvea-Mazur conjecture is known to be false, we do not consistently get the same set of slopes for weight k and weight $k + (p-1)$. However, one pattern that emerges is that as p increases, the slopes calculated for each subsequent value of k become increasingly comparable. In addition, even at low p-values, for $k+p(p-1)$, there are still certain "plateaus" of k values where the sets of slopes remain comparable, which may be due to the presence of particular congruences.

1 Analytical definition of modular forms

The most basic way to define modular forms is to do it analytically. In order to do so, we first define weakly modular forms as follows.

Definition 1.1:

A weakly modular form of weight k is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ such that $\forall\ \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$, $f(\gamma z) = (cz+d)^k f(z)$, where the action of γ on z is the Mobius transformation, i.e. $\gamma z = \frac{az+b}{cz+d}$.

Another way to define this is via the action of γ on f, rather than on z. We define $|_k\gamma(z)$ by $f|_k\gamma(z) = (cz+d)^{-k} f(\gamma z)$, which one can prove indeed defines an action. It is then clear that an equivalent definition of a weakly modular form of weight k is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ such that $f|_k\gamma = f\ \forall\ \gamma \in SL_2(\mathbb{Z})$.

Now, we define a modular form by looking at how a weakly modular form f acts at infinity. Indeed, we wish to define something that is valid on the full fundamental domain of the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$, $\mathcal{D} =_{SL_2(\mathbb{Z})}\backslash^{\mathbb{H}}$. This is a domain in $\mathbb{C}$ such that no two points in $\mathcal{D}$ are $SL_2(\mathbb{Z})$-conjugate. Note that $SL_2(\mathbb{Z})$ is generated by $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, thus a possible fundamental domain, and the one which we will use, is $\mathcal{D} = \left\{z \in \mathbb{H} : \frac{-1}{2} < \mathrm{Re}(z) \leq \frac{1}{2},\ |z| \geq 1\right\}$.

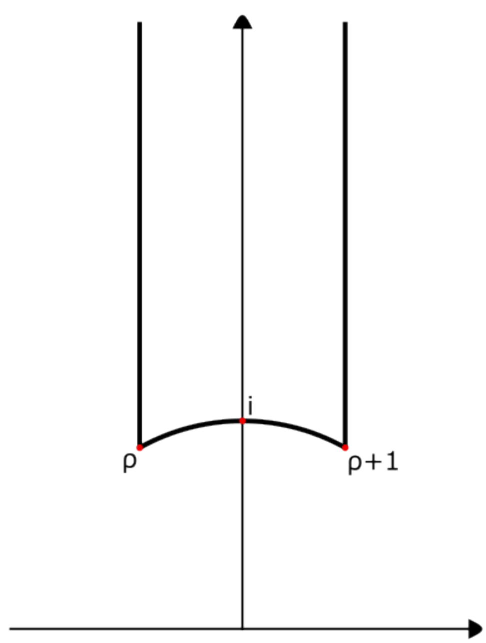

Figure 1: *The fundamental domain for the* $SL_2(\mathbb{Z})$*-action on* $\mathbb{H}$*, plotted on* $\mathbb{H}$*. Note that* $\rho = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ *and* $\rho + 1 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$.

The sides of the domain are given by T, and the arc is given by S. Indeed, from T, we have that $Tz = z+1$. Thus two points will be T-conjugate if they differ by exactly 1, which means that the fundamental domain must have a width of 1 on the real number axis, with only one side of the boundary included, generating the sides of the fundamental domain. Then, from S, we get that $Sz = \frac{-1}{z}$. Now, if $|z| < 1$, then $|\frac{-1}{z}| > 1$ and vice versa. Thus, the fundamental domain can only contain points either inside the circle of radius 1 centered at the origin or outside of the circle, in order to not contain the S-conjugate points. This gives the circle $|z| = 1$ as one of the boundaries of the fundamental domain, which then becomes an arc when intersecting with the lines generated by T.

This domain extends to infinity, so we need to check how f acts at infinity. In order to do this, we first need to define something called the q-expansion. Note that since $f|_k\gamma = f$, we have in particular that $f|_kT = f$. This implies that $f(z+1) = f(z)$, which then implies that f is periodic of period 1, and thus one can prove that $f(z) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i z n} = \sum_{n\in\mathbb{Z}} a_n q^n$ where $q = e^{2\pi i z}$. This is called the q-expansion of f.

Using this q-expansion, we can define what it means for a weakly modular form to be meromorphic, holomorphic or cuspidal at infinity:

Definition 1.2:

A weakly modular form is meromorphic at infinity if $f = \sum_{n>>-\infty} a_n q^n$, i.e. if there is a lower limit on the degree of the terms of its q-expansion.

Definition 1.3:

A weakly modular form is holomorphic at infinity if $f = \sum_{n=0} a_n q^n$, i.e. if there are no terms of negative degree in its q-expansion.

Definition 1.4:

A weakly modular form is cuspidal if $f = \sum_{n=1} a_n q^n$, i.e. if there are no terms of degree ≤ 0 in its q-expansion.

This is what finally allows us to define a modular form of weight k, as follows:

Definition 1.5:

A modular form of weight k is a weakly modular form of weight k which is holomorphic at infinity. We denote the set of all modular forms of weight k by $M(k)$.

Definition 1.6:

A cusp form of weight k is a weakly modular form of weight k which is cuspidal at infinity. We denote the set of all cusp forms of weight k by $S(k)$.

Also, note that since we have defined how the function acts at infinity, we can view the modular form as a function on $\mathbb{H} \cup \{\infty\}$, rather than on $\mathbb{H}$.

A simple example of a modular form, which will be used later in this thesis, is the Eisenstein series $E_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$, where $\sigma_{k-1}(n) = \sum_{d|n,\ d\geq 1} d^{k-1}$ and B_k are the Bernoulli numbers. These can be written as $\frac{1}{2\zeta(k)} \sum_{(m,n)\in\mathbb{Z}\setminus\{(0,0)\}} \frac{1}{(m+nz)^k}$, where $\zeta(k)$ is the Riemann zeta function. Indeed, the first formulation is simply the Fourier series of this second one. It is then trivial to see that for $k > 2$, k even, this is a modular form of weight k.

It is possible, and indeed required for the purposes of this thesis, to extend the definition further by introducing structures called principal subgroups and congruence subgroups. These are defined as follows:

Definition 1.7:

Let $N \geq 1$, $N \in \mathbb{Z}$. Then we define the principal subgroup of level N to be the subgroup $\left\{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod N\right\}$, and we denote it by $\Gamma(N)$.

Definition 1.8:

A congruence subgroup Γ is a subgroup of $SL_2(\mathbb{Z})$ of finite index such that $\exists\ N \geq 1$, $N \in \mathbb{Z}$, s.t. $\Gamma(N) \subseteq \Gamma \subset SL_2(\mathbb{Z})$.

The congruence subgroups relevant to this thesis, other than the principal subgroup itself, are:

$$\Gamma_0(N) = \left\{\gamma \in SL_2(\mathbb{Z}) :\ \gamma \equiv \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mod N\right\}.$$

and

$$\Gamma_1(N) = \left\{\gamma \in SL_2(\mathbb{Z}) :\ \gamma \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \mod N\right\}.$$

Congruence subgroups allow us to define weakly modular forms of weight k and level Γ where Γ is any congruence subgroup, as follows:

Definition 1.9:

A weakly modular form of weight k and level Γ is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ such that $f|_k\gamma = f\ \forall\ \gamma \in \Gamma$. Denote the space of weakly modular forms of weight k and level Γ by $m(\Gamma, k)$.

Note that this is a weaker condition than the original definition of weakly modular forms, as

Γ is contained within $SL_2(\mathbb{Z})$, thus extending the definition of weakly modular forms. However, as the fundamental domain of the action of Γ may not be the same as the fundamental domain of the action of $SL_2(\mathbb{Z})$, we need to examine how weakly modular forms act on this new fundamental domain in order to define our extended version of holomorphicity at ∞. To do this, we need to define the new fundamental domain. This is done in Prop 1.10, mentioned in the discussion immediately following the proof of corollary 2.3.5 in [9]:

Prop 1.10:

Let Γ be a congruence subgroup and let $\{\gamma_i\}_{i=1}^n$ be a set of representatives for $SL_2(\mathbb{Z})/\Gamma$. Then every $z \in \mathbb{H}/\Gamma$ has a representative in $\mathcal{D}_\Gamma = \bigcup_{i=1}^{n} \gamma_i \mathcal{D}$.

This shows that $\mathcal{D}_\Gamma$ is the fundamental domain of the action of Γ on $\mathbb{H}$, and that it is indeed not the same as the fundamental domain of the action of $SL_2(\mathbb{Z})$. We can even choose the $\{\gamma_i\}_{i=1}^n$ such that $\mathcal{D}_\Gamma$ is connected. This means that infinity may not be the only limit point of the fundamental domain, thus to define meromorphic, holomorphic and cuspidal, we must address these points. We call these limit points "cusp points". The set of all cusp points of a given congruence subgroup Γ, Cusp(Γ), is ${}_{\Gamma}\backslash^{SL_2(\mathbb{Z})}/_{\Gamma_\infty}$, where $\Gamma_\infty = \mathrm{Stab}_{SL_2(\mathbb{Z})}(\infty)$. Indeed, this means that to calculate Cusp(Γ), we take the modulus with respect to the set of matrices that go to infinity as z goes to infinity, and so we are left with only the ones which converge to a point other than infinity. Then we take the modulus with respect to Γ to make sure we stay inside the fundamental domain.

For this construction, defining meromorphic, holomorphic and cuspidal at infinity is no longer sufficient. Rather, these must now be defined on the cusps of the weakly modular form.

Definition 1.11:

Let f be a weakly modular form of weight k and level Γ. Let c be a cusp of Γ. Note that c is a class since Cusp(Γ) is a quotient group. Then we say:

- f is meromorphic at c if $f|_k\gamma_t$ is meromorphic at ∞, where t is a representative of the class c, $t \in \mathbb{Q} \cup \{\infty\}$, and γ_t is defined such that $\gamma_t \infty = t$.
- f is holomorphic at c if $f|_k\gamma_t$ is holomorphic at ∞, where t is a representative of the class c.
- f is cuspidal at c if $f|_k\gamma_t$ is cuspidal at ∞, where t is a representative of the class c.

Now that we have extended our definition of holomorphicity, we can also extend our definition of modular forms:

Definition 1.12:

A modular form of weight k and level Γ is a weakly modular form of weight k and level Γ which is holomorphic at all cusps of Γ. Denote the space of modular forms of weight k and level Γ by $M(\Gamma, k)$.

Definition 1.13:

A cusp form of weight k and level Γ is a weakly modular form of weight k and level Γ which is cuspidal at all cusps of Γ.

We must now define the Hecke operators themselves, in order to then define the Hecke eigenvalues which are the focus of this thesis. In order to do so, however, double cosets must first be defined:

Definition 1.14:

Let Γ_1 and Γ_2 be two congruence subgroups and let $\gamma \in GL_2(\mathbb{Q})^+ \cap M_2(\mathbb{Z})$ where $M_2(\mathbb{Z})$ are the 2x2 matrices with entries in $\mathbb{Z}$. Then we define the double coset to be $\{\gamma_1 \ \gamma \ \gamma_2 : \gamma_1 \in \Gamma_1 \ and \ \gamma_2 \in \Gamma_2\}$, and we denote it as $[\Gamma_1\gamma\Gamma_2]$. Further, note that $[\Gamma_1\gamma\Gamma_2] = \bigcup\limits_j \Gamma_1\alpha_j$ where α_j are the representatives of $\Gamma_1 \setminus \Gamma_1\gamma\Gamma_2$. We define the corresponding double coset operator from $M(\Gamma_1, k)$ to $M(\Gamma_2, k)$ as $f|_k\Big[\Gamma_1\gamma\Gamma_2\Big] = \sum\limits_{\alpha_j} f|_k\alpha_j$.

Definition 1.15:

The Hecke operators are defined as $T_\gamma := \big[\Gamma\gamma\Gamma\big]$ for Γ a congruence subgroup. This thesis will only require Hecke operators of level $\Gamma_1(N)$, i.e. Hecke operators of the form $T_\gamma := \big[\Gamma_1(N)\gamma\Gamma_1(N)\big]$. In particular, there are two important special cases of the Hecke operator. These are:

$T_p := \frac{1}{p}T_{\left[\begin{array}{cc} 1 & 0 \\ 0 & p \end{array}\right]}$ for p a prime number

and

$< d >:= T_{\gamma_d}, \, \gamma_d = \left[\begin{array}{cc} a & b \\ c & d \end{array}\right] \in \Gamma_0(N)$ for $d \in \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^X$.

Examining the structure of the Hecke eigenvalue more deeply, we immediately see that:

$$\left[\Gamma_1(N)\left[\begin{array}{cc} 1 & 0 \\ 0 & p \end{array}\right]\Gamma_1(N)\right] = \begin{cases} \bigcup\limits_{j=0}^{p-1} \Gamma_1(N)\beta_j & \text{if } p|N \\ \bigcup\limits_{j=0}^{p-1} \Gamma_1(N)\beta_j \bigcup \Gamma_1(N)\beta & \text{if } p \nmid N \end{cases},$$

where $\beta_j = \left[\begin{array}{cc} 1 & j \\ 0 & p \end{array}\right]$, $\beta = \left[\begin{array}{cc} 1 & 0 \\ 0 & p \end{array}\right]\left[\begin{array}{cc} ap & 1 \\ cN & 1 \end{array}\right]$, $cN \equiv -1 \mod p$ and a is some integer such that $\left[\begin{array}{cc} ap & 1 \\ cN & 1 \end{array}\right] \in SL_2(\mathbb{Z})$.

This gives, for example, that for N=46:

$$T_{23} = \frac{1}{23}\bigcup_{j=0}^{22}\Gamma_1(46)\begin{bmatrix} 1 & j \\ 0 & 23 \end{bmatrix}$$

and

$$T_{29} = \frac{1}{29}\bigcup_{j=0}^{28}\Gamma_1(46)\begin{bmatrix} 1 & j \\ 0 & 29 \end{bmatrix}\bigcup\Gamma_1(46)\begin{bmatrix} 1 & 0 \\ 0 & 29 \end{bmatrix}\begin{bmatrix} 29a & 1 \\ 46c & 1 \end{bmatrix}.$$

This leads to the definition of a Hecke eigenvalue and a Hecke eigenvector. A Hecke eigenvector of a particular Hecke operator T_p, p prime, is defined as a modular form $f \in M(\Gamma_1(N), k)$ such that $T_p f = \lambda_p f$, where λ_p is the Hecke eigenvalue of f. A Hecke eigenform f is a simultaneous Hecke eigenvector for all values of p s.t. there exists a character $\chi : (\frac{\mathbb{Z}}{N\mathbb{Z}})^\times \to \mathbb{C}^\times$ s.t. $< d > f = \chi(d)f$. In the rest of the thesis, when we refer to Hecke operators, we mean only the ones of the form T_p, p prime.

Finally, the action of the of the Hecke operator on the q-expansion of a modular form is as follows:

Definition 1.16:

If f is a modular form of weight k and level $\Gamma_1(N)$, with q-expansion $f = \sum\limits_{n=0} a_n q^n$, then:

$$T_p f = \begin{cases} \sum\limits_{n=0}^{\infty}\left(a_{pn} + p^{k-1}a_{\frac{n}{p}}(< p > f)\right)q^n & \text{if } p \nmid N \\ \sum\limits_{n=0}^{\infty} a_{pn}q^n & \text{if } p|N \end{cases}.$$

We now need to define a few concepts that are related to modular forms, which will be used later in this thesis. The first thing we will define is the Sturm bound, but in order to define this, we must use the Valence Formula:

Theorem 1.17 (Valence Formula):

Let $f \neq 0$ be a weakly modular form of weight $k \geq 0$, meromorphic on $\mathbb{H} \cup \{\infty\}$. Then $\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum\limits_{w \in W}\mathrm{ord}_w(f) = \frac{k}{12}$ where $W = \left[SL_2(\mathbb{Z}) \setminus \mathbb{H}\right] \setminus \{i, \rho\}$.

Proof:

We will use Cauchy's "argument principal" to prove this. Recall that the "argument principal" states that if we have a function f holomorphic on $C \subset \mathbb{C}$, where C is a domain inside $\mathbb{C}$, then $\int\limits_{\partial C}\frac{f'(z)}{f(z)}dz = 2\pi i \sum\limits_{z \in Int(C)}\mathrm{ord}_z(f)$, where $\mathrm{ord}_z(f) = \mathtt{residue}_z(\frac{f'}{f})$.

We will perform a contour integral around the fundamental domain and apply the "argument principal", and see that this will immediately result in the desired equation.

First, we set up the contour in the following diagram:

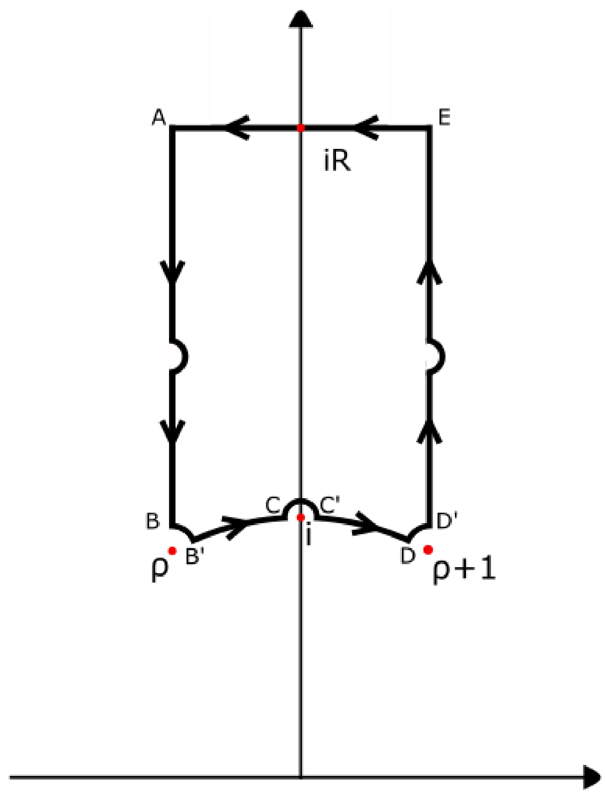

Figure 2: *The contour* e *over which we will perform our integration. Note that* ρ *is defined as usual for this fundamental domain.* $R > 1$ *is chosen arbitrarily as some upper bound in order to close the loop. The curves on the vertical paths are simply examples to indicate that any poles or zeros on the contour are avoided.*

Avoiding the points at i, ρ and $\rho + 1$, as well as avoiding any other pole or zero x on the boundary, we ensure that we have no zeros or poles on the contour, and that we can extract the orders of i, ρ and $\rho + 1$ later. Note that for the possible poles or zeros x, we circle them and their corresponding point on the other side in opposite directions, in order for them to cancel out.

Now, calculate the contour integral:

First, compare $\int\limits_{A}^{B}$ and $\int\limits_{D'}^{E}$:

Applying the change of variables $z \to z - 1$ to $\int\limits_{D'}^{E} \frac{f'(z)}{f(z)} dz$ gives the equation

$\int\limits_{D'}^{E} \frac{f'(z)}{f(z)} dz = \int\limits_{B}^{A} \frac{f'(z-1)}{f(z-1)} dz = -\int\limits_{A}^{B} \frac{f'(z)}{f(z)} dz$, so these two parts of the integral cancel out.

Now, compare $\int\limits_{C'}^{D}$ and $\int\limits_{C}^{B'}$:

Start with $\int\limits_{C'}^{D} \frac{f'(z)}{f(z)} dz$, then apply the change of variables $z \to \frac{-1}{z}$. Note that this maps $\int\limits_{C'}^{D}$ to $\int\limits_{C}^{B'}$.

This implies that $\int_{C'}^{D} \frac{f'(z)}{f(z)}dz = \int_{C}^{B'} \frac{1}{z^2}\frac{f'(\frac{-1}{z})}{f(\frac{-1}{z})}$, but note that $f(\frac{-1}{z}) = z^k f(z)$, as $\frac{-1}{z} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} z$, so $(cz+d)^k = z^k$. This then means that $z^{-2}f'(\frac{-1}{z}) = kz^{k-1}f(z) + z^k f'(z)$, and so we have $\frac{f'(\frac{-1}{z})}{z^2 f(\frac{-1}{z})} = \frac{k}{z} + \frac{f'(z)}{f(z)}$.

So:

$$\begin{aligned}
\int_{C'}^{D} \frac{f'(z)}{f(z)}dz &= \int_{C}^{B'} \frac{1}{z^2}\frac{f'(\frac{-1}{z})}{f(\frac{-1}{z})} \\
&= -\int_{B'}^{C} \frac{f'(z)}{f(z)}dz + \int_{C}^{B'} \frac{k}{z}dz \\
&= -\int_{B'}^{C} \frac{f'(z)}{f(z)}dz + k \int_{30\ degrees} \frac{1}{z}dz, \text{ since the arc of the section } C \text{ to } B' \text{ is 30 degrees} \\
&= -\int_{B'}^{C} \frac{f'(z)}{f(z)}dz + \frac{k2\pi i}{12} \\
&= -\int_{B'}^{C} \frac{f'(z)}{f(z)}dz + \frac{k\pi i}{6}.
\end{aligned}$$

Which finally gives $\int_{C'}^{D} \frac{f'(z)}{f(z)}dz + \int_{B'}^{C} \frac{f'(z)}{f(z)}dz = \frac{k\pi i}{6}$ by reordering.

Now, for $\int_{B}^{B'} \frac{f'(z)}{f(z)}dz$, the integral is around ρ and the angle is 60 degrees, so $\int_{B}^{B'} \frac{f'(z)}{f(z)}dz = \frac{-2\pi i}{6}\text{ord}_\rho(f)$
$= \frac{-\pi i}{3}\text{ord}_\rho(f)$.

Now, for $\int_{C}^{C'} \frac{f'(z)}{f(z)}dz$, the integral is around i and the angle is 180 degrees, so $\int_{C}^{C'} \frac{f'(z)}{f(z)}dz = -\pi \ \text{ord}_i(f)$.

Now, for $\int_{D}^{D'} \frac{f'(z)}{f(z)}dz$, the integral is around ρ and the angle is 60 degrees, so $\int_{D}^{D'} \frac{f'(z)}{f(z)}dz = \frac{-2\pi i}{6}\text{ord}_{\rho+1}(f)$
$= \frac{-\pi i}{3}\text{ord}_\rho(f)$.

Finally, for at ∞:

$\frac{f'(z)}{f(z)} = 2\pi i q \frac{f'(z)}{f(z)}$, $q = e^{2\pi i z}$ and $dq = q\ dz$, so $\int_{E}^{A} \frac{f'(z)}{f(z)}dz$ becomes $-\left(\int_{|q|=e^{-2\pi R}} \frac{f'(q)}{f(q)}dq\right)$, which is equal to $-2\pi i\ \text{ord}_\infty(f)$, under the change of variables $z \to q$, as R goes to infinity.

Thus, adding all of these together, we get:
$\int_{e} \frac{f'(z)}{f(z)}dz = \frac{k\pi i}{6} - \pi i\ \text{ord}_i(f) - \frac{2\pi i}{3}\text{ord}_\rho(f) - 2\pi i\ \text{ord}_\infty(f)$.

But now we can apply the "argument principal", to obtain $\int \frac{f'(z)}{f(z)}dz = 2\pi i \sum_{w \in \text{Int}(e)} \text{ord}_w(f)$. Note that we do not have to restrict w to only the poles or zeros, as other points will necessarily have an order of 0, and thus will not affect the result.

Applying this gives $2\pi i \sum\limits_{w\in \mathrm{Int}(e)} \mathrm{ord}_w(f) = \frac{k\pi i}{6} - \pi i \mathrm{ord}_i(f) - \frac{2\pi i}{3}\mathrm{ord}_\rho(f) - 2\pi i \mathrm{ord}_\infty(f)$, which then implies that $\frac{k}{12} = \sum\limits_{w\in W} \mathrm{ord}_w(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \mathrm{ord}_\infty(f)$ as we let $R \to \infty$.

Q.E.D.

This then allows us to prove the following theorem:

Theorem 1.18:

$M(k)$ are finite dimensional vector spaces, and $\dim\big(M(k)\big) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2 \bmod(12) \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \not\equiv 2 \bmod(12) \end{cases}$.

Proof:

First, for $k = 0, ..., 10$, we immediately have:

$\dim\big(M(0)\big) = 1$;
$\dim\big(M(2)\big) = 0$;
$\dim\big(M(4)\big) = 1$ (only E_4);
$\dim\big(M(6)\big) = 1$ (only E_6);
$\dim\big(M(8)\big) = 1$ (only E_4^2 and E_8, which are scalar multiples of each other);
$\dim\big(M(10)\big) = 1$ (only E_6E_4 and E_{10}, which are scalar multiples of each other).

Also, $\dim\big(S(k+12)\big) = \dim\big(M(k)\big)$, as they are in fact isomorphic under the isomorphism $\begin{array}{l} M(k) \to S(k+12) \\ \quad f \mapsto \Delta f \end{array}$ where $\Delta = \frac{(204E_4)^3-(504E_6)^2}{1728}$.

We are only left to prove that $\dim\big(M(k+12)\big) = \dim\big(S(k+12)\big) + 1$:

Consider the map: $\begin{array}{l} M(k+12) \to \mathbb{C}. \\ \sum\limits_{n=0}^{\infty} a_n q^n \mapsto a_0 \end{array}$

The kernel of this map is immediately $S(k+12)$, because it implies that $a_0 = 0$. Further, this map is surjective, because a_0 can have any value in $\mathbb{C}$. Thus:

$$\dim\big(M(k+12)\big) = \dim(kernel) + \dim(image) = \dim\big(S(k+12)\big) + \dim(\mathbb{C}) = \dim\big(S(k+12)\big) + 1,$$

and this thus allows us to calculate the dimension recursively:

$$\begin{aligned} \dim\big(M(k)\big) = \dim\big(S(k)\big) + 1 = \dim\big(M(k-12)\big) + 1 = \dim\big(S(k-12)\big) + 2 &= \dim\big(M(k-24)\big) + 2 \\ &= ... \\ &= \dim\big(M(k-12\lfloor \tfrac{k}{12} \rfloor)\big) + \lfloor \tfrac{k}{12} \rfloor. \end{aligned}$$

But $\dim\big(M_{k-12\lfloor \frac{k}{12} \rfloor}\big) = \begin{cases} 0 & \text{if } k \equiv 2 \bmod(12) \\ 1 & \text{if } k \not\equiv 2 \bmod(12) \end{cases}$, so $\dim\big(M(k)\big) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2 \bmod(12) \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \not\equiv 2 \bmod(12) \end{cases}$.

Q.E.D.

As a corollary of that theorem, we finally obtain the Sturm bound:

Corollary 1.19 (Sturm bound):

Let $f \in M(k)$ such that $f = \sum_{n=0}^{\infty} a_n q^n$ and $a_n = 0$ for $n = 0, 1, ..., \lfloor \frac{k}{12} \rfloor$. Then $f = 0$, and we call $\lfloor \frac{k}{12} \rfloor$ the Sturm bound.

There is also an extension of the Sturm bound which takes into account congruence subgroups, which is as follows:

Theorem 1.20 (Sturm bound)[1]:

Let $f \in M(\Gamma, K)$ such that $f = \sum_{n=0}^{\infty} a_n q^n$, let m be the index of Γ in $SL_2(\mathbb{Z})$ and let $a_n = 0$ for $0 \leq n \leq \lfloor \frac{km}{12} \rfloor$. Then $f = 0$, and we call $\lfloor \frac{km}{12} \rfloor$ the sturm bound.

2 Spectral Theorem

In this section, we will introduce the spectral theorem for compact operators acting on Banach spaces, which will allow us to order the eigenvalues of T_p by their p-adic valuations. In order to do this, we first need the following definitions and theorems. Note that the Banach spaces in this section are Banach spaces over a non-archimedian field:

Definition 2.1 [8]:

A compact operator $A : X \to Y$ is a specific type of linear operator between normed vector spaces X and Y with the added condition that it belongs to the closure of the subspace of continuous linear maps from X to Y of finite rank.

Definition 2.2 [8]:

A Banach space X is a normed vector space which is also complete, i.e. every Cauchy sequence in X converges to a point in X.

Definition 2.3 [8]:

Let A be a compact endomorphism operator acting on a Banach space X over a non-archimedian space K. If $|A| \leq 1$, then the Fredholm determinant is defined as follows:

Let X_0 be the set of $x \in X$ s.t. $|x| \leq 1$. Let R be the valuation ring of K, let $\mathfrak{m}$ be the maximal ideal of R, and let r be a non-zero ideal of R contained in $\mathfrak{m}$. Finally, let $X_a = \frac{X_0}{rX_0}$. Passing to the quotient, A defines an endomorphism A_r of X_r.

$\det(I - tA_r)$ is well defined, as the image of A_r is contained in a submodule of finite type of X_r, and has coefficients in $\frac{K}{r}$. We define the Fredholm determinant to be the projective limit of these determinants, $\det(I - tA) = \varprojlim_{r} \det(I - tA_r)$.

If $|A| > 1$, we simply choose a scalar c such that $|cA| \leq 1$, which allows us to define $\det(I - tcA)$, which then defines $\det(I - tA)$.

This then allows us to define the Fredholm resolvent:

Definition 2.4 [8]:

Let A be a compact operator acting on a Banach space X. For a Fredholm determinant $\det(I - tA) = \sum_{m=0}^{\infty} c_m t^m$, the Fredholm resolvent is defined as $P(t, A) = \frac{\det(I-tA)}{I-tA} = \sum_{m=0}^{\infty} \nu_m t^m$ where ν_n is defined by: $\nu_0 = I,\ \nu_n = c_n + A\nu_{n-1}$.

The last definition we will need is the following:

Definition 2.5:

Let X and Y be Banach spaces. Define $\mathcal{K}(X, Y)$ to be the vector space of continuous linear operators from X to Y.

Beyond these definitions, we need the following:

Theorem 2.6 [8, Prop 12]:

Let A be a compact endomorphism operator acting on a Banach space X. If we have a zero a of order h of the Fredholm determinant $\det(I - tA)$, then there exists a unique direct sum decomposition of X into closed stable subspaces:

$$X = N(a) + F(a)$$

Where:

1) $(I - aA)^n = 0$ for some n, over $N(a)$;
2) $(I - aA)^n$ is invertible over $F(a)$;
3) $\dim(N(a)) = h$.

Finally, we need the following proposition, and more specifically we need a fact that we can derive from this proposition:

Prop 2.7 [8, Prop 10]:

Let A be a compact operator acting on a Banach space X. The Fredholm resolvent $P(t, A)$ is the entire function of t with values in $\mathcal{K}(X, X)$. More precisely, for any real number M, we have $\lim_{n\to\infty} |\nu_n| M^n = 0$.

This proposition implies that $\lim_{n\to\infty} |\nu_n| M^n = \lim_{n\to\infty} |c_n + A\nu_{n-1}| M^n = \lim_{n\to\infty} |c_n + Ac_{n-1} + A^2 c_{n-2} + ... + A^{n-1}c_1 + A^n| M^n = 0$, and so, choosing $M = p$, we find that the coefficients c_n go to zero faster than any polynomial in p, which is the result that we will need.

Now, we are prepared to prove the spectral theorem:

Theorem 2.8 (Spectral Theorem):

Let A be a compact operator acting on a Banach space X. Then for any constant D, there are only finitely many zeros of $\det(I - tA)$ with Newton slope smaller than D.

Proof:

Assume by contradiction that we have infinitely many zeros of $\det(I - tA)$ with slope $< D$.

Now, by Theorem 2.6, we have that $(I - aA)^n = 0$ for some n, over $N(a)$, which implies that A has only eigenvalues a^{-1} on $N(a)$, and thus that $N(a)$ is made up of all generalized eigenvectors for a^{-1}.

By doing this for each $a \in \{\text{zeros of } \det(I - tA) \text{ with slope} < D\}$, we get an infinite amount of eigenvectors with eigenvalues a^{-1}.

We then use these to start constructing the characteristic series of A:

$\mathrm{Char}(A) = (1 - a_1^{-1}A)^{n_1}(1 - a_2^{-1}A)^{n_2}....$

But, since $\mathrm{slope}(a_i) < D \ \forall \ a_i$, we have, truncating the series to some integer m:
$(1 - a_1^{-1}A)^{n_1}...(1 - a_m^{-1}A)^{n_m} > (1 - p^{-D}A)^{n_1}...(1 - p^{-D}A)^{n_m}$,

which implies that the coefficients of the characteristic series do not go to zero faster than any polynomial in p, but this contradicts Prop 2.7, so for any constant D, there are only finitely many zeros of $\det(I - tA)$ with slope smaller than D.

Q.E.D.

This theorem is applied to the Hecke operator T_p, which is compact, acting on the space of overconvergent modular forms $M(R_0, r, N, k)$, which can be viewed as a Banach space over $\mathbb{Q}_p$. The structure of $M(R_0, r, N, k)$ is explored further in section 5.

3 Geometric definition of modular forms

A second way to define modular forms, found in "P-adic Properties of Modular Schemes and Modular Forms" by Nicholas M. Katz [5], is to define them with respect to elliptic curves over schemes.

Let S be any scheme. Then an elliptic curve over a scheme S is a proper smooth morphism of schemes $p : E \to S$ which is finitely presented, proper and flat, together with a section $O \in E(S)$ such that the geometric fibres, together with the points obtained by specializing O, are elliptic curves in the usual sense, i.e. as defined over algebraically closed fields.

Let E be any elliptic curve over S. Denote by $\underline{\omega}_{E/S}$ the invertible sheaf $p_*(\Omega^1_{E/S})$, and let $\Omega^1_{E/S}$ be the cotangent space. Then we define modular forms as follows.

Definition 3.1:

A weakly modular form f of weight k and level 1 is a rule $f : E/S \mapsto f(E/S)$ such that, for any elliptic curve E/S over any scheme S, $f(E/S)$ is a section of $(\underline{\omega}_{E/S})^{\bigotimes k}$ over S and such that:

1) $f\big(E/S\big)$ is stable with respect to the S-isomorphism classes of E/S. i.e. if $E/S \cong E'/S$, then $f\big(E/S\big) = f\big(E'/S\big)$;

2) Any change of basis $g : S' \to S$ commutes with f, i.e. $f\big(E_{S'}/S'\big) = g^* f\big(E/S\big)$.

We denote the space of weakly modular forms of weight k and level 1 by $m(k)$.

An equivalent definition, also presented in "P-adic Properties of Modular Schemes and Modular Forms" is:

Definition 3.2[5]:

A weakly modular form of weight k and level 1 is a rule $f : (E/R, \omega) \mapsto f(E/R, \omega)$ such that, for any 2-tuple $(E/R, \omega)$ where E/R is an elliptic curve over some ring R and ω is a basis of $\underline{\omega}_{E/S}$, $f(E/R, \omega)$ is an element of R and such that:

1)$f\big(E/R, \omega\big)$ is stable with respect to the R-isomorphism classes of $\big(E/R, \omega\big)$. i.e. if $\big(E/R, \omega\big) \cong \big(E'/R, \omega'\big)$, then $f\big(E/R, \omega\big) = f\big(E'/R, \omega'\big)$;

2)$f\big(E, \lambda\omega\big) = \lambda^{-k} f\big(E, \omega\big)\ \forall\ \lambda \in R^\times$;

3)Any extension of scalars $g : R \to R'$ commutes with f, i.e. $f\big(E_{R'}/R', \omega_{R'}\big) = g\Big(f\big(E/R, \omega\big)\Big)$.

We denote the space of weakly modular forms of weight k and level 1 by $m(k)$.

The correspondence between these two definitions stems from the equation $f(E/S) = f(E/R, \omega) \cdot \omega^{\bigotimes k}$, which is obtained as follows:

First, assume S is affine, i.e $S = \mathsf{Spec}(R)$ for some ring R, and define ω to be an invariant differential of $\underline{\omega}_{E/S}$. Then, from the elliptic curve E/S, we have a Weierstrass equation:

$E/S : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$, Where $a_1, \ ..., a_6 \in \mathcal{O}_S(S) = R$.

Rewriting this equation in the coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ gives the equation

$E/S : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Then, by [9, Prop III.1.5], we have that the invariant differential associated to a Weierstrass equation for E/S is holomorphic and non-vanishing, which means that any two invariant differentials of E/S, generated by two different Weierstrass equations, must differ only by scaling. For example, if $\mathsf{Char}(R) \neq 2$, then the invariant differential, up to scaling, is $\frac{dx}{y}$. This implies that E/S has only one invariant differential, up to scaling, and so that $\underline{\omega}_{E/S}$ is of rank 1. Thus, any section of $\underline{\omega}_{E/S} = \underline{\omega}_{E/\mathsf{Spec}(R)}$ can be written as a multiple of ω which depends on ω and on E/R. Furthermore, this also holds when taking tensor product, so that any section of $\left(\underline{\omega}_{E/\mathsf{Spec}(R)}\right)^{\bigotimes k}$ can be written as a multiple of $\omega^{\bigotimes k}$ which depends on ω and on E/R.

Now, note that $f(E/\mathsf{Spec}(R))$ is a section of $(\underline{\omega}_{E/\mathsf{Spec}(R)})^{\bigotimes k}$ by definition. This implies that $f(E/\mathsf{Spec}(R)) = f(E/R, \omega) \cdot \omega^{\bigotimes k}$, and so we have obtained the desired correspondence in the affine case.

Finally, if S is not affine, then it has an affine cover, so locally this equation still holds and we get the desired correspondence.

Now, we need to define the q-expansion, as we did in section 1. In order to do so, we restrict to schemes S lying over a fixed ring R_0, and for the base change property, we only consider base changes which are R_0-morphisms.

Definition 3.3:

Let $\mathsf{Tate}(q)$ be the Tate curve, i.e. the curve over $\mathbb{Z}[[q]]$ given by $y^2 + xy = x^3 + a_4x + a_6$ where $a_4 = 5\sum_n \frac{-n^3q^n}{1-q^n}$ and $a_6 = \sum_n \frac{-(7n^5+5n^3)q^n}{12(1-q^n)}$, and let $\omega_{can} = \frac{dx}{2y+x}$, the canonical differential of the Tate curve. Then we define the q-expansion of a weakly modular form F of weight k to be the Laurent series of $f\Big(\big(\mathsf{Tate}(q), \omega_{can}\big)_{R_0}\Big)$, i.e. q-expansion $= f\Big(\big(\mathsf{Tate}(q), \omega_{can}\big)_{R_0}\Big) = \sum a_nq^n$. Note that the subscript by R_0 simply means that we base change the Tate curve to this ring.

This allows us to define holomorphicity at ∞:

Definition 3.4:

A weakly modular form f of weight k is holomorphic at ∞ iff $f\Big(\big(\mathsf{Tate}(q), \omega_{can}\big)_{R_0}\Big) \in \mathbb{Z}[[q]] \bigotimes_{\mathbb{Z}} R_0$.

Which finally allows us to define modular forms:

Definition 3.5:

A modular form of weight k is a weakly modular form of weight k which is holomorphic at ∞. We denote the space of modular forms of weight k by $M(k)$.

Now, we can extend the definition of modular forms by adding a "level N structure". For weakly modular forms of level N, the definition is almost the same as the one previously stated, simply with an extra condition added.

Definition 3.6:

Define a level N structure on E/S to be an isomorphism $\alpha_N : E[N] \to \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^2_S$. A weakly modular form of weight k and level N is then a rule f such that for any 2-tuple $\big(E/S, \alpha_N\big)$ where E is an elliptic curve over a scheme S and α_N is a level N structure, $f(E/S, \alpha_N)$ is a section of $(\underline{\omega}_{E/S})^{\bigotimes k}$ which satisfies the same conditions as before, i.e. such that:

1) $f\big(E/S, \alpha_N\big)$ is stable with respect to the S-isomorphism classes of $\big(E/S, \alpha_N\big)$. i.e. if $\big(E/S, \alpha_N\big) \cong \big(E'/S, \alpha'_N\big)$, then $f\big(E/S, \alpha_N\big) = f\big(E'/S, \alpha'_N\big)$;

2) Any change of basis $g : S' \to S$ commutes with f, i.e. $f\big(E_{S'}/S', (\alpha_N)_{S'}\big) = g^* f\big(E/S, \alpha_N\big)$.

We denote the space of weakly modular forms of weight k and level N by $m(N, k)$.

The equivalent definition still holds as well, with the same modification:

Definition 3.7:

A weakly modular form of weight k and level N is a rule f such that for any triple $\big(E/R, \omega, \alpha_N\big)$ where E is an elliptic curve over a ring R, ω is a basis of $\underline{\omega}_{E/S}$ and α_N is a level N structure, $f\big(E/R, \omega, \alpha_N\big)$ is an element of R such that:

1)$f\big(E/R, \omega, \alpha_N\big)$ is stable with respect to the R-isomorphism classes of $\big(E/R, \omega, \alpha_N\big)$. i.e. if $\big(E/R, \omega, \alpha_N\big) \cong \big(E'/R, \omega', \alpha'_N\big)$, then $f\big(E/R, \omega, \alpha_N\big) = f\big(E'/R, \omega', \alpha'_N\big)$;

2)$f\big(E, \lambda\omega, \alpha_N\big) = \lambda^{-k} f(E, \omega, \alpha_N)\ \forall\ \lambda \in R^\times$;

3)Any extension of scalars $g : R \to R'$ commutes with f, i.e. $f\big(E_{R'}/R', \omega_{R'}, (\alpha_N)_{R'}\big) = g\Big(f\big(E/R, \omega, \alpha_N\big)\Big)$.

We denote the space of weakly modular forms of weight k and level N by $m(N, k)$.

Finally, exactly as in the previous definition, in order to define the q-expansions, we restrict to schemes S lying over a fixed ring R_0, and for the base change property, we only consider base changes which are R_0-morphisms. Then, analogously to the previous definition, we define:

Definition 3.8:

A q-expansion of a weakly modular form f of weight k and level N is $f\big(Tate(q^N), \omega_{can}, \alpha_N\big)$ for all level N structures α_N. Each choice of α_N corresponds to a cusp and to a primitive N^{th} root of unity.

Now, in order to make sense of the level N structure α_N in this definition, note that the n-torsion Tate curve $Tate(q)$ is:
$Tate(q)[n] \cong \{u \in \frac{\overline{K}^{\times}}{q^{\mathbb{Z}}} s.t. u^n \in q^{\mathbb{Z}}\}$

Now, solve the following equations:

1) Solve $u^n = 1$, getting $1, \zeta_n,\ \zeta_n^2,\ ..., \zeta_n^{n-1}$, where ζ_n is an n^{th} root of unity;

2) Solve $u^n = q$, getting $u = \{\zeta_n^i (q^{\frac{1}{n}})\}_{i=0}^{n-1}$;

3) Solve $u^n = q^2$, getting $u = \{\zeta_n^i (q^{\frac{2}{n}})\}_{i=0}^{n-1} = \{\zeta_n^i (q^{\frac{1}{n}})^2\}_{i=0}^{n-1}$;

...

n) Solve $u^n = q^{n-1}$, getting $u = \{\zeta_n^i (q^{\frac{n-1}{n}})\}_{i=0}^{n-1} = \{\zeta_n^i (q^{\frac{1}{n}})^{n-1}\}_{i=0}^{n-1}$.

This is the last equation we need to check. Indeed, if $u^n = q^n$, then we get $u = \{\zeta_n^i (q^{\frac{n}{n}})\}_{i=0}^{n-1} = \{\zeta_n^i (q)\}_{i=0}^{n-1}$, which are elements of $q^{\mathbb{Z}}$, and so are not in the quotient space.

Thus there are n^2 possible combinations of the solutions, which must be elements of $Tate(q)[n]$ since it is multiplicatively closed. Further, we know that $Tate(q)[n]$ has n^2 elements.

We thus obtain that, taking $n = N$ for level N, $Tate(q)[N] = \{\zeta_N^i (q^{\frac{1}{N}})^j : 0 \leq i,\ j \leq N-1,\ i, j \in \mathbb{Z}\}$, where ζ_N is a primitive N^{th} root of unity. Note that this only makes sense if $\zeta_N \in R_0$ and $q^{\frac{1}{N}} \in R_0$, since we need the torsion points to be defined over R_0. This then implies that all points of $Tate(q)[N]$ have coordinates in $\mathbb{Z}[[q]] \bigotimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{N},\ q^{\frac{1}{N}},\ \zeta_N]$, or that all points of $Tate(q^N)[N]$ have coordinates in $\mathbb{Z}[[q]] \bigotimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{N},\ \zeta_N]$. Thus that the level N structure α_N makes sense, as they depend on the choice of two N-torsion points.

Now, Definition 3.8 allows us to once again define holomorphicity at ∞:

Definition 3.9:

A weakly modular form f of weight k and level N is holomorphic at ∞ if $f\big(Tate(q^N), \omega_{can}, \alpha_N\big) \in \mathbb{Z}[[q]] \bigotimes_{\mathbb{Z}} R_0[\frac{1}{N}, \zeta_N]$ for all level N structures α_N where ζ_N is a primitive N^{th} root of unity. This definition only makes sense if $1 \in R_0$.

Which allows us to define modular forms of weight k and level N:

Definition 3.10:

A modular form of weight k and level N is a weakly modular form of weight k and level N that is holomorphic at ∞. We denote the space of modular forms of weight k and level N by $M(N, k)$.

Finally, we can find a certain base change theorem, which will be used in a later proof, but to do this, we must first define the modular curve M_N and $\overline{M_N}$, as well as extend our definition of modular forms even further.

Definition 3.11:

Define M_N as the scheme which is the representation of the functor "isomorphism classes of elliptic curves with level N structure". Thus M_N is what modular forms have been defined on so far, but it is not compact, so we define $\overline{M}_N$ to be the normalization of $\mathbb{P}^1_{\mathbb{Z}[\frac{1}{N}]}$ in M_N, which is proper.

Note that, as stated by Katz[5], $\overline{M}_N$ can be partitioned into $\phi(N)$ connected components, each corresponding to an N^{th} root of unity. This will be discussed in more detail over $\mathbb{C}$ in section 4, on page 26.

This definition then allows us to extend our definition of modular forms, via the following theorem:

Theorem 3.12:

let U be the set of primitive N-th roots of unity, and for $\zeta \in U$ let $(\overline{M}_N)_\zeta$ be the corresponding connected components of $\overline{M}_N$. We choose $(\alpha_N)_\zeta$ a cusp in each of the connected components $(\overline{M}_N)_\zeta$, i.e. a level N structure. Then the map:

$$\begin{aligned} \{ \text{ Modular forms of weight } k \text{ and level } N \} &\to \{ q\text{-expansion at } (\alpha_N)_\zeta \}_{\zeta \in U} \\ f &\mapsto \{ q\text{-expansion of } f \text{ at } (\alpha_N)_\zeta \}_{\zeta \in U} \end{aligned}$$

is injective.

Proof:

We do this by proving that for every N^{th} root of unity ζ and for every weight k, we have that the map:

$$\{ \text{ Modular forms of weight } k \text{ and level } N \text{ on } (\overline{M}_N)_\zeta \} \to \{ q\text{-expansion at } (\alpha_N)_\zeta \}$$

is injective.

Now, for the weight 0 case. We need to show that the map

$$\{ \text{ Modular forms of weight } 0 \text{ and level } N \text{ on } (\overline{M}_N)_\zeta \} \xrightarrow{g} \{ q\text{-expansion at } (\alpha_N)_\zeta \}$$

is injective. Assume that a modular form f vanishes on the stalk, i.e. $f \in \mathrm{ker}(g)$. The stalk at a point in $\overline{M}_N$ can be calculated by choosing an affine open containing the point, and localizing it on the ideal of functions vanishing at the cusp. This ideal is prime. Now, recall the following result about localizations: Given a ring A and a prime ideal P, if $f = 0$ in A_P, then $\frac{f}{1} = \frac{0}{1}$, i.e. $((f)(1) - (0)(1))x = 0$ for $x \in S = A \setminus P$. Note that "f vanishing in the stalk" is exactly $f = 0$ in a ring localized at a prime ideal, where the ring is the chosen affine open. Thus we see that there is some x not in the prime ideal such that $fx = 0$. But the modular curve is integral, so it has no non-zero divisors. Thus $f = 0$, and the kernel of the map is $\{0\}$, which implies that the map is injective.

For the weight $k > 0$ case, we simply need to return to the same situation as in the weight 0 case. Note that, locally, we have $\underline{\omega} = \frac{dx}{y}R$ over some $S = \mathrm{Spec}(R)$. Thus all invariant forms are multiples of $\frac{dx}{y}$. This implies that $\underline{\omega}$ is isomorphic to $\mathcal{O}_S$ via the map sending $\frac{dx}{y} \in \underline{\omega}(S)$ to $1 \in \mathcal{O}_S(S) = R$, and so it is the trivial sheaf. Thus $(\underline{\omega})^{\otimes k}$ also becomes the trivial sheaf locally, since it is locally the tensor product of the trivial sheaf. Thus we locally return to the same situation as in the case of $k = 0$, and so we can apply the proof identically for the case of $k > 0$. Thus, we prove that the map:

$$\{ \text{ Modular forms of weight k and level } N \text{ on } (\overline{M}_N)_\zeta\} \to \{ \text{ } q\text{-expansion at } (\alpha_N)_\zeta \text{ } \}$$

is injective.

Gluing these maps together, we get that our original map:

$$\{ \text{ Modular forms of weight } k \text{ and level } N \text{ } \} \to \{ \text{ } q\text{-expansion at } (\alpha_N)_\zeta \text{ } \}_{\zeta \in U}$$

is injective.

Q.E.D.

This then allows us to extend the definition of modular forms just a bit further:

Definition 3.13 [5]:

A modular form of weight k and level N holomorphic at ∞ over a ring R_0 s.t. $\frac{1}{N} \in R_0$ is an element a of $H^0\big(\overline{M}_N, (\underline{\omega})^{\otimes k} \bigotimes_{\mathbb{Z}[\frac{1}{N}]} R_0\big)$. We denote the space of these modular forms by $M(R_0, N, k)$.

Definition 3.14 [5]:

A modular form of weight k and level N holomorphic at ∞ with coefficients in K, for any $\mathbb{Z}[\frac{1}{N}]$-module K, is an element a of $H^0\big(\overline{M}_N, (\underline{\omega})^{\otimes k} \bigotimes_{\mathbb{Z}[\frac{1}{N}]} K\big)$.

Now that we have established a relation between cohomology and modular forms, we will define a base change theorem having to do with cohomology. However, in order to do so, we first need the following theorem:

Theorem 3.15 (Flat base change) [10, Lemma 68.11.2]:

Let S be a scheme. Consider a Cartesian diagram of algebraic spaces

$$\begin{tikzcd} X' \arrow[r, "g'"'] \arrow[d, "f'"] & X \arrow[d, "f"'] \\ Y' \arrow[r, "g"] & Y \end{tikzcd}$$

over S. Let F be a quasi coherent $\mathcal{O}_X$-module with pullback $F' = (g')^*F$. Assume that g is flat and that f is quasi-compact and quasi-separated. For any $i \geq 0$:

1) The base change map $g^*R^if_*F \to R^if'_*F'$ is an isomorphism ;

2) If $Y = \mathsf{Spec}(A)$ and $Y' = \mathrm{Spec}(B)$, then $H^i(X, F) \bigotimes_A B = H^i(X', F')$.

This allows us to prove the following theorem:

Theorem 3.16 (Base change) [5, 1.7.1]:

Let $n \geq 3$, and suppose either that $k \geq 2$ or that $k = 1$ and $n \leq 11$. Then for any $\mathbb{Z}[\frac{1}{n}]$-module K, the canonical map

$$K \bigotimes H^0\big(\overline{M}_n, (\underline{\omega})^{\bigotimes k}\big) \to H^0\big(\overline{M}_n, K \bigotimes (\underline{\omega})^{\bigotimes k}\big)$$

is an isomorphism.

Proof:

In order to prove this, we simply need to prove that $H^1\big(\overline{M}_n, (\underline{\omega})^{\bigotimes k}\big) = 0$. We will prove that this is indeed sufficient individually for $K = \frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]}$ and for $K = \mathbb{Q}_p$, which will be enough to prove it for any K.

Case 1: $K = \mathbb{Q}_p$:

Note that $\mathbb{Q}_p$ is flat as a $\mathbb{Z}[\frac{1}{n}]$-algebra, so if we have a map g such that $g^* = \mathbb{Q}_p \bigotimes_{\mathbb{Z}[\frac{1}{n}]} \bullet$, then g is flat. Thus we can obtain the desired result by applying the flat base change theorem with $F = (\underline{\omega})^{\bigotimes k}$ and the diagram

$$\begin{tikzcd} \overline{M}_n \arrow[r, "g'"'] \arrow[d, "f'"] & \mathrm{Spec}\big(\mathbb{Q}_p\big) \bigotimes_{\mathrm{Spec}\left(\mathbb{Z}[\frac{1}{n}]\right)} \overline{M}_n \arrow[d, "f"'] \\ \mathrm{Spec}\big(\mathbb{Z}[\frac{1}{n}]\big) \arrow[r, "g"] & \mathrm{Spec}\big(\mathbb{Q}_p\big) \end{tikzcd}$$

Indeed, $\mathrm{Spec}(\mathbb{Q}_p) \bigotimes_{\mathrm{Spec}\left(\mathbb{Z}[\frac{1}{n}]\right)} \overline{M}_n = \overline{M}_n$, so we obtain $\mathbb{Q}_p \bigotimes H^0(\overline{M}_n, (\underline{\omega})^{\otimes k}) \cong H^0(\overline{M}_n, \mathbb{Q}_p \bigotimes (\underline{\omega})^{\otimes k})$. Thus we have proven that the theorem holds for Case 1.

Case 2: $K = \frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]}$:

First, take the exact sequence $0 \to \mathbb{Z}[\frac{1}{n}] \xrightarrow{\text{Multiplication by } p} \mathbb{Z}[\frac{1}{n}] \to \frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]} \to 0$. The tensor product operation by $\underline{\omega}^{\otimes k}$ is exact, so applying $\bigotimes \underline{\omega}^{\otimes k}$ gives the exact sequence:

$$0 \to \mathbb{Z}[\frac{1}{n}] \bigotimes \underline{\omega}^{\otimes k} \xrightarrow{\text{Multiplication by } p} \mathbb{Z}[\frac{1}{n}] \bigotimes \underline{\omega}^{\otimes k} \to \frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]} \bigotimes \underline{\omega}^{\otimes k} \to 0$$

Passing to the long exact sequence in cohomology which is generated by this short exact sequence, we get:

$$0 \to H^0(\overline{M}_n, \mathbb{Z}[\tfrac{1}{n}] \bigotimes \underline{\omega}^{\otimes k}) \to H^0(\overline{M}_n, \mathbb{Z}[\tfrac{1}{n}] \bigotimes \underline{\omega}^{\otimes k}) \to H^0(\overline{M}_n, \tfrac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]} \bigotimes \underline{\omega}^{\otimes k}) \to$$
$$\to H^1(\overline{M}_n, \mathbb{Z}[\tfrac{1}{n}] \bigotimes \underline{\omega}^{\otimes k}) \to \dots$$

Now, if $H^1(\overline{M}_n, (\underline{\omega})^{\otimes k}) = 0$, then $H^1(\overline{M}_n, \mathbb{Z}[\frac{1}{n}] \bigotimes (\underline{\omega})^{\otimes k}) = 0$, because $\underline{\omega}^{\otimes k}$ is defined over $\mathbb{Z}[\frac{1}{n}]$, so $\mathbb{Z}[\frac{1}{n}] \bigotimes \underline{\omega}^{\otimes k} = \underline{\omega}^{\otimes k}$. This would give us the short exact sequence:

$$0 \to H^0(\overline{M}_n, \mathbb{Z}[\frac{1}{n}] \bigotimes \underline{\omega}^{\otimes k}) \to H^0(\overline{M}_n, \mathbb{Z}[\frac{1}{n}] \bigotimes \underline{\omega}^{\otimes k}) \to H^0(\overline{M}_n, \frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]} \bigotimes \underline{\omega}^{\otimes k}) \to 0$$

And since the first map is multiplication by p, we get $\frac{H^0\left(\overline{M}_n, \mathbb{Z}[\frac{1}{n}] \bigotimes \underline{\omega}^{\otimes k}\right)}{p\left(H^0\left(\overline{M}_n, \mathbb{Z}[\frac{1}{n}] \bigotimes \underline{\omega}^{\otimes k}\right)\right)} \cong H^0(\overline{M}_n, \frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]} \bigotimes \underline{\omega}^{\otimes k})$ by the basic properties of short exact sequences. Note that quotienting modulo p is the same as tensoring by $\frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]}$, which then implies that $\frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]} \bigotimes H^0(\overline{M}_n, \mathbb{Z}[\frac{1}{n}] \bigotimes \underline{\omega}^{\otimes k}) \cong H^0(\overline{M}_n, \frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]} \bigotimes \underline{\omega}^{\otimes k})$.

Now, recall that $\mathbb{Z}[\frac{1}{n}] \bigotimes \underline{\omega}^{\otimes k} = \underline{\omega}^{\otimes k}$, as previously noted, which implies that $\frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]} \bigotimes H^0(\overline{M}_n, \underline{\omega}^{\otimes k}) \cong H^0(\overline{M}_n, \frac{\mathbb{Z}[\frac{1}{n}]}{p\mathbb{Z}[\frac{1}{n}]} \bigotimes \underline{\omega}^{\otimes k})$. This is the result that we want, so we have proven that $H^1(\overline{M}_n, (\underline{\omega})^{\otimes k}) = 0$ is sufficient in this case.

Case 1 covers every case where the module is flat over $\mathbb{Z}[\frac{1}{n}]$, because if the module is flat, the proof of case 1 will hold identically. Thus, since a module is flat over $\mathbb{Z}[\frac{1}{n}]$ iff it is torsion free, it only remains to prove our claim for the case where K is not torsion free. But then this immediately implies that K is a product of quotients of $\mathbb{Z}[\frac{1}{n}]$, and so the proof of case 2 will apply. Thus we have proven that proving $H^1(\overline{M}_n, (\underline{\omega})^{\otimes k}) = 0$ is sufficient to prove the theorem for any possible $\mathbb{Z}[\frac{1}{n}]$-module K. Now it is left to prove that $H^1(\overline{M}_n, (\underline{\omega})^{\otimes k})$ is indeed 0.

First, for weight $k = 2$, note that $(\underline{\omega})^{\otimes 2} \cong \Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]}(\log(\overline{M}_n - M_n))$[5, Section 1.5]. Now, by definition, on any of the connected components of $\overline{M}_n \bigotimes \mathbb{Z}[\frac{1}{n}, \zeta_n]$, $\deg(\Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]}) = 2g - 2$, where g is the genus of the connected component. Further, note that each connected component has at least one cusp, and thus at least one pole. Since poles raise the degree, this implies that $\deg\Big(\Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]}\big(\log(\overline{M}_n - M_n)\big)\Big) > 2g-2$, which then implies that the restriction of $(\underline{\omega})^{\bigotimes 2}$ to any of the connected components has degree $> 2g-2$. For higher weights k, the tensor product simply sums the degrees, so once again we get that the degree is always $> 2g-2$.

Now, given any divisor D on $\overline{M}_n$, let $\ell(D)$ be the dimension of $H^0\big(X, LB(D)\big)$, where $LB(D)$ is the line bundle associated with D. Note that by the definition of Serre duality:

$$\dim\Big(H^1\big(\overline{M}_n, (\underline{\omega})^{\bigotimes k}\big)\Big) = \dim\Bigg(H^0\Big(\overline{M}_n, \big((\underline{\omega})^{\bigotimes k}\big)^{-1} \bigotimes \Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]}\Big)\Bigg).$$

Further, note that $\dim\Bigg(H^0\Big(\overline{M}_n, \big((\underline{\omega})^{\bigotimes k}\big)^{-1} \bigotimes \Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]}\Big)\Bigg) = \ell\big(\Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]} - (\underline{\omega})^{\bigotimes k}\big)$. Then, by the Riemann-Roch theorem[4], we have $\ell\big((\underline{\omega})^{\bigotimes k}\big) - \ell\big(\Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]} - (\underline{\omega})^{\bigotimes k}\big) = 1 - g + \deg\big((\underline{\omega})^{\bigotimes k}\big)$.

But also, as noted by Silverman [9, Corollary 5.5], we have that if $\deg(D) > 2g-2$, then $\ell(D) = \deg(D) - g + 1$, and we just proved that $\deg\big((\underline{\omega})^{\bigotimes k}\big) > 2g-2$ on any of the connected components. Together, these imply that $\deg\big((\underline{\omega})^{\bigotimes k}\big) - g + 1 - \ell\big(\Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]} - (\underline{\omega})^{\bigotimes k}\big) = 1 - g + \deg\big((\underline{\omega})^{\bigotimes k}\big)$. By cancelling, we see that this implies that $-\ell\big(\Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]} - (\underline{\omega})^{\bigotimes k}\big) = 0$, and so implies that $\ell\big(\Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]} - (\underline{\omega})^{\bigotimes k}\big) = 0$. Since $\ell\big(\Omega^1_{\overline{M}_n/\mathbb{Z}[\frac{1}{n}]} - (\underline{\omega})^{\bigotimes k}\big) = \deg\Big(H^1\big(\overline{M}_n, (\underline{\omega})^{\bigotimes k}\big)\Big)$, this then implies that $\deg\Big(H^1\big(\overline{M}_n, (\underline{\omega})^{\bigotimes k}\big)\Big) = 0$. Thus $H^1\big(\overline{M}_n, (\underline{\omega})^{\bigotimes k}\big) = 0$, which by the first part of this proof is sufficient to prove that $K \bigotimes H^0\big(\overline{M}_n, (\underline{\omega})^{\bigotimes k}\big) \to H^0\big(\overline{M}_n, K \bigotimes (\underline{\omega})^{\bigotimes k}\big)$ is an isomorphism for $k \geq 2$. Thus this Theorem is proven for $k \geq 2$.

For the case of weight $k = 1$, we can simply proceed by explicit calculation, as there are only 9 possible values of n. For this, we will use the equation [2, Theorem 3.6.1]: If $\epsilon_\infty^{reg} > 2g-2$, then $\dim\big(M(\Gamma, 1)\big) = \frac{\epsilon_\infty^{reg}}{2}$.

For example, for n=7, we have:

Genus of $\overline{M}_7 = g = 3$, which implies $2g - 2 = 4$.

and

Number of cusps of $\Gamma(7) = 24$.

And so we have that $\epsilon_\infty^{reg} > 2g-2$, so by the formula[2, p.90]:

$\deg\big(\lfloor div(f) \rfloor\big) = k(g-1) + \lfloor\frac{k}{3}\rfloor\epsilon_3 + \frac{k}{2}\epsilon_\infty^{reg} + \frac{k-1}{2}\epsilon_\infty^{irr}$, where ϵ_3 is the number of elliptic points of order 3, and ϵ_∞^{reg} is the number of regular cusps, and ϵ_∞^{irr} is the number of irregular cusps,

this gives $\deg\big(\lfloor div(f) \rfloor\big) > 2g-2$, where f is a meromorphic 1-form, which implies that the restriction of $\underline{\omega}$ to any connected component has degree $> 2g-2$, and then the proof proceeds as in the $k \geq 2$ case. Thus this theorem is proven is all cases.

Q.E.D.

4 Connections between analytic and geometric definitions

We will show that modular forms of weight k and level N in the geometric sense of section 3, restricted to elliptic curves $E/\mathbb{C}$ over $\mathbb{C}$, can be viewed as modular forms in the analytic sense of section 1. First, recall the definition of section 3:

A modular form is a rule $F : \Big\{\big(E/\mathbb{C}, \omega, \alpha_N\big)\Big\} \to \mathbb{C}$ s.t.

1)$F\big(E/\mathbb{C}, \lambda\omega, \alpha_N\big) = \lambda^{-k} F\big(E/, \omega, \alpha_N\big)$;

2)$F\big(E/\mathbb{C}, \omega, \alpha_N\big)$ is stable with respect to the $\mathbb{C}$-isomorphism classes of $\big(E/\mathbb{C}, \omega, \alpha_N\big)$;

3)Any extension of scalars $g : \mathbb{C} \to \mathbb{C}'$ commutes with F, i.e. $F\big(E_{\mathbb{C}'}/\mathbb{C}', \omega_{\mathbb{C}'}, (\alpha_N)_{\mathbb{C}'}\big) = g\Big(F\big(E/\mathbb{C}, \omega, \alpha_N\big)\Big)$;

4) F is holomorphic at ∞.

Now, note that over $\mathbb{C}$, an elliptic curve E is $E(\mathbb{C}) = \frac{\mathbb{C}}{\mathbb{Z}+z\mathbb{Z}}$. Also note that for $\tau \in \mathbb{C}$, $d\tau = d(\tau + c)$, so $d\tau$ on $E(\mathbb{C})$ is an invariant differential. Finally, note that $\underline{\omega}_{\frac{E}{\mathbb{C}}} = \mathbb{C}d\tau = \big\{\lambda d\tau : \lambda \in \mathbb{C}\big\}$. Indeed, any divisor must be of the form $f(\tau)d\tau$, because $d\tau$ is an invariant differential. But differentials in $\underline{\omega}_{\frac{E}{\mathbb{C}}}$ are invariant, so $\forall\ f(\tau)d(\tau) \in \underline{\omega}_{\frac{E}{\mathbb{C}}}$, $f(\tau + c)d(\tau + c) = f(\tau)d\tau\ \forall\ c \in \mathbb{C}$. As we just stated, $d(\tau + c) = d(\tau)$, so $f(\tau + c) = f(\tau)\ \forall\ c \in \mathbb{C}$, which implies that f is a constant function in $\mathbb{C}$, which in turn implies that $\underline{\omega}_{\frac{E}{\mathbb{C}}} = \mathbb{C}d\tau = \big\{\lambda d\tau : \lambda \in \mathbb{C}\big\}$.

Using this, and given F, we can now define $f(z) = F\Big(\frac{\mathbb{C}}{\mathbb{Z}+z\mathbb{Z}}, d\tau, < \frac{1}{N}, \frac{Z}{N} >\Big)$, for $z \in \mathbb{H}$, and we will show that this satisfies the definition of section 1.

First, note that f is indeed a map $\mathbb{H} \to \mathbb{C}$.

Also, note that $f(z)$ is holomorphic on $\mathbb{H}$. Indeed, a modular form F is itself a section of $(\underline{\omega}_{E/S})^{\bigotimes k}$. Now, we work locally over an open $U \in M_N$ for the modular curve M_N, which is an algebraic variety. Then we can fix a basis, and we can just pick ω as the basis, by choosing $U = Spec(R)$ small enough and affine. This basis allows us to pass between the two definitions of Katz, via the equation $F\big(E/U, \alpha_N\big) = F\big(E/R, \omega, \alpha_N\big) \cdot \omega^{\bigotimes k}$. Then $F\big(E, \omega, \alpha_N\big)$ is a section of $\mathcal{O}_{M_N}(U)$. Thus we can view $F\big(E/R, \omega, \alpha_N\big)$ as a function. Now, consider the $\mathbb{C}$-points $M_N(\mathbb{C})$. By the GAGA theorem, since this is a complex variety, functions on this ring define polynomial functions, and polynomial functions are by definition holomorphic. So we have $f(z) = F\Big(\frac{\mathbb{C}}{\mathbb{Z}+z\mathbb{Z}}, d\tau, < \frac{1}{N}, \frac{Z}{N} >\Big) \xrightarrow{\text{defines}} \{\text{polynomial functions}\}$, which implies that $f(z)$ is holomorphic on $\mathbb{H}$.

Now, let $\gamma \in SL_2(\mathbb{Z})$. Then $f(\gamma z) = F\Big(\frac{\mathbb{C}}{\mathbb{Z}+\gamma z\mathbb{Z}}, d\tau_\gamma, < \frac{1}{N}, \frac{\gamma Z}{N} >\Big)$, and we must prove that $f(\gamma z) = (cz + d)^k f(z)$.

First, we address the lattice. Note that $\mathbb{Z} + \gamma z\mathbb{Z} = \mathbb{Z} + \frac{az+b}{cz+d}\mathbb{Z}$, which is homothetic to $(cz + d)\mathbb{Z} + (az + b)\mathbb{Z}$. Now we must prove that this is equal to $\mathbb{Z} + z\mathbb{Z}$:

Note that $(az+b)d+(cz+d)(-b) = adz - bcz + bd - bd = (ad-bc)z$, but since we are in $SL_2(\mathbb{Z})$, $(ad-bc) = 1$, which implies that $(az+b)d+(cz+d)(-b) = z$.

Further, note that $(az+b)(-c)+(cz+d)a = -acz - bc + acz + ad = ac - bc = 1$. Taken together, we have found integers such that $(az+b)m+(cz+d)n = 1$ and $= z$, which implies that $(cz+d)\mathbb{Z}+(az+b)\mathbb{Z} = \mathbb{Z}+z\mathbb{Z}$. Thus $f(\gamma z) = F\Big(\frac{\mathbb{C}}{\mathbb{Z}+z\mathbb{Z}}, d\tau_\gamma, < \frac{1}{N}, \frac{\gamma Z}{N} > \Big)$, and we have proven that the lattice acts in the desired fashion.

Now, we address the $d\tau$ term:

Note that $(cz+d)\tau_\gamma = \tau$, i.e. $d\tau_\gamma = \frac{d\tau}{cz+d}$. Entering this into our modular form gives us $f(\gamma z) = F\Big(\frac{\mathbb{C}}{\mathbb{Z}+z\mathbb{Z}}, \frac{d\tau}{cz+d}, < \frac{1}{N}, \frac{\gamma Z}{N} > \Big)$, but by condition 1 of the geometric definition of a modular form, this is immediately equal to $(cz+d)^k F\Big(\frac{\mathbb{C}}{\mathbb{Z}+z\mathbb{Z}}, d\tau, < \frac{1}{N}, \frac{\gamma Z}{N} > \Big)$. This gives us both the factor of $(cz+d)^k$ we require as well as showing that the $d\tau$ term acts as required.

Finally, we address the level N structure:

Note that $< \frac{1}{N}, \frac{\gamma z}{N} > = < \frac{1}{N}, \frac{\frac{az+b}{cz+d}}{N} > = < \frac{cz+d}{N}, \frac{az+b}{N} >$. We know that these have to represent the same point in the lattice as $< \frac{1}{N}, \frac{z}{N} >$, because a modular form is stable under isomorphism. Thus $cz+d \equiv 1 \bmod N$ and $az+b \equiv z \bmod N$, which implies that $c \equiv 0 \bmod N$, $d \equiv 1 \bmod N$, $a \equiv 1 \bmod N$, and $b \equiv 0 \bmod N$. These are exactly the conditions for $\gamma \in \Gamma(N)$, and so $f(\gamma z) = (cz+d)^k F\Big(\frac{\mathbb{C}}{\mathbb{Z}+z\mathbb{Z}}, d\tau, < \frac{1}{N}, \frac{\gamma Z}{N} > \Big)$ for $\gamma \in \Gamma(N)$, i.e. $f(\gamma z) = (cz+d)^k f(z)\ \forall\ \gamma \in \Gamma(N)$.

Thus, we have proven that f is a weakly modular form of level $\Gamma(N)$, as defined in section 1. Note that it is not a weakly modular form in $M(k)$, as was assumed at the beginning of this proof, but rather an element of $M(\Gamma(N), k)$. This shows that a weakly modular form "à la Katz" defines a weakly modular form of level $\Gamma(N)$, but this definition is not unique. Indeed, by choosing a different basis of the N-torsion used when defining f, we could get a different weakly modular form in the sense of section 1. Two bases define the same form if the bases are $SL_2(\frac{\mathbb{Z}}{N\mathbb{Z}})$ equivalent, hence we can get $\phi(N)$ different weakly modular forms in the sense of section 1. The knowledge of these $\phi(N)$ is encoded in the original weakly modular form "à la Katz". We will refer to the level structure "à la Katz" as a "Katz level structure" for the remainder of this thesis.

Now, in the algorithm of section 6, we will need modular forms of level $\Gamma_1(N)$, so we need to modify the definition of Katz slightly, to find the level structure which corresponds to this. To do this, we replace our Katz level N structure $\alpha_N : (\frac{\mathbb{Z}}{N\mathbb{Z}})^2 \xrightarrow{\sim} E[N]$ by an injective map $\beta_N : \frac{\mathbb{Z}}{N\mathbb{Z}} \hookrightarrow E[N]$.

Indeed, first note that we have: $E[N] = \big\{\frac{a}{N} + \frac{b}{N}z : 0 \leq a,\ b \leq N-1,\ z \in \mathbb{C}\big\}$. Now, for the mapping under γ, we get the same relation as before, where $\big(\frac{1}{N},\ \frac{z}{N}\big) \mapsto \big(\frac{cz+d}{N}, \frac{az+b}{N}\big)$ implies $\frac{1}{N} \mapsto \frac{cz+d}{N} \equiv \frac{1}{N} \bmod N$ and $\frac{z}{N} \mapsto \frac{az+b}{N} \equiv \frac{z+b}{N} \bmod N$, since for $\gamma \in \Gamma_1(N)$, $a \equiv d \equiv 1 \bmod N$ and $c \equiv 0 \bmod N$. We can easily encode this information as a map, $\frac{1}{N} + \frac{1}{N}z \mapsto \frac{1}{N} + \frac{z+b}{N}$, which is clearly equivalent to the map $\beta_N : \frac{\mathbb{Z}}{N\mathbb{Z}} \hookrightarrow E[N]$,

$$1 \mapsto \frac{1}{N} + \frac{z+b}{N}$$

which is the map we assumed originally. Thus, with this modification, we have a correspondence between weakly modular forms of level $\Gamma_1(N)$, which is what we require.

Finally, in order to extend our correspondence to modular forms, we need to prove that holomorphicity at ∞ is equivalent in both cases. Recall that, in the Katz definition, the q-expansion is $F\big(\mathrm{Tate}(q^N), \omega_{can}, \alpha_N\big)$, and F is holomorphic at ∞ iff $F\Big(\big(\mathrm{Tate}(q^N), \omega_{can}\big)_{\mathbb{C}}\Big) \in \mathbb{Z}[[q]] \bigotimes_{\mathbb{Z}} \mathbb{C}$, i.e. iff $F\Big(\big(\mathrm{Tate}(q^N), \omega_{can}\big)_{\mathbb{C}}\Big) \in \Big\{ \sum_{n=0} b_n q^n : \ b_n \in \mathbb{Z} \Big\} \bigotimes_{\mathbb{Z}} \mathbb{C}$. Furthermore, in the definition of section 1, we note that we have holomorphicity at ∞ if $f = \sum_{n=0} a_n q^n$ for $a_n \in \mathbb{C}$. Written in this form, it is immediate that these two definitions are equivalent, and so we have a correspondence between the two definitions of modular forms of weight k and level $\Gamma_1(N)$. Further, this means that our definition of Hecke operators from section 1 can be used for modular forms "à la Katz", using this equivalence.

5 Overconvergent modular forms

Before covering overconvergent modular forms themselves, we first discuss the concepts of supersingular and ordinary elliptic curves.

Definition 5.1[9]:

For R a field of characteristic p and E/R an elliptic curve, we say that E/R is supersingular if $E[p^r](\overline{F}_p) = 0 \ \forall \ r \geq 1, \ r \in \mathbb{Z}$. Otherwise, E/R is said to be ordinary, and $E[p^r](\overline{F}_p) = \frac{\mathbb{Z}}{p^r\mathbb{Z}}$.

The concept of supersingular and ordinary elliptic curves is closely tied to the something called the Hasse invariant.

Definition 5.2 [7, Pages:3-22]:

For a curve C, the Hasse invariant of the curve is defined to be the rank of the matrix of the Frobenius mapping applied to the curve. In the case of an elliptic curve, since it is of genus 1, the Hasse invariant must be either 0 or 1.

The Hasse invariant is 0 iff the elliptic curve is supersingular, and it is 1 iff the elliptic curve is ordinary. Indeed, from "The Arithmetic of Elliptic Curves" by Joseph H. Silverman[9], we have the following proof of this fact:

Assume that the Hasse invariant of an elliptic curve E is 0. We will prove that it must be supersingular. First, as noted in [9, II.2.11b], the Frobenius map is purely inseparable. Thus, $\deg_s\big(\hat{\phi}_r\big) = \deg_s[p^r] = \big(\deg_s[p]\big)^r = \big(\deg_s(\hat{\phi})\big)^r \ \forall \ r \geq 1, r \in \mathbb{Z}$, where ϕ is the Frobenius mapping, $\hat{\phi}$ is the dual of the Frobenius mapping, and $\deg_s$ is the degree of separability.

Applying [9, III.4.10a] to what we just noted, we find that $\#E[p^r](\overline{F}_p) = \deg_s(\hat{\phi}_r) = \deg(\hat{\phi})^r$. Since we assume that the Hasse invariant is 0, the rank of the matrix is 0, therefore $\det(\hat{\phi})^r = 1$. This implies that $\#E[p^r](\overline{F}_p) = 1$. Since $0 \in E[p^r](\overline{F}_p)$, this then implies that $E[p^r](\overline{F}_p) = 0 \ \forall \ r \geq 1$, so E is supersingular.

This also works in the other direction, as if $E[p^r](\overline{F}_p) = 0 \ \forall \ r \geq 1$, then $\#E[p^r](\overline{F}_p) = 1$. The only way for this to be true is if $\det(\hat{\phi})^r = 1$, i.e. if the rank of the matrix of the Frobenius mapping is 0. Thus E is supersingular iff the Hasse invariant is 0. It then also follows that the Hasse invariant is 1 iff E is ordinary.

We now move on to defining overconvergent modular forms, referred to by Katz in "P-adic Properties of Modular Schemes and Modular Forms"[5] as p-adic modular forms with growth conditions, by adding onto the definition we already have.

First, in order to introduce the "p-adic" part of the modular forms, we introduce a ring R_0 s.t. $R_0 = \varprojlim_N \frac{R_0}{p^N R_0}$. Then, for the growth condition, we pick $r \in R_0$. With these in place we can define overconvergent weakly modular forms:

Definition 5.3:

Let $N \geq 1$ and N prime to p for some prime number p, and $3 \leq N \leq 11$ if $p = 2$, $N \geq 2$ if $p = 3$. Then, for any elliptic curve E/S, where we restrict S to be an R_0-scheme s.t. $\exists\, n >> 0$ s.t. $p^n = 0$ in S, for any level $\Gamma(N)$ structure α_N and for any Y section of $\underline{\omega}^{\bigotimes(1-p)}$ such that $Y \cdot E_{p-1} = r$, we define an r-overconvergent weakly modular form f of weight k and Katz level N, over R_0 to be a rule such that $f(E/S, \alpha_N, Y)$ is a section of $\left(\underline{\omega}_{E/S}\right)^{\bigotimes k}$ over S s.t.:

1) $f\big(E/S, \alpha_N, Y\big)$ is stable with respect to the S-isomorphism classes of $\big(E/S, \alpha_N, Y\big)$. i.e. if $\big(E/S, \alpha_N, Y\big) \cong \big(E'/S, \alpha'_N, Y'\big)$, then $f\big(E/S, \alpha_N, Y\big) = f\big(E'/S, \alpha'_N, Y'\big)$;

2) Any change of basis $g : S' \to S$ commutes with f.

The set of all such weakly modular forms is $m(R_0, r, N, k)$. Also, note that each modular form in this sense is equivalent to $\phi(N)$ modular forms in the sense of section 1, parameterized by the particular choice of level structure α_N.

As in section 3, we have an equivalent definition in terms of quadruples:

Definition 5.4:

Let $N \geq 1$ and N prime to p for some prime number p, $3 \leq N \leq 11$ and $p = 2$, or $N \geq 2$ and $p = 2$. Then, for any elliptic curve E/R, where we restrict R to be an R_0-algebra s.t. $\exists\, n >> 0$ s.t. $p^n = 0$ in S, for any level $\Gamma(N)$ structure α_N, for any basis ω of $\underline{\omega}_{E/S}$ and for any $Y \in R$ such that $Y \cdot E_{p-1}(E, \omega) = r$, we define an r-overconvergent weakly modular form f of weight k and Katz level N over R_0 to be a rule such that $f\big(E/R, \omega, \alpha_N, Y\big)$ is an element of R s.t.:

1) $f\big(E/R, \omega, \alpha_N, Y\big)$ is stable with respect to the R-isomorphism classes of $\big(E/R, \omega, \alpha_N, Y\big)$. i.e. if $\big(E/R, \omega, \alpha_N, Y\big) \cong \big(E'/R, \omega', \alpha'_N, Y'\big)$, then $f\big(E/R, \omega, \alpha_N, Y\big) = f\big(E'/R, \omega', \alpha'_N, Y'\big)$;

2) Any extension of scalars $g : R \to R'$ commutes with f;

3) $f\big(E/R, \lambda\omega, \alpha_N, Y\big) = \lambda^{-k} f\big(E/R, \omega, \alpha_N, Y\big)$ for $\lambda \in R^\times$.

The set of all of such weakly modular forms is $m(R_0, r, N, k)$.

To define holomorphicity at ∞, we use a similar definition as before.

Definition 5.5:

Let f be an r-overconvergent weakly modular form of weight k and Katz level N over R_0 . We consider

$f\bigg(Tate(q^N), \omega_{can}, \alpha_N, r\Big(E_{p-1}\big(Tate(q^N), \omega_{can}\big)\Big)^{-1}\bigg)$ to be the q-expansion of f. f is holomorphic at ∞ iff $\forall\, n \geq 1$, where n is an integer, and for all level $\Gamma(N)$ structures α_N,

$f\bigg(Tate(q^N), \omega_{can}, \alpha_N, r\Big(E_{p-1}\big(Tate(q^N), \omega_{can}\big)\Big)^{-1}\bigg) \in \mathbb{Z}[[q]] \bigotimes \left(\frac{R_0}{p^n R_0}\right)[\zeta_N]$, when considered over $\mathbb{Z}((q)) \bigotimes \left(\frac{R_0}{p^n R_0}\right)[\zeta_N]$.

Also, note that $\Big(E_{p-1}\big(Tate(q^N),\omega_{can}\big)\Big)^{-1}$ is not formally the inverse, as E_{p-1} is not invertible. It is simply formally defined such that, when multiplied by r, we obtain Y, from the equation $Y \cdot E_{p-1}\big(Tate(q^n),\omega_{can}\big) = r$.

As before, having defined holomorphicity at ∞, we can define overconvergent modular forms:

Definition 5.6:

An r-overconvergent modular form of weight k and Katz level N over R_0 is an r-overconvergent weakly modular form of weight k and Katz level N over R_0 which is holomorphic at ∞. The set of all such modular forms is $M(R_0, r, N, k)$.

In order to perform the calculations necessary for this thesis, we must examine the structure of $M(R_0, r, N, k)$. To do this, we first need to prove the following proposition about $m(R_0, r, N, k)$:

Prop 5.7 [5, 2.3.1]:

When p is nilpotent in R_0, and $n \geq 3$ is prime to p, there is a canonical isomorphism

$$\begin{aligned}
m(R_0, r, N, k) &= H^0\Big(\underline{\mathrm{Spec}}_{M_N \bigotimes R_0}\big(\tfrac{Symm(\mathcal{L}^\vee)}{(E_{p-1}-r)}\big), \underline{\omega}^{\bigotimes k}\Big) \\
&= H^0\left(M_N \bigotimes R_0, \frac{\bigoplus_{j\geq 0}(\underline{\omega})^{\bigotimes \left(k+j(p-1)\right)}}{(E_{p-1}-r)}\right) \\
&= \frac{H^0\left(M_N \bigotimes R_0, \bigoplus_{j\geq 0}(\underline{\omega})^{\bigotimes \left(k+j(p-r)\right)}\right)}{(E_{p-1}-r)} \quad \text{(because } M_N \text{ is affine)} \\
&= \bigotimes_{j\geq 0} \frac{m\left(R_0, N, k+j(p-1)\right)}{(E_{p-1}-r)}.
\end{aligned}$$

Proof:

Note that, for simplicity, we write $\underline{\omega}^{\bigotimes 1-p} = \mathcal{L}$. Now, the functor

$$F_{R_0,r,n} : S \mapsto \Big\{ \text{ S-isomorphism classes of triples } (E/S, \alpha_N, Y)\Big\}$$

is the same as the functor

$$F_{R_0,r,n} : S \mapsto \Big\{ R_0\text{-morphisms } g : S \to M_N \bigotimes R_0, \text{ with a section } Y \text{ of } g^*(\mathcal{L}) \text{ s.t. } Y \cdot g^*(E_{p-1}) = r\Big\}.$$

Indeed, M_N is the representation of the functor "isomorphism classes of elliptic curves with level N structure", so the map $S \mapsto \Big\{$S-isomorphism classes of $(E/S, \alpha_N)\Big\}$ is isomorphic to the functor $S \mapsto Hom\big(S, M_N\big) = \big\{$morphisms $S \to M_N\big\}$. Since we are now defined over the ring R_0, however, we actually have R_0-linear maps $g : S \to M_N \bigotimes R_0$, rather than $S \to M_N$. Thus the map $S \mapsto \Big\{$S-isomorphism classes of $(E/S, \alpha_N)\Big\}$ is isomorphic to the functor $S \mapsto Hom\big(S, M_N\big)$.

However, this isomorphism is not enough, as we need to deal with the section Y of $\mathcal{L}$ s.t. $Y \cdot E_{p-1} = r$. We can do this by noting that E_{p-1} is a modular form over E/R_0. Thus, to pull back over S, we apply g^* to Y and E_{p-1}. This implies that we must have a section Y of $g^*(\mathcal{L})$ s.t. $Y \cdot g^*(E_{p-1}) = r$. As this is derived using the map g, adding this preserves the isomorphism, and we have proven that these functions are indeed the same.

Now, further note that we can interpret the functor
$F_{R_0,r,n} : S \mapsto \Big\{ R_0\text{-morphisms } g : S \to M_N \bigotimes R_0, \text{ with a section } Y \text{ of } g^*(\mathcal{L}) \text{ s.t. } Y \cdot g^*(E_{p-1}) = r \Big\}$ as a sub-functor of the functor
$F_{R_0,n} : S \mapsto \Big\{ R_0\text{-morphisms } g : S \to M_N, \text{ with a section } Y \text{ of } g^*(\mathcal{L}) \Big\}$, as this second functor is simply the first functor with the last condition on Y removed. Note that this functor is representable by the $M_N \bigotimes R_0$-scheme $\underline{\mathrm{Spec}}_{M_N \bigotimes R_0}\big(\underline{\mathrm{Symm}}(\mathcal{L}^\vee)\big)$.

Indeed, first define open covers $M_N \bigotimes R_0 = \bigcup\limits_i \mathrm{Spec}(B_i)$ and $S = \bigcup\limits_k \mathrm{Spec}(A_k)$. Note that we choose the $\mathrm{Spec}(B_i)$ such that $\mathcal{L}^\vee$ admits an invertible section $l_i^\vee$. Now, for every space $\mathrm{Spec}(B_i)$, consider its preimage $g^{-1}\big(\mathrm{Spec}(B_i)\big)$, and note $S = \bigcup\limits_i g^{-1}\big(\mathrm{Spec}(B_i)\big)$. Then cover $g^{-1}\big(\mathrm{Spec}(B_i)\big)$ by an open cover $g^{-1}\big(\mathrm{Spec}(B_i)\big) = \bigcup\limits_j \mathrm{Spec}(A_{ij})$, which we can do because varieties are of finite type by definition, and the modular curve M_N defines a variety. Thus we have found an affine open cover $S = \bigcup\limits_{i,j} \mathrm{Spec}(A_{ij})$ of S such that $g|_{\mathrm{Spec}(A_{ij})}$ factors through $\mathrm{Spec}(B_i)$.

Now, note that $\underline{\mathrm{Spec}}\big(\underline{\mathrm{Symm}}(\mathcal{L}^\vee)\big)$ over $\mathrm{Spec}(B_i)$ is isomorphic to
$\underline{\mathrm{Spec}}\Big(\text{Ring of polynomials in } d \text{ variables, } d = \dim(\mathcal{L}^\vee)\Big)$ over $\mathrm{Spec}(B_i)$. Over $\mathrm{Spec}(B_i)$, $\mathcal{L}^\vee$ admits an invertible section $l_i^\vee$. This is the basis over $\mathrm{Spec}(B_i)$. Thus:

$$\begin{aligned}\underline{\mathrm{Spec}}\big(\underline{\mathrm{Symm}}(\mathcal{L}^\vee)\big) &= \underline{\mathrm{Spec}}\ \big(\text{ Ring of polynomials in the variable } l_i^\vee \text{ as a ring in } B_i\ \big)\\ &= \underline{\mathrm{Spec}}\big(B_i[l_i^\vee]\big)\\ &= \mathrm{Spec}\big(B_i[l_i^\vee]\big) \text{ because } B_i[l_i^\vee]) \text{ is affine.}\end{aligned}$$

$\Longrightarrow\ \underline{\mathrm{Spec}}\big(\underline{\mathrm{Symm}}(\mathcal{L}^\vee)\big) = \mathrm{Spec}\big(B_i[l_i^\vee]\big)$ over $\mathrm{Spec}(B_i)$.

Now, we can construct a homomorphism $\widetilde{g_{i,j}} : B_i[l_i^\vee] \to A_{i,j}$ via the formula
$\widetilde{g_{i,j}}\big(\sum\limits_k b_k (l_i^\vee)^k\big) = \sum g(b_k)\big(Y \cdot g^*(l_i^\vee)\big)^k$. We will use these to construct the morphism we will need to prove that the functor is indeed representable by $\underline{\mathrm{Spec}}_{M_N \bigotimes R_0}\big(\underline{\mathrm{Symm}}(\mathcal{L}^\vee)\big)$.

In order to construct the homomorphisms, we begin with the homomorphism $g : S \to M_N \bigotimes R_0$. Since we have the affine covers, and since $g|_{\mathrm{Spec}(A_{i,j})}$ factors through $\mathrm{Spec}(B_i)$, we get homomorphisms $g : \mathrm{Spec}(A_{i,j}) \to \mathrm{Spec}(B_i)$. But by the equivalence between homomorphisms of spectrums and homomorphisms of rings, this gives $g : B_i \to A_{i,j}$. This is the form of g that appears in the formula which defines $\widetilde{g_{i,j}}$.

Now, we prove that this formula indeed defines a homomorphism with the desired properties. First, we prove that the homomorphism $\widetilde{g_{i,j}}$ defined by this formula maps from $B_i[l_i^\vee]$ to $A_{i,j}$:

For the right hand side of the formula, note that $g(b_k) \in A_{i,j}$ since g maps from B_i to $A_{i,j}$. Further, note that Y is a section of $g^*(\mathcal{L})$ and that $g^*(l_i^\vee)$ is a section of $g^*(\mathcal{L}^\vee)$ because $l_i^\vee$ is a section of $\mathcal{L}^\vee$. Thus $Y \cdot g^*(l_i^\vee) \in A_{i,j} = g^*(\mathcal{L})^0$, which implies that $\sum g(b_k)\big(Y \cdot g^*(l_i^\vee)\big)^k \in A_{i,j}$, as we want.

For the left hand side of the formula, simply note that $\sum b_k(l_i^\vee)^k$ is exactly a polynomial in $B_i[l_i^\vee]$. Thus $\widetilde{g_{i,j}}$ does indeed map from $B_i[l_i^\vee]$ to $A_{i,j}$.

Now, we need to show that $\widetilde{g_{i,j}}$ is a homomorphism. Let $\sum\limits_k b_k(l_i^\vee)^k$ and $\sum\limits_m b'_m(l_i^\vee)^k$ be two elements of $B_i[l_i^\vee]$. Then:

$$\begin{aligned}
\widetilde{g_{i,j}}\big(\sum_k b_k(l_i^\vee)^k + \sum_m b'_m(l_i^\vee)^m\big) &= \widetilde{g_{i,j}}\big(\sum (b_k + b'_k)(l_i^\vee)^k\big) \\
&= \sum g(b_k + b'_k)\big(Y \cdot g^*(l_i^\vee)\big)^k \\
&= \sum \big(g(b_k) + g(b'_k)\big)\big(Y \cdot g^*(l_i^\vee)\big)^k \\
&= \sum g(b_k)\big(Y \cdot g^*(l_i^\vee)\big)^k + g(b'_k)\big(Y \cdot g^*(l_i^\vee)\big)^k \\
&= \sum g(b_k)\big(Y \cdot g^*(l_i^\vee)\big)^k + \sum g(b'_k)\big(Y \cdot g^*(l_i^\vee)\big)^k \\
&= \widetilde{g_{i,j}}\big(\sum_k b_k(l_i^\vee)^k\big) + \widetilde{g_{i,j}}\big(\sum_m b'_m(l_i^\vee)^m\big).
\end{aligned}$$

So this is indeed a homomorphism, thus $\widetilde{g_{i,j}}$ satisfies the desired properties.

Now, apply Spec to transform this map back to a homomorphism of the form $\widetilde{g_{i,j}} : \mathsf{Spec}(A_{i,j}) \to \mathsf{Spec}(B_i[l_i^\vee])$. We can glue these maps together to obtain a morphism $G : S \to \underline{\mathsf{Spec}}_{M_N \otimes R_0}\big(\underline{\mathsf{Symm}}(\mathcal{L}^\vee)\big)$. So now, what we have is a morphism $G : S \to \underline{\mathsf{Spec}}_{M_N \otimes R_0}\big(\underline{\mathsf{Symm}}(\mathcal{L}^\vee)\big)$ that is defined by (g, Y) where g is an R_0 morphism and Y is a section of $g^*(\mathcal{L})$.

This implies that $F_{R_0,n} : S \mapsto \big\{$ R_0-morphisms $g : S \to M_N$, with a section Y of $g^*(\mathcal{L})$ $\big\}$ is isomorphic to the functor $S \to \mathsf{Hom}\Big(S, \underline{\mathsf{Spec}}_{M_N \otimes R_0}\big(\underline{\mathsf{Symm}}(\mathcal{L}^\vee)\big)\Big)$, which in turn implies that $F_{R_0,n}$ is representable by $\underline{\mathsf{Spec}}_{M_N \otimes R_0}\big(\underline{\mathsf{Symm}}(\mathcal{L}^\vee)\big)$. Finally, this implies that $F_{R_0,r,n}$ is representable by $\underline{\mathsf{Spec}}_{M_N \otimes R_0}\Big(\frac{\underline{\mathsf{Symm}}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\Big)$, simply by adding in the condition $Y \cdot g^*(E_{p-1}) = r$. Thus we have proven that

$F_{R_0,r,n} : S \to \{$S-isomorphism classes of triples $(E/S, \alpha_N, Y))$ $\}$

is isomorphic to

$F_{R_0,r,n} : S \to \mathsf{Hom}\Big(S, \underline{\mathsf{Spec}}_{M_N \otimes R_0}\Big(\frac{\underline{\mathsf{Symm}}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\Big)\Big)$,

as desired. This then implies that the universal triple $(E/S, \alpha_N, Y)$ is the inverse image on $\underline{\mathsf{Spec}}_{M_N \otimes R_0}\Big(\frac{\underline{\mathsf{Symm}}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\Big)$ of the universal elliptic curve with Katz level N structure and growth condition r on $M_N \bigotimes R_0$, Thus every elliptic curve with Katz level N structure and growth condition r defines a point x of $\underline{\mathsf{Spec}}_{M_N \otimes R_0}\big(\frac{\underline{\mathsf{Symm}}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\big)$.

Using this fact, we can prove the isomorphism of the proposition. We want an isomorphism $m(R_0, r, N, k) \cong H^0\Big(\underline{\mathrm{Spec}}_{M_N \otimes R_0}\big(\frac{\mathrm{Symm}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\big), \underline{\omega}^{\otimes k}\Big)$, so, for every element $h \in H^0\Big(\underline{\mathrm{Spec}}_{M_N \otimes R_0}\big(\frac{\mathrm{Symm}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\big), \underline{\omega}^{\otimes k}\Big)$, we want to associate a modular form, i.e. a rule $(E/S, \alpha_N, Y) \to f(E/S, \alpha_N, Y) \in \underline{\omega}^{\otimes k}$. We just stated that each $(E/S, \alpha_N, Y)$ defines a point x of $\underline{\mathrm{Spec}}_{M_N \otimes R_0}\big(\frac{\mathrm{Symm}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\big)$, so we simply let $f(E/S, \alpha_N, Y) = h_x$, where h_x is the stalk of h at x. This clearly defines an isomorphism, so this is the isomorphism we want.

Thus $m(R_0, r, N, k) = H^0\Big(\underline{\mathrm{Spec}}_{M_N \otimes R_0}\big(\frac{\mathrm{Symm}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\big), \underline{\omega}^{\otimes k}\Big)$, as desired.

Q.E.D.

This then allows us to obtain a similar relation for $M(R_0, r, N, k)$:

Prop 5.8 [5, 2.4.1]:

Let $N \geq 3$, $p \nmid N$. Under the isomorphism of Prop 5.7, the submodule $M(R_0, r, N, k) \subset m(R_0, r, N, k)$ is the submodule $H^0\left(\underline{\mathrm{Spec}}_{\overline{M}_N \otimes R_0}\left(\frac{\mathrm{Symm}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\right), \underline{\omega}^{\otimes k}\right)$ of $H^0\left(\underline{\mathrm{Spec}}_{M_N \otimes R_0}\left(\frac{\mathrm{Symm}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\right), \underline{\omega}^{\otimes k}\right)$.

This immediately gives the following corollary, which is a result of the same form as Prop 5.7:

Corollary 5.9 [5, 2.4.1.1]:

$$\begin{aligned} H^0\left(\underline{\mathrm{Spec}}_{\overline{M}_N \otimes R_0}\left(\frac{\mathrm{Symm}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\right), \underline{\omega}^{\otimes k}\right) &= H^0\left(\overline{M}_N \otimes R_0, \underline{\omega}^{\otimes k} \otimes \frac{\mathrm{Symm}(\mathcal{L}^\vee)}{(E_{p-1}-r)}\right) \\ &= H^0\left(\overline{M}_N \otimes R_0, \frac{\bigoplus_{j \geq 0} \underline{\omega}^{k+j(p-1)}}{(E_{p-1}-r)}\right). \end{aligned}$$

Further, we have the following lemma:

Lemma 5.10 [5, 2.6.1]:

Let $N \geq 3$, and suppose either that $k \geq 2$ or that $k = 1$ and $N \leq 11$ or that $k = 0$ and $p \neq 2$, or that $k = 0$, $p = 2$, and $N \leq 11$. For each $j \geq 0$, the injective homomorphism

$$\textbf{(5.10.1)} \qquad H^0\left(\overline{M}_N \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+j(p-1)}\right) \xrightarrow{E_{p-1}} H^0\left(\overline{M}_N \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+(j+1)(p-1)}\right)$$

admits a section.

Proof:

To prove that this admits a section, we can simply show that $\mathrm{Coker}\left(H^0\left(\overline{M}_N \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+j(p-1)}\right) \xrightarrow{E_{p-1}} H^0\left(\overline{M}_N \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+(j+1)(p-1)}\right)\right)$ is a finite free $\mathbb{Z}_p$-module. Indeed, if the cokernel is such a module, then by extension it is a projective module. The relevant property of projective modules is that, for any projective module C and for any short exact sequence $0 \to A \to B \to C \to 0$, this exact sequence must be split.

Now, by definition of the cokernel, we have the following exact sequence:

$$0 \to \mathrm{Ker}(E_{p-1}) \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+j(p-1)}\right) \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+(j+1)(p-1)}\right) \to$$
$$\to \mathrm{Coker}(E_{p-1}) \to 0$$

But recall that the map E_{p-1} is injective, so $\mathrm{Ker}(E_{p-1}) = 0$. Applying this produces the short exact sequence:

$$0 \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+j(p-1)}\right) \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+(j+1)(p-1)}\right) \to \mathrm{Coker}(E_{p-1}) \to 0$$

We can now apply the fact that $\mathrm{Coker}(E_{p-1})$ is projective, and so this short exact sequence is split. Thus we have a section $f : \mathrm{Coker}(E_{p-1}) \mapsto H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+(j+1)(p-1)}\right)$, which immediately gives a section $h : H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+(j+1)(p-1)}\right) \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+j(p-1)}\right)$.

Thus, having proven that $\mathrm{Coker}(E_{p-1})$ being a finite free $\mathbb{Z}_p$-module is indeed sufficient, we must now prove that it is indeed such a module:

First, note that $\underline{\omega}^{\bigotimes k+j(p-1)} \xrightarrow{E_{p-1}} \underline{\omega}^{\bigotimes k+(j+1)(p-1)}$ is injective. Thus we have a short exact sequence:

$$0 \to \underline{\omega}^{\bigotimes k+j(p-1)} \xrightarrow{E_{p-1}} \underline{\omega}^{\bigotimes k+(j+1)(p-1)} \to \frac{\underline{\omega}^{\bigotimes k+(j+1)(p-1)}}{E_{p-1}\underline{\omega}^{\bigotimes k+j(p-1)}} \to 0$$

By definition of sheaf cohomology, we then have the exact sequence:

$$0 \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+j(p-1)}\right) \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{k+(j+1)(p-1)}\right) \underset{d_2}{\longrightarrow}$$
$$\underset{d_2}{\longrightarrow} H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \frac{\underline{\omega}^{k+(j+1)(p-1)}}{E_{p-1}\underline{\omega}^{k+j(p-1)}}\right) \underset{d_3}{\longrightarrow} H^1\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+j(p-1)}\right) \to \dots$$

But note that we can apply Theorem 3.16. Further, note that, as stated in its proof, this theorem implies that $H^1(\overline{M}_k, \underline{\omega}^{\bigotimes k}) = 0$. By considering the conditions on k in the statement of the current lemma, we find that, in terms of k, j, n and p, $H^1(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+j(p-1)}) = 0$
Applying this to the exact sequence of cohomologies results in:

$$0 \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+j(p-1)}\right) \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{k+(j+1)(p-1)}\right) \underset{d_2}{\longrightarrow}$$
$$\underset{d_2}{\longrightarrow} H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \frac{\underline{\omega}^{k+(j+1)(p-1)}}{E_{p-1}\underline{\omega}^{k+j(p-1)}}\right) \xrightarrow{d_3} 0$$

as an exact sequence of finite free $\mathbb{Z}_p$-modules. Further, this sequence commutes with arbitrary change of base, because they are all free $\mathbb{Z}_p$ modules. Thus:

$$
\begin{aligned}
\mathrm{Coker}(E_{p-1}) &= \frac{H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{k+(j+1)(p-1)}\right)}{\mathrm{im}(E_{p-1})} \\
&= \frac{H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{k+(j+1)(p-1)}\right)}{\mathrm{Ker}(d_2)} \\
&= \mathrm{im}(d_2) \\
&= \ker(d_3).
\end{aligned}
$$

This implies that $\mathrm{Coker}(E_{p-1}) = \ker(d_3)$, which then implies that $\mathrm{Coker}(E_{p-1}) = H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \frac{\underline{\omega}^{k+(j+1)(p-1)}}{E_{p-1}\underline{\omega}^{k+j(p-1)}}\right)$, which is a finite free $\mathbb{Z}_p$-module.

Q.E.D.

Now, for each possible choice of N, k, j, we choose a specific section of this map, whose existence we have just proven. Let the image of this section be denoted by $B(N, k, j+1)$. Note that $E_{p-1} \cdot H^0\left(\overline{M}_N, \underline{\omega}^{\bigoplus k+j(p-1)}\right)$ is of weight $k+(j+1)(p-1)$, the same weight as $H^0\left(\overline{M}_N, \underline{\omega}^{\bigoplus k+(j+1)(p-1)}\right)$, and note that we have the short exact sequence

$$
0 \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{\bigotimes k+j(p-1)}\right) \to H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \underline{\omega}^{k+(j+1)(p-1)}\right) \xrightarrow[d_2]{} \\
\xrightarrow[d_2]{} H^0\left(\overline{M}_N \bigotimes \mathbb{Z}_p, \frac{\underline{\omega}^{k+(j+1)(p-1)}}{E_{p-1}\underline{\omega}^{k+j(p-1)}}\right) \xrightarrow{d_3} 0.
$$

Together, these produce the direct sum decomposition:

(5.10.2) $$H^0\left(\overline{M}_N, \underline{\omega}^{\bigoplus k+(j+1)(p-1)}\right) \cong E_{p-1} \cdot H^0\left(\overline{M}_N, \underline{\omega}^{\bigoplus k+j(p-1)}\right) \bigoplus B(N, k, j+1)$$

where $B(N, k, j+1)$ is the complement since it is obtained by the section of lemma 5.10, and we define $H^0\left(\overline{M}_N, \underline{\omega}^{\bigoplus k}\right) := B(N, k, 0)$.

Now, we work over R_0, so define $B(R_0, N, k, j) := B(N, k, j) \bigotimes_{\mathbb{Z}_p} R_0$. Taking the tensor with R_0 on both sides of the relation gives us

$$
H^0\left(\overline{M}_N, \underline{\omega}^{\bigotimes k+(j+1)(p-1)}\right) \bigotimes_{\mathbb{Z}_p} R_0 \cong \left(E_{p-1} \cdot H^0\left(\overline{M}_N, \underline{\omega}^{\bigotimes k+j(p-1)}\right) \bigoplus B(N, k, j+1)\right) \bigotimes_{\mathbb{Z}_p} R_0
$$

i.e.

$$
H^0\left(\overline{M}_N \bigotimes_{\mathbb{Z}_p} R_0, \underline{\omega}^{\bigotimes k+(j+1)(p-1)}\right) \cong E_{p-1} \cdot H^0\left(\overline{M}_N \bigotimes_{\mathbb{Z}_p} R_0, \underline{\omega}^{\bigotimes k+j(p-1)}\right) \bigoplus B(R_0, N, k, j+1)
$$

Now, iterating the direct sum decomposition, we have:

$$
\begin{aligned}
H^0\left(\overline{M}_N, \underline{\omega}^{\bigotimes k+(j+1)(p-1)}\right) &\cong E_{p-1} \cdot H^0\left(\overline{M}_N, \underline{\omega}^{\bigotimes k+j(p-1)}\right) \bigoplus B(N, k, j+1) \\
&\cong E_{p-1} \cdot \left(E_{p-1} \cdot H^0\left(\overline{M}_N, \underline{\omega}^{\bigoplus k+(j-1)(p-1)}\right) \oplus B(N, k, j)\right) \bigoplus B(N, k, j+1) \\
&\cong (E_{p-1})^{j+1} H^0\left(\overline{M}_N, \underline{\omega}^{\bigotimes k}\right) \bigoplus B(N, k, j+1) \bigoplus E_{p-1}^{(j+1)-j} B(N, k, j) \bigoplus \ldots \bigoplus E_{p-1}^{j} \\
&\cong \bigoplus_{a=o}^{j+1} E_{p-1}^{(j+1)-a} B(N, k, a).
\end{aligned}
$$

This iteration also works for the R_0 analogue we just defined, which gives us that

$$\begin{aligned}
H^0\big(\overline{M}_N, \underline{\omega}^{\otimes k+j(p-1)}\big) \otimes R_0 &\cong \Big(\bigoplus_{a=o}^{j+1} E_{p-1}^{(j+1)-a} B(N,k,a)\Big) \otimes R_0 \\
&\cong \bigoplus_{a=o}^{j} E_{p-1}^{j-a}\big(B(N,k,a) \otimes R_0\big) \\
&\cong \bigoplus_{a=o}^{j} E_{p-1}^{j-a} B(R_0,N,k,a).
\end{aligned}$$

But note that $H^0\big(\overline{M}_N, \underline{\omega}^{\otimes k+j(p-1)}\big) \otimes R_0 = H^0\big(\overline{M}_N, \underline{\omega}^{\otimes k+j(p-1)} \otimes R_0\big)$, which is then equal to $M\big(R_0, N, k+j(p-1)\big)$. This implies that any element in $M\big(R_0, N, k+j(p-1)\big)$ can be written uniquely as $\sum E_{p-1}^{j-a} b_a$ for $b_a \in B(R_0,N,k,a)$, but the E_{p-1}^{j-a} do not depend on b_a, so we can use the b_a as "coordinates". Thus, we get an isomorphism:

(5.10.3)
$$\begin{aligned}
M\big(R_0, N, k+j(p-1)\big) &\cong \bigoplus_{a=0}^{j} B(R_0,N,k,a) \\
\sum E_{p-1}^{j-a} b_a &\cong \sum b_a
\end{aligned}$$

Where $b_a \in B(R_0,N,k,a)$.

Now, define:

$$B^{\mathrm{rigid}}(R_0,r,N,k) = \Big\{ \sum_{a=0}^{\infty} b_a,\ b_a \in B(R_0,N,k,a) : \forall\ N>0,\ N \in \mathbb{Z},\ \exists\ C_N > 0 \text{ s.t. } b_a \in p^N \cdot B(R_0,N,k,a)\ \forall\ a \geq C_N \Big\}$$

Now, before we use this definition to introduce the next proposition, we need to introduce the following lemma.

Lemma 5.11 [5, Section 2.1]:

The Eisenstein series E_{p-1} lifts to the Hasse invariant for $p \geq 5$.

Proof:

Recall the Eisenstein series $E_k = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$. Note that for $k = p-1,\ p \geq 5$, $\mathrm{ord}_p(\frac{-2(p-1)}{B_{p-1}}) = 1$. Thus $\frac{-2(p-1)}{B_{p-1}} = p\frac{a}{b}$ for some $\frac{a}{b} \in \mathbb{Q}$ s.t. $p \nmid \frac{a}{b}$. This implies that the coefficients a_n of the q-expansion of E_{p-1} are all elements of $\mathbb{Q} \bigcap \mathbb{Z}_p$, which means we can reduce modulo p to end up with a modular form over $\mathbb{F}_p$. Then the q-expansion is just 1 because the rest of the coefficients are multiples of p. But as noted in section 2.0 of "P-adic Properties of Modular Schemes and Modular Forms"[5], $A(\mathrm{Tate}(q), \omega_{can}) = 1$, where A is the Hasse invariant viewed as a modular form, so E_{p-1} and A are modular forms with the same q-expansion. Further note that they are also of the same level.

This implies that $A \equiv E_{p-1} \bmod p$, and thus E_{p-1} lifts to the Hasse invariant for $p \geq 5$.

Q.E.D.

Now we have everything required to prove the following proposition:

Prop 5.12 [5, 2.6.2]:

Let $N \geq 3$, and suppose either that $k \geq 2$ or that $k = 1$ and $N \leq 11$ or that $k = 0$ and $p \neq 2$, or that $k = 0$, $p = 2$, and $N \leq 11$. Let R_0 be any p-adically complete ring, and suppose $r \in R_0$ is not a zero divisor in R_0. Then the inclusion of $B^{rigid}(R_0, r, N, k)$ in the p-adic completion of $H^0\big(M_N, \bigoplus_{j\geq 0}(\underline{\omega})^{\bigotimes(k+j(p-1))}\big)$ induces, via the isomorphism (5.10.3), an isomorphism

$$B^{rigid}(R_0, r, N, k) \to M(R_0, r, N, k)$$
$$\sum b_a \to "\sum_{a\geq 0} \frac{r^a \cdot b_a}{(E_{p-1})^a}"$$

where $"\sum_{a\geq 0} \frac{r^a \cdot b_a}{(E_{p-1})^a}"$ has the value $\sum_{a\geq 0} b_a(E/S, \alpha_N) \cdot Y^a$ on $(E/S, \alpha_N, Y)$.

Proof:

First, we prove injectivity:

Note that the set

$$U = \Big\{ \sum_{a\geq 0} b_a \in B^{rigid}(R_0, r, N, k) \text{ s.t. it can be written as } (E_{p-1} - r) \cdot \sum_{a\geq 0} s_a \text{ with}$$
$$s_a \in M\big(R_0, N, k + a(p-1)\big) \text{ and } s_a \text{ tending to zero as } a \to \infty \Big\} \bigcup \Big\{0\Big\}$$

is the kernel of the isomorphism, i.e. it is the set of elements $\sum_{a\geq 0} b_a \in B^{rigid}(R_0, r, N, k,)$ s.t. $"\sum_{a\geq 0} \frac{r^a \cdot b_a}{(E_{p-1})^a}" = \sum_{a\geq 0} b_a(E/S, \alpha_N) \cdot Y^a = 0$. Indeed, first note that $(E_{p-1} - r)$ becomes 0 in $M(R_0, r, N, k)$ by definition, since $M(R_0, r, N, k)$ is defined by taking the quotient by $(E_{p-1} - r)$, so the elements of U are clearly elements of the kernel of the isomorphism. Furthermore, $(E_{p-1} - r)$ is the only thing that becomes 0 in $M(R_0, r, N, k)$, because the change between $M(R_0, r, N, k)$ and $M(R_0, N, k)$ is the addition of the $(E_{p-1} - r)$ condition, as seen in Prop 5.8. Thus, the isomorphism we just found relating $B(R_0, N, k, a)$ and $M(R_0, N, k + j(p-1))$ means that the only other possible element of the kernel is simply $0 \in B^{rigid}(R_0, r, N, k)$.

Thus, to prove injectivity, we simply need to prove that $U = \{0\}$, i.e. that $b_a = 0 \ \forall \ a \geq 0$ for $\sum_{a\geq 0} b_a \in U$.

Further, note that we actually only need to show that $\forall N > 0$, $N \in \mathbb{Z}$, then $b_a \equiv 0 \bmod p^N$. Indeed, if this is true, then we have:
$b_a \equiv 0 \bmod p$
$b_a \equiv 0 \bmod p^2$
$b_a \equiv 0 \bmod p^3$
...

$\implies b_a = 0$

Now, prove that this is the case:

First, note that $B^{rigid}(R_0, r, N, k)$ is such that given any $N > 0$, $\exists\, l > 0$ s.t. $b_a \in p^N \cdot B(R_0, N, k, a)\ \forall\, a \geq l$. This is equivalent to saying that given any $N > 0$, $\exists\, l > 0$ s.t. $b_a \equiv 0 \bmod p^N$ for $a \geq l$, which further implies that given any $N > 0$, $\exists\, l > 0$ s.t. $\sum\limits_{a \geq 0} b_a \equiv \sum\limits_{a=0}^{l-1} b_a \bmod p^N$.

Also, note that $\sum\limits_{a \geq 0} b_a = (E_{p-1} - r) \sum\limits_{a \geq 0} s_a$, and that $s_a \in M(R_0, N, k + a(p-1))$. Thus $s_a = \sum\limits_{c} E_{p-1}^{a-c} b_c$ for $b_c \in B(R_0, N, k, c)$, which then implies that $\sum\limits_{a \geq 0} s_a = \sum\limits_{a \geq 0} \sum\limits_{c} E_{p-1}^{a-c} b_c$. Entering this into our equation for $\sum\limits_{a \geq 0} b_a$ gives $\sum\limits_{a \geq 0} b_a = (E_{p-1} - r) \sum\limits_{a \geq 0} \sum\limits_{c} E_{p-1}^{a-c} b_c$.

Now take $\bmod p^N$ on both sides. Since we noted that given any $N > 0$, $\exists\, l > 0$ s.t. $\sum\limits_{a \geq 0} b_a \equiv \sum\limits_{a=0}^{l-1} b_a \bmod p^N$, we get $\sum\limits_{a=0}^{l-1} b_a \equiv (E_{p-1} - r) \sum\limits_{a \geq 0} \sum\limits_{c} E_{p-1}^{a-c} b_c \bmod p^N$.

Now, assume that the a on the right side of the equation is greater than $l - 1$, i.e. assume that this term does not go to zero. Then we have an element on the right side of the form xb_c for $b_c \in B(R_0, N, k, c)$ and $c > a$. Since $b_c \in B(R_0, N, k, c)$, then $b_c \notin B(R_0, N, k, a)$ for any $0 \leq a \leq l - 1$, which is a contradiction because then the two sides cannot be equal. Thus we must have $\sum\limits_{a \geq 0} \sum\limits_{c} E_{p-1}^{a-c} b_c \equiv \sum\limits_{a=0}^{l-1} \sum\limits_{c} E_{p-1}^{a-c} b_c \bmod p^N$, which then implies that $\sum\limits_{a \geq 0} s_a \equiv \sum\limits_{a=0}^{l-1} s_a \bmod p^N$. Thus, we have proven that $b_a \equiv s_a \equiv 0 \bmod p^N\ \forall\, a \geq l$, i.e. $b_a \equiv s_a \equiv 0 \bmod p^N\ \forall\, a > l - 1$.

Now, using this as our base case, we will prove that $b_a \equiv s_a \equiv 0 \bmod p^N\ \forall\, a \geq 0$ by induction:

Let $b_a \equiv s_a \equiv 0 \bmod p^N\ \forall\, a > M$ for some M. Now, $b_{M+1} \equiv 0 \bmod p^N$ by hypothesis, but also, $\sum\limits_{a \geq 0} b_a = (E_{p-1} - r) \sum\limits_{a \geq 0} s_a$, i.e. $\sum\limits_{a \geq 0} b_a = E_{p-1} \sum\limits_{a \geq 0} s_a - r \sum\limits_{a \geq 0} s_a$. Comparing the highest weight forms, we get $b_{M+1} \equiv E_{p-1} s_M - r s_{M+1} \equiv E_{p-1} s_M \bmod p^N$, which implies that $E_{p-1} s_M \equiv b_{M+1} \equiv 0 \bmod p^N$.

Now, restrict this equality to the ordinary locus, and note that the ordinary locus is dense on the set of modular forms. Further, by Lemma 5.11, E_{p-1} lifts to the Hasse invariant. Thus E_{p-1} is a unity on the ordinary locus, and so $E_{p-1} s_M \equiv s_M \bmod p^N$ on the ordinary locus. But $E_{p-1} s_M \equiv 0 \bmod p^N$, so $s_M \equiv 0 \bmod p^N$ on the ordinary locus.

But the ordinary locus is dense, so we have that s_M vanishes on an open dense subset of the modular curve. Further, since the modular curve is normal, the vanishing locus of a section must be the whole curve, have codimension 1 or be empty. Since it vanishes on a dense open, it cannot be empty, so it only remains to check that it cannot have codimension 1. If it had codimension 1, then the space would be defined by an ideal of height 1, which is a point on a modular curve. Since it vanishes on an open dense set, it cannot be generated by an ideal that is a point. Thus the vanishing locus cannot have codimension 1, and the only possibility remaining is that s_M is zero everywhere.

This implies that $s_M \equiv 0 \bmod p^N$.

Now, note that $b_M \equiv E_{p-1}s_{M-1} - rs_M \bmod p^N$, but we just showed that $s_M \equiv 0 \bmod p^N$, so $b_M \equiv E_{p-1}s_{M-1} \bmod p^N$, and in particular $b_M \bmod p^N \in \mathrm{im}(E_{p-1})$. But b_M is also an element of the complement of $\mathrm{im}(E_{p-1})$, since $b_M \in B(R_0, N, k, M)$ and
$H^0\big(\overline{M}_N, \underline{\omega}^{\otimes k+(j+1)(p-1)} \bigotimes_{\mathbb{Z}_p} R_0\big) \cong E_{p-1} \cdot H^0\big(\overline{M}_N, \underline{\omega}^{\otimes k+j(p-1)} \bigotimes_{\mathbb{Z}_p} R_0\big) \bigoplus B(R_0, N, k, j+1)$.

Therefore, $b_M \equiv 0 \bmod p^N$ is the only possibility which does not cause a contradiction. Thus we have proven that both $b_M \equiv 0 \bmod p^N$ and $s_M \equiv 0 \bmod p^N$. Thus $b_a \equiv s_a \equiv 0 \bmod p^N \ \forall\ a > (M-1)$ for some M, and so the inductive step is proven. Therefore, by induction, $b_a \equiv 0 \bmod p^N \ \forall\ N > 0,\ N \in \mathbb{Z},\ \forall\ a \geq 0$, which implies that $b_a = 0 \ \forall\ a \geq 0$, and thus that the map is injective.

Now, for surjectivity:

For this, use (5.10.3). Note that, by definition, $s_a = \sum_{p-1}^{a-j} b_j$. Then, defining $i = a - j$, we get $s_a = \sum_{i+j=a} (E_{p-1})^i b_j(a)$.

Also, note that $s_a \to 0$ as $a \to \infty$, which implies that $b_j(a) \to 0$ as $a \to \infty$. Also, note that
$\sum_a s_a = \sum_a \sum_{i+j=a} (E_{p-1})^i b_j(a)$
$\quad = \sum_a \sum_{i+j=a} r^i b_j(a) + (E_{p-1} - r) \sum_a \sum_{i+j=a} b_j(a) \sum_{u+v=i-1} (E_{p-1})^u \cdot r^v$.

But $(E_{p-1} - r) = 0$ in $M(R_0, r, N, k)$, so $\sum_a s_a = \sum_a \sum_{i+j=a} r^i b_j(a)$ in $M(R_0, r, N, k)$, i.e. $\sum_a s_a$ has the same image in $M(R_0, r, N, k)$ as $\sum_a \sum_{i+j=a} r^i b_j(a)$. Now, note that $b_j(i+j) \to 0$ as $i \to \infty$, which implies that $\forall j,\ \exists b_j' \in B(R_0, N, k, j)$ such that $\sum_i r^i b_j(i+j) \to b_j'$. Also, $b_j \to 0$ as $j \to \infty$, so $b_j' \to 0$ as $j \to \infty$. This implies that $\sum_a \sum_{i+j=a} r^i b_j(a) = \sum_j \sum_i r^i b_j(i+j) = \sum_{j \geq 0} b_j'$. As $\sum_a s_a = \sum_a \sum_{i+j=a} r^i b_j(a)$, this implies that $\sum_a s_a$ and $\sum_{j \geq 0} b_j'$ have the same image in $M(R_0, r, N, k)$ and $b_j' \to 0$ as $j \to \infty$.

This then implies that $\sum_{j \geq 0} b_j'$ is an element of $B^{\mathrm{rigid}}(R_0, r, N, k)$ which has the same image in $M(R_0, r, N, k)$ as $\sum_a s_a$. Since each element of $M(R_0, r, N, k)$ corresponds to some element of $M(R_0, N, k)$, since $M(R_0, r, N, k)$ is obtained by taking the quotient with the ideal $(E_{p-1} - r)$, this means that for any element a of $M(R_0, r, N, k)$, we have an element $\sum_{j \geq 0} b_j'$ of $B^{\mathrm{rigid}}(R_0, r, N, k)$ whose image under the map is a.

This implies that surjectivity is proven, and so we have proven both surjectivity and injectivity, which implies that the map is indeed an isomorphism.

Q.E.D.

With this proposition, we now have all of the structure necessary to introduce the algorithms.

6 Algorithms

In order to examine the Hecke eigenvalues of modular forms, the algorithm found in "Computations with classical and p-adic modular forms", by Alan G. B. Lauder [6] was used. The algorithm is split into two cases. The first case takes as inputs a prime number greater than or equal to 5, an integer k and a positive integer m, and returns the p-adic valuations of the inverse of the eigenvalues of T_p modulo p^m on $M(\mathbb{Z}_p, r, 1, k)$. The second case is a generalization of the first case, and takes an extra input N, and returns results for modular forms of level $\Gamma_1(N)$. We implemented these algorithms as Sagemath programs. The code we wrote for said programs can be found in the appendix.

Algorithm for level $\Gamma_1(1)$:

Step 1:

• Initialize the algorithm by letting p be a prime ≥ 5, letting k be an integer, and letting m be a positive integer.

• Calculate two additional variables, k_0 and j, as the unique solution to the formulas $k = k_0 + j(p-1)$ and $0 \leq k_0 < p-1$.

• Compute the variable n as $n = \left\lfloor \frac{p+1}{p-1}(m+1) \right\rfloor$.

• Compute the dimension d_i of the space of classical modular forms of level 1 and weight $k_0 + i(p-1)$, for i running over $i = 0, ..., n$.

• Compute the difference between each successive dimension, denoted by m_i, as $m_i = d_i - d_{i-1}$ for $i = 1, ..., n$ and $m_0 = d_0$.

• Compute the variable l as the sum of these differences, $l = \sum\limits_{i=0}^{n} m_i$.

• Compute the variable m' as $m' = m + \lfloor \frac{n}{p+1} \rfloor$, which will be used as the working precision of the algorithm.

Step 2:

• Calculate a row reduced basis of q-expansions of the space of classical modular forms of weight $k_0 + i(p-1)$ and level $\Gamma_1(1)$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{lp})}$, for i running from 0 to n. By a row reduced basis of q-expansions, we mean that if we form a matrix from a given basis of q-expansions of the space, where each row corresponds to one of the q-expansions and each column corresponds to a power of the variable q, then the row reduced basis is the basis consisting of the q-expansions obtained by row-reducing this matrix. Denote this row reduced basis by $D_{k_0+i(p-1)}$.

• For i running from 0 to n, define W_i to be the last m_i elements of $D_{k_0+i(p-1)}$.

Step 3:

• Compute the q-expansion of E_{p-1}, the Eisenstein series of weight $p-1$, in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{lp})}$. Call this $E_{p-1}(q)$.

• For i running from 0 to n and for s running from 1 to m_i, calculate the variables $e_{i,s} = p^{\left\lfloor \frac{i}{p-1} \right\rfloor} E_{p-1}^{-i}(q) W_i[s]$, where $W_i[s]$ is the s^{th} element of W_i, in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{lp})}$.

Step 4:

• Define $G(q) = \frac{E_{p-1}(q)}{E_{p-1}(q^p)}$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{lp})}$.

• For i running from 0 to n and for s running from 1 to m_i, calculate the variables $u_{i,s} = G(q)^j e_{i,s}$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{lp})}$.

• When implementing this algorithm as a computer program, it can be useful to compute $G(q)^j$ using a quick exponentiation algorithm to save on processing time.

Step 5:

• For i running from 0 to n and for s running from 1 to m_i, calculate the variables $t_{i,s} = T_p(u_{i,s})$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{lp})}$.

Step 6:

• Define the $l \times l$ matrix T in $\frac{\mathbb{Z}[[q]]}{(p^{m'})}$ using the elements $t_{i,s}$ where each row corresponds to one of the $t_{i,s}$ and each column corresponds to a power of q.

• Define the $l \times l$ matrix E in $\frac{\mathbb{Z}[[q]]}{(p^{m'})}$ using the elements $e_{i,s}$ where each row corresponds to one of the $e_{i,s}$ and each column corresponds to a power of q.

• Calculate the matrix A s.t. $T = AE$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'})}$. If this has no solution, instead solve the equation $pT = AE$ for A.

• Calculate $a = \det(1 - At) \bmod p^m$.

• Calculate the Newton slopes of a to find the p-adic valuations of the inverse of the eigenvalues of T_p modulo p^m, or of pT_p if $T = AE$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'})}$ has no solution.

Note that Newton polygons and slopes are defined as follows:

Definition 6.1 [3]:

Let K be a field which is complete with respect to the p-adic valuation. Let f be a polynomial $f = \sum_{i=0}^{n} a_i x^i$ of degree n with $a_i \in K$ such that $a_0 \neq 0$, its Newton polygon $NP(f)$ is defined to be the lower boundary of the convex hull of $\{(i, \mathrm{ord}_p(a_i)) : 0 \leq i \leq n\} \subset \mathbb{R}^2$, ignoring points where $a_i = 0$. As this provides information about the zeroes of the polynomial, we may also divide by a_0 and assume that $a_0 = 1$. We call the slopes of the line segments which make up the Newton polygon the newton slopes of the polynomial.

The Newton polygons give the p-adic valuations of the eigenvalues by the following theorem:

Theorem 6.2 [3]:

Let K be a field which is complete with respect to the p-adic valuation. Let $f(x) = 1 + a_1 x + a_2 x^2 + ... + a_n x^n \in K[x]$ be a polynomial and let $m_1, m_2, ...m_r$ be the slopes of its newton polygon (in increasing order). Let $i_1, i_2, ..., i_r$ be the corresponding lengths of the line segments. Then, for each k, $1 \leq k \leq r$, $f(x)$ has exactly i_k roots (in $\mathbb{C}_p$, counting multiplicities) of p-adic valuation $-m_k$.

Note that, when applying the Hecke operator T_p in this algorithm, it always acts as:

$$f \mapsto T_p f$$
$$\sum_{n=0}^{\infty} a_n q^n \mapsto \sum_{n=0}^{\infty} a_{pn} q^n$$

despite the fact that $p \nmid 1$. This is because we are working with p-adic modular forms of level $\Gamma_1(1)$, and so we are working in $\Gamma_1(1) \bigcap \Gamma_0(p)$, which ensures that this formula is correct. This also holds for the level $\Gamma_1(N)$ algorithm.

The algorithm for level $\Gamma_1(N)$ is similar, with only a few differences:

Algorithm for level $\Gamma_1(N)$:

Step 1:

• Initialize the algorithm by letting N be a positive integer, letting p be a prime ≥ 5 s.t. p does not divide N, letting k be an integer, and letting m be a positive integer.

• Calculate two additional variables, k_0 and j, as the unique solution to the formulas $k = k_0 + j(p-1)$ and $0 \leq k_0 < p-1$.

• Compute the variable n as $n = \left\lfloor \frac{p+1}{p-1}(m+1) \right\rfloor$.

• Compute the dimension d_i of the space of classical modular forms of level 1 and weight $k_0 + i(p-1)$, for i running over $i = 0, ..., n$.

• Compute the difference between each successive dimension, m_i, as $m_i = d_i - d_{i-1}$ for $i = 1, ..., n$ and $m_0 = d_0$.

• Compute the variable l as the sum of these differences, $l = \sum_{i=0}^{n} m_i$.

• Compute the variable m' as $m' = m + \lfloor \frac{n}{p+1} \rfloor$, which will be used as the working precision of the algorithm.

• Compute the Sturm bound l' of the space of classical modular forms of level $\Gamma_1(N)$ and weight $k_0 + n(p-1)$.

Step 2:

• Calculate a row reduced basis of q-expansions of the space of classical modular forms of weight $k_0 + i(p-1)$ and level $\Gamma_1(1)$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{l'p})}$, for i running from 0 to n. By a row reduced basis of q-expansions, we mean that if we form a matrix from a given basis of q-expansions of the space, where each row corresponds to one of the q-expansions and each column corresponds to a power of the variable q, then the row reduced basis is the basis consisting of the q-expansions obtained by row-reducing this matrix. Denote this row reduced basis by $D_{k_0+i(p-1)}$.

• For each i running from 0 to n, define W_i to be an empty set. Then, if i=0, W_0=$D_{k_0+0(p-1)}$. If $i \neq 0$, then, for w running from 0 to d_i, check if the degree of the lowest term of the w^{th} element of $D_{k_0+i(p-1)}$ is different from the lowest term of any element of $D_{k_0+(i-1)(p-1)}$. If so, add that element to the set W_i.

Step 3:

• Compute the q-expansion of E_{p-1}, the Eisenstein series of weight $p-1$, in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{l'p})}$. Call this $E_{p-1}(q)$.

• For i running from 0 to n and for s running from 1 to m_i, calculate the variables $e_{i,s} = p^{\lfloor \frac{i}{p-1} \rfloor} E_{p-1}^{-i}(q) W_i[s]$, where $W_i[s]$ is the s^{th} element of W_i, in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{l'p})}$.

Step 4:

• Define $G(q) = \frac{E_{p-1}(q)}{E_{p-1}(q^p)}$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{l'p})}$.

• For i running from 0 to n and for s running from 1 to m_i, calculate the variables $u_{i,s} = G(q)^j e_{i,s}$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{l'p})}$.

• When implementing this algorithm as a computer program, it can be useful to compute $G(q)^j$ using a quick exponentiation algorithm to save on processing time.

Step 5:

• For i running from 0 to n and for s running from 1 to m_i, calculate the variables $t_{i,s} = T_p(u_{i,s})$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'}, q^{l'p})}$.

Step 6:

• Define the $l \times l'$ matrix T in $\frac{\mathbb{Z}[[q]]}{(p^{m'})}$ using the elements $t_{i,s}$ where each row corresponds to one of the $t_{i,s}$ and each column corresponds to a power of q.

• Define the $l \times l'$ matrix E in $\frac{\mathbb{Z}[[q]]}{(p^{m'})}$ using the elements $e_{i,s}$ where each row corresponds to one of the $e_{i,s}$ and each column corresponds to a power of q.

• Calculate the matrix A s.t. $T = AE$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'})}$. If this is not able to be solved, instead solve the equation $pT = AE$ for A.

• Calculate $a = \det(1 - At) \bmod p^m$.

• Calculate the Newton slopes of a to then find the p-adic valuations of the inverse of the eigenvalues of T_p modulo p^m, or of pT_p if $T = AE$ in $\frac{\mathbb{Z}[[q]]}{(p^{m'})}$ has no solution.

Remark 6.3:

In order to prove the correctness of these algorithms, we require one last set of results. We follow the strategy of [6, 2.1 to 2.3]:

Let $0 < \text{ord}_p(r) < \frac{1}{p+1}$, Let Q be a p-adic field, and let Q_0 be the ring of integers of Q. Consider an ordered basis $\{b_{i,s}\}_{s=1}^{m_i}$ of $B(Q_0, N, k, j)$, and note that this indeed has enough elements to form a basis, since $H^0\big(\overline{M}_N, \underline{\omega}^{\bigoplus k+(j+1)(p-1)}\big) \cong E_{p-1} \cdot H^0\big(\overline{M}_N, \underline{\omega}^{\bigoplus k+j(p-1)}\big) \bigoplus B(N, k, j+1)$. Further, note that we have an isomorphism between $B^{\text{rigid}}(Q_0, r, N, k)$ and $M(Q_0, r, N, k)$ from Prop 5.12, which is $\sum b_a \to$ "$\sum\limits_{a \geq 0} \frac{r^a \cdot b_a}{(E_{p-1})^a}$", but note that a map of sums of this type can be separated into a set of maps $b_a \to$ "$\frac{r^a \cdot b_a}{(E_{p-1})^a}$" for each $B(Q_0, N, k, a)$. Applying these maps, we get an orthonormal basis $\{e_{i,s}\}_{i \geq 0,\ s=0}^{s=m_i}$ of $M(Q, r, N, k)$.

Now, write $T_p \circ G(q)^j(e_{i,s}) = \sum\limits_{u,v} A_{i,s}^{u,v}(j) e_{u,v}$, where $G(q)^j$ is defined as in the algorithm. This is possible, as we simply take $A_{i,s}^{u,v}(j)$ to be the matrix defined by this operator. Then, as noted by Wan [12, p.457], since $G(q)^j \in M(Q_0, r, N, 0)$, we get that $\text{ord}_p\big(A_{i,s}^{u,v}(j)\big) \geq u(p-1)\text{ord}_p(r) - 1$. This is the final result we need before we prove the correctness of the algorithms.

Proof of correctness for level $\Gamma_1(1)$ algorithm:

Let p be a prime ≥ 5, let k be an integer, and let m be a positive integer, as required for the algorithm of level $\Gamma_1(1)$.

First, $\forall\ i \geq 0$, define $d_i = \dim\big(M(\mathbb{Z}_p, 1, k_0 + i(p-1))\big)$ and $m_i = \dim\big(B(1, k, i)\big)$. Note that these definitions match up with the ones given in the algorithm, because the basis of $B(1, k, i)$ is W_i, which by definition has m_i elements. This implies that $d_0 = m_0$ and $d_i = m_i - m_{i-1}$ for $i \geq 1$ as in the algorithm.

Now, we have the following lemma:

Lemma 6.4 [6, Lemma 3.2]:

For $0 \leq i \leq N$, the elements in W_i are the reduction modulo $(p^{m'}, q^{lp})$ of a basis for some choice of the space $B(1, k, j)$.

Proof of lemma:

Let $D_{k_0+i(p-1)}$ be as defined in the algorithm. Then for any i, the lowest term of the r^{th} element of $D_{k_0+i(p-1)}$ is q^{r-1}[11, Remark 2.21], which implies that for f_r the r^{th} element of $D_{k_0+i(p-1)}$ and for g with lowest term 1, then clearly gf_r has lowest term q^{r-1} as well. Note that the normalized Eisenstein series E_{p-1} has lowest term 1 by definition. Thus we can use E_{p-1} in place of g, and so $E_{p-1}f_r$ has lowest term q^{r-1}, and so the r^{th} element of the set $\{E_{p-1}f_y : f_y \in D_{k_0+(i-1)(p-1)}\} = \{E_{p-1}f_1,\ E_{p-1}f_2,\ ...,\ E_{p-1}f_r,\ ...\}$ has lowest term q^{r-1}.

Now, note that the m_i elements of W_i are the t^{th} elements of $D_{k_0+i(p-1)}$ for $d_i \geq t > d_{i-1}$, since they are the last m_i elements of $D_{k_0+i(p-1)}$, i.e. they are the $(d_{i-1}+1)^{th}$ element through the d_i^{th} element inclusively. Thus the elements in W_i have lowest term q^{t-1} respectively, for $d_i \geq t > d_{i-1} = \#D_{k_0+i(p-1)}$. Thus, we have that:

Any element of $\{E_{p-1}f : f \in D_{k_0+(i-1)(p-1)}\}$ has lowest term q^{t-1} for some $t \leq d_{i-1}$;

and, as we just proved:

any element in W_i has lowest term q^{t-1} for some $t > d_{i-1}$.

This implies there is no element of W_i whose lowest term is equal to the lowest term of any element of $\{E_{p-1}f : f \in D_{k_0+(i-1)(p-1)}\}$. Further, note that taking this modulo $(p^{m'}, q^{lp})$ does not change this, because $l * p > d_i$. Thus we have proven that, for any element of $E_{p-1} \cdot M(\mathbb{Z}_p, 1, k_0 + (i-1)(p-1))$, we can not construct its reduction modulo $(p^{m'}, q^{lp})$ as a non-zero $\frac{\mathbb{Z}}{p^{m'}}$-linear combination of elements of W_i.

Note that $B(1, k, j)$ is the complement of $E_{p-1} \cdot M(\mathbb{Z}_p, 1, k_0+(i-1)(p-1))$, and so $M(\mathbb{Z}_p, N, k_0 + i(p-1)) = E_{p-1} \cdot M(\mathbb{Z}_p, 1, k_0 + (i-1)(p-1)) \bigoplus B(1, k, j)$, which finally implies that the elements of W_i are the reduction modulo $(p^{m'}, q^{lp})$ of a basis for some choice of the space $B(1, k, j)$.

Q.E.D.

Now, we will use this to prove correctness for a simplified version of the algorithm. The simplifications are:

Simplification 1) Let $\epsilon > 0$ be an arbitrary rational number. Define $n_\epsilon := \lfloor \frac{(p+1)+\epsilon}{p-1}(m+1) \rfloor$. Define $l_\epsilon := d_{n_\epsilon}$. For all instances of the variables n and l in the algorithm, replace n by n_ϵ and replace l by l_ϵ;

Simplification 2) Choose B some extension of $\mathbb{Z}_p$ and choose $r \in B$ such that $\mathrm{ord}_p(r) = \frac{1}{p+1+\epsilon}$. redefine $e_{i,s}$ in the algorithm as $e_{i,s} = r^i E_{p-1}^{-i}(q) W_i[s]$;

Simplification 3) Instead of doing all of the computations throughout the algorithm over the quotient space $\frac{\mathbb{Z}}{(p^{m'})}$, or rather $\frac{B}{(p^{m'})}$ after implementing simplification 2, do the computations directly in B without taking the modulus.

Proof of simplified algorithm:

First, we prove that the output of this algorithm is the top lefthand corner of the matrix $A_{i,s}^{u,v}(j)$ which is defined by the equation $T_p\big(G(q)^j(e_{i,s})\big) = \sum\limits_{u,v} A_{i,s}^{u,v}(j) e_{u,v}$ from remark 6.3.

Note that we have $T = AE$ from the algorithm. Note that, recalling the definition of T and E from the algorithm, $T = AE$ implies:

$$\begin{bmatrix} t_{1,1} \\ t_{1,2} \\ \dots \\ t_{i_{max},s_{max}} \end{bmatrix} = A \begin{bmatrix} e_{1,1} \\ e_{1,2} \\ \dots \\ e_{u_{max},v_{max}} \end{bmatrix}$$

with indices chosen to match $A_{i,s}^{u,v}(j)$. As A is an $l_\epsilon \times l_\epsilon$ matrix, and we have exactly l_ϵ elements $t_{i,s}$ and l_ϵ elements $e_{u,v}$, we can label the entries of A by the pairs (i,s) and (u,v), as $a_{(i,s),(u,v)}$. Then, performing the matrix multiplication, we obtain $t_{i,s} = a_{(i,s),(1,1)} e_{1,1} + \dots + a_{(i,s),(u_{max},v_{max})} e_{u_{max},v_{max}}$, i.e. $t_{i,s} = \sum\limits_{u,v} a_{(i,s),(u,v)} e_{u,v}$.

Furthermore, note that $T_p\big(G(q)^j(e_{i,s})\big) = t_{i,s}$ by definition, and so, combining these two equations, we have that $T_p\big(G(q)^j(e_{i,s})\big) = t_{i,s} = \sum\limits_{u,v} a_{(i,s),(u,v)} e_{u,v}$.

Finally, from simplification 2, we have that $0 < \mathrm{ord}_p(r) = \frac{1}{p-1+\epsilon} < \frac{1}{p-1}$, so we can see from (6.3) that $e_{i,s}$ for $0 \le i$, $1 \le s \le m_i$ forms an orthonormal basis for the p-adic Banach space $M(R, r, N, k)$ so the $e_{u,v}$ and $t_{i,s}$ indeed match up between these two cases. Thus A is indeed the top lefthand corner of $A_{i,s}^{u,v}(j)$, as desired.

Now, we examine the matrix $A_{i,s}^{u,v}(j)$ to determine that the output of the algorithm is indeed what is required.

Note that for $u \ge \frac{p+1+\epsilon}{p-1}(m+1)$, and for $1 \le v \le m_u$ we have:

$$\begin{aligned} \mathrm{ord}_p\big(A_{i,s}^{u,v}(j)\big) &\ge u(p-1)\mathrm{ord}_p(r) - 1 \text{ by (6.3)} \\ &= u(p-1)\frac{1}{p+1+\epsilon} - 1 \\ &\ge \frac{p+1+\epsilon}{p-1}(p-1)\frac{1}{p+1+\epsilon}(m+1) - 1 = m. \end{aligned}$$

Which implies that $\mathrm{ord}_p(A_{i,s}^{u,v}(j)) \ge m$, so all of the coefficients in the rows of $A_{i,s}^{u,v}(j)$ labeled by pairs (u,v) where $u \ge \frac{p+1+\epsilon}{p-1}(m+1)$ and $1 \le v \le m_u$ have p-adic valuation greater than or equal to m. Now, note that $u \geq 0$, $(p-1) \geq 0$ and $\mathrm{ord}_p(r) \geq 0$. Thus $\mathrm{ord}_p\big(A^{u,v}_{i,s}(j)\big) \geq -1$ by (6.3), and we can split this into two cases, $\mathrm{ord}_p\big(A^{u,v}_{i,s}(j)\big) = -1$ or ≥ 0.

If $\mathrm{ord}_p\big(A^{u,v}_{i,s}(j)\big) \geq 0$, then the entries are of the form x for $x \in \mathbb{Z}$, and thus the matrix $\big(A^{u,v}_{i,s}(j)\big)$ has integral entries. If $\mathrm{ord}_p\big(A^{u,v}_{i,s}(j)\big) = -1$, then the entries are of the form $\frac{x}{p}$ for $x \in \mathbb{Z}$, which then implies that $p\big(A^{u,v}_{i,s}(j)\big)$ has entries of the form x for $x \in \mathbb{Z}$, and so $p\big(A^{u,v}_{i,s}(j)\big)$ has integral entries.

In the case of $A^{u,v}_{i,s}(j)$ having integral entries, reducing $\big(A^{u,v}_{i,s}(j)\big)$ modulo p^m results in an $l_\epsilon \times \infty$ matrix, as stated by Lauder in "Computations with classical and p-adic modular forms"[6]. Indeed, for example, for $N \geq 2$, the proof is as follows:

Note that $\mathrm{ord}_p\big(A^{u,v}_{i,s}(j)\big) \geq m$ for $u \geq \frac{p+1+\epsilon}{p-1}(m+1)$, i.e. the entries of the rows are equivalent to $0 \bmod p^m$ for $u \geq \frac{p+1+\epsilon}{p-1}(m+1)$. Note also that $n_\epsilon = \lfloor \frac{p+1+\epsilon}{p-1}(m+1) \rfloor$. This implies that $u \geq n_\epsilon$, and so, in the worst case scenario, we have $\mathrm{ord}_p\big(A^{u,v}_{i,s}(j)\big) \geq m \ \forall\ u \geq n_\epsilon + 1$.

Now, note that we can view $\big(A^{u,v}_{i,s}(j)\big)$ modulo p^m as an $l_\epsilon \times \infty$ matrix if the entries for the rows past row l_ϵ are zero modulo p^m. Thus what we want is to prove that $\mathrm{ord}_p\big(A^{u,v}_{i,s}(j)\big) \geq m \ \forall\ u \geq l_\epsilon$. Recall the definition of l_ϵ: $l_\epsilon = d_{n_\epsilon}$, where d_i is defined to be the dimension of the space of modular forms of level $\Gamma_1(N)$ and weight $k_0 + i(p-1)$. Thus what we need to prove is that $l_\epsilon = d_{n_\epsilon} \geq n_\epsilon + 1$, i.e. we need to prove that $d_i \geq i + 1$.

This is indeed true for $N \geq 2$. Indeed, for modular forms of even weight, the equation for the dimension of the space of modular forms of level $\Gamma_1(N)$ and weight $k_0 + i(p-1)$ is [2] $\big(k_0 + i(p-1) - 1\big)(g_N - 1) + \lfloor \frac{k_0 + i(p-1)}{4} \rfloor \epsilon_2 + \lfloor \frac{k_0 + i(p-1)}{3} \rfloor \epsilon_3 + \frac{k_0 + i(p-1)}{2}$, where g_N is the genus of $\Gamma_1(N)$, ϵ_2 is the number of elliptic points of order 2, ϵ_3 is the number of elliptic points of order 3, and ϵ_∞ is the number of cusps. The rate at which this grows with respect to i increases as N increases, and even at $N = 2$, the genus is 3, so the dimension increases faster than i. Further, even at $i = 0$, $k_0 = 2$, we get $d_0 = 1 = 0 + 1$, so $d_i \geq i + 1$.

As for modular forms of odd weight, the equation for the dimension becomes [2] $\big(k_0 + i(p-1) - 1\big)(g_N - 1) + \lfloor \frac{k}{3} \rfloor \epsilon_3 + \frac{k}{2} \epsilon_\infty^{reg} + \frac{k-1}{2} \epsilon_\infty^{irr}$, where ϵ_∞^{reg} is the number of regular cusps and ϵ_∞^{irr} is the number of irregular cusps. Once again, as N increases, the rate at which the dimension grows with respect to i also increases, and even at $N = 3$, the smallest N where odd weights are possible, the genus is 8, so the dimension increases faster than i. Further, even at $i = 0$, $k_0 = 1$, we get $d_0 = 1 = 0 + 1$, so $d_i \geq i + 1$.

This implies that for $N \geq 2$, $d_i \geq i + 1$, which implies that $\mathrm{ord}_p(A^{u,v}_{i,s}(j)) \geq m \ \forall\ u \geq l_\epsilon$. Thus reducing $\big(A^{u,v}_{i,s}(j)\big)$ modulo p^m results in an $l_\epsilon \times \infty$ matrix for the $N \geq 2$ case.

The fact that reducing $\big(A^{u,v}_{i,s}(j)\big)$ modulo p^m results in an $l_\epsilon \times \infty$ matrix implies that the reverse characteristic series of $A^{u,v}_{i,s}(j)$ is congruent to the reverse characteristic polynomial of A $\bmod p^m$.

Indeed, as an example, for $l_\epsilon = 2$, let:

$$A_{i,s}^{u,v}(j) \bmod p^m = \begin{bmatrix} a & b & e & \dots \\ c & d & f & \dots \\ 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

and

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Now, calculate the reverse characteristic polynomial of $A_{i,s}^{u,v}(j) \bmod p^m$:

$$\det\big(I - tA_{i,s}^{u,v}(j)\big) \bmod p^m = \det\left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} -ta & -tb & -te \\ -tc & -td & -tf \\ 0 & 0 & 0 \end{bmatrix}\right) = \det\left(\begin{bmatrix} 1-ta & -tb & -te \\ -tc & 1-td & -tf \\ 0 & 0 & 1 \end{bmatrix}\right)$$

$$= \det\left(\begin{bmatrix} 1-ta & -tb \\ -tc & 1-td \end{bmatrix}\right).$$

Now, calculate the reverse characteristic polynomial of A:

$$\det(I - tA) = \det\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} -ta & -tb \\ -tc & -td \end{bmatrix}\right)$$

$$= \det\left(\begin{bmatrix} 1-ta & -tb \\ -tc & 1-td \end{bmatrix}\right).$$

Which is the same result as for $A_{i,s}^{u,v}$, and so the reverse characteristic polynomials of A and $A_{i,s}^{u,v}(j)$ are congruent modulo p^m, which concludes this example.

The fact that the two reverse characteristic polynomials are congruent implies that the second to last line of the algorithm is indeed the characteristic polynomial we want, which implies that the output of the algorithm is indeed the inverse of the eigenvalues that we want, modulo p^m.

Now, in the case of $A_{i,s}^{u,v}(j)$ not having integral entries, The same argument outputs the reverse characteristic series of $pT_p \bmod p^m$ instead of T_p. However, note that if we have $\det(1 - pAt) \bmod p^{f(p)m}$, where f is some polynomial function, then we can calculate $\det(1-At) \bmod p^m$. Indeed, we can show this as follows:

First, try $f(p) = p$, the smallest possible polynomial, in characteristic 0. In this case, we have: $\det(I - Apt) \bmod p^{pm} = 1 + a_1pt + a_2(pt)^2 + ... + a_l(pt)^l$, and what we want to calculate is $\det(I - At) \bmod p^m = 1 + b_1t + b_2t^2 + ... + b_lt^l$. In order to do this, we take $\frac{a_1}{p}, \frac{a_2}{p^2}, ..., \frac{a_l}{p^l}$, thus we lose at most a precision of l, and we get $\det(I - At) \bmod p^{pm-l} = 1 + \frac{a_1}{p}t + ... + \frac{a_l}{p^l}t^l$.

Thus, as long as $pm - l \geq m$, then we can reduce modulo p^m and get the coefficients we want. Thus to calculate $\det(1 - At) \bmod p^m$, we need $pm - m \geq l$, i.e. we need $(p-1)m \geq l$. We can increase m until this is true, as l increases more slowly than m, so for sufficiently large m, we can indeed calculate $\det(1 - At) \bmod p^m$. Since $f(p) = p$ is the smallest non-constant, non-zero polynomial then we can do this for any other polynomial as well, and so this is proven for any polynomial $f(p)$.

Furthermore, in both the original paper by Lauder and in our work, the second case never arose, so it is likely that this can be ignored for most situations. Thus, we have proven the simplified algorithm.

Q.E.D.

Now, we want to use the fact that the simplified algorithm is true to prove that the unmodified algorithm is true. We will do this by proving that we can remove each simplification in turn.

• To remove simplification 3, we require $\det(1 - At) \bmod p^m$ to give the same result when A is calculated modulo $p^{m'}$ rather than modulo p^m. In order to solve $T = AE$ for A, we invert the matrix E and solve $A = TE^{-1}$. In the case of working over $\frac{B}{(p^{m'})}$, this calculation is:

$$T = AE \bmod p^{m'} \implies A = TE^{-1} \bmod p^{m' + \mathrm{ord}_p(E^{-1})}$$

Now, the final result of the algorithm is reduced modulo p^m, so for the algorithm to output the same result without simplification 3, we need $m' + \mathrm{ord}_p(E^{-1}) \geq m$.

Note that $\mathrm{ord}_p(e_{i,s}) \leq \frac{n_\epsilon}{p+1}$. Since E is upper triangular, this implies that $\mathrm{ord}_p(E^{-1}) \geq \frac{-n_\epsilon}{p+1}$.

Indeed, let M be an upper triangular $n \times n$ matrix $\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \dots & a_{1,n} \\ 0 & a_{2,2} & a_{2,3} & \dots & a_{2,n} \\ 0 & 0 & a_{3,3} & \dots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{n,n} \end{bmatrix}$.

Then M^{-1} is:

$$\begin{bmatrix} \frac{1}{a_{1,1}} & \frac{-a_{1,2}}{a_{1,1}a_{2,2}} & \frac{\det(A)}{a_{1,1}a_{2,2}a_{3,3}} & \frac{\det(B)}{a_{1,1}a_{2,2}a_{3,3}a_{4,4}} & \frac{\det(C)}{a_{1,1}a_{2,2}a_{3,3}a_{4,4}a_{5,5}} & \dots \\ 0 & \frac{1}{a_{2,2}} & \frac{-a_{2,3}}{a_{2,2}a_{3,3}} & \frac{\det(D)}{a_{2,2}a_{3,3}a_{4,4}} & \frac{\det(E)}{a_{2,2}a_{3,3}a_{4,4}a_{5,5}} & \dots \\ \vdots & & \ddots & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ \vdots & & & & \ddots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \frac{1}{a_{n,n}} \end{bmatrix}$$

where we let $A = 2 \times 2$ submatrix of M with $a_{1,3}$ in its top right corner, $B = 3 \times 3$ submatrix of M with $a_{1,4}$ in its top right corner, $C = 4 \times 4$ submatrix of M with $a_{1,5}$ in its top right corner, $D = 2 \times 2$ submatrix of M with $a_{2,4}$ in its top right corner and $E = 3 \times 3$ submatrix of M with $a_{2,5}$ in its top right corner.

Note that we always have exactly one more element of M multiplied in the denominator than in the numerator. Since $\mathrm{ord}_p(e_{i,s}) \leq \frac{n_\epsilon}{p+1}$, if we assume every element has the maximal valuation of $\frac{n_\epsilon}{p+1}$, then each non-zero element of the inverse has p-adic valuation $\geq \frac{-n_\epsilon}{p+1}$, since all but one order cancel, which implies that $\mathrm{ord}_p(E^{-1}) \geq \frac{-n_\epsilon}{p+1}$, as expected. This implies that $m' + \mathrm{ord}_p(E^{-1}) \geq m' - \frac{n_\epsilon}{p+1}$, but $\frac{n_\epsilon}{p+1} \leq \lceil \frac{n_\epsilon}{p+1} \rceil = m' - m$, and so $m' + \mathrm{ord}_p(E^{-1}) \geq m' - \frac{n_\epsilon}{p+1} \geq m' - (m' - m) = m$, i.e. $m' + \mathrm{ord}_p(E^{-1}) \geq m$.

As mentioned earlier, this is sufficient to prove that the algorithm outputs the same result working over $\frac{B}{(p^{m'})}$, and so simplification 3 can be removed.

• To remove simplification 1, simply note that we can choose ϵ to be any real number > 0, so simply choose ϵ small enough that $n_\epsilon = \lfloor \frac{(p+1)+\epsilon}{p-1}(m+1) \rfloor = n$, and so $l = l_\epsilon$ as well. Thus simplification 1 can be removed.

• To remove simplification 2, note that the only difference left is that in the original algorithm we define $e_{i,s} = p^{\lfloor \frac{i}{p-1} \rfloor} E_{p-1}^{-i}(q) W_i[s]$ and in the simplified algorithm we define $e_{i,s} = r^i E_{p-1}^{-i}(q) W_i[s]$, $\text{ord}_p(r) = \frac{1}{p+1+\epsilon}$.

Note that we can define a diagonal matrix P_ϵ which acts as a change of basis matrix, where the entries on the diagonal are $\delta_{i,s} := r^i p^{-\lfloor \frac{i}{p-1} \rfloor}$, s.t $0 \leq \text{ord}_p(\delta_{i,s}) < 1$. For the order of r^i to be sufficient to cancel out the order of $p^{-\lfloor \frac{i}{p-1} \rfloor}$ such that $0 \leq \text{ord}_p(\delta_{i,s}) < 1$, we may need to shrink ϵ again, but this does not cause any issues.

This change of basis matrix does indeed transform from the basis of the original case to the basis of the simplified case. Indeed:

$P_\epsilon e_{i,s} = P_\epsilon \frac{p^{\lfloor \frac{i}{p-1} \rfloor}}{E_{p-1}^{-i}(q)} W_i[s]$

$= \delta_{i,s} \frac{p^{\lfloor \frac{i}{p-1} \rfloor}}{E_{p-1}^{-i}(q)} W_i[s]$ because $e_{i,s}$ is the reduction mod $(p^{m'}, q^{l,p})$ of the basis of $B(N,k,j)$ by lemma 6.4.

$= \frac{r^i p^{\lfloor \frac{i}{p-1} \rfloor} p^{-\lfloor \frac{i}{p-1} \rfloor}}{E_{p-1}^{i}(q)} W_i[s]$

$= \frac{r^i}{E_{p-1}^{i}(q)} W_i[s]$, which is the (reduced) basis we calculate in the simplified case.

Now, define $\gamma := max\{\text{ord}_p(\delta_{i,s})\} < 1$ and let A_ϵ be the matrix resulting from the application of the revised simplified algorithm, i.e. the algorithm with only simplification 2 applied, and let A be the matrix resulting from the full unmodified level $\Gamma_1(1)$ algorithm.

Now, the way we obtain A_ϵ is by using a different basis, so if we are working in characteristic 0, i.e. modulo p^∞, then P_ϵ immediately gives $P_\epsilon^{-1} A P_\epsilon = A$.

Now, for $\bmod m$ cases, for 2×2 matrices:

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, let $A_\epsilon = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$, and let $P_\epsilon = \begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix}$, where $x_1 = r^1 p^{\lfloor \frac{1}{p-1} \rfloor}$ and $x_2 = r^2 p^{\lfloor \frac{2}{p-1} \rfloor}$.

Then $P_\epsilon^{-1} A P_\epsilon = \begin{bmatrix} a & b\frac{x_2}{x_1} \\ c\frac{x_1}{x_2} & d \end{bmatrix}$. Thus we have a loss of precision only from $\frac{x_1}{x_2}$ and $\frac{x_2}{x_1}$. Now, $\gamma = max(\text{ord}_p(x_i))$, so in the worst case scenario, we lose a precision of γ. This implies we have the equality $\bmod p^{m-\gamma}$, rather than $\bmod p^m$, i.e. $P_\epsilon^{-1} A P_\epsilon \equiv A_\epsilon \bmod p^{m-\gamma}$. This proof holds in exactly the same way for $n \times n$ matrices of any size. This implies that $A_\epsilon \equiv P_\epsilon^{-1} A P_\epsilon \bmod p^{m-\gamma}$ in all cases.

If $A_{i,s}^{u,v}(j)$ has integral entries, this is sufficient to prove the correctness of the algorithm. Indeed, since $m - \gamma \geq m$, taking $\bmod p^m$ will not change the equality we have, and so we get $\det(1 - At) \equiv \det(1 - A_\epsilon t) \equiv \det\big(1 - A_{i,s}^{u,v}(j)t\big) \bmod p^m$ because $m - \gamma > m - 1$, as required.

Finally, if $A_{i,s}^{u,v}(j)$ does not have integral entries, simply define $p\big(A_{i,s}^{u,v}(j)\big)$, and then apply the same procedure to this matrix. We get the characteristic series of $pT_p \bmod p^m$ instead of T_p, as required.

Q.E.D.

Proof of correctness for the level $\Gamma_1(N)$ algorithm:

This proof is the same as for the level $\Gamma_1(1)$ algorithm, with one difference: instead of the lemma we use at the beginning of that proof, we instead use the following lemma:

Lemma 6.5 [6, Lemma 3.6]:

For $0 \leq i \leq n$, the elements in W_i from step 2 of the algorithm are the reduction modulo $(p^{m'}, q^{l'p})$ of a basis for some choice of the space $B(N, k, j)$.

Proof of lemma:

Note that $E_{p-1}(q)$ has leading term 1. This is a property of the normalized Eisenstein series. Then, by considering the row reduced bases $D_{k_0+i(p-1)}$ and $D_{k_0+(i-1)(p-1)}$, defined the same way as earlier, we can find a space C in $M\big(\mathbb{Z}_p, N, k_0 + i(p-1)\big)$ such that $M\big(\mathbb{Z}_p, N, k_0 + i(p-1)\big) = E_{p-1} \cdot M\big(\mathbb{Z}_p, N, k_0 + (i-1)(p-1)\big) \bigoplus C$. Indeed, as noted in Definition 3.13, modular forms of level $\Gamma(N)$ and weight k defined over $\mathbb{Z}_p$ can be viewed as elements of $H^0\big(\overline{M}_N, (\underline{\omega})^{\bigotimes k}\big)$. Thus, $M(\mathbb{Z}_p, N, k) = H^0\big(\overline{M}_N, (\underline{\omega})^{\bigotimes k}\big)$, and so, by (5.10.2), we know that $M\big(\mathbb{Z}_p, N, k_0 + i(p-1)\big) = E_{p-1} \cdot M\big(\mathbb{Z}_p, N, k_0 + (i-1)(p-1)\big) \bigoplus B(N, k, j)$.

Now, take an element u of $E_{p-1} \cdot M\big(\mathbb{Z}_p, N, k_0 + (i-1)(p-1)\big)$ which is also an element of the basis $E_{p-1} \cdot D_{k_0+(i+1)(p-1)}$ of $E_{p-1} \cdot M\big(\mathbb{Z}_p, N, k_0 + (i-1)(p-1)\big)$.
$\Longrightarrow$ $u = E_{p-1} \cdot x$ for some $x \in M\big(\mathbb{Z}_p, N, k_0 + (i-1)(p-1)\big)$
$= E_{p-1} \cdot b_{i,s}$ where $b_{i,s} \in D_{k_0+(i-1)(p-1)}$ since $D_{k_0+(i-1)(p-1)}$ is a basis.
This then implies that

$$\begin{aligned} \operatorname{ord}_p(u) &= \operatorname{ord}_p(E_{p-1} \cdot b_{i,s}) \\ &= \operatorname{ord}_p\big((1 - \sum_{n=1} a_n q^n) \cdot b_{i,s}\big) \\ &= \operatorname{ord}_p(b_{i,s} + b_{i,s} \sum_{n=1} a_n q^n) \\ &= \operatorname{ord}_p(b_{i,s}). \end{aligned}$$

This implies that for any element x of the basis $D_{k_0+i(p-1)}$ of $M\big(\mathbb{Z}_p, N, k_0 + i(p-1)\big)$, $x \in E_{p-1} \cdot M\big(\mathbb{Z}_p, N, k_0 + (i-1)(p-1)\big)$ iff $\operatorname{ord}_p(x) = \operatorname{ord}_p(b_{i,s})$ for some $b_{i,s} \in D_{k_0+(i+1)(p-1)}$. Note that looking at the position of the leading entries of the matrices gives the valuation of the corresponding q-expansion. Therefore, if the position of the leading entry of a certain row of the matrix corresponding to the base $D_{k_0+i(p-1)}$ is different from the position of the leading entry of any row of the matrix corresponding to the base $D_{k_0+(i+1)(p-1)}$, then it is not part of the basis of $E_{p-1} \cdot M\big(\mathbb{Z}_p, N, k_0 + (i-1)(p-1)\big)$.

But note that a property of the direct sum is $A = B \bigoplus C \Leftrightarrow \mathsf{basis}_A = \mathsf{basis}_B \bigcup \mathsf{basis}_C$, and we know that $\left(\mathsf{basis}_{M(\mathbb{Z}_p,N,k_0+i(p-1))}\right) = \left(\mathsf{basis}_{E_{p-1}\cdot M\left(\mathbb{Z}_p,N,k_0+(i-1)(p-1)\right)}\right) \bigcup W_i$. Together, this implies that $M\big(\mathbb{Z}_p, N, k_0 + i(p-1)\big) = E_{p-1} \cdot M\big(\mathbb{Z}_p, N, k_0 + (i-1)(p-1)\big) \bigoplus \mathit{Span}(W_i)$.

Note that we also know that $M\big(\mathbb{Z}_p, N, k_0 + i(p-1)\big) = E_{p-1} \cdot M\big(\mathbb{Z}_p, N, k_0 + (i-1)(p-1)\big) \bigoplus B(N, k, j)$, from (5.10.2). Further, note that since l' is the Sturm bound, then if one of the rows reduces to a row of zeros modulo $q^{l'}$, then by definition of the Sturm bound the q-expansion is itself zero, since this means that all coefficients of the q-expansion of order $< l'$ are 0, but this is impossible because 0 cannot be an element of a basis. Thus none of the rows reduce to a row of zeros.

Thus $B(N, k, j)$ and $\mathit{Span}(W_i)$ are equivalent, modulo $p^{m'}$ since the bases we used were already reduced, as defined in the algorithm.

Q.E.D.

So we have an analogue of lemma 6.4, and it is trivial to see that using this lemma, the rest of the proof is exactly the same as in the level $\Gamma_1(1)$ case.

7 Results

Using the Sagemath computer algebra program, we wrote a program to implement the algorithm described in the previous section, and ran it for many different combinations of inputs. As noted in the previous section, the algorithm takes as input 4 variables: p, a prime number greater than or equal to 5; an integer k, the weight of the modular forms; a positive integer N, which defines the level $\Gamma_1(N)$ of the modular forms; and a positive integer m, which defines the precision.

For each triplet (N, p, m), $N = 1$, $m = 100$, $5 \leq p \leq 19$ or 23, p prime, we calculated the slopes of the inverse of the first few eigenvalues of T_p for $k = 2 + (p^2)(p-1)j$ for j running from 0 to 10 or 20, as well as for $k = 4 + (p^2)(p-1)j$ for j running from 0 to 10 or 20. We then repeated a similar process for $N = 2$. After this, we repeated the same process, for $N = 1, 2$ and 3, using $k = 2 + p(p-1)j$ and $k = 4 + p(p-1)j$ rather than $k = 2 + (p^2)(p-1)j$ and $k = 4 + (p^2)(p-1)j$. The data is as follows:

Figure 3: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 1$ *and weight* $k = 2 + p^2(p-1)j$ *for* j *running from* 0 *to* 10.

(a) $p = 5$, $m = 100$

k	Slopes
2	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
102	0,-2,-5,-6,-9,-10,-11,-14,-15,
202	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
302	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
402	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
502	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
602	0,-2,-5,-6,-9,-10,-11,-14,-15,-21
702	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
802	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
902	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
1002	0,-2,-5,-6,-9,-10,-11,-14,-15,-20

(b) $p = 7$, $m = 100$

k	Slopes
2	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
296	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
590	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
884	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
1178	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
1472	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
1766	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
2060	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
2354	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
2648	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
2942	0,-2,-3,-4,-7,-8,-9,-11,-13,-14

(c) $p = 11$, $m = 100$

k	Slopes
2	0,0,-2,-3,-4,-5,-5,-6,-7,-8
1212	0,0,-2,-3,-4,-5,-5,-6,-7,-8
2422	0,0,-2,-3,-4,-5,-5,-6,-7,-8
3632	0,0,-2,-3,-4,-5,-5,-6,-7,-8
4842	0,0,-2,-3,-4,-5,-5,-6,-7,-8
6052	0,0,-2,-3,-4,-5,-5,-6,-7,-8
7262	0,0,-2,-3,-4,-5,-5,-6,-7,-8
8472	0,0,-2,-3,-4,-5,-5,-6,-7,-8
9682	0,0,-2,-3,-4,-5,-5,-6,-7,-8
10892	0,0,-2,-3,-4,-5,-5,-6,-7,-8
12102	0,0,-2,-3,-4,-5,-5,-6,-7,-8

(d) $p = 13$, $m = 100$

k	Slopes
2	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
2030	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
4058	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
6086	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
8114	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
10142	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
12170	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
14198	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
16226	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
18254	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
20282	0,-1,-2,-3,-4,-5,-6,-6,-6,-7

(e) $p = 17$, $m = 100$

k	Slopes
2	0,0,-1,-2,-3,-3,-4,-5,-6,-6
4626	0,0,-1,-2,-3,-3,-4,-5,-6,-6
9250	0,0,-1,-2,-3,-3,-4,-5,-6,-6
13874	0,0,-1,-2,-3,-3,-4,-5,-6,-6
18498	0,0,-1,-2,-3,-3,-4,-5,-6,-6
23122	0,0,-1,-2,-3,-3,-4,-5,-6,-6
27746	0,0,-1,-2,-3,-3,-4,-5,-6,-6
32370	0,0,-1,-2,-3,-3,-4,-5,-6,-6
36994	0,0,-1,-2,-3,-3,-4,-5,-6,-6
41618	0,0,-1,-2,-3,-3,-4,-5,-6,-6
46242	0,0,-1,-2,-3,-3,-4,-5,-6,-6

(f) $p = 19$, $m = 100$

k	Slopes
2	0,0,-1,-2,-2,-3,-4,-4,-5,-6
6500	0,0,-1,-2,-2,-3,-4,-4,-5,-6
12998	0,0,-1,-2,-2,-3,-4,-4,-5,-6
19496	0,0,-1,-2,-2,-3,-4,-4,-5,-6
25994	0,0,-1,-2,-2,-3,-4,-4,-5,-6
32492	0,0,-1,-2,-2,-3,-4,-4,-5,-6
38990	0,0,-1,-2,-2,-3,-4,-4,-5,-6
45488	0,0,-1,-2,-2,-3,-4,-4,-5,-6
51986	0,0,-1,-2,-2,-3,-4,-4,-5,-6
58484	0,0,-1,-2,-2,-3,-4,-4,-5,-6
64982	0,0,-1,-2,-2,-3,-4,-4,-5,-6

(g) $p = 23$, $m = 100$

k	Slopes
2	0,0,0,-1,-2,-2,-3,-3,-4,-4
11640	0,0,0,-1,-2,-2,-3,-3,-4,-4
23278	0,0,0,-1,-2,-2,-3,-3,-4,-4
34916	0,0,0,-1,-2,-2,-3,-3,-4,-4
46554	0,0,0,-1,-2,-2,-3,-3,-4,-4
58192	0,0,0,-1,-2,-2,-3,-3,-4,-4
69830	0,0,0,-1,-2,-2,-3,-3,-4,-4
81468	0,0,0,-1,-2,-2,-3,-3,-4,-4
93106	0,0,0,-1,-2,-2,-3,-3,-4,-4
104744	0,0,0,-1,-2,-2,-3,-3,-4,-4
116382	0,0,0,-1,-2,-2,-3,-3,-4,-4

Figure 4: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 1$ *and weight* $k = 4 + p^2(p-1)j$ *for* j *running from* 0 *to* 10.

(a) p=5, $m = 100$

k	Slopes
4	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
104	0,-1,-3,-5,-8,-10,-11,-12,-14
204	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
304	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
404	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
504	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
604	0,-1,-3,-5,-8,-10,-11,-12,-14,-19
704	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
804	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
904	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
1004	0,-1,-3,-5,-8,-10,-11,-12,-14,-18

(b) $p = 7$, $m = 100$

k	Slopes
4	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
298	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
592	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
886	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
1180	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
1474	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
1768	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
2062	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
2356	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
2650	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
2944	0,-1,-3,-4,-6,-7,-9,-10,-12,-14

(c) $p = 11$, $m = 100$

k	Slopes
4	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
1214	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
2424	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
3634	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
4844	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
6054	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
7264	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
8474	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
9684	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
10894	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
12104	0,-1,-1,-3,-4,-5,-6,-6,-7,-8

(d) $p = 13$, $m = 100$

k	Slopes
4	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
2032	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
4060	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
6088	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
8116	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
10144	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
12172	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
14200	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
16228	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
18256	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
20284	0,-1,-1,-1,-3,-4,-5,-6,-7,-7

(e) $p = 17$, $m = 100$

k	Slopes
4	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
4628	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
9252	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
13876	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
18500	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
23124	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
27748	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
32372	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
36996	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
41620	0,-1,-1,-1,-1,-3,-4,-4,-5,-6
46244	0,-1,-1,-1,-1,-3,-4,-4,-5,-6

(f) $p = 19$, $m = 100$

k	Slopes
4	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
6502	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
13000	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
19498	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
25996	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
32494	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
38992	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
45490	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
51988	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
58486	0,-1,-1,-1,-1,-3,-3,-4,-5,-5
64984	0,-1,-1,-1,-1,-3,-3,-4,-5,-5

(g) $p = 23$, $m = 100$

k	Slopes
4	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
11642	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
23280	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
34918	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
46556	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
58194	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
69832	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
81470	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
93108	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
104746	0,-1,-1,-1,-1,-1,-3,-3,-4,-4
116384	0,-1,-1,-1,-1,-1,-3,-3,-4,-4

Figure 5: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 2$ *and weight* $k = 2 + p^2(p-1)j$ *for* j *running from* 0 *to* 10.

(a) p=5, $m = 100$

k	Slopes
2	0,0,-1,-2,-2,-2,-4,-5,-5,-6
102	0,0,-1,-2,-2,-2,-4,-5,-5,-6
202	0,0,-1,-2,-2,-2,-4,-5,-5,-6
302	0,0,-1,-2,-2,-2,-4,-5,-5,-6
402	0,0,-1,-2,-2,-2,-4,-5,-5,-6
502	0,0,-1,-2,-2,-2,-4,-5,-5,-6
602	0,0,-1,-2,-2,-2,-4,-5,-5,-6
702	0,0,-1,-2,-2,-2,-4,-5,-5,-6
802	0,0,-1,-2,-2,-2,-4,-5,-5,-6
902	0,0,-1,-2,-2,-2,-4,-5,-5,-6
1002	0,0,-1,-2,-2,-2,-4,-5,-5,-6

(b) $p = 7$, $m = 100$

k	Slopes
2	0,0,0,-1,-2,-2,-3,-3,-3,-3
296	0,0,0,-1,-2,-2,-3,-3,-3,-3
590	0,0,0,-1,-2,-2,-3,-3,-3,-3
884	0,0,0,-1,-2,-2,-3,-3,-3,-3
1178	0,0,0,-1,-2,-2,-3,-3,-3,-3
1472	0,0,0,-1,-2,-2,-3,-3,-3,-3
1766	0,0,0,-1,-2,-2,-3,-3,-3,-3
2060	0,0,0,-1,-2,-2,-3,-3,-3,-3
2354	0,0,0,-1,-2,-2,-3,-3,-3,-3
2648	0,0,0,-1,-2,-2,-3,-3,-3,-3
2942	0,0,0,-1,-2,-2,-3,-3,-3,-3

(c) $p = 11$, $m = 50$

k	Slopes
2	0,0,0,0,-1,-1,-2
1212	0,0,0,0,-1,-1,-2
2422	0,0,0,0,-1,-1,-2
3632	0,0,0,0,-1,-1,-2
4842	0,0,0,0,-1,-1,-2
6052	0,0,0,0,-1,-1,-2
7262	0,0,0,0,-1,-1,-2
8472	0,0,0,0,-1,-1,-2
9682	0,0,0,0,-1,-1,-2
10892	0,0,0,0,-1,-1,-2
12102	0,0,0,0,-1,-1,-2

(d) $p = 13$, $m = 50$

k	Slopes
2	0,0,0,0,-1,-1,-1
2030	0,0,0,0,-1,-1,-1
4058	0,0,0,0,-1,-1,-1
6086	0,0,0,0,-1,-1,-1
8114	0,0,0,0,-1,-1,-1
10142	0,0,0,0,-1,-1,-1
12170	0,0,0,0,-1,-1,-1
14198	0,0,0,0,-1,-1,-1
16226	0,0,0,0,-1,-1,-1
18254	0,0,0,0,-1,-1,-1
20282	0,0,0,0,-1,-1,-1

(e) $p = 17$, $m = 50$

k	Slopes
2	0,0,0,0,0,-1,-1
4626	0,0,0,0,0,-1,-1
9250	0,0,0,0,0,-1,-1
13874	0,0,0,0,0,-1,-1
18498	0,0,0,0,0,-1,-1
23122	0,0,0,0,0,-1,-1
27746	0,0,0,0,0,-1,-1
32370	0,0,0,0,0,-1,-1
36994	0,0,0,0,0,-1,-1
41618	0,0,0,0,0,-1,-1
46242	0,0,0,0,0,-1,-1

(f) $p = 19$, $m = 36$

k	Slope
2	0,0,0,0,0,0
6500	0,0,0,0,0,0
12998	0,0,0,0,0,0
19496	0,0,0,0,0,0
25994	0,0,0,0,0,0
32492	0,0,0,0,0,0
38990	0,0,0,0,0,0
45488	0,0,0,0,0,0
51986	0,0,0,0,0,0
58484	0,0,0,0,0,0
64982	0,0,0,0,0,0

Figure 6: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 2$ *and weight* $k = 4 + p^2(p-1)j$ *for* j *running from* 0 *to* 10.

(a) p=5, $m = 100$

k	Slope
4	0,0,-1,-1,-1,-3,-3,-4,-5,-5
104	0,0,-1,-1,-1,-3,-3,-4,-5,-5
204	0,0,-1,-1,-1,-3,-3,-4,-5,-5
304	0,0,-1,-1,-1,-3,-3,-4,-5,-5
404	0,0,-1,-1,-1,-3,-3,-4,-5,-5
504	0,0,-1,-1,-1,-3,-3,-4,-5,-5
604	0,0,-1,-1,-1,-3,-3,-4,-5,-5
704	0,0,-1,-1,-1,-3,-3,-4,-5,-5
804	0,0,-1,-1,-1,-3,-3,-4,-5,-5
904	0,0,-1,-1,-1,-3,-3,-4,-5,-5
1004	0,0,-1,-1,-1,-3,-3,-4,-5,-5

(b) $p = 7$, $m = 100$

k	Slopes
4	0,0,-1,-1,-1,-1,-3,-3,-4,-4
298	0,0,-1,-1,-1,-1,-3,-3,-4,-4
592	0,0,-1,-1,-1,-1,-3,-3,-4,-4
886	0,0,-1,-1,-1,-1,-3,-3,-4,-4
1180	0,0,-1,-1,-1,-1,-3,-3,-4,-4
1474	0,0,-1,-1,-1,-1,-3,-3,-4,-4
1768	0,0,-1,-1,-1,-1,-3,-3,-4,-4
2062	0,0,-1,-1,-1,-1,-3,-3,-4,-4
2356	0,0,-1,-1,-1,-1,-3,-3,-4,-4
2650	0,0,-1,-1,-1,-1,-3,-3,-4,-4
2944	0,0,-1,-1,-1,-1,-3,-3,-4,-4

(c) $p = 11$, $m = 50$

k	Slopes
4	0,0,-1,-1,-1,-1,-1
1214	0,0,-1,-1,-1,-1,-1
2424	0,0,-1,-1,-1,-1,-1
3634	0,0,-1,-1,-1,-1,-1
4844	0,0,-1,-1,-1,-1,-1
6054	0,0,-1,-1,-1,-1,-1
7264	0,0,-1,-1,-1,-1,-1
8474	0,0,-1,-1,-1,-1,-1
9684	0,0,-1,-1,-1,-1,-1
10894	0,0,-1,-1,-1,-1,-1
12104	0,0,-1,-1,-1,-1,-1

(d) $p = 13$, $m = 50$

k	Slopes
4	0,0,-1,-1,-1,-1,-1
2032	0,0,-1,-1,-1,-1,-1
4060	0,0,-1,-1,-1,-1,-1
6088	0,0,-1,-1,-1,-1,-1
8116	0,0,-1,-1,-1,-1,-1
10144	0,0,-1,-1,-1,-1,-1
12172	0,0,-1,-1,-1,-1,-1
14200	0,0,-1,-1,-1,-1,-1
16228	0,0,-1,-1,-1,-1,-1
18256	0,0,-1,-1,-1,-1,-1
20284	0,0,-1,-1,-1,-1,-1

(e) $p = 17$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
4628	0,0,-1,-1,-1,-1
9252	0,0,-1,-1,-1,-1
13876	0,0,-1,-1,-1,-1
18500	0,0,-1,-1,-1,-1
23124	0,0,-1,-1,-1,-1
27748	0,0,-1,-1,-1,-1
32372	0,0,-1,-1,-1,-1
36996	0,0,-1,-1,-1,-1
41620	0,0,-1,-1,-1,-1
46244	0,0,-1,-1,-1,-1

(f) $p = 19$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
6502	0,0,-1,-1,-1,-1
13000	0,0,-1,-1,-1,-1
19498	0,0,-1,-1,-1,-1
25996	0,0,-1,-1,-1,-1
32494	0,0,-1,-1,-1,-1
38992	0,0,-1,-1,-1,-1
45490	0,0,-1,-1,-1,-1
51988	0,0,-1,-1,-1,-1
58486	0,0,-1,-1,-1,-1
64984	0,0,-1,-1,-1,-1

Figure 7: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 1$ *and weight* $k = 2 + p(p-1)j$ *for* j *running from* 0 *to* 10.

(a) $p = 7$, $m = 100$

k	Slopes
2	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
44	0,-2,-3,-4,-21,-21,-21,-21
86	0,-2,-3,-4,-7,-8,-9,-42
128	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
170	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
212	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
254	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
296	0,-2,-3,-4,-7,-8,-9,-11,-13,-14
338	0,-2,-3,-4,-8,-9,-10,-12,-14,-15
380	0,-2,-3,-4,-7,-8,-9,-12,-14,-15
422	0,-2,-3,-4,-7,-8,-9,-11,-13,-14

(b) $p = 11$, $m = 100$

k	Slopes
2	0,0,-2,-3,-4,-5,-5,-6,-7,-8
112	0,0,-2,-3,-4,-5,-5,-6,-7,-8
222	0,0,-2,-3,-4,-5,-5,-6,-7,-8
332	0,0,-2,-3,-4,-5,-5,-6,-7,-8
442	0,0,-2,-3,-4,-5,-5,-6,-7,-8
552	0,0,-2,-3,-4,-5,-5,-6,-7,-8
662	0,0,-2,-3,-4,-5,-5,-6,-7,-8
772	0,0,-2,-3,-4,-5,-5,-6,-7,-8
882	0,0,-2,-3,-4,-5,-5,-6,-7,-8
992	0,0,-2,-3,-4,-5,-5,-6,-7,-8
1102	0,0,-2,-3,-4,-5,-5,-6,-7,-8

(c) $p = 13$, $m = 100$

k	Slopes
2	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
158	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
314	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
470	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
626	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
782	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
938	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
1094	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
1250	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
1406	0,-1,-2,-3,-4,-5,-6,-6,-6,-7
1562	0,-1,-2,-3,-4,-5,-6,-6,-6,-7

(d) $p = 17$, $m = 50$

k	Slopes
2	0,0,-1,-2,-3,-3,-4
274	0,0,-1,-2,-3,-3,-4
546	0,0,-1,-2,-3,-3,-4
818	0,0,-1,-2,-3,-3,-4
1090	0,0,-1,-2,-3,-3,-4
1362	0,0,-1,-2,-3,-3,-4
1634	0,0,-1,-2,-3,-3,-4
1906	0,0,-1,-2,-3,-3,-4
2178	0,0,-1,-2,-3,-3,-4
2450	0,0,-1,-2,-3,-3,-4
2722	0,0,-1,-2,-3,-3,-4

(e) $p = 19$, $m = 50$

k	Slopes
2	0,0,-1,-2,-2,-3,-4
344	0,0,-1,-2,-2,-3,-4
686	0,0,-1,-2,-2,-3,-4
1028	0,0,-1,-2,-2,-3,-4
1370	0,0,-1,-2,-2,-3,-4
1712	0,0,-1,-2,-2,-3,-4
2054	0,0,-1,-2,-2,-3,-4
2396	0,0,-1,-2,-2,-3,-4
2738	0,0,-1,-2,-2,-3,-4
3080	0,0,-1,-2,-2,-3,-4
3422	0,0,-1,-2,-2,-3,-4

(f) $p = 23$, $m = 50$

k	Slopes
2	0,0,0,-1,-2,-2,-3
508	0,0,0,-1,-2,-2,-3
1014	0,0,0,-1,-2,-2,-3
1520	0,0,0,-1,-2,-2,-3
2026	0,0,0,-1,-2,-2,-3
2532	0,0,0,-1,-2,-2,-3
3038	0,0,0,-1,-2,-2,-3
3544	0,0,0,-1,-2,-2,-3
4050	0,0,0,-1,-2,-2,-3
4556	0,0,0,-1,-2,-2,-3
5062	0,0,0,-1,-2,-2,-3

Figure 8: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 1$ *and weight* $k = 4 + p(p-1)j$ *for* j *running from* 0 *to* 10*.*

(a) $p = 7$, $m = 100$

k	Slopes
4	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
46	0,-1,-3,-4,-22,-22,-22,-22
88	0,-1,-3,-4,-6,-7,-9,-10,-43
130	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
172	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
214	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
256	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
298	0,-1,-3,-4,-6,-7,-9,-10,-12,-14
340	0,-1,-3,-4,-7,-8,-10,-11,-13,-15
382	0,-1,-3,-4,-6,-7,-9,-10,-13,-15
424	0,-1,-3,-4,-6,-7,-9,-10,-12,-14

(b) $p = 11$, $m = 100$

k	Slopes
4	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
114	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
224	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
334	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
444	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
554	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
664	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
774	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
884	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
994	0,-1,-1,-3,-4,-5,-6,-6,-7,-8
1104	0,-1,-1,-3,-4,-5,-6,-6,-7,-8

(c) $p = 13$, $m = 100$

k	Slopes
4	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
160	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
316	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
472	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
628	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
784	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
940	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
1096	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
1252	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
1408	0,-1,-1,-1,-3,-4,-5,-6,-7,-7
1564	0,-1,-1,-1,-3,-4,-5,-6,-7,-7

(d) $p = 17$, $m = 50$

k	Slopes
4	0,-1,-1,-1,-1,-3,-4
276	0,-1,-1,-1,-1,-3,-4
548	0,-1,-1,-1,-1,-3,-4
820	0,-1,-1,-1,-1,-3,-4
1092	0,-1,-1,-1,-1,-3,-4
1364	0,-1,-1,-1,-1,-3,-4
1636	0,-1,-1,-1,-1,-3,-4
1908	0,-1,-1,-1,-1,-3,-4
2180	0,-1,-1,-1,-1,-3,-4
2452	0,-1,-1,-1,-1,-3,-4
2724	0,-1,-1,-1,-1,-3,-4

(e) $p = 19$, $m = 50$

k	Slopes
4	0,-1,-1,-1,-1,-3,-3
346	0,-1,-1,-1,-1,-3,-3
688	0,-1,-1,-1,-1,-3,-3
1030	0,-1,-1,-1,-1,-3,-3
1372	0,-1,-1,-1,-1,-3,-3
1714	0,-1,-1,-1,-1,-3,-3
2056	0,-1,-1,-1,-1,-3,-3
2398	0,-1,-1,-1,-1,-3,-3
2740	0,-1,-1,-1,-1,-3,-3
3082	0,-1,-1,-1,-1,-3,-3
3424	0,-1,-1,-1,-1,-3,-3

(f) $p = 23$, $m = 50$

k	Slopes
4	0,-1,-1,-1,-1,-1,-3
510	0,-1,-1,-1,-1,-1,-3
1016	0,-1,-1,-1,-1,-1,-3
1522	0,-1,-1,-1,-1,-1,-3
2028	0,-1,-1,-1,-1,-1,-3
2534	0,-1,-1,-1,-1,-1,-3
3040	0,-1,-1,-1,-1,-1,-3
3546	0,-1,-1,-1,-1,-1,-3
4052	0,-1,-1,-1,-1,-1,-3
4558	0,-1,-1,-1,-1,-1,-3
5064	0,-1,-1,-1,-1,-1,-3

Figure 9: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 1$ *and weight* $k = 4 + p(p-1)j$ *and* $k = 2 + p(p-1)j$, $p = 5$, $m = 100$, *for* j *running from* 0 *to* 20. *The number of* k *values was increased compared to other sets of data, in order to more clearly examine the patterns that appear.*

(a) $k = 2 + p(p-1)j$

k	Slopes
2	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
22	0,-2,-10,-10,-10,-10,-10,-10,-10,-19
42	0,-2,-5,-6,-20,-20,-20,-21
62	0,-2,-5,-6,-9,-30,-31
82	0,-2,-5,-6,-9,-10,-11,-40
102	0,-2,-5,-6,-9,-10,-11,-14,-15
122	0,-2,-6,-7,-10,-10,-10,-13,-14,-19
142	0,-2,-5,-6,-10,-11,-12,-15,-16,-20
162	0,-2,-5,-6,-9,-11,-12,-15,-16,-20
182	0,-2,-5,-6,-9,-10,-11,-15,-16,-20
202	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
222	0,-2,-6,-7,-10,-10,-10,-13,-14,-19
242	0,-2,-5,-6,-10,-11,-12,-15,-16,-22
262	0,-2,-5,-6,-9,-11,-12,-15,-16,-20
282	0,-2,-5,-6,-9,-10,-11,-15,-16,-20
302	0,-2,-5,-6,-9,-10,-11,-14,-15,-20
322	0,-2,-6,-7,-10,-10,-10,-13,-14,-19
342	0,-2,-5,-6,-10,-11,-12,-15,-16,-20
362	0,-2,-5,-6,-9,-11,-12,-15,-16,-20
382	0,-2,-5,-6,-9,-10,-11,-15,-16,-20
402	0,-2,-5,-6,-9,-10,-11,-14,-15,-20

(b) $k = 4 + p(p-1)j$

k	Slopes
4	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
24	0,-1,-3,-11,-11,-11,-11,-11,-11,-11
44	0,-1,-3,-5,-21,-21,-21,-21
64	0,-1,-3,-5,-8,-10,-31,-32
84	0,-1,-3,-5,-8,-10,-11,-12,-41
104	0,-1,-3,-5,-8,-10,-11,-12,-14
124	0,-1,-3,-6,-9,-11,-11,-11,-13,-16
144	0,-1,-3,-5,-9,-11,-12,-13,-15,-18
164	0,-1,-3,-5,-8,-10,-12,-13,-15,-18
184	0,-1,-3,-5,-8,-10,-11,-12,-15,-18
204	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
224	0,-1,-3,-6,-9,-11,-11,-11,-13,-16
244	0,-1,-3,-5,-9,-11,-12,-13,-15,-18
264	0,-1,-3,-5,-8,-10,-12,-13,-15,-18
284	0,-1,-3,-5,-8,-10,-11,-12,-15,-18
304	0,-1,-3,-5,-8,-10,-11,-12,-14,-18
324	0,-1,-3,-6,-9,-11,-11,-11,-13,-16
344	0,-1,-3,-5,-9,-11,-12,-13,-15,-18
364	0,-1,-3,-5,-8,-10,-12,-13,-15,-18
384	0,-1,-3,-5,-8,-10,-11,-12,-15,-18
404	0,-1,-3,-5,-8,-10,-11,-12,-14,-18

Figure 10: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 2$ *and weight* $k = 2 + p(p-1)j$ *for* j *running from* 0 *to* 10.

(a) p=5, $m = 100$

k	Slopes
2	0,0,-1,-2,-2,-2,-4,-5,-5,-6
22	0,0,-1,-2,-2,-2,-10, $\frac{-81}{8}$, $\frac{-81}{8}$, $\frac{-81}{8}$
42	0,0,-1,-2,-2,-2,-4,-5,-5,-6
62	0,0,-1,-2,-2,-2,-4,-5,-5,-6
82	0,0,-1,-2,-2,-2,-4,-5,-5,-6
102	0,0,-1,-2,-2,-2,-4,-5,-5,-6
122	0,0,-1,-2,-2,-2,-5,-6,-6,-7
142	0,0,-1,-2,-2,-2,-4,-5,-5,-6
162	0,0,-1,-2,-2,-2,-4,-5,-5,-6
182	0,0,-1,-2,-2,-2,-4,-5,-5,-6
202	0,0,-1,-2,-2,-2,-4,-5,-5,-6

(b) $p = 7$, $m = 50$

k	Slopes
2	0,0,0,-1,-2,-2,-3
44	0,0,0,-1,-2,-2,-3
86	0,0,0,-1,-2,-2,-3
128	0,0,0,-1,-2,-2,-3
170	0,0,0,-1,-2,-2,-3
212	0,0,0,-1,-2,-2,-3
254	0,0,0,-1,-2,-2,-3
296	0,0,0,-1,-2,-2,-3
338	0,0,0,-1,-2,-2,-3
380	0,0,0,-1,-2,-2,-3
422	0,0,0,-1,-2,-2,-3

(c) $p = 11$, $m = 36$

k	Slopes
2	0,0,0,0,-1,-1
112	0,0,0,0,-1,-1
222	0,0,0,0,-1,-1
332	0,0,0,0,-1,-1
442	0,0,0,0,-1,-1
552	0,0,0,0,-1,-1
662	0,0,0,0,-1,-1
772	0,0,0,0,-1,-1
882	0,0,0,0,-1,-1
992	0,0,0,0,-1,-1
1102	0,0,0,0,-1,-1

(d) $p = 13$, $m = 36$

k	Slopes
2	0,0,0,0,-1,-1
158	0,0,0,0,-1,-1
314	0,0,0,0,-1,-1
470	0,0,0,0,-1,-1
626	0,0,0,0,-1,-1
782	0,0,0,0,-1,-1
938	0,0,0,0,-1,-1
1094	0,0,0,0,-1,-1
1250	0,0,0,0,-1,-1
1406	0,0,0,0,-1,-1
1562	0,0,0,0,-1,-1

(e) $p = 17$, $m = 36$

k	Slopes
2	0,0,0,0,0,-1
274	0,0,0,0,0,-1
546	0,0,0,0,0,-1
818	0,0,0,0,0,-1
1090	0,0,0,0,0,-1
1362	0,0,0,0,0,-1
1634	0,0,0,0,0,-1
1906	0,0,0,0,0,-1
2178	0,0,0,0,0,-1
2450	0,0,0,0,0,-1
2722	0,0,0,0,0,-1

(f) $p = 19$, $m = 36$

k	Slopes
2	0,0,0,0,0,0
344	0,0,0,0,0,0
686	0,0,0,0,0,0
1028	0,0,0,0,0,0
1370	0,0,0,0,0,0
1712	0,0,0,0,0,0
2054	0,0,0,0,0,0
2396	0,0,0,0,0,0
2738	0,0,0,0,0,0
3080	0,0,0,0,0,0
3422	0,0,0,0,0,0

Figure 11: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 2$ *and weight* $k = 4 + p(p-1)j$ *for* j *running from* 0 *to* 10.

(a) p=5, $m = 100$

k	Slopes
4	0,0,-1,-1,-1,-3,-3,-4,-5,-5
24	0,0,-1,-1,-1,-3,-3,-11,-11,-11
44	0,0,-1,-1,-1,-3,-3,-4,-5,-5
64	0,0,-1,-1,-1,-3,-3,-4,-5,-5
84	0,0,-1,-1,-1,-3,-3,-4,-5,-5
104	0,0,-1,-1,-1,-3,-3,-4,-5,-5
124	0,0,-1,-1,-1,-3,-3,-5,-6,-6
144	0,0,-1,-1,-1,-3,-3,-4,-5,-5
164	0,0,-1,-1,-1,-3,-3,-4,-5,-5
184	0,0,-1,-1,-1,-3,-3,-4,-5,-5
204	0,0,-1,-1,-1,-3,-3,-4,-5,-5

(b) $p = 7$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
46	0,0,-1,-1,-1,-1
88	0,0,-1,-1,-1,-1
130	0,0,-1,-1,-1,-1
172	0,0,-1,-1,-1,-1
214	0,0,-1,-1,-1,-1
256	0,0,-1,-1,-1,-1
298	0,0,-1,-1,-1,-1
340	0,0,-1,-1,-1,-1
382	0,0,-1,-1,-1,-1
424	0,0,-1,-1,-1,-1

(c) $p = 11$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
114	0,0,-1,-1,-1,-1
224	0,0,-1,-1,-1,-1
334	0,0,-1,-1,-1,-1
444	0,0,-1,-1,-1,-1
554	0,0,-1,-1,-1,-1
664	0,0,-1,-1,-1,-1
774	0,0,-1,-1,-1,-1
884	0,0,-1,-1,-1,-1
994	0,0,-1,-1,-1,-1
1104	0,0,-1,-1,-1,-1

(d) $p = 13$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
160	0,0,-1,-1,-1,-1
316	0,0,-1,-1,-1,-1
472	0,0,-1,-1,-1,-1
628	0,0,-1,-1,-1,-1
784	0,0,-1,-1,-1,-1
940	0,0,-1,-1,-1,-1
1096	0,0,-1,-1,-1,-1
1252	0,0,-1,-1,-1,-1
1408	0,0,-1,-1,-1,-1
1564	0,0,-1,-1,-1,-1

(e) $p = 17$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
276	0,0,-1,-1,-1,-1
548	0,0,-1,-1,-1,-1
820	0,0,-1,-1,-1,-1
1092	0,0,-1,-1,-1,-1
1364	0,0,-1,-1,-1,-1
1636	0,0,-1,-1,-1,-1
1908	0,0,-1,-1,-1,-1
2180	0,0,-1,-1,-1,-1
2452	0,0,-1,-1,-1,-1
2724	0,0,-1,-1,-1,-1

(f) $p = 19$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
346	0,0,-1,-1,-1,-1
688	0,0,-1,-1,-1,-1
1030	0,0,-1,-1,-1,-1
1372	0,0,-1,-1,-1,-1
1714	0,0,-1,-1,-1,-1
2056	0,0,-1,-1,-1,-1
2398	0,0,-1,-1,-1,-1
2740	0,0,-1,-1,-1,-1
3082	0,0,-1,-1,-1,-1
3424	0,0,-1,-1,-1,-1

Figure 12: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 3$ *and weight* $k = 2 + p(p-1)j$ *for* j *running from* 0 *to* 10.

(a) p=5, $m = 100$

k	Slopes
2	0,0,0,-1,-2,-2,-2,-2,-4,-5
22	0,0,0,-1,-2,-2,-2,-2,-10,-10
42	0,0,0,-1,-2,-2,-2,-2,-4,-5
62	0,0,0,-1,-2,-2,-2,-2,-4,-5
82	0,0,0,-1,-2,-2,-2,-2,-4,-5
102	0,0,0,-1,-2,-2,-2,-2,-4,-5
122	0,0,0,-1,-2,-2,-2,-2,-5,-6
142	0,0,0,-1,-2,-2,-2,-2,-4,-5
162	0,0,0,-1,-2,-2,-2,-2,-4,-5
182	0,0,0,-1,-2,-2,-2,-2,-4,-5
202	0,0,0,-1,-2,-2,-2,-2,-4,-5

(b) $p = 7$, $m = 50$

k	Slopes
2	0,0,0,-1,-1,-2,-2
44	0,0,0,-1,-1,-2,-2
86	0,0,0,-1,-1,-2,-2
128	0,0,0,-1,-1,-2,-2
170	0,0,0,-1,-1,-2,-2
212	0,0,0,-1,-1,-2,-2
254	0,0,0,-1,-1,-2,-2
296	0,0,0,-1,-1,-2,-2
338	0,0,0,-1,-1,-2,-2
380	0,0,0,-1,-1,-2,-2
422	0,0,0,-1,-1,-2,-2

(c) $p = 11$, $m = 36$

k	Slopes
2	0,0,0,0,0,-1
112	0,0,0,0,0,-1
222	0,0,0,0,0,-1
332	0,0,0,0,0,-1
442	0,0,0,0,0,-1
552	0,0,0,0,0,-1
662	0,0,0,0,0,-1
772	0,0,0,0,0,-1
882	0,0,0,0,0,-1
992	0,0,0,0,0,-1
1102	0,0,0,0,0,-1

(d) $p = 13$, $m = 36$

k	Slopes
2	0,0,0,0,0,-1
158	0,0,0,0,0,-1
314	0,0,0,0,0,-1
470	0,0,0,0,0,-1
626	0,0,0,0,0,-1
782	0,0,0,0,0,-1
938	0,0,0,0,0,-1
1094	0,0,0,0,0,-1
1250	0,0,0,0,0,-1
1406	0,0,0,0,0,-1
1562	0,0,0,0,0,-1

(e) $p = 17$, $m = 36$

k	Slopes
2	0,0,0,0,0,0
274	0,0,0,0,0,0
546	0,0,0,0,0,0
818	0,0,0,0,0,0
1090	0,0,0,0,0,0
1362	0,0,0,0,0,0
1634	0,0,0,0,0,0
1906	0,0,0,0,0,0
2178	0,0,0,0,0,0
2450	0,0,0,0,0,0
2722	0,0,0,0,0,0

(f) $p = 19$, $m = 36$

k	Slopes
2	0,0,0,0,0,0
344	0,0,0,0,0,0
686	0,0,0,0,0,0
1028	0,0,0,0,0,0
1370	0,0,0,0,0,0
1712	0,0,0,0,0,0
2054	0,0,0,0,0,0
2396	0,0,0,0,0,0
2738	0,0,0,0,0,0
3080	0,0,0,0,0,0
3422	0,0,0,0,0,0

Figure 13: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 3$ *and weight* $k = 4 + p(p-1)j$ *for* j *running from* 0 *to* 10.

(a) p=5, $m = 100$

k	Slopes
4	0,0,-1,-1,-1,-1,-3,-3,-3,-4
24	0,0,-1,-1,-1,-1,-3,-3,-3,-11
44	0,0,-1,-1,-1,-1,-3,-3,-3,-4
64	0,0,-1,-1,-1,-1,-3,-3,-3,-4
84	0,0,-1,-1,-1,-1,-3,-3,-3,-4
104	0,0,-1,-1,-1,-1,-3,-3,-3,-4
124	0,0,-1,-1,-1,-1,-3,-3,-3,-5
144	0,0,-1,-1,-1,-1,-3,-3,-3,-4
164	0,0,-1,-1,-1,-1,-3,-3,-3,-4
184	0,0,-1,-1,-1,-1,-3,-3,-3,-4
204	0,0,-1,-1,-1,-1,-3,-3,-3,-4

(b) $p = 7$, $m = 50$

k	Slope
4	0,0,-1,-1,-1,-1,-1
46	0,0,-1,-1,-1,-1,-1
88	0,0,-1,-1,-1,-1,-1
130	0,0,-1,-1,-1,-1,-1
172	0,0,-1,-1,-1,-1,-1
214	0,0,-1,-1,-1,-1,-1
256	0,0,-1,-1,-1,-1,-1
298	0,0,-1,-1,-1,-1,-1
340	0,0,-1,-1,-1,-1,-1
382	0,0,-1,-1,-1,-1,-1
424	0,0,-1,-1,-1,-1,-1

(c) $p = 11$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
114	0,0,-1,-1,-1,-1
224	0,0,-1,-1,-1,-1
334	0,0,-1,-1,-1,-1
444	0,0,-1,-1,-1,-1
554	0,0,-1,-1,-1,-1
664	0,0,-1,-1,-1,-1
774	0,0,-1,-1,-1,-1
884	0,0,-1,-1,-1,-1
994	0,0,-1,-1,-1,-1
1104	0,0,-1,-1,-1,-1

(d) $p = 13$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
160	0,0,-1,-1,-1,-1
316	0,0,-1,-1,-1,-1
472	0,0,-1,-1,-1,-1
628	0,0,-1,-1,-1,-1
784	0,0,-1,-1,-1,-1
940	0,0,-1,-1,-1,-1
1096	0,0,-1,-1,-1,-1
1252	0,0,-1,-1,-1,-1
1408	0,0,-1,-1,-1,-1
1564	0,0,-1,-1,-1,-1

(e) $p = 17$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
276	0,0,-1,-1,-1,-1
548	0,0,-1,-1,-1,-1
820	0,0,-1,-1,-1,-1
1092	0,0,-1,-1,-1,-1
1364	0,0,-1,-1,-1,-1
1636	0,0,-1,-1,-1,-1
1908	0,0,-1,-1,-1,-1
2180	0,0,-1,-1,-1,-1
2452	0,0,-1,-1,-1,-1
2724	0,0,-1,-1,-1,-1

(f) $p = 19$, $m = 36$

k	Slopes
4	0,0,-1,-1,-1,-1
346	0,0,-1,-1,-1,-1
688	0,0,-1,-1,-1,-1
1030	0,0,-1,-1,-1,-1
1372	0,0,-1,-1,-1,-1
1714	0,0,-1,-1,-1,-1
2056	0,0,-1,-1,-1,-1
2398	0,0,-1,-1,-1,-1
2740	0,0,-1,-1,-1,-1
3082	0,0,-1,-1,-1,-1
3424	0,0,-1,-1,-1,-1

We can first observe that for each subsequent k, the slopes are not the same. This is expected, as the Gouvea-Mazur conjecture is known to be false. However, we note that, as p increases, the slopes for various values of k become more and more similar, until they become identical, up to the precision used. Further, this occurs sooner when using the equations $k = 2 + (p^2)(p-1)j$ and $k = 4 + (p^2)(p-1)j$ for k than when using the equations $k = 2 + p(p-1)j$ and $k = 4 + p(p-1)j$. This could indicate that this property of approaching the same slopes depends on the weight of the modular forms, and that the properties that cause the Gouvea-Mazur conjecture to fail become less and less dominant at high weights. Another possibility is that more eigenvalues must be calculated at high weights in order for the properties that cause the Gouvea-Mazur conjecture to fail to dominate the behavior of the slopes.

Also, as would be expected, there is no significant difference between using $k = 2 + (p^2)(p-1)j$ and $k = 4 + (p^2)(p-1)j$, or between using $k = 2 + p(p-1)j$ and $k = 4 + p(p-1)j$. The specific slopes are different, but the behavior of the slopes is essentially unchanged.

Table 1: *Slopes of the inverse eigenvalues of* T_p *for level* $N = 1$ *,* $p = 7$ *and* $m = 100$ *for various weights* k*.*

k	Slopes
44	0, -2, -3, -4, -21, -21, -21, -21
46	0, -1, -3, -4, -22, -22, -22, -22
48	0, -2, -2, -2, -5, -23, -23, -23
340	0, -1, -3, -4, -7, -8, -10, -11, -13, -15, -16
2104	0, -1, -3, -4, -8, -9, -11, -12, -14, -16, -17

We can also observe that, even at low weights, certain values of k do appear to produce the same slopes, creating "troughs" of sorts where the slopes do not match, surrounded by "plateaus" where they do match. An example of this structure can be found in figure 7 (a). Weights $k = 2,\ 128,\ 170,\ 212,\ 254,\ 296$ and 422 all have the same slopes, but $k = 44,\ k = 88$ and $k = 338,\ k = 380$, the "troughs", have slopes that do not match these usual slopes.

The reason for the existence of this pattern is unknown, but congruences do not appear to explain it on their own, as higher congruences are not always sufficient for the slopes to match. Indeed, for the case of $k = 46$, as seen in figure 8 (a), one would expect the output to match the case of $k = 340$, as these two values are congruent modulo $7^2(7-1) = 294$, and thus are close 7-adically in $\mathbb{Z}_7^*$. However, as can be seen in table 1, this is not the case, and even increasing the congruence to $7^3(7-1)$ does not cause the slopes to match.

Further, there appears to be an additional unusual phenomenon taking place around $k = 46$, as seen again in table 1, as the jump from -4 to -22 is quite large. This was unexpected, as only figure 7 (a) and figure 9 (a) and (b) show a similar sudden change in slope, and it is also very different from the slopes for other weights in the same tables. Further calculations showed that a similar phenomenon occurs at $k = 48$ and $k = 44$, as shown in table 1, thus this does not appear to be a one-off event. The reason for this jump is unknown as of now, but we have thoroughly troubleshot the program used to calculate these results, and the program outputs what is expected for certain known sets of slopes, so a bug in the program is likely not at fault.

References

[1] Jose Ignacio Burgos Gil and Ariel Pacetti. Hecke and Sturm bounds for Hilbert modular forms over real quadratic fields. *Math. Comp.*, 86(306):1949–1978, 2017.

[2] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[3] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[4] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[5] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., Vol. 350, pages 69–190. Springer, Berlin, 1973.

[6] Alan G. B. Lauder. Computations with classical and p-adic modular forms. *LMS J. Comput. Math.*, 14:214–231, 2011.

[7] Yu. I. Manin. *Selected papers of Yu. I. Manin*, volume 3 of *World Scientific Series in 20th Century Mathematics*. World Scientific Publishing Co., Inc., River Edge, NJ, 1996.

[8] Jean-Pierre Serre. Endomorphismes complètement continus des espaces de Banach p-adiques. *Inst. Hautes Études Sci. Publ. Math.*, (12):69–85, 1962.

[9] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[10] The Stacks project authors. The stacks project. https://stacks.math.columbia.edu/tag/073K, 2022.

[11] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[12] Daqing Wan. Dimension variation of classical and p-adic modular forms. *Invent. Math.*, 133(2):449–463, 1998.

Appendix A

Sagemath Code:

Code for level $\Gamma_1(1)$ algorithm:

Given p>= 5 prime, integer k and positive integer m:

Step 1

Compute the k0 and j:

[1]:
```
((k0,j),)=Polyhedron(ieqs=[[0,1,0], [p-2,-1,0]], eqns=[[-k, 1,p-1]]).
↪integral_points()
```

[2]:
```
k0=k % (p-1)
```

Compute n:

[3]:
```
n=floor(((p+1)/(p-1))*(m+1))
```

For i=0,…,n, compute d_i, the dimension of the space of classical modular forms of level 1 and weight k0+i(p-1):

[4]:
```
d=list('d_%d' % s for s in range(0,n))
for i in range(0,n):
    d[i]=dimension_modular_forms(Gamma1(1),k0+i*(p-1))
```

Compute the m_i:

[5]:
```
M=list(var('m_%d' % s) for s in range(0,n))
M[0]=d[0]
for i in range(1,n):
    M[i]=d[i]-d[i-1]
```

Compute l:

[6]:
```
l=sum(M[i] for i in range(0,n))
```

Compute the working precision mp:

[7]:
```
mp=m+floor(n/(p+1))
```

Step 2

For each 0≤i≤n, denote by $D_{k0+i(p-1)}$ a row reduced basis of q-expansions in $\frac{\mathbb{Z}[[q]]}{(p^{mp},q^{lp})}$ of the space of classical modular forms of weight k0+i(p-1) and level 1. First, define a function that returns the row-reduced basis of q-expansions:

[8]:
```
R.<q> = PowerSeriesRing(ZZ,default_prec=2*(p*l))
def Mrr(k0,i):
    return ModularForms(Gamma1(1),k0+i*(p-1)).q_echelon_basis(prec=(l*p))
```

Now, define a reduction modulo (p^{mp}, q^{lp}):

[9]:
```
def ordred2(a,p):
    a += O(q^((l*p)+1))
    a += q^(l*p)
    b=a.polynomial()
    ordred2_b=b.coefficients(sparse=False)
    ordred2_coeff=list('ordred2_coeff_%d' % s for s in range(0,(l*p)))
    for i in range(0,(l*p)):
        ordred2_coeff[i]=Mod(ordred2_b[i],p^mp)
    return R(ordred2_coeff)
```

Now calculate all the bases, reduce modulo (p^{mp}, q^{lp}), and store them in a list:

[10]:
```
ListBasis=list('M_%d' % s for s in range(0,n))
for i in range(0,n):
    if k0+i*(p-1) == 0:
        Mrri=list('Mrri_%d' % s for s in range(0,1))
        Mrri[0]=1
        ListBasis[i]=Mrri
    else:
        Mrri=list('Mrri_%d' % s for s in range(0,len(Mrr(k0,i))))
        for y in range(0,len(Mrr(k0,i))):
            Mrri[y]=ordred2(Mrr(k0,i)[y],p)
        ListBasis[i]=Mrri
```

Define Wi:

[11]:
```
def W(i):
    if M[i]==0:
        return []
    else:
        return ListBasis[i][-M[i]:]
```

Step 3

Compute the q-expansion in $\frac{\mathbb{Z}[[q]]}{(p^{mp},q^{lp})}$ of the Eisenstein series $E_{p-1}(q)$:

[12]:
```
eisen=ordred2(eisenstein_series_qexp(p-1,p*l,normalization='constant'),p)
```

Now define the elements $e_{i,s}$ by defining them in a double list:

[13]:
```
Matrixe=[[1 for s in range(0,M[i])] for i in range(0,n)]
```

[14]:
```
for i in range(0,n):
    if M[i]==0:
        adsadsa=3
    else:
        for s in range (0,M[i]):
            Matrixe[i][s]=ordred2((ordred2(p^floor(i/
 ↪(p+1))*(eisen)^(-i),p))*(ordred2(W(i)[s],p)),p)
```

Step 4

Define eisenq = $E_{p-1}(q^p)$:

[15]:
```
def ordredq2(a,p):
    a += O(q^((l*p)+1))
    a += q^(l*p)
    b=a.polynomial()
    ordredq2_b=b.coefficients(sparse=False)
    ordredq2_coeff=list('ordredq2_coeff_%s' % s for s in range(0,(l*p)))
    for i in range(0,(l*p)):
        ordredq2_coeff[i]=Mod(ordredq2_b[i],p^mp)
    return R(ordredq2_coeff)
```

[16]:
```
eisenq=ordredq2(eisenstein_series_qexp(p-1,l*p,normalization='constant').subs({q:
 ↪q^p}),p)
```

Now, use this to define $G(q)$:

[17]:
```
def G(q):
    return eisen/eisenq
```

Now, calculate $G(q)^j$ using a fast exponentiation routine:

[18]:
```
def FastPower(a,n):
    if (n==0):
        return 1
    X=power(a,n/2)
    X=X*X
    if(n%2==1):
        X=X*a
    return X
```

Now, define the $u_{i,s}$:

[19]:
```
Matrixu=[[1 for s in range(0,M[i])] for i in range(0,n)]
```

[20]:
```
for i in range(0,n):
    if M[i]==0:
        adsadsa=3
    else:
        for s in range (0,M[i]):
            Matrixu[i][s]=ordred2((G(q)^j)*Matrixe[i][s],p)
```

Step 5

Calculate the $t_{i,s}$:

[21]:
```
Matrixt=[[1 for s in range(0,M[i])] for i in range(0,n)]
for i in range(0,n):
    if M[i]==0:
        adsadsssa=3
    else:
        abcd=Matrixu[i][s].polynomial().coefficients(sparse=False)
        for s in range (0,M[i]):
            List_t=list('M_%d' % s for s in range(0,l))
            for y in range(0,l):
                List_t[y]=abcd[p*y]
            Matrixt[i][s]=R(List_t)
```

Step 6

Define the matrix T:

First, define the base ring:

[22]:
```
S=Integers(p^mp)
```

Now initialize the matrix:

[23]:
```
T=matrix(ring=S,nrows=l,ncols=l)
```

Now define a new function to reduce modulo q^l. This will return a list of coefficients, rather than a polynomial:

[24]:
```
def ordred3(a,p):
    a += O(q^(l+1))
    a += q^l
    b=a.polynomial()
    ordred3_b=b.coefficients(sparse=False)
    ordred3_coeff=list('ordred3_coeff_%d' % s for s in range(0,(l)))
    for i in range(0,(l)):
        ordred3_coeff[i]=Mod(ordred3_b[i],p^mp)
    return ordred3_coeff
```

Now calculate the entries of T. Each row of T corresponds to a non-zero element of Matrixt, and the l entries in that row correspond to the coefficients:

[25]:
```
j=0
i=0
s=0
while j<l:
    if M[i]==0:
        i += 1
    else:
        while s<M[i]:
            for k in range(0,l):
                T[j,k]=ordred3(Matrixt[i][s],p)[k]
            s+=1
            j+=1

        else:
            s=0
            i+=1
```

Define the matrix E:

[26]:
```
E=matrix(ring=S,nrows=l,ncols=l)
```

[27]:
```
j=0
i=0
s=0
while j<l:
    if M[i]==0:
        i += 1
    else:
        while s<M[i]:
            for k in range(0,l):
                E[j,k]=ordred3(Matrixe[i][s],p)[k]
            s+=1
            j+=1

        else:
            s=0
            i+=1
```

Solve T=AE for A. If this has no solution, multiply by p and try again:

[28]:
```
try:
    E.solve_left(T)
    A=E.solve_left(T)
except:
    A=E.solve_left(p*T)
```

[29]:
```
Poly.<x>=PolynomialRing(ZZ)
```

Define one last function for reduction:

[30]:
```
def ordred4(b,p):
    ordred4_b=b.coefficients(sparse=False)
    ordred4_coeff=list('ordred4_coeff_%d' % s for s in range(0,len(ordred4_b)))
    for i in range(0,len(ordred4_b)):
        ordred4_coeff[i]=Mod(ordred4_b[i],p^m)
    return Poly(ordred4_coeff)
```

Calculate the characteristic series of A, then calculate the Newton slopes:

[31]:
```
characteristic=ordred4((identity_matrix(S,1)-A*x).determinant(),p)
```

[32]:
```
characteristic.newton_slopes(p)
```

Code for level $\Gamma_1(N)$ algorithm:

Given N>=2, p>= 5 prime not dividing N, integer k and positive integer m:

Step 1

Compute the k0 and j:

[1]:
```
((k0,j),)=Polyhedron(ieqs=[[0,1,0], [p-2,-1,0]], eqns=[[-k, 1,p-1]]).
↪integral_points()
```

[2]:
```
k0=k % (p-1)
```

Compute n:

[3]:
```
n=floor(((p+1)/(p-1))*(m+1))
```

For i=0,...,n, compute d_i, the dimension of the space of classical modular forms of level 1 and weight k0+i(p-1)

[4]:
```
d=list('d_%d' % s for s in range(0,n))
for i in range(0,n):
    d[i]=dimension_modular_forms(Gamma1(N),k0+i*(p-1))
```

Compute the m_i:

[5]:
```
M=list(var('m_%d' % s) for s in range(0,n))
M[0]=d[0]
for i in range(1,n):
    M[i]=d[i]-d[i-1]
```

Compute lo :

[6]:
```
lo=sum(M[i] for i in range(0,n))
```

Compute the working precision mp:

[7]:
```
mp=m+floor(n/(p+1))
```

Compute the sturm bound l:

[8]:
```
l=ModularForms(Gamma1(N),k0+n*(p-1)).sturm_bound()
```

Step 2

For each 0≤i≤n, denote by $D_{k0+i(p-1)}$ a row reduced basis of q-expansions in $\frac{\mathbb{Z}[[q]]}{(p^{mp},q^{lp})}$ of the space of classical modular forms of weight k0+i(p-1) and level N.

[9]:
```
R.<q> = PowerSeriesRing(ZZ,default_prec=(p*l))
Poly.<x>=PolynomialRing(ZZ)
```

First, define a reduction modulo (p^{mp}, q^{lp}):

[10]:
```
def ordred2(a,p):
    b=Poly(a)
    b+= x^(2*(l*p))
    ordred2_b=b.coefficients(sparse=False)
    ordred2_coeff=list('ordred2_coeff_%d' % d for d in range(0,(l*p)))
    for i in range(0,(l*p)):
        ordred2_coeff[i]=Mod(ordred2_b[i],p^mp)
    return R(ordred2_coeff)
```

Now, define a function that returns the row-reduced basis of q-expansions:

[11]:
```
def Mrr(k0,i):
    return ModularForms(Gamma1(N),k0+i*(p-1)).q_echelon_basis(prec=(l*p))
```

Now calculate all the bases, reduce modulo (p^{mp}, q^{lp}), and store them in a list:

[12]:
```
ListBasis=list('M_%d' % s for s in range(0,n))
for i in range(0,n):
    if k0+i*(p-1) == 0:
        Mrri=list('Mrri_%d' % s for s in range(0,1))
        Mrri[0]=1
        ListBasis[i]=Mrri
    else:
        Mrri=list('Mrri_%d' % s for s in range(0,len(Mrr(k0,i))))
        for y in range(0,len(Mrr(k0,i))):
            Mrri[y]=ordred2(Mrr(k0,i)[y],p)
        ListBasis[i]=Mrri
```

[13]:
```
def W(i):
    F=list('f_%d' % s for s in range(0,M[i]))
    t=0
    if i==0:
        F=ListBasis[0]
    else:
        while t<M[i]:
            for w in range(0,d[i]):
                if all(R(ListBasis[i][w]).polynomial().ord() !=␣
↪R(ListBasis[i-1][y]).polynomial().ord() for y in range(0,d[i-1])):
                    F[t]=ListBasis[i][w]
                    t+=1
                else:
                    none=1
    return F
```

Step 3

Compute the q-expansion in $\frac{\mathbb{Z}[[q]]}{(p^{mp},q^{lp})}$ of the Eisenstein series $E_{p-1}(q)$:

[14]:
```
eisen=ordred2(eisenstein_series_qexp(p-1,p*l,normalization='constant'),p)
```

Now define the elements $e_{i,s}$ by defining them in a double list:

[15]:
```
Matrixe=[[1 for s in range(0,M[i])] for i in range(0,n)]
```

[16]:
```
for i in range(0,n):
        if M[i]==0:
            none=1
        else:
            for s in range (0,M[i]):
                Matrixe[i][s]=ordred2((ordred2(p^floor(i/
 ↪(p+1))*(eisen)^(-i),p))*(ordred2(W(i)[s],p)),p)
```

Step 4

Define eisenq = $E_{p-1}(q^p)$:

[17]:
```
eisenq=ordred2(eisenstein_series_qexp(p-1,l*p,normalization='constant').subs({q:
 ↪q^p}),p)
```

Now, use this to define $G(q)$:

[18]:
```
def G(q):
    return eisen/eisenq
```

Now, define the $u_{i,s}$:

[19]:
```
Matrixu=[[1 for s in range(0,M[i])] for i in range(0,n)]
```

[20]:
```
for i in range(0,n):
        if M[i]==0:
            none=1
        else:
            for s in range (0,M[i]):
                Matrixu[i][s]=ordred2((G(q)^j)*Matrixe[i][s],p)
```

Step 5

Calculate the $t_{i,s}$:

[21]:
```
Matrixt=[[1 for s in range(0,M[i])] for i in range(0,n)]
for i in range(0,n):
        if M[i]==0:
            none=1
        else:
            for s in range (0,M[i]):
                abcd=(R(Matrixu[i][s])+q^(l*p+1)).polynomial().
 ↪coefficients(sparse=False)
                List_t=list('M_%d' % s for s in range(0,l))
                for y in range(0,l):
                    List_t[y]=abcd[p*y]
                Matrixt[i][s]=R(List_t)
```

Step 6

Define the matrix T:

First, define the base ring:

[22]:
```
S=Integers(p^mp)
```

Now initialize the matrix:

[23]:
```
T=matrix(ring=S,nrows=lo,ncols=l)
```

Now define a new function to reduce modulo q^l. This will return a list of coefficients, rather than a polynomial:

[24]:
```
def ordred3(a,p):
    b=Poly(a)
    b+= x^(2*(l*p))
    ordred3_b=b.coefficients(sparse=False)
    ordred3_coeff=list('ordred3_coeff_%d' % s for s in range(0,(l)))
    for i in range(0,(l)):
        ordred3_coeff[i]=Mod(ordred3_b[i],p^mp)
    return ordred3_coeff
```

Now calculate the entries of T. Each row of T corresponds to a non-zero element of Matrixt, and the l entries in that row correspond to the coefficients:

[25]:
```
jv=0
i=0
s=0
while jv<lo:
        if M[i]==0:
            i += 1
        else:
            while s<M[i]:
                for k in range(0,l):
                    T[jv,k]=ordred3(Matrixt[i][s],p)[k]
                s+=1
                jv+=1
            else:
                s=0
                i+=1
```

Define the matrix E:

[26]:
```
E=matrix(ring=S,nrows=lo,ncols=l)
```

[27]:
```
j=0
i=0
s=0
while j<lo:
    if M[i]==0:
        i += 1
    else:
        while s<M[i]:
            for k in range(0,l):
                E[j,k]=ordred3(Matrixe[i][s],p)[k]
            s+=1
            j+=1

        else:
            s=0
            i+=1
```

Solve T=AE for A. If this has no solution, multiply by p and try again:

[28]:
```
try:
    E.solve_left(T)
    A=E.solve_left(T)
except:
    E.solve_left(p*T)
    A=E.solve_left(p*T)
```

Define one last function for reduction:

[29]:
```
def ordred4(b,p):
    ordred4_b=Poly(b).coefficients(sparse=False)
    ordred4_coeff=list('ordred4_coeff_%d' % s for s in range(0,len(ordred4_b)))
    for i in range(0,len(ordred4_b)):
        ordred4_coeff[i]=Mod(ordred4_b[i],p^m)
    return Poly(ordred4_coeff)
```

Calculate the characteristic series of A, then calculate the Newton slopes:

[30]:
```
characteristic=ordred4((identity_matrix(S,lo)-A*x).determinant(),p)
```

[31]:
```
characteristic.newton_slopes(p)
```