University of Copenhagen
Department of Mathematical Sciences

Ph.D. Dissertation

Algebra and Arithmetic of Modular Forms

by

Nadim Rustom

Supervisor: Ian Kiming

This thesis has been submitted to the PhD School of The Faculty of Science,
University of Copenhagen
Denmark, 2014

Author
Nadim Rustom
Department of Mathematical Sciences
University of Copenhagen
Universitetsparken 5
2100 Copenhagen

rustom@math.ku.dk
http://www.math.ku.dk/~rustom/

Supervisor
Ian Kiming
University of Copenhagen

Assessment committee
Carel Faber
KTH Stockholm and Utrecht University

Lars Halvard Halle (chairman)
University of Copenhagen

John Voight
Dartmouth College

This thesis has been submitted to the PhD School of The Faculty of Science, University of Copenhagen, Denmark, on September 30, 2014.

ISBN: 978-87-7078-966-0

To my parents

Contents

Acknowledgements

As a PhD student at the University of Copenhagen, I experienced living in the wonderful land of Denmark, and I had the oppurtunity to travel to conferences in many countries across Europe. I met amazing and inspiring people, from all over the globe, many of whom are likely to be life-long friends.

First and foremost, I would like to thank my parents, Fida and Radwan, and my brother Wassim, for their support during this journey. This thesis is dedicated to them. When I was still a child, my father inspired in me a love of science and mathematics, and a certain pleasure of finding things out, all of which have persisted with me to this day and have motivated me to pursue a career in mathematics. For that, I am forever grateful.

I thank my supervisor, Ian Kiming, for his continuous support, for providing me with guidance and with many questions to think about, and for passing a great deal of his knowledge and experience as a researcher and an academic to me.

I thank my fellow PhD students at the University of Copenhagen. In particular, I would like to thank my office mates for the friendships we developped, and the discussions we had, mathematical and otherwise. Special thanks goes to Giacomo Cherubini for proof-reading a first draft of this thesis and spotting an embarrassing amount of typographical errors.

Great thanks and appreciation are due to Miriam Lærke, who has been by my side for most of these three years. She continuously provided me with care and support, gave me new perspectives on life, and comforted me when I stumbled.

Abstract - Resumé

Abstract

In [Rus14b] and [Rus14a], we study graded rings of modular forms over congruence subgroups, with coefficients in subrings A of $\mathbb{C}$, and determine bounds of the weights of modular forms constituting a minimal set of generators, as well as on the degree of the generators of the ideal of relations between them. We give an algorithm that computes the structures of these rings, and formulate conjectures on the minimal generating weight for modular forms with coefficients in $\mathbb{Z}$.

We discuss questions of finiteness of systems of Hecke eigenvalues modulo p^m, for a prime p and an integer $m \geq 2$, in analogy to the classical theory that already exists for $m = 1$. In joint work with Ian Kiming and Gabor Wiese ([KRW14]), we show that these questions are intimately related to a question of Buzzard regarding the boundedness of the field of definition of Hecke eigenforms (over $\mathbb{Q}_p$), and we formulate precise conjectures. We prove the existence of bounds on the weight filtrations of eigenforms modulo p^m, which gives evidence as to the truth of these conjectures. These bounds are made explicit in the case $N = 1$, $p = 2$.

Resumé

I [Rus14b] og [Rus14a], studerer vi graduerede ringe af modulformer på kongruensundergrupper med koefficienter i underringe A af $\mathbb{C}$, bestemmer grænser for vægtene af formerne i et minimalt frembringersæt, samt grænser for graderne af frembringerne i relationsidealet. Vi angiver en algoritme, der beregner strukturen af disse ringe, og formulerer formodninger om de minimale vægte for frembringere for modulformer med koefficienter i $\mathbb{Z}$.

Vi diskuterer spørgsmål om endlighed af systemer af Hecke egenværdier modulo p^m, hvor p er et primtal og $m \geq 2$ et heltal, i analogi til den klassiske teori, der findes for $m = 1$. I et samarbejde med Ian Kiming og Gabor Wiese ([KRW14]) beviser vi, at disse spørgsmål er nært forbundne med et spørgsmål af Buzzard om definitionslegmerne frembragt af Hecke egenværdier (over $\mathbb{Q}_p$). Vi beviser, at egenformer mod p^m har begrænsede vægtfiltrationer.

Chapter 0

Introduction

0.1 Overview

The contents of this thesis describe the two main projects I worked on during the three years of my PhD studies at the University of Copenhagen.

0.1.1 Generators and relations for algebras of modular forms

The idea for the first project came after reading the paper "On the algebra of modular forms on a congruence subgroup" by A. J. Scholl ([Sch79]). In that paper, Scholl proves that for a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, and a subring $A \subset \mathbb{C}$, the graded A-algebra $M(\Gamma, A)$ generated by modular forms (of all weights) for Γ whose q-expansion coefficients at ∞ lie in A is finitely generated. This result had already been known, and a proof appears earlier in [DR73] (Theorem VII.3.4). However, Scholl's proof is both more elementary and constructive, and gives an explicit set of generators.

I wrote an algorithm (Algorithm 5.3.1) based on Scholl's proof that allowed me to compute minimal sets of generators for the algebras $M(\Gamma, \mathbb{C})$ where $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$. Scholl's proof depends on the construction of a special modular form, which he calls a T-form, and which has special integrality and vanishing properties. The algorithm's speed depends on the weight of the T-form: the smaller the weight, the faster the algorithm runs. I observed that Scholl's construction of a T-form is not always optimal regarding the weight. In [Rus14b], I gave a T-form T for $\Gamma_0(p)$, where $p \geq 5$ is prime, of lower weight (equal to $p-1$) than what Scholl's recipe gives (which is equal to $\frac{12(p-1)}{\gcd(24p, p-1)}$), and in [Rus14a], I proved that this T-form is optimal. Having computed generators for the algebras

$M(\Gamma, \mathbb{C})$ for various congruence subgroups Γ, I noticed that the highest weight of a form appearing in a minimal set of generators for these algebras was always quite small, and seemed to be bounded independently of N.

When $A = \mathbb{C}$, this question had been previously studied by various authors. Borisov and Gunnels ([BG03]) proved, using the theory of toric modular forms, that for any prime N, the $\mathbb{C}$-algebra $M(\Gamma_1(N), \mathbb{C})$ is generated in weight (at most) 3. For congruence subgroups $\Gamma_0(N)$ with N square-free, one can use the work of Böcherer and Nebe ([BN10]) to show that the algebra $M(\Gamma_0(N), \mathbb{C})$ is generated in weight 10, as I have shown in [Rus14b], Section 4.1. The structure of $M(\Gamma_0(N), \mathbb{C})$ was determined explicitly when $X_0(N)$ has genus 0 in [SS11] by producing enough generators and relations explicitly and then using dimension formulae to conclude that they describe the whole structure.

For $\Gamma(N)$, with $N \geq 3$, Khuri-Makdisi shows, using the theory of line bundles on projective curves, that $M(\Gamma(N), \mathbb{C})$ is generated in weight 1, by explicitly exhibiting a subalgebra $\mathcal{R}_N$, generated by weight 1 Eisenstein series, and containing all modular forms of weight at least 2. Khuri-Makdisi's proof uses the description of modular forms of weight k for $\Gamma = \Gamma(N)$ as global sections of a line bundle $\mathcal{L}^{\otimes k}$ on the modular curve $X = X(\Gamma)$, and relies on a criterion that guarantees the surjectivity of the canonical multiplication map:

$$H^0(X, \mathcal{L}^{\otimes i}) \otimes H^0(X, \mathcal{L}^{\otimes j}) \to H^0(X, \mathcal{L}^{\otimes (i+j)}).$$

The kernel and cokernel of the multiplication map for invertible sheaves on smooth projective curves had been studied earlier by Mumford ([Mum70b]), where he provides slightly sharper criteria for surjectivity. In [Rus14b], I used Mumford's criteria to determine bounds on the weights of generators for the algebras $M(\Gamma_1(N), \mathbb{C})$ for $N \geq 5$ and $M(\Gamma_0(N), \mathbb{C})$ where $\Gamma_0(N)$ does not contain any elliptic elements.

After the publication of [Rus14b], it came to my attention that Wagreich had in [Wag80] and [Wag81] studied the generators of the algebra (over $\mathbb{C}$) of automorphic forms for a finitely generated Fuchsian group of the first kind. In these articles, Wagreich gave a precise description of the number of generators needed in each weight. The description depends only on the signature of the Fuchsian group involved, that is, a knowledge of the genus, the number of cusps, and the number and orders of elliptic points. Wagreich's results give an affirmative answer to Conjecture 1 in [Rus14b], mainly that $M(\Gamma_0(N), \mathbb{C})$ is generated in weight at most 6. In addition, when the algebra can be generated by at most 4 generators, Wagreich gives bounds on the degrees of the generators of the ideal of relations.

Since I was interested in studying reductions of modular forms moduli prime powers, I sought generalisations of these results to graded algebras of modular forms with coefficients in subrings of $\mathbb{C}$ which are as small as possible. In [Rus14b] and [Rus14a], I studied the $\mathbb{Z}[\frac{1}{N}]$ algebras $M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$, and was able to prove the following Theorem:

Theorem 3.4.4.*Let $N \geq 5$. The $\mathbb{Z}[\frac{1}{N}]$-algebra:*

$$M = M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}]) = \mathbb{Z}[\frac{1}{N}] \oplus \bigoplus_{k \geq 2} M_k(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$$

is generated in weight 3. Choosing a minimal set of generators, M is related in degree 6.

The idea of the proof is to first to prove the theorem for the reduction of M modulo p for all primes p not dividing N, and then deduce the theorem in characteristic 0. For that, we use the existence of a fine moduli scheme $X_1(N)$ over $\mathbb{Z}[\frac{1}{N}]$ classifying isomorphism classes of elliptic curves over $\mathbb{Z}[\frac{1}{N}]$ with $\Gamma_1(N)$-structure, and an invertible sheaf ω on $X_1(N)$, such that the global sections $H^0(X_1(N), \omega^{\otimes k})$ can be identified with the modular forms of weight k for $\Gamma_1(N)$ with coefficients in $\mathbb{Z}[\frac{1}{N}]$. Moreover, the formation of the invertible sheaf ω commutes with base change. The bounds we want then follow from an application of Mumford's results on the cohomology of invertible sheaves on projective curves over a perfect field ([Mum70b]).

For algebras of modular forms for congruence subgroups $\Gamma_0(N)$, the situation is complicated by the non-existence of a fine moduli scheme classifying isomorphism classes of elliptic curves with $\Gamma_0(N)$, due to the existence of non-trivial automorphisms for these objects. Instead, one should consider the moduli stacks $\mathcal{X}_0(N)$, on which there exists an invertible sheaf ω, such that the global sections $H^0(\mathcal{X}_0(N), \omega^{\otimes k})$ can be identified with the modular forms of weight k for $\Gamma_0(N)$. In order to apply Mumford's theorems, we take the pushfowards $\mathcal{L}_k$ of the sheaves $\omega^{\otimes k}$ to the coarse moduli schemes $X_0(N)$ over $\mathbb{Z}[\frac{1}{6N\varphi(N)}]$. The formation of these coarse moduli schemes and the corresponding sheaves $\mathcal{L}_k$ then commutes with base change, but it is no longer true that the sheaves $\mathcal{L}_k$ are each the kth tensor power of a fixed invertible sheaf. However, we are still able to derive bounds on the weights of generators and the degree of relations that are independent of N. In particular:

Theorem 4.3.7. *Let $N \geq 5$. Let ϵ_∞ be the number of cusps for $\Gamma_0(N)$, and let ϵ_2 and ϵ_3 be respectively the number of elliptic points of order 2 and of order*

3. The algebra

$$M = M(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}]) = \mathbb{Z}[\frac{1}{6N\varphi(N)}] \oplus \bigoplus_{k\geq 2} M_k(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])$$

is:

- *generated in weight* 2 *and related in degree* 6*, if* $\epsilon_3 = \epsilon_2 = 0$ *and* N *is composite,*
- *generated in weight* 6 *and related in degree* 14 *if* $\epsilon_3 > 0$ *and* $\epsilon_2 = 0$*,*
- *generated in weight* 12 *and related in degree* 130 *if* $\epsilon_3 > 0$ *and* $\epsilon_2 > 0$*, and*
- *generated in weight* 4 *and related in degree* 10 *otherwise.*

While Wagreich's results on the weights necessary to generate these algebras of modular forms $\mathbb{C}$ are more precise, Theorems 3.4.4 and 4.3.7 are valid for algebras of modular forms with coefficients in rings which are arithmetically more significant. For example, Theorems 3.4.4 and 4.3.7 can be used to determine generators for the algebras of modular forms modulo prime powers p^m. Moreover, Wagreich determines the generators of the ideal of relations only in cases where the algebra is generated by at most 4 elements, while the results of Theorems 3.4.4 and 4.3.7 are valid regardless of the number of generators involved. Finally, it should be noted that, while the results of Theorem 4.3.7 are stated for modular forms with coefficients in $\mathbb{Z}[\frac{1}{6N\varphi(N)}]$, they remain valid for modular forms with coefficients in $\mathbb{Z}[\frac{1}{6N}]$. The choice of inverting $\varphi(N)$ over the base was made to ease the exposition.

Using Theorems 3.4.4 and 4.3.7, one can write down an algorithm that takes as input a congruence subgroup of the form $\Gamma_0(N)$ or $\Gamma_1(N)$ and output a minimal set of generators as well as generators for the ideal of relations, thus giving a presentation of the corresponding algebra of modular forms. In this thesis, this algorithm is presented as Algorithms 5.3.1 and 5.3.5. Computations of the structure of these algebras using the algorithms provided (see Sections A.1 and A.2) show that the bounds given in Theorem 4.3.7 are not optimal, although they are not too far off the optimal values (except perhaps in the case where there are elliptic points of both orders). This suggests that it is perhaps possible to develop Riemann-Roch theory for stacky curves, and to obtain a version of Mumford's theorems for stacks, which would in turn prove the following:

Conjecture A.1.1. *Let* $N \geq 1$*. The* $\mathbb{Z}[\frac{1}{6N}]$ *algebra:*

$$M = M(\Gamma_1(N), \mathbb{Z}[\frac{1}{6N}]) = \mathbb{Z}[\frac{1}{6N}] \oplus \bigoplus_{k\geq 2} M_k(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N}])$$

is generated in weight 6 *and related in weight* 12*.*

This approach is currently being pursued by John Voight and David Zureick-Brown in an upcoming work and promises to provide an optimal and conceptually more satisfactory answer to the question of calculating minimal sets of generators and relations for graded algebras of modular forms.

There remains the question of determining bounds for generators of the algebras $M(\Gamma_0(N), \mathbb{Z})$. Scholl's proof of finite generation gives an upper bound on the generating weight of $M(\Gamma_0(N), \mathbb{Z})$. For example, for the algebra $M(\Gamma_0(p), \mathbb{Z})$ where $p \geq 5$ is prime, the existence of a T-form in weight $p-1$ as shown in [Rus14b] implies that the algebra $M(\Gamma_0(p), \mathbb{Z})$ is generated in weight $p^2 + 11$. This bound grows quadratically with the level, and one might hope to do better, perhaps find a bound which is independent of the level, in analogy to the results described so far. Unfortunately, a bound which is independent of the level turns out to be too much to ask for. In [Rus14a], I showed that:

Theorem 4.4.4. *Let $N \geq 5$ and let $p \geq 5$ be a prime which divides N exactly once. Then any set of generators for $M(\Gamma_0(N), \mathbb{Z})$ contains a form of weight $p-1$. In particular, the generating weight of $M(\Gamma_0(N), \mathbb{Z})$ is at least $p-1$.*

However, computations of generating weights (see Section A.3) for the algebras $M(\Gamma_0(p), \mathbb{Z})$ using Algorithm 5.3.1 does reveal a structure: the generating weight seems to be $p-1$. More precisely:

Conjecture 4.4.11. *The weights of the modular forms appearing in a minimal set of generators for $M(\Gamma_0(p), \mathbb{Z})$ are in the set $\{2, 4, 6, p-1\}$, and there is only one generator of weight $p-1$ (which can be chosen to be the T-form T).*

In [Rus14a], I described a possible first step towards a resolution of Conjecture 4.4.11. Consider the Atkin-Lehner operator acting on modular forms $f \in M_k(\Gamma_0(p), \mathbb{C})$ by:

$$f \mapsto f|_k W_p$$

where:

$$W_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Define an operator:

$$f \mapsto \tilde{f} = p^{\frac{k}{2}} f|_k W_p.$$

Let S denote the subset of $M(\Gamma_0(p), \mathbb{Z})$ consisting of modular forms $f = \sum_{n \geq 0} a_n q^n$ satisfying $v_p(\tilde{f}) \geq 0$, where:

$$v_p(f) = \inf\{v_p(a_n) : n \geq 0\}$$

is the p-adic valuation of f, and let T be the T-form in weight $p-1$. Then we have:

Theorem 4.4.9. *The algebra $M(\Gamma_0(p), \mathbb{Z})$ is generated by T and S.*

The proof of Theorem 4.4.9 requires a generalisation of a result of Serre on congruences between modular forms for $\Gamma_0(p)$ and modular forms for $\mathrm{SL}_2(\mathbb{Z})$, which is the following:

Theorem 4.4.6. *Let $p \geq 5$, $f \in M_k(\Gamma_0(p), \mathbb{Z})$ with $v_p(f) = 0$ and $v_p(\tilde{f}) = k + a$. Then there exists $g \in M_{k-a(p-1)}(SL_2(\mathbb{Z}), \mathbb{Z})$ such that $f \equiv g \pmod p$.*

Serre proves the theorem in [Ser73b] in the case where $a \leq 0$. To prove the theorem in the case where $a > 0$, I used intersection theory on the moduli stack $\mathcal{X}_0(p)$ as developed by Deligne and Rapoport in [DR73]. By Theorem 4.4.9, Conjecture 4.4.11 is now reduced to the following conjecture:

Conjecture 4.4.10. *The $\mathbb{Z}$-subalgebra of $M(\Gamma_0(p), \mathbb{Z})$ generated by $S = \{f \in M(\Gamma_0(p), \mathbb{Z}) : v_p(\tilde{f}) \geq 0\}$ is generated in weight 6.*

0.1.2 Modular forms modulo p^m

Fix a congruence subgroup Γ (e.g. $\Gamma \in \{\Gamma_0(N), \Gamma_1(N)\}$), and a prime $p \nmid N$. Let $\mathfrak{S}$ be the set of normalised Hecke eigenforms for Γ. It is clear by classical theory that the set $\mathfrak{S}$ is infinite. It is also well known that normalised Hecke eigenforms have q-expansions whose coefficients are algebraic integers. It is therefore possible to consider their reductions $\overline{\mathfrak{S}}$ modulo p. As it turns out, the elements of $\mathfrak{S}$ often have congruent q-expansions modulo p. In fact, due to work of Serre, Tate, Jochnowitz ([Joc82a]), and Ash-Stevens ([AS86]), it is known that for any element $f \in \mathfrak{S}$, there exists a modular form g of weight at most $p^2 + p$ such that:

$$f \equiv g \pmod p.$$

Moreover, by the Deligne-Serre lifting lemma (Lemma 6.2.3), the modular form g can be chosen to be an element of $\mathfrak{S}$ as well. Therefore, the set $\overline{\mathfrak{S}}$ is finite.

This fact has numerous applications. For instance, one finds such an application in [Edi92] to Serre's modularity conjecture, which we will shortly describe. Given a normalised Hecke eigenform f, Deligne constructed Galois representations:

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

with controlled ramification and behaviour at the Frobenius element Frob_ℓ for each prime $\ell \neq p$. Serre then conjectured that for every semisimple, 2-dimensional odd representation:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

there exists a Hecke eigenform f such that:

$$\rho \cong \rho_f.$$

This is known as the weak form of Serre's conjecture. Additionally, Serre gave a precise recipe for the level N, weight k and character ϵ of f; this recipe is known as the strong Serre conjecture. In [Edi92], Edixhoven uses the theory of mod p modular forms to prove that the weak Serre conjecture (for the weight) implies the strong Serre conjecture.

The question of Galois representations modulo p^m when $m \geq 2$ is a natural one. In [CKW13], Chen, Kiming, and Wiese define three successively weaker notions of eigenforms modulo p^m: strong, weak, and dc-weak. In this thesis, I only consider strong and weak eigenforms modulo p^m.

In a nutshell, a modular form f modulo p^m is simply the reduction modulo p^m of the q-expansion of a modular form for Γ with coefficients in $\overline{\mathbb{Z}}_p$, and f is said to be a weak eigenform if $a_1(f) = 1$ and there exist constants $\lambda_\ell \in \overline{\mathbb{Z}/p^m\mathbb{Z}}$ for all primes ℓ such that:

$$T_\ell f = \lambda_\ell f$$

where T_ℓ are the reductions of the Hecke operators. If f is a weak eigenform of weight k, then one can always find a modular form $\tilde{f}$ of weight k such that $\tilde{f}$ reduces to f modulo p^m. If it is possible to choose $\tilde{f}$ to be a normalised Hecke eigenform in $M_k(\Gamma, \overline{\mathbb{Z}}_p)$, then we call f a strong eigenform.

One fundamental difference between the situation mod p and the situation mod p^m for $m \geq 2$ is pointed out in [CKW13]. When working mod p, one has the Deligne-Serre lifting lemma (Lemma 6.2.3), which ensures that every weak eigenform mod p is also strong. However, the Deligne-Serre lifting lemma is no longer valid modulo p^m. In [CKW13], an example is presented of a weak eigenform which is not strong at the same weight, i.e. it is not the reduction of an eigenform of the same weight in characteristic 0. In the same article, the question is raised about whether the notions of weak and strong coincide if one is allowed to vary the weight. In Corollary 6.2.7, we show that the answer to the question is negative. In particular, we present an eigenform modulo 4 of level 1 which is not the reduction of any Hecke eigenform in level 1 of any weight. However, it might still be possible that if one is allowed to vary the level as well as the weight, then one can still lift weak eigenforms.

In analogy with the situation mod p, we are lead to the following question:

Question 0.1.1 (Finiteness of Hecke eigenforms mod p^m)**.** *Are there only finitely many congruence classes of strong Hecke eigenforms modulo p^m? In other words, is the set $\mathfrak{S} \pmod{p^m}$ finite?*

Question 0.1.2 (Finiteness of Galois representations mod p^m)**.** *Are there only finitely many isomorphism classes of Galois representations mod p^m attached to strong Hecke eigenforms?*

One should note that the restriction of the above questions to strong eigenforms is a necessary one. Indeed, if one puts no restrictions on the coefficient rings of weak eigenforms mod p^m, then one can find infinitely many weak eigenforms at the same weight, as an argument of Calegari and Emerton shows in [CE04].

In a joint work ([KRW14]) together with Ian Kiming and Gabor Wiese, we elaborate these questions into precise conjectures, as described in Section 7.3. We found that these conjectures are intimately linked with a question posed by Kevin Buzzard in [Buz05] (Question 4.4):

Question 7.3.1. *For $f = \sum_{n\geq 0} a_n q^n \in \mathfrak{S}$, let:*

$$K_{f,p} := \mathbb{Q}_p(a_n : n \geq 0).$$

Is the quantity:

$$\sup_{f\in\mathfrak{S}} [K_{f,p} : \mathbb{Q}_p]$$

finite?

As it turns out, a positive answer to Buzzard's question implies a positive answer to the finiteness question. In fact, a positive answer to Buzzard's question is equivalent to finiteness together with some boundedness conditions on indices.

In Sections 7.1 and 7.2, we give some evidence towards these conjectures. First, as a warm up, we show the following:

Theorem 7.1.2. *There exists a constant $C(m)$ depending only on m such that whenever $f \in S_k(SL_2(\mathbb{Z}), \overline{\mathbb{Z}/2^m\mathbb{Z}})$ is a weak eigenform, then f is the reduction modulo 2^m of a form of weight bounded by a constant $\kappa(m)$ depending only on m, and which can be made explicit.*

The proof is based on Nicolas-Serre theory, as presented in [NS12]. One should note that a similar result can be obtained using analogous arguments for prime $p = 3$ (and still at level 1), since a Nicolas-Serre theory can also be developped in that setting, as shown in the appendix of [BK]. In Section 7.2, we generalize this proof, and we show the following:

Theorem 7.2.1. *There exists a constant $\kappa(N,p,m)$ depending only on N, p, and m such that every eigenform $f \in M(\Gamma_1(N),\overline{\mathbb{Z}/p^m\mathbb{Z}})$ is the reduction mod p^m of a modular form of weight at most $\kappa(N,p,m)$.*

Unlike Theorem 7.1.2, we have not made the constants $\kappa(N,p,m)$ explicit. A key step in the proof is the following result. Here, for a modular form f, $w_p(f)$ denotes the mod p weight filtration of f, which is the smallest weight in which one can find a modular form g such that $f \equiv g \pmod{p}$.

Proposition 7.2.2. *Let $f \in S_k(\Gamma_1(N),\overline{\mathbb{F}}_p)$. Suppose that for some integer d, there exists a system $\{\lambda_\ell\}_{\ell \ prime}$ of (cuspidal) Hecke eigenvalues such that:*

$$w_p(T_\ell f - \lambda_\ell f) \leq d$$

for all primes ℓ. Then:

$$w_p(f) \leq \eta(N,p,d)$$

where $\eta(N,p,d)$ is a constant depending only on N, p, and d.

If we adopt the convention that $w_p(0) = -\infty$, then we see that Proposition 7.2.2 is a generalisation of the bounds obtained by Jochnowitz ([Joc82a], [Joc82b]) on the mod p weight filtrations of Hecke eigenforms.

An important tool in the study of modular forms mod p is Ramanujan's θ operator. On q-expansions, it acts by:

$$\theta(\sum_{n\geq 0} a_n q^n) = \sum_{n \geq 1} n a_n q^n.$$

In characteristic 0, the θ operator does not send modular forms to modular forms. It is classically known, however, that the θ operator induces a derivation:

$$\theta_p : M_k(\Gamma, \overline{\mathbb{F}}_p) \to M_{k+p+1}(\Gamma, \overline{\mathbb{F}}_p).$$

The existence and properties of the operator θ_p are crucial to the proof of finiteness of mod p eigenforms in [Joc82a], and in Edixhoven's study of Serre's conjecture in [Edi92].

In [CK14], Chen and Kiming show that the θ operator induces an operator:

$$\theta_{p^m} : M_k(\Gamma_1(N), \mathbb{Z}/p^m\mathbb{Z}) \to M_{k+k(p)}(\Gamma_1(N), \mathbb{Z}/p^m\mathbb{Z})$$

where $k(p) = 2 + 2p^{m-1}(p-1)$. One might hope that, in analogy to the case of modular forms mod p, the operator θ_{p^m} might be useful in attacking the questions of finiteness and weight bounds. We discuss this operator in Section 6.3, and show through a computational investigation that the behaviour of the operator θ_{p^m} is much more complicated than that of θ_p.

0.2 Structure of the thesis

A basic overview of the theory of congruence subgroups and modular forms is given in Chapter 1.

In Chapter 2, the terminology and notation concerning graded algebras of modular forms is set up, and a basic lemma in linear algebra is proven. The structure of the graded algebra of modular forms of level 1 with coefficients in $\mathbb{Z}$ is determined. Although this is classical, I chose to include a proof as a warm up.

The algebras $M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$ are studied in Chapter 3, and bounds on the generating weight as well as on the degrees of generators of the ideal of relations are determined. The contents of this chapter are taking from the articles [Rus14b] and [Rus14a].

In Chapter 4, the algebras $M(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])$ are studied, and bounds for generators and relations are determined. The algebra $M(\Gamma_0(p), \mathbb{Z})$ is then examined, and a lower bound on the generating weight for these algebras is given, as well as a set of generators. The contents of this chapter are based on the articles [Rus14b] and [Rus14a], however, new and stronger results are presented.

Chapter 5 describes Scholl's proof of finite generation, and gives algorithms that are based on his proof for computing the structure of the algebra of modular forms for a given congruence subgroup and with coefficients in a subring A of $\mathbb{C}$. We examine Scholl's construction of a T-form for the congruence subgroups $\Gamma_0(N)$, and show that it is not always optimal (i.e. it is not of the smallest possible weight). For the groups $\Gamma_0(p)$, where $p \geq 5$, we explicitly construct the optimal T-form. This is taken mainly from the article [Rus14b]; the optimality of the T-form is discussed also in [Rus14a].

The basic theory of modular forms mod p^m is described in Chapter 6, and it is based on [CKW13] and [CK14]. The discussion of the θ_{p^m} cycles has not appeared elsewhere.

In Chapter 7, we prove the existence of bounds for the weight filtrations of weak eigenforms modulo p^m. In the case $N = 1$, $p = 2$, we make these bounds explicit. The discussion of Buzzard's questions and related conjectures, as well as the weight bounds for the case $N = 1, p = 2$, have appeared in [KRW14].

Finally, numerical results obtained through application of the theory presented in Chapters 1-7 are presented in Append A. These include bounds for generators and relations for the various algebras of modular forms studied in this thesis, as well as computational evidence supporting Conjecture 4.4.11. We also give some computations of θ_{p^2}-cycles, and explicit weight bounds for weak eigenforms modulo p^m.

Chapter 1

Modular forms

In this chapter, we give an exposition of the basic definitions and facts in the theory of modular form. This exposition closely follows that in Chapters 1-3 of [DS05], and additional references are given where needed.

1.1 Congruence subgroups

The modular group is the group $\mathrm{SL}_2(\mathbb{Z})$ of 2×2 integral matrices with determinant 1. The principal congruence subgroup of level N is the group:

$$\Gamma(N) := \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N\}.$$

That is, $\Gamma(N)$ is the group of matrices in $\mathrm{SL}_2(\mathbb{Z})$ which are congruent to the identity modulo N. In general, a congruence subgroup is a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, such that $\Gamma(N) \subset \Gamma$ for some $N \geq 1$. Note that $\Gamma(N) \subset \Gamma(M)$ if and only if $M|N$. If for some $N \geq 1$ we have $\Gamma(N) \subset \Gamma$, then we say that Γ is of level N.

The index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite, thus every congruence subgroup has finite index. We single out two special families of congruence subgroups:

$$\Gamma_0(N) := \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N\},$$

$$\Gamma_1(N) := \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N\}.$$

We note that $\Gamma_1(N) \subset \Gamma_0(N)$, and that for $i \in \{0,1\}$, $\Gamma_i(N) \subset \Gamma_i(M)$ if and only if $M|N$. Furthermore, the group homomorphism $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ sending

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $d \pmod N$ is surjective with kernel $\Gamma_1(N)$. Therefore $\Gamma_1(N) \lhd \Gamma_0(N)$ and $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$.

Lemma 1.1.1. *For any N, $\Gamma(N)$ is normal in $\Gamma_1(N)$, and $\Gamma_1(N)$ is normal in $\Gamma_0(N)$. Furthermore, the indices for the inclusions:*

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z})$$

are given by:

- $[\Gamma_1(N) : \Gamma(N)] = N$,
- $[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)$ *where φ is Euler's totient function, and*
- $[SL_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N}(1 + \frac{1}{p})$, *where the product is taken over primes p dividing N.*

Throughout the rest of this section, we let Γ be a congruence subgroup. In general, we define a left action of $\mathrm{GL}_2^+(\mathbb{Q})$ (rational matrices with positive determinant) on the extended upper half plane:

$$\mathcal{H} \cup \mathbb{Q} \cup \{\infty\} = \{z \in \mathbb{C} : \Im(z) > 0\} \cup \mathbb{Q} \cup \{\infty\}$$

by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az+b}{cz+d}.$$

This action then induces an action of Γ on $\mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{Q} \cup \{\infty\}$, then $\gamma \cdot z \in \mathbb{Q} \cup \{\infty\}$. A cusp of Γ is a Γ-equivalence class of elements in $\mathbb{Q} \cup \{\infty\}$ under the action of Γ. The group $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{Q} \cup \{\infty\}$, hence there is only one cusp of $\mathrm{SL}_2(\mathbb{Z})$. Since every congruence subgroup has finite index, it follows that there are only finitely many cusps of Γ. We will intentionally conflate a cusp of Γ with representatives of that cusp; for example, we will refer to the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of ∞ as the cusp ∞ of $\mathrm{SL}_2(\mathbb{Z})$.

For $z \in \mathcal{H}$, the isotropy subgroup of z is the subgroup Γ_z of Γ fixing z, that is:

$$\Gamma_z := \{\gamma \in \Gamma : \gamma \cdot z = z\}.$$

The point $z \in \mathcal{H}$ is called an elliptic point if the containment:

$$\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\} \subset \{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}\Gamma_z$$

is proper. It turns out that any elliptic point must be $\mathrm{SL}_2(\mathbb{Z})$-equivalent to either i, in which case we say it is of order 2, or to $\rho = e^{2\pi i/3}$, in which case we say it is of order 3. Note that the converse is not true: not every point which is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to either i or ρ is necessarily an elliptic point for Γ.

The width of a cusp s of Γ is the smallest positive integer h such that:

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \gamma^{-1}\Gamma\gamma$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ satisfying $\gamma \cdot \infty = s$. Let c be a cusp of width h. The quotient group $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{1, -1\}$ acts naturally on the upper half plane, and the stabiliser of c in $\mathrm{PSL}_2(\mathbb{Z})$ is conjugate to $\left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle$. If the stabiliser of c in $\mathrm{SL}_2(\mathbb{Z})$ is of the form $\left\langle -\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle$, then the cusp c is said to be irregular. Otherwise, we say that c is regular.

Lemma 1.1.2. *Let ϵ_∞, ϵ_2 and ϵ_3 and be respectively the number of elliptic points for Γ of order 2 and order 3, and the number of cusps. The values of these numbers are given in the following table ([DS05], Figure 3.3):*

Γ	ϵ_2	ϵ_3	ϵ_∞
$SL_2(\mathbb{Z})$	*1*	*1*	*1*
$\Gamma_0(N), N > 2$	$\prod_{p\mid N}\left(1+\left(\frac{-1}{p}\right)\right)$ *if* $4 \nmid N$ 0 *if* $4 \mid N$	$\prod_{p\mid N}\left(1+\left(\frac{-3}{p}\right)\right)$ *if* $9 \nmid N$ 0 *if* $9 \mid N$	$\sum_{d\mid N}\varphi(\gcd(d, \frac{N}{d}))$
$\Gamma_1(2) = \Gamma_0(2)$	*1*	*0*	*2*
$\Gamma_1(3)$	*0*	*1*	*2*
$\Gamma_1(4)$	*0*	*0*	*3*
$\Gamma_1(N), N > 4$	*0*	*0*	$\frac{1}{2}\sum_{d\mid N}\varphi(d)\varphi(\frac{N}{d})$

Here, $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol of quadratic reciprocity. Furthermore, out of all these congurence subgroups, only $\Gamma_1(4)$ has an irregular cusp.

1.2 Modular forms

1.2.1 Definitions

For $k \in \mathbb{Z}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$, we define an operator $-|_k\gamma$ acting on functions $f : \mathcal{H} \to \mathbb{C}$ by:

$$(f|_k\gamma)(z) = \det(\gamma)^{\frac{k}{2}}(cz+d)^{-k} f(\gamma \cdot z).$$

Lemma 1.2.1. *Let $\gamma, \gamma' \in GL_2(\mathbb{Q})$, $f, g : \mathcal{H} \to \mathbb{C}$, and $k, k' \in \mathbb{Z}$. The operators $-|_k-$ satisfy the following properties:*

1. *$(f+g)|_k\gamma = f|_k\gamma + g|_k\gamma$.*

2. $(fg)|_{k+k'}\gamma = f_k|\gamma \cdot g_{k'}|\gamma$.

3. $-|_k\gamma \circ -|_k\gamma' = -|_k(\gamma\gamma')$.

Let Γ be a congruence subgroup. A function $f : \mathcal{H} \to \mathbb{C}$ is said to be weakly modular of weight k with respect to Γ if f is meromorphic and:

$$f|_k\gamma = f$$

for all $\gamma \in \Gamma$.

Let f be a weakly modular function of weight k with respect to Γ, and let h be the width of the cusp ∞ of Γ. Thus Γ contains a matrix of the form $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$, hence $f(z+h) = f(z)$, that is, f is $h\mathbb{Z}$-periodic. Letting $q_h := e^{2i\pi z/h}$, the function f has then a Fourier series expansion of the form:

$$f(z) = \sum_{n=-m}^{\infty} a_n(f) q_h^n$$

which we call the q-expansion of f at ∞. Here, $a_n(f)$ are complex numbers that depend only on f and n, which we call the coefficients of f. When there is no ambiguity, we simply write a_n for $a_n(f)$. We say that f is holomorphic at ∞ if $a_n(f) = 0$ for all $n < 0$, that is, the q-expansion of f has the following form:

$$f(z) = \sum_{n=0}^{\infty} a_n q_h^n.$$

Let s be a cusp of Γ, and let h_s be the width of s. Since $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{Q} \cup \{\infty\}$, there exists a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $s = \gamma \cdot \infty$. Define $g_{s,\gamma} := f|_k\gamma$ and $\Gamma' := \gamma^{-1}\Gamma\gamma$. By Lemma 1.2.1, $g_{s,\gamma}$ is then weakly modular of weight k with respect to Γ'. The cusp ∞ of Γ' has width h_s. Thus $g_{s,\gamma}$ has a q-expansion at ∞:

$$g_{s,\gamma} = \sum_{n=-m}^{\infty} a_{n,s,\gamma} q_{h_s}^n.$$

We say that f is holomorphic at the cusps of Γ if, for each cusp s and each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $s = \gamma \cdot \infty$, $g_{s,\gamma}$ is holomorphic at ∞.

We are ready to define modular forms.

Definition 1.2.2. *A modular form of weight k with respect to Γ is a function $f : \mathcal{H} \to \mathbb{C}$ such that:*

1. f is weakly modular with respect to Γ,

2. *f is holomorphic on $\mathcal{H}$, and*

3. *f is holomorphic at the cusps of Γ.*

If Γ is of level N, we also say that f is of level N.

Definition 1.2.3. *A cusp form of weight k with respect to Γ is a modular form of weight k with respect to Γ that vanishes at the cusps, that is, $a_0(f|_k\gamma) = 0$ for all $\gamma \in SL_2(\mathbb{Z})$.*

Definition 1.2.4. *Let $A \subset \mathbb{C}$ be a ring. We say that a modular form of weight k with respect to Γ has coefficients in A if the coefficients q-expansion lies in $A[[q]]$. That is, if:*

$$f = \sum_{n=0}^{\infty} a_n q^n,$$

then $a_n \in A$ for all n. The set of modular forms of weight k with respect to Γ is denoted $M_k(\Gamma, A)$. The subset of $M_k(\Gamma, A)$ consisting of cusp forms is denoted $S_k(\Gamma, A)$. We write $M_k(\Gamma) = M_k(\Gamma, \mathbb{C})$ and $S_k(\Gamma) = S_k(\Gamma, \mathbb{C})$.

If $\Gamma \subset \Gamma'$ are congruence subgroups, then $M_k(\Gamma') \subset M_k(\Gamma)$ and $S_k(\Gamma') \subset S_k(\Gamma)$. In particular, $M_k(\Gamma)$ always contains $M_k(\mathrm{SL}_2(\mathbb{Z}))$.

1.2.2 First examples and properties

Having defined modular forms, we now exhibit explicit examples, showing that the definition is not vacuous. Every complex number is trivially a modular form of weight 0. We now describe non-trivial examples. In the following, ζ denotes the Riemann zeta function, and B_k the kth Bernoulli number.

Proposition 1.2.5. *Let $k \geq 4$ be an even integer. The Eisenstein series of weight k is the function:*

$$E_k(z) = \frac{1}{2\zeta(k)} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{1}{(cz+d)^k}, z \in \mathcal{H}.$$

Then $E_k \in M_k(SL_2(\mathbb{Z}), \mathbb{Z})$, and E_k has q-expansion:

$$E_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Now that we have some interesting modular forms, we can use them to construct others.

Lemma 1.2.6. *Let Γ be a congruence subgroup, and $k, k' \in \mathbb{Z}$. Let $f \in M_{k'}(\Gamma, A)$ and $g \in M_{k'}(\Gamma, A)$. Then:*

1. *$fg \in M_{k+k'}(\Gamma, A)$;*

2. *$f+g$ is a modular form if and only if $k = k'$, in which case $f+g \in M_k(\Gamma, A)$.*

Proof.

1. This is a direct consequence of the definitions and of Lemma 1.2.1.

2. If $k = k'$, then the definitions and Lemma 1.2.1 imply that $f+g \in M_k(\Gamma, A)$. For the reverse implication, see [Miy06], Lemma 2.1.1.

□

We now construct a very interesting modular form, which is our first example of a cusp form.

Proposition 1.2.7. *The modular discriminant is the modular form $\Delta \in M_{12}(SL_2(\mathbb{Z}))$ given by:*

$$\Delta := \frac{E_4^3 - E_6^2}{1728}.$$

The modular discriminant has coefficients in $\mathbb{Z}$. Indeed, Δ has q-expansion:

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - \cdots .$$

Thus Δ has a simple zero at the cusp ∞ of $SL_2(\mathbb{Z})$, and vanishes nowhere else, that is, $\Delta(z) \neq 0$ for each $z \in \mathcal{H}$.

Lemma 1.2.8. *The inverse Δ^{-1} of the modular discriminant has coefficients in $\mathbb{Z}$.*

Proof. Considering the product formula in Proposition 1.2.7, the inverse Δ^{-1} is recognised to be:

$$\Delta^{-1} = \frac{1}{q} \left(\sum_{n=0}^{\infty} p(n) q^n \right)^{24}$$

where $p(n)$ is the partition function. □

By Lemma 1.2.6, the spaces $M_k(\Gamma, A)$ and $S_k(\Gamma, A)$ are naturally A-modules; in particular, if $K = \mathbb{Q}$ or $\mathbb{C}$, then $M_k(\Gamma, K)$ is a K-vector space. For some weights, it is easy to describe the corresponding spaces of modular forms.

Lemma 1.2.9. *Let Γ be a congruence subgroup. Then $M_0(\Gamma, A) = A$. Furthermore, if $k \in \mathbb{Z}$, then $M_k(\Gamma, A) = 0$ if either:*

- *$k < 0$, or*

- *$-1 \in \Gamma$ and k is odd.*

Proof. A weight 0 modular form is a function from the compact curve $X(\Gamma)$ to the Riemann sphere $\mathbb{C} \cup \{\infty\}$ with no poles. By the theory of compact Riemann surfaces, such a function must be a constant.

Suppose now that f is a modular form of weight $k < 0$. Then the function $g := f^{12}\Delta^{-k}$ is a weight 0 modular form, hence a constant. Thus g is identically equal to the constant term $a_0(g)$ of its q-expansion. But by Proposition 1.2.7, $a_0(g) = 0$.

Let f be a modular form of weight k with respect to Γ. If $-1 \in \Gamma$, then by the definition of modular forms, we get:

$$f(z) = f(\frac{-z}{-1}) = (-1)^k f(z)$$

and hence $f = 0$. □

For other weights, we still have some control over the number of modular forms.

Proposition 1.2.10. *Let Γ be a congruence subgroup, and $k \in \mathbb{Z}$. Then:*

1. *The vector space $M_k(\Gamma)$ is finite dimensional.*
2. *The space $M_k(\Gamma)$ has an integral basis, that is, a basis whose elements are elements of $M_k(\Gamma, \mathbb{Z})$.*

In fact, using the Riemann-Roch theorem, one can derive precise formulae for the dimensions of the spaces $M_k(\Gamma)$. As an example, we look at the case of modular forms of level 1.

Proposition 1.2.11. *For modular forms of weight k and of level 1, we have the following dimension formula:*

$$\dim M_k(SL_2(\mathbb{Z})) = \begin{cases} \lfloor \frac{k}{12} \rfloor & k \equiv 2 \pmod{12}, \\ 1 + \lfloor \frac{k}{12} \rfloor & \textit{otherwise}. \end{cases}$$

1.3 Operators on modular forms

In this section, we introduce some important operators acting on spaces of modular forms, which we will use in this work. We will restrict our attention to a congruence subgroup $\Gamma_1(N)$ for a fixed $N \geq 1$, although these definitions make sense for other congruence subgroups as well. To obtain the definitions of these operators for congruence subgroups $\Gamma_0(N)$, simply replace the diamond operator $\langle - \rangle$ (see Definition 1.3.2) by the identity operator wherever it appears.

We begin by introducing Hecke operators through the following proposition.

Proposition 1.3.1. *For each prime p, there exist a linear operator T_p which acts on the space $M_k(\Gamma)$ of modular forms, whose effect on q-expansions is:*

$$T_p(f) = \begin{cases} \sum_{n\geq 0} a_{np}q^n + p^{k-1}\sum_{n\geq 0} a_n q^{np} & p \nmid N \\ \sum_{n\geq 0} a_{np}q^n & p|N. \end{cases}$$

Definition 1.3.2. *The operator T_p of Proposition 1.3.1 is called the pth Hecke operator on $M_k(\Gamma)$. For each $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, define the diamond operator acting on $f \in M_k(\Gamma_1(N))$ by:*

$$\langle d\rangle f = f|_k\gamma$$

for any $\gamma = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$ with $\delta \equiv d \pmod{N}$. For d not invertible mod N, define $\langle d\rangle f = 0$.
For a prime power p^r, we define the Hecke operator T_{p^r} recursively by:

$$T_1 = 1,$$

$$T_{p^r} = T_pT_{p^{r-1}} - \langle p\rangle T_{p^{r-2}} = \begin{cases} T_pT_{p^{r-1}} - T_{p^{r-2}} & p \nmid N \\ (T_p)^r & p|N. \end{cases}$$

For any positive integer n with prime factorisation $n = \prod p_i^{e_i}$, we define the nth Hecke operator by:

$$T_n = \prod T_{p^i}^{e_i}.$$

Proposition 1.3.3. *The Hecke operators $\{T_n\}_{n\geq 1}$ commute with each other, and with the diamond operators $\langle d\rangle$.*

Definition 1.3.4. *A modular form which is a simultaneous eigenvector for all Hecke operators is called a Hecke eigenform, or simply an eigenform. A modular form $f = \sum_{n\geq 1} a_nq^n$, is said to be normalised if it is cuspidal and $a_1 = 1$.*

Proposition 1.3.5. *Let f be a normalised eigenform. Then a_n is an algebraic integer for every n, and:*

$$T_nf = a_n(f)f$$

for all $n \geq 1$.

Additionally, we define three operators, U_p, V_p, and tr_p, as follows:

Definition 1.3.6. *Let p be a prime number. There exists an operator:*

$$V_p : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(pN))$$

$$\sum_{n\geq 0} a_nq^n \mapsto \sum_{n\geq 0} a_nq^{pn}.$$

If $p|N$, then the operator T_p is denoted by U_p, and we can define a trace operator:

$$tr_p : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(\frac{N}{p})),$$

$$f \mapsto \sum_{i=1}^{r} f|_k\gamma_i$$

where γ_i are representatives of the cosets of $\Gamma_1(N)$ in $\Gamma_1(\frac{N}{p})$.

We now switch to congruence subgroups $\Gamma_0(N)$. We define Atkin-Lehner involutions, and relate them to the operators tr and U defined in Definition 1.3.6.

Definition 1.3.7. *Let p be a prime number dividing N exactly once. The Atkin-Lehner involution is the operator acting on modular forms $f \in M_k(\Gamma_0(N))$ by:*

$$f \mapsto f|_kW_p^N$$

where:

$$W_p^N = \begin{pmatrix} p & a \\ N & bp \end{pmatrix},$$

a and b being any integers such that $\det W_p^N = p^2b - Na = p$. Note that this operator is really an involution, meaning that $(f|_kW_p^N)|_kW_p^N = f$.

Proposition 1.3.8 ([Ser73b], §2, Lemme 7)**.** *For modular forms on the congruence subgroup $\Gamma_0(p)$, the operators $tr = tr_p$, $U = U_p$, and the Atkin-Lehner involution given by the matrix $W_p = W_p^p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ are related by:*

$$tr(f) = f + p^{1-\frac{k}{2}}(f|_kW_p)|U.$$

Chapter 2

Graded algebras of modular forms

In this chapter, we set up the terminology and notation concerning graded algebras of modular forms, and, as a warm up, we determine the structure of the graded algebra of modular forms of level 1 with coefficients in $\mathbb{Z}$.

2.1 Definitions

As we have seen in Lemma 1.2.6, modular forms with respect to a certain congruence subgroup generate a graded ring. For technical reasons to be clarified later, we will leave out modular forms of weight 1 (see Theorem 3.2.3).

Definition 2.1.1. *Let Γ be a congruence subgroup, and $A \subset \mathbb{C}$ a subring. The graded A-algebra of modular forms with respect to Γ is the direct sum:*

$$M(\Gamma, A) := A \oplus \left(\bigoplus_{k \geq 2} M_k(\Gamma, A) \right).$$

We write $M(\Gamma) := M(\Gamma, \mathbb{C})$.

The q-expansion map sending a modular form f of weight k to its q-expansion is injective, giving an embedding $M_k(\Gamma) \hookrightarrow \mathbb{C}[[q]]$. Therefore, we can identify modular forms of a given weight k with their q-expansions. Let p be a prime. If f is a modular form with coefficients in $\mathbb{Z}$, we can define the modulo p reduction of f as the formal (coefficient-wise) reduction of its q-expansion. We formalise this definition.

Definition 2.1.2. *Let p be a prime, A a ring in which p is nilpotent (for example, an $\mathbb{F}_p$-algebra), Γ a congruence subgroup, and k a positive integer. A modular form of weight k with respect to Γ with coefficients in A is defined to be an element* *of $M_k(\Gamma, A) := M_k(\Gamma, \mathbb{Z}) \otimes A$, where here $M_k(\Gamma, \mathbb{Z})$ is considered as a subring of $\mathbb{Z}[[q]]$. When there is no ambiguity, we speak of modular forms mod p^m when A is a $\mathbb{Z}/p^m\mathbb{Z}$-algebra.*

By Lemma 1.2.6, the sum of modular forms (in characteristic 0) of distinct weights cannot be 0. As we shall see, this does not hold for the modular forms mod p defined in Definition 2.1.2. For example, for every prime $p \geq 5$, we have the congruence $E_{p-1} \equiv 1 \pmod{p}$. This means that modular forms mod p, defined as formal power series as in Definition 2.1.2, do not form a graded ring. This can be remedied later once we introduce the geometric interpretation of modular forms. For now however, we can define the graded algebra of modular forms mod p by taking the *external* direct sum across all weights.

Definition 2.1.3. *Let p be a prime, A an $\mathbb{F}_p$-algebra, and Γ a congruence subgroup. The graded A-algebra of modular forms with respect to Γ is the direct sum:*

$$M(\Gamma, A) := A \oplus \left(\bigoplus_{k \geq 2} M_k(\Gamma, A) \right),$$

where the graded A-algebra structure is defined as follows: addition is defined component-wise; multiplication of two elements $f, g \in M(\Gamma, A)$ is defined by first lifting f and g (component-wise) to elements F and G in characteristic 0 and then reducing the product $F \cdot G$ (component-wise) modulo p. When there is no ambiguity, we speak of the graded algebra of modular forms mod p.

2.2 Structure of a graded, finitely generated $\mathbb{Z}[\frac{1}{N}]$-algebra

Throughout this section, let $N \geq 1$ be an integer, $A = \mathbb{Z}[\frac{1}{N}]$ or $\mathbb{F}_p$ where $p \nmid N$ is a prime, and M a commutative $\mathbb{N}$-graded A-algebra without zero divisors. We denote by M_k the kth graded part of $M = \bigoplus_{k \geq 0} M_k$. If g is a homogeneous element of M, that is, $g \in M_k$ for some k, then the weight of g is $wt(g) := k$. We further assume that each M_k is a free A-module of finite rank.

Definition 2.2.1. *We say that M is finitely generated if there exists a finite subset $\{g_1, \cdots, g_m\} \subset M$ such that every element of M can be written as a polynomial in $g_1, \cdots, g_m$. In that case, we can choose the generators $g_1, \cdots, g_m$ to be homogeneous* [*]*, and if $n = \max\{wt(g_i) : 1 \leq i \leq m\}$, we say that M is generated in weight n. If n is the smallest non-negative integer such that M is generated in weight n, we say that n is the generating weight of M. Equivalently, the generating weight n of M is the smallest non-negative integer such that the*

[*] by choosing generators and then choosing their homogeneous parts.

smallest graded A-subalgebra of M containing:

$$\bigoplus_{k=0}^{n} M_k$$

is the whole algebra M.

Suppose that M is finitely generated. Let $\{g_1, \cdots, g_m\}$ be a set of homogeneous generators. Let $A[x_1, \cdots, x_m]$ be the weighted polynomial ring in $x_1, \cdots, x_m$ where each x_i is assigned weight $wt(g_i)$. Thus there is a surjective homomorphism of graded A-algebras:

$$\Phi : A[x_1, \cdots, x_m] \to M,$$

$$x_i \mapsto g_i,$$

and $\ker \Phi$ is a homogeneous ideal. As A is Noetherian, being the localisation of a Noetherian ring, so is $A[x_1, \cdots, x_m]$, hence $\ker \Phi$ is finitely generated, and we can choose homogeneous generators for it.

Definition 2.2.2. *Let Φ as above. The ideal of relations between the generators $g_1, \cdots, g_m$ is $I := \ker \Phi$. If $\{r_1, \cdots, r_s\}$ is a set of homogeneous generators of I, and $d := \max\{\deg r_i : 1 \leq i \leq s\}$, we say that I is generated in degree d, or equivalently, that M is related in degree d (always with respect to the generators chosen).*

For what follows, let $A = \mathbb{Z}[\frac{1}{N}]$. We describe a way of checking whether a subset $S \subset M$ generates M, and whether a set of corresponding relations R generates the ideal of relations, by checking generation for the corresponding reductions modulo primes p.

Proposition 2.2.3. *Let $S = \{g_1, \cdots, g_m\}$ be a set of homogeneous elements of M, $A[x_1, \cdots, x_m]$ the weighted algebra of polynomials with coefficients in A where $\deg x_i = wt(g_i)$:*

$$\Phi : A[x_1, \cdots, x_m] \to M$$

the map of graded A-algebras defined by $x_i \mapsto g_i$, and $I = \ker \Phi$. For each prime $p \nmid N$, let $\Phi_p : \mathbb{F}_p[x_1, \cdots, x_m] \to M \otimes \mathbb{F}_p$ the induced map of graded $\mathbb{F}_p$ algebras sending x_i to $\overline{g}_i$, the reduction modulo p of g_i, and $I_p = \ker \Phi_p$. Let $R = \{R_1, \cdots, R_s\} \subset I$ be a set of relations between the elements of S.

1. *If Φ_p is surjective for each prime $p \nmid N$, then so is Φ.*

2. *If for each prime $p \nmid N$, the reductions mod p of the elements of R generate I_p, then R generates I.*

To prove Proposition 2.2.3, we need the following lemma.

Lemma 2.2.4. *Let N and d be positive integers, V a $\mathbb{Q}$ vector space, and $v_1, \cdots, v_d \in V$. Let $v \in span_{\mathbb{Q}}\{v_1, \cdots, v_d\}$. For a prime p, let $V_p = V \otimes_{\mathbb{Q}} \mathbb{Q}_p$. If for each prime $p \nmid N$ we have $v \in span_{\mathbb{Z}_p}\{v_1, \cdots, v_d\} \subseteq V_p$, then $v \in span_{\mathbb{Z}[1/N]}\{v_1, \cdots, v_d\}$.*

Proof. Let $L = \text{span}_{\mathbb{Z}}\{v_1, \cdots, v_d\}$. The lattice L is a finitely generated $\mathbb{Z}$-module inside a $\mathbb{Q}$-vector space, so it is free, and has a $\mathbb{Z}$-basis $\{w_1, \cdots, w_e\}$ for some $e \le d$. The vectors $w_1, \cdots, w_e$ are $\mathbb{Q}$-linearly independent, thus can be extended to a $\mathbb{Q}$-basis $\{w_1, \cdots, w_e, \cdots, w_t\}$ of V. Thus we can write $v = \sum_{i=1}^{e} a_i w_i$, for some $a_i \in \mathbb{Q}$ (as $a_i = 0$ for $i > e$).
Note that for each prime p, we have $\text{span}_{\mathbb{Z}_p}\{w_1, \cdots, w_e\} = \text{span}_{\mathbb{Z}_p}\{v_1, \cdots, v_d\}$. Thus we have by the assumption that, for each prime $p \nmid N$, $v \in \text{span}_{\mathbb{Z}_p}\{w_1, \cdots, w_e\}$. Since $\{w_1, \cdots, w_t\}$ are also linearly independent in $\mathbb{Q}_p$, this means that $a_i \in \mathbb{Q} \cap \bigcap_{p \nmid N} \mathbb{Z}_p = \mathbb{Z}[1/N]$. As each v_i is a $\mathbb{Z}$-linear combination of the vectors $\{w_1, \cdots, w_e\}$, the statement is proven. □

Proof of Proposition 2.2.3.

1. Assume that Φ_p is surjective for each prime $p \nmid N$. Let $f_0 \in M_k$. Let $p \nmid N$ be a prime. By our assumption, there exists a homogeneous polynomial $P_0 \in A[x_1, \cdots, x_m]$ of degree k such that $f_0 \equiv \Phi(P_0) \pmod{p}$, that is, there exists some $f_1 \in M_k$ such that $f_0 - \Phi(P_0) = pf_1$. Similarly, there exists a homogeneous polynomial $P_1 \in A[x_1, \cdots, x_m]$ of degree k such that $f_1 \equiv \Phi(P_1)$ (mod p), that is, there exists some $f_2 \in M_k$ such that $f_1 - \Phi(P_1) = pf_2$. Continuing in this manner, we find that there exists a homogeneous polynomial $P \in \mathbb{Z}_p[x_1, \cdots, x_m]$ of degree k such that $f_0 = P(g_1, \cdots, g_m)$. That means that $f_0 \in \text{span}_{\mathbb{Z}_p}\{e_1, \cdots, e_t\}$, where $e_1, \cdots, e_t$ are the monomials in $g_1, \cdots, g_m$ that have weight k. Since this holds for each prime $p \nmid N$, it follows by Lemma 2.2.4 that $f_0 \in \text{span}_{\mathbb{Z}[1/N]}\{e_1, \cdots, e_t\}$, as we wanted to show.

2. Assume that S generates M, and that for each prime $p \nmid N$, the reductions mod p of $R_1, \cdots, R_s$ generate I_p, the ideal of relations between the elements of S_p. Let B_0 be a relation of degree k. By assumption, there exist polynomials $F_1^{(0)}, \cdots, F_s^{(0)} \in A[x_1, \cdots, x_m]$ such that:

$$B_0 \equiv \sum_{i=1}^{s} F_i^{(0)} R_i \pmod{p},$$

that is, there exists some $B_1 \in A[x_1, \cdots, x_m]$ such that:

$$B_0 - \sum_{i=1}^{s} F_i^{(0)} R_i = pB_1.$$

Apply the map Φ to this equality. As B_0 is a relation and each R_i is a relation, we find that $p\Phi(B_1) = 0$, hence B_1 is again a relation of degree k. Repeating the process, we find that:

$$B_1 - \sum_{i=1}^{s} F_i^{(1)} R_i = pB_2$$

for some $B_2, F_1^{(1)}, \cdots, F_s^{(1)} \in A[x_1, \cdots, x_m]$. Iterating this, we find that:

$$B_0 = \sum_{i=1}^{s} F_{i,p} R_i$$

where $F_{i,p} \in \mathbb{Z}_p[x_1, \cdots, x_n]$. As this holds for each prime $p \nmid N$, we deduce by Lemma 2.2.4 that there exists $F_1, \cdots, F_s \in \mathbb{Z}[\frac{1}{N}][x_1, \cdots, x_m]$ such that:

$$B_0 = \sum_{i=1}^{s} F_i R_i,$$

finishing the proof.

□

2.3 The case of level 1

In this section, we study the structure of the graded $\mathbb{Z}$-algebra $M(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$. The results are classical and elementary, but we provide detailed proofs, as the strategy employed to study graded algebras of modular forms in this thesis follow more or less the same outline. The strategy will be as follows. For a congruence subgroup Γ and an integer $N \geq 1$, we study the structure of the algebra $M(\Gamma, \mathbb{Z}[\frac{1}{N}])$ by first studying, for each prime $p \nmid N$ the structure of the reduction $M(\Gamma, \mathbb{F}_p)$ of the algebra modulo p. We then deduce the structure of the algebra in characteristic 0, by applying Proposition 2.2.3.

In the case of $M(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$, we can determine a set of generators by exploiting the existence of a modular form, namely Δ, which has the following properties (Proposition 1.2.7 and Lemma 1.2.8):

1. both Δ and Δ^{-1} have q-expansions with integer coefficients, and
2. Δ vanishes only at the cusp ∞.

Such an argument can be seen as motivating Scholl's work, which will be discussed later. Modular forms satisfying similar properties to Δ will be integral to that discussion.

Proposition 2.3.1. *Let k be an even positive integer. Then $M(SL_2(\mathbb{Z}), \mathbb{Z})$ is generated by E_4, E_6 and Δ, and $M_k(SL_2(\mathbb{Z}), \mathbb{Z})$ has a basis of the form:*

1. $\{E_4^a \Delta^b : 4a + 12b = k\}$ *if* $k \equiv 0 \pmod 4$, *and*

2. $\{E_6 E_4^a \Delta^b : 6 + 4a + 12b = k\}$ *if* $k \equiv 2 \pmod 4$.

Proof. We proceed by induction. First, note that for $k \in \{4, 6, 8, 10\}$, we have by Proposition 1.2.11:

$$\dim M_k(\mathrm{SL}_2(\mathbb{Z})) = 1.$$

Since $a_0(E_k) = 1$, we deduce that:

$$M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}) = \mathbb{Z}E_k,$$

and this implies that $E_8 = E_4^2$ and $E_{10} = E_4 E_6$, so the statement holds true for these values of k. Now let $k \geq 12$, and suppose that $f \in M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$. If $k \equiv 0 \pmod 4$, then we can choose a such that $4a = k$, in which case we define $g := f - a_0(f)E_4^a$. If $k \equiv 2 \pmod 4$, then $k - 6 \equiv 0 \pmod 4$, so we can choose a such that $6 + 4a = k$, in which chase we define $g := f - a_0(f)E_6E_4^a$. Having chosen g, we look at its q-expansion, noting that $a_0(g) = 0$. By Proposition 1.2.7, Δ vanishes simply at ∞, hence the quotient $\frac{g}{\Delta}$ is a modular form of weight $k-12$, and by Lemma 1.2.8, Δ^{-1} has coefficients in $\mathbb{Z}$, hence $\frac{g}{\Delta} \in M_{k-12}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$. By applying the induction hypothesis, we can conclude that $M(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ is generated by E_4, E_6, and Δ.

Consider the modular forms:

$$\{E_6^\epsilon E_4^a \Delta^b : 4a + 12b = k\}$$

where $\epsilon = 0$ if $k \equiv 0 \pmod 4$, and $\epsilon = 1$ if $k \equiv 2 \pmod 4$. Looking at q-expansions, we see that $E_6^\epsilon E_4^a \Delta^b = q^b + O(q^{b+1})$. Thus it is easily seen that these modular forms are linearly independent, hence form a basis of $M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$.

□

We now proceed to determining the structure of the reductions of $M(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ modulo a prime p.

Proposition 2.3.2. *Let p be a prime, and let $\overline{E}_4, \overline{E}_6$, and $\overline{\Delta}$ be the reductions modulo p of E_4, E_6, and Δ. The $\mathbb{F}_p$ algebra of modular forms of level 1 modulo p is given by:*

$$M(SL_2(\mathbb{Z}), \mathbb{F}_p) = \mathbb{F}_p[\overline{E}_4, \overline{E}_6, \overline{\Delta}]/(\overline{E}_4^3 - \overline{E}_6^2 - 1728\overline{\Delta}).$$

Proof. By Proposition 2.3.1, $M(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_p)$ is generated by $\overline{E}_4$, $\overline{E}_6$, and $\overline{\Delta}$. In fact, it can be seen that the space $M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ has a basis $\{f_0, \cdots, f_{d-1}\}$ where $f_i = q^i + O(q^{i+1})$ and $d = \dim M_k(\mathrm{SL}_2(\mathbb{Z}))$. The reduction modulo p of the elements of this basis is still linearly independent and spanning, hence a basis, so

$$\dim_{\mathbb{F}_p} M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_p) = \dim M(\mathrm{SL}_2(\mathbb{Z})).$$

We only need to determine the ideal of relations. Let $k \geq 12$. Consider the weighted polynomial algebra $A = \mathbb{F}_p[x, y, z]$ where x, y, and z are respectively given weights 4, 6, and 12. Denote by A_k the set of polynomials in A of degree k. We determine the dimension of A_k over $\mathbb{F}_p$. A simple counting argument shows that, if c is an integer, and $0 \leq c \leq \lfloor \frac{k}{12} \rfloor$, then:

$$|\{(a,b) \in \mathbb{Z}^2 : a, b \geq 0, 4a + 6b + 12c = k\}| = \begin{cases} \lfloor \frac{k}{12} \rfloor - c & k \equiv 2 \pmod{12} \\ 1 + \lfloor \frac{k}{12} \rfloor - c & \text{otherwise} \end{cases}$$

$$= \dim M_k(\mathrm{SL}_2(\mathbb{Z})) - c = \dim_{\mathbb{F}_p} M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_p) - c.$$

Thus, letting $d = \dim_{\mathbb{F}_p} M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_p)$:

$$\dim_{\mathbb{F}_p} A_k = \sum_{c=0}^{d-1} (d - c) = \frac{1}{2} d(d+1).$$

Let:

$$\Phi : A \to M(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_p)$$

be the map defined by:

$$x \mapsto \overline{E}_4,$$
$$y \mapsto \overline{E}_6,$$
$$z \mapsto \overline{\Delta}.$$

Then we have a short exact sequence:

$$0 \to I \to A \xrightarrow{\Phi} M(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_p) \to 0.$$

Thus for every non-negative k, we have a short exact sequence:

$$0 \to I_k \to A_k \xrightarrow{\Phi} M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_p) \to 0$$

where $I_k = I \cap A_k$. Hence:

$$\dim_{\mathbb{F}_p} I_k = \dim_{\mathbb{F}_p} A_k - \dim_{\mathbb{F}_p} M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}) = \frac{1}{2} d(d-1).$$

Now consider the map:

$$\eta : A_{k-12} \to I_k$$

$$F \mapsto (x^3 - y^2 - 1728z)F.$$

The map η is injective, and the dimension of its image is equal to $\dim_{\mathbb{F}_p} A_{k-12} = \frac{1}{2}d(d-1)$ since $\dim M_{k-12}(\mathrm{SL}_2(\mathbb{Z})) = \dim M_k - 1$ by Proposition 1.2.11. Therefore η is also surjective, and the ideal I of relations is principal, generated by $x^3 - y^2 - 1728z$.

□

Using our knowledge of the structures of the mod p algebras, we now determine the ideal of relations.

Theorem 2.3.3. *The $\mathbb{Z}$-algebra of modular forms of level 1 is given by:*

$$M(SL_2(\mathbb{Z}), \mathbb{Z}) = \mathbb{Z}[E_4, E_6, \Delta]/(E_4^3 - E_6^2 - 1728\Delta).$$

Proof. This follows from Proposition 2.3.2 by an application of Proposition 2.2.3.

□

Note that once we have determined the structure of the algebra of modular forms with coefficients in $\mathbb{Z}[\frac{1}{N}]$ for some N, we automatically get the structure of the algebra of modular forms with coefficients in $\mathbb{Q}$ and in $\mathbb{C}$, by virtue of Proposition 1.2.10. Thus, recalling that $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$, we have the following corollary:

Corollary 2.3.4. *The $\mathbb{C}$-algebra of modular forms of level 1 is given by:*

$$M(SL_2(\mathbb{Z})) = \mathbb{C}[E_4, E_6].$$

Chapter 3

The algebras $M(\Gamma_1(N), R)$

In this chapter, we study the algebras $M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$, and bounds on the generating weight as well as on the degrees of generators of the ideal of relations are determined. The contents of this chapter are taking from the articles [Rus14b] and [Rus14a].

3.1 Modular curves and moduli spaces

3.1.1 Modular curves over $\mathbb{C}$

Here we will take a look at modular curves defined as quotients of the upper-half plane, and at their moduli interpretation. This will follow Chapter 1 of [DS05].

In Section 1.1, we defined the left action of a congruence subgroup Γ on the upper half plane $\mathcal{H}$. The modular curve $Y(\Gamma)$ associated to Γ is the quotient space of orbits of $\mathcal{H}$ under the action of Γ, that is:

$$Y(\Gamma) := \Gamma \setminus \mathcal{H} = \{\Gamma \cdot z : z \in \mathcal{H}\}.$$

The modular curve $Y(\Gamma)$ can naturally be given a topology and a structure of a Riemann surface (with special care taken around elliptic points). We write:

$$Y_0(N) := Y(\Gamma_0(N)),$$

$$Y_1(N) := Y(\Gamma_1(N)).$$

The Riemann surface $Y(\Gamma)$ is not compact, but it can be compactified by adding to it a finite set of points consisting of the cusps of Γ (with special care taken around irregular cusps). The compactified modular curve is denoted by $X(\Gamma)$. We write:

$$X_0(N) := X(\Gamma_0(N)),$$
$$X_1(N) := X(\Gamma_1(N)).$$

Modular curves can be interpreted as moduli spaces classifying isomorphism classes of elliptic curves with certain marked structures, in the following sense. Let

$$S_{\Gamma_0(N)} = \{(E, C)\}$$

be the set of pairs (E, C) where E is an elliptic curve (over $\mathbb{C}$) and C is a subgroup of E of order N. Define an equivalence relation $\sim$ on $S_{\Gamma_0(N)}$ by: $(E, C) \sim (E', C')$ if and only if there exists an isomorphism $\varphi : E \xrightarrow{\cong} E'$ such that $\varphi(C) = C'$. Then there exists a bijection:

$$S_{\Gamma_0(N)}/\sim \longleftrightarrow Y_0(N).$$

Similarly, let $S_{\Gamma_1(N)} = \{(E, P)\}$ be the set of pairs (E, P) where E is an elliptic curve (over $\mathbb{C}$) and P is a point of E of exact order N. Define an equivalence relation $\sim$ on $S_{\Gamma_1(N)}$ by: $(E, P) \sim (E', P')$ if and only if there exists an isomorphism $\varphi : E \xrightarrow{\cong} E'$ such that $\varphi(P) = P'$. Then there exists a bijection:

$$S_{\Gamma_1(N)}/\sim \longleftrightarrow Y_1(N).$$

We would like to extend this moduli interpretation of the curves $Y_0(N)$ and $Y_1(N)$ in two ways. First, we would like a moduli interpretation for the compactifications $X_0(N)$ and $X_1(N)$, that is to say, we would like moduli interpretations of the cusps compatible with those of $Y_0(N)$ and $Y_1(N)$. Second, we would like a moduli interpretation that also classifies elliptic curves over fields other than $\mathbb{C}$, allowing even fields of positive characteristics, or even arbitrary commutative rings. This is achieved by the approach of moduli problems.

3.1.2 The moduli problem $\mathcal{P}_{\Gamma_1(N)}$

The exposition in this section follows [Gro90]. In this thesis, a smooth curve will always be a scheme whose structure morphism is smooth, separated, of finite presentation, and of relative dimension 1.

Let S be an arbitrary scheme. By an elliptic curve E/S, we mean a proper smooth curve $\pi : E \to S$, whose geometric fibres are connected curves of genus 1, together with a section $0 : S \to E$.

$$\begin{tikzcd} E \arrow[d, "\pi"'] \\ S \arrow[u, bend right, "0"'] \end{tikzcd}$$

Given an elliptic curve $\pi : E \to S$, there exists a sheaf on S given by:

$$\omega_E = \pi_* \Omega^1_{E/S}$$

and whose formation commutes with base change. One can show that in fact:

$$\omega_E \cong 0^* \Omega^1_{E/S}$$

and hence ω_E is an invertible sheaf. By a generalised elliptic curve, we mean a family of genus 1 curves whose fibres are either elliptic curves, or Néron polygons, together with a morphism $+ : E^{reg} \times_S E \to E$ whose restriction to E^{reg} makes E^{reg} into a commutative group scheme on E, and that on the fibres E_s with singular points, the translations by E_s^{reg} act by rotations on the graph of irreducible components. For a generalised elliptic curve E/S, we can define the invertible sheaf ω_E on S as the dual of the sheaf of Lie algebras $Lie(E^{reg})$.

Let E/S be an elliptic curve. A $\Gamma_1(N)$-structure on E/S, also called a "point of exact order N" in $E(S)$, is an isomorphism:

$$\alpha : \mathbb{Z}/N\mathbb{Z} \xrightarrow{\cong} E[N](S).$$

The point $P = \alpha(1)$ is the corresponding point of exact order N.

Definition 3.1.1. *The moduli problem $\mathcal{P}_{\Gamma_1(N)}$ is the contravariant functor:*

$$\mathcal{P}_{\Gamma_1(N)} : SCH/\mathbb{Z}[\frac{1}{N}] \to SETS$$

from the category of $\mathbb{Z}[\frac{1}{N}]$-schemes to that of sets which assigns to each such scheme S the set of isomorphism classes $[E, \alpha]$ consisting of a generalised elliptic curve E/S and a $\Gamma_1(N)$-structure α on E/S.

Recall that a functor $\mathcal{P} : SCH \to SETS$ is said to be representable if there exists a scheme X such that $\mathcal{P}$ is naturally isomorphic to the functor of points $\mathrm{Hom}(-, X)$. A necessary condition for a moduli functor to be representable is that the objects it is classifying do not possess any non-trivial automorphisms (see [Har10], Exercise 23.2). The key theorem here is the following ([Gro90]):

Theorem 3.1.2. *Let $N \geq 5$. Then $\mathcal{P}_{\Gamma_1(N)}$ is representable by a smooth, proper, and geometrically connected algebraic curve $X_1(N)$ over Spec$(\mathbb{Z}[\frac{1}{N}])$, called the fine moduli scheme, or the modular curve.*

Remark 3.1.3. *One might consider instead the moduli functor $\mathcal{P}$ classifying only (smooth) elliptic curves with $\Gamma_1(N)$-structure. It turns out that for $N \geq 4$, this functor is representable by an affine scheme $Y_1(N)$, which can be thought of as a subscheme of $X_1(N)$. Thus $X_1(N)$ can be seen as the compactification of $Y_1(N)$, obtained by adding the cusps, which correspond to generalised elliptic curves. See [DI95], Section 9.*

3.2 Geometric modular forms

Let $N \geq 5$, and let $X_1(N)$ be the modular curve. Let $\pi : \mathcal{E}_1(N) \to X_1(N)$ be the elliptic curve corresponding to the identity in $\mathrm{Hom}(X, X)$. Then $\mathcal{E}_1(N)$ is the universal elliptic curve over $X_1(N)$, as every elliptic curve $E/S/\mathbb{Z}[\frac{1}{N}]$ is the pullback of $\pi : \mathcal{E}_1(N) \to X_1(N)$ in a unique way. Let $\omega = \pi_* \Omega_{\mathcal{E}_1(N)/X_1(N)}$ be the invertible sheaf on $X_1(N)$ as defined in Section 3.1.2. For a $\mathbb{Z}[\frac{1}{N}]$-algebra R, we write $X_1(N)_R$ for the moduli scheme obtained from $X_1(N)$ through base change, and we write ω_R for the corresponding sheaf.

Forgetting for a moment the definition of modular forms presented in Section 1.2, let us make the following definition, again following [Gro90].

Definition 3.2.1. *Let $N \geq 5$, and R a $\mathbb{Z}[\frac{1}{N}]$-algebra. A (holomorphic) modular form for $\Gamma_1(N)$, defined over R and of weight k is a global section of the invertible sheaf $\omega_R^{\otimes k}$. We write:*

$$M_k(\Gamma_1(N), R) = H^0(X_1(N)_R, \omega_R^{\otimes k})$$

for the R-algebra of modular forms over R, with level N and weight k. These modular forms generate a graded ring:

$$M(\Gamma_1(N), R) := \bigoplus_{k=0}^{\infty} M_k(\Gamma_1(N), R).$$

We can check that for a $\mathbb{Z}[\frac{1}{N}]$-subalgebra R of $\mathbb{C}$, we recover the classical definition of modular forms with coefficients in R as defined in Section 1.2. For that, we need first to define the q-expansion of a modular form algebraically. This can be done using the Tate curve, which is a generalised elliptic curve $E_{Tate} = \mathbb{G}_m/q^{\mathbb{Z}}$ over $\mathbb{Z}[[q]]$. This curve has a canonical differential dt/t and a natural embedding* $Id_N : \mu_N \to E_{Tate}[N]$ over $\mathbb{Z}[\frac{1}{N}][[q]]$. The Fourier expansion of f is then defined to be $f(q)$ in the following identity:

$$f(\mathbb{G}_m/q^{\mathbb{Z}}, Id_N) = f(q)(dt/t)^{\otimes k}.$$

There is a unique morphism $\mathrm{Spec}(\mathbb{Z}[\frac{1}{N}][[q]]) \to X_1(N)$ by means of which the Tate curve arises as the pull-back of the universal curve $\mathcal{E}_1/X_1(N)$. The image of the prime ideal where $q = 0$ defines the section ∞ of $X_1(N)$ and q is a uniformising parameter. Thus the Fourier expansion of f is the holomorphic section f of $\omega^{\otimes k}$ near ∞.

When $R = \mathbb{C}$, it is proven in [DR73], VII.4, that $f(q)$ will be the q-expansion of f at ∞ in the classical sense. We also have the following theorem (cf [DI95], Theorem 12.3.4):

*This makes it a generalised elliptic curve with a $\Gamma_1(N)$-structure in the sense defined above, over a base that contains μ_N, once one chooses (non-canonically) a generator of μ_N. The inclusion of a Nth root of unity at this stage can be dealt away with Theorem 3.2.2.

Theorem 3.2.2 (q-expansion principle)**.** *Let R be a $\mathbb{Z}[\frac{1}{N}]$-algebra.*

1. *The map $H^0(X_1(N)_R, \omega_R^{\otimes k}) \to R[[q]]$ taking f to $f(q)$ is an injection of R-modules.*

2. *if R_0 is a $\mathbb{Z}[\frac{1}{N}]$-subalgebra of R, the modular form f is defined over R_0 if and only if $f(q) \in R_0[[q]]$.*

Applying this theorem with $R = \mathbb{C}$, we see that for subrings R_0 of $\mathbb{C}$ (in which N is invertible), we recover the classical notion of modular forms whose q-expansion has coefficients in R_0.
In order to deal with modular forms in positive characteristic, we need the following base change theorem ([DI95], Theorem 12.3.2):

Theorem 3.2.3 (Base change)**.** *If B is an A-algebra and either one of the following holds:*

1. *B is flat over A, or*

2. *$k > 1$ and N is invertible in B,*

then the natural map:

$$M_k(\Gamma_1(N), A) \otimes_A B \to M_k(\Gamma_1(N), B)$$

is an isomorphism.

In particular, we find that, when $p \nmid N$ and $k \geq 2$, we have $M_k(\Gamma_1(N), \mathbb{F}_p) = M_k(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}]) \otimes_{\mathbb{Z}[\frac{1}{N}]} \mathbb{F}_p$.

3.3 Mumford's theorems

We will repeatedly make use of the following results due to Mumford ([Mum70b]). Let X be a be a smooth, geometrically connected algebraic curve of genus g over a perfect field k. Let $\mathcal{L}$, $\mathcal{M}$, and $\mathcal{N}$ be three invertible sheaves on X. We have the following exact sequence:

$$0 \to R(\mathcal{L}, \mathcal{M}) \to H^0(X, \mathcal{L}) \otimes H^0(X, \mathcal{M}) \xrightarrow{\mu} H^0(X, \mathcal{L} \otimes \mathcal{M}) \to S(\mathcal{L}, \mathcal{M}) \to 0$$

where μ is the natural multiplication map: $\sum f_i \otimes g_i \mapsto \sum f_i g_i$, $R(\mathcal{L}, \mathcal{M})$ and $S(\mathcal{L}, \mathcal{M})$ are respectively its kernel and cokernel.

Theorem 3.3.1. *Let $\mathcal{L}$, $\mathcal{M}$, and $\mathcal{N}$ be as above.*

1. *If $\deg \mathcal{L} \geq 2g + 1$ and $\deg \mathcal{M} \geq 2g$, then μ is surjective.*

2. The natural map:

$$R(\mathcal{L}, \mathcal{M}) \otimes H^0(X, \mathcal{N}) \to R(\mathcal{L} \otimes \mathcal{N}, \mathcal{M})$$

mapping $(\sum f_i \otimes g_i) \otimes h \mapsto \sum (f_i h) \otimes g_i$ *is surjective if* $\deg \mathcal{L} \geq 3g + 1$*, and* $\min\{\deg \mathcal{M}, \deg \mathcal{N}\} \geq 2g + 2$*.*

3.4 Generators and relations for $M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$

In this section we fix $N \geq 5$, and we determine the generating weight for $M = M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$, and the degree in which M is related. We will do this first for the mod p reductions $M \otimes \mathbb{F}_p$ of M, and then use Proposition 2.2.3 to establish the bounds for M.

Let $p \nmid N$, and let $X_1(N)_{\mathbb{F}_p} = X_1(N) \otimes \mathbb{F}_p$ denote the reduction modulo p of the modular curve $X_1(N)/\mathbb{Z}[\frac{1}{N}]$. By Igusa's theorem ([DS05], Theorem 8.6.1), the base change to $\mathbb{F}_p$ corresponds to good reduction. Hence the genus of $X_1(N)_{\overline{\mathbb{F}}_p}$ (which is equal to the genus of $X_1(N)_{\mathbb{F}_p}$) is equal to g, the genus of the modular curve $X_1(N)_{\mathbb{C}}$ (since the latter is equal to the genus of $X_1(N)_{\mathbb{Q}}$ by flatness of base change). Let ω be the invertible sheaf defined at the beginning of Section 3.2, and let $\omega_{\mathbb{F}_p}$ be its pullback to $X_1(N)_{\mathbb{F}_p}$. First, we will calculate the degree of $\omega_{\mathbb{F}_p}$. We remark that one can calculate this degree in characteristic 0, and then use good base change theorems to show that the degree in characteristic p is the same. However, we will present a counting argument, which uses the existence of a special modular form in characteristic p, called the Hasse invariant.

Lemma 3.4.1. *For the invertible sheaf* $\omega_{\mathbb{F}_p}$ *on* $X_1(N)_{\mathbb{F}_p}$*, we have:*

$$\deg \omega_{\mathbb{F}_p} = \frac{1}{24}[SL_2(\mathbb{Z}) : \Gamma_1(N)].$$

Proof. Since base change along a field extension preserves the degree of an invertible sheaf ([Liu02], Proposition 7.3.7), it is enough to calculate the degree $\deg \omega_{\overline{\mathbb{F}}_p}$ on $X_1(N)_{\overline{\mathbb{F}}_p}$. The invertible sheaf $\omega_{\overline{\mathbb{F}}_p}^{\otimes(p-1)}$ contains a special global section, which is the Hasse invariant A. It has zeroes precisely at the points of $X_1(N)_{\overline{\mathbb{F}}_p}$ corresponding to isomorphism classes $[E, \alpha]$ where $E/\overline{\mathbb{F}}_p$ is a supersingular elliptic curve, and these zeroes are simple. Thus we need to count the number of points on $E/\overline{\mathbb{F}}_p$ corresponding to supersingular elliptic curves.

For an elliptic curve $E/\overline{\mathbb{F}}_p$, let $\mathcal{P}_1(E)$ be the set of points of exact order N on E. Since $E[n]$ has order n^2, by inclusion-exclusion we get that:

$$|\mathcal{P}_1(E)| = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right) = [SL_2(\mathbb{Z}) : \Gamma_1(N)].$$

Let $r = |\mathcal{P}_1(E)|$ and $P_1, \cdots, P_r$ be the points of exact order N on E. We want to count the number of distinct isomorphism classes in the set $\mathcal{P} = \{[E, P_1], \cdots, [E, P_r]\}$. The group $\operatorname{Aut}(E)$ acts on $\mathcal{P}$, and by representability of the moduli functor, this action is free. Thus the number of orbits is $|\mathcal{P}_1(E)|/|\operatorname{Aut}(E)|$. Summing over supersingular curves, we get:

$$\deg(\underline{\omega}_{\overline{\mathbb{F}}_p}) = \frac{[SL_2(\mathbb{Z}) : \Gamma_1(N)]}{p-1} \sum_{E \text{ supersingular}} \frac{1}{|\operatorname{Aut}(E)|} = \frac{1}{24}[SL_2(\mathbb{Z}) : \Gamma_1(N)]$$

where for the last inequality we used the Eichler-Deuring mass formula ([Sil09], Exercise V.5.9):

$$\sum_{E/\overline{\mathbb{F}}_p \text{ supersingular}} \frac{1}{|\operatorname{Aut}(E)|} = \frac{p-1}{24}.$$

□

Proposition 3.4.2. *Let $N \geq 5$, and let $p \nmid N$. Then the $\mathbb{F}_p$-algebra $M(\Gamma_1(N), \mathbb{F}_p)$ is generated in weight 3.*

Proof. We proceed as in the start of the proof of Theorem 5.1 in [KM12]. By Lemma 3.4.1, we have:

$$\deg(\omega_{\overline{\mathbb{F}}_p}) = \frac{1}{24}[SL_2(\mathbb{Z}) : \Gamma_1(N)].$$

On the other hand, as argued at the top of this section, the genus g of $X_1(N)_{\mathbb{F}_p}$ is equal to the genus of $X_1(N)_{\mathbb{C}}$. By Theorem 3.1.1 and Section 3.9 of [DS05], we find that:

$$g = 1 + \frac{1}{24}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] - \frac{\epsilon_\infty}{2},$$

where ϵ_∞ is the number of cusps for $\Gamma_1(N)$, and so:

$$\deg(\omega_{\mathbb{F}_p}) = g - 1 + \frac{\epsilon_\infty}{2}.$$

Additionally, By Lemma 1.1.2, we see that $\epsilon_\infty \geq 4$. Hence:

$$\deg(\omega_{\mathbb{F}_p}^{\otimes 2}) \geq 2g + 2.$$

Now let $k \geq 4$ be a positive integer. By Theorem 3.3.1, the canonical multiplication map:

$$H^0(X_1(N)_{\mathbb{F}_p}, \omega_{\mathbb{F}_p}^{\otimes 2}) \otimes H^0(X_1(N)_{\mathbb{F}_p}, \omega_{\mathbb{F}_p}^{\otimes (k-2)}) \to H^0(X_1(N)_{\mathbb{F}_p}, \omega_{\mathbb{F}_p}^{\otimes k})$$

is surjective. Therefore, the modular forms of weights 2 and 3 generate $M(\Gamma_1(N), \mathbb{F}_p)$.

□

Proposition 3.4.3. *Let $N \geq 5$, and let $p \nmid N$. Then the $\mathbb{F}_p$-algebra $M(\Gamma_1(N), \mathbb{F}_p)$ is related in degree 6 with respect to a minimal set of generators.*

Proof. Consider the graded $\mathbb{F}_p$-algebra $M = M(\Gamma_1(N), \mathbb{F}_p)$ and pick a minimal set of generators $\{g_1, \cdots, g_n\}$ for it. By Proposition 3.4.2, a minimal set of generators for $M(\Gamma_1(N), \mathbb{F}_p)$ consists of the union of a basis of $M_2(\Gamma_1(N), \mathbb{F}_p)$ and a basis of $M_3(\Gamma_1(N), \mathbb{F}_p)$. This provides us with a map of graded algebras:

$$\Phi : A \to M$$

$$x_i \mapsto g_i$$

where $A = \mathbb{F}_p[x_1, \cdots, x_n]$ is the polynomial algebra where each x_i is given the weight of g_i. We denote by A_k the $\mathbb{F}_p$-vector space spanned by degree k polynomials. We wish to examine generators of the homogeneous ideal $\ker \Phi$, which is the ideal of relations.

Clearly, there are no relations in degrees 2 or 3. Let $P \in A$ be a homogeneous polynomial of degree $k \geq 7$, representing a relation in M in weight $k \geq 7$. Let $a = 5$ if $k = 7$, and $a = 6$ otherwise. The polynomial P is the sum of homogeneous monomials, each of degree k. Since $k \geq 7$, each of these monomials is divisible by a monomial of degree a. Let $\{v_1, \cdots, v_n\}$ be a basis of A_{k-a}. Thus we can write:

$$P = \sum_{i=1}^{n} Q_i v_i$$

where for all i, Q_i is a homogeneous polynomial of degree a.

For some m, and possibly after a reordering of the v_i's, the set $\{\Phi(v_1), \cdots, \Phi(v_m)\}$ is a basis of M_{k-a}. This means that for every j such that $m+1 \leq j \leq n$ there are constants $\alpha_{1,j}, \cdots, \alpha_{m,j}$ such that:

$$\Phi(v_j) = \sum_{i=1}^{m} \alpha_{i,j} \Phi(v_i).$$

Hence letting

$$G_j := v_j - \sum_{i=1}^{m} \alpha_{i,j} v_i$$

for $m+1 \leq j \leq n$, we have $\Phi(G_j) = 0$, i.e., the G_j's are relations in weight $k - a$. Now if for $1 \leq i \leq m$ we set:

$$Q_i' := Q_i + \sum_{j=m+1}^{n} \alpha_{i,j} Q_j,$$

we can rewrite P as:

$$P = \sum_{i=1}^{m} Q_i' v_i + \sum_{j=m+1}^{n} G_j Q_j,$$

where, since $\Phi(P) = 0$ and $\Phi(\sum_{j=m+1}^{n} G_j Q_j) = 0$, we have $\Phi(\sum_{i=1}^{m} Q_i' v_i) = 0$. We see then that $\sum_{i=1}^{m} Q_i' v_i$ must be represented in $R(\mathcal{L}^{\otimes(k-a)}, \mathcal{L}^{\otimes a})$, that is:

$$\sum_{i=1}^{m} \Phi(Q_i') \otimes \Phi(v_i) \in R(\mathcal{L}^{\otimes(k-a)}, \mathcal{L}^{\otimes a}).$$

We have then the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & R(\mathcal{L}^{\otimes a}, \mathcal{L}^{\otimes (k-a)}) \arrow[r] & H^0(X, \mathcal{L}^{\otimes a}) \otimes H^0(X, \mathcal{L}^{\otimes (k-a)}) \arrow[r] & H^0(X, \mathcal{L}^{\otimes k}) \\
& R(\mathcal{L}^{\otimes 3}, \mathcal{L}^{\otimes (k-a)}) \otimes H^0(X, \mathcal{L}^{\otimes (a-3)}) \arrow[u, "\epsilon"] & &
\end{tikzcd}$$

By Theorem 3.3.1, the map ϵ is surjective. Thus for each i, we can find polynomials H_s in degree $3 - a + k \leq k - 2$, and polynomials $F_{i,s}$ in degree $a - 3$, satisfying:

$$\Phi(\sum_{i=1}^{m} F_{i,s} v_i) = 0$$

and such that:

$$\sum_{i=1}^{m} \Phi(\sum_{s} H_s F_{i,s}) \otimes \Phi(v_i) = \sum_{i=1}^{m} \Phi(Q'_i) \otimes \Phi(v_i),$$

so that:

$$\Phi(\sum_{s} H_s F_{i,s}) = \Phi(Q'_i),$$

hence

$$Q'_i = \sum_{s} H_s F_{i,s} + W_i$$

where for all i, $\Phi(W_i) = 0$, i.e. W_i is a relation in weight a. Putting all the above together, we get:

$$P = \sum_{i=1}^{m} (\sum_{s} H_s F_{i,s}) v_i + \sum_{i=1}^{m} W_i v_i + \sum_{j=m+1}^{n} G_j Q_j$$

so P can be written in terms of relations of degrees $k - (a - 3)$, a, and $k - a$, which are all $\leq k - 2$. □

We now have the following result:

Theorem 3.4.4. *Let $N \geq 5$. The $\mathbb{Z}[\frac{1}{N}]$-algebra $M = M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$ is generated in weight 3. Choosing a minimal set of generators, M is related in degree 6.*

Proof. This follows by combining Propositions 3.4.2 and 3.4.3 with Theorem 3.2.3 (base change), and then applying Proposition 2.2.3. □

Chapter 4

The algebras $M(\Gamma_0(N), R)$

In this chapter, we investigate the generating weight of the algebra $M(\Gamma_0(N), R_N)$, where $R_N := \mathbb{Z}[\frac{1}{6N\varphi(N)}]$, $N \geq 5$, and φ being the Euler totient function. Although the results in this chapter can be extended to modular forms with coefficients in $\mathbb{Z}[\frac{1}{6N}]$ by similar methods, we have chosen to restrict our attention to $\mathbb{Z}[\frac{1}{6N\varphi(N)}]$ for ease of exposition. The algebra $M(\Gamma_0(p), \mathbb{Z})$ is then examined, and a lower bound on the generating weight for these algebras is given, as well as a set of generators. The contents of this chapter are based on the articles [Rus14b] and [Rus14a], however, new and stronger results are presented.

4.1 Modular curves for $\Gamma_0(N)$

4.1.1 The moduli problem $\mathcal{P}_{\Gamma_0(N)}$

We refer to Section 3.1.2 for the definition of a generalised elliptic curve. Let E be a generalised elliptic curve over a scheme S. A $\Gamma_0(N)$-structure C on E is a cyclic group subscheme of order N of E^{reg} whose fibres over any geometric point s intersect all the irreducible components of the fibre of E over s.

Definition 4.1.1. *The moduli problem $\mathcal{P}_{\Gamma_0(N)}$ is the contravariant functor:*

$$\mathcal{P}_{\Gamma_0(N)} : SCH/R_N \to SETS$$

from the category of R_N-schemes to that of sets which assigns to each such scheme S the set of isomorphism classes $[E, C]$ consisting of a generalised elliptic curve E/S and a $\Gamma_0(N)$-structure C on E/S.

Unfortunately, the functor $\mathcal{P}_{\Gamma_0(N)}$ is never representable, since every pair (E, C) where E is an elliptic curve over a field k and C is a cyclic subgroup of order N

has a non-trivial automorphism:

$$\iota : E \to E$$

$$P \mapsto [-1]P$$

corresponding to the element $-1 \in \Gamma_0(N)$.

When $N = 1$, we can give another argument to show that this functor is not representable, taken from lecture notes by Bas Edixhoven. Suppose that it is representable by a scheme X. Let d be a positive integer which is not a square. Consider the elliptic curves[*]:

$$E : y^2 = x^3 + ax + b,$$

$$E' : dy^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Q}$. Then E and E' are not isomorphic over $\mathbb{Q}$, so they correspond to two distinct points in $X(\mathbb{Q})$. But E and E' are isomorphic over $\mathbb{Q}(\sqrt{d})$, so they correspond to a single point in $X(\mathbb{Q}(\sqrt{d}))$. Thus, the map $X(\mathbb{Q}) \to X(\mathbb{Q}(\sqrt{d}))$ is not injective. However, this map is injective for any scheme X.

Nonetheless, the functor $\mathcal{P}_{\Gamma_0(N)}$ is still well-behaved: it is representable by a stack, which is a category that behaves almost as a scheme. For more on moduli stacks of curves, see [Mum65], [DM69], and for stacks in general, [LMB00]. For the construction of the moduli stacks representing $\mathcal{P}_{\Gamma_0(N)}$, see [DR73] and [KM85].

4.1.2 Coarse moduli schemes revisited

If a moduli problem is not representable, we might still find a very good approximation for it. we call such an approximation a coarse moduli scheme ([DR73], Definition I.8.1). In what follows, let $\mathcal{X}_0(N)$ be the moduli stack representing the moduli problem $\mathcal{P}_{\Gamma_0(N)}$.

Definition 4.1.2. *Let SCH/S be the category of S-schemes, and*

$$\mathcal{P} : SCH/S \to SETS$$

be a moduli problem. A coarse moduli scheme for $\mathcal{P}$ is an S-scheme X, together with a natural transformation

$$\Phi : \mathcal{P} \to h_X$$

where $h_X = \mathrm{Hom}(-, X)$, such that:

[*] The curve E' obtained in this manner is said to be a “quadratic twist” of the curve E.

- *for every S-scheme Spec(k) with k an algebraically closed field, the map $\Phi(k) : \mathcal{P}(k) \to X(k)$ is bijective, and*
- *(X, Φ) is universal, in the sense that for every S-scheme Y and every morphism $\Psi : \mathcal{P} \to h_Y$, there is a unique morphism $f : X \to Y$ such that $\Psi = h_e \circ \Phi$, where $h_e : h_X \to h_Y$ is the induced natural transformation on the functors of points.*

The universality condition ensures that, if a coarse moduli scheme for a given moduli problem exists, then it must be unique. While a coarse moduli scheme classifies objects over algebraically closed fields, it does not do so in a continuous way, so it does not tell us much about where they sit in families (that is why a stack is needed). However, for our purposes, they are enough. Note that if $\mathcal{P}$ has a coarse moduli scheme X, and is representable by a scheme Y, then $X \cong Y$.

Let $\mathcal{P}_{\Gamma_0(N)}$ be the moduli problem from Definition 4.1.1. Then for any prime $p \notin R_N^\times$, one can naturally define the moduli problem $\mathcal{P}_{\Gamma_0(N)} \otimes \mathbb{F}_p$ (that is, by precomposing it with the functor $- \otimes \mathbb{F}_p : SCH/S \to SCH/\mathbb{F}_p$). We ask whether coarse moduli schemes exist for $\mathcal{P}_{\Gamma_0(N)}$ and $\mathcal{P}_{\Gamma_0(N)} \otimes \mathbb{F}_p$, and if so, how they are related.

Proposition 4.1.3. *The moduli problem $\mathcal{P}_{\Gamma_0(N)}$ admits a coarse moduli scheme, which we denote by $X_0(N)$. For any prime $p \notin R_N^\times$, the moduli problem :*

$$\mathcal{P}_{\Gamma_0(N)} \otimes \mathbb{F}_p$$

admits a coarse moduli scheme, which we denote by $X_0(N)_{\mathbb{F}_p}$. Moreover:

$$X_0(N)_{\mathbb{F}_p} = X_0(N) \otimes \mathbb{F}_p.$$

The schemes $X_0(N)$ and $X_0(N)_{\mathbb{F}_p}$ are all smooth, irreducible, and of the same genus.

Proof. For simplicity, we sketch a proof only for $N \geq 5$. By Theorem 3.1.2, the moduli problem $\mathcal{P}_{\Gamma_1(N)} \otimes R_N$ is representable by a scheme $X_1(N)$ over R_N, on which the group $G = \Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ acts naturally[†]. Define $X_0(N) := X_1(N)/G$ (for quotients of schemes by finite groups of automorphisms, see [Mum70a], §7). Then $X_0(N)$ can be shown to be the coarse moduli scheme of $\mathcal{P}_{\Gamma_0(N)}$ (see [DR73], I.8.2.2, and [KM85], §8.1). Since the order of G, which is $|G| = \varphi(N)$, is invertible in R_N, the formation of the coarse moduli scheme commutes with base change ([KM85], Proposition A7.1.3). For the last assertion, see [DR73], Corollaire IV.5.6. See also [Shi94], §7.4, and [Shi58], §9. □

[†] If $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ and (E, α) is a pair consisting of an elliptic curve E and a point α of exact order N, then the action of d sends (E, α) to $(E, d \cdot \alpha)$.

Remark 4.1.4. *The formation of the coarse moduli scheme does not in general commute with arbitrary base change, although it always commutes with flat base change. However, it commutes with arbitrary base change if the map from the moduli stack to the coarse moduli scheme is étale.*

Remark 4.1.5. *The construction can, of course, be carried out by taking appropriate quotients of any moduli problem "over" $\mathcal{P}_{\Gamma_0(N)}$ which is representable and satisfies certain finiteness conditions. It turns out that the formation of $X_0(N)$ is independent of the choice of the representable moduli problem.*

4.2 Modular forms for $\Gamma_0(N)$

Let $\mathcal{X}_0(N)$ be the moduli stack described above. Let $\pi : \mathcal{E} \to \mathcal{X}_0(N)$ be the universal elliptic curve. Then ([DR73], II.1.6) the relative dualising sheaf on $\mathcal{E}$ descends to an invertible sheaf ω on $\mathcal{X}_0(N)$. For an R_N-algebra R, write $\mathcal{X}_0(N)_R = \mathcal{X}_0(N) \otimes R$ and $\omega_R = \omega \otimes R$.

Once again, we forget for a moment the definition of modular forms presented in Section 1.2, and, following [DR73], VII.3.1, we make the following definition:

Definition 4.2.1. *Let R be an R_N-algebra. A (holomorphic) modular form for $\Gamma_0(N)$, defined over R and of weight k is a global section of the invertible sheaf $\omega_R^{\otimes k}$. We write:*

$$M_k(\Gamma_0(N), R) = H^0(\mathcal{X}_0(N) \otimes R, \omega_R^{\otimes k})$$

for the R-algebra of modular forms over R, with level N and weight k. These modular forms generate a graded ring:

$$M(\Gamma_0(N), R) := \bigoplus_{k=0}^{\infty} M_k(\Gamma_0(N), R).$$

The q-expansion of such a modular form is defined in the same way as in Section 3.2, again using the Tate curve, with its μ_N subgroup. We see then by [DR73], VII.4 that for R_N-subalgebras R_0 of $\mathbb{C}$, we recover the classical notion of modular forms. Indeed ([DR73], Théorème VII.3.9):

Theorem 4.2.2 (q-expansion principle)**.** *Let R be an R_N-algebra.*

1. *The map $M_k(\Gamma_0(N), R) \to R[[q]]$ taking f to $f(q)$ is an injection of R-modules.*

2. *if R_0 is an R_N-subalgebra of R, the modular form f is defined over R_0 if and only if $f(q) \in R_0[[q]]$.*

For positive characteristics, we have the following theorem ([Hid12], Corollary 3.1.3):

Theorem 4.2.3 (Base change)**.** *If R is an R_N-algebra, then the natural map:*

$$M_k(\Gamma_0(N), R_N) \otimes_{R_N} R \to M_k(\Gamma_0(N), R)$$

is an isomorphism.

4.3 Generators and relations for $M(\Gamma_0(N), R_N)$

In order to apply Theorem 3.3.1, we need to work over varieties.

Proposition 4.3.1. *There exists an invertible sheaf $\mathcal{L}_k$ on $X_0(N)$ such that:*

$$M_k(\Gamma_0(N), R_N) = H^0(X_0(N), \mathcal{L}_k).$$

For each prime $p \nmid 6N\varphi(N)$, we have:

$$M_k(\Gamma_0(N), \mathbb{F}_p) = H^0(X_0(N)_{\mathbb{F}_p}, \mathcal{L}_{k,p})$$

where $\mathcal{L}_{k,p} = \mathcal{L}_k \otimes \mathbb{F}_p$. Let ϵ_∞ be the number of cusps for $\Gamma_0(N)$, and let ϵ_2 and ϵ_3 be respectively the number of elliptic points of order 2 and of order 3. Let g be the genus of $X_0(N)$. Then:

$$\deg \mathcal{L}_k = \deg \mathcal{L}_{k,p} = k(g-1) + \lfloor \frac{k}{4} \rfloor \epsilon_2 + \lfloor \frac{k}{3} \rfloor \epsilon_3 + \frac{k}{2}\epsilon_\infty.$$

Proof. The scheme $X_0(N)$ is the coarse moduli scheme for $\mathcal{X}_0(N)$, so we have a map $\pi : \mathcal{X}_0(N) \to X_0(N)$. We can define $\mathcal{L}_k = \pi_*(\omega^{\otimes k})$. One can see that this construction is equivalent to the following one. As we have seen in Section 3.2, on the fine moduli scheme $X_1(N)_{R_N}$ we have an invertible sheaf ω_1, and the modular forms of weight k for $\Gamma_1(N)$ with coefficients in R_N are global sections of $\omega_1^{\otimes k}$. Moreover, ω_1 is a G-sheaf for $G = \Gamma_0(N)/\Gamma_1(N)$, which is the covering group of $\psi : X_1(N)_{R_N} \to X_0(N)$, meaning that G acts naturally on ω_1 in a manner compatible with its action on $X_1(N)_{R_N}$ over $X_0(N)$. We see then that $\mathcal{L}_k = \psi_*(\omega_1^{\otimes k})^G$, which is the G-invariant pushforward of $\omega_1^{\otimes k}$ (see [DI95], Section 12.1). Since the order of G is invertible on the base, it follows that $\mathcal{L}_k$ thus defined is an invertible sheaf, and its formation commutes with base change. The global sections of $\mathcal{L}_k$ are by definition those of $\omega^{\otimes k}$, and the global sections of $\mathcal{L}_{k,p}$ are those of $\omega_{\mathbb{F}_p}^{\otimes k}$. Finally, since the Euler characteristic of a coherent sheaf is locally constant, and $X_0(N)$ is irreducible (Proposition 4.1.3), it suffices to compute the degree at any closed point. The formula for the degree then follows from the degree formula over $\mathbb{C}$, given in [DI95], Section 12.1. See also [DS05], Section 3.5. □

Remark 4.3.2. *The coarse moduli schemes and the invertible sheaves of Proposition 4.3.1 are constructed in [Hid12] with no recourse to stacks.*

Proposition 4.3.3 (Projection formula)**.** *Let p be a prime number, $p \notin R_N^\times$. Let ϵ_∞ be the number of cusps for $\Gamma_0(N)$, and let ϵ_2 and ϵ_3 be respectively the number of elliptic points of order 2 and of order 3. Let r be as follows:*

$$r := \begin{cases} 2 & \textit{if } \epsilon_3 = \epsilon_2 = 0, \\ 4 & \textit{if } \epsilon_3 = 0 \textit{ and } \epsilon_2 > 0, \\ 6 & \textit{if } \epsilon_3 > 0 \textit{ and } \epsilon_2 = 0, \\ 12 & \textit{if } \epsilon_3 > 0 \textit{ and } \epsilon_2 > 0. \end{cases}$$

Then:

$$\mathcal{L}_{r+k,p} \cong \mathcal{L}_{r,p} \otimes \mathcal{L}_{k,p}.$$

Proof. Write $X_1 = X_1(N)_{\mathbb{F}_p}$, $X_0 = X_0(N)_{\mathbb{F}_p}$, and $\psi : X_1 \to X_0$ the covering map. Write ω_1 for the invertible sheaf on X_1. For each point $x \in X_1$, the stabiliser of x in the covering group G can be seen as a group of automorphisms of an elliptic curve in characteristic $p \geq 5$, and hence has order either 2, 4, or 6. The number r is precisely the least common multiple of the possible orders of these automorphism groups (see [Maz77], §II.2). It follows that G acts trivially on the fibre $\omega_1^{\otimes r} \otimes k(x)$. As the order of G is invertible on the base, $\omega_1^{\otimes r}$ descends to X_0, which means that $\omega_1^{\otimes r} = \psi^* \mathcal{L}_{r,p}$. Now we apply the projection formula ([Liu02], Proposition 5.2.32):

$$\begin{aligned} \mathcal{L}_{r+k,p} = \psi_*^G(\omega_1^{\otimes r} \otimes \omega_1^{\otimes k}) = \psi_*^G(\psi^* \mathcal{L}_{r,p} \otimes \omega_1^{\otimes k}) &= \mathcal{L}_{r,p} \otimes \psi_*^G(\omega_1^{\otimes k}) \\ &= \mathcal{L}_{r,p} \otimes \mathcal{L}_{k,p} \end{aligned}$$

and the statement is proven. □

Proposition 4.3.4. *Let $N \geq 5$, and $p \notin R_N^\times$ a prime number. Let ϵ_∞ be the number of cusps for $\Gamma_0(N)$, and let ϵ_2 and ϵ_3 be respectively the number of elliptic points of order 2 and of order 3. The algebra $M(\Gamma_0(N), \mathbb{F}_p)$ is generated:*

- *in weight 2, if $\epsilon_3 = \epsilon_2 = 0$ and N is composite,*
- *in weight 6, if $\epsilon_3 > 0$ and $\epsilon_2 = 0$,*
- *in weight 12, if $\epsilon_3 > 0$ and $\epsilon_2 > 0$, and*
- *in weight 4 otherwise.*

Proof. From the table of Lemma 1.1.2, we find that:

- if $\epsilon_2 = \epsilon_3 = 0$ and N is composite, then $\epsilon_\infty \geq 4$;
- if $\epsilon_2 = \epsilon_3 = 0$ and N is prime, then $\epsilon_\infty = 2$ and $g \geq 1$;
- if $\epsilon_3 = 0$ and $\epsilon_2 > 0$, then $\epsilon_2 \geq 2$ and $\epsilon_\infty \geq 2$;

- if $\epsilon_3 > 0$ and $\epsilon_2 = 0$, then $\epsilon_\infty \geq 2$;
- if $\epsilon_3 > 0$ and $\epsilon_2 > 0$, then $\epsilon_3 \geq 2$, $\epsilon_2 \geq 2$, and $\epsilon_\infty \geq 2$.

Hence, by using Lemma 4.3.1 to calculate the degrees of $\mathcal{L}_{k,p}$ for $k \in \{2, 4, 6, 8, 10, 12\}$, we find that:

- $\deg \mathcal{L}_{2,p} \geq 2g$ in all cases, and $\deg \mathcal{L}_{2,p} \geq 2g + 2$ if $\epsilon_2 = \epsilon_3 = 0$ and N is composite;
- $\deg \mathcal{L}_{4,p} \geq 2g + 1$ if $\epsilon_3 = 0$, and $\deg \mathcal{L}_{4,p} \geq 2g + 2$ if additionally $\epsilon_2 > 0$;
- $\deg \mathcal{L}_{6,p}, \deg \mathcal{L}_{8,p}, \deg \mathcal{L}_{10,p}, \deg \mathcal{L}_{12,p} \geq 2g + 1$ if $\epsilon_3 > 0$.

Let:

$$r := \begin{cases} 2 & \text{if } \epsilon_2 = \epsilon_3 = 0 \text{ and } N \text{ is composite,} \\ 6 & \text{if } \epsilon_3 > 0 \text{ and } \epsilon_2 = 0, \\ 12 & \text{if } \epsilon_3 > 0 \text{ and } \epsilon_2 > 0, \\ 4 & \text{otherwise.} \end{cases}$$

Let $k \geq r$, and write $k = ar + b$ where $a = \lfloor \frac{k}{r} \rfloor$ and $b \in \{2, 4, 6, 8, 10\}$. Then by Proposition 4.3.3:

$$\mathcal{L}_{k,p} \cong \mathcal{L}_{ar,p} \otimes \mathcal{L}_{b,p} \cong \mathcal{L}_{r,p}^{\otimes a} \otimes \mathcal{L}_{b,p}$$

By Theorem 3.3.1, the multiplication maps:

$$H^0(X_0(N), \mathcal{L}_{r,p}^{\otimes a}) \otimes H^0(X_0(N), \mathcal{L}_{b,p}) \to H^0(X_0(N), \mathcal{L}_{k,p})$$

and:

$$(H^0(X_0(N), \mathcal{L}_{r,p}))^{\otimes a} \to H^0(X_0(N), (\mathcal{L}_{k,p})^{\otimes a})$$

are surjective. □

Remark 4.3.5. *Unlike Proposition 3.4.2, Proposition 4.3.4 does not guarantee a minimal generating weight.*

Proposition 4.3.6. *Let $N \geq 5$, and $p \notin R_N^\times$ a prime number. Let ϵ_∞ be the number of cusps for $\Gamma_0(N)$, and let ϵ_2 and ϵ_3 be respectively the number of elliptic points of order 2 and of order 3. Choose a set of generators for $M = M(\Gamma_0(N), \mathbb{F}_p)$, lying in weight at most d, where d is as given in Proposition 4.3.4. Then the ideal of relations between these generators is generated:*

- *in degree 6 if $\epsilon_3 = \epsilon_2 = 0$ and N is composite;*
- *in degree 14 if $\epsilon_3 > 0$ and $\epsilon_2 = 0$;*
- *in degree 130 if $\epsilon_3 > 0$ and $\epsilon_2 > 0$;*

- *in degree* 10 *otherwise.*

Proof. We take the case where $\epsilon_3 > 0$ and $\epsilon_2 > 0$, since the rest are proven similarly. By Proposition 4.3.4, we can pick generators $g_1, \cdots, g_n$ in weights $2, 4, 6, 8, 10$, and 12. Let $k \geq 132$ be even. Then any homogeneous monomial in $g_1, \cdots, g_n$ of weight k must be divisible by a homogeneous monomial in $g_1, \cdots, g_n$ of degree k' where k' depends only on k, $12|k'$ and $k' \geq 24$[‡]. Write $k = k' + b$. Then by the projection formula of Proposition 4.3.3, we have a commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & R(\mathcal{L}_{k'}, \mathcal{L}_b) \arrow[r] & H^0(X, \mathcal{L}_{k'}) \otimes H^0(X, \mathcal{L}_b) \arrow[r] & H^0(X, \mathcal{L}_k) \\
R(\mathcal{L}_{k'-12}, \mathcal{L}_b) \otimes H^0(X, \mathcal{L}_a) \arrow[ur, "\epsilon"] & & &
\end{tikzcd}$$

where the map ϵ is surjective by Theorem 3.3.1 and by the calculation of degrees as in the proof of Proposition 4.3.4. Therefore we can argue in the same way as in the proof of Theorem 3.4.3. □

We combine these results and obtain:

Theorem 4.3.7. *Let $N \geq 5$. Let ϵ_∞ be the number of cusps for $\Gamma_0(N)$, and let ϵ_2 and ϵ_3 be respectively the number of elliptic points of order 2 and of order 3. The algebra $M(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])$ is:*

- *generated in weight* 2 *and related in degree* 6*, if $\epsilon_3 = \epsilon_2 = 0$ and N is composite,*
- *generated in weight* 6 *and related in degree* 14 *if $\epsilon_3 > 0$ and $\epsilon_2 = 0$,*
- *generated in weight* 12 *and related in degree* 130 *if $\epsilon_3 > 0$ and $\epsilon_2 > 0$, and*
- *generated in weight* 4 *and related in degree* 10 *otherwise.*

4.4 Modular forms with coefficients in $\mathbb{Z}$

We now investigate the generating weight for the algebras $M(\Gamma_0(N), \mathbb{Z})$. We will prove later (Corollary 5.2.5) that $M(\Gamma_0(p), \mathbb{Z})$ is generated in weight p^2+11. This bound, however, is not optimal, and one can wonder whether a better bound can be found. While for the algebras considered so far we found a generating weight that is independent of the level, we will see that when we restrict the base coefficient ring to $\mathbb{Z}$, the generating weight becomes unbounded.

[‡] This non-obvious fact can be checked on a computer.

4.4.1 The lower bound

Let $f \in M_k(\Gamma_0(N), \mathbb{Q})$, and write $f = \sum_{n \geq 0} a_n q^n$ for its q-expansion. The p-adic valuation of f is:

$$v_p(f) := \inf\{v_p(a_n) : n \geq 0\}.$$

Consider a level $N \geq 1$ and an odd prime p dividing N exactly once. Recall (Definition 1.3.7) the Atkin-Lehner involution acting on modular forms $f \in M_k(\Gamma_0(N))$:

$$f \mapsto f|_k W_p^N$$

where:

$$W_p^N = \begin{pmatrix} p & a \\ N & bp \end{pmatrix}$$

where a and b are any integers such that $\det W_p^N = p^2 b - Na = p$. The following lemma is due to Kilbourn (see [Kil07]), and it generalises a result obtained in prime level in [DR73], Proposition VII.3.20.

Lemma 4.4.1. *Let $N \geq 1$ and let p be an odd prime dividing N exactly once. Then for all $k \leq p-3$, :*

$$|v_p(f|W_p^N) - v_p(f)| \leq k/2.$$

For convenience, we will make the following definition.

Definition 4.4.2. *Let N and p be as in Lemma 4.4.1, $k \geq 0$ and $f \in M_k(\Gamma_0(N), \mathbb{Q})$. Then we define the following operator:*

$$\tilde{f} := \tilde{\omega}(f) := p^{k/2} f|_k W_p^N.$$

Then we have a corollary of Lemma 4.4.1:

Corollary 4.4.3. *Let N and p be as in Lemma 4.4.1, $0 \leq k \leq p-3$, and $f \in M_k(\Gamma_0(N), \mathbb{Q})$. Then:*

$$v_p(\tilde{f}) \geq v_p(f).$$

In particular, if $v_p(f) = 0$, then $v_p(\tilde{f}) \geq 0$.

The main result of this section is the following:

Theorem 4.4.4. *Let $N \geq 5$ and let $p \geq 5$ be a prime which divides N exactly once. Then any set of generators for $M(\Gamma_0(N), \mathbb{Z})$ contains a form of weight $p-1$. In particular, the generating weight of $M(\Gamma_0(N), \mathbb{Z})$ is at least $p-1$.*

Proof. The idea of the proof is to produce a modular form in weight $p-1$ that cannot be written as a polynomial with $\mathbb{Z}$ coefficients in modular forms with $\mathbb{Z}$ coefficients in weights $< p-1$. Define the following modular form:

$$T(z) := \left(\frac{\eta(pz)^p}{\eta(z)}\right)^2 \in M_{p-1}(\Gamma_0(p)) \subset M_{p-1}(\Gamma_0(N)),$$

where η is the Dedekind eta function, defined by the product:

$$\eta(z) = e^{\frac{2i\pi z}{24}} \prod_{n=1}^{\infty}(1-q^n).$$

Note that $\eta^{24} = \Delta$. To see that it is actually a modular form on $\Gamma_0(p)$, one can use the transformation formula for the eta function, which can be found in [Köh11]. It is obvious that T has q-expansion coefficients in $\mathbb{Z}$, and that $v_p(T) = 0$. The truth of Theorem 4.4.4 then clearly follows from the following lemma:

Lemma 4.4.5. *The form T is not a polynomial with $\mathbb{Z}$ coefficients in modular forms with $\mathbb{Z}$ coefficients in weights $< p-1$.*

Proof. We will prove the lemma by showing that T violates the inequality in Lemma 4.4.1, and that every modular form which is a polynomial in forms of weight $< p-1$ must satisfy the inequality.
We define the following matrices:

$$M_p = \begin{pmatrix} 1 & a \\ \frac{N}{p} & pb \end{pmatrix},$$

$$M'_p = \begin{pmatrix} p & a \\ \frac{N}{p} & b \end{pmatrix},$$

$$\gamma = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

We note that $W_p^N = M_p\gamma$, and that $\gamma W_p^N = pM'_p$, so γW_p^N acts on modular forms via the $-|_k$ operator in the same way as M'_p does. We wish to compute $v_p(\tilde{T})$ where $\tilde{T} = p^{\frac{p-1}{2}} T|W_p^N$. We have:

$$\tilde{T}(z) = p^{p-1}(Nz+pb)^{-(p-1)} \left(\frac{\eta(M'_p \cdot z)^p}{\eta(W_p^N \cdot z)}\right)^2.$$

By applying the appropriate transformation formula for the η function (see [Köh11]), we have:

$$\eta(M'_p \cdot z)^2 = p\nu_\eta(M'_p)^2(Nz+pb)\eta(z)^2,$$

$$\eta(W_p^N \cdot z)^2 = \nu_\eta(M_p)^2(Nz+pb)\eta(p\cdot z)^2,$$

where $\nu_\eta(-)$ is the eta multiplier. After writing out the multipliers explicitly, we find that:

$$\tilde{T}(z) = \epsilon p^{-1}\left(\frac{\eta(z)^p}{\eta(pz)}\right)^2$$

where:

$$\epsilon = \begin{cases} e\left(\frac{2Np-6p-2N/p+6}{24}\right) & \text{if } N/p \in 2\mathbb{Z} \\ e\left(\frac{2Np-6N+4N/p}{24}\right) & \text{otherwise} \end{cases},$$

and $e(z) = e^{2i\pi z}$. It is easy to show that $\epsilon = \pm 1$, and hence that $v_p(\tilde{T}) = -1$. All we need to show is that

$$Np - 3p - N/p + 3 \equiv 0 \pmod 6 \text{ if } \frac{N}{p} \equiv 0 \pmod 2$$

and that

$$Np - 3N + 2N/p \equiv 0 \pmod 6 \text{ if } \frac{N}{p} \equiv 1 \pmod 2.$$

Indeed, we have $p \equiv 1 \pmod 2$ and $p \equiv \pm 1 \pmod 3$, so if $\frac{N}{p} \equiv 0 \pmod 2$, then:

$$\begin{cases} Np - 3p - N/p + 3 \equiv 0 \pmod 2 & \text{, and} \\ Np - 3p - N/p + 3 \equiv 0 \pmod 3. \end{cases}$$

Similarly, if $\frac{N}{p} \equiv 1 \pmod 2$, then:

$$\begin{cases} Np - 3N + 2N/p \equiv 0 \pmod 2 & \text{, and} \\ Np - 3N + 2N/p \equiv 0 \pmod 3. \end{cases}$$

To finish the proof, note that the operator $\tilde{\omega}$ of Definition 4.4.2 defines an operator on the graded algebra of modular forms:

$$\widetilde{fg} = \tilde{f}\cdot\tilde{g},$$
$$\widetilde{f+g} = \tilde{f} + \tilde{g}.$$

Suppose now that

$$T = \sum c_{i_1,\cdots,i_n} g_1^{i_1}\cdots g_n^{i_n}$$

where $c_i \in \mathbb{Z}$ and $g_i \in M(\Gamma_0(N),\mathbb{Z})$ are modular forms in weights $\leq p-3$. Then:

$$\tilde{T} = \sum c_{i_1,\cdots,i_n}(\tilde{g_1})^{i_1}\cdots(\tilde{g_n})^{i_n},$$

which would force $v_p(\tilde{T}) \geq 0$ by Corollary 4.4.3, but that contradicts the above computation of $v_p(\tilde{T})$. □

We have now established Lemma 4.4.5, and Theorem 4.4.4 follows immediately. □

4.4.2 Intersection theory on $\mathcal{X}_0(p)$

For the convenience of the reader, we summarise here the main definitions regarding the intersection theory on the stacks $\mathcal{X}_0(p)$ studied in [DR73]. For our purpose, we only need the theory developed in [DR73]. However, the appendix by Brian Conrad in [BDP] contains a more explicit and more general treatment of the intersection theory on such stacks.

The stack $\mathcal{X}_0(p)$ is the moduli stack classifying elliptic curves (over $\mathbb{Z}$) with a choice of a subgroup of order p. These stacks are Deligne-Mumford (DM); the main property of DM stacks that we need is that they admit finite étale covers by schemes. Thus one can define sheaves on them as sheaves on the étale site, in particular, these stacks are locally ringed, and one can use the intersection theory of schemes to define intersection concepts on the stacks. For the definition and basic properties of these stacks, see [DM69].

The stack $\mathcal{X}_0(p)$ is not representable, i.e. it is not a scheme, since every pair (E, C) consisting of an elliptic curve E and a subgroup C of order p admits at least one non-trivial automorphism (the involution corresponding to $-1 \in \Gamma_0(p)$). It is regular ([DR73],Théorème V.1.16), of dimension 2 (of relative dimension 1) over $\mathrm{Spec}(\mathbb{Z})$.

Let $\mathcal{M}$ be such a stack, and let $\mathcal{L}$ be an invertible sheaf on $\mathcal{M}$. As in [DR73], VI.4.3, the degree of $\mathcal{L}$ is defined as follows. Suppose that $\mathcal{L}$ has a rational section f. Pick a geometric fibre (for example, say it is $\mathcal{M} \otimes k$ where k is an algebraically closed field), and at each closed geometric point x of this fibre, define:

$$\deg_x(f) = \begin{cases} \dim_k \widetilde{O_x}/(f) & \text{if } f \text{ is regular at } x \\ -\dim_k \widetilde{O_x}/(f^{-1}) & \text{otherwise} \end{cases}$$

where $\widetilde{O_x}$ is the henselian local ring of the fibre at x. Then the degree of $\mathcal{L}$ is defined by:

$$\deg \mathcal{L} = \sum_x \frac{\deg_x(f)}{|\operatorname{Aut}(x)|}$$

where $\operatorname{Aut}(x)$ is the automorphism group of the elliptic curve represented by the point x. This degree is independent of the choice of the fibre.

A reduced irreducible closed substack of codimension 1 is Cartier (Lemma B.2.2.8 in [BDP]). A Cartier divisor is effective if the ideal sheaf associated to the corresponding closed substack is invertible. If D is an effective Cartier divisor, there is an invertible sheaf $\mathcal{O}(D)$ associated to it that has a canonical regular global section s_D. By regularity of the stack, the henselian local ring at every codimension 1 point is a DVR, thus to every effective Cartier divisor one can associate an effective Weil divisor (i.e. a finite formal integral combination of closed reduced irreducible substacks of co-dimension 1, where all the coefficients are non-negative). For an invertible sheaf $\mathcal{L}$ on $\mathcal{M}$, and a global section s of $\mathcal{L}$

that is non-zero on every connected component of $\mathcal{M}$, we can associate a Weil divisor $\operatorname{div}(f)$ such that there is an isomorphism of sheaves $\mathcal{O}(\operatorname{div}(f)) \cong \mathcal{L}$.
Thus we can identify the concepts of an effective Cartier divisor and an effective Weil divisor. Given an invertible sheaf $\mathcal{L}$ with a global section s which is non-zero on every connected component, its divisor $D = \operatorname{div}(f)$ can be written as the sum of horizontal and vertical divisors. If N is an irreducible component of a geometric fibre, seen as a vertical divisor (by giving it the reduced structure), then one can define the intersection number:

$$(D, N) := \deg \mathcal{O}(D)|_N.$$

The degree of $\mathcal{L}$ can equally be defined as the intersection number of the divisor of a global section with a geometric fibral divisor.
The stack classifying generalised elliptic curves (without a choice of a structure) is denoted $\mathcal{X}_0(1)$. It is shown in [DR73] (Théorème V.1.16) that the reduction mod p, $\mathcal{X}_0(p) \otimes \mathbb{F}_p$ consists of two copies of $\mathcal{X}_0(1) \otimes \mathbb{F}_p$ glued together at the supersingular points.

4.4.3 Congruences of level 1 and level p modular forms

For this section, fix a prime $p \geq 5$. We look at congruence relations between modular forms on $SL_2(\mathbb{Z})$ and on $\Gamma_0(p)$, that is, congruences between their formal q-expansions at infinity. In [Ser73b], Serre proves that every modular form in $M(\Gamma_0(p), \mathbb{Z})$ is p-adically of level 1, that is, if $f \in M_k(\Gamma_0(p), \mathbb{Z})$ for some k, then for every integer $i > 0$, there exists an integer k_i and a modular form $f_i \in M_{k_i}(SL_2(\mathbb{Z}), \mathbb{Z})$ such that $f \equiv f_i \pmod{p^i}$. In particular one has the following result. Let $v = v_p(\tilde{f})$, and let:

$$E^*_{p-1} = E_{p-1} - \tilde{E}_{p-1}.$$

The form E^*_{p-1} has the following properties: $E^*_{p-1} \equiv 1 \pmod{p}$ and $v_p(\widetilde{E^*_{p-1}}) = p$. If $v \leq k$, this implies that $tr(f(E^*_{p-1})^{k-v}) \in M_{kp-v(p-1)}(SL_2(\mathbb{Z}))$ is p-integral and is congruent to f modulo p. Here, tr is the trace operator defined in Definition 1.3.6 and sending modular forms of level p to modular forms of level 1.
When $v > k$, if the above congruence still holds, then we expect to see f mod p in weight $kv - v(p-1) < k$. Since this weight is less than k, Serre's trace argument apparently no longer applies. The aim of this section is to show that a similar congruence relation still holds even when the "expected weight" for f is less than k. That is, we have:

Theorem 4.4.6. *Let $p \geq 5$, $f \in M_k(\Gamma_0(p), \mathbb{Z})$ with $v_p(f) = 0$ and $v_p(\tilde{f}) = k + a$. Then there exists $g \in M_{k-a(p-1)}(SL_2(\mathbb{Z}), \mathbb{Z})$ such that $f \equiv g \pmod{p}$.*

Proof. The case where $a \leq 0$ is covered by Serre's argument in [Ser73b]. We deal here with the case where $a > 0$. The proof relies on Deligne and Rapoport's study of the stack $\mathcal{X}_0(p)$ in [DR73]. The intersection theory on such stacks is summarised in Section 4.4.2.

The modular form f can be seen as a global section $f \in H^0(\mathcal{X}_0(p), \omega^{\otimes k})$. Let N_1 and N_2 be the two irreducible components of $\mathcal{X}_0(p) \otimes \mathbb{F}_p$ containing respectively the (reductions of the) cusps ∞ and 0. Then f does not vanish at the generic point of N_1, and it vanishes to order a at the generic point of N_2. Thus the divisor of f can be written as:

$$\operatorname{div}(f) = D + aN_2$$

where, without loss of generality after multiplying f by a constant of p-adic valuation 0, we can assume[§]that D is an effective horizontal Cartier divisor on $\mathcal{X}_0(p)$. As in [DR73], VII.3.19, we can calculate the intersection number (D, N_1) as follows: on $N_1 \cong \mathcal{X}_0(1) \otimes \mathbb{F}_p$, the degree of ω is $\frac{1}{24}$ ([DR73], VI.4.4.1), hence:

$$(\operatorname{div}(f), N_1) = \frac{k}{24}.$$

The components N_1 and N_2 intersect transversely at the supersingular points. It follows from [DR73] (Théorème V.1.16 and Théorème VI.4.9.1) that:

$$(N_2, N_1) = \frac{p-1}{24}$$

This gives then that:

$$(D, N_1) = \frac{k - a(p-1)}{24}.$$

Now D is an effective Cartier divisor, so it corresponds to an invertible sheaf $\mathcal{O}(D)$ together with a regular global section s_D. We then have:

$$(D, N_1) = \deg_{\overline{\mathbb{F}}_p}(\mathcal{O}(D)|_{N_1}) = \sum_x \frac{\deg_x(s_D)}{|\operatorname{Aut}(x)|}$$

where the sum is over the closed geometric points of the component N_1. Since s_D is regular, $\deg_x(s_D) \geq 0$ for each x, and $(D, N_1) \geq 0$. Since $p \geq 5$, it follows (see [Sil09], Theorem 10.1) that for each x, $|\operatorname{Aut}(x)| \leq 6$. In particular we have that if $(D, N_1) > 0$, then $(D, N_1) \geq \frac{1}{6}$.

First, if $k - a(p-1) = 2$, then $(D, N_1) = \frac{1}{12} < \frac{1}{6}$, which is impossible. So we

[§] While f might have some poles along certain vertical (i.e. fibral) divisors, it cannot have a pole along a horizontal divisor. This is because any horizontal divisor would meet the generic fibre, and so if f has a pole along a horizontal divisor, then f would have a pole when considered as a modular form over $\mathbb{C}$, which contradicts the holomorphy of f as a complex function of a complex variable. The vertical components of the divisor of poles correspond to the primes appearing in the denominators of the q-expansion of f. As these denominators are bounded, one can find a constant $K \in \mathbb{Z}$, $K \not\equiv 0 \pmod{p}$ such that Kf has no primes in the denominators of its q-expansion except possibly p. Multiplying by such a constant obviously preserves the p-adic valuation of f at both cusps.

must have that either $k - a(p-1) = 0$ or $k - a(p-1) > 2$. Denote by M_k^a the subset of $M_k(\Gamma_0(p), \mathbb{Z})$ consisting of modular forms h such that $v_p(h) = 0$ and $v_p(\tilde{h}) = k + a$. Define the mapping:

$$\phi : M_{k-a(p-1)}(SL_2(\mathbb{Z}), \mathbb{Z}) \to M_k(\Gamma_0(p), \mathbb{Z})$$

$$g \mapsto (E_{p-1}^*)^a g.$$

Recall here the convention that $M_0(SL_2(\mathbb{Z}), \mathbb{Z}) = \mathbb{Z}$. It is easy to check that the image under ϕ of $V = M_{k-a(p-1)}(SL_2(\mathbb{Z}), \mathbb{Z})$ lies in M_k^a. Recall also that V has a Victor Miller basis, which is the unique integral basis consisting of forms $f_0, \cdots, f_{d-1}$, where $d = \dim_{\mathbb{Q}} M_{k-a(p-1)}(SL_2(\mathbb{Z}), \mathbb{Q})$, such that $f_i = q^i + O(q^d)$ for $0 \leq i \leq d-1$ (see for instance Proposition 6.2 in [Kil08]). We also adopt the convention that the Victor Miller basis of $M_0(SL_2(\mathbb{Z}), \mathbb{Z})$ is the set $\{1\}$.

Assume f mod p is not in $\phi(V) \otimes \mathbb{F}_p$, then subtracting from f a suitable linear combination of the images in $\phi(V) \otimes \mathbb{F}_p$ of elements of the Victor Miller basis of V, we may assume that f has a mod p vanishing order at infinity $v_{\infty,p}(f) \geq d$, where $d = \dim_{\mathbb{Q}} M_{k-a(p-1)}(SL_2(\mathbb{Z}), \mathbb{Q})$; then so does the section s_D of $\mathcal{O}(D)$. As the cusp infinity has only an automorphism of order 2, we have:

$$\sum_{x \neq \infty} \frac{\deg_x(s_D)}{|\operatorname{Aut}(x)|} + \frac{v_{\infty,p}(s_D)}{2} = (D, N_1).$$

If $k - a(p-1) = 0$, then $(D, N_1) = 0$, and $d = \dim_{\mathbb{Q}} M_{k-a(p-1)}(SL_2(\mathbb{Z}), \mathbb{Q}) = 1$. As $\deg_x(s_D) \geq 0$ for each x, this means that $\deg_x(s_D) = 0$ for all x, so in particular, $v_{\infty,p}(s_D) = 0$, but this contradicts the inequality $v_{\infty,p}(f) \geq d$. So assume that $k - a(p-1) > 2$. We have:

$$\sum_{x \neq \infty} \frac{\deg_x(s_D)}{|\operatorname{Aut}(x)|} + \frac{v_{\infty,p}(s_D) - d}{2} = (D, N_1) - \frac{d}{2}.$$

Consider the form $f_{d-1} \in V$, which is the element of the Victor Miller basis of V with highest vanishing order at infinity, this vanishing order at infinity being $v_\infty(f_{d-1}) = d-1$. This form vanishes nowhere other than at infinity and possibly at the elliptic points of orders 2 and 3. Let $v_2(f_{d-1})$ and $v_3(f_{d-1})$ denote respectively the vanishing orders of f_{d-1} at the elliptic points of orders 2 and 3, and recall that $v_2(f_{d-1}) \leq 1$ and $v_3(f_{d-1}) \leq 2$. The valence formula for level 1 modular forms (see for example Proposition 3.2 in [Kil08]) then gives:

$$v_\infty(f_{d-1}) + \frac{1}{2} v_2(f_{d-1}) + \frac{1}{3} v_3(f_{d-1}) = \frac{k - a(p-1)}{12},$$

and therefore:

$$\frac{k - a(p-1)}{12} - (d-1) \leq \frac{1}{2} + \frac{2}{3} = \frac{7}{6}.$$

Thus using the above calculation for (D, N_1), we find that:

$$\sum_{x \neq \infty} \frac{\deg_x(s_D)}{|\operatorname{Aut}(x)|} + \frac{v_{\infty,p}(s_D) - d}{2} \leq \frac{1}{12},$$

which forces:

$$\sum_{x \neq \infty} \frac{\deg_x(s_D)}{|\operatorname{Aut}(x)|} + \frac{v_{\infty,p}(s_D) - d}{2} = 0$$

and hence:

$$(D, N_1) = \frac{d}{2}$$

which in turn gives:

$$d = \frac{k - a(p-1)}{12}.$$

This however is contradicted by the dimension formula for modular forms in level 1 (Proposition 1.2.11), which says that if $k - a(p-1) \equiv 0 \pmod{12}$, then $d = 1 + \frac{k-a(p-1)}{12}$.

□

Remark 4.4.7. *A weaker version of Theorem 4.4.6 can be proven by elementary methods. This can be done by adapting the argument due to Kilbourn (see [Kil07]) by which he proves Lemma 4.4.1. This is a sketch of the argument: if f satisfies the hypothesis of Theorem 4.4.6 with $a \geq 1$, then $h = tr(f) \equiv f \pmod{p^2}$. Let $g = \frac{f-h}{p^{v_p(f-h)}}$. let $-|V : M_k(SL_2(\mathbb{Z})) \to M_k(\Gamma_0(p), \mathbb{Z})$ denote the operator defined by $V(\sum a_n q^n) = \sum a_n q^{pn}$. Then one can show that $h|V \equiv p^{m-k}\tilde{g} \pmod{p}$. On the other hand, $v_p(p^{m-k}\tilde{\tilde{g}}) = v_p(p^{m-k}p^k g) \geq a+1 \geq 2$, so $p^{m-k}\tilde{g}$ is congruent to some modular form of level 1 in weight $kp - (a+1)(p-1)$. If w_p denotes the mod p filtration of level 1 modular forms (see Section 6.1), defined by:*

$$w_p(F) = \inf\{k : F \equiv G \pmod{p} \text{ for some } G \in M_k(SL_2(\mathbb{Z}), \mathbb{Z})\},$$

we know that $w_p(h|V) = p w_p(h)$ so this forces $w_p(h) \leq k - (p-1)$. It might be possible to find a variation of this argument that would give an alternative and elementary proof of Theorem 4.4.6. I was however unable to find such an argument.

A simple corollary of this theorem concerns the form T defined in the proof of Theorem 4.4.4.

Corollary 4.4.8. $p\tilde{T} \equiv 1 \pmod{p}$.

Proof. This can be proven directly from the computation of $\tilde{T}$ as in the previous section, but this follows easily from Theorem 4.4.6, by noting that $v_p(p\tilde{T}) = 0$, $v_p(\widetilde{p\tilde{T}}) = p$ and that $p\tilde{T}$ is of weight $p-1$. The theorem then implies that $p\tilde{T}$ is congruent mod p to a modular form of weight 0, that is, a constant, and this constant is found to be 1 by examining the first coefficient of the q-expansion. □

4.4.4 Generators of $M(\Gamma_0(p), \mathbb{Z})$

In this section we identify a set of generators for $M(\Gamma_0(p), \mathbb{Z})$. Let T denote the form T defined in the proof of Theorem 4.4.4:

$$T(z) := \left(\frac{\eta(pz)^p}{\eta(z)} \right)^2 \in M_{p-1}(\Gamma_0(p), \mathbb{Z}).$$

Let S denote the subset of $M(\Gamma_0(p), \mathbb{Z})$ consisting of modular forms f satisfying $v_p(\tilde{f}) \geq 0$. We prove the following:

Theorem 4.4.9. *The algebra $M(\Gamma_0(p), \mathbb{Z})$ is generated by T and S.*

Proof. Let $f \in M_k(\Gamma_0(p), \mathbb{Z})$, $f \notin S$. Put $a = -v_p(\tilde{f}) > 0$. We argue by induction on a. Let $g = p^a \tilde{f}$. Then $v_p(g) = 0$ and $v_p(\tilde{g}) = a + v_p(\tilde{\tilde{f}}) = a + v_p(p^k f) \geq k + a$, so by Theorem 4.4.6, there exists $h \in M_{k-a(p-1)}(SL_2(\mathbb{Z}), \mathbb{Z})$ such that:

$$h \equiv g \pmod{p},$$

and by Corollary 4.4.8, this can be rewritten as:

$$(p\tilde{T})^a h \equiv g \pmod{p}$$

where now $(p\tilde{T})^a h$ and g have the same weight. Thus there exists $u \in M_k(\Gamma_0(p), \mathbb{Z})$ such that:

$$(p\tilde{T})^a h + pu = g.$$

Recall that $\widetilde{p\tilde{T}} = p^p T$, and that $\tilde{h} = p^{k-a(p-1)} h|V$ since h is of level 1 and of weight $k - a(p-1)$. So applying the $\tilde{w}$ operator again, we get:

$$p^{k+a} T^a h|V + p\tilde{u} = p^{k+a} f$$

and hence $p\tilde{u} = p^{k+a} v$ for some $v \in M_k(\Gamma_0(p), \mathbb{Z})$. Now we have:

$$f = T^a h|V + v.$$

An easy calculation now shows that $v_p(\tilde{v}) \geq 1 - a = v_p(f)$ (since $v_p(u) \geq 0$). By induction it then follows that we have the following decomposition of f:

$$f = T^a f_a|V + T^{a-1} f_{a-1}|V + \cdots + T f_1|V + f_0$$

where for each $1 \leq i \leq a$, $f_i \in M_{k-i(p-1)}(SL_2(\mathbb{Z}), \mathbb{Z})$, and hence $v_p(\tilde{f_i}|V) = v_p(f_i) \geq 0$, and $v_p(\tilde{f_0}) \geq 0$, which proves the theorem. □

Numerical evidence points to the following conjecture:

Conjecture 4.4.10. *The $\mathbb{Z}$-subalgebra of $M(\Gamma_0(p), \mathbb{Z})$ generated by:*

$$S = \{f \in M(\Gamma_0(p), \mathbb{Z}) : v_p(\tilde{f}) \geq 0\}$$

is generated in weight 6.

Conjecture 4.4.10 and Theorem 4.4.9 together imply the following:

Conjecture 4.4.11. *The weights of the modular forms appearing in a minimal set of generators for $M(\Gamma_0(p), \mathbb{Z})$ are in the set $\{2, 4, 6, p-1\}$, and there is only one generator of weight $p-1$ (which can be chosen to be the T-form T).*

Section A.3 provides numerical evidence supporting Conjecture 4.4.11.

Chapter 5

Calculating the structure of $M(\Gamma, R)$

In this chapter, we describe Scholl's proof of finite generation, and give algorithms that are based on his proof for computing the structure of the algebra of modular forms for a given congruence subgroup and with coefficients in a subring A of $\mathbb{C}$. We examine Scholl's construction of a T-form for the congruence subgroups $\Gamma_0(N)$, and show that it is not always optimal (i.e. it is not of the smallest possible weight). For the groups $\Gamma_0(p)$, where $p \geq 5$, we explicitly construct the optimal T-form. This is taken mainly from the article [Rus14b]; the optimality of the T-form is discussed also in [Rus14a].

5.1 Scholl's proof of finite generation

For various subrings A of $\mathbb{C}$, Scholl ([Sch79]) provides an easy proof that the algebra $M(\Gamma_0(N), A)$ is finitely generated. We state the theorem:

Theorem 5.1.1. *Let Γ be a subgroup of $SL_2(\mathbb{Z})$ of finite index, such that $-1 \in \Gamma$, A a subring of $\mathbb{C}$. Assume the cusp at infinity has width 1, and $q = e^{2i\pi z}$ is a uniformising parameter. If the following conditions hold:*

1. *$M_k(\Gamma, \mathbb{C}) = M_k(\Gamma, A) \otimes \mathbb{C}$ for all $k \geq 0$;*

2. *for some $t > 0$, there exists $T \in M_t(\Gamma, A)$ such that, T is non-zero away from the cusp at infinity, and its q-expansion is a unit in $A((q))$.*

Then $M(\Gamma, A)$ is finitely generated as an A-algebra.

Proof. Let r be the vanishing order of T at infinity. Write:

$$T = q^r \sum_{n=0}^{\infty} a_i q^i, a_0 \in A^*, a_n \in An \geq 1$$

Let $m_k = \dim_{\mathbb{C}} M_k(SL_2(\mathbb{Z}), \mathbb{C})$. For $F \in M_k(\Gamma, A)$, there exists a form $G \in M_k(SL_2(\mathbb{Z}), A)$ such that $F - G$ has vanishing order at least m_k (to see this, we can use Victor-Miller basis to construct G). Thus if $m_k \geq r$, the function $\frac{F-G}{T}$ is a modular form of weight $k - t$ with coefficients in A (follows from the defining properties of T). We can then use induction on k. Fix $k \geq t$ for which $m_k \geq r$, then write:

$$M_k(\Gamma, A) = M_k(SL_2(\mathbb{Z}), A) + T \cdot M_{k-t}(\Gamma, A).$$

Thus $M(\Gamma, A)$ is generated by T and the forms in weights $\{k : m_k < r \text{ or } k < t\}$. □

Definition 5.1.2. *A modular form satisfying the condition* (2) *above is called a T-form over A. A T-form over $\mathbb{Z}$ is simply called a T-form. Obviously, a T-form is a T-form over A for any $A \subset \mathbb{C}$. For example, when $\Gamma = SL_2(\mathbb{Z})$, and $A = \mathbb{Z}$, then the discriminant Δ is such a T-form.*

This gives a recipe to prove that, for given Γ and A, the algebra $M(\Gamma, A)$ is finitely generated: we only have to produce a T-form over A.

5.2 Scholl's construction of the T-form for $\Gamma_0(N)$

Scholl's construction of the T-form over $\mathbb{Z}$ for $\Gamma_0(N)$ rests on the following lemma ([New59]):

Lemma 5.2.1. *Let N be a positive integer. Consider the eta product:*

$$f = \prod_{0<d|N} \eta(dz)^{r(d)}$$

where:

1. *$r(d) \in \mathbb{Z}$ and $\sum r(d) = 0$,*

2. *$\prod d^{r(d)}$ is a rational square,*

3. *f has integral order of vanishing (that is, in the local parameter) at every cusp of $\Gamma_0(N)$.*

Then f is a modular function on $\Gamma_0(N)$.

Let Q_i be the cusps of $\Gamma_0(N)$, and $\frac{r_i}{s_i}$ be representatives of Q_i, with Q_1 being the cusp at infinity. Let t_i be the width of Q_i. We can choose $r_1 = 1, s_1 = N$ and $t_1 = 1$. The set G_N of eta products satisfying the above conditions is a multiplicative free, finitely generated abelian group, of rank at most $\sigma(N) - 1$, where $\sigma(N)$ is the number of divisors of N. Let ν be the number of cusps. By (f) we denote the divisor of f. We will need the following lemma ([Sch79]):

Lemma 5.2.2. *Let d be a positive divisor of N, and r/s representing a cusp of width t of $\Gamma_0(N)$. Then the order of vanishing of $\Delta(dz)$ at r/s is $t\gcd(d,s)^2/d$.*

Recalling that $\eta^{24} = \Delta$, this allows us to calculate the divisor of an eta product, such as the ones described above. We have then the following proposition:

Proposition 5.2.3. *Let $\{n_1, \cdots, n_\nu\}$ be integers such that $\sum_{i=1}^{\nu} n_i = 0$. Then there is a function $f \in G_N$ and an integer m such that*

$$(f) = m \sum_{i=1}^{\nu} n_i Q_i$$

if and only if for all i, j such that $1 \leq i, j \leq \nu$, we have:

$$s_i = s_j \Rightarrow \frac{n_i}{t_i} = \frac{n_j}{t_j}$$

Proof. We briefly sketch Scholl's proof, since it provides a way to construct the T-form we are after. Write $x(d) = r(d)/m$. We need:

$$(f) = \sum_{i=1}^{\nu} \sum_{0<d|N} (r(d) t_i \gcd(d, s_i)^2/24d) Q_i = m \sum_{i=1}^{\nu} n_i Q_i$$

which means that we need, for each $1 \leq i \leq \nu$:

$$\sum_{0<d|N} \gcd(d, s_i)^2 x(d)/d = 24 n_i/t_i$$

Scholl proves that this system is consistent and so f and m can be found. □

Having constructed such f and m as in the lemma, chosen so that $n_i = t_i$ for $i \geq 2$ and $n_1 = -\sum_{i \geq 2} t_i$ (following p.464 in [Sch79]), we can find a T-form for $\Gamma_0(N)$:

$$T = \frac{\Delta^m}{f}$$

and it has divisor:

$$(T) = m \left(\sum_{i=1}^{\nu} n_i \right) Q_1,$$

that is, it only vanishes at infinity.

For $N = p$ a prime, we know that $\Gamma_0(p)$ has only two cusps. It is then easy to explicitly solve for the smallest m that works:

$$m = \frac{p-1}{\gcd(24p, p-1)}.$$

We may need to multiply m by 2 in order to ensure that the second condition holds, i.e. that $p^{r(p)}$ is a square. Supposing that this condition holds, we get:

$$r(1) = -r(p) = \frac{24mp}{p-1} = \frac{24p}{\gcd(24p, p-1)}$$

and therefore:

$$f(z) = \left(\frac{\eta(z)}{\eta(pz)}\right)^{\frac{24p}{\gcd(24p,p-1)}}$$

giving the T-form:

$$T(z) = \left(\frac{\eta(pz)^p}{\eta(z)}\right)^{\frac{24}{\gcd(24p,p-1)}}$$

with vanishing order at infinity:

$$r = \frac{p^2-1}{\gcd(24p, p-1)}$$

and weight:

$$w = \frac{12(p-1)}{\gcd(24p, p-1)}.$$

We remark that Scholl's construction is not optimal, in the sense that it does not give the T-form with the lowest vanishing order at infinity. Recall the modular form defined in the proof of Theorem 4.4.4:

$$T(z) = \left(\frac{\eta(pz)^p}{\eta(z)}\right)^2$$

for a prime $p \geq 5$. It can easily be seen that this form T satisfies the properties of a T-form and has a vanishing order of $\frac{p^2-1}{12}$ at infinity and weight $p-1$. Moreover, we can show that this is the T-form with the lowest possible weight for $\Gamma_0(p)$:

Proposition 5.2.4. *Let $p \geq 5$ be a prime. The lowest weight in which one can find a T-form for $\Gamma_0(p)$ is $p-1$.*

Proof. Let T be the T-form:

$$T(z) = \left(\frac{\eta(pz)^p}{\eta(z)}\right)^2$$

in weight $p-1$. Suppose there exists a T-form T' of lower weight. By the defining properties of T-forms, it follows that T' divides T in the algebra of modular forms, and that $\frac{T}{T'} = T''$ is a T-form in weight $< p-1$. Then $T = T'T''$, but this contradicts Lemma 4.4.5. □

The existence of this T-form over $\mathbb{Z}$ in weight $p-1$ gives us an upper bound on the generating weight of the algebra $M(\Gamma_0(p), \mathbb{Z})$:

Corollary 5.2.5. *Let $p \geq 5$ be a prime. The algebra $M(\Gamma_0(p), \mathbb{Z})$ is generated in weight p^2+11.*

Proof. The vanishing order of the T-form in weight $p-1$ is $r = \frac{p^2-1}{12}$. Let $m_k = \dim_{\mathbb{C}} M_k(\mathrm{SL}_2(\mathbb{Z}))$. By the proof of Theorem 5.1.1, the algebra $M(\Gamma_0(p), \mathbb{Z})$ is generated in weight $d = \max\{k : m_k < r \text{ or } k \leq p-1\}$. By Proposition 1.2.11:

$$m_k = \begin{cases} \lfloor \frac{k}{12} \rfloor & k \equiv 2 \pmod{12}, \\ 1 + \lfloor \frac{k}{12} \rfloor & \text{otherwise.} \end{cases}$$

Hence $d = p^2 + 11$. □

5.3 Algorithms

Here we present algorithms to compute the structure of the algebras $M(\Gamma, A)$. Numerous examples are calculated explicitly using these algorithms, and the results are listed in Appendix A.

5.3.1 Generators

Once we have a T-form over A, we also have an algorithm to calculate a set of generators for $M(\Gamma, A)$, which we can ensure to be minimal if A is a PID. Note that by Theorems 4.3.7 and 3.4.4, when $(\Gamma, A) \in \{(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}]), (\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])\}$, one can substitute the halting condition 3 below by the appropriate bound provided by these theorems and ensure that the output is a full list of generators for the algebra.

Algorithm 5.3.1.

```
1. $r$ = vanishing order of $T$-form at infinity.
2. GENERATORS = $A$-basis of $M_2(\Gamma, A)$ (we know an integral basis exists).
3. for each ($k \in 2\mathbb{Z}$ if $\Gamma = \Gamma_0(N)$, $k \in \mathbb{Z}$ otherwise), $k > 2, m_k < r$:
    a) BASIS = $A$-basis of $M_k(\Gamma, A)$.
    b) MONOMIALS = homogeneous polynomials in the elements of GENERATORS
       of weight $k$ which form an $A$-rational basis for $F$, the $A$-submodule of
       $M_k(\Gamma, A)$ spanned by homogeneous monomials of GENERATORS of
       weight $k$.
```

c) *Express elements of MONOMIALS in terms of elements of BASIS. Using the Smith normal form algorithm, find a new A-rational basis* $D = \{y_1, \cdots, y_n\}$ *for* $M_k(\Gamma, A)$*, and elements* $a_1, \cdots, a_m \in A$*,* $m \leq n$ *such that* $\{a_1y_1, \cdots, a_my_m\}$ *spans F. Add the elements of D which are not in F to GENERATORS.*

Theorem 5.3.2. *For A a PID, Algorithm 5.3.1 outputs a minimal list of generators for* $M(\Gamma, A)$*.*

Proof. Each generator added for each weight is indispensable. Since we are adding generators while increasing the weight, we have a minimal list of generators. □

Remark 5.3.3. *For Algorithm 5.3.1 to run as fast as possible, we should choose the T-form with the least possible order of vanishing at infinity.*

Remark 5.3.4. *A trick can be used to make the algorithm run much faster. For the sake of giving a concrete example, let us suppose we are working with the congruence subgroup* $\Gamma_0(p)$*, for prime* $p \geq 5$*. At each iteration, say for weight k, we can perform the following check. We let S be the set of the vanishing orders of all the homogeneous monomials in the elements of GENERATORS of weight k whose first non-zero coefficient is a unit in A. If S contains all integers from 0 up to and including the vanishing order of the T-form, then by taking suitable linear combinations, we can always divide by T to reduce the case to a lower weight. Since* $M_2(\Gamma_0(p), \mathbb{Z})$ *is not empty, and always contains a modular form which is non-vanishing at infinity (for example, an Eisenstein series), it would follow that for any higher weight, the situation described above will still be true, we can again reduce the case to a weight lower than k, and hence we can halt the algorithm.*

5.3.2 Relations

We describe an algorithm that calculates the relations of degree at most d for generators of the algebras $M(\Gamma, A)$ where $\Gamma \in \{\Gamma_0(N), \Gamma_1(N)\}$ and A is a PID. These generators can for example be obtained using Algorithm 5.3.1. Note that by Theorems 4.3.7 and 3.4.4, when $(\Gamma, A) \in \{(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}]), (\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])\}$, we can choose d so that the algorithm outputs a list of generators for the whole ideal of relations.

Algorithm 5.3.5.

```
1. GENERATORS = $\{g_1, \cdots, g_r\}$ list of generators for $M(\Gamma_1(N), A)$.
2. RELATIONS = $\{\}$.
3. for each ($k \in 2\mathbb{Z}$ if $\Gamma = \Gamma_0(N)$, $k \in \mathbb{Z}$ otherwise), $k \leq d$:
```

a) B = integral basis of $M_k(\Gamma, A)$.

b) $M = \begin{pmatrix} m_1 \\ \vdots \\ m_s \end{pmatrix}$, the monomials of weight k in the elements of $GENERATORS$.

c) Express elements of M as an integral linear combination of elements of B, obtaining an integral matrix C such that $M = CB$.

d) Calculate D, the Smith Normal Form of the matrix C, as well as the transformation matrices U and V, such that $D = UCV$.

e) For every diagonal entry D_{ii} of D, check if D_{ii} is invertible in A:

   - if D_{ii} is not invertible in A, then the ith row of UCB is a relation. Add it to $RELATIONS$.

f) For every row D_j of D:

   - if D_j is a zero row, then the jth row of UCB is a relation. Add it to $RELATIONS$.

4. Represent each generator g_i as a variable x_i. Find the ideal I of $A[x_1, \cdots, x_r]$ generated by $RELATIONS$. This is the ideal of relations. Output a Gröbner basis for I.

Chapter 6

Modular forms modulo p^m

In this chapter, we explore some questions related to the reductions of modular forms modulo p^m. The exposition is based on [CKW13] and [CK14]. The discussion of the θ_{p^m} cycles has not appeared elsewhere.

6.1 Congruences between modular forms

Let p be a prime number, and fix an algebraic closure $\overline{\mathbb{Q}}_p$, and an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$. Let v_p be the normalised p-adic valuation on $\overline{\mathbb{Q}}_p$ (i.e. $v_p(p) = 1$). We define:

$$\overline{\mathbb{Z}/p^m\mathbb{Z}} = \overline{\mathbb{Z}}_p/\{x \in \overline{\mathbb{Z}} : v_p(x) > m-1\}.$$

Note that when $m = 1$, then modulo p means modulo a prime ideal $\mathfrak{p}$ over p of some extension of $\mathbb{Q}_p$. This definition is also invariant under field extensions.
For $a, b \in \overline{\mathbb{Z}}_p$, we say that $a \equiv b \pmod{p^m}$ if the images of a and b in $\overline{\mathbb{Z}/p^m\mathbb{Z}}$ coincide. Equivalently, if a and b lie in the ring of integers $\mathcal{O}_K$ of some extension $K/\mathbb{Q}_p$, then $a \equiv b \pmod{p}$ means that:

$$a - b \in \mathfrak{p}^{e(m-1)+1}$$

where e is the ramification index. Note that for $a, b \in \mathbb{Z}_p$, this notion coincides with the usual notion of congruence modulo p^m. By "reducing modulo p^m", we understand taking the image under the natural map $\overline{\mathbb{Z}}_p \twoheadrightarrow \overline{\mathbb{Z}/p^m\mathbb{Z}}$.

Let $\Gamma \in \{\Gamma_0(N), \Gamma_1(N)\}$ be a congruence subgroup, and suppose that $p \nmid N$.

Definition 6.1.1. *A modular form modulo p^m of weight k for Γ is the reduction modulo p^m of the q-expansion of a modular form in $M_k(\Gamma, \overline{\mathbb{Z}}_p)$, and we denote the space of these modular forms by $M_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$. Similarly, a cuspidal modular* *form modulo p^m is the reduction modulo p^m of the q-expansion of a cuspidal modular form, and we denote the space of these modular forms by $S_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$. If*

$$f = \sum_{n\geq 0} a_n q^n \in M_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$$

and

$$g = \sum_{n\geq 0} b_n q^n \in M_{k'}(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}}).$$

We say that f and g are congruent mod p^m, and we write:

$$f \equiv g \pmod{p^m}$$

if $a_n \equiv b_n$ for all $n \geq 0$.

Note the inclusion $\mathbb{Z}/p^m\mathbb{Z} \hookrightarrow \overline{\mathbb{Z}/p^m\mathbb{Z}}$, which gives an embedding:

$$M_k(\Gamma, \mathbb{Z}/p^m\mathbb{Z}) \hookrightarrow M_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}}),$$

where $M_k(\Gamma, \mathbb{Z}/p^m\mathbb{Z}) = M_k(\Gamma, \mathbb{Z}) \otimes \mathbb{Z}/p^m\mathbb{Z}$ as defined in 2.1.2. Congruences between modular forms force congruences on the weights, as we see in the following theorem ([Ser73b]).

Theorem 6.1.2. *Let $f \in M_k(\Gamma, \mathbb{Z}_p)$, and $g \in M_{k'}(\Gamma, \mathbb{Z}_p)$, and suppose we have a congruence:*

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

Then we have a congruence on the weights:

$$k \equiv k' \begin{cases} \pmod{p^{m-1}(p-1)} & p \geq 3 \\ \pmod{2^{m-2}} & p = 2. \end{cases}$$

Now let $p \geq 5$, and let E_{p-1} be the level 1 Eisenstein series of weight $p-1$. Recall Deligne's congruence:

$$E_{p-1} \equiv 1 \pmod{p}.$$

This gives us, for each $m \geq 1$, a congruence:

$$E_{p-1}^{p^{m-1}} \equiv 1 \pmod{p^m}.$$

Therefore, multiplication by $E_{p-1}^{p^m}$ induces an embedding:

$$M_k(\Gamma, \mathbb{Z}/p^m\mathbb{Z}) \hookrightarrow M_{k+p^{m-1}(p-1)}(\Gamma, \mathbb{Z}/p^m\mathbb{Z}).$$

This observation, combined with Theorem 6.1.2, gives the following:

Proposition 6.1.3. *Let $p \geq 5$. Let $f \in M_k(\Gamma, \mathbb{Z}_p)$, and $g \in M_{k'}(\Gamma, \mathbb{Z}_p)$, where $k' \geq k$. Then we have a congruence:*

$$f \equiv g \pmod{p^m}$$

if and only if there exists a non-negative integer $a \geq 0$ such that

$$k' = k + ap^{m-1}(p-1)$$

and:

$$fA^a \equiv g \pmod{p^m}$$

where $A = E_{p-1}^{p^{m-1}}$.

We now make the following definition:

Definition 6.1.4. *Let $f \in M_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$. The mod p^m filtration of f is the number:*

$$w_{p^m}(f) = \inf\{j : f \in M_j(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})\}.$$

If $g \in M_k(\Gamma, \overline{\mathbb{Z}}_p)$, then we define the mod p^m filtration $w_{p^m}(g)$ of g to be the mod p^m filtration of its reduction modulo p^m.

Let us examine these concepts from a geometric point of view, for modular forms mod p. Let $p \geq 5$, and $\Gamma = \Gamma_1(N)$ for $N \geq 5$, with $p \nmid N$. Recall (Section 3.2) that modular forms mod p of weight k for $\Gamma_1(N)$ are global sections of an invertible sheaf $\omega_{\mathbb{F}_p}^{\otimes k}$ on the modular curve $X_1(N)_{\mathbb{F}_p}$. In the proof of Lemma 3.4.1, we made use of a special modular form mod p, which is the Hasse invariant A: it is the unique modular form mod p of weight $p-1$ which has simple zeros at the supersingular points and vanishes nowhere else. One can show ([Kat73], Section 2.0) that q-expansion of A is 1 at all cusps. Hence Deligne's congruence:

$$E_{p-1} \equiv 1 \pmod{p}$$

and the q-expansion principle (Theorem 3.2.2) tell us that E_{p-1} is a lift of A. Therefore if $f \in M_k(\Gamma_1(N), \mathbb{F}_p)$ is a mod p modular form, then $w_p(f) = k$ if and only if f is not divisible by A in the algebra $M(\Gamma_1(N), \mathbb{F}_p)$ of mod p modular forms. Equivalently, if t is the highest power of A dividing f in $M(\Gamma_1(N), \mathbb{F}_p)$, then $w_p(f) = k - t(p-1)$.

6.2 Weak and strong eigenforms mod p^m

Fix a congruence subgroup $\Gamma \in \{\Gamma_0(N), \Gamma_1(N)\}$, and a prime p not dividing N. We define Hecke operators modulo p^m.

Definition 6.2.1. *Let $f = \sum_{n\geq 0} a_n q^n \in M_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$. For a positive integer n, the Hecke operator T_n modulo p^m is the reduction* of the Hecke operator T_n acting on $M_k(\Gamma, \mathbb{Z})$.*

Following [CKW13], we make the following definition. Let $\Gamma \in \{\Gamma_0(N), \Gamma_1(N)\}$, and $p \nmid N$.

Definition 6.2.2. *Let $f = q + \sum_{n\geq 2} a_n q^n \in S_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$. We say that f is:*

- *a strong Hecke eigenform of weight k, level N, over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$, if there exists a Hecke eigenform $\tilde{f} \in S_k(\Gamma, \overline{\mathbb{Z}}_p)$ that reduces to f modulo p^m;*
- *a weak Hecke eigenform of weight k, level N, over $\overline{\mathbb{Z}/p^m\mathbb{Z}}$, if there is a sequence $\{\lambda_\ell\}_{(\ell \text{ prime })} \subset \overline{\mathbb{Z}/p^m\mathbb{Z}}$ such that $T_\ell(f) = \lambda_\ell f$ for all primes ℓ.*

The notions of weak and strong eigenforms coincide when $m = 1$ by the Deligne-Serre lifting lemma ([DS74], Lemma 6.11):

Lemma 6.2.3 (Deligne-Serre liting lemma)**.** *Let $f \in M_k(\Gamma, \overline{\mathbb{F}}_p)$ be a weak eigenform. Then f is also a strong eigenform, i.e. there exists a lift $\tilde{f}$ of f to $M_k(\Gamma, \overline{\mathbb{Z}}_p)$ which is a normalised eigenform for all Hecke operators.*

Proof. For a proof in the context of modular forms, see [CKW13], Lemma 16. □

When $m \geq 2$ however, the lifting lemma fails: there exists weak eigenforms mod p^m with $m \geq 2$ that are not strong. We will refer to these as strictly weak eigenforms, and we will give some examples.

A fundamental result in the theory of mod p modular forms is the following theorem (see [Joc82a], Theorem 2.2, and [Joc82b], Lemma 4.4):

Theorem 6.2.4. *Let $f \in M_k(\Gamma, \overline{\mathbb{F}}_p)$ be an eigenform. Then $w_p(f) \leq p^2 + p$, and so there are finitely many congruence classes of eigenforms modulo p.*

We call the statement "$w_p(f) \leq p^2 + p$ for any mod p eigenform f" a weight bound mod p, and the statement "there are finitely many congruence classes of eigenforms modulo p" a finiteness statement. Note that a weight bound implies a finiteness statement mod p only because of the Deligne-Serre liting lemma (and the fact that in characteristic 0 there are only finitely many normalised eigenforms of a given weight).

We are interested in the extent to which Theorem 6.2.4 can be generalised in the context of modular forms modulo p^m with $m \geq 2$. Thanks to work of Hatada ([Hat77], Theorems 3 and 4), we know the following in the case of modular forms of level 1 modulo 2^m, where $m \in \{1, 2, 3\}$:

*Because of the existence of an integral structure on $M_k(\Gamma)$, we know that there is a matrix representation of T_n with entries in $\mathbb{Z}$.

Theorem 6.2.5 (Hatada)**.** *Let $f \in S_k(SL_2(\mathbb{Z}), \overline{\mathbb{Z}}_2)$ be a normalised eigenform. For each Hecke operator T_p, let λ_p be the eigenvalue of T_p associated to f. Then:*

$$\lambda_p \equiv \begin{cases} 0 \pmod 8 & p = 2, \\ 1 + p \pmod 8 & p > 2. \end{cases}$$

Corollary 6.2.6. *There are finitely many (only one) congruence classes of eigenforms for $SL_2(\mathbb{Z})$ modulo 2^m for $m \in \{1, 2, 3\}$.*

So for the case $N = 1$, $p = 2$, $m \in \{1, 2, 3\}$, we have a finiteness statement. However, one can show that, for any $m \geq 2$, there are infinitely many weak eigenforms. In fact, if one picks two normalized eigenforms $f, g \in S_k(\Gamma_1(N), \overline{\mathbb{Z}}_p)$ such that:

$$f \equiv g \pmod p,$$
$$f \not\equiv g \pmod{p^2},$$

then:

$$\{\frac{\alpha f + \beta g}{\alpha + \beta} : (\alpha, \beta) \in (\overline{\mathbb{Z}}_p^{ur})^2 \text{ and } \alpha + \beta \text{ invertible } \},$$

where $\overline{\mathbb{Z}}_p^{ur}$ is the maximal unramified extension of $\overline{\mathbb{Z}}_p$, is an infinite set of weak eigenforms modulo p^m, only finitely many of which can lift to eigenforms in characteristic 0 and weight k (see [CE04]).

In [CKW13], an explicit example is given of a weak eigenform that is not strong *at the same weight*, meaning a modular form $f \in M_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$ that is a weak eigenform and that is not the reduction of any normalised eigenform in $M_k(\Gamma, \overline{\mathbb{Z}}_p)$. The question is raised concerning whether the notions of strong and weak eigenforms at a fixed level coincide in general when the weight is allowed to vary. That is, f might not be strong at weight k, but it might in general be congruent to a strong eigenform g at a different weight. We show that the answer to this question is negative: there exists weak eigenforms that do not lift at any weight.

Corollary 6.2.7. *The modular form $f \in M_{42}(SL_2(\mathbb{Z}), \overline{\mathbb{Z}/2^2\mathbb{Z}})$ given by*

$$f = E_4^6\Delta + 2\Delta^3 \pmod 4$$

is a weak eigenform of level 1 mod 2^2 which is not congruent to any strong eigenform of level 1 mod 2^2 at any weight.

Proof. By Hatada's theorem (6.2.5), any strong eigenform modulo 2^2 must be congruent to Δ. Hence it is obvious that f is not a strong eigenform. It remains to check that f is indeed a weak eigenform. Using a computer, we check that f is an eigenform for the Hecke operators T_2, T_3, T_5:

$$T_2(f) = 0,$$

$$T_3(f) = T_5(f) = 2f.$$

The Sturm bound ([Kil08], Theorem 3.13) then implies that f is an eigenform for all Hecke operators. □

6.3 The θ operator

6.3.1 modulo p

The Ramanujan θ operator:

$$\theta := q\frac{d}{dq} = \frac{1}{2\pi i}\frac{d}{dz}$$

has the following effect on q-expansions:

$$\theta(\sum_{n\geq 0} a_n q^n) = \sum_{n\geq 1} n a_n q^n.$$

However, θ destroys modularity: if f is a modular form, then $\theta(f)$ is not a modular form, as it does not transform the right way (Proposition 2.28, [Kil08]). One can adjust for the loss of modularity, and obtain a differential operator on modular forms:

$$\partial := \partial_k := 12\theta - kE_2.$$

Then one finds that ∂f is again a modular form of weight $k+2$, with the same ring of coefficients. The Eisenstein series:

$$E_2 = 1 - 24\sum_{n\geq 1}\sigma(n)q^n$$

is not a classical modular form. However, it is a p-adic modular form, meaning that there exists an increasing sequence k_i of non-negative integers, and p-integral modular forms G_{k_i} of weight k_i for each i, such that ([Ser73b], §2):

$$E_2 \equiv G_{k_i} \pmod{p^i}.$$

For the rest of this section, fix a prime $p \geq 5$. One finds that:

$$E_2 \equiv E_{p+1} \pmod{p}.$$

More generally:

Proposition 6.3.1 (Chen, Kiming [CK14]). *Let $m \geq 2$. Then for $j \in \{0 \cdots m-1\}$, there exists modular forms $f_j \not\equiv 0 \pmod{p}$, of level 1 and coefficients in $\mathbb{Z}/p^m\mathbb{Z}$, and weights:*

$$k_j := \begin{cases} 2 + p^{m-j-2}(p^{j+1}-1) & j \in \{0 \cdots m-2\} \\ p^{m-1}(p-1) & j = m-1, \end{cases}$$

such that:

$$E_2 \equiv -24 \sum_{j=0}^{m-1} p^j f_j.$$

Moreover, f_{m-1} can be chosen to be $f_{m-1} = cE_{p+1}^{p^{m-1}}$ for some normalising constant c.

Thus the θ operator induces a differential operator on mod p^m modular forms. For $m = 1$, we have:

$$\theta_p : M_k(\Gamma, \mathbb{F}_p) \to M_{k+p+1}(\Gamma, \mathbb{F}_p)$$

$$f \mapsto \frac{1}{12}\partial f E_{p-1} - \frac{k}{12}E_{p+1}f.$$

Similarly, for $m \geq 2$, we have:

Theorem 6.3.2 (Chen, Kiming [CK14])**.** *The Ramanujan theta operator induces, for each $m \geq 2$, operators:*

$$\theta_{p^m} : M_k(\Gamma, \mathbb{Z}/p^m\mathbb{Z}) \to M_{k+k(p)}(\Gamma, \mathbb{Z}/p^m\mathbb{Z})$$

where $k(p) = 2 + 2p^{m-1}(p-1)$. Moreover, the following commutation rule holds for every primes ℓ:

$$T_\ell \circ \theta_{p^m} = l\theta_{p^m} \circ T_\ell.$$

A well known fact from the classical theory of mod p modular forms is the following:

Theorem 6.3.3. *Let f be a mod p modular form of weight k. Then:*

$$w_p(\theta f) \leq w_p(f) + p + 1,$$

with equality if and only if $w_p(f) \not\equiv 0 \pmod{p}$.

Proof. A proof in the case of level 1 is given in [Ser73a], and generalised for higher levels in [Kat77]. □

It is clear from the effect of the θ_{p^m} operator on q-expansions (and by Fermat's little theorem) that one have the equality in q-expansions:

$$\theta_{p^m}^{\varphi(p^m)} f = \theta_{p^m} f$$

for any $f \in M(\Gamma, \mathbb{Z}/p^m\mathbb{Z})$ where φ is the Euler totient function. Hence we make the following definition:

Definition 6.3.4. *Let $f \in M_k(\Gamma, \mathbb{Z}/p^m\mathbb{Z})$. The θ_{p^m}-cycle of f is the following sequence of integers:*

$$(w_{p^m}(\theta_{p^m} f), w_{p^m}(\theta_{p^m}^2 f), \cdots, w_{p^m}(\theta_{p^m}^{\varphi(m)} f)).$$

When $m = 1$, θ_p cycles can take a limited number of forms. The structure theorem for θ_p-cycles is described in [Joc82b], Section 7. In particular:

Proposition 6.3.5. *Let $f \in M_k(\Gamma, \mathbb{Z}/p^m\mathbb{Z})$. If $i \in \{1 \cdots \varphi(p^m)\}$ is such that $w_{p^m}(\theta_{p^m}^{i+1} f) < w_{p^m}(\theta_{p^m}^{i} f)$, we say that i is a drop in the θ_{p^m} cycle. If $m = 1$, then for any modular form f mod p, there is at most one drop in the θ_p cycle of f.*

The operator θ_p plays a central role in the theory of modular forms mod p, and in [Joc82a], it is the key to proving the finiteness statement for eigenforms mod p. In [Edi92], θ_p cycles, are involved in Edixhoven's study of the weights in Serre's conjectures, where he proved that the weak and strong forms of Serre's conjecture are equivalent. Therefore it is natural to wonder about whether the operators θ_{p^m} for $m \geq 2$ behave as nicely as in the case of $m = 1$. We will see however that their behaviour is more complicated.

6.3.2 modulo p^m

The θ operator modulo p^m was studied by Ian Kiming and Imin Chen in [CK14]. In Section 6.3.1 above, we saw that when $m \geq 2$, the mod p^m theta operator $\theta := \theta_{p^m}$ increases the weight by $2 + 2p^{m-1}(p-1)$, while the mod p theta operator θ_p increases the weight by $p + 1 = 2 + \varphi(p)$. In view of Theorem 6.3.3, one might expect the generalization to be:

$$w_{p^m}(\theta f) \leq w_{p^m}(f) + 2 + \varphi(p^m) = w_{p^m}(f) + 2 + p^{m-1}(p-1).$$

This however turns out to be false. The following lemma is a previous version of Lemma 3 in [CK14], and which was generalised by Chen and Kiming to all levels.

Lemma 6.3.6. *Let $N \geq 5$, and $b \in M_\kappa(\Gamma_1(N), \mathbb{F}_p)$, $b \neq 0$, and $w_p(b) = \kappa$. Then:*

$$w_p(E_{p+1} b) = w_p(b) + p + 1.$$

Proof. As in Section 3.2, we regard our modular forms E_{p-1}, E_{p+1}, and b respectively as sections of the invertible sheaves $\omega_{\mathbb{F}_p}^{\otimes(p-1)}$, $\omega_{\mathbb{F}_p}^{\otimes(p+1)}$, and $\omega_{\mathbb{F}_p}^{\otimes\kappa}$ on the fine modular scheme $X_1(N)_{\mathbb{F}_p}$. Then E_{p-1} is the Hasse invariant, and vanishes precisely at the supersingular points of $X_1(N)_{\mathbb{F}_p}$. Note that the filtration requirement on b means that b is not divisible by E_{p-1} in the algebra $M(\Gamma_1(N), \mathbb{F}_p)$, i.e. b must be invertible at some supersingular point. Since the weight of $E_{p+1}b$ is $\kappa + p + 1$, it suffices to prove that E_{p+1} is invertible on the supersingular locus of $X_1(N)_{\mathbb{F}_p}$. We have the following identity ([Ser73a], Exemple after Théorème 4):

$$\theta_p \Delta \equiv E_{p+1} \Delta \pmod{p}.$$

Therefore it is enough to show that the equality of orders of vanishing: $\mathrm{ord}_x(\theta_p \Delta) = \mathrm{ord}_x(\Delta)$ (which is 0, although we won't use this). By Katz' local description of the action of θ_p (see [Kat77], last statement in the proof of Part (1) of Theorem), and looking at the orders of vanishing of $\theta_p\Delta$ and Δ at every supersingular point x, we have:

$$\mathrm{ord}_x(\theta_p\Delta) = \mathrm{ord}_x(\Delta B)$$

($12 \not\equiv 0 \pmod p$ as $p \geq 5$) where B (Katz' notation) is a function which is invertible (Remark on p. 57 of loc. sit.) on the supersingular locus, and so $\mathrm{ord}_x(\theta_p\Delta) = \mathrm{ord}_x(\Delta)$ and $\mathrm{ord}_x(E_{p+1}) = 0$. □

One can use Lemma 6.3.6 to prove the following theorem in the case where $N \geq 5$.

Theorem 6.3.7 (Chen, Kiming)**.** *Let $N \geq 1$. Suppose that $f \in M_k(\Gamma_1(N), \mathbb{Z}_p)$, $f \not\equiv 0 \pmod p$, and that $w_p(f) = k \not\equiv 0 \pmod p$. Then:*

$$w_{p^m}(\theta f) = w_{p^m}(f) + 2 + 2p^{m-1}(p-1).$$

Proof. We sketch a proof for congruence subgroups $\Gamma_1(N), N \geq 5$. For ease of notation, let $w := w_{p^m}$, $\theta := \theta_{p^m}$, and $k(m) = 2 + 2p^{m-1}(p-1)$. Suppose that $w(\theta f) = k' < w(f) + 2 + \varphi(p^m)$, i.e. there exists $g \in M_{k'}(\Gamma_1(N), \mathbb{Z}_p)$ such that $f \equiv g \pmod{p^m}$. By Theorem 6.1.2, we know that:

$$k' \equiv k + k(m) \pmod{p^{m-1}(p-1)},$$

say $k + k(m) = k' + tp^{m-1}(p-1)$ with $t \geq 1$. Define:

$$h := E_{p-1}^{p^{m-1}} g.$$

Then θf and $E_{p-1}^{p^{m-1}}$ have the same weight, and:

$$\theta f \equiv E_{p-1}^{p^{m-1}}.$$

Combining this identity with Proposition 6.3.1,

$$2kp^{m-1}E_{p-1}^{t_{m-1}} f_{m-1} f \equiv E_{p-1}^{p^{m-1}} h + \frac{1}{12} E_{p-1}^{2p^{m-1}} \partial f - 2kf \sum_{j=0}^{m-2} p^j E_{p-1}^{t_j p^{m-j-1}} f_j \pmod{p^m}$$

where the numbers t_j, defined by:

$$t_j := \frac{k(m) - k_j}{p^{m-j-1}(p-1)}$$

are integers since $k(m) \equiv k_j \pmod{p^{m-j-1}(p-1)}$. Now it can easily be checked that:

$$t_{m-1} < \min\{p^{m-1}, p^{m-j-1}t_j\}$$

for $j \in \{0 \cdots m-2\}$. We deduce that:

$$p^{m-1}E_{p-1}^{t_{m-1}} f_{m-1} f \equiv E_{p-1}^{tm-1+1} h' \pmod{p^m}$$

where h' has weight $k + k(m) - (p-1)(t_{m-1}+1)$. We now have that $h' \equiv 0 \pmod{p^{m-1}}$, hence there exists h'' of weight $k + k(m) - (p-1)(t_{m-1}+1)$ such that $h'' \not\equiv 0 \pmod{p}$, and:

$$f_{m-1} f \equiv E_{p-1} h''.$$

Recalling that f_{m-1} is a constant times $E_{p+1}^{p^{m-1}}$, it follows that:

$$w_p(E_{p+1}^{p^{m-1}} f) < k + p^{m-1}(p+1).$$

Since $w_p(f) = k$, this contradicts Lemma 6.3.6. □

In Section 6.3.1, we also saw that the θ_p cycles for mod p modular forms have a simple structure, which is independent of the prime p. We ask whether this is still true modulo p^m where $m \geq 2$.

To compute the θ_{p^m} cycle for a modular form mod p^m, we make use of the fact that θ_{p^m} is a derivation on the algebra of $\overline{\mathbb{Z}/p^m\mathbb{Z}}$ modular forms, that is, for any two modular forms $f, g \in M_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$, we have:

$$\theta_{p^m}(f+g) = \theta_{p^m} f + \theta_{p^m} g,$$

and, if $f \in M_k(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$ and $g \in M_{k'}(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$:

$$\theta_{p^m}(fg) = \theta_{p^m}(f) g + f \theta_{p^m}(g).$$

The procedure is as follows, for a modular form $f \in M(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$ and $p \geq 5$:

Algorithm 6.3.8.

1. *Find generators and relations for the algebra $M(\Gamma, \overline{\mathbb{Z}/p^m\mathbb{Z}})$ (For example, using Algorithms 5.3.1 and 5.3.5).*

2. *Compute the action of θ_{p^m} on the generators.*

3. *Represent the modular form f as a polynomial F in the generators.*

4. *Represent the Hasse invariant (as $p \geq 5$, this is the reduction mod p^m of E_{p-1}) as a polynomial A in the generators.*

5. *Compute the representation F_i of the iteration $\theta_{p^m}^i$ as a polynomial in the generators by using the fact that θ_{p^m} is a derivation, this is a simple algebraic operation.*

6. *Compute the highest power t of A dividing F_i, modulo the ideal of relations between the generators. Thus $w_{p^m}(\theta_{p^m}^i) = \deg F_i - t\varphi(p^m)$.*

Computation results for θ_{p^2}-cycles of Δ modulo p^2 in level 1 displayed in Section A.5 suggests that the number of drops increases with p. Therefore, we do not expect that any simple classification of θ-cycles modulo higher powers similar to that of the case of modulo p should exist.

The θ_{p^m} operator can be used to find weak eigenforms that are not strong at the same weight. For example, consider the reduction modulo 5^2 of the modular discriminant Δ. By using Algorithm 6.3.8, one can calculate that:

$$w_{5^2}(\theta_{5^2}^{12}(\Delta)) = 76.$$

The form $\theta_{5^2}^{12}(\Delta)$ is a weak eigenform by Theorem 6.3.2. Inspecting the mod 5^2 weight filtrations of the Hecke eigenforms in $M_{76}(\mathrm{SL}_2(\mathbb{Z}), \overline{\mathbb{Q}})$, we find that they all have filtrations at most 56. We suspect that $\theta_{5^2}^{12}(\Delta)$ does not lift at any weight. This might be checked in the future once the weak weight bounds in Theorem 7.2.1 are made explicit.

Chapter 7

Weight bounds modulo p^m

In this chapter, we prove the existence of weight bounds on the filtrations of mod p^m weak eigenforms. We discuss a connection between these results and a question of Buzzard. This is based on joint work with Ian Kiming and Gabor Wiese ([KRW14]).

7.1 Weak weight bounds in the case $N = 1, p = 2$

In this section, we will prove a weight bound for eigenforms modulo 2^m, $m \geq 1$. We will use the following notation: $Q := E_4$ and $R := E_6$. By Theorem 2.3.3, the reductions of Q, R, and Δ generate the algebra $M(\mathrm{SL}_2(\mathbb{Z}), \overline{\mathbb{Z}/2^m\mathbb{Z}})$. Thus if $f \in M_k(\mathrm{SL}_2(\mathbb{Z}), \overline{\mathbb{Z}/2^m\mathbb{Z}})$, we can write:

$$f = \sum_{4a+12c=k} \alpha_{a,c} Q^a \Delta^c$$

if $k \equiv 0 \pmod 4$, and:

$$f = R \cdot \sum_{4a+12c=k-6} \alpha_{a,c} Q^a \Delta^c$$

if $k \equiv 2 \pmod 4$. By Proposition 2.3.1, the coefficients $\alpha_{a,c}$ are uniquely determined. We make the following definition:

Definition 7.1.1. *Let $f \in S_k(SL_2(\mathbb{Z}), \overline{\mathbb{Z}/2^m\mathbb{Z}})$. The degree* $\deg_m f$ *of f is the highest power of Δ occurring in the expansion of f as above. In situations where m does not vary and it is clear what it is, we may suppress the m from the notation and just write* $\deg f$ *for* $\deg_m f$*.*

In joint work with Ian Kiming and Gabor Wiese ([KRW14]), we prove the following:

Theorem 7.1.2. *There exists a constant $C(m)$ depending only on m such that whenever $f \in S_k(SL_2(\mathbb{Z}), \overline{\mathbb{Z}/2^m\mathbb{Z}})$ is a weak eigenform then:*

$$\deg_m f \leq C(m).$$

Any such form is the reduction modulo 2^m of a form of weight bounded by a constant $\kappa(m)$ depending only on m, that can be taken to be $12C(m)$ for $m = 1, 2, 3$, and to be $6 + 2^{m-2} + 12C(m)$ if $m \geq 4$.

We will give the proof. Recall Hatada's theorem, stated here as Theorem 6.2.5. Combined with the Deligne-Serre lifting lemma (Lemma 6.2.3), we obtain the following corollary.

Corollary 7.1.3. *Suppose that f is a weak eigenform modulo 2 on $SL_2(\mathbb{Z})$. Then $f \equiv \Delta \pmod 2$ and the T_p eigenvalue attached to f is 0 mod 2 for any prime p.*

Proof. Clearly, the reduction mod 2 of weak eigenform f is a weak eigenform. By the Deligne-Serre lifting lemma, f mod 2 is also a strong eigenform. Thus Theorem 6.2.5 shows that every T_p eigenvalue attached to f is 0 mod 2. □

7.1.1 Serre-Nicolas codes

In this subsection we work exclusively with modular forms mod 2 on $\mathrm{SL}_2(\mathbb{Z})$. As $Q \equiv R \equiv 1 \pmod 2$, the algebra of modular forms mod 2 of level 1 is $\mathbb{F}_2[\Delta]$. We call an element of $\mathbb{F}_2[\Delta]$ even resp. odd if the occurring powers of Δ all have even resp. odd exponents. By [NS12], Section 2.2, the subspaces of even and odd elements are both invariant under the action of every Hecke operator T_ℓ where ℓ is an odd prime. If $f \in \mathbb{F}_2[\Delta]$ we can write, in a unique fashion:

$$f = f_e + f_o$$

where f_e and f_o are even and odd, respectively. On the basis of results in [NS12], particularly Section 4, we obtain the following result.

Proposition 7.1.4. *For every odd integer $k \geq 0$, there exists a constant $N(k)$ depending only on k such that, whenever $f \in \mathbb{F}_2[\Delta]$ is odd with*

$$\sup\{\deg T_3(f), \deg T_5(f)\} \leq k,$$

then:

$$\deg f \leq N(k).$$

We need to recall some definitions from [NS12], Section 4.

Definition 7.1.5. *Let $k \geq 0$ be an integer, and write it in a binary expansion: $k = \sum_{i=0}^{\infty} \beta_i 2^i$. Define:*

$$n_o(k) := \sum_{i=0}^{\infty} \beta_{2i+1} 2^i,$$

$$n_e(k) := \sum_{i=0}^{\infty} \beta_{2i+2} 2^i,$$

$$h(k) := n_o(k) + n_e(k).$$

The ordered pair $[n_o(k), n_e(k)]$ is called the code of k, and we denote it by $\mathrm{co}\,(k)$.

The map $k \mapsto \mathrm{co}\,(k)$ defines a bijection between the set of odd (resp. even) non-negative integers and $(\mathbb{Z}_{\geq 0})^2$. Note that $n_o(2l+1) = n_o(2l)$, $n_e(2l+1) = n_e(2l)$, and $h(2l+1) = h(2l)$.

Definition 7.1.6. *If $k, l \geq 0$ are integers, then we say l dominates k, and we write $k \prec l$ or $l \succ k$ if we have $h(k) < h(l)$, or $h(k) = h(l)$ and $n_e(k) < n_e(l)$. We say that $\mathrm{co}\,(k) \preceq \mathrm{co}\,(l)$ if $k \preceq l$.*

The relation $\preceq$ thus defined is a total order on the set of odd (resp. even) non-negative integers, and is a total order on the set of codes.

Definition 7.1.7. *Suppose that $0 \neq f = \Delta^{m_1} + \Delta^{m_2} + \cdots + \Delta^{m_r} \in \mathbb{F}_2[\Delta]$ is odd, i.e., all m_i are odd. Assume that:*

$$m_1 \preceq m_2 \preceq \cdots \preceq m_r.$$

We then define $\mathrm{dom}\,(f) := m_r$ and we call it the dominant exponent of f. We also define:

$$\mathrm{co}\,(f) := \mathrm{co}\,(\mathrm{dom}\,(f)),$$

$$n_o(f) := n_o(\mathrm{dom}\,(f)),$$

$$n_e(f) := n_e(\mathrm{dom}\,(f)),$$

$$h(f) := h(\mathrm{dom}\,(f)).$$

If $f = 0$ we define all of the above quantities to be 0.

Proposition 7.1.8 (Serre-Nicolas)**.** *Let $0 \neq f \in \mathbb{F}_2[\Delta]$ be odd. Then:*

1. *If $n_o(f) \geq 1$ then $\mathrm{co}\,(T_3(f)) = [n_o(f) - 1, n_e(f)]$ and $h(T_3(f)) = h(f) - 1$.*
2. *If $n_e(f) \geq 1$ then $\mathrm{co}\,(T_5(f)) = [n_o(f), n_e(f) - 1]$ and $h(T_5(f)) = h(f) - 1$.*

The Proposition follows by combining Propositions 4.3 and 4.4 of [NS12].

Proof of Proposition 7.1.4. If $n_o(f) = n_e(f) = 0$ then $\mathrm{co}\,(f) = [0,0]$, and hence $\mathrm{dom}\,(f) = 1$, i.e. $f = \Delta$. If we take care to ensure that our definition $N(k)$ is such that $N(k) \geq 1$ in any case, we may thus assume that $h(f) = n_o(f) = n_e(f) \geq 1$.

Assume now that $\sup\{\deg T_3(f), \deg T_5(f)\} \leq k$ for some odd, positive integer k.

Case 1: $n_o(f) \geq 1$. Define $\phi(l)$ to be the unique odd non-negative integer with code $[n_o(l)+1, n_e(l)]$. Then it is easy to check that whenever $l \preceq l'$, we have $\phi(l) \preceq \phi(l')$.

We have $\mathrm{dom}\,(f) = \phi(l)$ for some odd l. By Proposition 7.1.8, we see that then $\mathrm{dom}\,(T_3(f)) = l$ so that $l \leq k$. Let s be the supremum of the set $\{1, 3, 5\cdots, k\}$ with respect to the order relation $\preceq$. Then $\mathrm{dom}\,(f) \preceq \phi(s)$. But the set $\{t|\ t \preceq \phi(s)\}$ is finite, hence there exists $N(k)$ depending only on k such that $\deg f \leq N(k)$.

Case 2: $n_e(f) \geq 1$. The argument in this case is similar to that of Case 1, with $\phi(l)$ being the unique odd non-negative integer with code $[n_o(l), n_e(l)+1]$. □

7.1.2 Bounding the weight

Before the proof of Theorem 7.1.2 we need the following theorem that is a slight generalisation of Theorem 6.1.2. The proof in [Ser73b] generalises immediately, mutatis mutandis.

Theorem 7.1.9. *Let f and g be modular forms on $SL_2(\mathbb{Z})$ with coefficients in the valuation ring of some finite extension K of $\mathbb{Q}_2$ and weights k and k_1, respectively. Assume that at least one of the coefficients of f is a unit and that we have $f \equiv g \pmod{2^m}$ for some $m \in \mathbb{N}$. Then*

$$k \equiv k_1 \pmod{2^{\alpha(m)}}$$

where

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

Concerning the proof we recall our definition of $\pmod{2^m}$: If v is the valuation extending the normalised valuation v_2 on $\mathbb{Q}_2$, i.e., $v = \frac{1}{e}v_{\mathfrak{p}}$ where e is the ramification index of $K/\mathbb{Q}_2$, the prime of K is $\mathfrak{p}$, and $v_{\mathfrak{p}}$ is the normalised valuation on K, then $f \equiv g \pmod{2^m}$ means that

$$v(a_n(f) - a_n(g)) > m - 1$$

for all n. Working with v in the proof given in [Ser73b], one obtains the result. Of course, there is a version of the theorem for odd primes, but we will not need that.

Proof of Theorem 7.1.2. Let us first show that the last statement of the theorem, i.e., the weak weight bound, follows from the first. From the first statement, any weak eigenform modulo 2^m is the reduction of a form that can be written as a linear combination of monomials $Q^a\Delta^c$, or $RQ^a\Delta^c$, and where $c \leq C(m)$. Now, from the q-expansion of Q we have that $Q \equiv 1 \pmod{2^4}$ whence $Q^{2^s} \equiv 1 \pmod{2^{4+s}}$. Suppose that $m \geq 4$. Then for any non-negative a we have $Q^a \equiv Q^{a'} \pmod{2^m}$ for some $a' \leq 2^{m-4}$. For such an a' the weight of a monomial $RQ^{a'}\Delta^c$ is $\leq 6 + 4 \cdot 2^{m-4} + 12C(m) = 6 + 2^{m-2} + 12C(m)$, and the claim follows. For $m = 1, 2, 3$ the claim follows from the congruences $Q \equiv R \equiv 1 \pmod{2^3}$.

We now show the existence of the constant $C(m)$ by induction on m. For $m = 1$, the result is classical, and it is implied by Corollary 7.1.3 that we can take $C(1) = 1$.

Assume $m > 1$ and that the statement is true for $m - 1$. Let f be a weak eigenform modulo 2^m. The reduction of f modulo 2^{m-1} is a weak eigenform modulo 2^{m-1}. By the induction hypothesis, $\deg_{m-1}(f \pmod{2^{m-1}}) \leq C(m-1)$. Thus, $(f \pmod{2^{m-1}})$ is the reduction modulo 2^{m-1} of a form g of weight at most $\kappa(m-1)$ and coefficients in $\overline{\mathbb{Z}}_2$ and for which the highest power of Δ occurring in the expansion of g as a sum of monomials $Q^a\Delta^c$, or $RQ^a\Delta^c$, is bounded by $C(m-1)$.

Let the weights of f and g be k and k_1, respectively. Since f and g have the same reduction modulo 2^{m-1} we know by Theorem 7.1.9 that

$$k \equiv k_1 \pmod{2^{\alpha(m-1)}}.$$

Replacing f by fQ^{2^s} with a sufficiently large s, we may assume that $k \geq k_1 + 6$. Write $k = k_1 + t \cdot 2^{\alpha(m-1)}$. Suppose first that $m \geq 5$. Then $Q^{2^{m-5}} \equiv 1 \pmod{2^{m-1}}$ and so the form

$$g_1 := g \cdot (Q^{2^{m-5}})^t$$

is of weight k, and has the same reduction modulo 2^{m-1} as f. In the cases $2 \leq m \leq 4$ one also finds a form g_1 with these properties, by taking $g_1 := g \cdot Q^r$ when $k \equiv k_1 \pmod 4$, and $g_1 := g \cdot RQ^r$ when $k \equiv k_1 + 2 \pmod 4$ with the appropriate power r. It works because $Q \equiv R \equiv 1 \pmod{2^3}$.

Also, the highest power of Δ occurring when we expand g_1 in a sum of monomials in Q, Δ, and, possibly, R, is bounded from above by $C(m-1)$. This follows because g has that same property. By the argument in the beginning of the proof, it follows that the form g_1 is congruent modulo 2^m to a form g_2 of weight bounded by a constant $w(m)$ depending only on m (specifically, one can take the weight bound from the beginning of the proof with $C(m)$ replaced by $C(m-1)$.) Clearly then, if p is any prime number we must have

$$\deg_m T_p g_1 = \deg_m T_p g_2 \leq \frac{1}{12} w(m).$$

Consider now that we have

$$f \equiv g_1 + 2^{m-1}h \pmod{2^m}$$

with some modular form h with coefficients in $\overline{\mathbb{Z}}_2$ and weight k.
Now, $h \pmod 2$ is a polynomial in Δ, and if we can bound the degree of this polynomial we are done.
Let λ_2, λ_3 and λ_5 be respectively the eigenvalues of the operators T_2, T_3, and T_5 associated to f. By Corollary 7.1.3, we know that $\lambda_2 \equiv \lambda_3 \equiv \lambda_5 \equiv 0 \pmod 2$. Thus for $p \in \{2, 3, 5\}$, we have:

$$T_p f \equiv T_p g_1 + 2^{m-1} T_p h \equiv \lambda_p f \equiv \lambda_p g_1 \pmod{2^m}$$

which gives

$$2^{m-1} T_p h \equiv \lambda_p g_1 - T_p g_1 \pmod{2^m}$$

for $p \in \{2, 3, 5\}$. Thus,

$$\deg_m(2^{m-1} T_p h) \leq \frac{1}{12} w(m)$$

and hence

$$\deg_1(T_p h) \leq \frac{1}{12} w(m)$$

for $p \in \{2, 3, 5\}$.
Now split $(h \pmod 2)$ into even and odd parts as explained above:

$$(h \pmod 2) = h_e + h_o.$$

We have

$$\deg_1 T_p h_e \ , \ \deg_1 T_p h_o \leq \frac{1}{12} w(m)$$

for $p \in \{2, 3, 5\}$.
Consider the classical U and V operators on mod 2 modular forms. For the even part h_e we have $h_e = \phi^2 = V(\phi)$ for some mod 2 modular form ϕ. Since $T_2 \equiv U \pmod 2$, we see that:

$$T_2 h_e = UV(\phi) = \phi.$$

Hence $\deg_1 \phi \leq \frac{1}{12} w(m)$, and so $\deg_1 h_e \leq \frac{1}{6} w(m)$.
For the odd part, we have $\deg_1 T_p h_o \leq \frac{1}{12} w(m)$ for $p \in \{3, 5\}$. By Proposition 7.1.4, it follows that $\deg_1 h_o$ is bounded by $N(\lfloor \frac{1}{12} w(m) \rfloor)$ if $\lfloor \frac{1}{12} w(m) \rfloor$ is odd, and by $N(\lfloor \frac{1}{12} w(m) \rfloor + 1)$ if $\lfloor \frac{1}{12} w(m) \rfloor$ is even.
This finishes the proof. □

It is natural to ask for an explicit "formula" for the constants $C(m)$, but we have not been able to find one. For any given m, though, a constant $C(m)$ that works in Theorem 7.1.2 can in principle be determined, the main obstacle being determining constants $N(\cdot)$ that work in Proposition 7.1.4. For some explicit values of the constants $C(m)$ for low values of m, see Section A.6.

7.2 Weight bounds in general

We can generalize the argument presented in Section 7.1, and prove the following:

Theorem 7.2.1. *Let $p \geq 5$, $p \nmid N$. There exists a constant $\kappa(N,p,m)$ depending only on N, p, and m such that, for all weak eigenforms $f \in M(\Gamma_1(N), \overline{\mathbb{Z}/p^m\mathbb{Z}})$, we have:*

$$w_{p^m}(f) \leq \kappa(N,p,m).$$

We have not made the constants $\kappa(N,p,m)$ explicit. Section A.7 provides a hint as to the form of the constant κ.

The proof of Theorem 7.2.1 will rely on the following generalisation of Proposition 7.1.4:

Proposition 7.2.2. *Let $f \in S_k(\Gamma_1(N), \overline{\mathbb{F}}_p)$ be a cuspidal modular form mod p. Suppose that for some integer d, there exists a system $\{\lambda_\ell\}_{\ell \text{ prime}}$ of Hecke eigenvalues (coming from a cuspidal eigenform) such that:*

$$w_p(T_\ell f - \lambda_\ell f) \leq d$$

for all primes ℓ. Then:

$$w_p(f) \leq \eta(N,p,d)$$

where $\eta(N,p,d)$ is a constant depending only on N, p, and d.

We will describe how Proposition 7.2.2 implies Theorem 7.2.1. This is the same strategy we have used in Section 7.1.

Lemma 7.2.3. *Proposition 7.2.2 implies Theorem 7.2.1.*

Proof. We argue by induction on the exponent m. Weight bounds for $m = 1$ are known, as in Theorem 6.2.4. Suppose that $m \geq 2$ and that we know weight bounds modulo p^{m-1}.

Let $f \in M_k(\Gamma_1(N), \overline{\mathbb{Z}}_p)$ be a modular form whose image in $\overline{\mathbb{Z}/p^m\mathbb{Z}}$ is a weak eigenform. For now, assume that $f \in S_k(\Gamma_1(N), \overline{\mathbb{Z}}_p)$, and that $a_1(f) = 1$.

The reduction of f modulo p^{m-1} is a weak cuspidal eigenform modulo p^{m-1}. By the induction hypothesis, we can find $g \in S_{k'}(\Gamma_1(N), \overline{\mathbb{Z}}_p)$ with $k' \leq \kappa(N,p,m-1)$ such that $a_1(g) = 1$ and f reduces to g modulo p^{m-1}. Without loss of generality, we can assume that $k' \leq k$. It follows from the Sturm bound ([Kil08], Theorem 3.13) that the coefficients of f modulo p^m are determined by a finite subset $\{a_n(f) : 0 \leq n \leq d\}$ for some d. So we may assume that the coefficients of f and g lie in the ring of integers $\mathcal{O}_K$ of some finite extension K of $\mathbb{Q}_p$.

Let π be a generator of the maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, and let e be the ramification degree. Then the congruence of f and g modulo p^{m-1} means that:

$$\pi^{e(m-2)+1} | (a_n(f) - b_n(f))$$

for all $n \geq 0$. Moreover, by an argument similar to the proof of Theorem 7.1.9, we have $k \equiv k' \pmod{p^{m-2}(p-1)}$. Thus, letting $A = E_{p-1}$, there exists some $t \geq 0$ such that $p^{m-2}|t$, f and $A^t g$ have the same weight, and:

$$f = A^t g - \pi^{e(m-2)+1} h$$

for some $h \in S_k(\Gamma_1(N), \mathcal{O}_K)$. All we need to do is to find an upper bound for $w_{p^m}(\pi^{e(m-2)+1} h) = w_p(h)$.

Suppose that for some prime ℓ and some $\lambda_\ell \in \mathcal{O}_K$, the Hecke operator $T_\ell - \lambda_\ell I$ annihilates f modulo p^m. That is:

$$T_\ell f - \lambda_\ell f \equiv 0 \pmod{p^m}.$$

Then:

$$T_\ell(A^t g) - \lambda_\ell(A^t g) \equiv \pi^{e(m-2)+1}(T_\ell h - \lambda_\ell h) \pmod{p^m}.$$

Since $A^{p^{m-1}} \equiv 1 \pmod{p^m}$, it follows that the difference:

$$w_{p^m}(T_\ell(A^t g) - \lambda_\ell(A^t g)) - w_{p^m}(g) = w_{p^m}(T_\ell(A^t g) - \lambda_\ell(A^t g)) - k'$$

is bounded above by a constant d depending only on p and m (since $A^{p^{m-1}} \equiv 1 \pmod{p^m}$). Therefore:

$$w_p(h) \leq d + \kappa(N, p, m-1).$$

Since ℓ was arbitrary, and the system $\{\lambda_\ell\}_{\ell \text{ prime}}$ reduces to cuspidal system of Hecke eigenvalues modulo p, we see that h satisfies the condition of Proposition 7.2.2, which gives the required upper bound on $w_p(h)$.

If $f \in M_k(\Gamma_1(N), \overline{\mathbb{Z}}_p)$ is not cuspidal, then by Theorem 6.3.2, we may find a modular form $f' \in S_{k'}(\Gamma_1(N), \overline{\mathbb{Z}}_p)$ which lifts $\theta_{p^m}(\tilde{f})$, where:

$$k' = k + 2 + 2p^{m-1}(p-1)$$

and $\tilde{f}$ is the reduction of f modulo p^m. Then f' is a cuspidal modular form whose reduction is a cuspidal weak eigenform mod p^m and hence has bounded weight filtration mod p^m by the above argument. This concludes the proof. □

We will devote the rest of this section to the proof of Proposition 7.2.2. To achieve this, we will introduce a new notion of filtration, called the nilpotency filtration. The proof will rely on using the weight filtration to control the nilpotency filtration and vice versa.

7.2.1 The Hecke algebra modulo p

Throughout this section, we let S_k be the image of the q-expansion map:

$$S_k(\Gamma_1(N), \overline{\mathbb{F}}_p) \to \overline{\mathbb{F}}_p[[q]].$$

We also let $S = \sum_{k \geq 2} S_k$. Note that this is not a direct sum. Deligne's congruence:

$$E_{p-1} \equiv 1 \pmod{p}$$

induces embeddings:

$$S_k \hookrightarrow S_{k+p-1}.$$

However, we have the following decomposition. For $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$, let:

$$S^\alpha := \bigcup_{\substack{k \equiv \alpha \pmod{p-1} \\ k \geq 2}} S_k.$$

Then:

$$S = \bigoplus_{\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}} S^\alpha.$$

Let $\mathbb{T}_k$ be $\overline{\mathbb{F}}_p$-subalgebra of $\mathrm{End}_{\overline{\mathbb{F}}_p}(S_k)$ generated by the (reductions modulo p of) the Hecke operators $\{T_\ell : \ell \text{ prime }\}$. The embeddings:

$$S_k \hookrightarrow S_{k+p-1}$$

commute with Hecke operators (since $k \geq 2$), and therefore induce, via restrictions, surjective maps:

$$\mathbb{T}_{k+p-1} \twoheadrightarrow \mathbb{T}_k.$$

Definition 7.2.4. *The Hecke algebra modulo p for $\Gamma_1(N)$ is the projective limit:*

$$\mathbb{T} := \varprojlim_k \mathbb{T}_k.$$

It follows from the deformation theory of Galois representations that the Hecke algebra $\mathbb{T}$ is Noetherian. The maximal ideals of $\mathbb{T}$ are the kernels of $\overline{\mathbb{F}}_p$-algebra homomorphisms:

$$\Phi : \mathbb{T} \to \overline{\mathbb{F}}_p$$

and are in 1-to-1 correspondence with systems $\{\lambda_\ell\}_{\ell \text{ prime}}$ of mod p Hecke eigenvalues. Thus by the mod p theory of modular forms, $\mathbb{T}$ has finitely many maximal ideals.

Proposition 7.2.5. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$. The quotient $\mathbb{T}/\mathfrak{m}^n$ is an Artinian $\mathbb{T}$-module.*

Proof. Since $\mathbb{T}$ is Noetherian, $\mathfrak{m}$ is finitely generated. The quotients $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ for $i \in \{0, \cdots, n-1\}$ (with the convention that $\mathfrak{m}^0 = \mathbb{T}$) are thus each a finite dimensional $\mathbb{T}/\mathfrak{m}$-vector space. Moreover, the $\mathbb{T}$-submodules of each $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ are exactly the $\mathbb{T}/\mathfrak{m}$-vector subspaces. Thus we see that for each i, the quotient $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is Artinian.

Now consider the finite chain of $\mathbb{T}$-modules:

$$0 \subseteq \mathfrak{m}^{n-1}/\mathfrak{m}^n \subseteq \mathfrak{m}^{n-2}/\mathfrak{m}^n \subseteq \cdots \subseteq \mathbb{T}/\mathfrak{m}^n.$$

Since the quotient of each two consecutive modules in the chain is Artinian, it follows that $\mathbb{T}/\mathfrak{m}^n$ is Artinian. □

7.2.2 Weight and nilpotency filtrations

For an ideal $I \subset \mathbb{T}$ and a submodule $N \subset M$, we let $N[I]$ be the subspace of N which is killed by I. That is:

$$N[I] := \{f \in N : Tf = 0 \quad \forall T \in I\}.$$

We let:

$$N[I^\infty] := \bigcup_{n \geq 0} N[I^n].$$

Thus $N[I^\infty]$ is the subspace of N on which I acts nilpotently.

Remark 7.2.6. *In this context, $N[I^\infty]$ is an abuse of notation. The space $N[I^\infty]$ will **not** in general be the kernel of:*

$$I^\infty = \bigcap_{n \geq 0} I^n$$

acting on N. The space $N[I^\infty]$ is defined to be the part of N on which I acts nilpotently.

For a commutative ring R, we denote by $\mathrm{Max}(R)$ the maximal spectrum of R, that is, $\mathrm{Max}(R)$ is the set of maximal ideals of R.

Definition 7.2.7. *Let $\mathfrak{m} \in Max(\mathbb{T})$, and let $f \in S[\mathfrak{m}^\infty]$. We define the $\mathfrak{m}$-nilpotency filtration of f by:*

$$g_{\mathfrak{m}}(f) = \inf\{t : f \in S[\mathfrak{m}^t]\}.$$

When $\mathfrak{m}$ is understood from the context, we simply write $g(f)$ for the $\mathfrak{m}$-nilpotency filtration.

Let $\Phi : \mathbb{T} \to \overline{\mathbb{F}}_p$ be a system of mod p Hecke eigenvalues. For each prime ℓ, let $\lambda_\ell = \Phi(T_\ell)$, and:

$$T_\ell^{\mathfrak{m}} := T_\ell - \lambda_\ell I$$

where I is the identity operator. Then the operators $\{T_\ell^{\mathfrak{m}}\}_{\ell \text{ prime}}$ generate the ideal $\mathfrak{m}$. This leads to the following useful characterisation of the nilpotency filtration.

Lemma 7.2.8. *Let $f \in S[\mathfrak{m}^\infty]$, and let $g = g(f)$ be the $\mathfrak{m}$-nilpotency filtration of f. Then g is the smallest integer such that, for any sequence $\ell_1, \cdots, \ell_g$ of primes, we have:*

$$(T_{\ell_1}^{\mathfrak{m}} \cdots T_{\ell_g}^{\mathfrak{m}})f = 0.$$

Lemma 7.2.9. *We have the following direct sum decomposition:*

$$S = \bigoplus_{\mathfrak{m} \in Max(\mathbb{T})} S[\mathfrak{m}^\infty].$$

Proof. Let $k \geq 2$. We can define a pairing:

$$\mathbb{T}_k \times S_k \to \overline{\mathbb{F}}_p, \tag{$*$}$$

$$(T, f) \mapsto a_1(Tf).$$

We check that this is a perfect pairing. Suppose that for some $f \in S_k$ we have:

$$a_1(T_n f) = a_n(f) = 0$$

for all $n \geq 1$. Then f is a constant, and since f is cuspidal, it follows that $f = a_0(f) = 0$. Now suppose that for some $T \in \mathbb{T}_k$ we have $a_1(Tf) = 0$ for all $f \in S_k$. Then, for all $n \geq 1$ and $f \in S_k$, we have:

$$a_1(TT_n f) = a_n(Tf) = 0.$$

As $Tf \in S_k$, we have $a_0(Tf) = 0$, and hence $Tf = 0$ for all $f \in S_k$, which means that $T = 0$, since it is by definition an endomorphism of S_k.

Since $\mathbb{T}_k$ is a finite dimensional $\overline{\mathbb{F}}_p$-vector space, it is an Artinian $\overline{\mathbb{F}}_p$-algebra. Therefore, it can be decomposed as:

$$\mathbb{T}_k \cong \prod_{\mathfrak{m} \in \mathrm{Spec}(\mathbb{T}_k)} \mathbb{T}_k / \mathfrak{m}^\infty.$$

The perfect pairing $*$ gives rise to perfect pairings:

$$\mathbb{T}_k/\mathfrak{m}^n \times S_k[\mathfrak{m}^n] \to \overline{\mathbb{F}}_p \tag{$\dagger$}$$

$$(T_\ell \pmod{\mathfrak{m}^n}, f) \mapsto a_1(T_\ell f) = a_\ell(f).$$

for every $\mathfrak{m} \in \mathrm{Spec}(\mathbb{T}_k)$ and $n \geq 0$. It follows that there exists a decomposition of $\mathbb{T}_k$-modules:

$$S_k = \bigoplus_{\mathfrak{m}\in\mathrm{Spec}(\mathbb{T}_k)} S_k[\mathfrak{m}^\infty].$$

For $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$, we now see that we have a decomposition:

$$S^\alpha = \bigoplus_{\mathfrak{m}\in\mathrm{Max}(\mathbb{T})} S^\alpha[\mathfrak{m}^\infty].$$

Therefore:

$$\begin{aligned} S &= \bigoplus_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} S^\alpha = \bigoplus_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} \bigoplus_{\mathfrak{m}\in\mathrm{Max}(\mathbb{T})} S^\alpha[\mathfrak{m}^\infty] \\ &= \bigoplus_{\mathfrak{m}\in\mathrm{Max}(\mathbb{T})} \bigoplus_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} S^\alpha[\mathfrak{m}^\infty] = \bigoplus_{\mathfrak{m}\in\mathrm{Max}(\mathbb{T})} S[\mathfrak{m}^\infty]. \end{aligned}$$

□

Let $\mathfrak{m} \in \mathrm{Max}(\mathbb{T})$. We have, as in †, a pairing of $\mathbb{T}$-modules:

$$\mathbb{T}/\mathfrak{m}^n \times S[\mathfrak{m}^n] \to \overline{\mathbb{F}}_p,$$

$$(T_\ell \pmod{\mathfrak{m}^n}, f) \mapsto a_1(T_\ell f) = a_\ell(f).$$

As above, this pairing is perfect, and hence $\mathbb{T}/\mathfrak{m}^n$ is dual to $S[\mathfrak{m}^n]$.

The following fact was kindly pointed out to us by Frank Calegari in a private communication.

Proposition 7.2.10. *For every $n \geq 0$ and $\mathfrak{m} \in$ Max$(\mathbb{T})$, there exists an integer $k_\mathfrak{m}(n, N, p) \geq 0$ depending only on $\mathfrak{m}$, n, N, and p such that, for all $k \geq 2$ and for all $f \in S_k[\mathfrak{m}^n]$, we have:*

$$w_p(f) \leq k_\mathfrak{m}(n, N, p)$$

Proof. Let $k \geq 2$ and $f \in S_k[\mathfrak{m}^n]$. Since $S[\mathfrak{m}^n]$ is dual to $\mathbb{T}/\mathfrak{m}^n$, it follows by Proposition 7.2.5 that $S[\mathfrak{m}^n]$ is a Noetherian $\mathbb{T}/\mathfrak{m}^n$ module. Let:

$$N_i = \{f' \in S_{k'}[\mathfrak{m}^n] : w_p(f) \leq i \text{ and } k' \equiv k \pmod{p-1}\}.$$

Then $N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$. The space $S[\mathfrak{m}^n]$ is a $\mathbb{T}/\mathfrak{m}^n$-module, and each N_i is a $\mathbb{T}/\mathfrak{m}^n$-submodule. By Noetherianity, this ascending chain must stabilise. Thus there exists $k_0 \geq 0$ such that:

$$f \in \bigcup_{i=0}^\infty N_i = N_{k_0},$$

This k_0 depends only on $\mathfrak{m}$, n, N and p (and possibly on the congruence class of $k \pmod{p-1}$, but there are only finitely many such congruence classes). Thus the required constant $k_\mathfrak{m}(n, N, p)$ exists. □

Proposition 7.2.10 allows us to control the weight filtration of a modular form knowing its nilpotency filtration. We can also control the nilpotency filtration knowing the weight filtration.

Proposition 7.2.11. *For every $k \geq 0$, there exists an integer $h(k, N, p) \geq 0$ depending only on k, N, and p such that:*

$$S_k[\mathfrak{m}^\infty] = S_k[\mathfrak{m}^h].$$

Proof. The action of the elements of $\mathfrak{m}$ on $S_k[\mathfrak{m}^\infty]$ can be represented by $d \times d$ nilpotent matrices, where $d = \dim S_k[\mathfrak{m}^\infty]$. From basic linear algebra, the product of any d such matrices is zero, and we can take $h = \dim S_k \geq d$. □

We can now prove Proposition 7.2.2.

Proof of Proposition 7.2.2. Let $f \in S_k$ be a mod p cuspidal modular form, and suppose that for some fixed d and some $\mathfrak{m}_1 \in \mathrm{Max}(\mathbb{T})$, we have:

$$w_p(T_\ell^{\mathfrak{m}_1} f) \leq d$$

for all primes ℓ. By Lemma 7.2.9, we can write $f = \sum_{\mathfrak{m} \in \mathrm{Max}(\mathbb{T})} f_\mathfrak{m}$ where $f_\mathfrak{m} \in S[\mathfrak{m}^\infty]$. Since the Hecke operators respect this decomposition, it follows that:

$$w_p(T_\ell^{\mathfrak{m}_1} f_\mathfrak{m}) \leq d$$

for all $\mathfrak{m} \in \mathrm{Max}(\mathbb{T})$ and primes ℓ. Thus it suffices to consider the following two cases.

Case 1. Suppose that $f \in S[\mathfrak{m}_1^\infty]$. Let $\alpha = g(f)$. By Lemma 7.2.8, there exists a sequence $\ell_1, \cdots, \ell_{\alpha-1}$ such that:

$$(T_{\ell_1}^{\mathfrak{m}_1} \cdots T_{\ell_{\alpha-1}}^{\mathfrak{m}_1}) f \neq 0.$$

Then clearly:

$$\alpha - 1 \leq \beta = \min\{g(T_{\ell_i}^{\mathfrak{m}} f) : i = 1 \cdots \alpha - 1\}$$

and hence $\alpha \leq \beta + 1$. Since for all ℓ we have:

$$w_p(T_\ell^{\mathfrak{m}_1} f) \leq d$$

it follows that by Proposition 7.2.11 that:

$$\beta \leq h(d, N, p),$$

hence:

$$\alpha \leq h(d, N, p) + 1.$$

Then from Proposition 7.2.10, we have:

$$w_p(f) \leq k_{\mathfrak{m}_1}(h(d, N, p) + 1, N, p).$$

Case 2. Suppose that $f \in S[\mathfrak{m}^\infty]$ where $\mathfrak{m} \in \mathrm{Max}(\mathbb{T}) \setminus \{\mathfrak{m}_1\}$. Let $\alpha = g(f)$. By Lemma 7.2.8, there exists a sequence $\ell_1, \cdots, \ell_{\alpha-1}$ such that:

$$f' := (T_{\ell_1}^{\mathfrak{m}} \cdots T_{\ell_{\alpha-1}}^{\mathfrak{m}}) f \neq 0.$$

There must exist a prime ℓ such that $T_\ell^{\mathfrak{m}_1} f' \neq 0$. For, if that is not the case, then that would mean that:

$$f' \in S[\mathfrak{m}_1] \cap S[\mathfrak{m}^\infty] = \{0\},$$

which would give a contradiction. For such a prime ℓ, we have:

$$\alpha \leq g(T_\ell^{\mathfrak{m}_1} f).$$

Since $w_p(T_\ell^{\mathfrak{m}_1} f) \leq d$, we get by Proposition 7.2.11:

$$\alpha \leq g(T_\ell^{\mathfrak{m}_1} f) \leq h(d, N, p).$$

And so by Proposition 7.2.10:

$$w_p(f) \leq k_{\mathfrak{m}}(h(d, N, p), N, p).$$

This concludes the proof. □

7.3 Connection with a question of Buzzard

Let $\mathfrak{S}_0(N)$ and $\mathfrak{S}_1(N)$ be respectively the sets of normalised Hecke eigenforms in characteristic zero for $\Gamma_0(N)$ and $\Gamma_1(N)$. Fix a prime p. For $f \in \mathfrak{S}_0(N) \cup \mathfrak{S}_1(N)$, define:

$$K_{f,p} = \mathbb{Q}_p(a_\ell(f) : \ell \text{ is prime and } \ell \nmid Np).$$

In [Buz05], Question 4.4, Buzzard asks:

Question 7.3.1. *Is the following quantity:*

$$\sup_{f \in \mathfrak{S}_0(N)} [K_{f,p} : \mathbb{Q}_p]$$

finite?

In joint work with Ian Kiming and Gabor Wiese ([KRW14]), we investigate the connection between Buzzard's question and finiteness statements mod p^m of the numbers of strong eigenforms and attached Galois representations.

We introduce the following statements. Let (B) be the following statement, inspired by Buzzard's question:

$$\text{For fixed } N \text{ with } p \nmid N \text{ we have: } \sup_{f \in \mathfrak{S}_1(N)} [K_{f,p} : \mathbb{Q}_p] < \infty. \tag{B}$$

Let (Strong_m) be the statement:

$$\text{There are finitely many strong eigenforms modulo } p^m \text{ for } \Gamma_1(N). \tag{Strong_m}$$

If $f \in \mathfrak{S}_1(N)$, then one can attach to f a p-adic Galois representation:

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

and a mod p^m Galois representation:

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

by composing with the reduction map $\overline{\mathbb{Z}}_p \twoheadrightarrow \overline{\mathbb{Z}/p^m\mathbb{Z}}$. Let $\mathfrak{R}_m(N)$ be the set of characters of the mod p^m Galois representations attached to the forms $f \in \mathfrak{S}_1(N)$. Let (Repr_m) be the following statement:

$$\text{For fixed } N \text{ with } p \nmid N, \text{ the set } \mathfrak{R}_m(N) \text{ is finite.} \tag{Repr_m}$$

One more statement is needed to make the connection. With $K_{f,p}$ as above, let $\mathcal{O}_{f,p}$ be its valuation ring, and $\mathfrak{p}_{f,p}$ its maximal ideal. Let $e_{f,p}$ be the ramification index of $K_{f,p}/\mathbb{Q}_p$. Let:

$$\mathbb{Z}_p[a_\ell(f)] = \mathbb{Z}_p[a_\ell : \ell \text{ is primes with } \ell \nmid Np],$$

and consider the index:

$$I_{f,p} = [\mathcal{O}_{f,p}/\mathfrak{p}_{f,p}^{e_{f,p}(m-1)+1} : ((\mathbb{Z}/p^m\mathbb{Z})[a_\ell(f) \pmod{p^m})])].$$

We define the "index finiteness" statement (I_m):

$$\text{For fixed } N \text{ and } p \nmid N, \text{ we have: } \sup_{f \in \mathfrak{S}_1(N)} I_{f,p} < \infty. \tag{I_m}$$

In [KRW14], we have shown the following implications:

Theorem 7.3.2.

- (B) $\Rightarrow$ (Strong_m) $\Rightarrow$ (Repr_m).
- (B) $\Leftrightarrow$ (I_m) + (Repr_m).

In [KRW14], we also stated the following conjectures.

Conjecture 7.3.3. *For every $m \geq 1$, the statement* (Repr_m) *is true.*

$$(\mathrm{C}_1)$$

Conjecture 7.3.4. *For every $m \geq 1$, the statement* (Strong_m) *is true.*

$$(\mathrm{C}_2)$$

As already stated, the truth of Conjecture (C_2) implies that of Conjecture (C_1). Moreover, the truth of Conjecture (C_2) would imply the truth of the following conjecture:

Conjecture 7.3.5. *Given N, p, m as well as $k \in \mathbb{N}$, there are only finitely many $f \in \mathfrak{S}_1(N)$ such that $w_{p^m}(f) \leq k$.*

$$(\mathrm{C}_3)$$

It is clear now that Conjecture (C_3) together with Theorem 7.2.1 imply Conjecture (C_2). We see that by Hatada's theorem (see Corollary 6.2.6), Conjecture (C_2) holds for $N = 1$, $p = 2$, and $m = \{1, 2, 3\}$.

It remains to say that, based on the work of Coleman ([Col97], Theorem D) and Wan ([Wan98], Theorem 1.1), we can show that Conjecture 1 holds true if one fixes the slope of the eigenform to which the Galois representation is attached. We recall the definition of slope:

Definition 7.3.6. *Let $f \in \mathfrak{S}_1(N)$. The slope of f is the rational number $\alpha = v_p(a_p(f))$.*

Explicitly ([KRW14], Proposition 4):

Proposition 7.3.7. *Fix N, p, m, and $\alpha \in \mathbb{Q}_{\geq 0}$. There are only finitely many Galois representations modulo p^m attached to eigenforms for $\Gamma_1(N)$ of p-slope α.*

Appendices

Appendix A

Numerical results

A.1 Generating weights for $M(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])$

The following table shows the maximal weight needed to generate the algebra $M(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])$, for levels N up to 83, up to the weight given in the third column. These have been calculated using Algorithm 5.3.1 up to the bounds given by Theorem 4.3.7. Each entry shows the number ϵ_2 of elliptic points of order 2, the number ϵ_3 of elliptic points of order 3, as well as the number ϵ_∞ of cusps for the group $\Gamma_0(N)$.

N	ϵ_2	ϵ_3	ϵ_∞	generated in weight
1	1	1	1	6
2	1	0	2	4
3	0	1	2	6
4	0	0	3	2
5	2	0	2	4
6	0	0	4	2
7	0	2	2	6
8	0	0	4	2
9	0	0	4	2
10	2	0	4	4
11	0	0	2	4
12	0	0	6	2
13	2	2	2	6
14	0	0	4	2
15	0	0	4	2
16	0	0	6	2
17	2	0	2	4
18	0	0	8	2
19	0	2	2	6
20	0	0	6	2
21	0	2	4	6
22	0	0	4	2
23	0	0	2	4
24	0	0	8	2
25	2	0	6	4
26	2	0	4	4
27	0	0	6	2
28	0	0	6	2
29	2	0	2	4
30	0	0	8	2
31	0	2	2	6
32	0	0	8	2
33	0	0	4	2
34	2	0	4	4
35	0	0	4	2
36	0	0	12	2
37	2	2	2	6
38	0	0	4	2
39	0	2	4	6
40	0	0	8	2

N	ϵ_2	ϵ_3	ϵ_∞	generated in weight
41	2	0	2	4
42	0	0	8	2
43	0	2	2	6
44	0	0	6	2
45	0	0	8	2
46	0	0	4	2
47	0	0	2	4
48	0	0	12	2
49	0	2	8	6
50	2	0	12	4
51	0	0	4	2
52	0	0	6	2
53	2	0	2	4
54	0	0	12	2
55	0	0	4	2
56	0	0	8	2
57	0	2	4	6
58	2	0	4	4
59	0	0	2	4
60	0	0	12	2
61	2	2	2	6
62	0	0	4	2
63	0	0	8	2
64	0	0	12	2
65	4	0	4	4
66	0	0	8	2
67	0	2	2	6
68	0	0	6	2
69	0	0	4	2
70	0	0	8	2

N	ϵ_2	ϵ_3	ϵ_∞	generated in weight
71	0	0	2	4
72	0	0	16	2
73	2	2	2	6
74	2	0	4	4
75	0	0	12	2
76	0	0	6	2
77	0	0	4	2
78	0	0	8	2
79	0	2	2	6
80	0	0	12	2
81	0	0	12	2
82	2	0	4	4
83	0	0	2	4

We see from the table that $M(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])$ seems to always be generated in weight at most 6. This is predicted by Theorem 4.3.7 for any level N for which $\epsilon_2\epsilon_3 = 0$. In the case where $\epsilon_2\epsilon_3 > 0$, Theorem 4.3.7 gives a bound of 12 on the generating weight. However, we see from the table above that this bound is not optimal. This is an inherent limitation in working on the coarse moduli scheme instead of on the stack. We believe that a version of Mumford's theorems (Theorem 3.3.1) might hold for the stacks $\mathcal{X}_0(N)$. We make the following conjecture:

Conjecture A.1.1. *For any $N \geq 1$, the generating weight for the algebra $M(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])$ is 6.*

A.2 Relations for $M(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])$

We calculate the smallest degree in which the ideal of relations between minimal generators of $M(\Gamma_0(N), \mathbb{Z}[\frac{1}{6N\varphi(N)}])$ is generated. In the table below, N indicates the congruence subgroup $\Gamma_0(N)$, ϵ_2 the number of elliptic points of order 2, ϵ_3 the number of elliptic points of order 3, and ϵ_∞ the number of cusps. Algorithm 5.3.5 was used to generate this table.

N	ϵ_2	ϵ_3	ϵ_∞	related in degree
1	1	1	1	0
2	1	0	2	0
3	0	1	2	8
4	0	0	3	0
5	2	0	2	8
6	0	0	4	4
7	0	2	2	12
8	0	0	4	4
9	0	0	4	4
10	2	0	4	8
11	0	0	2	8
12	0	0	6	4
13	2	2	2	12
14	0	0	4	4
15	0	0	4	4
16	0	0	6	4
17	2	0	2	8

A.3 Generating weights for $M(\Gamma_0(p), \mathbb{Z})$

Recall that the set S is defined as the set of modular forms $f \in M(\Gamma_0(p), \mathbb{Z})$ such that $v_p(\tilde{f}) \geq 0$. Recall also the T-form $T(z) := \left(\frac{\eta(pz)^p}{\eta(z)}\right)^2$. In Theorem 4.4.9, we proved that S and T generate the algebra $M(\Gamma_0(p), \mathbb{Z})$. We will provide computational evidence for Conjecture 4.4.11:

Conjecture 4.4.11. *The weights of the modular forms appearing in a minimal set of generators for $M(\Gamma_0(p), \mathbb{Z})$ are in the set $\{2, 4, 6, p-1\}$, and there is only one generator of weight $p-1$ (which can be chosen to be the T-form T).*

We use Algorithm 5.3.1 to calculate the degrees of generators in a minimal set of generators for $M(\Gamma_0(p), \mathbb{Z})$. The following table details the results. The last column shows the highest weight k such that the generators listed generated the algebra up to weight k. When the last column contains a dash, it means the generators found generate the whole algebra. In each level p above, the form in weight $p-1$ can be chosen to be the T-form.

p	weights of generators	up to
5	2, 4, 4	-
7	2, 4, 4, 6, 6	-
11	2, 2, 4, 6, 10	-
13	2, 4, 4, 4, 4, 6, 6, 12	-
17	2, 2, 4, 4, 4, 6, 16	-
19	2, 2, 4, 4, 4, 6, 6, 18	-
23	2, 2, 2, 4, 4, 6, 22	-
29	2, 2, 2, 4, 4, 4, 4, 6, 28	-
31	2, 2, 2, 4, 4, 4, 4, 6, 6, 30	-
37	2, 2, 2, 4, 4, 4, 4, 4, 4, 6, 6, 36	56
41	2, 2, 2, 2, 4, 4, 4, 4, 4, 6, 40	54
43	2, 2, 2, 2, 4, 4, 4, 4, 4, 6, 6, 42	48
47	2, 2, 2, 2, 2, 4, 4, 4, 4, 6, 46	46

A.4 Relations for $M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$

In the following table we provide the number of relations needed to generate the ideal of relations of $M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$, detailing the total number of generators of $M(\Gamma_1(N), \mathbb{Z}[\frac{1}{N}])$ and the number of generators in weights 2 and 3, as well as the total number of relations and the number of relations in each degree.

N	generators	weight 2	weight 3	relations	degree 4	degree 5	degree 6
5	7	3	4	17	1	6	10
6	7	3	4	17	1	6	10
7	12	5	7	58	6	24	28
8	12	5	7	58	6	24	28
9	17	7	10	124	15	54	55
10	17	7	10	124	15	54	55
11	25	10	15	281	35	125	121
12	22	9	13	215	28	96	91
13	33	13	20	502	64	226	212
14	30	12	18	412	54	186	172
15	40	16	24	749	104	344	301
16	38	15	23	673	89	306	278
17	52	20	32	1281	166	584	531
18	43	17	26	869	118	398	353
19	63	24	39	1902	246	867	789
20	56	22	34	1495	207	690	598
21	72	28	44	2497	346	1156	995
22	65	25	40	2027	270	930	827

A.5 Computations of θ_{p^2}-cycles

Computation results for θ_{p^2}-cycles of Δ modulo p^2 in level 1 displayed below suggests that there is no simple classification of θ-cycles modulo higher powers similar to that of the case of modulo p. Computation was carried out following Algorithm 6.3.8.

p	Total drops	Length of cycle $= p(p-1)$
5	7	20
7	8	42
11	18	110
13	22	156
17	25	272
19	28	342
23	30	506
29	44	812
31	47	930
37	54	1332
41	61	1640
43	66	1806

A.6 Weight bounds mod $2, 4, 8, 16$ for $N = 1$

We give now examples for the low values $m = 1, 2, 3, 4$. We have $C(1) = 1$ as already remarked and used in the above. To determine constants $C(m)$ for $m = 2, 3, 4$, we refer back to the inequalities appearing at the end of the proof of Theorem 7.1.2:

$$\deg_1 h_e \leq \frac{1}{6} w(m),$$

and:

$$\deg_1 h_o \leq \begin{cases} N(\lfloor \frac{1}{12} w(m) \rfloor) & \text{if } \lfloor \frac{1}{12} w(m) \rfloor \text{ is odd} \\ N(\lfloor \frac{1}{12} w(m) \rfloor + 1) & \text{if } \lfloor \frac{1}{12} w(m) \rfloor \text{ is even} \end{cases}$$

where, as in the beginning of the proof, we have:

$$w(m) \leq \begin{cases} 6 + 2^{m-2} + 12C(m-1) & \text{if } m \geq 4 \\ 12C(m-1) & \text{if } m = 2, 3. \end{cases}$$

By the proof of Theorem 7.1.2, it then follows that we can take:

$$C(m) = \sup\{C(m-1), \lfloor \frac{1}{6} w(m) \rfloor, N(\lfloor \frac{1}{12} w(m) \rfloor)\}.$$

Using a computer, we compute the following values for the function $N(\cdot)$:

k	$N(k)$
1	5
5	17
17	65

We also check that the function N is non-decreasing on the set of odd integers k such that $1 \leq k \leq 100$. The calculation of the values of $C(m)$ are summarized in the following table:

m	$w(m) \leq$	$\lfloor \frac{1}{6} w(m) \rfloor \leq$	$\lfloor \frac{1}{12} w(m) \rfloor \leq$	$N(\lfloor \frac{1}{12} w(m) \rfloor) \leq$	$C(m)$
1	-	-	-	-	1
2	19	3	1	5	5
3	68	11	5	17	17
4	214	35	17	65	65

A computer search shows that these values are sharp for $m = 2$ and $m = 3$, i.e., in each of these cases there exists a weak eigenform modulo 2^m for which $\deg_m$ attains the upper bound $C(m)$. We do not know whether the value for $C(4)$ is sharp, as the calculations become too demanding.

A.7 Weight bounds for strong eigenforms mod p^m

We will finally present a bit of numerical data that can be seen as experimental approach to the constant $\kappa(N, p, m)$ of Theorem 7.2.1.

For each entry in the following table, we generated all eigenforms of weight $\leq k_{max}$ on the group in question; then, we looked at the reduction modulo p^m of each of these eigenforms f and determined the smallest weight $k(f)$ where it occurs weakly modulo p^m; the number κ in the corresponding entry is the maximum of the $k(f)$ for f in this particular set of eigenforms.

Group	p	m	κ	k_{max}
$\Gamma_0(1)$	5	2	76	320
$\Gamma_0(1)$	5	3	276	288
$\Gamma_0(1)$	7	2	148	246
$\Gamma_0(1)$	11	2	364	374
$\Gamma_0(2)$	5	2	76	174
$\Gamma_0(2)$	5	3	276	316
$\Gamma_0(2)$	7	2	148	246
$\Gamma_0(2)$	11	2	364	370
$\Gamma_0(3)$	5	2	76	174
$\Gamma_0(3)$	5	3	276	278
$\Gamma_0(3)$	7	2	148	222
$\Gamma_0(5)$	5	2	76	138
$\Gamma_0(9)$	5	2	76	150
$\Gamma_1(3)$	5	2	76	174
$\Gamma_1(3)$	5	3	276	296
$\Gamma_1(3)$	7	2	148	204
$\Gamma_1(11)$	5	2	76	88

Thus, the number κ can be seen as an “experimental value” for the constants occurring in Conjecture C_3. The values of κ in the table would be consistent with a more precise version of the statement of Conjecture C_3, namely that it holds with a constant $\kappa(N,p,m)$ that is in fact independent of N, and has the following precise value:

$$\kappa(N,p,m) = 2p^m + p^2 + 1$$

when $m \geq 2$.

We curiously remark that:

$$2p^m + p^2 + 1 = p^2 + p + (p^{m-1} - 1)(p-1) + p^{m-1}(p+1).$$

This significance of this observation is that $(p^{m-1}-1)(p-1)$ is the highest value that the Hasse invariant E_{p-1} can contribute to the mod p^m filtration (since $E_{p-1}^{p^{m-1}} \equiv 1 \pmod{p^m}$), and p^2+p is the highest weight filtration of a mod p eigenform, as established in [Joc82a]. The number $p+1$ is the weight of the Eisenstein series E_{p+1}, which plays a central role in the mod p theory of modular forms. Additionally, $p^{m-1}(p+1)$ is the number of elements of $\mathbb{P}^1(\mathbb{Z}/p^m\mathbb{Z})$, and hence the number of irreducible components of the reduction modulo p of the modular curve $Y(\Gamma(p^m))$. We still do not know any theoretical justification for this remark, but it might indicate a possible hint as to the true form of the constants κ of Theorem 7.2.1.

Bibliography

[AS86] Avner Ash and Glenn Stevens, *Modular forms in characteristic l and special values of their L-functions*, Duke Math. J. **53** (1986), no. 3, 849–868. MR 860675 (88h:11036) [cited at p. 10]

[BDP] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *p-adic L-functions and the coniveau filtration on Chow groups*, preprint, http://www.math.mcgill.ca/darmon/pub/Articles/Research/60.BDP5-coniveau/paper.pdf. [cited at p. 56]

[BG03] Lev A. Borisov and Paul E. Gunnells, *Toric modular forms of higher weight*, J. Reine Angew. Math. **560** (2003), 43–64. [cited at p. 6]

[BK] Joël Bellaïche and Chandrasekhar Khare, *Hecke algebras of modular forms modulo p*, preprint, http://people.brandeis.edu/~jbellaic/preprint/Heckealgebra4.pdf. [cited at p. 12]

[BN10] Siegfried Böcherer and Gabriele Nebe, *On theta series attached to maximal lattices and their adjoints*, J. Ramanujan Math. Soc. **25** (2010), no. 3, 265–284. [cited at p. 6]

[Buz05] Kevin Buzzard, *Questions about slopes of modular forms*, Astérisque (2005), no. 298, 1–15, Automorphic forms. I. MR 2141701 (2005m:11082) [cited at p. 12, 96]

[CE04] Frank Calegari and Matthew Emerton, *The Hecke algebra T_k has large index*, Math. Res. Lett. **11** (2004), no. 1, 125–137. MR 2046205 (2005e:11051) [cited at p. 12, 75]

[CK14] Imin Chen and Ian Kiming, *On the theta operator for modular forms modulo prime powers*, arXiv:1301.3087v3 [math.NT] (2014), preprint, http://arxiv.org/pdf/1301.3087v3.pdf. [cited at p. 13, 14, 71, 76, 77, 78]

[CKW13] Imin Chen, Ian Kiming, and Gabor Wiese, *On modular Galois representations modulo prime powers*, Int. J. Number Theory **9** (2013), no. 1, 91–113. MR 2997492 [cited at p. 11, 14, 71, 74, 75]

[Col97] Robert F. Coleman, *p-adic Banach spaces and families of modular forms*, Invent. Math. **127** (1997), no. 3, 417–479. MR 1431135 (98b:11047) [cited at p. 98]

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. [cited at p. 37, 38, 39, 49]

[DM69] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. (1969), no. 36, 75–109. MR 0262240 (41 #6850) [cited at p. 46, 56]

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. [cited at p. 5, 10, 38, 46, 47, 48, 53, 56, 57, 58]

[DS74] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530 (1975). MR 0379379 (52 #284) [cited at p. 74]

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. [cited at p. 17, 19, 35, 40, 41, 49]

[Edi92] Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594. MR 1176206 (93h:11124) [cited at p. 10, 11, 13, 78]

[Gro90] Benedict H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. **61** (1990), no. 2, 445–517. [cited at p. 36, 37, 38]

[Har10] Robin Hartshorne, *Deformation theory*, Graduate Texts in Mathematics, vol. 257, Springer, New York, 2010. MR 2583634 (2011c:14023) [cited at p. 37]

[Hat77] Kazuyuki Hatada, *Congruences of the eigenvalues of Hecke operators*, Proc. Japan Acad. Ser. A Math. Sci. **53** (1977), no. 4, 125–128. MR 0453642 (56 #11902) [cited at p. 74]

[Hid12] Haruzo Hida, *Geometric modular forms and elliptic curves*, second ed., World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012. MR 2894984 (2012j:11100) [cited at p. 48, 49]

[Joc82a] Naomi Jochnowitz, *Congruences between systems of eigenvalues of modular forms*, Trans. Amer. Math. Soc. **270** (1982), no. 1, 269–285. MR 642341 (83e:10033b) [cited at p. 10, 13, 74, 78, 109]

[Joc82b] ———, *A study of the local components of the Hecke algebra mod l*, Trans. Amer. Math. Soc. **270** (1982), no. 1, 253–267. MR 642340 (83e:10033a) [cited at p. 13, 74, 78]

[Kat73] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. MR 0447119 (56 #5434) [cited at p. 73]

[Kat77] ______, *A result on modular forms in characteristic p*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Springer, Berlin, 1977, pp. 53–61. Lecture Notes in Math., Vol. 601. MR 0463169 (57 #3127) [cited at p. 77, 79]

[Kil07] Timothy Kilbourn, *Congruence properties of Fourier coefficients of modular forms*, ProQuest LLC, Ann Arbor, MI, 2007, Thesis (Ph.D.)–University of Illinois at Urbana-Champaign. MR 2711108 [cited at p. 53, 60]

[Kil08] L. J. P. Kilford, *Modular forms*, Imperial College Press, London, 2008, A classical and computational introduction. MR 2441106 (2009m:11001) [cited at p. 59, 76, 89]

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR 772569 (86i:11024) [cited at p. 46, 47]

[KM12] Kamal Khuri-Makdisi, *Moduli interpretation of Eisenstein series*, Int. J. Number Theory **8** (2012), no. 3, 715–748. [cited at p. 41]

[Köh11] Günter Köhler, *Eta products and theta series identities*, Springer Monographs in Mathematics, Springer, Heidelberg, 2011. [cited at p. 54]

[KRW14] Ian Kiming, Nadim Rustom, and Gabor Wiese, *On certain finiteness questions in the arithmetic of modular forms*, arXiv:1408.3249v1 [math.NT] (2014), preprint, http://arxiv.org/pdf/1408.3249v1.pdf. [cited at p. 3, 12, 15, 83, 96, 97, 98]

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications. MR 1917232 (2003g:14001) [cited at p. 40, 50]

[LMB00] Gérard Laumon and Laurent Moret-Bailly, *Champs algébriques*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 39, Springer-Verlag, Berlin, 2000. MR 1771927 (2001f:14006) [cited at p. 46]

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978). MR 488287 (80c:14015) [cited at p. 50]

[Miy06] Toshitsune Miyake, *Modular forms*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006, Translated from the 1976 Japanese original by Yoshitaka Maeda. MR 2194815 (2006g:11084) [cited at p. 22]

[Mum65] David Mumford, *Picard groups of moduli problems*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 33–81. MR 0201443 (34 #1327) [cited at p. 46]

[Mum70a] ———, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Oxford University Press, 1970. [cited at p. 47]

[Mum70b] ———, *Varieties defined by quadratic equations*, Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969), Edizioni Cremonese, Rome, 1970, pp. 29–100. MR 0282975 (44 #209) [cited at p. 6, 7, 39]

[New59] Morris Newman, *Construction and application of a class of modular functions. II*, Proc. London Math. Soc. (3) **9** (1959), 373–387. [cited at p. 64]

[NS12] Jean-Louis Nicolas and Jean-Pierre Serre, *Formes modulaires modulo 2: l'ordre de nilpotence des opérateurs de Hecke*, C. R. Math. Acad. Sci. Paris **350** (2012), no. 7-8, 343–348. MR 2922080 [cited at p. 12, 84, 85]

[Rus14a] Nadim Rustom, *Generators and relations of the graded algebra of modular forms*, arXiv:1402.0405 [math.NT] (2014), preprint, http://arxiv.org/pdf/1402.0405v1.pdf. [cited at p. 3, 5, 7, 9, 14, 35, 45, 63]

[Rus14b] ———, *Generators of graded rings of modular forms*, J. Number Theory **138** (2014), 97–118. MR 3168924 [cited at p. 3, 5, 6, 7, 9, 14, 35, 45, 63]

[Sch79] A. J. Scholl, *On the algebra of modular forms on a congruence subgroup*, Math. Proc. Cambridge Philos. Soc. **86** (1979), no. 3, 461–466. [cited at p. 5, 63, 65]

[Ser73a] Jean-Pierre Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, Springer, Berlin, 1973, pp. 319–338. Lecture Notes in Math., Vol. 317. MR 0466020 (57 #5904a) [cited at p. 77, 78]

[Ser73b] ———, *Formes modulaires et fonctions zêta p-adiques*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Springer, Berlin, 1973, pp. 191–268. Lecture Notes in Math., Vol. 350. MR 0404145 (53 #7949a) [cited at p. 10, 25, 57, 72, 76, 86]

[Shi58] Goro Shimura, *Correspondances modulaires et les fonctions ζ de courbes algébriques*, J. Math. Soc. Japan **10** (1958), 1–28. MR 0095173 (20 #1679) [cited at p. 47]

[Shi94] ———, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1. MR 1291394 (95e:11048) [cited at p. 47]

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094 (2010i:11005) [cited at p. 41, 58]

[SS11] Hayato Saito and Tomohiko Suda, *An explicit structure of the graded ring of modular forms of small level (pre-print)*, arXiv:1108.3933v3 [math.NT] (2011). [cited at p. 6]

[Wag80] Philip Wagreich, *Algebras of automorphic forms with few generators*, Trans. Amer. Math. Soc. **262** (1980), no. 2, 367–389. MR 586722 (82e:10044) [cited at p. 6]

[Wag81] ______, *Automorphic forms and singularities with* $\mathbb{C}^*$*-action*, Illinois J. Math. **25** (1981), no. 3, 359–382. MR 620423 (82m:10045) [cited at p. 6]

[Wan98] Daqing Wan, *Dimension variation of classical and p-adic modular forms*, Invent. Math. **133** (1998), no. 2, 449–463. MR 1632794 (99d:11039) [cited at p. 98]

Index