HIGHER CONGRUENCES BETWEEN MODULAR FORMS

by

CATHERINE M. HSU

A DISSERTATION

Presented to the Department of Mathematics
and the Graduate School of the University of Oregon
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

June 2018

DISSERTATION APPROVAL PAGE

Student: Catherine M. Hsu

Title: Higher Congruences Between Modular Forms

This dissertation has been accepted and approved in partial fulfillment of the requirements for the Doctor of Philosophy degree in the Department of Mathematics by:

Ellen Eischen	Chair
Nicolas Addington	Core Member
Benjamin Elias	Core Member
Victor Ostrik	Core Member
Jennifer Ruef	Institutional Representative

and

Sara D. Hodges	Interim Vice Provost and Dean of the Graduate School

Original approval signatures are on file with the University of Oregon Graduate School.

Degree awarded June 2018

DISSERTATION ABSTRACT

Catherine M. Hsu

Doctor of Philosophy

Department of Mathematics

June 2018

Title: Higher Congruences Between Modular Forms

In his seminal work on modular curves and the Eisenstein ideal, Mazur studied the existence of congruences between certain Eisenstein series and newforms, proving that Eisenstein ideals associated to weight 2 cusp forms of prime level are locally principal. In this dissertation, we re-examine Eisenstein congruences, incorporating a notion of "depth of congruence," in order to understand the local structure of Eisenstein ideals associated to weight 2 cusp forms of squarefree level N. Specifically, we use a commutative algebra result of Berger, Klosin, and Kramer to bound the depth of mod p Eisenstein congruences (from below) by the p-adic valuation of $\varphi(N)$. We then show how this depth of congruence controls the local principality of the associated Eisenstein ideal.

CURRICULUM VITAE

NAME OF AUTHOR: Catherine M. Hsu

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon, Eugene, OR
University of North Carolina at Chapel Hill, Chapel Hill, NC
Rice University, Houston, TX

DEGREES AWARDED:

Doctor of Philosophy, Mathematics, 2018, University of Oregon
Master of Science, Mathematics, 2015, Univ. of North Carolina at Chapel Hill
Bachelor of Arts, Mathematics, 2012, Rice University

AREAS OF SPECIAL INTEREST:

Algebraic number theory

PROFESSIONAL EXPERIENCE:

Doctoral Research Fellow, University of Oregon, 2017-2018

Graduate Teaching Fellow, University of Oregon, 2015-2017

GAANN Fellow, Univ. of North Carolina at Chapel Hill, 2013-2015

Graduate Teaching Assistant, Univ. of North Carolina at Chapel Hill, 2012-2013

GRANTS, AWARDS AND HONORS:

Doctoral Research Fellowship, Congruences of Modular Forms, University of Oregon, 2017

American Dissertation Fellowship, Higher Congruences of Modular and Automorphic Forms, American Association for University Women, 2017

PUBLICATIONS:

Hsu, C. (2016). Two classes of number fields with a non-principal Euclidean ideal. *International Journal of Number Theory*, 12.04, 1123-1136.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor, Ellen Eischen, whose mathematical instruction, constructive feedback, and ongoing guidance have been invaluable. I am also grateful to Krzysztof Klosin for generously taking time to provide helpful insights and detailed comments on this project during the past two years. I thank Farshid Hajir, Kimball Martin, Jim Brown, Preston Wake, and Carl Wang-Erickson for many useful conversations.

During my time in graduate school, my research and travel have been generously supported through various fellowships and grants, including a GAANN fellowship, a Johnson Travel Fellowship, and Eischen's UMRP funding. I am especially grateful to have received an AAUW American Dissertation Fellowship and a University of Oregon Doctoral Research Fellowship, both of which supported my research during the 2017-2018 academic year.

My teachers and professors over the last fifteen years have largely shaped the mathematician I am today. In particular, the encouragement of my undergraduate advisor, Professor Tim Cochran, was a large part of my decision to pursue a PhD in mathematics, and I will be forever grateful to him for believing in me.

Lastly, I want to thank my friends and family, especially my parents, for their continuing love and support.

Dedicated to my parents, Rose and Albert, who have supported me no matter what.

TABLE OF CONTENTS

Chapter Page

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

CHAPTER I

INTRODUCTION

Modular forms have played a pivotal role in modern algebraic number theory. They appear in a wide range of contexts, often linking seemingly unrelated areas of mathematics as perhaps most famously seen in the celebrated proof of Fermat's Last Theorem. My research explores the interplay between certain analytic and algebraic objects that arise in the study of congruences between modular forms. Specifically, I focus on the arithmetic properties of the Fourier coefficients of modular forms and how this data is related to the local structure of associated Eisenstein ideals.

In this chapter, I begin by stating the main results of this dissertation, which pertain to higher congruences between weight 2 Eisenstein series and newforms of squarefree level. I then present two levels of motivation for my research. First, I outline the proof of the Herbrand–Ribet Theorem on the structure of ideal class groups in cyclotomic fields, which illustrates how congruences between modular forms can be used to understand the local structure of certain algebraic objects. Second, I recall two results of Mazur, concerning the Eisenstein ideal, which have directly motivated my research.

1.1. Higher congruences between modular forms

In his 1976 proof of the converse to Herbrand's theorem, Ribet [39] introduced the strategy of using congruences between modular forms to construct elements of related class groups. His approach centers on realizing a special value $L(1-k,\chi)$ of an even Dirichlet character as the constant term of an Eisenstein series $E_{k,\chi}$. He shows that if a prime p divides $L(1-k,\chi)$, there exists a cuspidal Hecke eigenform

f whose Hecke eigenvalues are congruent (mod p) to those of $E_{k,\chi}$. This congruence then allows him to use the residual Galois representation attached to f to construct a non-zero element in the class group of the cyclotomic field $\mathbb{Q}(\mu_p)$.

In this dissertation, I generalize Ribet's strategy within the context of higher Eisenstein congruences to establish new properties of other algebraic structures, namely Hecke algebras and Eisenstein ideals. First, following Ribet, I use divisibility properties of the constant term of an Eisenstein series $E_{k,N}$ to establish the existence of a congruence between a newform f and $E_{k,N}$. However, rather than directly using the residual representation $\overline{\rho}_f$ to construct non-zero elements of a class group, I consider all deformations of $\overline{\rho}_f$ to $\mathrm{GL}_2(\overline{\mathbb{Q}}_p)$, which allows me to relate the index of the Eisenstein ideal inside of an associated Hecke algebra to the total depth of Eisenstein congruences for weight k and level N. I then show that this total depth of congruence controls the local structure of the Eisenstein ideal.

1.1.1. Main results with weight $k = 2$. To relate congruences between modular forms to the structure of associated Hecke algebras (rather than class groups as Ribet did), I require *higher congruences*, a refined notion of congruence introduced by Berger–Klosin–Kramer [4], which incorporates a "depth" of congruence. More specifically, for a fixed weight k and level N, let $f_1, \ldots, f_r$ be all newforms of level dividing N. Also, let ϖ_N be a uniformizer in the ring of integers of a sufficiently large extension $E/\mathbb{Q}_p$ with ramification index e_N. Given an Eisenstein series $E_{k,N}$, the depth of congruence between each f_i and $E_{k,N}$ is defined to be the highest power $\varpi_N^{m_i}$ of ϖ_N such that the Hecke eigenvalues (at primes $\ell \nmid N$) of f_i and $E_{k,N}$ are congruent modulo $\varpi_N^{m_i}$. The total depth of congruence for a fixed weight and level is then the sum of the m_i's, normalized by the ramification index e_N.

To connect this total depth of congruence to the structure of the associated Eisenstein ideal, I use a commutative algebra result of Berger–Klosin–Kramer [4], which centers on fitting ideals. More specifically, I examine higher congruences between weight 2 newforms and the weight 2 normalized Eisenstein series given by

$$E_{2,N} = (-1)^{t+1}\frac{\varphi(N)}{24} + \sum_{n=1}^{\infty}\sigma^*(n)q^n,$$

where $N > 1$ is a squarefree integer with t prime factors, φ is Euler's totient function, and $\sigma^*(n)$ is the sum of the divisors of n which are coprime to N. Indeed, by a famous result of Mazur [30], it is known that if a prime $p \geq 5$ divides the constant term of $E_{2,N}$, there exists a newform f of (prime) level dividing N that is congruent modulo p to $E_{2,N}$. In Section 4.2, I give the following lower bound for the total depth of congruence in terms of the p-adic valuation of the index $\#\mathbb{T}/J$, where $\mathbb{T} \subseteq \mathrm{End}(S_2(\Gamma_0(N)))$ is the Hecke algebra generated by Hecke operators T_ℓ for primes $\ell \nmid N$ and J is the associated Eisenstein ideal:

Theorem 1.1.1. *For $i = 1, \ldots, r$, let $\varpi_N^{m_i}$ be the highest power of ϖ_N such that the Hecke eigenvalues of f_i are congruent to those of $E_{2,N}$ modulo $\varpi_N^{m_i}$ for Hecke operators T_ℓ for all primes $\ell \nmid N$. Then, we have*

$$\frac{1}{e_N}(m_1 + \cdots + m_r) \geq \mathrm{val}_p(\#\mathbb{T}/J). \tag{1.1}$$

Now, when the inequality in Eq. (1.1) is strict, the Eisenstein ideal J is not locally principal. So, to use Theorem 1.1.1 to generate examples of squarefree levels for which the Eisenstein ideal is not locally principal, we need to (i) determine the p-adic valuation of $\#\mathbb{T}/J$, ideally in terms of a related L-value, and (ii) show that the depth of Eisenstein congruence modulo p is strictly greater than this p-adic valuation.

Using admissibility results of Ribet–Yoo [50] to show the existence of sufficiently many Eisenstein congruences, I give the following strict lower bound on the total depth of congruence:

Theorem 1.1.2. *If N has at least three prime divisors, then for any $p \geq 5$ dividing $\varphi(N)$, the depth of Eisenstein congruences modulo p is strictly greater than the p-adic valuation of $\varphi(N)$, i.e.,*

$$\frac{1}{e_N}(m_1 + \cdots + m_r) > \mathrm{val}_p(\varphi(N)).$$

If, in addition, $\mathrm{val}_p(\#\mathbb{T}/J) = \mathrm{val}_p(\varphi(N))$, the Eisenstein ideal J is not locally principal.

Note that for prime level N, Mazur [30] proved that the Eisenstein ideal is locally principal. It is not expected that this will carry over to non-prime level, and the second statement in Theorem 1.1.2 establishes a way to show this. Moreover, in Chapter V, I prove an equality between the total depth of Eisenstein congruence and a certain Hilbert–Samuel multiplicity. In future work, I hope to use this to give an explicit bound on the number of generators needed for the localized Eisenstein ideal.

1.2. The Herbrand–Ribet theorem

The *ideal class group* $\mathrm{Cl}(K)$ of a number field K, defined to be the quotient $\mathcal{I}(K)/\mathcal{P}(K)$ of fractional ideals by principal ideals, is an important algebraic structure that encodes a variety of arithmetic data attached to K. To understand its behavior as K varies across families of fields, number theorists have established reciprocities between ideal class groups and other arithmetic objects, the most striking examples arising in class field theory. In this section, we recall certain results about the p-

divisibility of the class group $\mathrm{Cl}(K)$ as K varies across the family of cyclotomic fields $\mathbb{Q}(\zeta_p)$. Indeed, we begin with the following definition:

Definition 1.2.1. An odd prime p is called *irregular* if p divides the class number of $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity.

Kummer introduced this notion of regular and irregular primes as he studied the failure of unique factorization in cyclotomic fields. Indeed, Kummer [25] gives the following classification of irregular primes:

Theorem 1.2.2 (Kummer's criterion)**.** *An odd prime p is irregular if and only if there exists an even integer $2 \leq k \leq p-3$ such that p divides the numerator of the kth Bernoulli number B_k, where B_k is given by the Taylor series*

$$\frac{t}{e^t - 1} = \sum_{n \geq 0} \frac{B_n}{n!} t^n.$$

Now, while Kummer's criterion specifies a straightforward way to determine whether or not a prime p is irregular, it fails to give any additional information about the p-part of the class group of the cyclotomic field $\mathbb{Q}(\zeta_p)$. For example, Theorem 1.2.2 implies that the size of the ideal class group $\mathrm{Cl}(\mathbb{Q}(\zeta_{691}))$ is divisible by 691 (since $p = 691$ divides the numerator of $B_{12}/24 = -691/65520$) but does not specify any structure in the p-part of $\mathrm{Cl}(\mathbb{Q}(\zeta_{691}))$. Using classical algebraic number theory techniques, Herbrand [19] refined Kummer's criterion by giving a a "piece-by-piece" description of the structure of the p-part of $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ in terms of the p-divisibility of certain Bernoulli numbers. To state his result precisely, we require the following notation.

Let A be the p-Sylow subgroup of the ideal class group $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ of $\mathbb{Q}(\zeta_p)$, and let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. The character group $\hat{G}$ of G is then given by

$$\hat{G} = \{\omega^i \,|\, 0 \leq i \leq p-2\},$$

where ω is the Teichmüller character, i.e., the character $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ such that for each $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\omega(a) \in \mathbb{Z}_p$ is the $(p-1)$st root of unity satisfying

$$\omega(a) \equiv a \pmod{p}.$$

Since we are viewing ω as a p-adic character (rather than as a complex character), we may consider the group ring $\mathbb{Z}_p[G]$ and construct its orthogonal idempotents

$$\varepsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1} \in \mathbb{Z}_p[G], \qquad 0 \leq i \leq p-2.$$

Since $p^n A = 0$ for sufficiently large n, we may consider A as a $\mathbb{Z}_p$-module, and so, since G also acts on A, A is a $\mathbb{Z}_p[G]$-module. In particular, A decomposes as

$$A = \bigoplus_{i=0}^{p-2} A_i, \qquad \text{where } A_i = \varepsilon_i A.$$

Given this decomposition of A as a $\mathbb{Z}_p[G]$-module, Herbrand improved Kummer's criterion by relating each submodule A_i to the p-divisibility of a Bernoulli number:

Theorem 1.2.3 (Herbrand)**.** *Let i be odd with $3 \leq i \leq p-2$. If $A_i \neq 0$, then $p \,|\, B_{p-i}$.*

Herbrand's proof of this theorem uses only classical algebraic number theory tools, including the Stickelberger element of $\mathbb{Q}(\zeta_p)$ and Stickelberger's Theorem, and can be found in [47, §6.3]. Over forty years later, Ribet proved the converse to

Herbrand's theorem. However, unlike Herbrand's (classical) proof, Ribet required much more machinery. Indeed, he utilized Galois representations and algebraic properties of modular forms to prove:

Theorem 1.2.4 (Ribet)**.** *Let i be odd with $3 \leq i \leq p-2$. If $p \mid B_{p-i}$, then $A_i \neq 0$.*

The proof of this theorem is quite insightful, even when considered independently of Herbrand's theorem, in part because Ribet explicitly constructs an unramified abelian extension of $\mathbb{Q}(\zeta_p)$ that has exponent p and satisfies specific local conditions. It is of particular interest to us because it illustrates one way that congruences between modular forms are useful. While we do not include Ribet's proof in detail, we outline his approach, adapting a summary by Mazur [33, Figure 1]. Indeed, Figure 1 gives the six main components of Ribet's proof; our goal is to briefly explain the role of each, with a particular focus on the relationships between the components, i.e., the arrows appearing throughout the circle.

First, note that $\boxed{1} \to \boxed{2}$ is addressed by Herbrand's theorem. To obtain the converse direction $\boxed{2} \to \boxed{1}$, Ribet works (counter-clockwise) around the circle:

$\boxed{2} \to \boxed{3}$: Ribet begins by realizing a special value $L(1-k, \chi)$ of an even Dirichlet character as the constant term of an Eisenstein series $E_{k,\chi}$, which allows him to use the rich theory of modular forms to study the arithmetic properties of Bernoulli numbers. In particular, the idea of recognizing L-values as constant terms of modular forms arises in many contexts, such as Serre's construction of p-adic modular forms [42], and was introduced by Klingen [24] and Siegel [43, 44].

$\boxed{3} \to \boxed{4}$: While mathematicians had studied congruences between modular forms prior to this proof, Ribet requires the existence of specific congruences, namely congruences between weight 2 cusp forms and weight k Eisenstein series

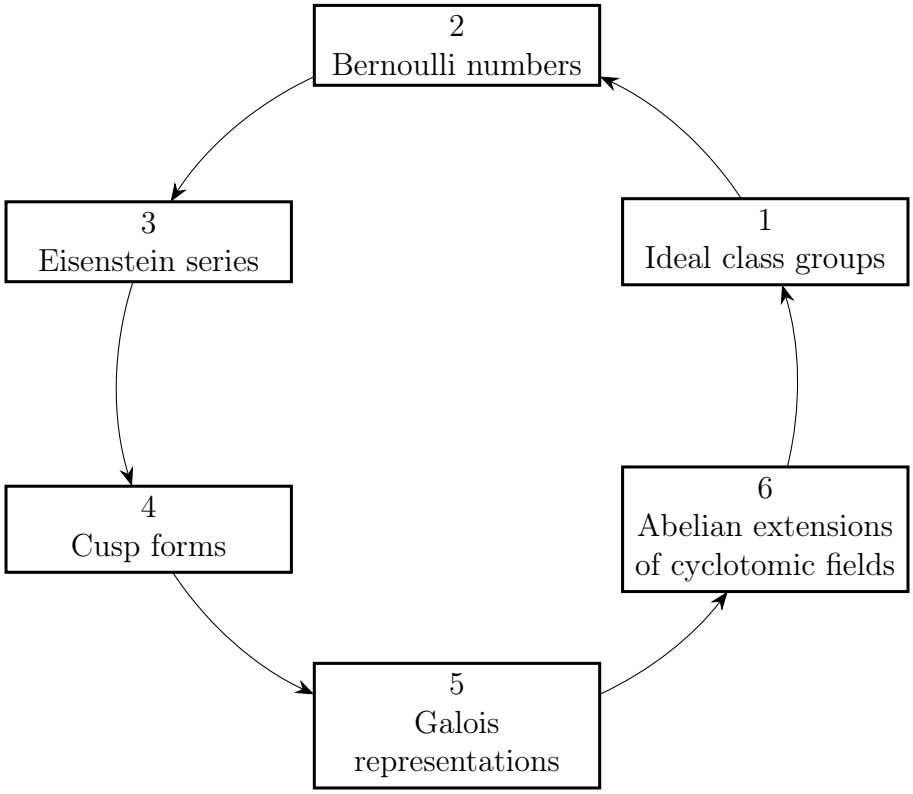

Figure 1. Facets of number theory

of level 1. Note that Ribet could have instead looked for Eisenstein congruences with cusp forms of higher weights but chooses weight 2 in part because of convenient properties of the associated Galois representations. The fact that Ribet could have worked in any weight illustrates a more general principle discovered later, namely that modulo p, all modular forms are weight 2 [23].

$\boxed{4} \rightarrow \boxed{5}$: Following the work of Serre and Deligne [13], Ribet is able to associate to any weight 2 cusp form f an irreducible Galois representation ρ_f that satisfies certain algebraic properties. In particular, since the cusp form f satisfies an Eisenstein congruence, Ribet studies the residual Galois representation $\overline{\rho}_f$, whose semi-simplification is the direct sum of two characters determined by the Eisenstein series under consideration. See [40] for more details on Galois representations attached to cusp forms.

$\boxed{5} \rightarrow \boxed{6} \rightarrow \boxed{1}$: By choosing a suitable lattice for $\overline{\rho}_f$, Ribet explicitly constructs an unramified abelian extension of $\mathbb{Q}(\zeta_p)$ that has exponent p and satisfies specific local conditions. (Because of its importance to Ribet's proof, Mazur refers to this step as the "Ribet wrench".) Once Ribet has constructed the required extension of $\mathbb{Q}(\zeta_p)$, class field theory gives the last arrow back to $\boxed{1}$.

We end this section by highlighting two important ideas that follow from this discussion. First, beginning with Kummer's criterion, we have seen a somewhat surprising phenomenon: the existence of a close relationship between seemingly unrelated analytic and algebraic objects. In this case, the work of Kummer, Herbrand, and Ribet establish an explicit relationship between the p-structure of certain ideal class groups and the p-divisibility of Bernoulli numbers. This phenomenon occurs in many other areas of algebraic number theory, including the Langlands program. Second, we note that the components in Figure 1 utilize a wide range of number

theory techniques with varying levels of accessibility. For example, the behavior of ideal class groups in families of number fields is quite hard to predict while Bernoulli numbers are easily computable. As we have seen, it is advantageous to use a more accessible object to understand a more mysterious one.

My research is most closely connected to components $\boxed{3}$, $\boxed{4}$, $\boxed{5}$ in Figure 1. As I will explain in the next section, while my strategy is based upon Ribet's method, there are several key differences between the two approaches.

1.3. Mazur's Eisenstein ideal

In his seminal work *Modular curves and the Eisenstein ideal* [30], Mazur studies the $\mathbb{Q}$-rational points of the modular curves $X_1(N)$ and $X_0(N)$ when N is a prime number. While this paper contains many results, two particular theorems, which we now recall, have largely motivated my research.

Theorem 1.3.1 (Mazur)**.** *Let $N > 1$ be prime. If a prime p divides the numerator of $\frac{N-1}{12}$, then there exists a weight 2 newform $f \in S_2(\Gamma_0(N))^{\text{new}}$ such that*

$$f \equiv E_{2,N} \pmod{p},$$

where $E_{2,N}$ is a normalized weight 2 Eisenstein series of level N.

Note that in contrast to Ribet's converse to Herbrand's theorem, whose proof utilizes a congruence between a weight 2 cusp form and a weight k Eisenstein series of level 1, this result establishes the existence of a congruence between a weight 2 cusp form and a weight 2 Eisenstein series of level N.

Now, Theorem 1.3.1 arose in connection to Mazur's work on the local structure of the Eisenstein ideal inside a certain Hecke algebra. While we use slightly modified definitions of these algebraic objects in later chapters, we recall their definitions as

they appear in [30]. Indeed, let $J_0(N)$ denote the Jacobian (over $\mathbb{Q}$) of the modular curve $X_0(N)$.

Definition 1.3.2. The *Hecke algebra* $\mathbb{T} \subseteq \mathrm{End}(J_0(N))$ is defined to be the subring generated over $\mathbb{Z}$ by Hecke operators T_ℓ for all $\ell \neq N$ and the involution w induced by $(z \mapsto 1/Nz)$ on the upper half-plane.

Definition 1.3.3. The *Eisenstein ideal* $\mathfrak{J}$ is defined to be the ideal of $\mathbb{T}$ generated by $1 + \ell - T_\ell$ for all $\ell \neq N$ and $1 + w$.

Remark 1.3.4. As explained in [30, II.6], while the algebra $\mathbb{T}$ acts, by definition, on $J_0(N)$, it also acts on many other objects, including various spaces of modular forms. In particular, the Hecke algebras we consider, cf. Definitions 2.2.4, 2.2.5, operate on spaces of elliptic modular forms. To see that these definitions are compatible with Definition 1.3.2, we note that the space $S_2(\Gamma_0(N))$ can be identified with the cotangent space at 0 of $J_0(N)$. See [48, §2.1.3] for more details.

Given these definitions, Mazur proves the following theorem about the local structure of $\mathfrak{J}$:

Theorem 1.3.5 (Mazur)**.** *The Eisenstein ideal* $\mathfrak{J}$ *is locally principal in* $\mathbb{T}$*.*

By "locally principal in $\mathbb{T}$," we mean that for every prime ideal $\mathfrak{P} \subset \mathbb{T}$, the ideal $\mathfrak{J} \cdot \mathbb{T}_\mathfrak{P}$ is principal, where $\mathbb{T}_\mathfrak{P} = \varprojlim_n \mathbb{T}/\mathfrak{P}^n$ denotes the completion of $\mathbb{T}$ at $\mathfrak{P}$. For certain primes called *Eisenstein primes*, Mazur actually gives an explicit numerical criterion for the element $\eta_\ell = 1 + \ell + T_\ell$ to be a local generator of $\mathfrak{J}$ at the Eisenstein prime $\mathfrak{P}$. See [30, Theorem I.11, Theorem II.16.6, and §II.7] for more details.

These results of Mazur raise the following two questions:

Question 1.3.6. For a fixed level N, is there a precise way to quantify all such Eisenstein congruences (as in Theorem 1.3.1), including a notion of "depth"?

Question 1.3.7. For a fixed squarefree level N, can we determine the local structure of the associated Eisenstein ideal?

When the level N is prime, Question 1.3.6 is answered by a result of Berger–Klosin–Kramer [4, Proposition 3.1]. When the level N is squarefree, I answer this question two ways. First, in Theorem 4.0.1, I give a strict lower bound for the total depth of congruence using Euler's totient function. Additionally, I show in Theorem 5.1.1 that this depth of congruence can be interpreted as a Hilbert–Samuel multiplicity. For Question 1.3.7, I use the higher congruences framework to show that the total depth of congruence controls the local principality of the Eisenstein ideal; I then give a conditional answer as to when the Eisenstein ideal is not locally principal.

This dissertation is organized as follows. Chapter II gives background information on modular forms and Hecke algebras. Chapter III recalls important commutative algebra results, including on Hilbert–Samuel multiplicities. Chapter IV presents and proves the main results of this dissertation, and Chapter V gives computational examples and an interesting application of the main results. Appendix A provides the algorithm used to compute examples of Eisenstein congruences, and Appendix B gives a geometric construction of modular forms.

CHAPTER II

MODULAR FORMS AND HECKE THEORY

In this chapter, we focus on the relationship between modular forms and Hecke theory. Indeed, we begin by developing some of the rich theory of modular forms for various congruence subgroups. We then recall portions of Hecke theory, including several compatible formulations of Hecke operators, and state the main result of Atkin–Lehner theory, i.e., the multiplicity one theorem. We conclude by explaining the important duality that exists between Hecke algebras and certain spaces of modular forms. Throughout this chapter, we follow the notation of [14, 15].

2.1. Elliptic modular forms

Let $\mathfrak{h}$ denote the complex upper half-plane, and consider the action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathfrak{h}$ given by Möbius transformations: for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ and $z \in \mathfrak{h}$,

$$\gamma z := \frac{az+b}{cz+d}\,.$$

A subgroup $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$ is called a congruence subgroup if it contains

$$\Gamma(N) = \left\{ \gamma \in \mathrm{SL}(2,\mathbb{Z}) \,|\, \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

for some positive integer N. Note that $\Gamma(N)$ is called the principal congruence subgroup (of level N). Throughout this dissertation, we are primarily concerned

with the following two congruence subgroups:

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}(2,\mathbb{Z}) \,|\, \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}(2,\mathbb{Z}) \,|\, \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Given a non-negative k and a congruence subgroup $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$, a modular form (of weight k with respect to Γ) is a complex analytic function on $\mathfrak{h}$ that satisfies a certain functional equation with respect to the group action of Γ as well as growth condition at the cusps:

Definition 2.1.1. Let k be a non-negative integer, and let Γ be a congruence subgroup. A *modular form of weight k with respect to* Γ is a complex function $f : \mathfrak{h} \to \mathbb{C}$ that satisfies the following properties:

(i) f is holomorphic on $\mathfrak{h}$;

(ii) $f(\gamma z) = (cz+d)^k f(z), \quad \forall\, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$;

(iii) f is holomorphic at the cusps.

To give a more precise explanation of Condition (iii) above, we need to recall a useful fact about modular forms, namely that each has a Fourier expansion at ∞. Indeed, since the congruence subgroup Γ contains the principal subgroup for some level N, there is some positive integer h such that $f(z+h) = f(z)$. Thus, $f \in M_k(\Gamma)$ has a Fourier expansion at ∞ of the form

$$f(z) = \sum_{-\infty}^{\infty} a_n q_h^n, \qquad q_h = e^{2\pi i z/h}. \tag{2.1}$$

Note that since $\Gamma_0(N)$ and $\Gamma_1(N)$ both contain the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we take $h = 1$ for these congruence subgroups and drop the subscript h. Given the Fourier expansion

of f at ∞, we say that f is holomorphic (resp. vanishes) at ∞ if $a_n(f) = a_n = 0$ for all $n < 1$ (resp. $n \leq 0$). More generally, f is holomorphic (resp. vanishes) at the cusps if for all $\alpha \in \mathrm{SL}(2, \mathbb{Z})$,

$$(f|[\alpha]_k)(z) := (c_\alpha z + d_\alpha)^{-k} f(\alpha z) \tag{2.2}$$

is holomorphic (resp. vanishes) at ∞. We denote the space (over $\mathbb{C}$) of modular forms of weight k with respect to Γ by $M_k(\Gamma)$ and the space of cusp forms, i.e., modular forms which vanish at the cusps, by $S_k(\Gamma)$.

Example 2.1.2. Let $k > 2$ be an even integer and define for each $z \in \mathfrak{h}$

$$G_k(z) = \sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z},\\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}. \tag{2.3}$$

One can show that $G_k(z)$ is a modular form of weight k with respect to $\mathrm{SL}(2, \mathbb{Z})$, i.e., $G_k(z) \in M_k(\mathrm{SL}(2, \mathbb{Z}))$, and that its Fourier expansion is given by

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right),$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ and the Bernoulli numbers B_k are defined by

$$\frac{te^t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

In particular, by restricting the sum in Eq. (2.3) to relatively prime pairs (m, n), we obtain the *normalized Eisenstein series*

$$E_k(z) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \tag{2.4}$$

See [14, §2.2] or [7, Ch. 1 §2.1] for more details as well as additional examples.

Remark 2.1.3. Because this construction might seem unmotivated, we briefly give two natural ways to view Eisenstein series. First, we can interpret the sum in Eq. (2.4) as an "averaging" over a certain quotient space in $\mathrm{SL}(2,\mathbb{Z})$. Indeed, given a linear action $v \mapsto v|g$ of the group G on a vector space V, we can try to construct a G-invariant vector in V by taking an arbitrary vector $v_0 \in V$ and forming the sum $\sum_{g\in G} v_0|g$. When v_0 is stabilized by an infinite subgroup of G, this sum often converges. So, if we take $G = \mathrm{SL}(2,\mathbb{Z})$ and quotient by the stabilizer Γ_∞ of the cusp at infinity, we can write Eisenstein series as the sum $\sum_{\Gamma_\infty/\mathrm{SL}(2,\mathbb{Z})} 1|[\gamma]_k$, which yields Eq. (2.4). (See Example 2.1.6 for the definition of Γ_∞.) A second way to construct Eisenstein series is to use an alternative definition of modular forms which views them as functions on complex lattices that satisfy certain transformation properties. This important perspective leads to Eq. (2.3) and is revisited in Section 2.2.4. See [7, Ch. 1 §1.1, 2.1] for more details.

Example 2.1.4. When $k = 2$, the right-hand side of Eq. (2.4), i.e.,

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n) q^n, \tag{2.5}$$

makes sense as a complex function (and is holomorphic on $\mathfrak{h}$ and at ∞) but fails to be a modular form since it does not satisfy the weight 2 modularity property with respect to $\mathrm{SL}(2,\mathbb{Z})$. Using the following technique of Hecke [18, §2], we can use $E_2(z)$ to construct weight 2 Eisenstein series for the congruence subgroup $\Gamma_0(N)$.

For any integer $N > 0$, define the function

$$E_2(z) - NE_2(Nz) = E_2(z) - c(\pi y)^{-1} + c(\pi y)^{-1} - NE_2(Nz),$$

with some $c \neq 0$. $E_2(z) - c(\pi y)^{-1}$ is a nearly holomorphic function and satisfies the weight 2 modularity property for $\mathrm{SL}(2,\mathbb{Z})$. (See [7, Ch. 1 §5.3] for the definition of a nearly holomorphic function.) Hence, the function $E_{2,N}(z) = E_2(z) - NE_2(Nz)$ is a holomorphic function satisfying the weight 2 modularity property for $\Gamma_0(N)$, i.e., $E_{2,N}(z) \in M_2(\Gamma_0(N))$. More generally, given numbers $c_d \in \mathbb{C}$ for $d \,|\, N$ such that $\sum_{d|N} c_d/d = 0$, the function $\sum_{d|N} c_d E_2(dz)$ belongs to $M_2(\Gamma_0(N))$. For example, when $N = p$ is a prime, then the function

$$E_2(z) - pE_2(pz) = (1-p) - 24\sum_{n=1}^{\infty}\Big(\sum_{\substack{(d,p)=1,\\ d|n}} d\Big)q^n \tag{2.6}$$

is a weight 2 modular form of level p.

Example 2.1.5. Let

$$\Delta(z) = \frac{1}{1728}\left(E_4^3(z) - E_6^2(z)\right).$$

Then $\Delta(z)$ is a weight 12 modular form for the congruence subgroup $\mathrm{SL}(2,\mathbb{Z})$. Since the constant term in its q-expansion is 0, as seen from the formulas in Eq. (2.4), $\Delta(z)$ vanishes at ∞. Moreover, since $(\Delta|[\alpha]_{12})(z) = \Delta(z)$ for all $\alpha \in \mathrm{SL}(2,\mathbb{Z})$, we see that Δ vanishes at all the cusps, i.e., $\Delta \in S_{12}(\mathrm{SL}(2,\mathbb{Z}))$. Its q-expansion is given by

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

Now, let $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character mod N. Abusing notation, this character extends to a multiplicative map $\varepsilon : \mathbb{Z} \to \mathbb{C}$, where, by convention, we define $\varepsilon(n) = 0$ if $\gcd(n, N) > 1$. A modular form of weight k, level N, and character (or Nebentypus) ε is an element of $M_k(\Gamma_1(N))$ that also transforms under $\Gamma_0(N)$ by

the character ε, i.e.,

$$f(\gamma z) = \varepsilon(d)(cz+d)^k f(z)), \quad \forall\, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

We denote the space of modular forms of weight k, level N, and character ε by $M_k(\Gamma_0(N), \varepsilon) = M_k(N, \varepsilon)$. In particular, there is a direct sum decomposition

$$M_k(\Gamma_1(N)) = \bigoplus_{\varepsilon} M_k(N, \varepsilon), \tag{2.7}$$

where ε runs over all Dirichlet characters mod N such that $\varepsilon(-1) = (-1)^k$. Moreover, by defining $S_k(N, \varepsilon)$ to be the space of cusp forms in $M_k(N, \varepsilon)$, we obtain an analogous decomposition of $S_k(\Gamma_1(N))$.

Example 2.1.6. For an integer $k \geq 1$ and a Dirichlet character $\varepsilon \pmod N$ such that $\varepsilon(-1) = (-1)^k$, Hecke [18] defines an Eisenstein series in $M_k(N, \varepsilon)$ by

$$E_{k,N,\varepsilon}(z) = \sum_{\gamma \in \Gamma_\infty / \Gamma_0(N)} \frac{\overline{\varepsilon}(d_\gamma)}{(c_\gamma z + d_\gamma)^k},$$

where $\Gamma_\infty = \{\pm \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right) \mid m \in \mathbb{Z}\}$ is the stabilizer of ∞ in $\Gamma_0(N)$ and $\overline{\varepsilon}(d_\gamma))$ denotes the complex conjugate of $\varepsilon(d_\gamma)$. In particular, when ε is primitive, the Fourier expansion of $E_{k,N,\varepsilon}$ is given by

$$E_{k,N,\varepsilon}(z) = 1 - \frac{2k}{B_{k,\varepsilon}} \sum_{n=1}^{\infty} \left(\sum_{d|n} \varepsilon(d)\, d^{k-1} \right) q^n,$$

where $B_{k,\varepsilon}$ is a generalized Bernoulli number [14, pg. 44]. If $\varepsilon \pmod N$ is not primitive, then $E_{k,N,\varepsilon}$ can be written as a linear combination of the Eisenstein series $E_{k,C,\varepsilon_0}(dz)$ over divisors d of N/C, where C is the conductor of the ε_0, the primitive

character associated to ε. There are many additional ways to construct Eisenstein series, which are discussed extensively in [15, Ch. 4].

2.2. Hecke theory

In this section, our goal is to find a canonical basis for the space of cusp forms $S_k(\Gamma_1(N))$. To accomplish this, we use Hecke theory to decompose $S_k(\Gamma_1(N))$ into *old* and *new* subspaces, the latter of which has a basis of simultaneous eigenfuctions under the action of all Hecke operators. The old subspace is a direct sum of images of new subspaces under level raising maps and has a basis of simultaneous eigenfunctions under the Hecke action for operators away from N. We start by defining Hecke operators as double coset operators and then express this action in terms of Fourier coefficients of cusp forms. We end the section by giving compatible Hecke actions on elliptic curves and modular curves and explaining the connection between them.

2.2.1. The double coset operator. Let Γ_1 and Γ_2 be congruence subgroups of $\mathrm{SL}(2,\mathbb{Z})$. For each $\alpha \in \mathrm{GL}^+(2,\mathbb{Q})$, we consider the double set in $\mathrm{GL}^+(2,\mathbb{Q})$ defined by

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 : \gamma_1 \in \Gamma_1,\ \gamma_2 \in \Gamma_2\}.$$

We may consider a group action of Γ_1 on the double coset $\Gamma_1\alpha\Gamma_2$ given by left multiplication, and the resulting orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is finite [15, §5.1]. In particular, the finiteness of this orbit space allows us to define an action of the double coset on modular forms as follows:

Definition 2.2.1. For congruence subgroups Γ_1 and Γ_2 of $\mathrm{SL}(2,\mathbb{Z})$ and $\alpha \in \mathrm{GL}^+(2,\mathbb{Q})$, the *weight-k* $\Gamma_1\alpha\Gamma_2$ *operator* takes functions $f \in M_k(\Gamma_1)$ to

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f|[\beta_j]_k \in M_k(\Gamma_2), \tag{2.8}$$

where $\{\beta_j\}$ are orbit representations, i.e., $\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$ is a disjoint union.

Note that the double coset operator $\Gamma_1\alpha\Gamma_2$ transforms modular forms with respect to Γ_1 into modular forms with respect to Γ_2 [15, §5.1].

2.2.2. Hecke action on $M_k(\Gamma_1(N))$. We now use two specific types of double coset operators with $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ to define the Hecke operators on $M_1(\Gamma_1(N))$. Indeed, for any $\alpha \in \Gamma_0(N)$, we first consider the weight-k double coset operator $[\Gamma_1(N)\alpha\Gamma_1(N)]_k$. Since $\Gamma_1(N) \lhd \Gamma_0(N)$, we have $\Gamma_1(N)\alpha\Gamma_1(N) = \Gamma_1(N)\alpha$, and hence, this operator acts on $M_k(\Gamma_1(N))$ by mapping each $f \in M_k(\Gamma_1(N))$ to

$$f[\Gamma_1(N)\alpha\Gamma_1(N)]_k = f[\Gamma_1(N)\alpha]_k = f|[\alpha]_k, \qquad \alpha \in \Gamma_0(N).$$

We may thus view this action as the group $\Gamma_0(N)$ acting on $M_k(\Gamma_1(N))$, and so, since the action of $\Gamma_1(N)$ is trivial, we may also view it as an action of the quotient $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. In particular, since the action of $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is completely determined by $d \pmod N$, we may write it as $\langle d\rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$, where

$$\langle d\rangle f = f|[\gamma]_k, \text{ for any } \gamma = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N) \text{ with } \delta \equiv d \pmod N.$$

Such an operator is called a *diamond operator* and is the first type of Hecke operator that we consider. A particularly nice feature of these operators is that for any Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, the space $M_k(N,\varepsilon)$ of modular forms of weight k, level

N, and character ε is exactly the ε-eigenspace of the diamond operators. Note that this implies that the diamond operators $\langle d \rangle$ both act trivially on $S_k(\Gamma_0(N))$ and respect the decomposition of $M_k(\Gamma_1(N))$ in Eq. (2.7).

The second type of Hecke operator we consider is also defined by a weight-k double coset operator $[\Gamma_1(N)\alpha\Gamma_1(N)]_k$, except now with

$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \quad p \text{ prime.}$$

To explicitly describe the action of this Hecke operator, denoted T_p, in terms of Fourier coefficients, we require orbit representatives for $\Gamma_1(N)\backslash\Gamma_1(N)\alpha\Gamma_1(N)$. Indeed, the desired representatives appear in the following proposition, which gives a formula for the action of T_p on $M_k(\Gamma_1(N))$:

Proposition 2.2.2. *The operator $T_p = [\Gamma_1(N)\alpha\Gamma_1(N)]_k$, where $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$, acts on the space $M_k(\Gamma_1(N))$ by*

$$T_p f = \begin{cases} \displaystyle\sum_{j=0}^{p-1} f|[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k & \text{if } p \mid N, \\ \displaystyle\sum_{j=0}^{p-1} f|[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k + f|[\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_k & \text{if } p \nmid N, \text{ where } mp - nN = 1. \end{cases}$$

To simplify notation, for the remainder of the chapter, we write

$$\beta_j = \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) \quad \text{for } 0 \le j < p, \quad \beta_\infty = \left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \quad \text{if } p \nmid N. \tag{2.9}$$

While this proposition would immediately allow us to express the action of Hecke operators T_p on the Fourier coefficients of a modular form $f \in M_k(\Gamma_1(N))$, we first explain how to extend the definitions of the operators $\langle d \rangle$ and T_p to all positive integers $n \in \mathbb{Z}_+$. Indeed, since the diamond operators $\langle d \rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ and the

Hecke operators T_p for primes p all commute [15, Proposition 5.2.4], it makes sense to extend these operators multiplicatively. So, for diamond operators $\langle n \rangle$, $n \in \mathbb{Z}_+$, we define $\langle nm \rangle = \langle n \rangle \langle m \rangle$ for all $n, m \in \mathbb{Z}_+$, with $\langle n \rangle = 0$ if $(n, N) > 1$ and $\langle n \rangle$ determined by $n \pmod N$ otherwise. For Hecke operators T_n, $n \in \mathbb{Z}_+$, we cannot use a totally multiplicative definition because $T_{p^2} \neq T_p T_p$. Rather we set $T_1 = 1$ and then use the following inductive definition for T_{p^r}:

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}, \qquad \text{for } r \geq 2.$$

Given this definition and the fact that $T_{p^r} T_{q^s} = T_{q^s} T_{p^r}$ for $(p, q) = 1$, we may define T_n for all $n \in \mathbb{Z}_+$ by $T_n = \prod T_{p^{e_i}}$, where $n = \prod p^{e_i}$. In particular, this definition implies that all T_n commute and satisfy $T_{mn} = T_m T_n$ if $(n, m) = 1$.

Since we want to find a basis simultaneous eigenfunctions under the action of the Hecke operators T_n, it is useful to describe Hecke action of T_n in terms of Fourier expansions of modular forms. Indeed, computing the Fourier expansions of $f|[\beta_j]_k$ and $f|[\beta_\infty]_k$ in Proposition 2.2.2 yields the following formula for the Hecke action of T_n on the Fourier coefficients of a modular form:

Proposition 2.2.3. *Let $\sum_0^\infty a_n q^n$ be the q-expansion of $f \in M_k(N, \varepsilon)$, and let $\sum_0^\infty b_n q^n$ be the q-expansion of $T_m f$. Then the coefficients b_n are given by*

$$b_n = \sum_{d | (m,n)} \varepsilon(d) d^{k-1} a_{mn/d^2}. \tag{2.10}$$

It is important to remember that by convention, $\varepsilon(p) = 0$ when $p \,|\, N$, and so for $p \,|\, N$, T_p has a modified formula for its action on Fourier expansions, as reflected in Proposition 2.2.2. To emphasize this difference, we write U_p to denote the Hecke operator T_p for $p \,|\, N$.

2.2.3. Hecke eigenforms. For $k \geq 2$ and $N > 1$, we now consider two different subrings of $\mathrm{End}_{\mathbb{C}}(M_k(\Gamma_1(N)))$, each of which is generated by certain Hecke and diamond operators. Since it is important whether or not these subrings include the operators U_p, we distinguish between these cases with the following definitions:

Definition 2.2.4. The *full Hecke algebra*, denoted $\tilde{\mathbb{T}}_N$, is the subring of $\mathrm{End}_{\mathbb{C}}(M_k(\Gamma_1(N)))$ generated over $\mathbb{Z}$ by $\{T_n\}$ for all $n \in \mathbb{N}$.

Definition 2.2.5. The *anemic Hecke algebra*, denoted $\tilde{\mathbb{T}}^{(N)}$, is the subring of $\mathrm{End}_{\mathbb{C}}(M_k(\Gamma_1(N)))$ generated over $\mathbb{Z}$ by $\{T_p, \langle q \rangle\}$ for all primes $p \nmid N$ and all primes $q \nmid N$.

As discussed in [14, Proposition 3.5.1], there are many ways to generate these Hecke algebras. For example, the set $\{T_p, \langle q \rangle\}$ for all primes p and all primes $q \nmid N$ also generates $\tilde{\mathbb{T}}_N$. Since each choice of generating set yields the same subring of $\mathrm{End}_{\mathbb{C}}(M_k(\Gamma_1(N)))$, we continue to use those in Definitions 2.2.4, 2.2.5.

Remark 2.2.6. (i) We use the subscript or superscript of N to distinguish between the full and anemic Hecke algebras. When it clear from context which Hecke algebra we are using, we drop the N from our notation.

(ii) As defined above, both $\tilde{\mathbb{T}}_N$ and $\tilde{\mathbb{T}}^{(N)}$ are $\mathbb{Z}$-subalgebras of $\mathrm{End}_{\mathbb{C}}(M_k(\Gamma_1(N)))$; in later sections, we consider analogous Hecke algebras generated over other rings. When there are multiple rings being considered, we use an additional subscript to distinguish between them. If no additional subscript is used, we assume that the Hecke algebra is a $\mathbb{Z}$-subalgebra.

(iii) Since the Hecke and diamond operators all preserve cusp forms, we may restrict the actions of $\tilde{\mathbb{T}}_N$ and $\tilde{\mathbb{T}}^{(N)}$ to $S_k(\Gamma_1(N))$. We denote their respective images in $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_1(N)))$ by $\mathbb{T}_N$ and $\mathbb{T}^{(N)}$.

For $\tilde{\mathbb{T}} = \tilde{\mathbb{T}}_N$ or $\tilde{\mathbb{T}}^{(N)}$, a modular form is called a $\tilde{\mathbb{T}}$-eigenform if it is a common eigenvector under all operators $T \in \tilde{\mathbb{T}}$. Using the generators of the Hecke algebras $\tilde{\mathbb{T}}_N$ and $\tilde{\mathbb{T}}^{(N)}$ described in Definitions 2.2.4, 2.2.5, we give a more precise definition:

Definition 2.2.7. A modular form $f \in M_k(\Gamma_1(N))$ is a $\tilde{\mathbb{T}}_N$-*eigenform* if and only if it is a simultaneous eigenvector under all T_n; it is a $\tilde{\mathbb{T}}^{(N)}$-*eigenform* if and only if it has Nebentypus ε (for some character ε) and is a common eigenvector under T_p for all primes $p \nmid N$. An eigenform $f(z) = \sum_{n=0}^{\infty} a_n q^n$ is said to be *normalized* when $a_1(f) = 1$.

Given any $\tilde{\mathbb{T}}$-eigenform f, we define a homomorphism

$$\theta_f : \tilde{\mathbb{T}} \to \mathbb{C}, \quad Tf = \theta_f(T) f,$$

which is called the *eigencharacter* of f. In particular, its image is contained in a number field, and the eigenvalues $\lambda_n(f) = \theta_f(T_n)$ lie in its ring of integers [14, Corollary 12.4.5].

Now, since $\tilde{\mathbb{T}}^{(N)}$ is a subring of $\tilde{\mathbb{T}}_N$, a $\tilde{\mathbb{T}}_N$-eigenvector is necessarily a $\tilde{\mathbb{T}}^{(N)}$-eigenvector; the converse is not true. However, the commutativity of the Hecke operators involved implies that a $\tilde{\mathbb{T}}^{(N)}$-eigenform is a $\tilde{\mathbb{T}}_N$-eigenform if the $\tilde{\mathbb{T}}^{(N)}$-eigenspace it belongs to is one-dimensional. As we will see in §2.3.1, $\tilde{\mathbb{T}}^{(N)}$-eigencharacters usually occur with multiplicity greater than one but appear with multiplicity one for certain modular forms called *newforms*.

We end this subsection by observing that Proposition 2.2.3 implies that every $\tilde{\mathbb{T}}_N$-eigenspace is at most one-dimensional. Indeed, suppose that $f \in M_k(N, \varepsilon)$ is a (non-zero) $\tilde{\mathbb{T}}_N$-eigenform, and let $\sum_0^{\infty} a_n q^n$ be the q-expansion of f. If λ_n denotes the

nth eigenvalue, i.e., $T_n f = \lambda_n f$, then Eq. (2.10) applied to $a_1(T_n f)$ gives that

$$a_n = \lambda_n a_1 \text{ for all } n \in \mathbb{N}.$$

In fact, if $a_0 \neq 0$, then Eq. (2.10) applied to $a_0(T_n f)$ gives that

$$\lambda_n = \sum_{d|n} \varepsilon(d) d^{k-1}.$$

Thus, if two forms in $M_k(N, \varepsilon)$ are $\tilde{\mathbb{T}}_N$-eigenforms with the same eigencharacter $\{\lambda_n\}$, then one must be a scalar multiple of the other. Note that throughout this discussion, we have fixed a level N; we give a much stronger statement in Section 2.3.2 regarding the multiplicity of Hecke eigencharacters as we vary the level.

2.2.4. Revisiting the double coset operator. So far, we have defined the Hecke operator T_p as a double coset operator on $M_k(\Gamma_1(N))$ with its linear action given in terms of Fourier coefficients. While this definition of T_p is sufficient for the higher congruences framework used in later chapters, we give two additional compatible interpretations of T_p, one using modular curves and one using elliptic curves.

For a congruence subgroup Γ of $\mathrm{SL}(2, \mathbb{Z})$, we define the associated *modular curve* $Y(\Gamma)$ to be the quotient space $Y(\Gamma) = \Gamma \setminus \mathfrak{h}$. Such a modular curve is a (non-compact) Riemann surface [15, §1.5], and so we can use certain algebraic characteristics of $Y(\Gamma)$ to reformulate the notion of the Hecke operator T_p. Specifically, for $\Gamma = \Gamma_1(N)$ or $\Gamma_0(N)$, we use modular correspondences on $Y(\Gamma) \times Y(\Gamma)$ to define the operator T_p as a homomorphism on the divisor group $\mathrm{Div}(Y(\Gamma))$. While this reformulation is interesting on its own, it becomes especially useful if we interpret the curves $Y_1(N) = Y(\Gamma_1(N))$ and $Y_0(N) = Y(\Gamma_0(N))$ as moduli spaces for certain complex elliptic curves.

Indeed, we first consider the modular curve $Y_1(N)$, whose points are naturally in bijection with isomorphism classes of pairs (E, Q), where E is a complex elliptic curve and Q is a point of E of order N. (Note that two pairs (E, Q) and (E', Q') are said to be isomorphism if some isomorphism $E \xrightarrow{\sim} E'$ takes Q to Q'.) To establish this bijection, we associate to each $\tau \in \mathfrak{h}$ the pair

$$\mathbb{E}_\tau = (\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau), \tag{2.11}$$

where Λ_τ is the lattice $\mathbb{Z} + \mathbb{Z}_\tau$. We define $S_1(N)$ to be the set of isomorphism classes $[E, Q]$ of pairs (E, Q) so that there is a natural bijection between the set $S_1(N)$ and the modular curve $Y_1(N)$. Similarly, the points of $Y_0(N)$ naturally parametrize the set $S_0(N)$ of isomorphism class of pairs (E, R), where E is again a complex elliptic curve but R is a cyclic subgroup of E of order N. Because we have realized the modular curves $Y_1(N)$ and $Y_0(N)$ as moduli spaces of elliptic curves, it is useful to describe the Hecke action of T_p in terms of modular correspondences on these curves. Throughout the rest of this subsection, we focus primarily on the modular curve $\Gamma_1(N)$; there are analogous statements for $\Gamma_0(N)$ which can be found in [14, §7.2-7.3].

Remark 2.2.8. The moduli-theoretic interpretations of the modular curves $Y_1(N)$ and $Y_0(N)$ can actually be obtained via base-change within broader moduli problems. Indeed, we can define a contravariant functor $\mathcal{F}_1(N)$ from $\mathbb{Z}[1/N]$-schemes to sets by taking a scheme over $\mathbb{Z}[1/N]$ to a set of isomorphism classes of elliptic curves over S. Under certain conditions, we can then find a scheme $\mathcal{Y}_1(N)$ which represents the functor $\mathcal{F}_1(N)$. In particular, this moduli problem plays an important role in viewing modular forms as sections of line bundles on modular curves and is presented in Appendix B.

We now give a geometric interpretation of T_p in terms of transferring points on the modular curve $Y_1(N)$ and then naturally translate this to a moduli-theoretic point of view. Indeed, for $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \in \mathrm{GL}^+(2, \mathbb{Q})$, consider the following configuration of the congruence subgroups $\Gamma_1 = \Gamma_1(N)$, $\Gamma_2 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_1$, and $\Gamma_2' = \alpha\Gamma_2\alpha^{-1}$:

$$\begin{array}{ccc} \Gamma_2 & \xrightarrow{\sim} & \Gamma_2' \\ \big\downarrow & & \big\downarrow \\ \Gamma_1 & & \Gamma_1 \end{array}$$

Note that the group isomorphism is given by $\gamma \mapsto \alpha\gamma\alpha^{-1}$ and the vertical arrows are inclusions. The corresponding configuration of modular curves is then given by

$$\begin{array}{ccc} Y_2 & \xrightarrow{\sim} & Y_2' \\ {\scriptstyle \pi_1}\big\downarrow & & \big\downarrow{\scriptstyle \pi_1} \\ Y_1 & & Y_1 \end{array}$$

where the modular curve isomorphism $Y_2 \xrightarrow{\sim} Y_2'$ is given by $\Gamma_2\tau \mapsto \Gamma_2'\alpha\tau$ and denoted α. In particular, since $\Gamma_1\alpha\Gamma_1 = \bigcup_j \Gamma_1\beta_j$, where the β_j are as in Eq. (2.9), each point of Y_1 is taken by $\pi_1 \circ \alpha \circ \pi_1^{-1}$ to a set of points of Y_1:

$$\begin{array}{ccc} \{\Gamma_2\alpha^{-1}\beta_j\tau\} & \xrightarrow{\alpha} & \{\Gamma_2'\beta_j\tau\} \\ {\scriptstyle \pi_1^{-1}}\big\uparrow & & \big\downarrow{\scriptstyle \pi_1} \\ \Gamma_1\tau & & \{\Gamma_1\beta_j\tau\} \end{array}$$

Because π_1^{-1} takes each point $x \in Y_1$ to a multiset of points $y \in Y_2$ (which includes multiplicity according to its ramification degree) and we want $\pi_1 \circ \alpha \circ \pi_1^{-1}$ to reflect this multiplicity, we express $\pi_1 \circ \alpha \circ \pi_1^{-1}$ in terms of the divisor group of Y_1:

$$[\Gamma_1\alpha\Gamma_1]_k : Y_1 \to \mathrm{Div}(Y_1), \qquad \Gamma_1\tau \mapsto \sum_j \Gamma_1\beta_j\tau. \tag{2.12}$$

The Hecke operator T_p can then be viewed as the unique $\mathbb{Z}$-linear extension

$$T_p : \mathrm{Div}(Y_1) \to \mathrm{Div}(Y_1). \tag{2.13}$$

Moreover, by identifying points of $Y_1(N)$ with pairs (E, Q) as in Eq. (2.11), we obtain the following moduli-theoretic interpretation of T_p:

$$T_p : \mathrm{Div}(S_1(N)) \to \mathrm{Div}(S_1(N)), \qquad [E, Q] \mapsto \sum_C [E/C, Q + C], \tag{2.14}$$

where the sum is taken over all order p subgroups $C \subset E$ such that $C \cap \langle Q \rangle = \{0_E\}$. In particular, each of the subgroups C appearing in the summation of Eq. (2.14) is asoociated to one of the elements β_j (including β_∞ if $p \nmid N$). Indeed, for $0 \leq j < p$, we associate $C_j = \langle (\tau + j)/p \rangle + \Lambda_\tau$ to β_j and for $j = \infty$, we associate $C_\infty = \langle 1/p \rangle + \Lambda_\tau$ to β_∞. See [15, §5.2] for more details.

It is important to note that the actions of T_p defined in Eqs. (2.12) and (2.14) are compatible, i.e., we have the following commutative diagrams:

$$\begin{array}{ccc} \mathrm{Div}(Y_1(N)) & \xrightarrow{T_p} & \mathrm{Div}(Y_1(N)) \\ \wr\downarrow & & \downarrow\wr \\ \mathrm{Div}(S_1(N)) & \xrightarrow{T_p} & \mathrm{Div}(S_1(N)) \end{array} \qquad \begin{array}{ccc} \Gamma_1(N)\tau & \longmapsto & \sum_j \Gamma_1(N)\beta_j\tau \\ \downarrow & & \downarrow \\ [E_\tau, \frac{1}{N} + \Lambda_\tau] & \longmapsto & \sum_C [E_\tau/C, \frac{1}{N} + C] \end{array}$$

We end this section with a brief discussion of the action of the diamond operators $\langle d \rangle$, $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, on $Y_1(N)$ and $S_1(N)$. Indeed, recall that we have identified $(\mathbb{Z}/N\mathbb{Z})^\times$ with the quotient space $\Gamma_0(N)/\Gamma_1(N)$, and so, since the action of $\Gamma_0(N)$ on $\mathfrak{h}$ induces an action of $\Gamma_0(N)/\Gamma_1(N)$ on $Y_1(N)$, we have a corresponding action of $\langle d \rangle$ on Y_1. In particular, the automorphism $\langle d \rangle$ of $Y_1(N)$ has the moduli-theoretic interpretation $[E, Q] \mapsto [E, dQ]$, and so, since $\langle -1 \rangle$ acts as the identity, the action of $(\mathbb{Z}/N\mathbb{Z})^\times$ actually factors through $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$. We can thus realize the modular curve $Y_0(N)$ as the quotient of $Y_1(N)$ by the action of $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, and the natural projection $Y_1(N) \to Y_0(N)$ has the moduli-theoretic interpretation $[E, Q] \mapsto [E, \langle Q \rangle]$, where $\langle Q \rangle$ is the subgroup of E generated by Q.

Remark 2.2.9. As mentioned above, for a congruence subgroup $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$, the modular curve $Y(\Gamma)$ is a non-compact Riemann surfaces; we can compactify it by adjoining the cusps in a the following way. Let $\mathfrak{h}^* = \mathfrak{h} \cup \mathbb{Q} \cup \{\infty\}$, and take the extended quotient

$$X(\Gamma) = \Gamma \setminus \mathfrak{h}^* = Y(\Gamma) \cup \Gamma \setminus (\mathbb{Q} \cup \{\infty\}).$$

See [14, §9] and [15, Ch. 2] for more details. While we do not require compact modular curves in this section, we use them in Appendix B when we construct modular forms as sections of line bundles on modular curves.

2.3. Atkin–Lehner theory

We now restrict our attention to the action of Hecke operators on the space of weight k cusp forms of level N; note that we fix a weight k but allow the level to vary. To further study the space $S_k(\Gamma_1(N))$, we first make it into an inner product space by using the *Petersson inner product*, which is defined as follows. Let $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ be a congruence subgroup. The Petersson inner product

$$\langle\ ,\ \rangle_\Gamma : S_k(\Gamma) \times S_k(\Gamma) \to \mathbb{C}$$

is given by

$$\langle f, g\rangle = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)}(\mathrm{Im}(\tau))^k d\mu(\tau),$$

where $1/V_\Gamma$ is a normalizing factor and $d\mu$ is the hyperbolic measure on the upper half plane. This product is linear in f, conjugate linear in g, Hermitian-symmetric, and positive definite; for more details see [15, Definition 5.4.1] or [14, §3.6]

Given the space $S_k(\Gamma_1(N))$ endowed with the Petersson inner product, we consider the adjoint operators of $\langle p \rangle$ and T_p for $p \nmid N$. Specifically, it can be shown that the Hecke operators $\langle n \rangle$ and T_n for $(n, N) = 1$ commute with their adjoints, i.e., they are normal operators [15, Theorem 5.5.3]. Hence, since $\mathbb{T}^{(N)}$ is a commuting family of normal operators acting on the finite-dimensional inner product space $S_k(\Gamma_1(N))$, spectral theory guarantees that $S_k(\Gamma_1(N))$ has an orthogonal basis of $\mathbb{T}^{(N)}$-eigenforms; our goal in this section is to give such a basis in a canonical way. To do so, we need to consider modular forms of different levels at the same time, which is the main focus of Section 2.3.2 on the multiplicity one theorem.

Note that while we formulate results for the space $S_k(\Gamma_1(N))$ throughout the section, there are analogous statements for each subspace $S_k(N, \varepsilon)$.

2.3.1. Old and new subspaces. We are now ready to use the action of $\mathbb{T}_N$ and $\mathbb{T}^{(N)}$ on $S_k(\Gamma_1(N))$ to give a canonical basis for $S_k(\Gamma_1(N))$. Indeed, let $d, M, N > 0$ be integers such that $dM \mid N$, and consider the injective map

$$\begin{aligned} \iota^*_{d,M,N} : S_k(\Gamma_1(M)) &\to S_k(\Gamma_1(N)), \\ f(z) &\mapsto d^{k-1} f(dz). \end{aligned}$$

When a prime p does not divide N, the action of $\iota^*_{d,M,N}$ is compatible with the action of the Hecke operators T_p, i.e., $T_p(\iota^*_{d,M,N}(f)) = \iota^*_{d,M,N}(T_p(f))$, where T_p on the left side (resp. right side) of the equation is relative to the level N (resp. M). Thus, the map $\iota^*_{d,M,N}$ is a homomorphism of $\mathbb{T}^{(N)}$-modules where we regard $S_k(\Gamma_1(M))$ as a $\mathbb{T}^{(N)}$ module using the inclusion $\mathbb{T}^{(N)} \subset \mathbb{T}^{(M)}$. In particular, if $f \in S_k(\Gamma_1(M))$ is a $\mathbb{T}^{(M)}$-eigenform, then for d dividing N/M, the form $\iota^*_{d,M,N}(f) \in S_k(\Gamma_1(N))$ is a $\mathbb{T}^{(N)}$-eigenform with the same eigenvalues away from N.

For a fixed N, we define the *old subspace* of $S_k(\Gamma_1(N))$ by

$$S_k(\Gamma_1(N))^{\text{old}} = \bigoplus_{\substack{dM|N \\ M \neq N}} \iota^*_{d,M,N} \left(S_k(\Gamma_1(M)) \right), \tag{2.15}$$

where the direct sum is taken over all d, M with $dM \,|\, N$ and $M \neq N$. Note that it is non-trivial to show that the direct sum in Eq. (2.15) is in fact a direct sum; as discussed in [14, Remark 6.3.4], this follows from multiplicity one and the linear independence of the images of a fixed eigenform under the maps $\iota^*_{d,M,N}$.

We now define the *new subspace* of $S_k(\Gamma_1(N))$, denoted $S_k(\Gamma_1(N))^{\text{new}}$, to be the orthogonal complement of the $S_k(\Gamma_1(N))^{\text{old}}$ with respect to the Petersson inner product. Given this definition, we can rewrite Eq. (2.15) as

$$S_k(\Gamma_1(N))^{\text{old}} = \bigoplus_{\substack{dM|N \\ M \neq N}} \iota^*_{d,M,N} \left(S_k(\Gamma_1(M)^{\text{new}}) \right)$$

so that

$$S_k(\Gamma_1(N)) = \bigoplus_{dM|N} \iota^*_{d,M,N} \left(S_k(\Gamma_1(M)^{\text{new}}) \right).$$

In particular, for each M, the spectral decomposition theorem for normal operators implies that the $\mathbb{T}^{(M)}$-module $S_k(\Gamma_1(M))^{\text{new}}$ admits a basis consisting of $\mathbb{T}^{(M)}$-eigenforms [14, §3.6]. Thus, $S_k(\Gamma_1(N))$ has a basis of $\mathbb{T}^{(N)}$-eigenforms $\{f\}$, where each f is of the form $f = \iota^*_{d,M,N}(g_i)$ for some $\mathbb{T}^{(M)}$-eigenform $g_i \in S_k(\Gamma_1(M))^{\text{new}}$ with $dM \,|\, N$. While the existence of a basis of $S_k(\Gamma_1(N))$ consisting of $\mathbb{T}^{(N)}$-eigenforms is guaranteed by the spectral decomposition theorem, the decomposition of $S_k(\Gamma_1(N))$ into old and new subspaces yields a canonical way to find this basis. Moreover, as we will see in Section 2.3.2, it allows us to simultaneously consider modular forms of different levels.

Now, since the level raising maps $\iota^*_{d,M,N}$ commute with the action of $(\mathbb{Z}/N\mathbb{Z})^\times$, where we define the action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $S_k(\Gamma_1(M))$ via the natural projection $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times$, there is a $\mathbb{T}^{(N)}$-equivariant decomposition

$$S_k(\Gamma_1(N))^{\text{old}} = \bigoplus_{\varepsilon} S_k(N,\varepsilon)^{\text{old}},$$

where $S_k(N,\varepsilon)^{\text{old}} = S_k(N,\varepsilon) \cap S_k(\Gamma_1(N))^{\text{old}}$. Moreover, there is an analogous decomposition of the new subspace into eigenspaces $S_k(N,\varepsilon)^{\text{new}}$ which satisfy

$$S_k(N,\varepsilon) = S_k(N,\varepsilon)^{\text{old}} \oplus S_k(N,\varepsilon)^{\text{new}}. \tag{2.16}$$

When ε is the trivial character, Eq. (2.16) gives a decomposition of $S_k(\Gamma_0(N))$ into old and new subspaces. Alternatively, for any ε, we can give intrinsic definitions of the old and new subspaces of $S_k(N,\varepsilon)$ by appropriately modifying the maps $\iota^*_{d,M,N}$ and then considering Dirichlet characters mod M for all $M \mid N$. See [14, pgs. 60-61] for more details.

Example 2.3.1. The space $S_2(\mathrm{SL}(2,\mathbb{Z})) = S_2(\Gamma_1(1))$ is empty, so when $k = 2$ and $N = p$ is prime, we have the decomposition $S_2(\Gamma_1(N)) = S_2(\Gamma(N))^{\text{new}}$.

Example 2.3.2. Let $k = 2$ and $N = 33$. Using the dimension formulas given in [14, Example 12.1.3], we can compute that $S_2(\Gamma_1(33))$ is 21-dimensional, $S_2(\Gamma_1(3)) = 0$, and $S_2(\Gamma_1(11)) = S_2(\Gamma_0(11))$ is one-dimensional. So, let f be the normalized $\mathbb{T}_{11}$-eigenform generating $S_2(\Gamma_1(11))$. Using the level raising maps $\iota^*_{1,11,33}$ and $\iota^*_{3,11,33}$, we see that $S_2(\Gamma_1(33))^{\text{old}} = S_2(\Gamma_0(33))^{\text{old}}$ is two-dimensional, spanned by the linearly independent forms $f(z)$ and $f(3z)$. Now, the space $S_2(\Gamma_1(33))^{\text{new}}$ decomposes as

$$S_k(\Gamma_1(33))^{\text{new}} = \bigoplus_{\varepsilon} S_k(33,\varepsilon)^{\text{new}},$$

where ε runs over the 10 Dirichlet characters mod 33 which satisfy $\varepsilon(-1) = 1$. For the trivial character ε, we can compute that $S_2(\Gamma_1(33), \varepsilon)^{\text{new}} = S_2(33)^{\text{new}}$ is one-dimensional, generated by a $\mathbb{T}_{33}$-eigenform. For the nontrivial characters ε, we can apply dimension formulas to groups intermediate to $\Gamma_1(33)$ and $\Gamma_0(33)$. In particular, to simply computations, we can partition the characters into orbits under the Galois action of $\text{Gal}(\mathbb{Q}(\zeta_{10})/\mathbb{Q})$ and compute the appropriate dimensions for a representative of each orbit. Then [14, Proposition 12.3.11] gives the dimensions for the remaining characters. Note that while $f(z)$ and $f(3z)$ are not $\mathbb{T}_{33}$-eigenforms, suitable linear combinations of them are, and so, $S_2(\Gamma_1(33))$ is actually spanned by $\mathbb{T}_{33}$-eigenforms. As is discussed in Section 2.3.2, this does not always happen.

It is important to note that while both $S_2(\Gamma_1(N))^{\text{old}}$ and $S_2(\Gamma_1(N))^{\text{new}}$ are stable under the action of the full Hecke algebra $\mathbb{T}_N$, only $S_2(\Gamma_1(N))^{\text{new}}$ is guaranteed to have a basis of $\mathbb{T}_N$-eigenforms. Such eigenforms are the main focus of the next section and play an important role in finding a canonical basis for $S_2(\Gamma_1(N))$.

2.3.2. Multiplicity one theorem. We now state the main result of Atkin–Lehner theory, which establishes that a Hecke eigencharacter occuring in the new subspace $S_k(\Gamma_1(N))^{\text{new}}$ does so with multiplicity one. Indeed, because we want to compare eigenforms of varying weight, we need to consider a broader set of modular forms, namely forms which are simultaneous eigenvectors under the Hecke operators T_p for almost all primes p. To do this, we introduce an auxiliary positive integer D and consider the action of $\mathbb{T}^{(ND)}$.

We first recall the following key fact from [14, Proposition 6.2.1], which is the foundation for proving the multiplicity one theorem:

Proposition 2.3.3. *Let $f = \sum_1^\infty a_n q^n$ be a cusp form on $\Gamma_1(N)$ and suppose there is an integer $D \geq 1$ such that for all $(n, ND) = 1$, we have $a_n = 0$. Then there exists*

a cusp form g_p on $\Gamma_1(N/p)$ for each prime $p \,|\, N$ such that

$$f = \sum_{p|N} \iota_p^*(g_p),$$

i.e., $f \in S_k(\Gamma_1(N))^{\text{old}}$.

From this proposition and Eq. (2.10), it follows that if f is a cusp form on $\Gamma_1(N)$ which is a simultaneous eigenfunction under T_p for almost all primes $p \nmid N$, then if $a_1(f) = 0$, f is in the old subspace. Hence, we can normalize any (non-zero) $\mathbb{T}^{(ND)}$-eigenform $f \in S_k(\Gamma_1(N))^{\text{new}}$ so that $a_1(f) = 1$.

We now state the multiplicity one theorem [14, Theorem 6.2.3]:

Theorem 2.3.4. *Let $f, g \in S_k(\Gamma_1(N))$ be $\mathbb{T}^{(ND)}$-eigenforms with the same Hecke eigencharacters, i.e., $\theta_f(T_p) = \theta_g(T_p)$ for all $p \nmid ND$. If $f \in S_k(\Gamma_1(N))^{\text{new}}$ with f normalized, then g is a scalar multiple of f. In particular, if g is in the old subspace, then $g = 0$.*

This theorem is called the multiplicity one theorem because it implies that the subspace $S_k(\Gamma_1(N))^{\text{new}}$ is an orthogonal sum of $\mathbb{T}^{(ND)}$-eigenspaces in $S_k(\Gamma_1(N))$ whose eigencharacters occur with multplicity one. In fact, $S_k(\Gamma_1(N))^{\text{new}}$ is exactly the orthogonal sum of all such eigenspaces. Indeed, for $g \in S_k(\Gamma_1(M))^{\text{new}}$ with $M \neq N$, we've established that the cusp forms $g = \iota_{1,M,N}^*(g)$ and $\iota_{d,M,N}^*(g)$ (with $d > 1$, $dM \,|\, N$) have the same $\mathbb{T}^{(ND)}$-eigencharacter. Since they are also linearly independent [14, Corollary 6.3.1], Theorem 2.3.4 implies that $S_k(\Gamma_1(N))^{\text{old}}$ is the orthogonal sum of the $\mathbb{T}^{(ND)}$-eigenspaces in $S_k(\Gamma_1(N))$ whose eigencharacters occur with multiplicity strictly greater than 1.

Now, as explained at the end of Section 2.2.3, a $\mathbb{T}^{(N)}$-eigenform whose eigenspace is one-dimensional is always a $\mathbb{T}_N$-eigenform. Hence, the following are equivalent in the new subspace $S_k(\Gamma_1(N))^{\text{new}}$:

(i) f is a $\mathbb{T}_N$-eigenform;

(ii) f is a $\mathbb{T}^{(N)}$-eigenform;

(iii) f is a $\mathbb{T}^{(ND)}$-eigenform for some D.

Such an eigenform form f that has been normalized so that $a_1 = 1$ is called a *newform* or a *primitive* cusp form, and these forms play an important role in establishing a duality between the anemic Hecke algebra and a certain space of cusp forms. Note that while Conditions (ii) and (iii) are equivalent in the old subspace, they do not imply Condition (i). The subspace $S_k(\Gamma_1(N))^{\text{old}}$ is, however, stable under the action of the larger Hecke algebra $\mathbb{T}_N$ [15, Proposition 5.6.2].

Remark 2.3.5. The most important feature of the multiplicity one theorem is that it holds as the level varies. Indeed, let $f_i \in S_k(\Gamma_1(N_i))$, for $i = 1, 2$, be two normalized Hecke eigenforms with eigenvalues a_p^i under T_p for primes p, and suppose that $a_p^1 = a_p^2$ for all but finitely many primes. By considering their functional equations [14, Remark 5.0.2], we see that $N_1 = N_2$, and hence, by Theorem 2.3.4, we must have $f_1 = f_2$. Thus, for a $\mathbb{T}^{(ND)}$-eigenspace in $S_k(\Gamma_1(N))$, there exists a unique pair (f, M) such that f is in the eigenspace and a newform of level M.

2.4. Duality between modular forms and Hecke algebras

In our original definition of a modular form (Definition 2.1.1), we consider complex-analytic functions that satisfy certain growth results as well as a functional equation. However, it is useful for a variety of reasons, particularly in the context

of congruences between modular forms, to consider modular forms whose Fourier coefficients lie in rings other than $\mathbb{C}$. Indeed, by relating modular forms to the cohomology of modular curves, we can develop a rich theory of such forms, including a q-expansion principle. The details of this perspective are given in Appendix B.

The main goal of this section is to describe a duality between various Hecke algebras and spaces of cusp forms. In the case of the full Hecke algebra and the space $S_k(\Gamma_0(N))$, such a relationship is given in the literature [41, 17, 14]. We outline these results in the first subsection. In the case of the anemic Hecke algebra, we give an analogous duality and explain how this case differs from that of the full Hecke algebra. As far as I know, the results for the anemic Hecke algebra do no appear in the literature. To simplify notation, particularly in the case of the anemic Hecke algebra, we assume trivial Nebentypus through the end of this section, i.e., we restrict our attention to the space $S_k(\Gamma_0(N))$.

2.4.1. The full Hecke algebra. Recall that $S_k(\Gamma_0(N))$ is the $\mathbb{C}$-vector space of weight k cusp forms on the congruence subgroup $\Gamma_0(N)$, where $N \geq 1$ and $k \geq 2$ are integers. We define $\mathbf{S}_k(\Gamma_0(N); \mathbb{Z})$ to be the cusp forms in $S_k(\Gamma_0(N))$ whose Fourier coefficients lie in $\mathbb{Z}$ and consider the space $\mathbf{S}_k(\Gamma_0(N); R) = \mathbf{S}_k(\Gamma_0(N); \mathbb{Z}) \otimes R$ for an arbitrary ring R. From a naive perspective, we want $\mathbf{S}_k(\Gamma_0(N); R)$ to be the space of modular forms whose Fourier coefficients lie in R. Indeed, as a consequence of the q-expansion principle [14, Theorem 12.3.4], we can make such an identification for suitable rings R. (See the discussion after Theorem B.4.2 for instances where this fails.) So, while we give a precise relationship between these spaces of cusp forms in Appendix B, for now, we think of $\mathbf{S}_k(\Gamma_0(N); R)$ as the space of modular forms over R.

The following proposition [14, Proposition 12.4.13] establishes a duality between the space of cusp forms $\mathbf{S}_k(\Gamma_0(N); R)$ and the Hecke ring $\mathbb{T}_N$:

Proposition 2.4.1. *For every ring R, $\mathbf{S}_k(\Gamma_0(N); R)$ is isomorphic to* $\mathrm{Hom}_R(\mathbb{T}_N, R)$.

Proof. We prove this statement for $R = \mathbb{Z}$; the general case follows by extending scalars. Indeed, let $S(\mathbb{Q})$ denote the subspace of $S_2(\Gamma_0(N))$ consisting of cusp forms whose Fourier coefficients are rational numbers. Also, let $M \subset S(\mathbb{Q})$ be the lattice consisting of cusp forms with integral Fourier coefficients. By the q-expansion principle, we have an injective map

$$\begin{aligned} \phi_\infty : M &\to \mathbb{Z}[\![q]\!], \\ f &\mapsto \textstyle\sum_0^\infty a_n q^n, \end{aligned} \tag{2.17}$$

which maps a form to its Fourier expansion. Moreover, by the definition of M, the cokernel of ϕ_∞ is torsion free. So, consider the bilinear pairing

$$\begin{aligned} \mathbb{T}_N \times M &\to \mathbb{Z}, \\ (T, f) &\mapsto a_1(Tf), \end{aligned} \tag{2.18}$$

where $a_n(Tf)$ denotes the nth Fourier coefficient of Tf. This pairing induces maps

$$\begin{aligned} \varphi : M &\to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_N, \mathbb{Z}) = \mathbb{T}_{\mathbb{Z}}^\vee, \\ \psi : \mathbb{T}_N &\to \mathrm{Hom}_{\mathbb{Z}}(L, \mathbb{Z}) = L^\vee. \end{aligned} \tag{2.19}$$

We show that φ is an isomorphism. First, since $a_n(f) = a_1(T_n f)$, the injectivity and torsion free cokernel of ϕ_∞ immediately implies that φ is also injective with torsion free cokernel. So, since $\mathbb{T}_N$ and M are free finite rank $\mathbb{Z}$-modules (see [14, Corollary 12.4.3] or [15, page 234] for a proof of the fact that $\mathbb{T}_N$ is a free finite rank $\mathbb{Z}$-module), it suffices to show that ψ is injective. Indeed, if $T \mapsto 0 \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$, then $a_1(Tf) = 0$ for all $f \in M$. Substituting $T_n f$ for f and using the commutativity

of $\mathbb{T}_N$, we obtain

$$a_1(T(T_n f)) = a_1(T_n(Tf)) = a_n(Tf) = 0,$$

for all $n \geq 1$, and hence, $Tf = 0$ by the injectivity of ϕ_∞. Since this holds for all $f \in M$, we must have $T = 0$. The last equality follows from the fact that $S_2(\Gamma_0(N))$ has a basis in $\mathbf{S}_k(\Gamma_0(N); \mathbb{Z})$ [14, Corollary 12.3.8]. Thus, the rank of $\mathbb{T}_N$ is at most that of M, and $\varphi : M \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_N, \mathbb{Z})$ is an isomorphism, as desired. □

Remark 2.4.2. Rather than using the fact that the cokernel of ϕ_∞ is torsion free, we could show that φ is surjective by extending scalars to $\mathbb{C}$. Indeed, since both $M \otimes \mathbb{C}$ and $\mathbb{T}_N \otimes \mathbb{C}$ are finite-dimensional vector spaces over $\mathbb{C}$, the injectivity of φ and ψ immediate imply that φ is an isomorphism. This approach is used in [17].

2.4.2. The anemic Hecke algebra. As discussed in Section 2.3, there is not necessarily a basis for $S_k(\Gamma_0(N))$ consisting of $\mathbb{T}_N$-eigenforms, and so it can be useful to exclude the Hecke operators U_p for $p \,|\, N$ from the Hecke algebra. When the level N is prime, this exclusion does not actually have an effect because the operator U_p acts as the identity [8, Proposition 3.19]. However, for squarefree level, U_p can act as ± 1 on each newform $f \in S_k(\Gamma_0(N))^{\mathrm{new}}$ [1, Theorem 3], and so the anemic and full Hecke algebras no longer coincide. While we focus more on the relationship between these Hecke algebras in Chapter IV, we now give an analogue of Proposition 2.4.1 for the anemic Hecke algebra.

For any subring $R \subset \mathbb{C}$, we write $\mathbb{T}_R^{(N)}$ for the R-subalgebra of $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_0(N)))$ generated by the Hecke operators T_ℓ for primes $\ell \nmid N$. Note that since $\mathbb{Z}$ is a PID,

$$\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_0(N))) = \mathrm{End}_{\mathbb{C}}(\mathbf{S}_k(\Gamma_0(N); \mathbb{Z}) \otimes \mathbb{C}) = \mathrm{End}_{\mathbb{Z}}(\mathbf{S}_k(\Gamma_0(N); \mathbb{Z})) \otimes \mathbb{C},$$

and so we are viewing $\mathbb{T}_R^{(N)}$ as the subalgebra $\mathbb{T}_{\mathbb{Z}}^{(N)} \otimes R \subseteq \mathbb{T}_N \otimes \mathbb{R}$. Note also that the algebra $\mathbb{T}_{\mathbb{Z}}^{(N)}$ coincides with the anemic Hecke algebra in Definition 2.2.5.

In the case of the full Hecke algebra, the duality between $\mathbb{T}_N$ and $\mathbf{S}_k(\Gamma_0(N); \mathbb{Z})$ follows from the fact that the map ϕ_∞ in Eq. (2.17) is both injective and has a torsion free cokernel. So, in the case of the anemic Hecke algebra, we would like to define a ring R and an R-submodule $L \subseteq \mathbf{S}_k(\Gamma_0(N); R)$ for which the modified map

$$\begin{aligned} \phi_\infty^{(N)} : L &\to \mathbb{Z}[\![q]\!], \\ f &\mapsto \sum_{\substack{(n,N)=1 \\ n \geq 1}} a_n q^n, \end{aligned} \tag{2.20}$$

is both injective and has a torsion free cokernel. Indeed, in order for $\phi_\infty^{(N)}$ to be injective, we immediately know that L cannot contain any cusp forms of type $\iota_{d,M,N}^*(g)$, where $dM \mid N$ with $d > 1$, i.e.,

$$L \subseteq \bigoplus_{M|N} S_k(\Gamma_0(M))^{\text{new}}. \tag{2.21}$$

However, the direct sum in Eq. (2.21), which we denote L', need not have a basis in $\mathbf{S}_k(\Gamma_0(N); \mathbb{Z})$, and so to restrict to an R-submodule in L' in a reasonable way, we need to choose a ring R that contains all of the Fourier coefficients of the newforms spanning L'. For commutative algebra reasons discussed in Chapter III, R also needs to be a local ring, and thus, we take R to be the ring of integers $\mathcal{O}$ in a sufficiently large extension of $\mathbb{Q}_p$, where p is any prime number. Note that since $\mathbb{Z}_p$ is flat over $\mathbb{Z}$ (since $\mathbb{Z}_p$ is torsion free and $\mathbb{Z}$ is a PID), we do not need to assume that $p \nmid N$.

The natural analogue of Proposition 2.4.1 would then be a duality between the $\mathcal{O}$-module of $\mathbf{S}_k(\Gamma_0(N); \mathcal{O})$ spanned by all newforms $f_1, \ldots, f_r$ of level N_{f_i} dividing N and the anemic Hecke algebra $\mathbb{T}_{\mathcal{O}}^{(N)}$. However, while $\phi_\infty^{(N)}$ is injective (as established

by Lemma 2.4.5), a problem arises with this analogue because the modified map $\phi_\infty^{(N)}$ does not have a torsion free cokernel. The following example illustrates this:

Example 2.4.3. Let $k = 2$, $N = 182 = 2 \times 7 \times 13$, and $p = 3$. Consider the following newforms of levels 14, 26, and 91, respectively:

$$f_1 = q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 + O(q^8) \in S_2(\Gamma_0(14)),$$
$$f_2 = q - q^2 + q^3 + q^4 - 3q^5 - q^6 - q^7 + O(q^8) \in S_2(\Gamma_0(26)),$$
$$f_3 = q - 2q^3 - 2q^4 - 3q^5 + q^7 + O(q^9) \in S_2(\Gamma_0(91)).$$

Each of these newforms is congruent to the Eisenstein series $E_{2,182}$ away from N, and so the Fourier coefficients of the modular form $g = \frac{1}{3}(f_1 + f_2 + f_3)$ all lie in $\mathbb{Z}_3$ for all $(n, N) = 1$. Moreover, we can check directly that $a_7(g) = \frac{1}{3} \notin \mathbb{Z}_3$, and so, g is not an element of $\mathbf{S}_2(\Gamma_0(N); \mathbb{Z}_3)$. However, we clearly have $3g \in \mathbf{S}_2(\Gamma_0(N); \mathbb{Z}_3)$, which illustrates the fact that $\phi_\infty^{(N)}$ might have torsion in its cokernel. More generally, we can construct examples of torsion in the cokernel of $\phi_\infty^{(N)}$ by using the fact that the Hecke eigenvalue of U_p, $p|N$ is always ± 1 [36, Lemma 4.1].

To eliminate such torsion in the cokernel of $\phi_\infty^{(N)}$, we could define L to be the $\mathcal{O}$-submodule of $S_k(\Gamma_0(N))$ with $\mathcal{O}$-integral coefficients away from N. While this $\mathcal{O}$-module allows us to generalize the argument from the previous section, it is not a natural space to consider. We therefore take $R = \mathbb{C}$ and establish a duality between the anemic Hecke algebra $\mathbb{T}_{\mathbb{C}}^{(N)}$ and the $\mathbb{C}$-subspace L of $S_k(\Gamma_0(N))$ spanned by newforms $f_1, \ldots, f_r$. In particular, this duality between vector spaces suffices to give a (weaker) relationship between $\mathbb{T}_{\mathcal{O}}^{(N)}$ and the newforms $f_1, \ldots, f_r$ because we can extend scalars from $\mathbb{T}_{\mathcal{O}}^{(N)}$ to $\mathbb{T}_{\mathbb{C}}^{(N)}$.

Consider the bilinear pairing

$$\begin{aligned} \mathbb{T}_{\mathbb{C}}^{(N)} \times L &\to \mathbb{C} \\ (T, f) &\mapsto a_1(Tf), \end{aligned} \tag{2.22}$$

where $a_n(Tf)$ denotes the nth Fourier coefficient of Tf. This pairing induces maps

$$\begin{aligned} L &\to \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}^{(N)}, \mathbb{C}) = \mathbb{T}_{\mathbb{C}}^{(N)^\vee}, \\ \mathbb{T}_{\mathbb{C}}^{(N)} &\to \mathrm{Hom}_{\mathbb{C}}(L, \mathbb{C}) = L^\vee. \end{aligned} \tag{2.23}$$

Proposition 2.4.4. *The above maps are isomorphisms.*

Proof. Since a finite-dimensional vector space and its dual have the same dimension, it suffices to show that each map is injective. To show these maps are injective, we require the following lemma, which uses Atkin–Lehner theory:

Lemma 2.4.5. *Any $f \in L$ with $a_n(f) = 0$ for all $(n, N) = 1$ is 0.*

Proof. Consider any $f \in L$ with $a_n(f) = 0$ for all $(n, N) = 1$. Since L is the $\mathbb{C}$-subspace of $S_2(\Gamma_0(N))$ spanned by all newforms of level dividing N, Atkin–Lehner theory implies that there is a maximal positive divisor M of N such that f can be written as

$$f = f^{\mathrm{new}} + f^{\mathrm{old}} \in S_2(M),$$

with $f^{\mathrm{new}} \in S_2(\Gamma_0(M))^{\mathrm{new}}$ and $f^{\mathrm{old}} \in S_2(\Gamma_0(M))^{\mathrm{old}}$. In particular, $f \in L$ is 0 if and only if $f^{\mathrm{new}} = 0$. Now, since $a_n(f) = 0$ for all $(n, N) = 1$ by assumption, we may apply Proposition 2.3.3, with $D = N/M \geq 1$, to see that $f \in S_2(\Gamma_0(M))^{\mathrm{old}}$. But this implies that $f^{\mathrm{new}} \in S_2(\Gamma_0(M))^{\mathrm{old}}$, i.e., $f^{\mathrm{new}} = 0$, and hence, $f = 0$. □

Given this lemma, we prove the injectivity of the maps in Eq. (2.23) as follows. First, suppose that $f \mapsto 0 \in \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}^{(N)}, \mathbb{C})$. Then $a_1(Tf) = 0$ for all $T \in \mathbb{T}_{\mathbb{C}}^{(N)}$, so $a_n = a_1(T_n f) = 0$ for all $(n, N) = 1$. By Lemma 2.4.5, $f = 0$.

Next, suppose $T \mapsto 0 \in \mathrm{Hom}_{\mathbb{C}}(L, \mathbb{C})$ so that $a_1(Tf) = 0$ for all $f \in L$. Substituting $T_n f$ for f and using the commutativity of $\mathbb{T}_{\mathcal{O}}$, we obtain

$$a_1(T(T_n f)) = a_1(T_n(Tf)) = a_n(Tf) = 0,$$

for all $(n, N) = 1$, and so, Lemma 2.4.5 implies that $Tf = 0$. Since this holds for all $f \in L$, we have $T = 0 \in \mathrm{End}_{\mathbb{C}}(S_2(\Gamma_0(N)))$. The last equality follows from the fact that any $g \in S_2(\Gamma_0(N))$ can be written as a linear combination of $\mathbb{T}_{\mathbb{C}}^{(N)}$-eigenforms, each of which shares its $\mathbb{T}_{\mathbb{C}}^{(N)}$-eigencharacter with some $f \in L$ [11, Theorems 1.20, 1.22]. Thus, if $T \mapsto 0 \in L^{\vee}$, then $Tg = 0$ for all $g \in S_2(\Gamma_0(N))$, as desired. $\square$

CHAPTER III

COMMUTATIVE ALGEBRA

Throughout this section, we use the following notation. Let p be a prime, and let $\mathcal{O}$ be the valuation ring of a finite extension E of $\mathbb{Q}_p$. Also, let ϖ be a uniformizer of $\mathcal{O}$, and write $\mathbb{F}_\varpi = \mathcal{O}/\varpi\mathcal{O}$ for the residue field.

Let $s \in \mathbb{Z}_+$, where $\mathbb{Z}_+$ is the set of positive integers, and let $\{n_1, n_2, \ldots, n_s\}$ be a set of s positive integers. Set $n = \sum_{i=1}^{s} n_i$. Let $A_i = \mathcal{O}^{n_i}$ with $i \in \{1, 2, \ldots, s\}$, and set $A = \prod_{i=1}^{s} A_i = \mathcal{O}^n$. Let $\varphi_i : A \twoheadrightarrow A_i$ be the canonical projection. Let $T \subset A$ be a local complete $\mathcal{O}$-subalgebra which is of full rank as an $\mathcal{O}$-submodule, and let $J \subset T$ be an ideal of finite index. Set $T_i = \varphi_i(T)$ and $J_i = \varphi_i(J)$. Note that each T_i is also a (local complete) $\mathcal{O}$-subalgebra and the projections $\varphi_i|_T$ are local homomorphisms so that J_i is also an ideal of finite index in T_i.

We first recall a result of Berger, Klosin, and Kramer [4, Theorem 2.1] which is key to proving Proposition 4.2.1. We then define the Hilbert–Samuel function of the module T as well as the associated multiplicity $e(J, T)$ of the ideal $J \subset T$. In particular, we prove that

$$e(J, T) = \sum_{i=1}^{s} \text{length}(T_i/J_i).$$

3.1. Result of Berger, Klosin, and Kramer

Using the Fitting ideal $\text{Fit}_{\mathcal{O}}(M)$ associated to a finitely presented $\mathcal{O}$-module M, cf. [32, Appendix], Berger, Klosin, and Kramer prove the following commutative algebra result [4, Theorem 2.1], which is widely applicable in the context of congruences between automorphic forms:

Theorem 3.1.1 (Berger–Klosin–Kramer, 2013)**.** *If* $\mathbb{F}_\varpi^\times \geq s-1$ *and each* J_i *is principal, then*

$$\#\prod_{i=1}^{s} T_i/J_i \geq \#T/J.$$

Moreover, the ideal J *is principal if and only if equality holds.*

As noted in [4, Remark 2.2], the following example shows that the inequality in Theorem 3.1.1 can be strict:

Example 3.1.2. Let $T = \{(a,b) \in \mathcal{O}\times\mathcal{O} \,|\, a \equiv b \pmod{\varpi}\} \subset \mathcal{O}\times\mathcal{O} = A$ with $A_i = \mathcal{O}$ for $i = 1,2$. Also, let $J = \{(\varpi a, \varpi b) \in \mathcal{O}\times\mathcal{O} \,|\, a,b \in \mathcal{O}\}$ be the maximal ideal of T. Then

$$T/J \cong T_1/J_1 \cong T_2/J_2 \cong \mathcal{O}/\varpi.$$

Moreover, if J is is only assumed to be an $\mathcal{O}$-submodule of T rather than ideal, then the statement of Theorem 3.1.1 is actually false:

Example 3.1.3. Again, let $T = \{(a,b) \in \mathcal{O}\times\mathcal{O} \,|\, a \equiv b \pmod{\varpi}\} \subset \mathcal{O}\times\mathcal{O} = A$ with $A_i = \mathcal{O}$ for $i = 1,2$. Now, let $J = \{(a,b) \in \mathcal{O}\times\mathcal{O} \,|\, a \equiv b \pmod{\varpi^2}\}$. Then

$$T/J \cong \mathcal{O}/\varpi \quad \text{while} \quad T_1/J_1 \cong T_2/J_2 \cong 0.$$

3.2. The Hilbert–Samuel function and multiplicities

Let R be a local ring with maximal ideal $\mathfrak{m}$. For a finitely generated R-module M and an ideal $\mathfrak{q} \subset R$ of finite colength on M, define the *Hilbert–Samuel function* of M with respect to $\mathfrak{q}$ to be (cf. [16, pg. 272])

$$H_{\mathfrak{q},M}(n) = \text{length}(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M).$$

By [16, Theorem 12.4], we have

$$\dim M = 1 + \deg P_{\mathfrak{q},M},$$

where $P_{\mathfrak{q},M}(n)$ is a polynomial that agrees with $H_{\mathfrak{q},M}(n)$ for large enough n.

Moreover, by [16, Exercise 12.6], we may write

$$P_{\mathfrak{q},M}(n) = \sum_{i=0}^{d} a_i F_i(n),$$

where $F_i(n) = \binom{n}{i}$ is the binomial coefficient regarded as a polynomial in n of degree i, and the a_i are integers with $a_d \neq 0$. Given these functions, we have the following definition:

Definition 3.2.1. The coefficient a_d is called the *multiplicity* of $\mathfrak{q}$ on M and is denoted $e(\mathfrak{q}, M)$.

Note that the leading coefficient of $P_{\mathfrak{q},M}$ equals $e(\mathfrak{q}, M)/d!$. In particular, when M is a finitely generated free R-module and $\dim R = 1$, we have $\dim M := \dim R/\mathrm{Ann}_R M = 1$, and hence, $P_{\mathfrak{q},M}$ will be a constant function for large enough n. Thus, in this case,

$$P_{\mathfrak{q},M} = e(\mathfrak{q}, M).$$

To relate the multiplicity $e(J, T)$ to $\sum_i \mathrm{length}(T_i/J_i)$, we use the following proposition:

Proposition 3.2.2. *If each J_i is principal, then we have*

$$e(J, T) = \sum_{i=1}^{s} e(J_i, T_i). \tag{3.1}$$

Remark 3.2.3. When $J = (\alpha)$ is principal, this equality follows immediately from [4, Proposition 2.3]. Indeed, since multiplication by α gives T-module isomorphisms

$$T/J \cong J/J^2 \cong J^2/J^3 \cong \cdots,$$

$H_{J,T}(n)$ is a constant fuction and $e(J,T) = \text{length}(T/J)$. Similarly, $e(J_i,T_i) = \text{length}(T_i/J_i)$. Additionally, we note that for any J,

$$\sum_{i=1}^{n} \text{length}\left(J_i^r/J_i^{r+1}\right) = \text{length}\left(\prod_{i=1}^{n} J_i^r/J_i^{r+1}\right) = \text{length}\left(\frac{\prod_{i=1}^{n} J_i^r}{\prod_{i=1}^{n} J_i^{r+1}}\right),$$

and hence,

$$\sum_{i=1}^{n} e(J_i,T_i) = e\left(\prod_{i=1}^{n} J_i, \prod_{i=1}^{n} T_i\right). \tag{3.2}$$

We now prove Proposition 3.2.2 using the following two lemmas:

Lemma 3.2.4 (Properties of Multiplicities, [5, Exercise 12.11.a.ii])**.** *Let*

$$0 \to M' \to M \to M'' \to 0$$

be an exact sequence of modules over the local ring $(R,\mathfrak{m})$*, and suppose that* $\mathfrak{q} \subset R$ *is an ideal of finite colength on* M*,* M'*,* M''*. If* $\dim M = \dim M' > \dim M''$*, then* $e(\mathfrak{q},M) = e(\mathfrak{q},M')$*.*

Lemma 3.2.5. *We have*

$$J\prod_{i=1}^{s} T_i \subseteq \prod_{i=1}^{s} J_i,$$

with equality whenever the J_i *are principal.*

Proof. The left-hand side consists of elements of the form

$$\sum_j \left(\varphi_1(\alpha_j)\varphi_1(t_1^j), \ldots, \varphi_s(\alpha_j)\varphi_s(t_s^j)\right)$$

with $\alpha_j \in J$ and $t_1^j, \ldots, t_s^j \in T$, and hence, the containment is clear. When the J_i are principal, [4, Proposition 2.6] guarantees the existence of some $\alpha \in J$ such that $\varphi_i(\alpha)$ generates J_i for all i. Thus, we may write an element of the right-hand side as

$$(\varphi_1(\alpha)\varphi_1(t_1), \ldots, \varphi_s(\alpha)\varphi_s(t_s)) = \alpha \cdot (\varphi_1(t_1), \ldots, \varphi_s(t_s))$$

for some $t_1, \ldots, t_s \in T$. □

Proof of Proposition 3.2.2. Consider the exact sequence

$$0 \to T \to \prod_{i=1}^{s} T_i \to K \to 0,$$

where K denotes the cokernel. Since T has full rank in A^n, Lemma 3.2.4 gives

$$e(J, T) = e\left(J, \prod_{i=1}^{s} T_i\right),$$

and hence, since the J_i are principal,

$$e\left(J, T\right) = e\left(J, \prod_{i=1}^{s} T_i\right) = e\left(J \prod_{i=1}^{s} T_i, \prod_{i=1}^{s} T_i\right) = e\left(\prod_{i=1}^{s} J_i, \prod_{i=1}^{s} T_i\right).$$

Thus, by Eq. (3.2),

$$e(J, T) = \sum_{i=1}^{s} e(J_i, T_i).$$

□

Corollary 3.2.6. *If each J_i is principal, then*

$$e(J,T) = \sum_{i=1}^{s} \text{length}(T_i/J_i).$$

Proof. As established in Remark 3.2.3, if each J_i is principal, $e(J_i, T_i) = \text{length}(T_i/J_i)$. Hence,

$$e(J,T) = \sum_{i=1}^{s} e(J_i, T_i) = \sum_{i=1}^{s} \text{length}(T_i/J_i).$$

□

CHAPTER IV

HIGHER EISENSTEIN CONGRUENCES FOR SQUAREFREE LEVEL

We now examine higher congruences between weight 2 newforms and Eisenstein of squarefree level. Let $f_1, \ldots, f_r$ be all weight 2 normalized cuspidal simultaneous eigenforms of level $\Gamma_0(N)$ with N prime. A celebrated result of Mazur [30, Proposition II.5.12, Proposition II.9.6] states that if a prime p divides the numerator $\mathcal{N}$ of $\frac{N-1}{12}$, then at least one of these forms is congruent modulo p to the weight 2 normalized Eisenstein series

$$E_{2,N} = \frac{N-1}{24} + \sum_{n=1}^{\infty} \sigma^*(n) q^n, \tag{4.1}$$

where $\sigma^*(n)$ is the sum of all non-zero divisors d of n such that $(d, N) = 1$. Berger, Klosin, and Kramer [4, Proposition 3.1] refine this result to give a precise relation between $\mathrm{val}_p(\mathcal{N})$ and the depth of congruence between the newforms $f_1, \ldots, f_r$ and $E_{2,N}$. Using a commutative algebra result (restated as Theorem 3.1.1 of this paper), they show that if ϖ_N is a uniformizer in the valuation ring of a finite extension of $\mathbb{Q}_p$ (of ramification index e_N) that contains all Hecke eigenvalues of the f_i's and m_i is the largest integer such that the Hecke eigenvalues of f_i and $E_{2,N}$ satisfy

$$\lambda_\ell(f_i) \equiv \lambda_\ell(E_{2,N}) \pmod{\varpi_N^{m_i}},$$

for all Hecke operators T_ℓ with $\ell \nmid N$ prime, then

$$\frac{1}{e_N} \sum_{i=1}^{r} m_i \geq \mathrm{val}_p(\mathcal{N}). \tag{4.2}$$

Moreover, Theorem 3.1.1 implies that this expression is an equality if and only if the Eisenstein ideal is locally principal. Since the Eisenstein ideal is locally principal

when N is prime [30, Theorem II.18.10], Eq. (4.2) is always an equality in this case. However, the approach of comparing the depth of Eisenstein congruences modulo p, i.e., the left side of Eq. (4.2), to a certain p-adic value suggests a way to determine if the Eisenstein ideal is locally principal for a fixed squarefree level N.

Let $N = \prod_{j=1}^{t} q_j > 6$ be a squarefree positive integer. The weight 2 Eisenstein subspace of level $\Gamma_0(N)$, denoted $E_2(\Gamma_0(N))$, is spanned by $2^t - 1$ Eisenstein series, each of which is a simultaneous eigenform for all Hecke operators. Since a basis of such eigenforms can be obtained using level raising techniques [48, §2.2], each eigenform in $E_2(\Gamma_0(N))$ has Hecke eigenvalues $\lambda_\ell = 1 + \ell$ for Hecke operators T_ℓ with $\ell \nmid N$ prime. Moreover, since we are only interested in congruences away from N, i.e., congruences between the ℓ^{th} Hecke eigenvalues for primes $\ell \nmid N$, any normalized Eisenstein series $E \in E_2(\Gamma_0(N))$ works for our generalization to squarefree level. We therefore consider congruences between all weight 2 newforms $f_1, \ldots, f_r$ of level N_{f_i} dividing N and the weight 2 Eisenstein series of level N,

$$E_{2,N}(z) = \sum_{d|N} \mu(d) d E_2(dz), \tag{4.3}$$

where $\mu : \mathbb{Z}_+ \to \{-1, 0, 1\}$ is the Möbius function defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n \text{ is squarefree with an even number of prime factors,} \\ -1 & \text{if } n \text{ is squarefree with an odd number of prime factors,} \\ 0 & \text{if } n \text{ has a squared prime factor,} \end{cases}$$

and $E_2(z)$ is the weight 2 Eisenstein series for $\mathrm{SL}(2,\mathbb{Z})$, normalized so that the Fourier coefficient of q is 1. Note that the Eisenstein series in Eq. (4.3) has q-expansion

$$E_{2,N} = (-1)^{t+1}\frac{\varphi(N)}{24} + \sum_{n=1}^{\infty}\sigma^*(n)q^n$$

and coincides with Eq. (4.1) for prime N.

Since the Hecke eigenvalues of $E_{2,N}$ and E_{2,q_j} agree for Hecke operators away from N, Mazur's original congruence result implies that if $p \geq 5$ is a prime dividing $\varphi(N)$, then at least one of the newforms (of prime level) is congruent to $E_{2,N}$ away from N. The first main result of this paper (Proposition 4.2.1) extends the higher congruences framework of Berger, Klosin, and Kramer to squarefree level $N > 6$ so that with a slight modification, the inequality in Eq. (4.2) still holds. The second main result then sharpens this inequality under certain conditions, proving the following statement about the local principality of the Eisenstein ideal:

Theorem 4.0.1. *If N has at least three prime divisors, then for any $p \geq 5$ dividing $\varphi(N)$, the depth of Eisenstein congruences modulo p is strictly greater than the p-adic valuation of $\varphi(N)$, i.e.,*

$$\frac{1}{e_N}(m_1 + \cdots + m_r) > \mathrm{val}_p(\varphi(N)). \tag{4.4}$$

If, in addition, $\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) = \mathrm{val}_p(\varphi(N))$, the Eisenstein ideal $J_{\mathbb{Z}} \subseteq \mathbb{T}_{\mathbb{Z}}$ is not locally principal.

The key feature of this result is the strictness of the inequality in Eq. (4.4), which is controlled by the existence of a newform of composite level that is congruent to $E_{2,N}$ away from N. When $p \nmid N$, Ribet and Yoo [50, Theorems 2.2, 2.3] give necessary and sufficient conditions for the existence of such a newform and also address more general

Eisenstein congruences. Using the Jacquet–Langlands correspondence, Martin [29, Theorem A] independently obtains Ribet's sufficient condition, even in the case $p \mid N$.

In the next chapter, as an application of these results, we express the depth of congruence $\frac{1}{e_N} \sum_{i=1}^{r} m_i$ (from Proposition 4.2.1) as the Hilbert–Samuel multiplicity of the Eisenstein ideal in the Hecke algebra. While the depth of Eisenstein congruences modulo p detects whether the associated (localized) Eisenstein ideal is principal, this connection to multiplicities might allow us to give a more precise statement regarding the minimal number of generators.

Additionally, using an algorithm adapted from Naskręcki [35, §4.2], we provide computational examples to illustrate our main results. While Naskręcki has computed a large number of Eisenstein congruences, his work concerns congruences of q-expansions rather than congruences away from N. As a result, his data does not necessarily agree with ours. For example, if $N = 97$ and $p = 2$, then $\mathrm{val}_2(\frac{96}{12}) = 3$. Since the constant term of $E_{2,N}$ has a 2-adic valuation of 2, Naskręcki's algorithm returns 2 as the depth of congruence. On the other hand, our algorithm returns 3, which agrees with the equality in Eq. (4.2). Moreover, Naskręcki's algorithm determines the exact Eisenstein series in $E_2(\Gamma_0(N))$ for which a congruence holds; we do not require this information since the Hecke eigenvalues of all Eisenstein series in $E_2(\Gamma_0(N))$ coincide away from N. Because of these differences, we use our modified algorithm for congruence computations.

Lastly, we note that work of Wake and Wang-Erickson [46] studies similar questions about the rank of the Eisenstein ideal. In particular, their methods are based on pseudodeformation theory.

4.1. Congruence modules associated to weight 2 Eisenstein series

Recall that in Example 2.1.4, given $c_d \in \mathbb{C}$ for $d \mid N$ such that $\sum_{d|N} c_d/d = 0$, we defined a weight 2 Eisenstein series of level N and trivial character by

$$E_{2,N,c_d}(z) = \sum_{d|N} c_d E_2(dz), \tag{4.5}$$

where

$$E_2(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n. \tag{4.6}$$

When $N = p$ is prime, Eq. (4.5), with $c_1 = 1$ and $c_p = p$, agrees (up to normalization) with Eq. (4.1). In fact, this is the only Eisenstein series of weight 2, level p, and trivial character (again, up to normalization). When N has more than one prime factor, there are several weight 2 Eisenstein series of level N and trivial character, including the Eisenstein series given in Eq. (4.3). To study congruences between newforms and Eisenstein series of squarefree level, we would like a natural basis of all such Eisenstein series, which we obtain using level raising techniques and the Fourier series in Eq. (4.6).

For a fixed squarefree level N, the space $M_2(\Gamma_0(N))$ of weight 2 modular forms for the congruence subgroup $\Gamma_0(N)$ decomposes into its subspace of cusp forms $S_2(\Gamma_0(N))$ and the *Eisenstein space* $E_2(\Gamma(N))$, which is isomorphic to the quotient space $M_2(\Gamma_0(N))/S_2(\Gamma_0(N))$ [15, §4.2]. By applying dimension formulas from [15, Ch. 3], specifically [15, Eq. (4.3)], we see that the dimension of $E_2(\Gamma_0(N))$ is equal to the number of cusps of the (compact) modular curve $X_0(N)$, i.e., $2^t - 1$, where t is the number of prime divisors of N.

Using the Fourier series $E_2(z)$ in Eq. (4.6), we can construct weight 2 Eisenstein series of level N with the following level raising operators:

Definition 4.1.1. Given a modular form $g \in M_2(\Gamma_0(N))$ and prime $p \nmid N$, we define

$$\begin{aligned} [p]^+(g)(z) &= g(z) - pg(pz), \\ [p]^-(g)(z) &= g(z) - g(pz), \end{aligned} \tag{4.7}$$

both of which are weight 2 modular forms of level Np.

Since $E_2(z)$ is not a genuine modular form, the above definition might not make sense when applied to $E_2(z)$. However, as established in Example 2.1.4, $[p]^+(E_2)(z)$ is a genuine modular form, and so, we may define weight 2 Eisenstein series of level N as follows:

Definition 4.1.2. For $1 \leq s \leq t$, let $N = \prod_{i=1}^{t} p_i$ and $M = \prod_{j=1}^{s} p_j$. We define

$$E_{M,N}(z) = [p_t]^- \circ \cdots \circ [p_{s+1}]^- \circ [p_s]^+ \circ \cdots \circ [p_1]^+(E_2)(z). \tag{4.8}$$

Yoo [48, Proposition 2.6] proves that each $E_{M,N}$ is a weight 2 Eisenstein series of level N as well as an eigenform for all Hecke operators. Moreover, since there are exactly $2^t - 1$ distinct choices for $M > 1$, we have found a natural basis for $E_2(\Gamma_0(N))$, namely the Eisenstein series $E_{M,N}$ with $M > 1$.

Now, to detect the existence of Eisenstein congruences, we use a congruence module $\mathbb{T}/J$ where $\mathbb{T}$ is a Hecke algbra and J is an Eisenstein ideal [37, 4, 17]. Our particular approach to studying such congruences is rooted in a commutative algebra result (Theorem 3.1.1) which requires that a certain space of cusp forms is simultaneously diagonalizable under a Hecke action. We therefore work with the anemic Hecke algebra $\mathbb{T}^{(N)}$, which excludes operators U_p for $p \,|\, N$. Since we are only concerned with computing Eisenstein congruences away from N and the Fourier coefficients of the Eisenstein series constructed above coincide away from N, we may actually consider any $E_{M,N}$. (Our choice in Eq. (4.3) is made to coincide with

Eq. (4.1) for prime N.) Before proving the main results of this dissertation, we briefly discuss some related work of Ribet–Yoo [48] and Ohta [37, 38] which concerns congruence modules associated to specific Eisenstein series $E_{M,N}$.

To distinguish between Eisenstein congruences for different Eisenstein series $E_{M,N}$, we consider the Fourier coefficients at primes dividing N, and so, we need to enlarge the Hecke algebra to detect these coefficients. Indeed, the main two ways to augment the anemic Hecke algebra, described in Sections 4.1.1 and 4.1.2, respectively, are to include the Hecke operators U_p, for primes $p \,|\, N$, or include the Atkin–Lehner operators [1] w_d, for $d \,|\, N$. In either case, before we can study the appropriate congruence module, we must restrict the Hecke action on $S_2(\Gamma_0(N))$ to a Hecke-invariant subspace.

4.1.1. Full congruence module. In [48], Ribet and Yoo examine Eisenstein ideals in the full Hecke algebra $\mathbb{T}_N$, which is generated by Hecke operators T_n for all $n \geq 0$. In particular, they generalize the work of Mazur [30], and so much of their paper focuses on modular curves and their associated Jacobians when N is squarefree. Specifically, for each $M > 1$ that divides a fixed squarefree level N, Ribet and Yoo define the ideal

$$I_M = (U_p - 1, U_q - q, T_r - r - 1 : \text{ for primes } p \,|\, M, q \,|\, N/M, \text{ and } r \nmid N).$$

By previous work of Yoo [49], any Eisenstein maximal ideal of $\mathbb{T}_N$ contains some I_M, and so to compute the index of certain Eisenstein ideals inside of the full Hecke algebra, Yoo proves the following theorem [48, Theorem 1.1]:

Theorem 4.1.3 (Yoo)**.** *For any prime $y \nmid 2N$, we have*

$$\mathbb{T}_N/I_M \otimes \mathbb{Z}_y \cong \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}_y,$$

where m is the numerator of $\frac{1}{24} \cdot \varphi(N) \cdot \prod_{\ell | N/M} (\ell + 1)$.

Note that in [48, Theorem 3.3], Ribet and Yoo also give an analogous statement for the index of a "new" Eisenstein ideal of $\mathbb{T}_N$. Currently, it does not appear that these results can be used directly to understand the anemic congruence module $\mathbb{T}^{(N)}/J$ which is considered in Sections 4.2 and 4.3. However, they may be useful for counting Eisenstein congruences in specific new subspaces.

4.1.2. Atkin–Lehner congruence module. A second way to augment the anemic Hecke algebra is to include the Atkin–Lehner operators w_d for all positive divisors d of N. (For details on these involutions, see [1] or [14, §4].) Indeed, in [37, 38], Ohta studies such congruence modules, determining the index of the Eisenstein ideal in various Hecke algebras within this setting. While we include the details of Ohta's results at the end of Section 4.3, we note that his method requires a different congruence module for each Eisenstein series $E_{M,N}$.

Remark 4.1.4. When the level $N = p$ is prime, the U_p operator acts as the identity [8] and the w_p operator acts as either ± 1, and hence, the full, Atkin–Lehner, and anemic Hecke algebras coincide. However, when N is not prime, the involution w_N does not commute with the Hecke operators T_n for $(n, N) \neq 1$, and so, it is important to distinguish between the full, Atkin–Lehner, and anemic congruence modules. For example, while the decomposition of $S_2(\Gamma_0(N))$ into simultaneous eigenspaces under the action of the anemic Hecke algebra is compatible with its decomposition into w_N-eigenspaces, it is in general not equivariant under the action of the full Hecke algebra. See [14, §4, §6.3] for more details on the relationship between w_N and U_p.

4.2. Higher congruences framework

For each prime $p \geq 5$, we would like to bound the depth of Eisenstein congruences modulo p by the p-adic valuation of the index of an Eisenstein ideal in the associated Hecke algebra. In particular, since we are only interested in congruences away from N, we exclude Hecke operators T_r for primes $r \mid N$. When the level N is prime, this exclusion makes no difference since T_N acts as the identity in the associated Hecke algebra [8, Proposition 3.19]. However, for composite level N, we must make a distinction between the anemic Hecke algebra $\mathbb{T}$, which does not include T_r for primes $r \mid N$, and the full Hecke algebra $\mathbb{T}(N)$.

Indeed, let $S_2(\Gamma_0(N))$ denote the $\mathbb{C}$-space of modular forms of weight 2 and level $\Gamma_0(N)$. For any subring $R \subset \mathbb{C}$, write $\mathbb{T}_R$ for the R-subalgebra of $\mathrm{End}_{\mathbb{C}}(S_2(\Gamma_0(N))$ generated by the Hecke operators T_ℓ for primes $\ell \nmid N$. Let J_R be the Eisenstein ideal, i.e., the ideal of $\mathbb{T}_R$ generated by $T_\ell - (1+\ell)$ for primes $\ell \nmid N$. For a prime ideal $\mathfrak{n}$ of $\mathbb{T}_R$, write $\mathbb{T}_{R,\mathfrak{n}}$ for the localization of $\mathbb{T}_R$ at $\mathfrak{n}$, and set $J_{R,\mathfrak{n}} := J_R\mathbb{T}_{R,\mathfrak{n}}$.

We now apply Theorem 3.1.1 to Eisenstein congruences of elliptic modular forms of squarefree level. Fix an embedding $\overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ and let E be a finite extension of $\mathbb{Q}_p$ that contains all Hecke eigenvalues of the f_i's and whose residue field has order at least s. Write $\mathcal{O}_N$ for the ring of integers in E, ϖ_N for a choice of uniformizer, e_N for the ramification index of $\mathcal{O}_N$ over $\mathbb{Z}_p$, and d_N for the degree of its residue field over $\mathbb{F}_p$. The following result relates the depth of Eisenstein congruences modulo p to the p-adic valuation of $\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}$ and shows that this depth detects whether the localized Eisenstein ideal $J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}$ is principal:

Proposition 4.2.1. *For $i = 1, \ldots, r$, let $\varpi_N^{m_i}$ be the highest power of ϖ_N such that the Hecke eigenvalues of f_i are congruent to those of $E_{2,N}$ modulo $\varpi_N^{m_i}$ for Hecke*

operators T_ℓ for all primes $\ell \nmid N$. Then, we have

$$\frac{1}{e_N}(m_1 + \cdots + m_r) \geq \mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}). \tag{4.9}$$

This inequality is an equality if and only if the Eisenstein ideal $J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}$ is principal.

Proof. To simplify notation, write $\mathcal{O}$ for $\mathcal{O}_N$ and ϖ for ϖ_N, and let $\mathfrak{m} = J_{\mathcal{O}} + \varpi\mathbb{T}_{\mathcal{O}}$ be the unique maximal ideal of $\mathbb{T}_{\mathcal{O}}$ containing $J_{\mathcal{O}}$. By Atkin–Lehner theory, each newform $f_1, \ldots, f_r$ (of level N_{f_i}) is a simultaneous eigenform under the action of the anemic Hecke algebra $\mathbb{T}_{\mathcal{O}}$, and so we can consider the map

$$\mathbb{T}_{\mathcal{O}} \to \prod_{i=1}^{s} \mathcal{O}, \;\; T_\ell \mapsto \prod_{i=1}^{s} (\lambda_\ell(f_i)). \tag{4.10}$$

In particular, the perfect pairing established by Proposition 2.4.4 implies that this map is an injection. Indeed, if $T \in \mathbb{T}_{\mathcal{O}}$ maps to 0, then by viewing T as a $\mathbb{C}$-linear form on L via an extension of scalars, we see that $T \mapsto 0 \in L^\vee$ in Eq. (2.23), i.e., $T = 0$.

Now, renumber $f_1, \ldots, f_r$ so that $f_1, \ldots, f_s$ satisfy an Eisenstein congruence away from N while $f_{s+1}, \ldots, f_r$ do not. Eq. (4.10) then induces an injection

$$\mathbb{T}_{\mathcal{O},\mathfrak{m}} \hookrightarrow \prod_{i=1}^{s} \mathcal{O}, \;\; T_\ell \mapsto \prod_{i=1}^{s} (\lambda_\ell(f_i)).$$

Since $\mathbb{T}_{\mathcal{O},\mathfrak{m}} \subset \prod_{i=1}^{s} \mathcal{O}$ is a local complete $\mathcal{O}$-subalgebra of full rank, we apply Theorem 3.1.1 with $T = \mathbb{T}_{\mathcal{O},\mathfrak{m}}$, $J = J_{\mathcal{O},\mathfrak{m}}$, $T_i = \mathcal{O}$, and $\varphi_i : T \to T_i$ as the canonical projection. (Note that by construction, E satisfies the hypothesis in Theorem 3.1.1 on the order of its residue field.) For each projection T_i/J_i, we have

$$\mathrm{val}_p(\#T_i/J_i) = (\#\,\mathcal{O}/\varpi^{m_i}\mathcal{O}) = m_i d_N = m_i \frac{[\mathcal{O} : \mathbb{Z}_p]}{e_N}. \tag{4.11}$$

On the other hand, if $\mathfrak{m}_{\mathbb{Z}_p} = \mathfrak{m} \cap \mathbb{T}_{\mathbb{Z}_p}$, then since $\mathbb{T}_{\mathcal{O},\mathfrak{m}} = \mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}} \otimes_{\mathbb{Z}_p} \mathcal{O}$ [11, Lemma 3.27 and Proposition 4.7] and $J_{\mathcal{O},\mathfrak{m}} = J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}} \otimes_{\mathbb{Z}_p} \mathcal{O}$, we have

$$\mathrm{val}_p(\#T/J) = \mathrm{val}_p\left(\#\frac{\mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}}{J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}} \otimes_{\mathbb{Z}_p} \mathcal{O}\right) = [\mathcal{O} : \mathbb{Z}_p]\mathrm{val}_p\left(\#\frac{\mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}}{J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}}\right).$$

Combining these equalities yields

$$\frac{1}{e_N}(m_1 + \cdots + m_r) \geq \mathrm{val}_p\left(\#\frac{\mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}}{J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}}\right),$$

and hence, the result follows from the fact that $\mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}/J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}} \cong \mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}$. □

4.3. Local principality of the Eisenstein ideal

To use Proposition 4.2.1 to generate examples of squarefree levels for which the Eisenstein ideal is not locally principal, we need to (i) determine the p-adic valuation of $\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}$, ideally in terms of a related L-value, and (ii) show that the depth of Eisenstein congruence modulo p is strictly greater than this p-adic valuation. While this paper discusses some progress towards (i) at the end of this section, its main results focus on (ii).

Indeed, Theorem 4.0.1, which we now prove, establishes that if N has at least three prime divisors, then for any prime $p \geq 5$ dividing $\varphi(N)$, the depth of Eisenstein congruences modulo p is strictly greater than the p-adic valuation of $\varphi(N)$, i.e.,

$$\frac{1}{e_N}(m_1 + \cdots + m_r) > \mathrm{val}_p(\varphi(N)). \tag{4.12}$$

Furthermore, it states that if, in addition, $\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) = \mathrm{val}_p(\varphi(N))$, the Eisenstein ideal $J_{\mathbb{Z}} \subseteq \mathbb{T}_{\mathbb{Z}}$ is not locally principal.

Proof of Theorem 4.0.1. If necessary, renumber the newforms $f_1, \ldots, f_s$ so that $f_1, \ldots, f_{s_p}$ are of prime level while $f_{s_p+1}, \ldots, f_s$ are of composite level. Since the level $N = \prod_{j=1}^{t} q_j$ is squarefree, we have

$$\mathrm{val}_p\left(\varphi(N)\right) = \sum_{j=1}^{t} \mathrm{val}_p(q_j - 1).$$

In particular, since $p \geq 5$ by assumption, the result of Berger, Klosin, and Kramer for prime level [4, Proposition 3.1] gives that the depth of congruence between newforms of level $N_{f_i} = q_j$ and the Eisenstein series E_{2,q_j} equals $\mathrm{val}_p(q_j - 1)$ for each $1 \leq j \leq t$. So, if we consider only newforms of prime level q_j dividing N, we obtain the equality

$$\frac{1}{e_N}(m_1 + \cdots + m_{s_p}) = \mathrm{val}_p(\varphi(N)).$$

Thus, the inequality in Eq. (4.12) is strict if and only if $s_p < s$, i.e., there exists a newform of composite level which satisfies an Eisenstein congruence away from N. By [50, Theorem 2.2] (for $p \nmid N$) or [29, Theorem A] (for any p), such a newform exists whenever N has at least three prime factors, and hence, Eq. (4.12) follows. The second statement in Theorem 4.0.1 now follows immediately by combining Eq. (4.12) with Proposition 4.2.1. Specifically, if $\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) = \mathrm{val}_p(\varphi(N))$, then the localized Eisenstein ideal $J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}$ is non-principal. □

Replacing [50, Theorem 2.2] in the proof above with [50, Theorem 2.3] yields the following corollary, which addresses the case where N has exactly two prime divisors:

Corollary 4.3.1. *If $N = qr$ and $p \geq 5$ satisfies $(p, N) = 1$ and $q \equiv 1 \pmod{p}$, then the depth of Eisenstein congruences modulo p is strictly greater than the p-adic valuation of $\varphi(N)$ if and only if $r \equiv \pm 1 \pmod{p}$ or r is a p-th power modulo q. If,*

in addition, $\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) = \mathrm{val}_p(\varphi(N))$*, the Eisenstein ideal* $J_{\mathbb{Z}} \subseteq \mathbb{T}_{\mathbb{Z}}$ *is not locally principal.*

Now, Theorem 4.0.1 and Corollary 4.3.1 reduce the task of finding examples where $J_{\mathbb{Z}}$ is not locally principal to determining conditions under which $\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) = \mathrm{val}_p(\varphi(N))$. While we are currently unable to specify such conditions (due to certain difficulties arising from the anemic Hecke algebra described in more detail below), we do use the work of Ohta [38] to give a lower bound for $\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p})$. In particular, this bound suggests some cases for which the desired equality holds.

For the remainder of this section, we assume that $p \nmid N$ so that $\mathbb{Z}_p$ is a $\mathbb{Z}[1/N]$-algebra. Following [38, §2-3], we consider the action on $S_2(\Gamma_0(N))$ of the Atkin–Lehner involutions w_d for all positive divisors d of N. More specifically, for $N = \prod_{j=1}^{t} q_j$, set $\boldsymbol{E} = \{\pm 1\}^t$. Then for each $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_t) \in \boldsymbol{E}$, we define $S_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}}$ to be the maximum direct summand of $S_2(\Gamma_0(N))$ on which w_{q_j} acts as multiplication by ε_j $(1 \leq j \leq t)$. Since the Atkin–Lehner operators w_d commute with the Hecke operators T_ℓ for $\ell \nmid N$, the subspace $S_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}}$ is invariant under the action of $\mathbb{T}_{\mathbb{Z}_p}$. So, let $\mathbb{T}^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_p}$ (resp. $J^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_p}$) denote the restriction of $\mathbb{T}_{\mathbb{Z}_p}$ (resp. $J_{\mathbb{Z}_p}$) to $S_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}}$.

We would like to use a result of Ohta which computes the p-adic valuation of the index of the Eisenstein ideal inside of a certain Hecke algebra. Since Ohta's notation differs significantly from ours, we briefly explain his notation and how it relates to our conventions. Indeed, in his work on Eisenstein ideals and rational torsion subgroups, Ohta studies three different spaces of modular forms which he denotes $M_k^{\mathrm{A}}(\Gamma_0(N); R)$, $M_k^{\mathrm{B}}(\Gamma_0(N); R)$, and $M_k^{\mathrm{reg}}(\Gamma_0(N); R)$. The first (resp. the second) space consists of modular forms in the sense of Deligne–Rapoport and Katz (resp. Serre and Swinnerton–Dyer), and the third space consists of regular differentials on

the modular curve. Note that the spaces $M_k^{\mathrm{A}}(\Gamma_0(N);R)$, $M_k^{\mathrm{B}}(\Gamma_0(N);R)$ coincide respectively with the spaces $\mathcal{M}_k(\Gamma_0(N);R)$, $\mathbf{M}_k(\Gamma_0(N);R)$ defined in Appendix B.

Now, since $\mathbb{Z}_p$ is flat over $\mathbb{Z}[1/N]$, these three spaces of modular forms coincide [38, Eq. (1.3.4) and Cor 1.4.10], and so, although Ohta defines his Hecke algebra $\mathbf{T}(N;R)$ as a subring of $\mathrm{End}_R(S_2^{\mathrm{reg}}(\Gamma_0(N);R)$, we can view it as subring of $\mathrm{End}_R(S_2(\Gamma_0(N)))$. Moreover, while the Hecke algebra $\mathbf{T}(N;\mathbb{Z}_p)$ does not coincide with the anemic Hecke algebra $\mathbb{T}_{\mathbb{Z}_p}$ in general (as is discussed in Section 4.1), its restriction to $S_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}}$ does coincide with $\mathbb{T}^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_p}$. Hence, when $\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+$, where $\varepsilon_+ = (1,1,1,\ldots,1)$, we may apply [38, Theorem 3.1.3] to obtain the equality

$$\mathrm{val}_p(\#\mathbb{T}^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_p}/J^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_p}) = \mathrm{val}_p\Big(\prod_{j=1}^{t}(q_j+\varepsilon_j)\Big). \tag{4.13}$$

In particular, since $p \geq 5$ is odd, $\mathrm{val}_p(q_j+\varepsilon_j)$ is positive for at most one $\varepsilon_j \in \{\pm 1\}$. So, assuming that $q_j \not\equiv -1 \pmod{p}$ for some j, there is some $\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+ \in \mathbf{E}$ such that

$$\mathrm{val}_p(\#\mathbb{T}^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_p}/J^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_p}) = \mathrm{val}_p\Big(\prod_{j=1}^{t}(q_j+\varepsilon_j)\Big) = \mathrm{val}_p\Big(\prod_{j=1}^{t}(q_j^2-1)\Big). \tag{4.14}$$

Hence, since $\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p} \twoheadrightarrow \mathbb{T}^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_p}/J^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_p}$ for each $\boldsymbol{\varepsilon} \in \boldsymbol{E}$, we conclude

$$\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) \geq \mathrm{val}_p\Big(\prod_{j=1}^{t}(q_j^2-1)\Big). \tag{4.15}$$

There are two particularly encouraging features of this lower bound. First, the value on the right-hand side of Eq. (4.15) is divisible by all primes for which there exists an Eisenstein congruence modulo p. (See [50] for more details.) If this were not the case, then while this value might be a valid lower bound for the p-adic valuation of $\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}$, it could not possibly be a valid upper bound since the index of the

congruence module $\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}$ must be divisible by any prime for which there is an Eisenstein congruences modulo p. Second, if we assume that $q_j \not\equiv -1 \pmod{p}$ for $j = 1, \ldots, t$, then Eq. (4.15) simplifies to

$$\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) \geq \mathrm{val}_p(\varphi(N)),$$

which gives half of the equality required by Theorem 4.0.1 to prove local principality results about the Eisenstein ideal. Hence, this lower bound suggests that $J_{\mathbb{Z}}$ is not locally principal whenever N has at least three prime divisors, none of which are congruent to -1 modulo p, and there exists a prime $p \geq 5$ dividing $\varphi(N)$.

We end this section by briefly discussing the main obstacle that arises when computing the index $\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}$ of the Eisenstein ideal inside of the anemic Hecke algebra. Indeed, many of the current methods for determining a relationship between the full and anemic Hecke algebras use deformation theory and an $R = \mathbb{T}$ argument [11, 31, 6]. For example, in [45], Skinner and Wiles examine the relationship between ordinary universal deformation rings and Hecke rings within the context of weight 2 modular forms. In particular, these methods require that the primes for which operators are excluded from the Hecke algebra satisfy certain conditions, e.g., [45, §2]. Because we are considering Eisenstein congruences between weight 2 modular forms with trivial Nebentypus, the prime divisors of N do not satisfy the required conditions, and thus, to establish an equality in Eq. (4.15), we need a different approach.

Remark 4.3.2. When $q_j \equiv -1 \pmod{p}$ for some $j = 1, \ldots, t$, Proposition 4.2.1 combined with Eq. (4.15) yields the inequality

$$\frac{1}{e_N}(m_1 + \cdots + m_r) \geq \mathrm{val}_p\Big(\prod_{j=1}^{t}(q_j^2 - 1)\Big),$$

where the value on the right side is greater than $\mathrm{val}_p(\varphi(N))$. While this (greater) lower bound is useful for computing the depth of Eisenstein congruences modulo p, we currently cannot obtain a result analogous to Theorem 4.0.1 about the local principality of the Eisenstein ideal since the inequality is not necessarily strict. However, in future work, we may be able to show that it is strict by combining the higher congruences framework with methods of Martin [29] related to the Jacquet–Langlands correspondence.

Remark 4.3.3. Since we have assumed $p \geq 5$ throughout this section, we now briefly address the cases $p = 2, 3$. Indeed, with $N = \prod_{j=1}^{t} q_j$, two problems arise when $p = 2, 3$. First, in the prime level case, the depth of Eisenstein congruences modulo p is equal to the p-adic valuation of the numerator of $\frac{N-1}{12}$. When $p \geq 5$, we may ignore the denominator of this value (as we did in the proof of Theorem 4.0.1). However, since this is not the case for $p = 2, 3$, we no longer have a guarantee, a priori, that a newform of prime level satisfies an Eisenstein congruence away from N. So, while Proposition 4.2.1 still holds, we cannot obtain the strict inequality as in Theorem 4.0.1. Second, Eq. (4.13) does not hold for $p = 2, 3$, and so, we do not expect the equality $\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) = \mathrm{val}_p(\varphi(N))$. Despite these issues, we include $p = 3$ in the computational approach in Section V since the depth of Eisenstein congruences modulo p is of independent interest. We completely exclude $p = 2$ since these congruences behave much differently but note that Martin addresses mod 2 Eisenstein congruences in [28].

4.4. General Eisenstein congruences

We may apply the higher congruences framework to many other settings, e.g., congruence primes for primitive forms or congruences to Saito–Kurokawa lifts [4, §5].

Below we discuss one such setting with general (higher) Eisenstein congruences for $S_k(Np, \chi)$, where $k \geq 2$, $(N, p) = 1$, and χ has conductor N or Np.

4.4.1. Eisenstein ideals associated to cusp forms of higher weights. Let p be an odd prime and χ a Dirichlet character of order prime to p. Let the conductor of χ be Np^r with $(N, p) = 1$ (so that $r = 0$ or 1 since the order of χ is prime to p). For each integer $k \geq 2$ such that $\chi(-1) = (-1)^k$, let $S_k(Np, \chi)$ be the space of cusp forms of weight k, level Np, and character χ. Let $\mathcal{S}_0$ be the complex vector space of modular forms $S_k(Np, \chi) \oplus \mathbb{C}E_\chi$, where $E_\chi \in M_k(Np, \chi)$ is the Eisenstein series with Hecke eigenvalues $1 + \chi(\ell)\ell^{k-1}$ for $\ell \nmid Np$.

As before, let $\mathcal{O}$ be the ring of integers in a sufficiently large extension E of $\mathbb{Q}_p$. Let ϖ be a choice of uniformizer in $\mathcal{O}$, e be the ramification index of $\mathcal{O}$ over $\mathbb{Z}_p$, and d be the residue degree $[\mathcal{O}/\varpi\mathcal{O} : \mathbb{F}_p]$. Also, let $\mathbb{T}_0$ be the $\mathcal{O}$-subalgebra of endomorphisms of $\mathcal{S}_0$ generated be the Hecke operators T_ℓ for $\ell \nmid Np$. Write Π_0 for the set of systems of eigenvalues of $\mathbb{T}_0$ and λ_0 for the Hecke eigencharacter corresponding to E_χ, and set $\Pi = \Pi_0 \setminus \{\lambda_0\}$. Then the Eisenstein ideal J is generated by $T_\ell - \ell - \chi(\ell)\ell^{k-1}$ for $\ell \nmid Np$ in the cuspidal Hecke algebra $\mathbb{T}$.

We can ask similar questions about the local principality of the Eisenstein ideal J associated to the spaces $S_k(Np, \chi)$ of cusp forms. Indeed, in [4, Example 5.1], Berger, Klosin, and Kramer prove the following result regarding the depth of congruence in this setting:

Theorem 4.4.1 (Berger–Klosin–Kramer)**.** *For every $\lambda \in \Pi$, let m_λ be the largest integer such that $\lambda_0(T) \equiv \lambda(T) \mod \varpi^{m_\lambda}$ for all $T \in \mathbb{T}_0$. Then*

$$\frac{1}{e} \sum_{\lambda \in \Pi} m_\lambda \geq \mathrm{val}_p(\#\mathcal{O}/L(\chi, 1-k)). \tag{4.16}$$

If J is principal, then Eq. (4.16) becomes an equality.

Thus, if we can establish the upper bound

$$\mathrm{val}_p\left(\#\mathbb{T}/J\right) \leq \mathrm{val}_p\left(\#\mathcal{O}/L(\chi, 1-k)\right), \tag{4.17}$$

we will be able to use the higher congruences framework to determine if the Eisenstein ideal J is locally principal.

4.4.2. Modularity theorems. To establish an upper bound as in Eq. (4.17), we consider deformation theory and an $R = \mathbb{T}$ argument. Indeed, for Σ a finite set of primes including the odd prime p (from the previous section), let $\mathbb{Q}_\Sigma$ be the maximal extension of $\mathbb{Q}$ unramified outside of Σ and ∞. Suppose that $\mathbb{F}$ is a finite field of characteristic p and that $\chi : \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}) \to \mathbb{F}^\times$ is an odd character ramified at p. Suppose also that

$$\rho_0 : \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}) \tag{4.18}$$

is a continuous representation satisfying

$$\rho_0 = \begin{pmatrix} \chi & * \\ & 1 \end{pmatrix} \tag{4.19}$$

and having scalar centralizer, i.e., ρ_0 is reducible but not semisimple. In [45], Skinner and Wiles give technical conditions for the representation ρ_0 to be *modular*. Their argument centers on understanding the relationship between universal deformation rings R_Σ associated to ρ_0 and certain Hecke algebras $\mathbb{T}_\Sigma$ (from which we have excluded the appropriate Hecke operators for primes $q \in \Sigma$). In particular, in establishing the isomorphism $R_\Sigma \cong \mathbb{T}_\Sigma$, Skinner and Wiles [45, Proposition 3.1, §6] compute the index $\#\mathbb{T}/J$ in Eq. (4.17) for $k = 2$ and certain choices of the character χ.

Now, for a given choice of χ and Σ, it is crucial to the Skinner–Wiles argument that the residual representation is essentially unique, and so, they require χ and Σ to satisfy the following conditions:

- the χ-eigenspace of the p-part of $\mathrm{Cl}(\mathbb{Q}(\chi))$ is trivial;
- if $q \in \Sigma$, then either χ is ramified at q or $\chi(q) \neq q$.

To apply the Skinner–Wiles argument in the general Eisenstein congruences setting described above, we take ρ_0 to be the residual representation $\overline{\rho}_f$, where ρ_f is the Galois representation attached to a cusp form f that satisfies an Eisenstein congruence. (For details on Galois representations associated to cusp forms with Nebentypus, see [40].) When $k = 2$ and $\chi = 1$, which is the setting of Sections 4.2 and 4.3, the assumptions on χ and Σ force us to take $\Sigma = \{p\}$, which implies that $\mathbb{T}_\Sigma$ is necessarily larger than the anemic Hecke algebra $\mathbb{T}_{\mathbb{Z}_p}$. So, while the Skinner–Wiles method is not applicable in this specific case, we should be able to generalize it to give the upper bound in Eq. (4.17) when $k > 2$ or $\chi \neq 1$.

Remark 4.4.2. There is a method of Berger and Klosin [2, 3] which studies similar deformation problems over imaginary quadratic fields. In particular, their approach can be thought of as "perpendicular" to the one of Skinner–Wiles in the sense that the assumptions of each exactly fail to satisfy the assumptions of the other. Specifically, Berger and Klosin consider a different choice of extension in Eq. (4.19) and require the existence of several such extensions. In the case of $k = 2$ and $\chi = 1$, this alternative method might give the desired index because it uses $\chi(q) \neq q^{-1}$ (rather than $\chi(q) \neq q$) in the second condition above, which allows more flexibility in the choice of Σ.

CHAPTER V

APPLICATIONS AND EXAMPLES

For squarefree level N, Proposition 4.2.1 bounds the depth of Eisenstein congruences modulo p by the p-adic valuation of $\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}$. In this section, we first express this depth of congruence as the multiplicity

$$\frac{1}{e_N}\sum_{i=1}^{r} m_i = e(J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}, \mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}).$$

We then use MAGMA [5] to give computational examples of our main results.

5.1. Hilbert–Samuel multiplicities and elliptic modular forms

We apply the commutative algebra result stated in Corollary 3.2.6 in the context of elliptic modular forms to obtain the following proposition:

Proposition 5.1.1. *For $i = 1, \ldots, r$, let $\varpi_N^{m_i}$ be the highest power of ϖ_N such that the Hecke eigenvalues of f_i are congruent to those of $E_{2,N}$ modulo $\varpi_N^{m_i}$ for Hecke operators T_ℓ for all primes $\ell \nmid N$. Then*

$$\frac{1}{e_N}\sum_{i=1}^{r} m_i = e(J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}, \mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}).$$

Proof. As in the proof of Proposition 4.2.1, take $T = \mathbb{T}_{\mathcal{O},\mathfrak{m}}$ and $J = J_{\mathcal{O},\mathfrak{m}}$, where $\mathfrak{m}$ is the unique maximal ideal of $T_{\mathcal{O}}$ containing $J_{\mathcal{O}}$. Let $T_i = \mathcal{O}$ and $\varphi_i : T \to T_i$ be the map sending a Hecke operator to its eigenvalue corresponding to f_i. Also, let

$\varphi_i(\mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}) = T_{\mathbb{Z}_{p_i}}$, $\varphi_i(J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}) = J_{\mathbb{Z}_{p_i}}$. We then have

$$\begin{aligned}
\text{length}_{\mathcal{O}}(T_i/J_i) &= \text{val}_{\varpi}(\#T_i/J_i) \\
&= \frac{1}{d_N} \cdot \text{val}_p(\#T_i/J_i) \\
&= \frac{[\mathcal{O} : \mathbb{Z}_p]}{d_N} \cdot \text{val}_p(\#T_{\mathbb{Z}_{p_i}}/J_{\mathbb{Z}_{p_i}}) \\
&= e_N \cdot \text{length}_{\mathbb{Z}_p}(T_{\mathbb{Z}_{p_i}}/J_{\mathbb{Z}_{p_i}}).
\end{aligned}$$

Since J_i, and $J_{\mathbb{Z}_{p_i}}$ are principal for each i, we may apply Corollary 3.2.6 to obtain

$$e(J_{\mathcal{O},\mathfrak{m}}, \mathbb{T}_{\mathcal{O},\mathfrak{m}}) = e_N \cdot e(J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}, \mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}).$$

Thus,

$$\sum_{i=1}^{s} \text{val}_p\left(\#T_i/J_i\right) = d_N \cdot e(J_{\mathcal{O},\mathfrak{m}}, \mathbb{T}_{\mathcal{O},\mathfrak{m}}) = [\mathcal{O} : \mathbb{Z}_p] \cdot e(J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}, \mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}),$$

and combining this with Eq. (4.11) yields the desired result. □

5.2. Computational examples

We now compute Eisenstein congruences (away from N) for a selection of squarefree levels. Recall from Chapter IV that we want to compute congruences between the Hecke eigenvalues of weight 2 newforms $f_1, \ldots, f_r$ of level N_{f_i} dividing N and the weight 2 Eisenstein series $E_{2,N}$. Since these forms are normalized eigenforms for all Hecke operators T_ℓ with $\ell \nmid N$ prime, this is equivalent to computing congruences between Fourier coefficients, i.e., congruences of the type

$$a_\ell(f_i) \equiv a_\ell(E_{2,N}) \pmod{\lambda_i{}^r}, \tag{5.1}$$

for all primes $\ell \nmid N$. While the algorithm we use is discussed in more detail in Appendix A, we give a sample data entry and a brief explanation below.

Table 1. $N = 165$, $p = 5$

level	r	ramindex	resfield	conjclass
11	1	1	5	1
165	1	1	5	3

Each line of this table corresponds to a newform f_i that represents its Galois orbit under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Column 1 gives the level N_{f_i} of f_i, and Column 5 gives the number of the Galois orbit of f_i with respect to the internal MAGMA numbering. For each congruence, λ_i is a prime ideal, above the prime $p \in \mathbb{Z}$, in the ring of integers of the coefficient field K_{f_i}. Column 2 gives the exponent of each congruence, i.e., the value of r in Eq. (5.1), and Coumns 3 and 4 give the ramification index and the order of the residue field, respectively, of the ideal λ_i at p. Note that to simplify calculations, we compute each congruence in the ring of integers of the individual coefficient field K_{f_i}. In particular, because ramification indices are multiplicative, we can easily translate this data into congruences modulo a uniformizer of the ring of integers in the composite coefficient field $E/\mathbb{Q}_p$, as required by Proposition 4.2.1.

Remark 5.2.1. As discussed in Section 4.3, when $\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) = \mathrm{val}_p(\varphi(N))$, Theorem 4.0.1 and Corollary 4.3.1 can be used to show that the Eisenstein ideal $J_{\mathbb{Z}}$ is not locally principal. By combining explicit computations with the multiplicity result in Proposition 5.1.1, we might be able to give a more precise bound on the minimal number of generators that each (localized) Eisenstein ideal $J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}$ requires.

5.2.1. Examples where N has at least three prime divisors. In each of these examples, the level N has at least 3 prime divisors and $p \geq 5$ divides $\varphi(N)$. Hence, from Theorem

4.0.1, we know that the depth of Eisenstein congruences modulo p is strictly greater than the p-adic valuation of $\varphi(N)$.

Table 2. $N = 66$, $p = 5$

level	r	ramindex	resfield	conjclass
11	1	1	5	1
66	1	1	5	3

Table 3. $N = 330$, $p = 5$

level	r	ramindex	resfield	conjclass
11	1	1	5	1
66	1	1	5	3
110	1	1	5	3
165	1	1	5	3

Table 4. $N = 418$, $p = 5$

level	r	ramindex	resfield	conjclass
11	1	1	5	1
38	1	1	5	2
209	1	1	5	3
418	1	1	5	6

5.2.2. Examples where N has exactly two prime divisors. Let $N = qr$. When $p \geq 5$ is coprime to N, Corollary 4.3.1 specifies when the depth of Eisenstein congruences modulo p is strictly greater than the p-adic valuation of $\varphi(N)$, and the computations below verify our results.

Table 5. $N = 217$, $p = 5$

level	r	ramindex	resfield	conjclass
31	1	2	5	1

Table 6. $N = 319$, $p = 5$

level	r	ramindex	resfield	conjclass
11	1	1	5	1
319	1	1	5	4

Table 7. $N = 319$, $p = 7$

level	r	ramindex	resfield	conjclass
29	1	1	7	1

Table 8. $N = 341$, $p = 5$

level	r	ramindex	resfield	conjclass
11	1	1	5	1
31	1	2	5	1
341	1	2	5	1

When $p \geq 5$ divides N, Corollary 4.3.1 does not apply. However, we can use direct computations to determine if the depth of Eisenstein congruences modulo p is strictly greater than the p-adic valuation of $\varphi(N)$.

Table 9. $N = 55$, $p = 5$

level	r	ramindex	resfield	conjclass
11	1	1	5	1

Table 10. $N = 155$, $p = 5$

level	r	ramindex	resfield	conjclass
31	1	2	5	1
155	1	1	5	3

Table 11. $N = 203$, $p = 7$

level	r	ramindex	resfield	conjclass
29	1	1	7	1

5.2.3. Examples with $p = 3$. As discussed in Remark 4.3.3, Theorem 4.0.1 and Corollary 4.3.1 do not hold for $p = 3$ because of the powers of 3 that appear in the computation of the index $\#\mathbb{T}^{\epsilon}_{\mathbb{Z}_p}/J^{\epsilon}_{\mathbb{Z}_p}$ [38, Proposition 3.1.3]. However, using direct computations, we can compare the depth of Eisenstein congruences modulo p to the p-adic valuation of $\varphi(N)$. The examples below illustrate that this depth can be strictly greater than, equal to, or strictly less than the p-adic valuation of $\varphi(N)$.

Table 12. $N = 57$, $p = 3$

level	r	ramindex	resfield	conjclass
19	1	1	3	1

Table 13. $N = 91$, $p = 3$

level	r	ramindex	resfield	conjclass
91	1	1	3	2

Table 14. $N = 182$, $p = 3$

level	r	ramindex	resfield	conjclass
14	1	1	3	1
26	1	1	3	1
91	1	1	3	2
182	1	1	3	5

Table 15. $N = 217$, $p = 3$

level	r	ramindex	resfield	conjclass
217	1	3	3	2

Table 16. $N = 399$, $p = 3$

level	r	ramindex	resfield	conjclass
19	1	1	3	1
133	2	1	3	3
399	2	1	3	7

Table 17. $N = 418$, $p = 3$

level	r	ramindex	resfield	conjclass
19	1	1	3	1
38	1	1	3	1
209	1	1	3	1
209	1	3	3	4
418	1	1	3	5
418	1	2	3	6

5.2.4. An example where p does not divide $\varphi(N)$. While the main results of this paper focus on Eisenstein congruences modulo primes that divide $\varphi(N)$, we give an example of an Eisenstein congruence modulo a prime that does not divide $\varphi(N)$. Indeed, for $N = 203 = 7 \times 29$, the prime $p = 5$ does not divide $\varphi(N)$. However, since 5 divides $29 + 1 = 30$, the admissibility results in [50, Theorem 2.3] and [29, Theorem A] imply there is an Eisenstein congruence (away from N) modulo $p = 5$. In particular, the lower bounds given in Theorem 4.0.1 and Corollary 4.3.1 still holds in such cases but are not useful in terms of determining the local principality of the Eisenstein ideal since we know $\mathrm{val}_p(\#\mathbb{T}_{\mathbb{Z}_p}/J_{\mathbb{Z}_p}) \neq \mathrm{val}_p(\varphi(N))$.

Table 18. $N = 203$, $p = 5$

level	r	ramindex	resfield	conjclass
203	1	1	5	2

APPENDIX A

ALGORITHM FOR COMPUTING EISENSTEIN CONGRUENCES

We give the algorithm implemented in MAGMA [5] to compute the depth of Eisenstein congruences in Section V. This algorithm has been adapted from [35, §4.2]. Indeed, our main modification is to the Sturm bound in [35, Theorem 2]:

Lemma A.0.1. *Let N be a positive integer, and let $f \in M_2(\Gamma_0(N))$ be a modular form with coefficients in $\mathcal{O}_K$ for some number field K. Let $\mathfrak{p}$ be a fixed prime lying over some rational prime p, and suppose the Fourier coefficients of f satisfy*

$$a_\ell(f) \equiv 0 \mod \mathfrak{p}^m$$

for all primes $\ell \leq \mu'/6$ with $\ell \nmid N$, where

$$\mu' = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N')] \text{ for } N' = N \cdot \prod_{p|N} p.$$

Then $a_\ell(f) \equiv 0 \mod \mathfrak{p}^m$ for all primes $\ell \nmid N$.

Proof. Apply [34, Lemma 4.6.5] to obtain a modular form $f' \in M_2(\Gamma_0(N'))$ defined by

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

Note that $N' = N \cdot \prod_{p|N} p$ as above. Since the Fourier coefficients of f' vanish at any n such that $\gcd(n, N) \neq 1$, the hypotheses of this lemma imply that

$$a_n(f') \equiv 0 \mod \mathfrak{p}^m$$

for all $n \leq \mu'/6$. Hence, by the straightforward generalization of Sturm's theorem stated in [10, Proposition 1], we have $f' \equiv 0 \mod \mathfrak{p}^m$, and hence,

$$a_\ell(f) \equiv 0 \mod \mathfrak{p}^m$$

for all primes $\ell \nmid N$. □

By Lemma A.0.1, it is sufficient for our algorithm to check only for congruences between the Hecke eigenvalues of newforms $f_1, \ldots, f_r$ and Eisenstein series $E_{2,N}$ for Hecke operators T_ℓ with $\ell \leq \mu'/6$ and $\ell \nmid N$. Thus, we replace the Sturm bound in Naskręcki's algorithm with

$$B = \frac{1}{6} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N')] = \frac{1}{6} \cdot N \cdot \prod_{p|N}(p+1).$$

Since the utilization of orders in number fields in Naskręcki's computations of congruences is unrelated to whether or not the level N is prime, this adjusted Sturm bound allows us to generalize Naskręcki's algorithm:

Input: A positive squarefree integer N. For each non-prime divisor M of N:

1. Compute Galois conjugacy classes of newforms in $S_2(\Gamma_0(M))$. Call the set *New*.
2. Compute the Sturm bound $B = \frac{1}{6} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N')] = \frac{1}{6} \cdot N \cdot \prod_{p|N}(p+1)$.
3. Compute the coefficients $a_\ell(E_{2,N})$ for primes $\ell \leq B$ with $\ell \nmid N$.
4. Calculate the set of primes $P = \{p \text{ prime} : p \,|\, \text{Numerator}\,(\varphi(N))\}$.
5. For each pair $(p, f) \in P \times \mathit{New}$, compute K_f, the coefficient field of f.
6. Find an algebraic integer θ such that $K_f = \mathbb{Q}(\theta)$.

7. Compute a p-maximal order $\mathcal{O}$ above $\mathbb{Z}[\theta]$.

8. Compute the set $\mathcal{S} = \{\lambda \in \operatorname{Spec} \mathcal{O} : \lambda \cap \mathbb{Z} = p\mathbb{Z}\}$.

9. For each $\lambda \in \mathcal{S}$, compute

$$r_\lambda = \min_{\substack{\ell \text{ prime} \\ \ell \leq B,\ \ell \nmid N}} \left(\operatorname{ord}_\lambda(a_\ell(f) - a_\ell(E_{2,N}))\right).$$

Output: If $r_\lambda > 0$, then we have a congruence

$$a_\ell(f) \equiv a_\ell(E_{2,N}) \mod (\lambda \mathcal{O}_f)^{r_\lambda}$$

for all primes $\ell \nmid N$.

Remark A.0.2. Since this algorithm computes congruences modulo prime ideals in the ring of integers of a global field, we must reinterpret its output within the local framework used in Proposition 4.2.1. More specifically, let $f_1, \ldots, f_r$ be all newforms of level M, and let $L/\mathbb{Q}$ contain all Fourier coefficients of the f_i's. If $\mathfrak{p} \subseteq \mathcal{O}_L$ corresponds to our choice of embedding $\overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$, then Proposition 4.2.1 requires us to check for congruences modulo $\mathfrak{p}$ for every $\operatorname{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)$-orbit in the set of newforms $\{f_1, \ldots, f_r\}$. Our algorithm accomplishes this by fixing one representative of each $\operatorname{Gal}(L/\mathbb{Q})$-orbit in $\{f_1, \ldots, f_r\}$ and checking for congruences modulo all prime ideals in $\mathcal{O}_L$ lying over p.

APPENDIX B

A GEOMETRIC CONSTRUCTION OF MODULAR FORMS

We now discuss an algebraic notion of a modular form with coefficients in an arbitrary ring A. The theory of such modular forms is useful in many different contexts, especially in the study of congruences between Hecke eigenvalues. Because of complications that arise from the existence of torsion in certain congruence subgroups, we restrict our attention to the congruence subgroup $\Gamma_1(N) \subset \mathrm{SL}(2,\mathbb{Z})$ for $N > 4$ in the first three sections. However, the constructions described below can be generalized for any congruence subgroup in $\mathrm{SL}(2,\mathbb{Z})$. See [14, §12] for details.

This appendix is organized as follows. We first give an equivalent definition of modular forms (over $\mathbb{C}$) as sections of certain line bundles on modular curves. We then reinterpret the relevant line bundles as arising in the context of certain moduli problems, which allows us to give a definition of modular forms over an arbitrary ring. Finally, we state the q-expansion principle as well as a few important corollaries.

B.1. Line bundles on modular curves

Let $k \geq 0$ be an integer, and for $N > 4$, let $\Gamma = \Gamma_1(N)$ be the usual congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$. Also, let $X = X_1(N)$ denote the (compact) modular curve $\Gamma \setminus \mathfrak{h}^*$ and Y the open subspace $\Gamma \setminus \mathfrak{h}$. We define an action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathfrak{h} \times \mathbb{C}$ by

$$\alpha \cdot (z, \xi) = (\alpha z, (cz + d)^k \xi), \tag{B.1}$$

where $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$, $z \in \mathfrak{h}$, and $\xi \in \mathbb{C}$. Since the image of Γ in $\mathrm{PSL}(2,\mathbb{Z})$ has no nontrivial elements of finite order, the quotient $\Gamma \setminus (\mathfrak{h} \times \mathbb{C})$, with the natural projection map to Y, has the structure of a complex line bundle over Y. In particular,

we may extend it to a line bundle over X using the trivialization (over a neighborhood of the cusps [14, §9.1]) defined by

$$\Gamma \cdot \gamma(z, \xi) \mapsto (\Gamma \cdot \gamma z, \xi)$$

for $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ and $z = x + iy$ with $y > 0$. We denote the resulting line bundle by G_k and write $\psi : G_k \to X$ for the projection map.

We next consider the sheaf $\mathcal{G}_k$ on X of holomorphic sections of G_k. First, when $k = 0$, the action of $\mathrm{SL}(2, \mathbb{Z})$ on $\mathfrak{h} \times \mathbb{C}$ given in Eq. (B.1) simplifies to

$$\alpha \cdot (z, \xi) = (\alpha z, \xi),$$

i.e., $\mathcal{G}_0$ is the trivial line bundle. For $k > 0$, $\mathcal{G}_k$ is always an invertible sheaf of $\mathcal{O}_X$-modules. Now, if f is a modular form of weight k with respect to Γ, we can define an element of $\mathcal{G}_k(Y)$ by

$$\Gamma \cdot z \mapsto \Gamma \cdot (z, f(z)).$$

Note this map is well-defined because of the weight-k modularity property of $f(z)$:

$$\begin{aligned} \Gamma \cdot (\gamma z) &\mapsto \Gamma \cdot ((\gamma z, f(\gamma z)) \\ &= \Gamma \cdot (\gamma z, (cz + d)^k f(z)), \\ &= \Gamma\gamma \cdot (z, f(z)), \qquad \forall \gamma \in \Gamma. \end{aligned}$$

Moreover, the condition that f is holomorphic at the cusps translates to the condition that this section extends to a holomorphic section $\phi_f : X \to G_k$. Hence, the map $f \mapsto \phi_f$ gives a natural bijection between the spaces $M_k(\Gamma)$ and $\mathcal{G}_k(X) = H^0(X, \mathcal{G}_k)$.

Similarly, we may interpret $S_k(\Gamma)$, the cusp forms of weight k with respect to Γ, as global sections of a certain invertible sheaf on X. Indeed, let $\mathcal{C}_k \subset \mathcal{O}_X$ denote the

sheaf of holomorphic functions on X which vanish at the cusps. We define $\mathcal{F}_k$ to be the invertible sheaf $\mathcal{G}_k \otimes_{\mathcal{O}_X} \mathcal{C}_k$ of $\mathcal{O}_X$-modules on X. Then $\mathcal{F}_k$ is naturally a subsheaf of $\mathcal{G}_k$ and we may identify $\mathcal{F}_k(X) \subset \mathcal{G}_k(X)$ with $S_k(\Gamma) \subset M_k(\Gamma)$.

The case $k = 2$ is particularly interesting because we can identify $\mathcal{F}_2$ with Ω^1_X, the sheaf of holomorphic differentials on X. Indeed, to give an explicit description of the isomorphism $\Omega^1_X \cong \mathcal{F}_2$, we consider $\omega \in \Omega^1_X(U)$ for an open subset U of X. We can write $\varrho^*\omega = f(z)dz$ for a holomorphic function f on $\varrho^{-1}(U)$, where ϱ is the natural map $\mathfrak{h} \to X$. In particular, in order for $\omega \in \Omega^1_X(U)$ to be a well-defined differential on X, it must be invariant under the action of Γ, i.e.,

$$f(\gamma z)d(\gamma z) = f(z)dz, \qquad \forall \gamma \in \Gamma. \tag{B.2}$$

Since $\frac{d(\gamma z)}{dz} = (cz + d)^{-2}$, Eq. (B.2) is equivalent to

$$f(\gamma z) = (cz + d)^2 f(z), \qquad \forall \gamma \in \Gamma,$$

i.e., $f(z)$ is a weight 2 modular forms with respect to Γ. So, for $U^\circ = U \cap Y$, the holomorphic map $U^\circ \to G_2$ defined by $\Gamma \cdot z \mapsto \Gamma \cdot (z, f(z))$ is an element of $\mathcal{G}_2(U^\circ) = \mathcal{F}_2(U^\circ)$ which extends uniquely to an element ϕ_ω of $\mathcal{F}_2(U)$. In particular, the map $\omega \mapsto \phi_\omega$ defines an $\mathcal{O}_x(U)$-linear isomorphism $\Omega^1_X(U) \to \mathcal{F}_2(U)$ that is compatible with restriction, and hence,

$$\Omega^1_X \cong \mathcal{F}_2. \tag{B.3}$$

For additional details, see [34, Theorem 2.3.2].

Remark B.1.1. For a congruence subgroup $\Gamma \neq \Gamma_1(N)$, the isomorphism

$$M_k(\Gamma) \cong \mathcal{G}_k(X) \tag{B.4}$$

can be established identically if Γ is k-small, cf. [14, §12.1]. When Γ is not k-small, Eq. (B.4) still holds, but its proof requires a few modifications.

Remark B.1.2. Using Riemann–Roch, we can compute the dimension of $M_k(\Gamma)$ and $S_k(\Gamma)$, assuming $k \neq 1$. For example, when $k = 2$, we immediately see (from Eq. (B.3)) that the dimension of $S_2(\Gamma)$ is the genus of the modular curve X. Such dimension formulas are provided in [14, Eqs. (12.1.5) and (12.1.6)].

B.2. Moduli problems

To generalize the above construction to an arbitrary base scheme, we need to regard the sheaves $\mathcal{G}_k$ as arising naturally within the context of certain moduli problems. Indeed, in Section 2.2.4, we used the modular curve $Y_1(N)$ to classify isomorphism classes of certain complex elliptic curves. We now consider similar moduli problems with elliptic curves over arbitrary schemes.

Definition B.2.1. An *elliptic curve over a scheme* S is a proper smooth morphism $p : \mathcal{E} \to S$, whose geometric fibres are connected curves of genus one, together with a section $e : S \to \mathcal{E}$:

$$\begin{array}{c} \mathcal{E} \\ {\scriptstyle p}\big\downarrow \big\uparrow{\scriptstyle e} \\ S \end{array}$$

A section $\mathcal{P} : S \to \mathcal{E}$ is said to have exact order N if for all geometric points $s : \operatorname{Spec} k \to S$, the composition $\mathcal{P} \circ s$ has order N in $\mathcal{E}(k)$.

Given this definition, we define the following contravariant functor $\mathcal{F}_1(N)$ from $\mathbb{Z}[1/N]$-schemes to sets. For a scheme S over $\mathbb{Z}[1/N]$, let $\mathcal{F}_1(N)(S)$ be the the set of isomorphism classes of pairs $(\mathcal{E}, \mathcal{P})$, where $\mathcal{E}$ is an elliptic curve over S and $\mathcal{P}$ is an element of $\mathcal{E}(S)$ of exact order N. If $f : S \to T$ is a morphism of schemes, then we define $\mathcal{F}_1(N)(f) : \mathcal{F}_1(N)(T) \to \mathcal{F}_1(N)(S)$ via base-change, cf. [14, §8.2].

As in the case with complex elliptic curves, we would like a curve (or scheme) which represents the functor $\mathcal{F}_1(N)$. The following theorem, whose proof is essentially due to Igusa [20] but can also be found in [22], establishes the existence of such a scheme:

Theorem B.2.2. *If $N > 3$, then there is a scheme $\mathcal{Y}_1(N)$ which represents the functor $\mathcal{F}_1(N)$. Moreover, $\mathcal{Y}_1(N)$ is smooth of relative dimension one over $\mathbb{Z}[1/N]$ with irreducible geometric fibers.*

In this theorem, "$\mathcal{Y}_1(N)$ represents $\mathcal{F}_1(N)$" means that there is a natural isomorphism from the functor $\mathrm{Hom}(-, \mathcal{Y}_1(N))$ and $\mathcal{F}_1(N)$. If we take $S = \mathcal{Y}_1(N)$, then the identity map $\mathcal{Y}_1(N) \to \mathcal{Y}_1(N)$ corresponds to a pair $(\mathcal{E}_{\mathrm{univ}}, \mathcal{P}_{\mathrm{univ}})$, which is the *universal elliptic curve with a point of order N*. This pair is universal in the sense that we can obtain any pair $(\mathcal{E}_T, \mathcal{P}_T)$ over a $\mathbb{Z}[1/N]$-scheme T from $(\mathcal{E}_{\mathrm{univ}}, \mathcal{P}_{\mathrm{univ}})$ by base-change for a unique morphism $T \mapsto \mathcal{Y}_1(N)$, i.e., we can define $(\mathcal{E}_T, \mathcal{P}_T)$ so that the squares in the following diagram are cartesian:

$$\begin{array}{ccc} T & \longrightarrow & \mathcal{Y}_1(N) \\ \downarrow{\scriptstyle \mathcal{P}_T} & & \downarrow{\scriptstyle \mathcal{P}_{univ}} \\ \mathcal{E}_T & \longrightarrow & \mathcal{E}_{univ} \\ \downarrow & & \downarrow \\ T & \longrightarrow & \mathcal{Y}_1(N) \end{array}$$

In the case $S = \operatorname{Spec} \mathbb{C}$, this construction gives a natural bijection between $\mathcal{Y}_1(N)(\mathbb{C})$ and the modular curve $Y_1(N)$. (Recall from Section 2.2.4 that the points of $Y_1(N)$ parametrize isomorphism classes of complex elliptic curves with a points of level N.)

Remark B.2.3. Depending on the situation, it can be convenient to use models for $Y_1(N)$ with different sets of conventions. (A model for a modular curve Y over a subring R of $\mathbb{C}$ is a pair $(\mathcal{Y}, \phi)$ such that $\mathcal{Y}$ is a scheme over $\operatorname{Spec} R$ with one-dimensional fibers, and ϕ is analytic isomorphism $Y \cong \mathcal{Y}(\mathbb{C})$.) For example, in the discussion above, we use the model $(\mathcal{Y}_1(N)(\mathbb{C}), \phi)$ for the modular curve $Y_1(N)$, where ϕ is the natural bijection between $\mathcal{Y}_1(N)(\mathbb{C})$ and $Y_1(N)$. However, when studying q-expansions, a slightly different model is more convenient. Indeed, [14, Variant 8.2.2] describes one such model, which parametrizes pairs $(\mathcal{E}, i)$, where i is a closed immersion $(\mu_N)_S \hookrightarrow S$. While we do not recall the details of this choice of convention, we denote the resulting model by $\mathcal{Y}_\mu(N)$ and use it later.

To define canonical models for the compact modular curves $X_1(N)$, we consider similar moduli problems but with *generalized elliptic curves*. In this case, when $N > 4$, the corresponding functor $\mathcal{G}_1(N)$ is representable by a smooth curve $\mathcal{X}_1(N)$ over $\operatorname{Spec} \mathbb{Z}[1/N]$. In particular, using the alternate convention mentioned in Remark B.2.3, we obtain a model $\mathcal{X}_\mu(N)$ over $\mathbb{Z}$ for $X_1(N)$ which contains $\mathcal{Y}_\mu(N)$ as an open subscheme. Additional details are given in [14, §9.3, page 79].

Remark B.2.4. Rather than using the congruence subgroup $\Gamma_1(N)$, we could take $\Gamma = \Gamma_0(N)$ and formulate analogous moduli problems using isomorphism classes of pairs $(\mathcal{E}, \mathcal{C})$, where $\mathcal{E}$ is an elliptic curve over S and $\mathcal{C}$ is a finite flat subscheme of $\mathcal{E}$ whose geometric fibers are cyclic groups of order N. However, the question of representability in this case is complicated by torsion in $\Gamma_0(N)$. Indeed, it can be shown that the functors $\mathcal{F}_0(N)$ and $\mathcal{G}_0(N)$ do not have fine moduli spaces but

rather have coarse moduli spaces, which we denote $\mathcal{Y}_0(N)$ and $\mathcal{X}_0(N)$, respectively. Additional details can be found in [14, §8.2 and §9.3].

B.3. Modular forms over an arbitrary ring

We now give a moduli-theoretic interpretation of the line bundle G_1, which allows us to define modular forms over arbitrary rings. Indeed, let E_{univ} denote the complex points of $\mathcal{E}_{\text{univ}}$, the universal elliptic curve over $\mathcal{Y}_\mu(N)$ and $P_{\text{univ}} : Y_1(N) \to E_{\text{univ}}$ denote the corresponding family of points of order N:

$$\begin{array}{ccc}
Y_1(N) & \longrightarrow & \mathcal{Y}_1(N) \\
\downarrow{\scriptstyle P_{\text{univ}}} & & \downarrow{\scriptstyle \mathcal{P}_{\text{univ}}} \\
E_{\text{univ}} & \longrightarrow & \mathcal{E}_{\text{univ}} \\
\downarrow & & \downarrow \\
Y_1(N) & \longrightarrow & \mathcal{Y}_1(N) \\
\downarrow & & \downarrow \\
\operatorname{Spec}\mathbb{C} & \longrightarrow & \operatorname{Spec}\mathbb{Z}[1/N]
\end{array}$$

Remark B.3.1. Using the variant model $\mathcal{Y}_\mu(N)$ that is described in Remark B.2.3, we can give a concrete description of E_{univ}. See [14, §12.3] for details.

We identify the line bundle $G_1|_{Y_1(N)}$ on $Y_1(N)$ with the restriction along the zero section of the relative cotangent bundle of E_{univ} over $Y_1(N)$. More precisely, the latter bundle is canonically isomorphic to $\Gamma_1(N) \setminus (\mathfrak{h} \times V)$, where V is the cotangent space of $\mathbb{C}$ at the origin and the action of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is given by

$$(z, d\zeta) \mapsto (\gamma z, (cz + d)d\zeta).$$

So, we can identify with $G_1|_{Y_1(N)}$ via $(z,\xi) \leftrightarrow (z, 2\pi i \xi d\zeta)$. Moreover, we can extend this moduli-theoretic description of G_1 to the cusps by considering the universal generalized elliptic curve. See [14, §9.3] for details.

Now, we can use this moduli-theoretic interpretation of the line bundle G_1 to construct analogous invertible sheaves on $\mathcal{X}_\mu(N)$ which are canonical models for G_1 over arbitrary schemes. Indeed, let $\underline{\omega}$ denote the pullback along the zero section $e : \mathcal{X}_\mu(N) \to \mathcal{E}_{\text{univ}}$ of the sheaf $\Omega^1_{\mathcal{E}_{\text{univ}}/\mathcal{X}_\mu(N)}$:

$$\begin{array}{c} \mathcal{E}_{\text{univ}} \\ \pi \big\downarrow \big\uparrow e \\ \mathcal{X}_1(N) \\ \big\downarrow \\ \operatorname{Spec} \mathbb{Z}[1/N] \end{array} \qquad \underline{\omega} := e^* \Omega^1_{\mathcal{E}_{\text{univ}}/\mathcal{X}_\mu(N)} \tag{B.5}$$

Remark B.3.2. Rather than defining $\underline{\omega}$ via a pullback as above, we could use a pushforward, i.e., $\underline{\omega} = \pi_*(\Omega^1_{\mathcal{E}_{\text{univ}}/\mathcal{X}_\mu(N)})$. This alternative approach is given in [21]. Note that both of these formulations can be used for constructions analogous to Eq. (B.5) in cases of more general families of automorphic forms. (See [26, 27] for definitions using a pullback or [9] for definitions using a pushforward.)

Since $\mathcal{E}_{\text{univ}}$ is a smooth curve over $\mathcal{X}_1(N)$, $\underline{\omega}$ is an invertible sheaf on $\mathcal{X}_\mu(N)$. In particular, the complex analytic sheaf on $X_1(N)$ associated to $\underline{\omega}_{\mathbb{C}}$ via base-change can be identified with the sheaf $\mathcal{G}_1$ from above. Moreover, $\underline{\omega}^{\otimes k}$ is a model for $\mathcal{G}_k$ (which we have identified with $M_k(\Gamma_1(N))$), and using the Gauss–Manin connection, cf. [12, §VI.4.5], [21, A1.3], we can show that $\underline{\omega}^{\otimes(k-2)} \otimes \Omega^1_{\mathcal{X}_\mu(N)/\mathbb{Z}}$ is a model for $\mathcal{F}_k$ (which we have identified with $S_k(\Gamma_1(N))$). Hence, we can give the following definition of a modular form over an arbitrary ring A:

Definition B.3.3. For an arbitrary ring A, *a modular form over* A (of weight k with respect to $\Gamma_1(N)$) is an element of

$$H^0\big(\mathcal{X}_\mu(N)_A,\, \underline{\omega}_A^{\otimes k}\big).$$

Similarly, *a cusp form over* A is an element of

$$H^0\big(\mathcal{X}_\mu(N)_A,\, \underline{\omega}_A^{\otimes(k-2)} \otimes \Omega^1_{\mathcal{X}_\mu(N)/A}\big).$$

We write $\mathcal{M}_k(\Gamma_1(N); A)$ for the A-module of modular forms over A and $\mathcal{S}_k(\Gamma_1(N); A)$ for the cusp forms which we regard as a submodule of $\mathcal{M}_k(\Gamma_1(N); A)$.

We can formulate an equivalent definition of a modular form $f \in \mathcal{M}_k(\Gamma_1(N); A)$ as follows. A modular form over A (of weight k with respect to $\Gamma_1(N)$) is a rule f which assigns to every triple $(\mathcal{E}/A, \mathcal{P}, \omega)$ consisting of an elliptic curve over (the spectrum of) the ring A and a section $\mathcal{P}$ of exact order N, together with a basis ω of $\underline{\omega}_{\mathcal{E}/A}$ (i.e., a nowhere vanishing section of $\Omega^1_{\mathcal{E}/A}$ on $\mathcal{E}$), an element $f(\mathcal{E}/A, \mathcal{P}, \omega) \in A$, such that the following three conditions are satisfied.

1. $f(\mathcal{E}/A, \mathcal{P}, \omega)$ depends only on the A-isomorphism class of the triple $(\mathcal{E}/A, \mathcal{P}, \omega)$.

2. f is homogeneous of degree $-k$ in the third variable, i.e., for any $\lambda \in A^\times$, we have $f(\mathcal{E}, \mathcal{P}, \lambda\omega) = \lambda^{-k} f(\mathcal{E}, \mathcal{P}, \omega)$.

3. The formation of $f(\mathcal{E}/A, \mathcal{P}, \omega)$ commutes with arbitrary extension of scalars $g : A \to A'$, i.e., $f(\mathcal{E}_{A'}/A', \mathcal{P}', \omega_{A'}) = g(f(\mathcal{E}/A, \mathcal{P}, \omega_A)$.

The correspondence between these two notions is given by the formula

$$f(\mathcal{E}/\operatorname{Spec} A, \mathcal{P}) = f(\mathcal{E}/A, \mathcal{P}, \omega) \cdot \omega^{\otimes k}.$$

(See [21] for more details of this formulation.)

Now, identifying $\mathcal{G}_k$ with the complex analytic sheaf associated to $\underline{\omega}_{\mathbb{C}}^{\otimes k}$ gives natural isomorphisms

$$M_k(\Gamma_1(N)) \cong \mathcal{M}_k(\Gamma_1(N); \mathbb{C});$$
$$S_k(\Gamma_1(N)) \cong \mathcal{S}_k(\Gamma_1(N); \mathbb{C}).$$

Moreover, base change arguments (see [21, §1.7] and [30, §II.3]) and properties of the scheme $\mathcal{X}_\mu(N)$ yield the following theorem [14, Theorem 12.3.2]:

Theorem B.3.4. *If B is an A-algebra and either of the following hold*

- *B is flat over A;*
- *$k > 1$ and N is invertible in B,*

then the natural maps

$$\mathcal{M}_k(\Gamma_1(N); A) \otimes_A B \to \mathcal{M}_k(\Gamma_1(N); B);$$
$$\mathcal{S}_k(\Gamma_1(N); A) \otimes_A B \to \mathcal{S}_k(\Gamma_1(N); B)$$

are isomorphisms.

As we will see in the next section, this theorem is quite useful when developing the theory of modular forms over arbitrary rings because it allows us to work with $\mathcal{M}_k(\Gamma_1(N); \mathbb{Z})$ and then extend scalars to any $\mathcal{M}_k(\Gamma_1(N); A)$.

B.4. The q-expansion principle

Let $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$, and consider the injective map

$$\mathcal{M}_k(\Gamma; \mathbb{C}) \to \mathbb{C}[\![q]\!], \tag{B.6}$$

which sends a modular form to its Fourier expansion at ∞ as in Eq. (2.1). Let $\mathbf{M}_k(\Gamma;\mathbb{Z})$ denote the set of elements of $\mathcal{M}_k(\Gamma;\mathbb{C})$ with Fourier coefficients in $\mathbb{Z}$, i.e., the preimage of $\mathbb{Z}[\![q]\!]$. For an arbitrary ring A, we write $\mathbf{M}_k(\Gamma;A)$ for $\mathbf{M}_k(\Gamma;\mathbb{Z})\otimes A$. In particular, since $\mathbf{M}_k(\Gamma;\mathbb{Z})\to\mathbb{Z}[\![q]\!]$ has torsion-free cokernel, the map

$$\mathbf{M}_k(\Gamma;A)\to A[\![q]\!],$$

obtained by tensoring with A, is also injective. We define $\mathbf{S}_k(\Gamma;A)$ similarly using cusp forms and identify it with an A-submodule of $\mathbf{M}_k(\Gamma;A)$.

Now, for an arbitrary ring A, the q-expansion principle (stated as Theorem B.4.1 below) often allows us to identify the space of modular forms $\mathcal{M}_k(\Gamma;A)$ defined over A with the space of modular forms $\mathbf{M}_k(\Gamma;A)$. However, before we can state this result, we need a way to write q-expansions for the algebraic notion of modular forms over A. Indeed, Deligne and Rapoport's algebraic description of the cusps [12], whose details we omit, allows us to write a q-expansion homomorphism

$$\phi_{\infty,A}:\mathcal{M}_k(\Gamma_1(N);A)\to A[\![q]\!]. \tag{B.7}$$

Note that the restriction of $\phi_{\infty,A}$ to $\mathcal{S}_k(\Gamma_1(N);A)$ maps to $qA[\![q]\!]$. Moreover, the maps $\phi_{\infty,A}$ are functorial in A, and in the case $A=\mathbb{C}$, the image under $\phi_{\infty,A}$ in Eq. (B.7) becomes the usual q-expansion at ∞.

Given the q-expansion homomorphism $\phi_{\infty,A}$, we state the q-expansion principle as it appears in [14, Theorem 12.3.4]:

Theorem B.4.1. *1. The homomorphism $\phi_{\infty,A}$ is injective for every ring A.*

2. If A is a subring of B, then the commutative diagram

$$\begin{array}{ccc} \mathcal{M}_k(\Gamma_1(N); A) & \xrightarrow{\phi_{\infty,A}} & A[\![q]\!] \\ \downarrow & & \downarrow \\ \mathcal{M}_k(\Gamma_1(N); B) & \xrightarrow{\phi_{\infty,B}} & B[\![q]\!] \end{array}$$

is Cartesian, i.e., the image of $\mathcal{M}_k(\Gamma_1(N); A)$ in $\mathcal{M}_k(\Gamma_1(N); B)$ is precisely the set of modular forms whose q-expansions at ∞ have coefficients in A.

3. *The above assertions hold with $\mathcal{M}_k$ replaced by $\mathcal{S}_k$.*

The proof of this theorem uses the moduli space $\mathcal{X}_\mu(N)$ and arguments of Deligne–Rapoport [12, Theorem VII.3.9] or Katz [21, §1.6]. In particular, Statement 2 establishes that if R is a subring of $\mathbb{C}$, we can identify $\mathcal{M}_k(\Gamma_1(N); R)$ with the set of modular forms in $S_2(\Gamma_1(N))$ whose Fourier coefficients at ∞ lie in R. Combining this with Theorem B.3.4, we obtain the following Theorem [14, Theorem 12.3.7], which gives a precise relationship between the spaces $\mathcal{M}_k(\Gamma_1(N); R)$ and $\mathbf{M}_k(\Gamma_1(N); R)$:

Theorem B.4.2. *The natural maps*

$$\begin{aligned} \mathbf{M}_k(\Gamma_1(N); A) &\to \mathcal{M}_k(\Gamma_1(N); A); \\ \mathbf{S}_k(\Gamma_1(N); A) &\to \mathcal{S}_k(\Gamma_1(N); A) \end{aligned} \tag{B.8}$$

are injective, and are isomorphisms provided one of the following holds

- *A is flat over $\mathbb{Z}$;*
- *$k > 1$ and N is invertible in A.*

While the maps in Eq. (B.8) are often isomorphisms, in certain cases, we can exhibit an element of $\mathcal{M}_k(\Gamma_1(N); R)$ that is not in $\mathbf{M}_k(\Gamma_1(N); R)$ and vice versa. Indeed, for a fixed prime integer $N \geq 5$, define a power series

$$\delta = \sum_{n=1}^{\infty} \sigma^*(n) q^n,$$

where σ^* is the sum of all non-zero divisors d of n such that $(d, N) = 1$. When R has characteristic 2 and $N \equiv 5 \pmod 8$, [30, Proposition II.5.12] implies that $\delta \pmod 2$ is (the q-expansion) of an element of $\mathcal{M}_2(\Gamma_1(N); R)$ but not $\mathbf{M}_2(\Gamma_1(N); R)$. Another such element arises from the Hasse invariant: $\mathcal{M}_2(\Gamma_0(1); \mathbb{Z}/3\mathbb{Z})$ is generated by the form corresponding to the Hasse invariant while $\mathbf{M}_2(\Gamma_0(1); \mathbb{Z}/3\mathbb{Z}) = \{0\}$. (See [38, Proposition 2.3.9] for details on when this form lifts to $\mathbf{M}_2(\Gamma_0(N); \mathbb{Q})$.)

On the other hand, the Eisenstein series

$$E_{2,N} = 1 - N - 24 \sum_{n=1}^{\infty} \sigma^*(n) q^n$$

is an element of $\mathbf{M}_2(\Gamma_1(N); \mathbb{Z})$ but not $\mathcal{M}_2(\Gamma_1(N); \mathbb{Z})$ since its q-expansion at the cusp 0 lies in $N^{-1}\mathbb{Z}$ and is therefore not integral.

We end this section with a brief discussion of the Hecke theory for modular forms defined over an arbitrary ring R. Indeed, the action of the Hecke operators T_m preserves the space $\mathbf{M}_k(\Gamma; \mathbb{Z})$, cf. [14, Proposition 12.4.1], and so, we can regard $\mathbf{M}_k(\Gamma; \mathbb{Z})$ as a $\tilde{\mathbb{T}}$-module, where $\tilde{\mathbb{T}}$ is the Hecke algebra generated over $\mathbb{Z}$ as in Definition 2.2.4. For an arbitrary ring R, we may regard

$$\mathbf{M}_k(\Gamma; R) = \mathbf{M}_k(\Gamma; \mathbb{Z}) \otimes R$$

as a $\tilde{\mathbb{T}} \otimes R$-module, which gives a way (via Theorem B.4.2) to view $\mathcal{M}_k(\Gamma_1(N); R)$ as a Hecke module. If we restrict to the subspace of cusp forms, the duality between $\mathbf{S}_k(\Gamma_1(N); R)$ and $\mathrm{Hom}_R(\mathbb{T}, R)$, discussed in Section 2.4, allows us to relate the structure of the Hecke module $\mathbf{S}_k(\Gamma_1(N); R)$ and the Hecke ring $\mathbb{T} \otimes R$. See [14, §12.4] for more details.

APPENDIX C

LIST OF SYMBOLS

$a_n(f)$	nth Fourier coefficient of f, 15
B_k	kth Bernoulli number, 5
$\mathrm{Cl}(K)$	ideal class group of a number field K, 4
$\langle d \rangle$	diamond operator, 20
$\mathrm{Div}(Y(\Gamma))$	divisor group of $Y(\Gamma)$), 25
$e(\mathfrak{q}, M)$	Hilbert–Samuel multiplicity of $\mathfrak{q}$ on M, 45
$E_k(z)$	weight k Eisenstein series of level 1, 15
$E_{2,N}(z)$	weight 2 Eisenstein series of level N, 16
$\mathcal{E}_{\mathrm{univ}}$	universal elliptic curve, 82
E_{univ}	complex points of $\mathcal{E}_{\mathrm{univ}}$, 84
$\mathrm{Fit}(M)$	Fitting ideal associated to M, 43
$\mathcal{F}_1(N)$	moduli problem for elliptic curves over schemes, 82
$\mathcal{G}_1(N)$	moduli problem for generalized elliptic curves, 83
Γ	congruence subgroup, 13
$[\Gamma_1 \alpha \Gamma_2]_k$	weight-k double coset operator, 20
$\mathfrak{h}$	complex upper-half plane, 13
$\mathfrak{h}^*$	extended complex upper-half plane, 29
$\iota^*_{d,M,N}$	level raising map with $dM \mid N$, 30
$J_{\mathbb{Z}_p}$	Eisenstein ideal in $\mathbb{T}_{\mathbb{Z}_p}$, 57
$J_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}$	localized Eisenstein ideal in $\mathbb{T}_{\mathbb{Z}_p,\mathfrak{m}_{\mathbb{Z}_p}}$, 57
$\lambda_n(f)$	Hecke eigenvalue of f under action of T_n, 24
μ	Möbius function, 50
$M_k(\Gamma)$	modular forms of weight k with respect to Γ, 15

$M_k(N, \varepsilon)$	cusp forms of weight k, level N, Nebentypus ε, 18
$\mathcal{M}_k(\Gamma; A)$	modular forms defined over A, 86
$\mathbf{M}_k(\Gamma; \mathbb{Z})$	elements of $M_k(\Gamma)$ with Fourier coefficients in $\mathbb{Z}$, 36
$\mathcal{O}$	ring of integers in a finite extension of $\mathbb{Q}_p$, 39
ω	Teichmüller character, 6
Ω^1_X	sheaf of holomorphic differentials on X, 81
φ	Euler's totient function, 3
ϕ_∞	q-expansion homomorphism, 37
$\phi_\infty^{(N)}$	anemic q-expansion homomorphism, 39
ρ_f	Galois representation associated to f, 9
σ	sum of positive divisors function, 3
$S_k(\Gamma)$	cusp forms of weight k with respect to Γ, 15
$S_2(\Gamma)^{\text{old}}$	old subspace, 31
$S_2(\Gamma)^{\text{new}}$	new subspace, 31
$S_k(N, \varepsilon)$	cusp forms of weight k, level N, Nebentypus ε, 18
$\mathcal{S}_k(\Gamma; A)$	cusp forms defined over A, 86
$\mathbf{S}_k(\Gamma; \mathbb{Z})$	elements of $S_k(\Gamma)$ with Fourier coefficients in $\mathbb{Z}$, 36
θ_f	eigencharacter of f, 24
$\tilde{\mathbb{T}}_N$	full Hecke algebra generated over $\mathbb{Z}$, 23
$\mathbb{T}_N$	full cuspidal Hecke algebra generated over $\mathbb{Z}$, 24
$\tilde{\mathbb{T}}^{(N)}$	anemic Hecke algebra generated over $\mathbb{Z}$, 23
$\mathbb{T}^{(N)}$	anemic cuspidal Hecke algebra generated over $\mathbb{Z}$, 24
$\mathbb{T}_{\mathbb{Z}_p}$	anemic cuspidal Hecke algebra generated over $\mathbb{Z}_p$, 57
$\mathbb{T}_{\mathbb{Z}_p, \mathfrak{m}_{\mathbb{Z}_p}}$	localization of $\mathbb{T}_{\mathbb{Z}_p}$ at $\mathfrak{m}_{\mathbb{Z}_p}$, 57
T_p	Hecke operator, 21

U_p	Hecke operator T_p when p divides the level N, 22
w_d	Atkin-Lehner operator, 56
$X(\Gamma)$	modular curve $\Gamma \setminus \mathfrak{h}^*$, 29
$\mathcal{X}_\mu(N)$	moduli space for $\mathcal{G}_1(N)$, 83
$Y(\Gamma)$	modular curve $\Gamma \setminus \mathfrak{h}$, 25
$\mathcal{Y}_\mu(N)$	moduli space for $\mathcal{F}_1(N)$, 83
$\mathbb{Z}_+$	positive integers, 21

APPENDIX D

INDEX

REFERENCES CITED

[1] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160. MR 0268123

[2] Tobias Berger and Krzysztof Klosin, *A deformation problem for Galois representations over imaginary quadratic fields*, J. Inst. Math. Jussieu **8** (2009), no. 4, 669–692. MR 2540877

[3] ———, *On deformation rings of residually reducible Galois representations and* $R = T$ *theorems*, Math. Ann. **355** (2013), no. 2, 481–518. MR 3010137

[4] Tobias Berger, Krzysztof Klosin, and Kenneth Kramer, *On higher congruences between automorphic forms*, Math. Res. Lett. **21** (2014), no. 1, 71–82. MR 3247039

[5] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478

[6] N. Boston and B. Mazur, *Explicit universal deformations of Galois representations*, **17** (1989), 1–21. MR 1097607

[7] Jan Hendrik Bruinier, Gerard van der Geer, Günter Harder, and Don Zagier, *The 1-2-3 of modular forms*, Universitext, Springer-Verlag, Berlin, 2008, Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004, Edited by Kristian Ranestad. MR 2385372

[8] Frank Calegari and Matthew Emerton, *On the ramification of Hecke algebras at Eisenstein primes*, Invent. Math. **160** (2005), no. 1, 97–144. MR 2129709

[9] Ana Caraiani, Ellen Eischen, Jessica Fintzen, Elena Mantovan, and Ila Varma, *p-adic q-expansion principles on unitary Shimura varieties*, Directions in number theory, Assoc. Women Math. Ser., vol. 3, Springer, 2016, pp. 197–243. MR 3596581

[10] Imin Chen, Ian Kiming, and Jonas B. Rasmussen, *On congruences mod* p^m *between eigenforms and their attached Galois representations*, J. Number Theory **130** (2010), no. 3, 608–619. MR 2584844

[11] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Int. Press, Cambridge, MA, 1994, pp. 1–154. MR 1474977

[12] 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. MR 0337993

[13] Pierre Deligne, *Formes modulaires et représentations l-adiques*, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, pp. Exp. No. 355, 139–172. MR 3077124

[14] 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. MR 1357209

[15] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR 2112196

[16] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 1322960

[17] Eknath Ghate, *An introduction to congruences between modular forms*, Currents trends in number theory (Allahabad, 2000), Hindustan Book Agency, New Delhi, 2002, pp. 39–58. MR 1925640

[18] E. Hecke, *Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik*, vol. 5, 1927, pp. 199–224. MR 3069476

[19] Jacques Herbrand, *Sur les classes des corps circulaires*, Journal de Mathématiques Pures et Appliquées **11** (1932), 417–441.

[20] Jun-ichi Igusa, *Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves*, Amer. J. Math. **81** (1959), 453–476. MR 0104669

[21] 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

[22] 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

[23] Chandrashekhar Khare, *Notes on Ribet's converse to Herbrand*, (2000), 273–284. MR 1802388

[24] Helmut Klingen, *Über die Werte der Dedekindschen Zetafunktion*, Math. Ann. **145** (1961/1962), 265–272. MR 0133304

[25] E. E. Kummer, *Über eine allgemeine Eigenschaft der rationalen Entwickelungscoefficienten einer bestimmten Gattung analytischer Functionen*, J. Reine Angew. Math. **41** (1851), 368–372. MR 1578727

[26] Kai-Wen Lan, *Arithmetic compactifications of PEL-type Shimura varieties*, London Mathematical Society Monographs Series, vol. 36, Princeton University Press, Princeton, NJ, 2013. MR 3186092

[27] ———, *Compactifications of PEL-type Shimura varieties and Kuga families with ordinary loci*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2018. MR 3729423

[28] Kimball Martin, *Congruences for modular forms mod 2 and quaternionic S-ideal classes*, arXiv:1701.07864 (2017).

[29] ———, *The Jacquet-Langlands correspondence, Eisenstein congruences, and integral L-values in weight 2*, Math. Res. Lett. **24** (2017), no. 6, 1775–1795. MR 3762695

[30] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978). MR 488287

[31] ———, *Deforming Galois representations*, **16** (1989), 385–437. MR 1012172

[32] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. **76** (1984), no. 2, 179–330. MR 742853

[33] Barry Mazur, *How can we construct abelian Galois extensions of basic number fields?*, Bull. Amer. Math. Soc. (N.S.) **48** (2011), no. 2, 155–209. MR 2774089

[34] 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

[35] Bartosz Naskręcki, *On higher congruences between cusp forms and Eisenstein series*, Computations with Modular Forms, Springer, 2014, pp. 257–277.

[36] ———, *On higher congruences between cusp forms and Eisenstein series II*, preprint, 2016.

[37] Masami Ohta, *Congruence modules related to Eisenstein series*, vol. 36, 2003, pp. 225–269. MR 1980312

[38] ———, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II*, Tokyo J. Math. **37** (2014), no. 2, 273–318. MR 3304683

[39] Kenneth A. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. **34** (1976), no. 3, 151–162. MR 0419403

[40] ———, *Galois representations attached to eigenforms with Nebentypus*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Springer, Berlin, 1977, pp. 17–51. Lecture Notes in Math., Vol. 601. MR 0453647

[41] ———, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), no. 1, 193–205. MR 688264

[42] Jean-Pierre Serre, *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

[43] Carl Ludwig Siegel, *Berechnung von Zetafunktionen an ganzzahligen Stellen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II **1969** (1969), 87–102. MR 0252349

[44] ———, *Über die Fourierschen Koeffizienten von Modulformen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II **1970** (1970), 15–56. MR 0285488

[45] C. M. Skinner and A. J. Wiles, *Ordinary representations and modular forms*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), no. 20, 10520–10527. MR 1471466

[46] Preston Wake and Carl Wang-Erickson, *The rank of Mazur's Eisenstein ideal*, arXiv:1707.01894 (2017).

[47] Lawrence C. Washington, *Introduction to cyclotomic fields*, Second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575

[48] Hwajong Yoo, *The index of an Eisenstein ideal and multiplicity one*, Math. Z. **282** (2016), no. 3-4, 1097–1116. MR 3473658

[49] ———, *On Eisenstein ideals and the cuspidal group of $J_0(N)$*, Israel J. Math. **214** (2016), no. 1, 359–377. MR 3540618

[50] ———, *Non-optimal levels of a reducible mod ℓ modular representation*, arXiv:1409.8342 (2017).