INSIGHTS FROM NUMBER THEORY: FROM ARITHMETIC GEOMETRY TO QUANTUM TOPOLOGY

Eleanor Grace McSpirit
Denver, Colorado

B.A. Pure Mathematics, University of California, Berkeley, 2020
U.G. Gender & Women's Studies, University of California, Berkeley, 2020

A Dissertation presented to the Graduate Faculty
of the University of Virginia in Candidacy for the Degree of
Doctor of Philosophy

Department of Mathematics

University of Virginia
May 2024

Ken Ono (Thesis Advisor)

Slava Krushkal

You Qi

Karen Kafadar

Contents

Acknowledgments

This thesis would not have been possible were it not for the people who have supported me through this journey. Foremost, I would like to thank my advisor Ken Ono for his exceptional mentorship, both personally and professionally. From our initial meeting, his belief in my potential has been a driving force that has gotten me where I am today. I am immensely thankful to Slava Krushkal, a central figure in my academic journey at the University of Virginia, who has not only been instrumental in my graduate studies but also kept my passion for topology alive. I am also very grateful to my other thesis defense committee members You Qi and Karen Kafadar for their support. I owe a significant debt of gratitude to my other collaborators, Louisa Liles, Alice Lin, Kristen Scheckelhoff, and Adit Vishnu, whose contributions have greatly enriched the results presented in this thesis and my time researching. My deepest appreciation goes to my parents Nicole and Dan, my sister Evelyn, and my partner Aydin for their unwavering love and support.

Abstract

Venturing beyond the traditional confines of number theory, this dissertation explores various intersections of the theory of modular forms with other disciplines. In particular, this body of work concerns interconnected discoveries spanning the subjects of the representation theory of the symmetric group, the arithmetic-geometric mean and its finite-field analogue, and newly defined invariants of 3-manifolds.

We first derive asymptotic formulas for two families of zeros within the character tables of the symmetric groups, focusing on those indexed by ℓ-core partitions for primes $\ell \geq 5$. These results answer a question of McKay and shed light on the properties of large ℓ-core partitions. These results originally appeared in a joint paper with Ono [35].

We also revisit the classical arithmetic-geometric mean through a modern lens by investigating a finite field analogue first defined and studied by Griffin, Ono, Saikia, and Tsai [24]. In drawing parallels with the work of Gauss on the classical arithmetic-geometric mean, we uncover the underlying structure of "jellyfish swarms" – directed graphs that organize the finite field arithmetic-geometric mean. These swarms serve as a novel framework for organizing Legendre elliptic curves over finite fields. This exploration yields new identities for Gauss' class numbers and offers insights into the interplay between jellyfish sizes and the orders of certain elements in related class groups appearing as endomorphism rings of elliptic curves. These results originally appeared in an expository paper with Ono [34].

Lastly, we extend our research to the realm of quantum modular forms, which surprisingly arise in the study of 3-manifold invariants. Inspired by the pioneering work of Lawrence and Zagier, we give infinite families of quantum modular invariants whose radial limits toward roots of unity may be thought of as a deformation of the Witten-Reshetikhin-Turaev invariants. We use a recently developed theory of Akhmechet, Johnson, and Krushkal (AJK) which extends lattice cohomology and BPS q-series of 3-manifolds [1]. As part of this work, we provide the first calculation of the AJK series invariant $\widehat{\widehat{Z}}$ for an infinite family of 3-manifolds. These results originally appeared in a joint paper with Liles [32].

Chapter 1

Introduction

In the course of my doctoral research, I took a rather unconventional approach to studying number theory. I spent most of my time thinking about problems that arise well beyond the typical boundaries of the subject. In particular, I thought deeply about the representation theory of the symmetric group, the arithmetic dynamics of two-term sequences, and invariants of 3-manifolds. These are subjects which at first glance appear to have no interrelationship. They range from being classical to contemporary questions and span markedly disparate fields of mathematics.

However, there is a unifying theme underlying the particular questions I sought to answer. In each of these cases, the behavior of the fundamental objects at the center of the problem are governed by modular forms. Studying q-series whose coefficients are arithmetically interesting is at the heart of the classical theory of modular forms, as well as many related fields. This thesis relies on a range of combinatorial and analytic tools arising from this field of study. In each case, the problem at hand is fundamentally about the long-term behavior of a sequence which can be studied using number-theoretic tools. The results specifically involve asymptotic formulas and bounds arising from the analytic behavior of Dirichlet series and the circle method, as well as the theory of complex multiplication informing the action of particular groups on sequences over finite fields. In the following subsections of this introduction, I will give a more focused overview of the results in each of these three settings.

1.1 Zeros in Character Tables of Symmetric Groups

Perhaps the most well-known example of using modular forms to understand a combinatorially defined sequence is in the study of the partition function. The results presented in this section will crucially rely on the fact that the representation theory of the symmetric group connects to modular forms through partitions, and hence tools from the study of modular forms can be used to study S_n. A *partition* λ of n is a sequence of non-increasing positive integers $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s > 0$ which sum to n. While for a general finite group the number of conjugacy classes of the group equals the number of its inequivalent complex irreducible representations, there is typically no way to construct a natural bijection between these two sets. In the case of the symmetric group, however, one can naturally parametrize both sets by the partitions of n.

The above fact gives only a first glimpse into the way that the combinatorics of partitions govern the representation theory of symmetric groups. For example, one can explicitly construct the irreducible representation of S_n corresponding to a partition λ of n by analyzing the action of Young symmetrizers on particular equivalence classes of Young tableaux of shape λ. The dimension d_λ of this representation is equal to the number of standard Young tableaux of shape λ, and can be computed using the Frame-Robinson-Thrall hook length formula $d_\lambda = \dfrac{n!}{\prod h_\lambda(i,j)}$, where the denominator computes the product of *hook lengths* of all cells (i, j) in the Young diagram of λ.

Hook lengths play a integral role in the following results, so we define them and their related notions here. The hook for the cell in position (k, j) of the Young diagram of λ is the set of cells below or to the right of that cell, including the cell itself, and so its hook length $h_\lambda(k, j)$ is given by $(\lambda_k - k) + (\lambda'_j - j) + 1$. Here λ'_j is the number of boxes in the jth column of the diagram. We say that λ is an *ℓ-core partition* if none of its hook lengths are multiples of ℓ. If $c_\ell(n)$ denotes the number of ℓ-core partitions of n, then we have (for example, see [20, 29]) the generating function

$$\sum_{n=0}^{\infty} c_\ell(n) q^n = \prod_{n=1}^{\infty} \frac{(1 - q^{\ell n})^\ell}{(1 - q^n)}.$$

The Young diagram of the partition $\lambda = (5, 4, 1)$, where each cell is labelled with its hook length, is given in Figure 1.1. By inspection, we see that λ is an ℓ-core for every prime $\ell > 7$.

7	5	4	3	1
5	3	2	1	
1				

Figure 1.1: Hook lengths for $\lambda = (5, 4, 1)$

We will be particularly interested in the characters of the irreducible representations of symmetric groups. The information of all irreducible characters of a finite group can be organized in a character table; by the preceding discussion, each entry in the character table of S_n can be indexed by a pair of partitions (λ, μ). The value of this entry $\chi_\lambda(\mu)$ is known to be an integer, and moreover counts certain statistics of Young tableaux of shape λ. The Murnaghan-Nakayama rule gives a combinatorial formula for computing such values.

Surprisingly, we have very little idea about what numbers generally populate the character tables of symmetric groups. Recent work of Peluse and Soundararajan proves that as $n \to \infty$, 100% of the entries of the character table of S_n are divisible by any given integer m. In view of this, it is natural to ask how many true zeros there are in a character table as $n \to \infty$, and for this question little is known.

Recent work of Miller and Schneinerman gives the best known numerics on the behavior of the proportion of zeros in the character tables of S_n as $n \to \infty$. The authors conduct Monte Carlo simulations to approximate the density of zeros in these character tables, providing new insights that give a clearer picture of the asymptotic behavior of zeros. Their numerical data prompted them to conjecture that the proportion of zeros in the character table of S_n approaches 0 as n approaches infinity. In conjunction with this data and their own work, Peluse and Soundararajan conjecture the following:

Conjecture 1.1. *As $n \to \infty$, $Z(n) \sim 2/\log(n)$, where $Z(n) := \#\{(\lambda, \mu) : \chi_\lambda(\mu) = 0\}$.*

The first result presented in this thesis gives a lower bound for the number of zeros in the character table. For primes $\ell \geq 5$, we obtain asymptotic formulas for

$$Z_\ell(n) := \#\left\{(\lambda, \mu) : \chi_\lambda(\mu) = 0 \text{ with } \lambda \text{ an } \ell\text{-core}\right\}. \tag{1.1.1}$$

To state the asymptotics formulas, we let $L\left(\left(\frac{\cdot}{\ell}\right), s\right)$ be the Dirichlet L-function for the Legendre symbol $\left(\frac{\cdot}{\ell}\right)$, and let

$$\alpha_\ell := \frac{(2\pi)^{\frac{\ell-1}{2}}}{\left(\frac{\ell-3}{2}\right)! \cdot \ell^{\frac{\ell}{2}} \cdot L\left(\left(\frac{\cdot}{\ell}\right), \frac{\ell-1}{2}\right)}. \tag{1.1.2}$$

By the functional equations of these Dirichlet L-functions and the theory of generalized

Bernoulli numbers, we have that $1/\alpha_\ell$ is always a positive integer. In addition, we require the integers $\delta_\ell := (\ell^2-1)/24$, and the twisted Legendre symbol divisor functions

$$\sigma_\ell(n) := \sum_{1\le d|n} \left(\frac{n/d}{\ell}\right) d^{\frac{\ell-3}{2}}. \tag{1.1.3}$$

In joint work with Ono, I obtain the following asymptotic for $Z_\ell(n)$.

Theorem 1.2 (M-Ono, [35]). *If $\ell \geq 5$ is prime, then as $n \to \infty$ we have*

$$Z_\ell(n) \sim \alpha_\ell \cdot \sigma_\ell(n+\delta_\ell) p(n) \gg_\ell n^{\frac{\ell-5}{2}} e^{\pi\sqrt{2n/3}}.$$

Remark 1.3. *Apart from a density zero subset, we have $Z_\ell(n) = 0$ for $\ell \in \{2,3\}$ (see [22]).*

As a corollary, we find that $Z(n)/p(n)$ grows faster than any power of n.

Corollary 1.4 (M-Ono, [35]). *If $d > 0$, then*

$$\lim_{n\to\infty} \frac{Z(n)}{p(n)\cdot n^d} = \infty.$$

Central to proving such asymptotic formulas is the theory of modular forms. Studying generating functions for partition statistics allows for powerful number-theoretic results to be leveraged in this setting. By incorporating the theory of abaci, which combinatorially encode partitions in a way conducive to studying ℓ-cores, we are also able to show that for n large with respect to ℓ, pairs of ℓ-core partitions always generate zeros.

Theorem 1.5 (M-Ono, [35]). *Suppose that ℓ is prime, and let $N_\ell := (\ell^6 - 2\ell^5 + 2\ell^4 - 3\ell^2 + 2\ell)/24$. If $n > N_\ell$ and $\lambda, \mu \vdash n$ are $\ell-$core partitions, then $\chi_\lambda(\mu) = 0$.*

If $Z_\ell^*(n)$ denotes the number of vanishing entries $\chi_\lambda(\mu) = 0$ indexed by ℓ-core partitions $\lambda, \mu \vdash n$, then we have the following corollary.

Corollary 1.6 (M-Ono, [35]). *For primes ℓ, the following are true.*

(1) Apart from a density zero subset, we have that $Z_\ell^*(n) = 0$ when $\ell \in \{2, 3\}$.

(2) If $\ell \geq 5$, then as $n \to \infty$ we have

$$Z_\ell^*(n) \sim \alpha_\ell^2 \cdot \sigma_\ell(n + \delta_\ell)^2 \gg_\ell n^{\ell-3}.$$

The above results initially appeared in joint work with Ono [35]. An in-depth treatment of these results and their proofs appears in Chapter 3. In Section 3.1, we give a brief overview of the representation theory of the symmetric group. In Section 3.2, we discuss known asymptotics for various partition functions which inform our results. In Section 3.3, we introduce the theory of abaci to study the behavior of ℓ-core partitions and in Section 3.4 we offer proofs of Theorems 1.2 and 1.5.

1.2 Jellyfish and the Finite-Field AGM

Modular forms also famously appear in connection with elliptic curves. The Modularity Theorem, formerly known as the Taniyama-Shimura-Weil conjecture, confirmed that for every elliptic curve E over $\mathbb{Q}$ with conductor N, there exists a modular form f of weight 2 and level N such that

$$L(E, s) = L(f, s).$$

where $L(E,s)$ and $L(f,s)$ respectively denote the associated L-series of the elliptic curve E and the modular form f. This theorem was famously proven for semistable elliptic curves by Andrew Wiles and Richard Taylor in 1995, and has since been extended to the full theorem and used in the breakthrough proof of Fermat's Last Theorem.

Preceding the modularity theorem, there is classical work of Gauss on periods of elliptic curves in which modular forms, hypergeometric functions, and elliptic functions all prominently appear. Recall that an elliptic curve in Legendre form is given by an equation

$$E_\lambda : y^2 = x(x-1)(x-\lambda), \tag{1.2.1}$$

where $\lambda \neq 0, 1$. The periods of such a curve are given by elliptic integrals of the first kind. In particular, the following integral gives the real period of the elliptic curve E_λ:

$$\Omega(E_\lambda) = \int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}.$$

The periods of an elliptic curve E correspond to the fundamental periods of a lattice Λ_E for which $E \cong \mathbb{C}/\Lambda_E$ as groups, with such an isomorphism given by the elliptic Weierstrass $\wp$ function. The j-invariant, which parameterizes elliptic curves up to isomorphism over $\mathbb{C}$, or equivalently lattices up to homothety, can be realized as a holomorphic function on $\mathbb{H}$ and in particular a weakly holomorphic modular function for $\mathrm{SL}_2(\mathbb{Z})$.

One of the most tantalizing consequences of this connection with periods of elliptic curves is captured by what at first glance appears to be child's play, namely combining the arithmetic mean and geometric mean. Recall that the classical *arithmetic-geometric mean* iteration is defined for positive real numbers a and b by the sequence of pairs

$$\mathrm{AGM}_{\mathbb{R}}(a,b) := \{(a_1,b_1),(a_2,b_2),\ldots\},$$

where $a_1 := a$, $b_1 := b$, and successive terms are given by

$$a_n := \frac{a_{n-1}+b_{n-1}}{2} \quad \text{and} \quad b_n := \sqrt{a_{n-1}b_{n-1}}.$$

It is well known that both (a_n) and (b_n) rapidly converge to the same limit (p. 2, [3]). One of the most famous results on the $\mathrm{AGM}_{\mathbb{R}}$ is due to Gauss, who showed using the theory of elliptic integrals that one can generate extraordinary approximations for π with relatively few iterations by considering the related sequence

$$p_n := \frac{a_n^2}{1-\sum_{i=1}^{n} 2^{i-2}(a_i^2-b_i^2)}.$$

For example, $p_1 = 4$, $p_2 \approx 3.18767$, and $p_3 \approx 3.14168$ are good, but $p_4 \approx 3.14159265389$ and $p_5 \approx 3.14159265358979323846$ are already astoundingly accurate.

The transformations of elliptic integrals are intrinsically linked to the analysis of limits of arithmetic sequences like $\mathrm{AGM}_{\mathbb{R}}$. For $a > b > 0$ let

$$I_{\mathbb{R}}(a,b) := \frac{1}{2a}\int_1^{\infty} \frac{dx}{\sqrt{x(x-1)(x-(1-b^2/a^2))}}. \tag{1.2.2}$$

A straightforward check shows that $I_{\mathbb{R}}(a,b) = I_{\mathbb{R}}(\frac{a+b}{2},\sqrt{ab})$, and so if μ is the limit of $\mathrm{AGM}_{\mathbb{R}}(a,b)$, then $I_{\mathbb{R}}(a,b) = I_{\mathbb{R}}(\mu,\mu)$. This relationship allowed Gauss to derive a formula for limit of the $\mathrm{AGM}_{\mathbb{R}}$ iteration and gives a natural link between the $\mathrm{AGM}_{\mathbb{R}}$ and elliptic curves, as $I_{\mathbb{R}}(a,b)$ is essentially the period of a Legendre elliptic curve ([3], Section 1.2).

Once these connections are known, it is natural to question ask whether there is a similar story if we look to finite fields. In [24], Griffin, Saikia, Tsai, and the second author define a finite-field analogue of $\mathrm{AGM}_{\mathbb{R}}$ over $\mathbb{F}_q$ when $q = p^r \equiv 3 \bmod 4$. In this setting, -1 is not a square mod q, mirroring the fact that -1 is not a square in $\mathbb{R}$. This allows us to choose square roots such that the iterated geometric means are well-defined. That is, there is always a unique choice of $b_n = \sqrt{a_{n-1}b_{n-1}}$ such that $a_n b_n$ is a square mod q when one starts with $a, b \in \mathbb{F}_q^\times$, $a \neq \pm b$, and ab a square mod q.

For example, consider $q = 7$ and $(a,b) = (4,2)$. Then

$$\mathrm{AGM}_{\mathbb{F}_7}(4,2) = \{(4,2), \overline{(3,6),(1,2),(5,3),(4,1),(6,5),(2,4)}, \dots\}$$

where the overlined pairs form a repeating orbit. The pairs $(6,3)$, $(2,1)$, $(3,5)$, $(1,4)$, and $(5,6)$ also enter this orbit after one $\mathrm{AGM}_{\mathbb{F}_q}$ iteration. In [24], the authors explore the properties of the connected components of the directed graph representing the sequences of $\mathrm{AGM}_{\mathbb{F}_q}(a,b)$ over all admissible pairs (a,b). They show that all components always consist of one cycle and one "tentacle" of length one connected to each cycle vertex, for which they coin the name *jellyfish*. For example, the following figure shows the unique connected component of the $\mathrm{AGM}_{\mathbb{F}_7}$ graph $\mathcal{J}_{\mathbb{F}_7}$.

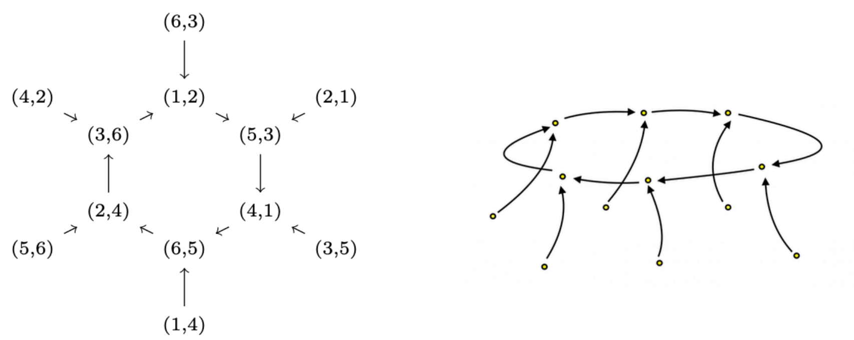

Figure 1.2: The jellyfish comprising $\mathcal{J}_{\mathbb{F}_7}$

In general, the graph $\mathcal{J}_{\mathbb{F}_q}$ consists of many such jellyfish, which together comprise a *swarm*. Swarms often contain jellyfish of varying sizes and multiplicities, as exemplified by the following figure showing the swarm $\mathcal{J}_{\mathbb{F}_{19}}$.

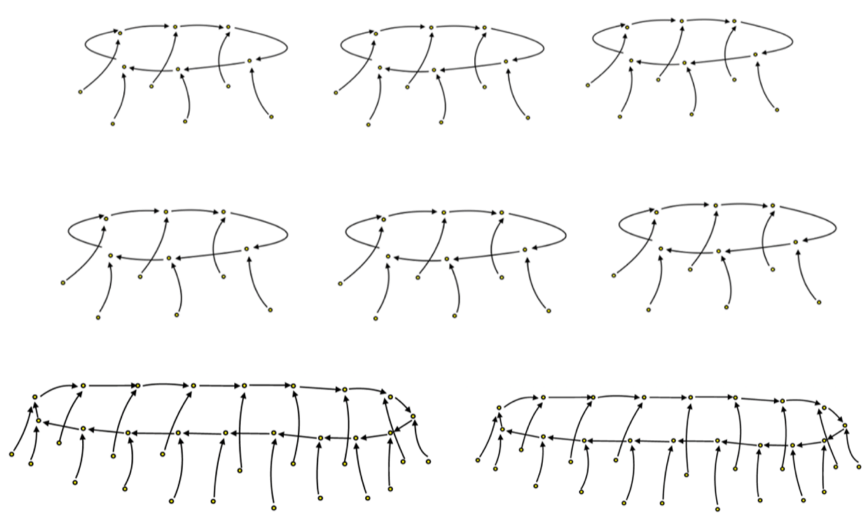

Figure 1.3: The jellyfish swarm $\mathcal{J}_{\mathbb{F}_{19}}$

Echoing the history of the $\mathrm{AGM}_{\mathbb{R}}$, it is natural to consider if elliptic curves over finite fields make contact with this newly defined analogue. First, one can associate to each vertex of these $\mathrm{AGM}_{\mathbb{F}_q}$ graphs an elliptic curve: to an admissible pair (a, b) over $\mathbb{F}_q$, define the associated Legendre elliptic curve

$$E_{b^2/a^2}\colon\ y^2 = x(x-1)(x-b^2/a^2).$$

It turns out that each iteration of the arithmetic-geometric mean, and hence each edge of the graph connecting two vertices, corresponds to an isogeny of degree 2 between these curves (see Theorem 3 (2) of [24]).

Following this observation, we can employ tools from the study of elliptic curves in order to understand the structure of $\mathrm{AGM}_{\mathbb{F}_q}$. Our approach will rely on the theory of complex multiplication. In particular, we will study the action of the class group of an imaginary quadratic order $\mathcal{O}$ on the set of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}$.

Our setup in some ways mirrors the robust theory of "isogeny volcanoes," graphs which organize isomorphism classes of elliptic curves over finite fields and their isogenies. The seminal work on such graphs is due to Kohel[1], who studied endomorphism rings of elliptic curves over finite fields by understanding the structure of ℓ-isogeny graphs $\mathcal{G}_\ell(\mathbb{F}_q)$, which are visually quite similar to our jellyfish [30]. However, there are two main differences between our isogeny graphs and the graphs $\mathcal{G}_2(\mathbb{F}_q)$ studied by Kohel and others. First, only particular 2-isogenies between the represented elliptic curves will appear in our setting. Second, different vertices can correspond to elliptic curves in the same $\bar{\mathbb{F}}_q$-isomorphism class. What's more, some jellyfish may in fact be identical after identifying nodes with their corresponding

[1]Kohel did not use this language to describe the graphs he studied. The terminology came later, in a paper by Fouquet and Morain, which applied the work of Kohel to the Schoof-Atkin-Elkies point-counting algorithm [19].

elliptic curves. These multiplicities will require attention for all of our results.

We first show that $\mathrm{AGM}_{\mathbb{F}_q}$ provides new information in the context of Gauss' theory of class numbers of imaginary quadratic fields and class numbers of positive definite binary quadratic forms. To make this connection, we count the $\bar{\mathbb{F}}_q$-isomorphism classes of elliptic curves that are represented in these graphs. To this end, the authors of [24] made use of a correspondence between isomorphism classes of elliptic curves with prescribed torsion and certain class numbers to count the number of distinct j-invariants which appear.

Recall that the Hurwitz class number $H(D)$ is a modification of the class number of binary quadratic forms of discriminant $D \leq 0$. If f is a quadratic form, then a matrix $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ is an automorphism of f if $f(\alpha x + \beta y, \gamma x + \delta y) = f(x, y)$. Then $H(D)$ weights forms of discriminant D by $2/g$, where g is the order of their automorphism group. We additionally declare $H(0) = -1/12$.

Following the approach of [24], we obtain new class number formulas that are relatives of classical results like the Hurwitz-Kronecker class number formula, which for p prime gives

$$\sum_{|t| \leq 2\sqrt{p}} H(4p - t^2) = 2p.$$

Generalizations of the above were proven by Eichler and Zagier, the latter achieved through the construction of a weight 3/2 non-holomorphic Eisenstein series whose coefficients are Hurwitz class numbers [16], [53]. More recently, Mertens [36] analyzed the holomorphic projection of the Rankin-Cohen bracket of the Harmonic Maass form $\mathcal{H}(\tau)$ with certain theta functions in order to obtain weighted class number formulas and their asymptotics as $q \to \infty$. Additionally, many more such identities were recently proven using the trace formula and the combinatorics of j-invariants of elliptic curves over finite fields [8]. Our addition to this area is the following:

Theorem 1.7. *Let $q = p^r \equiv 3 \bmod 4$ where $p > 3$. The following sums are taken over t such that $|t| \leq 2\sqrt{q}$.*

1. *If $q \equiv 3 \bmod 8$, then we have*

$$q = 3 + 4 \sum_{\substack{(t,q)=1 \\ t \equiv q+1(8)}} H\left(\frac{4q - t^2}{4}\right).$$

2. *If $q \equiv 7 \bmod 8$, then we have*

$$q = 3 + 4 \cdot \left[h(-p) + \sum_{\substack{(t,q)=1 \\ t \equiv q+1(8)}} H\left(\frac{4q - t^2}{4}\right) \right],$$

where $h(D)$ denotes the class number of discriminant D.

There are many questions one can immediately ask about $\mathrm{AGM}_{\mathbb{F}_q}$ once the "jellyfish swarm" structure is known. For example, how many jellyfish $\mathcal{J}_i$ appear in a swarm? How large do we expect jellyfish to be? These questions are not easily answered. To start, the number of jellyfish varies greatly across prime powers q. For example, Table 1.1 gives numerics for $d(q)$, the number of jellyfish in $\mathcal{J}_{\mathbb{F}_q}$.

q	7	11	19	23	27	31	43	47	$\cdots$	161047	161051	161059	161071
$d(q)$	1	3	8	5	39	10	7	4	$\cdots$	6499	25558635	4902	33744

Table 1.1: Selected values of $d(q)$ for prime powers q

These questions are complicated by the fact that the sizes of jellyfish within a single swarm can vary widely. For example, for $q = 161051 = 11^5$, the swarm $\mathcal{J}_{\mathbb{F}_q}$, one has tiny jellyfish of size 10 alongside those of massive size 7500.

Here we show that these sizes are related to the algebraic properties of the endomorphism rings $\mathrm{End}(E)$ of elliptic curves and their class groups (see Section 4.2 for background and definitions). Using Theorem 1.7 and the theory of complex multiplication, we are able to show the following:

Theorem 1.8. *Let $q = p^r \equiv 3 \bmod 4$ where $p > 3$. Suppose (a, b) satisfies the conditions to appear in the $AGM_{\mathbb{F}_q}$ graph on the jellyfish $\mathcal{J}$, and let $\lambda := b^2/a^2$. Let $\#\mathcal{J}$ denote the number of vertices in $\mathcal{J}$. If $\mathcal{O} := \mathrm{End}(E_\lambda)$ and $h_2(\mathcal{O})$ denotes the order of $[\mathfrak{p}_2]$ in $cl(\mathcal{O})$, where $\mathfrak{p}_2$ is a prime above (2) in $\mathcal{O}$, then we have*

$$2 \cdot h_2(\mathcal{O}) \;\Big|\; \#\mathcal{J}.$$

Additionally, if $m(\mathcal{J})$ denotes the multiplicity with which a jellyfish appears, then

$$m(\mathcal{J}) \cdot \#\mathcal{J} = 2(q-1) \cdot h_2(\mathcal{O}).$$

Example 1.9. We illustrate the theorem with $q = 271$.

$\mathcal{J}$	t	$h(\mathcal{O})$	$h_2(\mathcal{O})$	$\#\mathcal{J}$	$m(\mathcal{J})$
$\mathcal{J}_1$	-32	2	2	540	2
$\mathcal{J}_2$	-24	5	5	900	3
$\mathcal{J}_3$	-16	6	6	1620	2
$\mathcal{J}_4$	-16	3	3	810	2
$\mathcal{J}_5$	-8	12	6	1620	2
$\mathcal{J}_6$	-8	12	6	1620	2
$\mathcal{J}_7$	0	11	11	2970	2
$\mathcal{J}_8$	8	12	6	1620	2
$\mathcal{J}_9$	8	12	6	1620	2
$\mathcal{J}_{10}$	16	6	6	1620	2
$\mathcal{J}_{11}$	16	3	3	810	2
$\mathcal{J}_{12}$	24	5	5	2700	1
$\mathcal{J}_{13}$	32	2	2	108	10

Table 1.2: Jellyfish swarm statistics for $\mathcal{J}_{\mathbb{F}_{271}}$

Proofs of the above appear in an exposition on jellyfish by Ono and myself [34]. These results and their proofs will be discussed in greater detail in Chapter 4. In Section 4.1, we recall the basic theory of class groups and class numbers for orders in imaginary quadratic fields. In Section 4.2, we discusss the theory of elliptic curves, with a particular focus on elliptic curves over finite fields and the theory of complex multiplication. In Section 4.3, the relevant prior work on jellyfish is recalled and in Section 4.4 we offer proofs of Theorems 1.7 and 1.8.

1.3 Quantum Modularity of 3-Manifold Invariants

Just as modular forms and special functions play an important role in the previous works on the representation theory of the symmetric group and the AGM over finite fields, research in the last few decades has surprisingly shown that modular forms have deep connections to low-dimensional topology. In 1999, Lawrence and Zagier established a connection between modular forms and invariants of 3-manifolds arising from quantum topology and physics [31]. The Witten-Reshetihkin-Turaev (WRT) invariants were first conceptualized by Witten in terms of a path integral for $SU(2)$ Chern-Simons theory and were made mathematically precise by Reshetikhin and Turaev using the representation theory of quantum groups [52, 44]. These ultimately give a family of 3-manifold invariants indexed by roots of unity.

Lawrence and Zagier gave an instance of unification of these invariants by producing a holomorphic function $A(q)$ on the unit disk whose limiting values at roots of unity recover the invariants of the Poincaré homology sphere. Interestingly, the function $A(q)$ is in some sense an integral of a theta function; its obstruction to modularity on the unit circle is given by a factor introduced by integrating. It is one of the first key examples of a *quantum modular form*, a term coined by Zagier in 2010 with this series in mind [55]. Zagier's seminal work has inspired an extensive and ongoing body of research on quantum modular forms; see Chapter 21 of [4] and the references listed therein.

Recent work of Gukov, Pei, Putrov, and Vafa (GPPV) provides a construction of analogous series $\widehat{Z}(q)$ for a large class of 3-manifolds equipped with a spin^c structure and motivates a conjecture that such series exist for all 3-manifolds [26, 27]. These unified invariants were further extended in [25, 10] and the quantum modularity of these series for certain classes of manifolds were established in [5, 6].

Recently, Akhmechet, Johnson, and Krushkal defined a two-variable series invariant $\widehat{\widehat{Z}}_Y(t,q)$ based on lattice cohomology a theory developed by Némethi in [38] which was inspired by the study of normal surface singularities. This AJK series invariant gives a natural extension of the GPPV invariant $\widehat{Z}(q)$.

In joint work with Liles, I show that this two-variable series gives rise to infinitely many quantum modular forms whose values at roots of unity can be considered deformations of the WRT invariants. These results realize the work of Lawrence and Zagier as a special case. We first calculate $\widehat{\widehat{Z}}_\Sigma(t,q)$ when Σ is a Brieskorn homology sphere, generating the first known calculation of this invariant for an infinite family of manifolds. In particular, we find explicit formulas for the coefficients $\varphi(n;t)$ of the q-series $\widehat{\widehat{Z}}$, which are Laurent polynomials in t. The result is, for each Brieskorn sphere Σ, a q-series of the form

$$\widehat{\widehat{Z}}_\Sigma(t,q) = q^\Delta\Big(C - \sum_{n\geq 0}\varphi(n;t)q^{\frac{n^2}{4p}}\Big), \tag{1.3.1}$$

where $\Delta \in \mathbb{Q}$, $p \in \mathbb{Z}$, and C is zero unless Σ is the Poincaré homology sphere, in which case it equals $q^{1/120}(t+t^{-1})$; see Section 5.2 for full definitions.

A priori, $\widehat{\widehat{Z}}_\Sigma(t,q)$ is convergent as a two-variable series for $t \in \mathbb{C}$ and $|q| < 1$. By leveraging the arithmetic properties of the coefficients $\varphi(n;t)$ when t is a root of unity, we are able to show the following:

Theorem 1.10 (Liles-M, [32]). *Let ζ be a jth root of unity, ξ a Kth root of unity, and Σ a*

Brieskorn sphere. Define $\widehat{\widehat{Z}}_\Sigma(\zeta,\xi) := \lim_{t\to 0^+} \widehat{\widehat{Z}}_\Sigma(\zeta,\xi e^{-t})$*. This limit exists and we have*

$$\widehat{\widehat{Z}}_\Sigma(\zeta,\xi) = \xi^{\Delta}\left(D + \sum_{n=1}^{2pjK}\left(\frac{n}{2pjK} - \frac{1}{2}\right)\varphi(n;\zeta)\xi^{\frac{n^2}{4p}}\right),$$

where $D = \xi^{1/120} Re(\zeta)$ *when* Σ *is the Poincaré homology sphere and is zero otherwise.*

The topological interpretation of this family of "t-deformed" WRT invariants is yet unknown. However, using the above results we prove that for t a fixed root of unity, $\widehat{\widehat{Z}}_\Sigma(t,q)$ is, up to normalization, a quantum modular form:

Theorem 1.11 (Liles-M, [32])**.** *Let* $q = e^{2\pi i\tau}$*. If* ζ *is a* j*th root of unity and* Σ *is a Brieskorn sphere, then*

$$\widehat{\widehat{Z}}_\Sigma(\zeta,q) = q^{\Delta}\left(C - A_\zeta(\tau)\right),$$

where $A_\zeta(\tau)$ *is a quantum modular form of weight* $1/2$ *with respect to* $\Gamma(4pj^2)$*.*

Remark 1.12. *The definition of a quantum modular form is deferred until Section 2.3. We further have that* $A_\zeta(\tau)$ *is a "strong" quantum modular form in the sense of [55].*

The classical theory of theta functions involves forms of weight 1/2 and 3/2 that are related through differentiation of the Jacobi theta function. Because of the existence of the second variable, one can differentiate $\widehat{\widehat{Z}}_\Sigma(t,q)$, summand by summand, with respect to t and consider the new invariant that arises. This series, under specialization, also enjoys quantum modularity properties; the result is a sum of quantum modular forms of mixed weight:

Theorem 1.13 (Liles-M, [32])**.** *Define* $\widehat{\widehat{Z}}'_\Sigma(t,q) := t\frac{\partial}{\partial t}\widehat{\widehat{Z}}_\Sigma(t,q)$*. Let* ζ *be a* j*th root of unity. Then*

$$\widehat{\widehat{Z}}'_\Sigma(\zeta,q) = q^{\Delta}\left(C' - A'_\zeta(\tau)\right),$$

where $A'_\zeta(\tau)$ *is a sum of quantum modular forms of weight* $1/2$ *and* $3/2$ *for* $\Gamma(4pj^2)$*, where* $C' = q^{1/120}(t - t^{-1})$ *when* Σ *is the Poincaré homology sphere and is zero otherwise.*

These results originally appeared in joint work with Liles. The proofs of these results will be discussed in greater detail in Chapter 5. Section 5.1 will discuss the construction of the AJK invariant and the class of manifolds for which it is defined. In Section 5.2, we analyze the properties of this series for a nice class of manifolds and offer the first known explicit computation of the coefficients. In Section 5.3, we prove Theorems 1.10, 1.11, and 1.13.

Chapter 2

Modular Forms

This chapter will develop the necessary notation and results in the theory of modular forms which are needed for the remainder of this dissertation. For more details on the theory of modular forms, see [4, 41]. We first recall the classical theory of integer weight modular forms and then turn to modular forms of half-integer weight. The last section will discuss the modern theory of quantum modular forms, with a brief aside on the Mellin transform, which will be needed to prove the main results on quantum modular forms which are used.

2.1 Integer Weight Modular Forms

Given $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, γ acts on $\tau \in \mathbb{C} \cup \{\infty\}$ by the linear fractional transformation

$$\gamma\tau := \frac{a\tau + b}{c\tau + d}.$$

We have that $\Im(\gamma\tau) = \dfrac{\Im(\tau)}{|c\tau + d|^2}$, and so if $\tau \in \mathbb{H} := \{\tau \in \mathbb{C} \colon \Im(\tau) > 0\}$, then $\gamma\tau \in \mathbb{H}$, i.e. the action of $\mathrm{SL}_2(\mathbb{Z})$ restricts to $\mathbb{H}$. A fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ is the set

$$\mathcal{F} := \left\{\tau \in \mathbb{H} : -\frac{1}{2} \leq \Re(\tau) < \frac{1}{2}, |\tau| > 1\right\} \cup \left\{\tau \in \mathbb{H} : -\frac{1}{2} \leq \Re(\tau) \leq 0, |\tau| = 1\right\}.$$

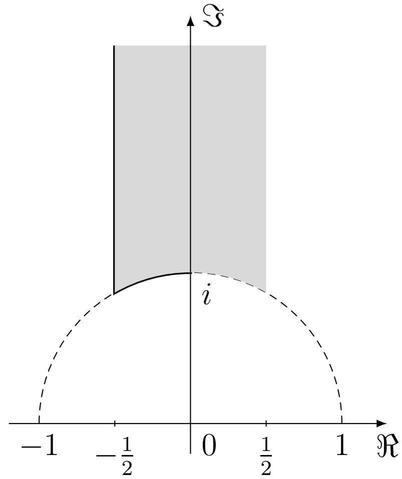

Figure 2.1: The fundamental domain $\mathcal{F}$

We are often interested in the action of particular subgroups Γ of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. The *principal congruence subgroup of level* N is defined as the kernel of the homomorphism $\pi_N \colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ given by reduction modulo N. We write

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

Definition 2.1. *A congruence subgroup of $SL_2(\mathbb{Z})$ is a subgroup Γ such that Γ contains $\Gamma(N)$ for some N. The level of Γ is the smallest such N.*

Note that the above definition implies congruence subgroups have finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Two families of congruence subgroups we are interested are

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \ c \equiv 0 \pmod{N} \right\};$$
$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \ a \equiv d \equiv 1 \pmod{N}, \ c \equiv 0 \pmod{N} \right\}.$$

We note the containments $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$, and so $\Gamma_1(N)$ and $\Gamma_0(N)$ are congruence subgroups of level N. The equivalence classes of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ under the action of a congruence subgroup Γ are called the *cusps* of Γ. Note that there is only one cusp when $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ for which we will choose the representative ∞.

Suppose $f\colon \mathbb{H} \to \mathbb{C}$ is holomorphic and is invariant under $\tau \mapsto \tau + 1$. Then f has a Fourier series expansion at infinity given by

$$\sum_{n=-\infty}^{\infty} a_n q^n, \qquad (q = e^{2\pi i \tau}).$$

We say that f is *meromorphic at infinity* if there exists an $n_0 >> -\infty$ such that $n < n_0$ implies $a_n = 0$ and *holomorphic at infinity* if $n_0 \geq 0$.

In order to simplify exposition, we introduce the some notation. For functions $f\colon \mathbb{H} \to \mathbb{C}$, the Petersson slash operator of weight $k \in \mathbb{Z}$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ is defined as $f|_k\gamma(\tau) := (c\tau + d)^{-k} f(\gamma\tau)$. Note that $f|_k(\gamma_1\gamma_2) = (f|_k\gamma_1)|_k\gamma_2$.

Observe that if $f|_k = f$ for all $\gamma \in \Gamma$ where Γ is a congruence subgroup and if $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then $f|_k\alpha =: f^{[\alpha]_k}$ satisfies $f^{[\alpha]_k}|_k\gamma = f^{[\alpha]_k}$ for all $\gamma \in \alpha^{-1}\Gamma\alpha$. Since $\alpha^{-1}\Gamma\alpha$ is a finite index subgroup, it contains an element of the form $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ for some $h \geq 1$. Then $f^{[\alpha]_k}(\tau+h) = f^{[\alpha]_k}(\tau)$

and so $f^{[\alpha]_k}$ has a Fourier expansion at infinity of the form

$$\sum_{n=-\infty}^{\infty} a_n(p/q)q^{n/h}$$

in $q^{1/h} = e^{2\pi i\tau/h}$. We call the minimal such h the *width* of the cusp $\alpha(\infty) = p/q$ relative to Γ. We say that f is meromorphic (resp. holomorphic) at p/q if $f^{[\alpha]_k}$ is meromorphic (resp. holomorphic) at infinity. We can now define modular forms.

Definition 2.2. *A weakly holomorphic (resp. holomorphic) modular form of weight k for a subgroup $\Gamma \subseteq SL_2(\mathbb{Z})$ is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ such that for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, we have*

$$f(\tau) - f|_k\gamma(\tau) \equiv 0$$

and $f|_k\gamma$ is meromorphic (resp. holomorphic) at infinity.

For convenience, we will refer to holomorphic modular forms simply as modular forms. We also explicitly define a particular kind of modular form which we will often see.

Definition 2.3. *A modular form of weight k for $\Gamma \subseteq SL_2(\mathbb{Z})$ is called a cusp form if for all $\gamma \in \Gamma$, $f|_k\gamma$ vanishes at infinity. Equivalently, $a_0(p/q) = 0$ for all cusps p/q of Γ.*

Remark 2.4. *If $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \Gamma$ and k is odd, then any modular form of weight k for Γ is necessarily trivial because the modular transformation condition forces $f(\tau) = (-1)^k f(\tau)$.*

Due to its invariance under $\tau \mapsto \tau + 1$, a modular form f of weight k has a Fourier expansion at infinity given by $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$ where $q = e^{2\pi i\tau}$ and $a_n \in \mathbb{C}$. For cusp forms, we necessarily have $a_0 = 0$.

To give some key concrete examples of modular forms, we first define some auxilliary functions. If k is a positive integer, define the kth power divisor function by

$$\sigma_k(n) := \sum_{1 \geq d | n} d^k.$$

We also define the Bernoulli numbers B_k by their generating function

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}, \qquad (t < 2\pi).$$

Definition 2.5. *For $k \geq 2$ an even integer, the weight k Eisenstein series $E_k(\tau)$ is given by*

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

Proposition 2.6. *For $k \geq 4$ an even integer, $E_k(\tau)$ is a holomorphic modular form of weight k for $SL_2(\mathbb{Z})$.*

We will also need to consider modular forms with Nebentypus, for which we need the following definitions. For a positive integer N, a Dirichlet character modulo N is a function $\chi \colon \mathbb{Z} \to \mathbb{C}$ satisfying $\chi(n + N) = \chi(n)$ for all $n \in \mathbb{Z}$, $\chi(n) \neq 0$ if and only if $(n, N) = 1$, and $\chi(mn) = \chi(m)\chi(n)$ for all $m, n \in \mathbb{Z}$. Such functions are in one-to-one correspondence with homomorphisms from $(\mathbb{Z}/N\mathbb{Z})^\times$ to $\mathbb{C}^\times$. A Dirichlet character χ modulo N is *primitive* if it does not arise as the induction of a character modulo d for any $d < N$. From the definition, it is clear that $\chi(-1) = \pm 1$. We say that χ is even when $\chi(-1) = 1$ and that χ is odd when

$\chi(-1) = -1$. Every Dirichlet character χ with conductor r can be written as a product

$$\chi = \prod_{p|r} \chi_p,$$

where χ_p is a character with conductor $p^e \mid\mid r$. We say that χ is *totally even* if $\chi_p(-1) = 1$ for every $p \mid r$. Such Dirichlet characters will be important in the following subsection.

If χ is a Dirichlet character modulo N and f is a modular form of weight k with respect to $\Gamma_1(N)$, we say that f has Nebentypus character χ if $\chi(d)f(\tau) - f|_k\gamma(\tau) = 0$ for all $\gamma \in \Gamma_0(N)$.

Since modular forms of a given level and weight behave nicely with respect to addition and scaling, it is sensible to consider vector spaces of modular forms. Let us establish notation for and fundamental properties of these spaces. We will denote the $\mathbb{C}$-vector space of modular forms of weight k for $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ by $M_k(\Gamma)$ and the space of such cusp forms by $S_k(\Gamma)$. A well-known fact is that when $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, each such space of modular forms is generated by monomials in E_4 and E_6. Indeed,

$$\mathbb{C}[E_4, E_6] \cong \bigoplus_{k \geq 0} M_k(\mathrm{SL}_2(\mathbb{Z}))$$

as $\mathbb{C}$-algebras. For the later sections, we will need some results on the dimensions of spaces of modular forms of particular weight with level structure.

Proposition 2.7. *For each $N \geq 1$, the space $M_k(\Gamma_1(N))$ is finite-dimensional.*

The space of modular forms with Nebentypus character χ of modulus N for $\Gamma_0(N)$ will likewise be denoted $M_k(\Gamma_0(N), \chi)$. Complementary to our original definition, we have the following decomposition of spaces

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(\Gamma_0(N), \chi),$$

where the sum runs over all even Dirichlet characters of modulus N. This decomposition descends to spaces of cusp forms.

We now turn our attention to a collection of linear transformations that naturally act on the spaces of modular forms. For simplicity, we restrict our definition to primes p. Given explicitly in terms of Fourier coefficients, the pth Hecke operator T_p acts on $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$ by

$$f(\tau) \mid T_p := \sum_{n=0}^{\infty} \left(a_{pn} + \chi(p)p^{k-1}a_{n/p}\right) q^n.$$

If $f \in M_k(\Gamma)(N), \chi)$ then so is $f \mid T_p$. Note that if f is a cusp form, so is $f \mid T_p$.

Definition 2.8. *A modular form f is called a Hecke eigenform if for each prime p, there exists a scalar λ_p such that*

$$f \mid T_p = \lambda_p f.$$

Equivalently, this means $a_p = \lambda_p$ for all n when f is normalized such that $a_1 = 1$.

One can make new modular forms out of old. Note that if $f \in S_k(\Gamma_0(N), \chi)$ and $M \mid N$, then both $f(\tau)$ and $f(\frac{N}{M}\tau)$ belong to $S_k(\Gamma_0(M), \chi')$ where

$$\chi'(n) := \begin{cases} \chi(n) & \text{if } (n, M) = 1; \\ 0 & \text{otherwise,} \end{cases}$$

is the extension of χ modulo M. If a modular form obtained in such a way from a lower level, it is called an *oldform*, and we denote the space of such forms by $S_k^{old}(\Gamma_0(N), \chi)$. It turns out that the orthogonal complement (with respect to the Petersson inner product) of this space, denoted $S_k^{new}(\Gamma_0(N), \chi)$, has a basis of Hecke eigenforms; elements of $S_k^{new}(\Gamma_0(N), \chi)$ which are Hecke eigenforms are called *newforms*.

Let $f(\tau) = \sum_{n=1}^{\infty} a_n q^n$ be a newform of weight k and Nebentypus character χ for $\Gamma_0(N)$. Deligne's proof of the Weil Conjectures implies a bound on the coefficients of newforms.

Theorem 2.9 (Deligne)**.** *If $p \nmid N$, we have $|a_p| \leq 2p^{(k-1)/2}$.*

We also recall a result due to Miyake which offers a better bound in the case where N is a multiple of p.

Theorem 2.10 ([37], Theorem 4.6.17)**.** *If $p \mid N$, we have $|a_p| \leq p^{(k-1)/2}$.*

Together, these allow for one to bound $|a_n|$ for general n. In particular, we have:

Lemma 2.11 ([22], Lemma 2)**.** *If $f(\tau) = q + \sum_{n=2}^{\infty} a_n q^n$ is a normalized newform of weight k, level N, and Nebentypus character χ, then*

$$|a(n)| \leq n^{\frac{k-1}{2}}(1+\sqrt{2})^{\Omega(n)},$$

where $\Omega(n)$ is the total number of prime divisors of n, counted with multiplicity.

2.2 Half-Integer Weight Modular Forms

While half-integral weight modular forms have been studied in some capacity since the 18th century, it was Shimura's 1973 *Annals of Mathematics* paper that connected their arithmetic to that of integral weight modular forms and hence showed their relationship to and importance in the classical theory [47]. Here we recall the standard setup and results, particularly in the cases of weight 1/2 and 3/2 which are best understood.

Throughout, we let $\sqrt{z}$ be the branch of the square root with argument in $(-\pi/2, \pi/2]$. To state the appropriate transformation law for half-integral weight modular forms, we need the following definitions. For odd d, define

$$\varepsilon_d := \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4; \\ i & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

For positive odd d, let $\left(\frac{\cdot}{\cdot}\right)$ denote the Jacobi symbol, and for negative d, define

$$\left(\frac{c}{d}\right) = \begin{cases} \left(\frac{c}{|d|}\right) & \text{if } d < 0 \text{ and } c > 0; \\ \left(-\frac{c}{|d|}\right) & \text{if } d < 0 \text{ and } c < 0. \end{cases}$$

For functions $f\colon \mathbb{H} \to \mathbb{C}$, the Petersson slash operator of weight $k \in \frac{1}{2} + \mathbb{Z}$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ is defined by $f|_k\gamma(\tau) := \varepsilon_d^{2k} \left(\frac{c}{d}\right)^{2k} (c\tau + d)^{-k} f(\gamma\tau)$.

Definition 2.12. *A holomorphic function $f\colon \mathbb{H} \to \mathbb{C}$ is called a holomorphic half-integral weight modular form of weight $k \in \frac{1}{2} + \mathbb{Z}$ if for all $\gamma \in \Gamma_0(N)$, we have $f(\tau) - f|_k\gamma(\tau) \equiv 0$ and f is holomorphic at the cusps of $\Gamma_0(N)$.*

Example 2.13. The classical theta function

$$\theta_0(\tau) := \sum_{n=-\infty}^{\infty} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \dots$$

is a modular form of weight 1/2 for $\Gamma_0(4)$.

This example gives rise to families of modular forms of weight 1/2 and weight 3/2 by twisting by Dirichlet characters. In particular, we have the following:

Theorem 2.14. *Let φ be a Dirichlet character modulo N.*

1. *If φ is even, then*

$$\theta(\varphi, 0; \tau) := \sum_{n=-\infty}^{\infty} \varphi(n) q^{n^2} \in M_{1/2}(\Gamma_0(4N^2), \varphi).$$

2. *If φ is odd, then*

$$\theta(\varphi, 1; \tau) := \sum_{n=1}^{\infty} \varphi(n) n q^{n^2} \in S_{3/2}(\Gamma_0(4N^2), \varphi\chi_{-4}),$$

where χ_{-4} is the unique nontrivial Dirichlet character modulo 4.

Using Shimura's definition of the Hecke operators for half-integral weight modular forms, Serre and Stark proved that the collection of theta functions $\theta(\varphi, 0; \tau)$ form a basis for weight 1/2 modular forms.

Theorem 2.15 ([46]). *Suppose χ is an even Dirichlet character modulo $4N$. A basis for the space $M_{1/2}(\Gamma_0(4N), \chi)$ is given by the set of theta functions $\theta(\varphi, 0; t\tau)$ such that:*

1. *φ is an even primitive Dirichlet character;*
2. *$r^2 t \mid N$, where r is the conductor of φ;*
3. *$\chi(n) = \varphi(n) \left(\frac{t}{n}\right)$ for every n coprime to $4N$.*

Moreover, the set of such theta functions where φ is not totally even forms a basis for the space of cusp forms $S_{1/2}(\Gamma_0(N), \chi)$.

Lastly, we note that the Shimura correspondence gives a deep link between modular forms of half-integral weight and modular forms of integral weight. Specifically, it maps cusp forms of weight $k + \frac{1}{2}$ on $\Gamma_0(4N)$ to cusp forms of weight $2k$ on $\Gamma_0(N)$ in a way that respects the Hecke operators and relates the Fourier coefficients of these forms through certain L-series.

2.3 Quantum Modular Forms

Quantum modular forms, introduced by Don Zagier in 2010, represent an intriguing and relatively recent development in the study of modular forms [55]. Quantum modular forms extend the traditional notion of modular forms by relaxing both their transformation properties and their analytic conditions. Unlike classical modular forms, which are defined on the upper half-plane and transform predictably with respect to the action of $\mathrm{SL}_2(\mathbb{Z})$, quantum modular forms are defined on the rationals (or subsets thereof) and may only satisfy their transformation properties in a weaker sense, often exhibiting surprising and intricate behavior. Zagier's introduction of the concept was motivated by the discovery of certain functions arising in quantum topology, particularly in the study of knot invariants, that did not fit within the classical framework but still exhibited interesting modular-like transformation properties. To make this precise, we offer the following definition.

Fix a congruence subgroup Γ of level N such that $4 \mid N$, and suppose $\mathcal{Q} = \mathbb{Q} \backslash S$ where S is discrete and $\mathcal{Q}$ is closed under the action of Γ. We define a *quantum modular form* of weight $k \in \frac{1}{2}\mathbb{Z}$ with multiplier χ for Γ to be a function $f \colon \mathcal{Q} \to \mathbb{C}$ such that for all

$\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, the function $h_\gamma \colon \mathcal{Q}\backslash\{\gamma^{-1}(i\infty)\}) \to \mathbb{C}$,

$$h_\gamma(x) := f(x) - \overline{\chi}(d) f|_k\gamma(x) \tag{2.3.1}$$

extends to some "nice" function on $\mathbb{R}$, where the slash operator is defined as in the previous sections depending on whether k is an integer or half-integer. The set $\mathcal{Q}$ is called the quantum set of f, and is often but not always $\mathbb{Q}$ itself.

Remark 2.16. *This definition is intentionally vague, as it was built to fit the particular examples naturally arising from disparate areas of study. While this definition is still under construction, there have been a variety of alterations made to the original definition that are still considered to fall under the "quantum modular" umbrella.*

Example 2.17. In a lecture on the analytic continuation of Feynman integrals, Kontsevich introduced the "strange" function $F(q) = \sum_{n=0}^{\infty}(q;q)_n$. In [54], Zagier proved that

$$\sum_{n=0}^{\infty}(q;q)_n \text{``}=\text{''} -\frac{1}{2}\sum_{n=0}^{\infty} n\chi_{12}(n) q^{\frac{n^2-1}{24}},$$

an equality that requires explanation. The function $F(q)$ does not converge on any open subset of $\mathbb{C}$ but becomes a finite sum for q a root of unity. In contrast, the right series converges for $|q| < 1$. This strange equality should be read as stating that the radial limit as q approaches ζ in the right side equals the evaluation of the left side at ζ. In [55], Zagier showed that $\varphi(x) = q^{1/24}F(q)$, where $q = e^{2\pi i x}$, is a quantum modular form using the functional equation apparent from the definition of $F(q)$ and analyzing the asymptotic expansion of $\varphi(1/n)$. The connection of $F(q)$ to generating functions of particular unimodal sequences was later studied by Bryson, Pitman, Ono, and Rhoades [9].

While unnecessary for the present works in this thesis, we briefly discuss the relationship of quantum modular forms to mock modular forms. In Srinivasa Ramanujan's last letter to G. H. Hardy in 1920, he identified functions with modular-like properties that lacked complete modular transformation behavior. These series garnered great interest over the last century and their precise modular properties were eventually determined by Sander Zwegers, who realized mock modular forms as holomorphic parts of harmonic Maass forms. This development provided a rigorous foundation for mock modular forms, elucidating their relationship with classical modular forms and automorphic forms more generally.

Much of Ramanujan's work on the mock theta functions concerned their asymptotic properties as q approached roots of unity. He claimed (and Griffin, Ono, and Rolen [23] proved) that the exponential singularities of these series could not be "cut out" by a weakly holomorphic modular form. However, he did write for the mock theta function $f(q)$ that for $2k$th roots of unity, we have

$$f(q) - (-1)^k(1-q)(1-q^3)(1-q^5)\cdots(1-2q+2q^4-\cdots) = O(1).$$

Folsom, Ono, and Rhoades [18] have recast his findings: the "$O(1)$" are actually numbers that are special values of quantum modular forms. Indeed, Choie, Lim and Rhoades [11] proved that there is a linear injective map from the space of mock modular forms to quantum modular forms that captures a broader framework in which identities of this form hold.

2.3.1 Mellin Transform

Here we include a brief discussion of the Mellin transform, the fundamental tool which will allow us to study the asymptotic behavior of the series in question. Let $\varphi\colon \mathbb{R}_{>0} \to \mathbb{C}$ be continuous. We are interested in asymptotic expansions of $\varphi(t)$ as $t \to 0^+$. In particular, we will be interested in the existence of expansions of the form

$$\varphi(t) \sim \sum_{n=0}^{\infty} a_n t^n, \qquad (t \to 0^+)$$

which means that the difference $\varphi(t) - \sum_{n=0}^{N-1} a_n t^n = O(t^N)$ as $t \to 0^+$. Note that $\sum_{n=0}^{\infty} a_n t^n$ need not be convergent for any positive t for this definition to be sensible, but we will often consider situation where there is a positive radius of convergence.

In our case, we will gain information about such asymptotic expansions by considering the *Mellin transform* of $\varphi(t)$, which is given by

$$\tilde{\varphi}(s) := \int_0^{\infty} \varphi(t) t^{s-1}\, dt.$$

The convergence of such an indefinite integral depends on the properties of $\varphi(t)$ as t approaches zero and infinity. Typically, $\tilde{\varphi}(s)$ will be an analytic function of within some strip $a < \Re(s) < b$. If for example we assume φ is of rapid decay at infinity but grows like t^{-a} for some $a \in \mathbb{R}$ as $t \to 0^+$, this implies convergence for s such that $\Re(s) > a$. The analytic continuation of such functions informs the asymptotic properties of φ as t approaches 0.

In particular, suppose that $\varphi(t) \sim \sum_{n=0}^{\infty} a_n t^n$ as $t \to 0^+$ and $\varphi(t)$ is of rapid decay at infinity. Then for any s such that $\Re(s) > 0$, $\int_0^{\infty} \varphi(t) t^{s-1}\, dt$ converges and can be broken up to analyze the effect of the behavior of φ as $t \to 0^+$ and $t \to \infty$. We have

$$\begin{aligned}\tilde{\varphi}(s) &= \int_0^1 \varphi(t)t^{s-1}\,dt + \int_1^\infty \varphi(t)t^{s-1}\,dt \\ &= \int_0^1 \Big(\varphi(t) - \sum_{n=0}^{N} a_n t^n\Big)t^{s-1}\,dt + \sum_{n=0}^{N}\frac{a_n}{n+s} + \int_1^\infty \varphi(t)t^{s-1}\,dt\end{aligned}$$

The first integral converges for $\Re(s) > -N$ and the second converges for all $s \in \mathbb{C}$, so $\tilde{\varphi}(s)$ has a meromorphic continuation to $\Re(s) > -N$ with simple poles at nonpositive integers $-N+1 \le -n \le 0$ each with residue a_n.

Example 2.18. Let $\varphi(t) = e^{-t}$. This has as an asymptotic expansion $\sum_{n=0}^{\infty} \frac{(-t)^n}{n!}$ as $t \to 0^+$. By definition, $\tilde{\varphi}(s) = \Gamma(s)$ Euler's Gamma function, which has a meromorphic continuation to all s with simple pole of residue $(-1)^n/n!$ at each $s = -n$. It is also useful to note that if $\varphi(t) = e^{\lambda t}$, we have $\tilde{\varphi}(s) = \Gamma(s)\lambda^{-s}$.

Example 2.19. Let $\varphi(t) = 1/(e^t - 1)$. This gives a shifted generating function for the Bernoulli numbers

$$\frac{1}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}, \qquad (t < 2\pi).$$

One can also expand as geometric series $1/(e^t - 1) = \sum_{k=1}^{\infty} e^{-kt}$ for $t > 0$ since $e^t > 1$. This allows us to use the previous example to see that $\tilde{\varphi}(s) = \Gamma(s)\zeta(s)$, where

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is the Riemann zeta function. Using this, one can deduce the well-known fact that $\zeta(s)$ has a meromorphic continuation to all of $\mathbb{C}$ with a simple pole at $s = 1$ with residue 1. Moreover, we have

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}$$

for all $0 \leq n$. In a natural extension of the above, one computes the values of the Hurwitz zeta functions

$$\zeta(s,a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s}$$

at negative integers as

$$\zeta(-n,a) = -\frac{B_{n+1}(a)}{n+1},$$

Where $B_n(x)$ is the nth Bernoulli polynomial evaluated at x, which have the generating function

$$\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}.$$

Example 2.20. In an intimately related example, we consider the theta function

$$\theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}, \qquad (t > 0).$$

Using Example 2.18 one can show that $\tilde{\theta}(s) = 2\xi(2s)$ where $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$. The Poisson summation formula applied to θ yields the functional equation

$$\theta(t) = \frac{1}{\sqrt{t}}\, \theta\left(\frac{1}{t}\right).$$

The fact that the exponential terms for $n \neq 0$ decay rapidly coupled with this functional equation give that $\theta(t) \sim 1$ as $t \to \infty$ and $\theta(t) \sim t^{-1/2}$ as $t \to 0^+$. Then $\tilde{\theta}(s)$ has a meromorphic continuation with simple poles with residues 1 and -1 at $s = 1/2$ and $s = 0$ respectively.

This approach, while giving less information about the poles and zeros of the Riemann zeta function than the previous example, allows us to derive the famous functional equation

$$\xi(s) = \xi(1-s)$$

by leveraging the functional equation for θ and the properties of the Mellin transform.

As we will later be interested in computing asymptotic expansions for particular functions, we need to investigate the inverse problem where we know something about the analytic behavior of the associated Dirichlet series. One such way to approach this problem is to consider the inverse Mellin transform

$$\varphi(t) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \tilde{\varphi}(s) t^{-s} ds.$$

One finds an asymptotic expansion of $\varphi(t)$ as t approaches 0 by moving the contour of integration to the left. Then each term in the asymptotic expansion appears as a residue from some pole in the meromorphic continuation of $\tilde{\varphi}(s)$. The following result formalizes this principle in the particular case we will later need.

Proposition 2.21 (Proposition p. 98, [31])**.** *Let $C\colon \mathbb{Z} \to \mathbb{C}$ be a periodic function with mean value zero. Then the associated Dirichlet series $L(s, C) := \sum_{n=1}^{\infty} \frac{C(n)}{n^s}$, $\Re(s) > 1$, extends analytically to all of $\mathbb{C}$ and the function $\sum_{n=1}^{\infty} C(n) e^{-n^2 t}$, $t > 0$, has the asymptotic* *expansion*

$$\sum_{n=1}^{\infty} C(n)e^{-n^2 t} \sim \sum_{r=0}^{\infty} L(-2r, C)\frac{(-t)^r}{r!}$$

as $t \to 0^+$*, and the numbers* $L(-r, C)$ *are given explicitly by*

$$L(-2r, C) = -\frac{M^r}{r+1}\sum_{n=1}^{M} C(n)B_{r+1}\left(\frac{n}{M}\right), \quad (r = 0, 1, \ldots),$$

where $B_k(x)$ *is the* k*th Bernoulli polynomial and* M *is any period of the function* $C(n)$*.*

Proof. We begin by finding an asymptotic expansion for $\sum_{n=1}^{\infty} C(n)e^{-nt}$. By summing geometric series, we get

$$\begin{aligned}\sum_{n=1}^{\infty} C(n)e^{-nt} = \sum_{n=1}^{M} C(n)\frac{e^{-nt}}{1-e^{-Mt}} &= \sum_{n=1}^{M} C(n)\sum_{r=-1}^{\infty}\frac{B_{r+1}(n/M)}{(r+1)!}(-Mt)^r \\ &= \sum_{r=-1}^{\infty} -\frac{M^r}{r+1}\sum_{n=1}^{M} C(n)B_{r+1}\left(\frac{n}{M}\right)\frac{(-t)^r}{r!}, \qquad (|t| < 2\pi/M).\end{aligned}$$

For convenience, we denote the coefficient of $(-t)^r/r!$ in this expansion by a_r. Then recognizing the Mellin integral representation

$$\Gamma(s)L(s, C) = \int_0^{\infty}\left(\sum_{n=0}^{\infty} C(n)e^{-nt}\right)t^{s-1}\,dt, \qquad (\Re(s) > 1),$$

one can use the same argument at the beginning of this section to show that for each $R \in \mathbb{Z}_{\geq 0}$, $\Gamma(s)L(s, C)$ has a meromorphic continuation to $\Re(s) > -R$ with simple poles at nonpositive integers $-R+1 \leq -r \leq 0$, each with residue a_r. This gives the analytic continuation of $L(s, C)$ and shows that $L(-r, C) = a_r$ for each $r \in \mathbb{Z}_{\geq 0}$.

Again analyzing the Mellin transform

$$\Gamma(s)L(2s,C) = \int_0^\infty \left(\sum_{n=0}^{\infty} C(n) e^{-n^2 t} \right) t^{s-1}\, dt, \qquad (\Re(s) > 1/2),$$

we find that $L(2s, C)$ has an analytic continuation to $\mathbb{C}$, or equivalently that $\Gamma(s)L(2s, C)$ has a meromorphic continuation to $\mathbb{C}$ with residue $L(-2r, C)$ for each $r \in \mathbb{Z}_{\geq 0}$. By analyzing the inverse Mellin transform of $\Gamma(s)L(2s, C)$ and moving the contour to the left, each subsequent residue contributes a term in the asymptotic expansion of $\sum_{n=1}^{\infty} C(n)e^{-n^2 t}$. The value of $L(-2r, C)$ in terms of Bernoulli polynomials and the coefficients $C(n)$ are known by our analysis of $\sum_{n=0}^{\infty} C(n)e^{-nt}$, so we are done.

□

2.3.2 Eichler Quantum Modular Forms

The utilization of Eichler integrals to construct quantum modular forms has its roots in the work of Lawrence and Zagier [31]. Many authors have since extended and generalized this procedure to systematically construct families of quantum modular forms: see e.g. [7, 18, 21]. Here we sketch the procedure by which the authors of [7] construct quantum modular forms, modified to fit our context.

Suppose a function $F(\tau)$ for $\tau \in \mathbb{H}$ may be written as

$$F(\tau) = \sum_{n \geq 0} a(n) q^{\frac{n^2}{4pj}}, \qquad (q = e^{2\pi i \tau})$$

for some integers $p,\ j$. Further suppose that

$$f(\tau) := \sum_{n\geq 0} na(n)q^{\frac{n^2}{4pj}}$$

is a cusp form of weight 3/2 for $\Gamma_1(N)$. We consider the *non-holomorphic Eichler integral* of f, given by

$$F^*(\tau) := \frac{\sqrt{-2\pi i}}{\Gamma(1/2)} \int_{\overline{\tau}}^{i\infty} \frac{f(\omega)}{\sqrt{-i(\omega - \tau)}}\, d\omega, \qquad (\tau \in \mathbb{H}^-)$$

where $\mathbb{H}^-$ denotes the lower half plane.

Bringmann and Rolen show that, after suitable renormalization, the functions $F(\tau)$ and $F^*(\tau)$ "agree to infinite order" at any $x \in \mathbb{Q}$. That is, for any x there exists a sequence $\beta(0), \beta(1), \ldots$ such that as $t \to 0^+$,

$$F\left(x + \frac{it}{2\pi}\right) \sim \sum_{r\geq 0} \beta(r)\frac{(-t)^r}{r!} \text{ and } F^*\left(x - \frac{it}{2\pi}\right) \sim \sum_{r\geq 0} \beta(r)\frac{t^r}{r!}.$$

This is accomplished by first integrating F^* term-by-term to obtain a series expansion for $F^*(\tau)$ involving Γ-factors. Then using Proposition 2.21 and carefully treating the Mellin transform of special functions, they obtain the asymptotic expansions of both of these functions and verify that they agree in the above sense.

This tells us that if we are interested in the behavior of $F(\tau)$ as we approach elements of $\mathbb{Q}$, it suffices to study the properties of $F^*(\tau)$. We note that the function $F^*(\tau)$ admits an explicit obstruction to modularity from its definition; for $\tau \in \mathbb{H}^-$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$, we have

$$F^*(\tau) - F^*|_{1/2}\gamma\,(\tau) = r_\gamma(\tau),$$

where

$$r_\gamma(\tau) := \frac{\sqrt{-2\pi i}}{\Gamma(1/2)} \int_{\gamma^{-1}(i\infty)}^{i\infty} \frac{f(\omega)}{\sqrt{-i(\omega - \tau)}}\, d\omega. \tag{2.3.2}$$

which extends to a C^∞ function on $\partial\mathbb{H}^- = \mathbb{R}$ which is real-analytic on $\mathbb{R}\backslash\{\gamma^{-1}(i\infty)\}$ and gives h_γ for the resulting quantum modular form.

Ultimately, we need the following lemma in order to renormalize the powers of q that appear in the proof of Theorem 1.11. Using the definitions, one can verify the following:

Lemma 2.22. *If $\psi(\tau)$ is a quantum modular form of weight $1/2$ for $\Gamma(4pj)$ with multiplier χ, then $\psi(j\tau)$ is a quantum modular form of weight $1/2$ for $\Gamma(4pj^2)$ with the same multiplier.*

Chapter 3

Zeros in Character Tables of Symmetric Groups

We begin this chapter by giving a brief overview of the representation theory of the symmetric group and its relationship to partitions, culminating in a statement of the Murnaghan-Nakayama Rule. We then discuss asymptotic formulas for various partition statistics and a combinatorial tool called abaci in the study of partitions. We end by giving a new criteria that guarantees certain entries vanish in the character tables of S_n vanish and gives asymptotic formulas for the sizes of two families of zeros.

3.1 Partitions and the Symmetric Group

Recall that the conjugacy classes of S_n are in one-to-one correspondence with the partitions of n; each conjugacy class is represented by the common cycle type of the permutations in that class, and a cycle type uniquely determines a partition.

Less obvious is that the partitions of n also naturally parameterize the irreducible complex representations of S_n. For a given partition λ of n, one can associate a partition λ of n with a Young diagram containing n boxes. A *Young tableau* T of shape λ is created by filling the boxes of a Young diagram with the numbers 1 through n, each used exactly once.

$$\begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 4 & 6 & \multicolumn{1}{c}{} \\ \cline{1-2} 5 & \multicolumn{2}{c}{} \\ \cline{1-1} \end{array}$$

Figure 3.1: A Young tableau of shape $\lambda = (3, 2, 1)$

Tabloids are then defined as equivalence classes of Young tableaux under the relation that considers two fillings equivalent if are related by permuting the entries within any row. For a given Young tableau T of shape λ, the notation $\{T\}$ denotes the corresponding tabloid. Since S_n acts on the collection of Young tableaux of shape λ by permuting the entries of the filling, it also acts on the set of tabloids and thus the $\mathbb{C}$-vector space V with basis the set of tabloids. Now, define

$$E_T := \sum_{\sigma \in Q_T} \operatorname{sgn}(\sigma)\{\sigma(T)\} \in V$$

where Q_T is the subgroup of permutations that fix the entries of T column-wise (though possibly permuting elements within columns). The *Specht module* S^λ is then generated by the elements E_T as T varies over all tableaux of shape λ. Over $\mathbb{C}$, this construction results in an irreducible representation of S_n, and form a complete set of all irreducible representations of the symmetric group.

Such a construction allows for the combinatorics of partitions to enter naturally into the study of the symmetric group. For example, the dimension of S^λ can be computed by counting the number of standard Young tableau of shape λ, or equivalently using the hook-length formula of Frame, Robinson, and Thrall. One of the most celebrated such applications gives an algorithmic approach to computing entries in the *character table* of S_n.

The *character* χ_λ of a representation $\rho_\lambda \colon S_n \to \mathrm{GL}_k(\mathbb{C})$ corresponding to S^λ is defined by $\chi_\lambda(g) = \operatorname{Tr}(\rho_\lambda(g))$. Note that since the trace is invariant under conjugation, each character is a class function. The character table of S_n is then a matrix whose rows correspond to irreducible characters and whose columns correspond to conjugacy classes, both of which are indexed by the partitions of n. The entry in row λ and column μ is $\chi_\lambda(\mu)$.

	(1)	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
(5)	1	1	1	1	1	1	1
$(4,1)$	4	2	1	0	-1	0	-1
$(3,2)$	5	1	-1	-1	0	1	1
$(3,1^2)$	6	0	0	0	1	-2	0
$(2^2,1)$	5	-1	-1	1	0	1	-1
$(2,1^3)$	4	-2	1	0	-1	0	1
(1^5)	1	-1	1	-1	1	-1	-1

Table 3.1: Character table of S_5

3.1.1 Murnaghan-Nakayama

The Murnaghan-Nakayama Rule gives a combinatorial interpretation of the value $\chi_\lambda(\mu)$ in terms of partition statistics of λ and μ. Moreover, this rule gives a way to recursively compute character table values. To precisely state this rule, we need the following notation.

A border strip in a Young diagram is a connected skew shape along the edge of the diagram that contains no 2 x 2 square and whose removal results in another valid Young diagram. The length of a border strip is the total number of boxes it contains, and its height is one less than the number of rows it spans.

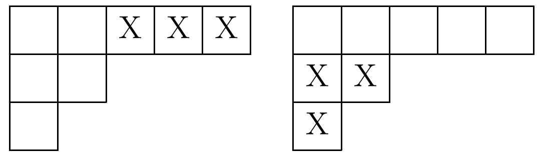

Figure 3.2: The two border strips of length 3 of $\lambda = (5, 2, 1)$

With the preceding notion, we are able to state a useful formulation of the Murnaghan-Nakayama Rule.

Theorem 3.1 (Murnaghan-Nakayama)**.** *Suppose λ and μ are partitions of n. Then we have*

$$\chi_\lambda(\mu) = \sum_{\xi \in BS(\mu,\lambda_1)} (-1)^{ht(\xi)} \chi_{\lambda \setminus \lambda_1}(\mu \setminus \xi)$$

where the sum is over the set $BS(\mu, \lambda_1)$ of border strips within the Young diagram of shape μ with length λ_1. The notation $\mu \setminus \xi$ represents the partition that results from removing the border strip ξ from μ, and $\lambda \setminus \lambda_1$ denotes the partition that results from removing the first part λ_1 from λ.

This rule gives us a standard partition-theoretic criterion that guarantees the vanishing of a character value $\chi_\lambda(\mu)$. Suppose that $\lambda = (\lambda_1, \ldots, \lambda_s)$ and $\mu = (\mu_1, \ldots, \mu_t)$ are partitions of size n, and let $\{h_\lambda(i, j)\}$ be the multiset of hook lengths for λ. Then we have that $\chi_\lambda(\mu) = 0$ when $\{\mu_i\}$ is not a subset of $\{h_\lambda(i, j)\}$.

Given a prime ℓ, this immediately gives natural families of vanishing character table entries indexed by pairs of partitions (λ, μ) of n, where μ has a part that is a multiple of ℓ, and λ is an ℓ-core partition.

Lemma 3.2. *If ℓ is prime, then the following are true.*

1. *If $\mu \vdash n$ is not an ℓ-regular partition and $\lambda \vdash n$ is an ℓ-core partition, then $\chi_\lambda(\mu) = 0$.*

2. If n is a positive integer, then we have

$$Z_\ell(n) \geq (p(n) - p_\ell(n)) \cdot c_\ell(n).$$

Proof. (1) By hypothesis, μ is not ℓ-regular, meaning that it has a part that is a multiple of ℓ. As λ is an ℓ-core, none of its hook lengths are multiples of ℓ. Therefore, $\chi_\lambda(\mu) = 0$ by Murnaghan-Nakayama. (2) The number of partitions of n that are not ℓ-regular is $p(n) - p_\ell(n)$. Therefore, (1) gives the conclusion that

$$Z_\ell(n) \geq (p(n) - p_\ell(n))c_\ell(n).$$

□

3.2 Asymptotics for Partition Statistics

In 1918, Hardy and Ramanujan achieved a remarkable breakthrough in number theory by providing an asymptotic formula for $p(n)$. They proved that as $n \to \infty$, we have

$$p(n) \sim \frac{1}{4n\sqrt{3}} \cdot \exp(\pi\sqrt{2n/3}). \tag{3.2.1}$$

This work also introduced the circle method, a technique developed further in later works with John E. Littlewood and which has become a cornerstone of analytic number theory, enabling profound insights into the distribution of prime numbers, asymptotics of partition statistics, and much more. The basic idea of the circle method is to integrate the generating function of the sequence of interest along a contour, which by the residue theorem can isolate its coefficients, and push that contour towards the unit circle where the generating function is typically not defined.

As the radius r approaches 1, the path is divided into "major arcs" and "minor arcs." The integral over the major arcs yields the main term, capturing the principal contribution to the coefficient's asymptotic estimate, while the integral over the minor arcs should contribute the error term. Crucially, the analysis hinges on the behavior of the generating function near roots of unity, since the function's behavior at these points critically influence the precision of the main term's approximation and control over the error term.

While we will not use the circle method directly in this thesis, we will appeal to both the asymptotic of $p(n)$ and another asymptotic for a partition statistic due to the circle method.

3.2.1 ℓ-regular Partitions

It is standard in the modern study of partitions to consider partitions with restrictions on their parts. A partition μ is A-*regular* if none of its parts μ_i are multiples of A. If $p_A(n)$ denotes the number of A-regular partitions of n, then one easily confirms the generating function

$$\sum_{n=0}^{\infty} p_A(n)q^n = \prod_{n=1}^{\infty} \frac{(1-q^{An})}{(1-q^n)} = \prod_{n=1}^{\infty} \left(1 + q^n + q^{2n} + \cdots + q^{(A-1)n}\right),$$

which shows that $p_A(n)$ also is the number of partitions of n where parts appear at most $A-1$ times. Using the circle method, Hagis obtained asymptotics for $p_A(n)$, the number of A-regular partitions of n. Letting $t = A - 1$ in Corollary 4.2 of [43], we have the following asymptotic formula.

Theorem 3.3. *If $A \geq 2$, then we have*

$$p_A(n) = C_A(24n - 1 + A)^{-\frac{3}{4}} \exp\left(C\sqrt{\frac{A-1}{A}\left(n + \frac{A-1}{24}\right)}\right)\left(1 + O(n^{-\frac{1}{2}})\right),$$

where $C := \pi\sqrt{2/3}$ and $C_A := \sqrt{12}A^{-\frac{3}{4}}(A-1)^{\frac{1}{4}}$.

3.2.2 Aymptotics for ℓ-core Partitions

In [22], Granville and Ono resolve the t-core partition conjecture, which claims that for any $t \geq 4$ and for any n, there exists a t-core partition of n. To do so, they analyze the generating function of t-core partitions as a modular form and control the size of the coefficients using Deligne's bound, discussed in a previous chapter. In the course of the proof, they also find asymptotics for the number of ℓ-core partitions of n for prime ℓ. In particular, they prove the following:

Theorem 3.4 ([22])**.** *The following are true.*

1. *We have that*

$$c_2(n) = \begin{cases} 1 & \text{if } n \text{ is a triangular number,} \\ 0 & \text{otherwise.} \end{cases}$$

2. *If n is a non-negative integer, then*

$$c_3(n) = \sum_{d|(3n+1)} \left(\frac{d}{3}\right).$$

   In particular, $c_3(n) = 0$ for almost all n.

3. *If $t \geq 4$ and n is a non-negative integer, then $c_t(n) > 0$.*

4. If n is a non-negative integer, then $c_5(n) = \sigma_5(n+1)$.

5. If $\ell \geq 7$ is prime, then as $n \to +\infty$ we have

$$c_\ell(n) \sim \alpha_\ell \cdot \sigma_\ell(n + \delta_\ell).$$

6. If $\ell \geq 11$ is prime and n is sufficiently large, then we have

$$c_\ell(n) > \frac{2\alpha_\ell}{5} \cdot n^{\frac{\ell-3}{2}}.$$

Here we give an indication of the proof of part (5) of the theorem, as this is the most relevant for our work. One first realizes a generating function for the number of ℓ-core partitions of n as the eta-quotient

$$\sum_{n=0}^{\infty} c_\ell(n) q^{n+\frac{\ell^2-1}{24}} = \frac{\eta^\ell(\ell\tau)}{\eta(\tau)},$$

which is a modular form of weight $(\ell-1)/2$ on $\Gamma_0(\ell)$ with character $\chi(d) := \left(\frac{d}{p}\right)$ when $\ell \geq 5$ prime. By work of Almkvist in [2], one can write

$$\frac{\eta^\ell(\ell\tau)}{\eta(\tau)} = \alpha_\ell E_\ell(\tau) + f(\tau)$$

where α_ℓ is defined in Equation (1.1.2), $f(\tau) \in S_{\frac{\ell-1}{2}}(\Gamma_0(\ell), \chi)$, and

$$E_\ell(\tau) := \sum_{n=1}^{\infty} \sigma_\ell(n) q^n,$$

where $\sigma_\ell(n) := \sum_{d|n} \chi(n/d) d^{\frac{\ell-3}{2}}$. Since there are no lower levels dividing ℓ with non-trivial character χ, $f \in S^{new}_{\frac{\ell-1}{2}}(\Gamma_0(\ell), \chi)$. Then one uses the upper bounds on the Fourier coefficients of newforms discussed in Section 2.1 and a low er bound on $\sigma_\ell(n)$ on the order of $n^{\frac{\ell-3}{2}}$ to prove that, asymptotically, the coefficients of $\alpha_\ell \cdot E_\ell(\tau)$ contribute the main term.

3.3 Abaci

We make use of the theory of *abaci* for partitions (for example, see [17, 28]). In particular, let $\lambda = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s > 0$ be a partition of n. For each $1 \leq i \leq s$, define the *ith structure number* $B_i := \lambda_i - i + s$, so that $B_i = h_\lambda(i,1)$, the hook length of cell $(i,1)$.

Using these structure numbers, we represent the partition λ as an ℓ-abacus $\mathfrak{A}_\lambda$, consisting of beads placed on rods numbered from 0 to $\ell - 1$. For each B_i, there is a unique pair of integers (r_i, c_i) for which $B_i = \ell(r_i - 1) + c_i$ and $0 \leq c_i \leq \ell - 1$. The abacus $\mathfrak{A}_\lambda$ then consists of s beads, where for each i, one places a bead in position (r_i, c_i).

Lemma 3.5 (Lemma 2.7.13, [28]). *Assuming the notation above, λ is an ℓ-core if and only if all of the beads in $\mathfrak{A}_\lambda$ lie at the top of their respective rods without gaps.*

In view of this lemma, we may represent an abacus of an ℓ-core partition by ℓ-tuples of non-negative integers, say $(b_0, \ldots, b_{\ell-1})$, where b_i denotes the number of beads in column i. However, such representations are not unique as they generally allow for parts of size zero. We have the following elementary lemma.

Lemma 3.6 (Lemma 1, [42]). *The following abaci both represent the same ℓ-core partition:*

$$(b_0, b_1, \ldots, b_{\ell-1}) \quad \textit{and} \quad (b_{\ell-1} + 1, b_0, b_1, \ldots, b_{\ell-2}).$$

By repeatedly applying this lemma, we may canonically define the unique abacus representation for an ℓ-core to be the one with zero beads in the first column. Thus, when we talk about *the* abacus representation of an ℓ-core λ, we will always mean the abacus of the form $\mathfrak{A}_\lambda = (0, b_1, \cdots, b_{\ell-1})$.[1] Using these abaci, we offer the following lemma that will allow us to rule out the existence of partitions that are simultaneously ℓ-core and ℓ-regular for all but finitely many n.

Lemma 3.7. *Suppose that $\mathfrak{A}_\lambda = (0, b_1, \ldots, b_{\ell-1})$ is the abacus corresponding to an ℓ-core λ, and suppose that there is an integer $k \geq 0$ such that for each $1 \leq i \leq \ell - 1$ we have either $b_i \leq k$ or $b_i \geq k + \ell$. If there is at least one j for which $b_j \geq k + \ell$, then λ is not an ℓ-regular partition.*

Remark 3.8. *Let $\mathfrak{A}_\lambda = (0, b_1, \cdots, b_{\ell-1})$ be the abacus of an ℓ-core λ. If $\min(b_1, \cdots b_{\ell-1}) \geq \ell$, then the proof of the lemma will show that λ has a part of exact size ℓ. These are the cases where one can choose $k = 0$ in the lemma.*

Proof. By our hypothesis, we may fix j for which $b_j \geq k + \ell$. Let δ denote the total number of columns with length at least $k+\ell$. Note that if B_i and $B_{i'}$ are structure numbers corresponding to consecutive beads in column j between rows $k+1$ and $k+\ell$, then $|i-i'| = \delta$. Further, we have $|B_i - B_{i'}| = \ell$. Generalizing the observation that $B_{i-1} - B_i = \lambda_{i-1} - \lambda_i + 1$, we have

$$|\lambda_i - \lambda_{i'}| = |B_i - B_{i'}| - \delta = \ell - \delta.$$

In particular, the difference between parts corresponding to consecutive beads in column j between rows $k + 1$ and $k + \ell$ is fixed and coprime to ℓ. As a consequence, these parts form a modulus $\ell - \delta$ arithmetic progression consisting of ℓ values. Thus, the parts cover all residue classes modulo ℓ, and so includes a part that is a multiple of ℓ. □

[1] These abaci correspond to those representations of λ without parts of size 0.

Example 3.9. Let $\ell = 3$, and consider the 3-core abacus $(0, 4, 1)$ as shown below.

$$\begin{array}{c|ccc} 1 & \cdot & \circ & \circ \\ 2 & \cdot & \circ & \cdot \\ 3 & \cdot & \circ & \cdot \\ 4 & \cdot & \circ & \cdot \end{array}$$

We illustrate Lemma 3.7 with $k = 1$. Since $b_1 = 3 + 1 = 4$ and $b_2 = 1$, the lemma asserts that λ has a part that is a multiple of 3. The structure numbers are found to be $B_1 = 10$, $B_2 = 7$, $B_3 = 4$, $B_4 = 2$, and $B_1 = 1$, and we compute that $\lambda_1 = 10 + 1 - 5 = 6$, $\lambda_2 = 4$, $\lambda_3 = 2$, and $\lambda_4 = \lambda_5 = 1$. In particular, λ_1 is a multiple of 3.

Finally, consider the abacus with the bead in row 4 removed. One easily checks that the corresponding partition is 3-regular, demonstrating that the condition on the size of the gap in column lengths cannot be relaxed.

For the purpose of obtaining N_ℓ, the following lemma allows us to restrict our attention to those abaci where the b_i are weakly increasing.

Lemma 3.10. *Suppose that $\lambda = (\lambda_1, \ldots, \lambda_s)$ is an ℓ-core partition of n with abacus $\mathfrak{A}_\lambda = (0, b_1, \ldots, b_{\ell-1})$. If there exist $1 \leq i < j \leq \ell - 1$ for which $b_j < b_i$, then the abacus $\mathfrak{A}'$ obtained by swapping b_i and b_j represents an ℓ-core partition λ' with $\lambda' \vdash n' > n$.*

Proof. We may write

$$n = \sum_{k=1}^{s} \lambda_k = \sum_{k=1}^{s} (B_k + k - s) = \sum_{k=1}^{s} B_k + \sum_{k=1}^{s} (k - s),$$

and likewise $n' = \sum_{k=1}^{s} B'_k + \sum_{k=1}^{s} (k - s)$, where s remains the same because we have not changed the total number of beads. Since the second sum is the same in both expressions, it suffices to prove that $\sum_{i=1}^{s} B_k < \sum_{i=1}^{s} B'_k$. Computing column-wise, we have

$$\begin{aligned}
\sum_{k=1}^{s} B_k &= \sum_{m=1}^{b_i}(3(m-1)+i) + \sum_{m=1}^{b_j}(3(m-1)+j) + \sum_{\substack{k=1\\k\neq i,j}}^{\ell-1}\sum_{m=1}^{b_k}(3(m-1)+k) \\
&< \sum_{m=1}^{b_i}(3(m-1)+j) + \sum_{m=1}^{b_j}(3(m-1)+i) + \sum_{\substack{k=1\\k\neq i,j}}^{\ell-1}\sum_{m=1}^{b_k}(3(m-1)+k) \\
&= \sum_{k=1}^{s} B'_k
\end{aligned}$$

as desired, where the inequality holds since $i < j$ and $b_i > b_j$. $\square$

We now introduce terminology coined by McDowell in [33] to succinctly describe what was proven in Lemma 3.7 and give their superior calculation of the size of the largest ℓ-regular ℓ-core partition than originally appeared in [35].

Definition 3.11. *For $1 \leq i \leq \ell - 1$, the ith row multiplicity of an ℓ-core partition with weakly increasing column lengths is the number of rows containing exactly i gaps and $p - i$ beads.*

This language allows us to show:

Proposition 3.12. *Suppose that ℓ is prime, and let $N_\ell := (\ell^6 - 2\ell^5 + 2\ell^4 - 3\ell^2 + 2\ell)/24$. If $n > N_\ell$, then every ℓ-core partition of size n has a part that is a multiple of ℓ.*

Remark 3.13. *We note that $N_\ell < \ell^6/24$ is not optimal. Indeed, if we let $N_\ell^{\max}$ be the largest n admitting an ℓ-regular ℓ-core partition, then it turns out that $N_3^{\max} = 10$ and $N_3 = 16$. Indeed, work of McDowell in [33] has improved this bound and has also given a* *lower bound on the size of the largest ℓ-regular ℓ-core partition also on the order of ℓ^6, which was subsequently sharpened by [14].*

Proof. First, note that the largest ℓ-regular ℓ-core partition must have $b_1 \neq 0$: otherwise, one could permute the b_i's as described in Lemma 3.6 and then rearrange so the column lengths were strictly increasing, ending up with a strictly larger ℓ-regular ℓ-core partition. Then we observe that increasing a row multiplicity always increases the size of a partition. This fact, paired with Lemma 3.7, which bounds the row multiplicities of an ℓ-regular partition ℓ-regular ℓ-core partition by $\ell-1$, tells us that the size of the partition with all row multiplicities equal to $\ell - 1$ will give an upper bound.

Then if Λ is the partition with abacus $\mathfrak{A}_\Lambda = (0, \ell - 1, 2(\ell - 1), \ldots, (\ell - 1)^2)$, by direct calculation we find that

$$|\Lambda| = \sum_{i=1}^{s}(B_i + i - s) = \sum_{i=1}^{\ell-1} \sum_{j=1}^{i(\ell-1)} (\ell(j-1) + i) + \sum_{i=1}^{s}(i - s) = \frac{\ell^6 - 2\ell^5 + 2\ell^4 - 3\ell^2 + 2\ell}{24},$$

where $s = \ell(\ell - 1)^2/2$, giving the desired conclusion. $\square$

3.4 Proofs of Theorems

In this section, we assemble the ideas in the previous sections to prove Theorems 1.2 and 1.5.

3.4.1 Proof of Theorem 1.2

We note that the Hardy-Ramanujan asymptotic and Theorem 3.3 together imply that

$$\lim_{n\to+\infty} \frac{p(n) - p_\ell(n)}{p(n)} = 1.$$

The claim now follows by combining Lemma 3.2 (2) and Theorem 3.4 (4-6).

3.4.2 Proof of Theorem 1.5

By Proposition 3.12, every ℓ-core partition of size $n > N_\ell$ has a part that is a multiple of ℓ. Since every hook length of an ℓ-core is not a multiple of ℓ, it follows from Murnaghan-Nakayama that whenever $\lambda, \mu \vdash n$ are ℓ-cores with $n > N_\ell$, we have $\chi_\lambda(\mu) = 0$.

Proof of Corollary 1.6. Thanks to Theorem 1.5, we have that $Z_\ell^*(n) = c_\ell(n)^2$ for sufficiently large n. The claimed asymptotics and inequalities follow from Theorem 3.4 (4-6). $\square$

Chapter 4

Jellyfish and the Finite-Field AGM

We begin this chapter with a discussion of class groups and class numbers of orders in imaginary quadratic fields, which play a central role in the study of elliptic curves with complex multiplication.

4.1 Class Groups of Imaginary Quadratic Orders

Let $K = \mathbb{Q}(\sqrt{d})$, where $d < 0$ and $d \in \mathbb{Z}$ is square-free, be an imaginary quadratic field.

Definition 4.1. *An imaginary quadratic order $\mathcal{O}$ is a subring of the ring of integers $\mathcal{O}_K$ of K which is a rank two $\mathbb{Z}$-module.*

Example 4.2. Both $\mathcal{O} := \mathbb{Z}[\sqrt{-3}]$ and $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ are orders in $K = \mathbb{Q}(\sqrt{-3})$.

It is well known that the ring of integers $\mathcal{O}_K$ admits an integral basis of the form $[1, w_K]$ where if $d \not\equiv 1 \bmod 4$ then we can take $w_K = \sqrt{d}$ and if $d \equiv 1 \bmod 4$ then we can take $w_K = \frac{1+\sqrt{d}}{2}$. In these cases, the discriminant of $\mathcal{O}_K$ is respectively $d_K = 4d$ or $d_K = d$. If $\mathcal{O}$ is an imaginary quadratic order, then since both $\mathcal{O}$ and $\mathcal{O}_K$ are free $\mathbb{Z}$-modules of the same rank, we have that the index $f = [\mathcal{O} : \mathcal{O}_K]$ is finite. We call f the *conductor* of $\mathcal{O}$. Moreover, one can show that $\mathcal{O}$ admits the integral basis $[1, fw_K]$ and we declare the discriminant of $\mathcal{O}$ to be $f^2 d_K$. Due to the following result, one can equivalently consider the set of discriminants to parameterize the set of imaginary quadratic orders.

Proposition 4.3 ([12], Proposition 5.1.3)**.** *If $D \equiv 0, 1 \pmod 4$, then $D = f^2 d_K$ for some unique fundamental discriminant d_K and there exists a unique order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{d_K})$ with discriminant D.*

We also extend the notion of ideals to non-maximal orders of imaginary quadratic fields. A *fractional ideal* of an order $\mathcal{O}$ is an $\mathcal{O}$-submodule I of K such that there exists an $a \in \mathcal{O}$ such that $xI \subseteq \mathcal{O}$. An ideal is *invertible* if there exists another fractional ideal J such that $IJ = \mathcal{O}$ For imaginary quadratic orders, this notion agrees with an ideal being proper. A *principal ideal* is an ideal which is generated by a single element of $\mathcal{O}$. As in the classical case, invertible fractional ideals form a group and principal ideals a subgroup.

Definition 4.4. *The class group of an order, denoted $cl(\mathcal{O})$, is the quotient of the group of invertible fractional ideals $I(\mathcal{O})$ by the subgroup of principal ideals $P(\mathcal{O})$. The class number of $\mathcal{O}$ is defined to be the order of this group. That is, $h(\mathcal{O}) := |cl(\mathcal{O})|$.*

4.2 Elliptic Curves

This section will give a brief overview of elliptic curves, primarily focusing on their traces and endomorphism rings over finite fields.

Definition 4.5. *An elliptic curve over a field K (with characteristic not equal to 2 or 3) is a cubic curve defined by an equation of the form*

$$E \colon y^2 = x^3 + ax + b$$

where $a, b \in K$ *and the discriminant* $\Delta = -16(4a^3 + 27b^2) \neq 0$*.*

It is well-known that if E is an elliptic curve, then points of E together with the point at infinity, labeled O, form an abelian group. Over $\mathbb{R}$, the group law is geometrically realized by the chord-tangent law. To add two points P and Q, one draws the unique line through P and Q (or the tangent line at P if $P = Q$). This line will intersect the curve in exactly one other point R. Then $P + Q$ is defined to be the point of E given by reflecting R across the x-axis.

Theorem 4.6 (Mordell-Weil)**.** *Let* E *be an elliptic curve defined over a number field* K*. Then the group of* K*-rational points on* E*, denoted* $E(K)$*, is finitely generated.*

Definition 4.7. *An isogeny between two elliptic curves* E *and* E' *over a field* K *is a non-constant morphism* $\varphi : E \to E'$ *that is defined over* K *and maps the point at infinity to the point at infinity. Isogenies are notably* K*-rational maps that preserve the group structure.*

The endomorphism ring of an elliptic curve E is the set of all $\bar{\mathbb{F}}_q$-endomorphisms of E together with the zero map and the operations of addition and composition. It contains a copy of the integers, $\mathbb{Z}$, since for any integer n, the map that sends each point P on the curve to its n-fold sum nP is an endomorphism of the curve. While for many curves this is the whole endomorphism ring, there are elliptic curves with endomorphism rings strictly larger and these will be the types of curves we study.

Definition 4.8. *An elliptic curve* E *is said to have complex multiplication by an imaginary quadratic order* $\mathcal{O}$ *if we have* $\mathrm{End}(E) = \mathcal{O}$*.*

We will later characterize which elliptic curves these are in our case. We will also appeal to a well-studied invariant of elliptic curves. While this invariant has many formulations, for

Legendre elliptic curves, the j-invariant of E_λ is the quantity

$$j(E_\lambda) := 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

In the following subsection, we will discuss which elliptic curves it distinguishes.

4.2.1 Elliptic curves over finite fields

We now restrict our attention to elliptic curves over finite fields $\mathbb{F}_q$. In particular, a fundamental first question to ask is how many $\mathbb{F}_q$-rational points any such curve has.

The *trace of Frobenius* is an important invariant of an elliptic curve over a finite field which arises from the action of Frobenius. The q-power Frobenius endomorphism maps each point (x, y) on the curve to (x^q, y^q). Its trace t is then given by $t = q + 1 - \#E(\mathbb{F}_q)$, where $\#E(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points on the curve, including the point at infinity. It then suffices to understand the quantity t to determine the sizes of curves over $\mathbb{F}_q$. In the 1930s, Hasse proved a bound on the possible size of t.

Theorem 4.9 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field. Then if $t = q + 1 - \#E(\mathbb{F}_q)$, then $|t| \leq 2\sqrt{q}$.*

The following result due to Waterhouse gives something of a converse statement; it gives criteria for when $|t| \leq 2\sqrt{q}$ is the trace of an elliptic curve over $\mathbb{F}_q$.

Theorem 4.10 (Theorem 4.1 of [51])**.** *Let $q = p^k$ be a power of a prime p. Let $t \in \mathbb{Z}$ and let $N = q + 1 - t$. The integer N is the cardinality of $E(\mathbb{F}_q)$ for some elliptic curve $E/\mathbb{F}_q$ if and only if one of the following conditions is satisfied:*

1. $|t| \leq 2\sqrt{q}$ *and* $(t,p) = 1$*;*

2. k *is odd and* $t = 0$*;*

3. k *is odd,* $t = \pm\sqrt{pq}$*, and* $p = 2$ *or 3;*

4. k *is even,* $t = 0$*,* $p \not\equiv 1 \bmod 4$*;*

5. k *is even,* $t = \pm\sqrt{q}$*,* $p \not\equiv 1 \bmod 3$*;*

6. k *is even,* $t = \pm 2\sqrt{q}$*.*

Since in our case $q \equiv 3 \pmod 4$ and $p > 3$, only the first two cases can occur in our setup. The two cases will correspond to *ordinary* and *supersingular* elliptic curves respectively. While we will not detail the complete definitions of these terms here, we do recall some necessary characterizations and results for our work.

Definition 4.11. *An elliptic curve* $E/\mathbb{F}_q$ *is supersingular if* $t \equiv 0 \pmod p$*, where* t *is the trace of Frobenius of* E*. Else, we say* $E/\mathbb{F}_q$ *is ordinary.*

It turns out that in either case, the endomorphism ring of E is larger than $\mathbb{Z}$; what precisely this endomorphism looks like however is highly dependent on whether E is ordinary or supersingular.

Theorem 4.12 ([15])**.** *If* E *is an ordinary elliptic curve over* $\mathbb{F}_q$*, then End*(E) *is an order in an imaginary quadratic field. If* E *is supersingular, then End*(E) *is an order in a quaternion algebra.*

However, it turns out that one restricts their attention to the ring of endomorphisms of a supersingular elliptic curve which are defined over $\mathbb{F}_q$, one can identify this rational endomorphism ring with an imaginary quadratic order in the case where $t = 0$; for more details, see [51].

We lastly need to understand when two Legendre elliptic curves with distinct Legendre parameters are actually isomorphic.

Lemma 4.13. *Let $L_{\mathbb{F}_q}(t, j)$ denote the number of distinct $\lambda \in \mathbb{F}_q^{\times 2} \setminus \{0, 1\}$ such that E_λ has trace t and j-invariant j. Then for all pairs (t, j) such that $L_{\mathbb{F}_q}(t, j) \neq 0$, we have $L_{\mathbb{F}_q}(t, j) = 2$.*

Proof. First fix t and j and recall that there are exactly six λ in $\overline{\mathbb{F}}_q \backslash \{0, 1\}$ corresponding to each j-invariant not equal to 0 or 1728 (see [49] Section III.1). What's more, given one such λ we can find expressions for the other five by considering the orbit of λ under the group generated by the transformations $\lambda \mapsto 1/\lambda$ and $\lambda \mapsto 1 - \lambda$ on $\mathbb{P}^1$. We can write this set as

$$[\lambda] := \{\lambda, 1/\lambda, 1 - \lambda, 1/(1 - \lambda), \lambda/(\lambda - 1), (\lambda - 1)/\lambda\}.$$

Now suppose that $\lambda \in \mathbb{F}_q^{\times 2} \backslash \{1\}$ and that E_λ has trace t and j-invariant j. We first note that all other elements of $[\lambda]$ are also in $\mathbb{F}_q^{\times} \backslash \{1\}$. We must also check which are squares. If λ is a square, then $1/\lambda$ is a square as well. Moreover, since $E_\lambda^{(\lambda)} \cong E_{1/\lambda}$ and λ is a square, this twist is trivial and the trace and j-invariant are unchanged. Note that only one of $1 - \lambda$ and $\lambda - 1$ can be a square since -1 is not a square in $\mathbb{F}_q$. Then only one of $\{1 - \lambda, 1/(1 - \lambda)\}$ and $\{\lambda/(\lambda - 1), (\lambda - 1)/\lambda\}$ is a set of squares. One also has that $E_\lambda^{(-1)} \cong E_{1-\lambda}$ and $E_{1/\lambda}^{(-1)} \cong E_{(\lambda-1)/\lambda}$. Since -1 is not a square, both of these are nontrivial twists, and so do not have the same trace as E_λ. Then the only contributions to $L_{\mathbb{F}_q}(t, j)$ are E_λ and $E_{1/\lambda}$.

Now we deal with the two exceptional cases. First, suppose E_λ has trace t and satisfies $j(E_\lambda) = 0$. Then λ satisfies $\lambda^2 - \lambda + 1 = 0$ by the equation

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

Moreover, the other solution to $x^2 - x + 1 = 0$ is $1/\lambda$, so there are exactly two Legendre elliptic curves with trace t and j-invariant 0.

Finally, when $j(E_\lambda) = 1728$, we have that $\lambda \in \{-1, 2, 1/2\}$. We know that -1 is not a sqaure in our setting, so either both 2 and 1/2 are squares or neither are. Thus, $L_{\mathbb{F}_q}(t, j) = 0$ or 2. $\square$

4.2.2 Classical Complex Multiplication

We first recall the classical theory of complex multiplication of elliptic curves over $\mathbb{C}$ (for example, see Chapter 2 of [48]): Let $\mathcal{O}$ be an order in an imaginary quadratic field. If $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal, then the torus $\mathbb{C}/\mathfrak{a}$ corresponds to an elliptic curve $E(\mathbb{C})$ with complex multiplication by $\mathcal{O}$. Equivalent ideals correspond to isomorphic elliptic curves, and we have a bijection between the ideal class group $cl(\mathcal{O})$ and the set

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) := \{j(E/\mathbb{C}) \mid \mathrm{End}(E) \cong \mathcal{O}\}$$

of j-invariants of elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$.

Further, another invertible $\mathcal{O}$-ideal $\mathfrak{b}$ uniquely determines a separable isogeny of degree

$N(\mathfrak{b})$ with kernel

$$E[\mathfrak{b}] := \{P \in E \mid \alpha \cdot P = O \text{ for all } \alpha \in \mathfrak{b}\}$$

such that the target curve also has multiplication by $\mathcal{O}$. One can check that principal ideals act trivially, and that this defines a faithful $cl(\mathcal{O})$-action on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$.

While this correspondence is pleasing, we are concerned with the case where $\mathbb{C}$ is replaced by the finite field $\mathbb{F}_q$. It turns out that the story in this setting is largely the same. Let E be an ordinary elliptic curve over $\mathbb{F}_q$, and let π_E denote the Frobenius endomorphism of E. One may compute the trace of Frobenius to be $t = q + 1 - \#E(\mathbb{F}_q)$. Using the characteristic equation for π_E, one derives the *norm equation*

$$t^2 - 4q = v^2 D_K,$$

where $v^2 D_K$ is the discriminant of the imaginary quadratic order $\mathbb{Z}[\pi_E]$ and D_K is the discriminant of its field of fractions K. Then if $\mathcal{O} := \mathrm{End}(E/\mathbb{F}_q)$, we have

$$\mathbb{Z}[\pi_E] \subseteq \mathcal{O} \subseteq \mathcal{O}_K,$$

and $\mathcal{O}$ has discriminant $u^2 D_K$, where $u = [\mathcal{O}_K : \mathcal{O}]$ divides $v = [\mathcal{O}_K : \mathbb{Z}[\pi_E]]$.

Now, consider the set

$$\mathrm{Ell}_t(\mathbb{F}_q) := \{j(E/\mathbb{F}_q) \mid \mathrm{tr}(\pi_E) = t\}$$

of $\overline{\mathbb{F}}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ with trace of Frobenius t. Tate's Isogeny

Theorem [50] implies that $\mathrm{Ell}_t(\mathbb{F}_q)$ determines an isogeny class. Further, as K is determined by t and q, this set can be written as the disjoint union

$$\mathrm{Ell}_t(\mathbb{F}_q) = \bigsqcup_{\mathbb{Z}[\pi_E]\subseteq\mathcal{O}\subseteq\mathcal{O}_K} \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q),$$

where $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is defined in the same way as $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. As a consequence of the Deuring Lifting Theorem, the norm equation implies that over $\mathbb{F}_q[x]$, the Hilbert class polynomial $H_{u^2D_K}(x)$ of degree $h(\mathcal{O})$ splits completely and the roots are precisely the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$. Then so long as $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is nonempty, the set has cardinality $h(\mathcal{O})$.

Recall the definition of the *Hurwitz class number* for an imaginary quadratic order $\mathcal{O}$:

$$H(\mathcal{O}) := \sum_{\mathcal{O}\subseteq\mathcal{O}'\subseteq\mathcal{O}_K} h(\mathcal{O}') \tag{4.2.1}$$

If D is the discriminant of $\mathcal{O}$, we may define $H(D) := H(\mathcal{O})$. This agrees with the definition given earlier. From the results above we immediately have that the cardinality of $\mathrm{Ell}_t(\mathbb{F}_q)$ is equal to $H(t^2 - 4q)$.

As in the characteristic 0 case, we again have a faithful action of $cl(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$. What's more, if $\varphi\colon E \to E'$ is an isogeny of degree ℓ such that $\mathcal{O} := \mathrm{End}(E) = \mathrm{End}(E')$, then φ results from the action of an invertible $\mathcal{O}$-ideal $\mathfrak{l}$ of norm ℓ. This action is what will ultimately allow us to compare edges in $\mathcal{J}_{\mathbb{F}_q}$ with elements of class groups. The following result of Kohel guarantees that we are in the case where the above action applies.

Theorem 4.14 (Proposition 23, [30])**.** *Let ℓ be a prime not dividing v, where v is the conductor of $\mathbb{Z}[\pi_E]$. Then every isogeny of degree ℓ starting at E leads to a curve with* *endomorphism ring isomorphic to $\mathcal{O}$.*

4.3 Jellyfish Statistic Counts

First we briefly recall some of the main results on jellyfish from [24]. Then we give some natural extensions of their results which will inform the main theorems in this chapter. In particular, we will be interested in which elliptic curves occur in jellyfish swarms as well as which elliptic curves can appear on the same component. To answer these questions, the authors study the group structures and the j-invariants of the curves that appear.

Theorem 4.15 (Theorems 1 (2) and 3 (1) of [24]). *The following are true.*

1. *The jellyfish swarm $\mathcal{J}_{\mathbb{F}_q}$ has $(q-3)(q-1)/2$ vertices.*

2. *Each E_λ for $\lambda \in \mathbb{F}_q^{\times 2}\backslash\{0,1\}$ appears exactly $q-1$ times.*

The proof of (1) counts the number of admissible pairs (a,b), and the proof of (2) relies on the fact that if (a,b) corresponds to an elliptic curve E_λ, then so does every pair (ka,kb) for $k \in \mathbb{F}_q^\times$.

The above imply that the number of distinct λ that occur in $\mathcal{J}_{\mathbb{F}_q}$ is $(q-3)/2$. However, we have alternative ways of counting the λ that appear using the tools developed in Section 3 of [24]. In particular, recall that the j-invariants parameterize $\overline{\mathbb{F}}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$, and that the trace and j-invariant determine an isomorphism class over $\mathbb{F}_q$. Further, Lemma 4.13 tells us that we count each distinct pair (j,t) exactly twice by looking at the possible values for the Legendre parameter λ. If we are able to count the possible traces and the possible j-invariants corresponding to each trace, as well as the number of distinct λ corresponding to each j-invariant, we will be able to get an alternative formula for the number of λ which occur.

Let $M_{\mathbb{F}_q}(t)$ be the number of distinct j-invariants of curves in jellyfish swarm with trace of Frobenius t. By the previous section, all such curves are isogenous, but they may not be connected by an isogeny in our graphs, and what's more, a priori not all possible j-invariants need appear. The following theorem implies that indeed all possible j-invariants are realized and they are moreover counted by class numbers.

Theorem 4.16 (Theorem 6 of [24])**.** *Suppose* $q \equiv 3 \bmod 8$ *and* $p > 3$*. If* $|t| \leq 2\sqrt{q}$ *such that* $(t,p) = 1$ *and* $t \equiv q + 1 \bmod 8$*, then we have*

$$H\left(\frac{t^2 - 4q}{4}\right) = M_{\mathbb{F}_q}(t).$$

The above relies primarily on the correspondence between the number of distinct j-invariants of elliptic curves with trace t and the Hurwitz class number $H(t^2 - 4q)$ discussed in Subsection 4.2.2 with the extra observation that the removal of a factor of 2 from the conductor u is equivalent to the requirement that $E[2] \subset E(\mathbb{F}_q)$ [45], which must be satisfied as all of our elliptic curves admit a Legendre normal form. Since $q \equiv 3 \bmod 4$, one can also show that every elliptic curve over $\mathbb{F}_q$ is of the form E_λ for $\lambda \in \mathbb{F}_q^{\times 2} \backslash \{0, 1\}$ by 2-descent.

By the same arguments as that which prove Theorem 4.16, we get the following for the ordinary traces when $q \equiv 7 \bmod 8$:

Theorem 4.17. *Suppose* $q \equiv 7 \bmod 8$ *and* $p > 3$*. If* $|t| \leq 2\sqrt{q}$ *such that* $(t,p) = 1$ *and*

$t \equiv q+1 \bmod 8$, *then we have*

$$H\left(\frac{t^2-4q}{4}\right) = M_{\mathbb{F}_q}(t)$$

We now turn to the case where E is supersingular (i.e. where $t=0$, as we shall see). While we need to amend the correspondence to avoid orders whose conductors are not coprime to p, we end up with a similar result:

Lemma 4.18. *Suppose $q \equiv 7 \bmod 8$ and $p > 3$. Then we have $h(-q) = M_{\mathbb{F}_q}(0)$.*

Proof. When $t = 0$, the rational endomorphism ring of E can be identified with an imaginary quadratic order in $\mathbb{Q}(\pi_E)$ with conductor prime to p (Theorem 4.1, [51]) containing $\mathcal{O}(-q)$ (Proposition 3.7, [45]). Since q is a power of p, there is only one such order, namely $\mathcal{O}(-p)$. □

4.4 Proofs of Theorems

In this section, we offer proofs of Theorems 1.7 and 1.8, which rely heavily on the results presented in Sections 4.1 to 4.3.

4.4.1 Proof of Theorem 1.7

We will demonstrate the argument for the case when $q \equiv 3 \bmod 8$. The case when $q \equiv 7 \bmod 8$ is the same except for the care needed to deal with the supersingular elliptic curves, for which one applies Lemma 4.18. For $q \equiv 3 \bmod 8$, the theorem is equivalent to proving that

$$\frac{(q-1)(q-3)}{2} = \sum_{\substack{|t|\le 2\sqrt{q} \\ t\equiv q+1 (8)}} 2(q-1)\cdot H\left(\frac{4q-t^2}{4}\right).$$

The left hand side is the number of vertices in $\mathcal{J}_{\mathbb{F}_q}$, so it suffices to show the right hand side is also a count of the vertices in this graph. The sum runs over all the admissible traces of elliptic curves in $\mathcal{J}_{\mathbb{F}_q}$, so it suffices to show that each summand is the count of the number of vertices of trace t. Fixing t, each j invariant defines a curve up to $\mathbb{F}_q$-isomorphism. The number of such j is counted by $H\left(\frac{t^2-4q}{4}\right)$ by Theorem 4.16. Corresponding to each isomorphism class, there are exactly 2 such λ by Lemma 4.13. Finally, by Theorem 4.15 (2), each λ appears in the graph with multiplicity $q-1$.

4.4.2 Proof of Theorem 1.8

By Theorem 3 (2) of [24], every edge corresponds to the unique isogeny with kernel generated by $\langle(0,0)\rangle$. In particular, this isogeny has degree 2.

By Corollary 4 (1) of [24], the groups $E(\mathbb{F}_q)$ are isomorphic for all E on a jellyfish, and so their endomorphism rings are all the same; call it $\mathcal{O}$. This implies that this isogeny is the image of the class of an ideal $\mathfrak{p}_2$ of norm 2 in $\mathcal{O}$ with $E[\mathfrak{p}_2] = \langle(0,0)\rangle$. Since E_λ and $E_{1/\lambda}$ are isomorphic over $\mathbb{F}_q$, the edge emanating from vertices corresponding to both of these curves must have the same target curve. In particular, every vertex at the end of a tentacle has a corresponding vertex in the cycle with the same j-invariant. Thus, it suffices to consider the action of $[\mathfrak{p}_2]$ on the cycles of the jellyfish with endomorphism ring $\mathcal{O}$. Since this action is faithful and all j-invariants in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ are represented on some cycle, every cycle must have length divisible by the order of $[\mathfrak{p}_2]$ in $cl(\mathcal{O})$. Since the size of a jellyfish is twice the length of its cycle due to its tentacles of length one, our count must be multiplied by 2.

To see that $m(\mathcal{J}) \cdot \#\mathcal{J} = 2(q-1) \cdot h_2(\mathcal{O})$, note that the action of $[\mathfrak{p}_2]$ partitions the set of vertices into $[cl(\mathcal{O}) : \langle [\mathfrak{p}_2] \rangle]$ subsets of size $2(q-1) \cdot h_2(\mathcal{O})$ by Theorem 1.7. Now if n is the order of $[\mathfrak{p}_2]$ in $cl(\mathcal{O})$, then $[\mathfrak{p}_2^n] \cdot E_\lambda = E_\lambda$, and so if $\lambda = b^2/a^2$, the nth pair in the sequence of $\mathrm{AGM}_{\mathbb{F}_q}(a, b)$ is (ka, kb) for some k in $\mathbb{F}_q^\times$. Then if $\mathrm{ord}(k)$ denotes the multiplicative order of k in $\mathbb{F}_q$, each jellyfish must have size $2 \cdot h_2(\mathcal{O}) \cdot \mathrm{ord}(k)$ and multiplicity $(q-1)/\mathrm{ord}(k)$ by partitioning by the orbits of the action of $\langle k \rangle$.

Chapter 5

Quantum Modularity of 3-Manifold Invariants

We will first discuss the construction of the 3-manifold invariant of interest in this thesis and its connection to invariants in the literature prior to the work of Akhmechet, Johnson, and Krushkal. Then we show how for particular manifolds one can obtain an alternative formulation of the invariant that is amenable to the tools we implement. Following this, we use tools from the theory of quantum modular forms to characterize the behavior of these invariants under the action of $\mathrm{SL}_2(\mathbb{Z})$. This work has already appeared in [32].

5.1 The AJK Series Invariant

This section will present an overview of the construction of the $\widehat{\widehat{Z}}$ invariant, which offers a common refinement of two existing 3-manifold invariants, the GPPV invariant $\widehat{Z}$ [26] and lattice cohomology [38]. This invariant will be defined for a class of manifolds called negative-definite plumbed 3-manifolds, and will require extra data called a spin^c structure. To such a pair, one associates a combinatorial object called a graded root. The authors of [1] determined a method for assigning two-variable Laurent polynomial weights to the vertices of this graded root in a way that preserves invariance. The series $\widehat{\widehat{Z}}_Y(t,q)$ is the result of taking a limit of these weights as the grading increases. Setting $t = 1$ in this series recovers the GPPV invariant $\widehat{Z}(q)$. We will first compute of the $\widehat{\widehat{Z}}$ series for an infinite family of 3-manifolds. Below, we cover details of this construction necessary for our work.

5.1.1 Negative Definite Plumbed Manifolds

Let Γ be a finite tree where the vertices have integer weights. Let $m : v(\Gamma) \to \mathbb{Z}$ be the corresponding weight function and denote $s := |v(\Gamma)|$. Choosing an order on $v(\Gamma)$ enables us to write a weight vector $m \in \mathbb{Z}^s$ given by $m_i = m(v_i)$ and a degree vector $\delta \in \mathbb{Z}^s$ given by $\delta_i = \delta(v_i)$. With this ordering, we can associate to Γ a symmetric $s \times s$ matrix M given by

$$M_{i,j} = \begin{cases} m_i & i = j \\ 1 & i \neq j \text{ and } v_i \text{ and } v_j \text{ are connected by an edge} \\ 0 & \text{otherwise.} \end{cases}$$

We say Γ is negative definite whenever M is negative definite.

To obtain a 3-manifold from Γ, one constructs a framed link $\mathcal{L}(\Gamma) \subset S^3$ by associating to each vertex v_i an unknot with framing m_i and Hopf-linking unknots together whenever their corresponding vertices share an edge. The resulting linking matrix of $\mathcal{L}(\Gamma)$ is the adjacency matrix M. $Y(\Gamma)$ is defined to be the 3-manifold obtained by Dehn surgery on $\mathcal{L}(\Gamma)$. Equivalently, $Y = \partial X$ where X is obtained by adding 2-handles to $\mathbb{D}^4$ along $\mathcal{L}(\Gamma)$. From this perspective, M represents the intersection form of X.

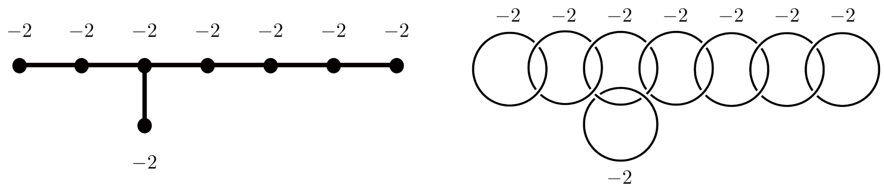

Figure 5.1: A plumbing tree and link for the Poincaré homology sphere $\Sigma(2,3,5)$

In general, we say Y is a negative-definite plumbed 3-manifold if it is homeomorphic to $Y(\Gamma)$ for some negative-definite plumbing graph Γ. Two distinct plumbing trees may result in homeomorphic manifolds; in fact this is the case if and only if the trees can be related by a finite sequence of Neumann moves of type (a) and (b) [39].

As with the GPPV invariant, $\hat{\hat{Z}}_Y(t,q)$ takes as inputs a negative-definite plumbed 3-manifold Y and a chosen spin^c structure. The set of spin^c structures can be given in terms of the plumbing data; it is known that

$$\mathrm{spin}^c(Y) \cong \frac{m + 2\mathbb{Z}^s}{2M\mathbb{Z}^s} \cong \frac{\delta + 2\mathbb{Z}^s}{2M\mathbb{Z}^s}, \tag{5.1.1}$$

where the second isomorphism is given by $[k] \mapsto [k-(m+\delta)]$. For a more detailed discussion of spin^c structures, see Section 2.2 of [1].

Key example: Brieskorn homology spheres

Let (b_1, b_2, b_3) be pairwise relatively prime positive integers $b_1 < b_2 < b_3$. The corresponding Brieskorn sphere $\Sigma(b_1, b_2, b_3)$ is given by

$$\Sigma(b_1,b_2,b_3) = \{(z_1,z_2,z_3) \in \mathbb{C}^3 \ \mid \ z_1^{b_1} + z_2^{b_2} + z_3^{b_3} = 0\} \cap S^5 \subset \mathbb{C}^3,$$

the intersection of a singular complex surface with the unit sphere in $\mathbb{C}^3$. Given (b_1, b_2, b_3), Neumann and Reymond provide an algorithm by which one can find a plumbing tree Γ for the associated Brieskorn sphere [40]. This process guarantees that Γ is always a star graph with one 3-valent vertex and 3 legs, as is the case in Figure 5.1.

As integral homology spheres, Brieskorn spheres have only one spin^c structure, and $\widehat{\widehat{Z}}$ is independent of choice of spin^c representative. Therefore, in calculations involving Brieskorn spheres we will suppress the dependence in the notation.

The general formula for $\widehat{\widehat{Z}}_Y(t, q)$ involves plumbing data, but in Section 5.2 we give a formula for Brieskorn spheres which only depends on (b_1, b_2, b_3). To achieve this, we use methods similar to those of Gukov and Manolescu, who provide a formula for the GPPV invariant in terms of (b_1, b_2, b_3); see Proposition 4.8 of [25].

5.1.2 Construction of the AJK Series

For a choice $k \in \mathbb{Z}^s$ of a spin^c representative $[k] \in \dfrac{m + 2\mathbb{Z}^s}{2M\mathbb{Z}^s}$, and for any $x \in \mathbb{Z}^s$, let

$$\chi_k(x) := \frac{-k \cdot x + \langle x, x\rangle}{2} \in \mathbb{Z},$$

where $(\cdot)$ denotes the Euclidean dot product and $\langle -, -\rangle$ denotes the bilinear form given by the plumbing matrix M. For $r \in \mathbb{Z}$ and $n \in \mathbb{N}$, let

$$\widehat{F}_n(r) := \begin{cases} \frac{1}{2}\mathrm{sgn}(r)^n \binom{\frac{n+|r|}{2}-2}{n-3} & |r| \geq n-2, r \equiv n \pmod 2 \\ 0 & \text{otherwise,} \end{cases} \tag{5.1.2}$$

and define

$$\widehat{F}_{\Gamma,k}(x) := \prod_{v_i \in v(\Gamma)} \widehat{F}_{\delta_i}((2Mx + k - Mu)_i).$$

Note that $\widehat{F}_n(r) : \mathbb{Z} \to \mathbb{Q}$ describes the coefficient on z^{-r} in the expansion of $(z - z^{-1})^{2-n}$. To state the definition of $\widehat{\widehat{Z}}$ we will use for our calculations, we define $u := (1, 1, \ldots)$ as well as

$$\Theta_k = \frac{k \cdot u - \langle u, u\rangle}{2}, \qquad \varepsilon_k = -\frac{(k - Mu)^2 + 3s + \sum_v m_v}{4} + 2\chi_k(x) + \langle x, u\rangle.$$

Then we have the following:

Theorem 5.1 (Theorems 6.3 and 7.6 of [1])**.** *Let Y be a negative-definite plumbed 3-manifold with spin^c structure $[k]$. The series*

$$\widehat{\widehat{Z}}_{Y,[k]}(t, q) := \sum_{x \in \mathbb{Z}^s} \widehat{F}_{\Gamma,k}(x) q^{\varepsilon_k(x)} t^{\Theta_k + \langle x, u\rangle} \tag{5.1.3}$$

is an invariant of the pair $(Y, [k])$, and

$$\widehat{Z}_a(q) = \widehat{\widehat{Z}}_{Y,[k]}(1, q),$$

where $\widehat{Z}_a(q)$ is the GPPV invariant for $(Y, [a])$ and a corresponds to k via (5.1.1)*.*

5.2 Series Analysis

We now develop an explicit formula for the coefficients of $\widehat{\widehat{Z}}_\Sigma(t, q)$ as a series in q whenever Σ is a Brieskorn sphere. The arithmetic properties of these coefficients will allow us to take limits toward roots of unity and establish quantum modularity properties in Theorems 1.10

and 1.11. For a general negative-definite plumbed 3-manifold Y, one can use a program created by Johnson[1] to calculate the first N coefficients of $\widehat{\widehat{\widehat{Z}}}_Y(t,q)$.

Let k be a spin^c representative for the unique spin^c structure $[k]$ of Σ, and set $a = k - Mu$. For $x \in \mathbb{Z}^s$ we let $\ell := a + 2Mx$. Using the fact established in [1] that $\frac{\ell^T M \ell}{4} = \frac{a^2}{4} - 2\chi_k(x) - \langle x, u\rangle$, we write

$$\widehat{\widehat{\widehat{Z}}}_\Sigma(t,q) = q^{-\frac{3s+\sum_v m_v}{4}} \sum_{x\in\mathbb{Z}^s} \prod_{v_i \in v(\Gamma)} \widehat{F}_{\delta_i}(\ell_i) q^{-\frac{\ell^T M^{-1}\ell}{4}} t^{\Theta_k + \langle x,u\rangle}.$$

Below is the plumbing graph of a Brieskorn sphere with the vertices ordered as needed for this section.

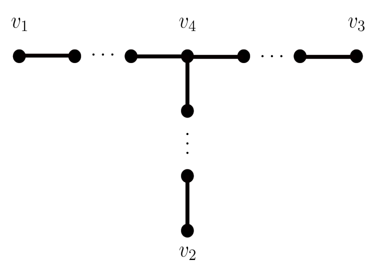

Figure 5.2: The plumbing graph for a general Brieskorn sphere

The only $x \in \mathbb{Z}^s$ for which $\prod_{v_i} \widehat{F}_{\delta_i}(\ell_i) \neq 0$ are those of the form $\ell = (\varepsilon_1, \varepsilon_2, \varepsilon_3, m, 0, \ldots)$ for $\varepsilon_i \in \{\pm 1\}$ and m odd. In this case, we have that $\widehat{F}_1(\varepsilon_i) = -\varepsilon_i$ and $\widehat{F}_3(m) = \frac{1}{2}\mathrm{sign}(m)$, so

$$\prod_{v_i\in v(\Gamma)} \widehat{F}_{\delta_i}(\ell_i) = -\frac{1}{2}\varepsilon_1\varepsilon_2\varepsilon_3 \mathrm{sign}(m).$$

Since Brieskorn spheres have unimodular plumbing matrices M, every possible combination

[1] Available at https://github.com/peterkj1/plum

$(\varepsilon_1, \varepsilon_2, \varepsilon_3, m, 0, \dots)$ is in $a + 2M\mathbb{Z}^s$. Therefore we can write

$$\widehat{\widehat{Z}}_\Sigma(t,q) = \frac{-q^{-\frac{3s+\sum_v m_v}{4}}}{2} \sum_{\varepsilon_i \in \{\pm 1\}} \sum_{m \text{ odd}} \varepsilon_1\varepsilon_2\varepsilon_3 \mathrm{sign}(m) q^{-\frac{\ell^T M^{-1}\ell}{4}} t^{\Theta_k + \langle x,u\rangle}.$$

One can check that $\langle u, x\rangle = \frac{\varepsilon_1+\varepsilon_2+\varepsilon_3+m-a^T u}{2}$. Moreover, since $\widehat{\widehat{Z}}$ does not depend on a choice of spin^c representative, we make the convenient choice of $a = (1,1,1,1,0,\dots) \in \delta + 2M\mathbb{Z}^s$. In this case, $\Theta_k = 2$ and the exponent on t becomes $(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + m)/2$.

Remark 5.2. *Following Section 4.6 of [25] we can can rewrite*

$$\frac{-\ell^t M^{-1}\ell}{4} = \frac{b_1b_2b_3}{4}\left(m + \sum_i \frac{\varepsilon_i}{b_i}\right)^2 - \frac{b_1b_2b_3}{4}\sum \frac{1}{b_i^2} + \frac{\sum_i h_i}{4},$$

where h_i refers to the cardinality of $H_1(\Sigma')$ for Σ' the plumbed manifold that results from removing the ith vertex of the plumbing graph for Σ. Setting

$$\Delta = \frac{1}{4}\left(\sum_i h_i - 3s - \sum_v m_v - \frac{b_2b_3}{b_1} - \frac{b_1b_3}{b_2} - \frac{b_1b_2}{b_3}\right)$$

and $\varepsilon := \varepsilon_1 + \varepsilon_2 + \varepsilon_3$, we now have

$$\widehat{\widehat{Z}}_\Sigma(t,q) = \frac{-q^\Delta}{2} \sum_{m \ odd} \sum_{\varepsilon_i \in \{\pm 1\}} \varepsilon_1\varepsilon_2\varepsilon_3 sign(m) q^{\frac{b_1b_2b_3}{4}(m + \sum_i \frac{\varepsilon_i}{b_i})^2} t^{\frac{\varepsilon + m}{2}}. \tag{5.2.1}$$

Now, set $p := b_1b_2b_3$ and

$$\alpha_1 := b_1b_2b_3 - b_1b_2 - b_1b_3 - b_2b_3;$$

$$\alpha_2 := b_1b_2b_3 + b_1b_2 - b_1b_3 - b_2b_3;$$

$$\alpha_3 := b_1b_2b_3 - b_1b_2 + b_1b_3 - b_2b_3;$$

$$\alpha_4 := b_1b_2b_3 + b_1b_2 + b_1b_3 - b_2b_3.$$

Theorem 5.3. *Let $\Sigma(b_1, b_2, b_3)$ be a Brieskorn sphere. Then*

$$\widehat{\widehat{Z}}_\Sigma(t, q) = q^\Delta \left(C - \sum_{n \geq 1} \varphi(n; t) q^{\frac{n^2}{4p}} \right),$$

where C is nonzero and equals $q^{\frac{1}{120}}(t + t^{-1})$ only when $(b_1, b_2, b_3) = (2, 3, 5)$ and

$$\varphi(n;t) = \begin{cases} \mp\frac{1}{2}(t^{\frac{\mp n+(\alpha_1+2p)}{2p}} + t^{\frac{\pm n-(\alpha_1+2p)}{2p}}) & n \equiv \pm\alpha_1 \pmod{2p}, \\ \pm\frac{1}{2}(t^{\frac{\mp n+\alpha_k}{2p}} + t^{\frac{\pm n-\alpha_k}{2p}}) & n \equiv \pm\alpha_k \pmod{2p},\ k = 2, 3 \\ \mp\frac{1}{2}(t^{\frac{\mp n+(\alpha_4-2p)}{2p}} + t^{\frac{\pm n-(\alpha_4-2p)}{2p}}) & n \equiv \pm\alpha_4 \pmod{2p}, \\ 0 & \textit{otherwise}. \end{cases}$$

Remark 5.4. *Note that when $t = 1$, this collapses back to the GPPV invariant as calculated by Gukov and Manolescu in [25]. Fixing $\Sigma = \Sigma(2, 3, 5)$, the function $\varphi(n; 1)$ is equal to $\chi_+(n)$ as defined in [31].*

Proof. Begin with the calculation given by (5.2.1). Using the fact that $(\varepsilon_1)(\varepsilon_2)(\varepsilon_3)(\text{sign}(m)) = (-\varepsilon_1)(-\varepsilon_2)(-\varepsilon_3)(\text{sign}(-m))$, replacing m odd with $2n + 1$, and setting $\varepsilon' := \frac{\varepsilon+2n+1}{2}$, we write

$$\widehat{\widehat{Z}}_\Sigma(t,q) = \frac{-q^\Delta}{2} \sum_{\varepsilon_i \in \{\pm 1\}} \sum_{n \geq 0} \varepsilon_1\varepsilon_2\varepsilon_3 q^{p(n^2+n+\frac{1}{4}+(n+\frac{1}{2})\sum_i \frac{\varepsilon_i}{b_i}+\frac{1}{4}(\sum_i \frac{\varepsilon_i}{b_i})^2)}(t^{\varepsilon'}+t^{-\varepsilon'}).$$

Following [25], fix ε_2 and ε_3 and split into two cases based on the value of ε_1. If $\varepsilon_1 = -1$, observe that $b_1b_2b_3(1+\sum_i \frac{\varepsilon_i}{b_i}) = \alpha_k$ for some $k \in \{1,2,3,4\}$. The corresponding summation over n for this triple of ε_i's is

$$-\varepsilon_2\varepsilon_3 \sum_{n\geq 0} q^{pn^2+\alpha_k n+\frac{\alpha_k^2}{4p}}(t^{\frac{\varepsilon_2+\varepsilon_3+2n}{2}}+t^{\frac{-(\varepsilon_2+\varepsilon_3+2n)}{2}}). \tag{5.2.2}$$

On the other hand, when $\varepsilon_1 = 1$, we can replace n with $n-1$ in the corresponding sum to get

$$\varepsilon_2\varepsilon_3 \sum_{n\geq 1} q^{pn^2-\alpha_j n+\frac{\alpha_j^2}{4p}}(t^{\frac{\varepsilon_2+\varepsilon_3+2n}{2}}+t^{\frac{-(\varepsilon_2+\varepsilon_3+2n)}{2}}), \tag{5.2.3}$$

where for each k the corresponding j is given by

k	1	2	3	4
j	4	3	2	1.

Remark 5.5. *In [25], it is incorrectly claimed that $j = k$ for each k. This fact does not change the outcome of their calculations, but it does affect ours.*

Summing over all four possible values of $(\varepsilon_2, \varepsilon_3)$ gives eight sums, each of which has exponent on q of the form $pn^2 \pm \alpha_k n + \frac{n^2}{4p}$ as in (5.2.2) and (5.2.3). The sums involving $+\alpha_k n$ begin at $n = 0$ and the sums involving $-\alpha_k n$ begin at $n = 1$. The four values of $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$

for which $\varepsilon_2 = -\varepsilon_3$ contribute

$$\sum_{n\geq 0} q^{pn^2+\alpha_2 n+\frac{\alpha_2^2}{4p}}(t^n+t^{-n}) - \sum_{n\geq 1} q^{pn^2-\alpha_2 n+\frac{\alpha_2^2}{4p}}(t^n+t^{-n});$$

$$\sum_{n\geq 0} q^{pn^2+\alpha_3 n+\frac{\alpha_3^2}{4p}}(t^n+t^{-n}) - \sum_{n\geq 1} q^{pn^2-\alpha_3 n+\frac{\alpha_3^2}{4p}}(t^n+t^{-n}), \tag{5.2.4}$$

whereas when $\varepsilon_2 = \varepsilon_3$ we have

$$-\sum_{n\geq 0} q^{pn^2+\alpha_4 n+\frac{\alpha_4^2}{4p}}(t^{n+1}+t^{-(n+1)}) + \sum_{n\geq 1} q^{pn^2-\alpha_4 n+\frac{\alpha_4^2}{4p}}(t^{n-1}+t^{-(n-1)});$$

$$-\sum_{n\geq 0} q^{pn^2+\alpha_1 n+\frac{\alpha_1^2}{4p}}(t^{n-1}+t^{-(n-1)}) + \sum_{n\geq 1} q^{pn^2-\alpha_1 n+\frac{\alpha_1^2}{4p}}(t^{n+1}+t^{-(n+1)}). \tag{5.2.5}$$

For $t = 1$ and $\alpha_k \geq 0$, each of the above collapse to the false theta functions $\tilde{\Psi}_p^{(\alpha_k)}$ into which $\widehat{Z}$ is decomposed in [25]. The only case in which $\alpha_k < 0$ for some k is $\Sigma(2,3,5)$, for which $\alpha_1 = -1$. We momentarily postpone this case and take $(b_1, b_2, b_3) \neq (2,3,5)$. Working with (5.2.4), we write $pn^2 \pm n\alpha_3 + \frac{a_3^2}{4p} = p(n \pm \frac{\alpha_3}{2p})^2$ and perform the changes of variables $m = 2pn \pm \alpha_3$. This gives

$$\sum_{\substack{m\geq 0\\ m\equiv\alpha_3\ (2p)}} q^{\frac{m^2}{4p}}(t^{\frac{m-\alpha_3}{2p}}+t^{-\frac{m-\alpha_3}{2p}}) - \sum_{\substack{m\geq 0\\ m\equiv-\alpha_3\ (2p)}} q^{\frac{m^2}{4p}}(t^{\frac{m+\alpha_3}{2p}}+t^{-\frac{m+\alpha_3}{2p}}).$$

The calculation is the same when α_3 is replaced with α_2. When $\varepsilon_1 = \varepsilon_3 = 1$, we get the sums

$$-\sum_{\substack{m\geq 0\\ m\equiv\alpha_4\ (2p)}} q^{\frac{m^2}{4p}}(t^{\frac{m-\alpha_4}{2p}+1}+t^{-(\frac{m-\alpha_4}{2p}+1)}) + \sum_{\substack{m\geq 0\\ m\equiv-\alpha_4\ (2p)}} q^{\frac{m^2}{4p}}(t^{\frac{m+\alpha_4}{2p}-1}+t^{-(\frac{m+\alpha_4}{2p}-1)}),$$

and when $\varepsilon_2 = \varepsilon_3 = -1$ we get

$$-\sum_{\substack{m\geq 0\\ m\equiv \alpha_1\ (2p)}} q^{\frac{m^2}{4p}}(t^{\frac{m-\alpha_1}{2p}-1} + t^{-(\frac{m-\alpha_1}{2p}-1)}) + \sum_{\substack{m\geq 0\\ m\equiv -\alpha_1\ (2p)}} q^{\frac{m^2}{4p}}(t^{\frac{m+\alpha_1}{2p}+1} + t^{-(\frac{m+\alpha_1}{2p}+1)}).$$

If $(b_1, b_2, b_3) \neq (2, 3, 5)$ we are done. We conclude with the special case of the Poincaré homology sphere. The argument is the same up through the calculation of (5.2.5). In this case, we have that

$$\begin{aligned}
&-\sum_{n\geq 1} q^{30n^2-n+\frac{1}{120}}(t^{n-1} + t^{-(n-1)}) + \sum_{n\geq 0} q^{30n^2+n+\frac{1}{120}}(t^{n+1} + t^{-(n+1)}) \\
&= -\sum_{\substack{m\geq 0\\ m\equiv -1\ (60)}} q^{\frac{m^2}{120}}(t^{\frac{m-59}{60}} + t^{-(\frac{m-59}{60})}) + \sum_{\substack{m\geq 0\\ m\equiv 1\ (60)}} q^{\frac{m^2}{120}}(t^{\frac{m+59}{60}} + t^{-(\frac{m+59}{60})}),
\end{aligned}$$

and the bounds on the sums on the left hand side do not agree with those in (5.2.5). The solution is to subtract $2q^{\frac{1}{120}}(t + t^{-1})$ from (5.2.5), as they only disagree in the sign of their constant term. $\square$

We end this section with a lemma that will be convenient for the calculations in the following proofs.

Lemma 5.6. *Let α_k, $1 \leq k \leq 4$, be as above. Then $\alpha_1^2 \equiv \alpha_2^2 \equiv \alpha_3^2 \equiv \alpha_4^2 \pmod{4p}$.*

We will denote this common congruence class modulo $4p$ by w for the remainder of the paper.

5.3 Proofs of Theorems

In this section, we prove the main theorems stated in Section 1.3.

5.3.1 Proof of Theorem 1.10

Let ξ be a root of unity and set $C(n) := \varphi(n;\zeta)\xi^{\frac{n^2}{4p}}$. If K is a period of ξ, then $C(n)$ is $2pjK$-periodic and has mean value zero since $C(2pjK-n) = -C(n)$. Let

$$A_\zeta(q) := \sum_{n\geq 0} \varphi(n;\zeta) q^{\frac{n^2}{4p}}, \tag{5.3.1}$$

and observe that

$$A_\zeta(\xi e^{-t}) = \sum_{n=1}^{\infty} C(n) e^{-n^2(t/4p)} \sim \sum_{r=0}^{\infty} L(-2r, C) \frac{(-t/4p)^r}{r!}$$

as $t \to 0^+$ by Proposition 2.21. Then the limiting value is given by

$$A_\zeta(\xi) := \lim_{t\to 0^+} A_\zeta(\xi e^{-t}) = L(0, C),$$

where the analytic continuation of this L-function evaluated at $s=0$ is given by the sum

$$-\sum_{n=1}^{2pjK} \left(\frac{n}{2pjK} - \frac{1}{2}\right) \varphi(n;\zeta)\xi^{\frac{n^2}{4p}}.$$

Evaluating both q^Δ the extra term $C = q^{\frac{1}{120}}(t+t^{-1})$ (which appears only when Σ is the Poincaré homology sphere) at (ζ, ξ) gives the desired formula. $\square$

5.3.2 Proof of Theorem 1.11

In light of the work summarized in Section 2.3, it suffices to show that

$$\sum_{n\geq 0} n\varphi(n;\zeta)q^{\frac{n^2}{4pj}} \tag{5.3.2}$$

is a cusp form for $\Gamma(4pj)$. Then in conjunction with Lemma 2.22, this implies

$$\sum_{n\geq 0} \varphi(n;\zeta)q^{\frac{n^2}{4p}}$$

is a quantum modular form. We begin with an elementary lemma which will be useful for simplifying our expressions later.

Lemma 5.7. *Let $0 \leq n < 2pj$ be such that $n \equiv \pm\alpha_k \pmod{2p}$ for some k. Then we have $n^2 \equiv w + 4pi \pmod{4pj}$ for some $0 \leq i < j$, where w is the common congruence class modulo $4p$ of the α_k^2's coming from Lemma 5.6.*

We are now ready to analyze (5.3.2). Since $\varphi(n;\zeta)$ is $2pj$-periodic, we have

$$\sum_{n\geq 0} n\varphi(n;\zeta)q^{\frac{n^2}{4pj}} = \sum_{0\leq\alpha<2pj} \varphi(\alpha;\zeta)\sum_{n\geq 0}(2pjn+\alpha)q^{\frac{(2pjn+\alpha)^2}{4pj}}.$$

Every α for which $\varphi(\alpha;\zeta)$ is nonzero satisfies $\alpha \equiv \pm\alpha_k \pmod{2p}$ for some k. Thus, we can write this sum as

$$\sum_{\substack{0\leq\alpha<2pj\\ \alpha\equiv\alpha_k(2p)}} \varphi(\alpha,\zeta)\sum_{n\geq 0}(2pjn+\alpha)q^{\frac{(2pjn+\alpha)^2}{4pj}}$$
$$+\sum_{\substack{0<\alpha\leq 2pj\\ \alpha\equiv\alpha_k(2p)}} \varphi(2pj-\alpha,\zeta)\sum_{n\geq 0}(2pjn+(2pj-\alpha))q^{\frac{(2pjn+(2pj-\alpha))^2}{4pj}}.$$

Using the fact that $\varphi(n;\zeta)$ is odd and $2pj$-periodic, the second set of sums can be rewritten as

$$\sum_{\substack{0<\alpha\leq 2pj\\ \alpha\equiv\alpha_k(2p)}} -\varphi(\alpha,\zeta)\sum_{n\geq 0}(2pj(n+1)-\alpha)q^{\frac{(2pj(n+1)-\alpha))^2}{4pj}}.$$

Reindexing by $n+1\mapsto -n$ and combining with the first set of sums gives

$$\sum_{n\geq 0} n\varphi(n;\zeta)q^{\frac{n^2}{4pj}} = \sum_{\substack{0\leq\alpha<2pj\\ \alpha\equiv\alpha_k(2p)}} \varphi(\alpha;\zeta)\sum_{\substack{n\in\mathbb{Z}\\ n\equiv\alpha(2pj)}} nq^{\frac{n^2}{4pj}}. \tag{5.3.3}$$

The inner sum of the above equation is a theta function which is modular of weight 3/2. More precisely, define

$$\Theta(\tau;k,M) := \sum_{\substack{n\in\mathbb{Z}\\ n\equiv k(M)}} nq^{\frac{n^2}{2M}}.$$

By Proposition 2.1 of [47], we have that for $\gamma\in\Gamma_1(2M)$ that

$$\Theta(\gamma\tau;k,M) = e^{\frac{\pi iabk^2}{M}}\varepsilon_d^{-3}\left(\frac{2Mc}{d}\right)(c\tau+d)^{3/2}\Theta(\tau;ak,M),$$

and since $k \equiv ak \pmod{M}$, we have

$$\Theta(z; ak, M) = \Theta(z; k, M).$$

By Lemma 6.1, every n for which the coefficient of $q^{\frac{n^2}{4pj}}$ in (5.3.3) is nonzero satisfies $n^2 \equiv w + 4pi \pmod{4pj}$ for some $0 \leq i < j$. Then

$$e^{\frac{\pi i a b n^2}{2pj}} = e^{\frac{\pi i a b (w+4pi)}{2pj}}$$

for some $0 \leq i < j$. Then one may group the n's based on the corresponding i to get j functions $f_i(\tau)$ which for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(4pj)$ satisfy

$$f_i(\gamma\tau) = e^{\frac{\pi i a b (w+4pi)}{2pj}} \varepsilon_d^{-3} \left(\frac{4pjc}{d}\right) (c\tau + d)^{3/2} f_i(\tau).$$

Note the dependence of this transformation law on w. If one restricts to $\gamma \in \Gamma(4pj) \subset \Gamma_1(4pj)$, the multipliers for each f_i become identical. Thus the sum of the f_i's transform together as a cusp form on $\Gamma(4pj)$. $\square$

5.3.3 Proof of Theorem 1.13

As in the study of the Jacobi Triple Product formula, one is often able to generate a modular object of dual-weight by differentiating with respect to one variable (see e.g. [13]). Following this approach, we find a second infinite family of quantum invariants by differentiating $\hat{\hat{Z}}_\Sigma(t, q)$, summand by summand, with respect to t. Our contribution to this principle is

Theorem 1.13. Here we offer of proof of this result.

Fix ζ a jth root of unity. Consider the series

$$A'_\zeta(\tau) := \sum_{n\geq 0} \varphi'(n;\zeta) q^{\frac{n^2}{4p}},$$

where $\varphi'(n;\zeta)$ is the derivative of $\varphi(n;t)$ evaluated at $t=\zeta$. By Theorem 5.3, this is

$$\varphi'(n;\zeta) := \begin{cases} \frac{n\mp(\alpha_1+2p)}{4p}(\zeta^{\frac{\mp n+(\alpha_1+2p)}{2p}} - \zeta^{\frac{\pm n-(\alpha_1+2p)}{2p}}) & n \equiv \pm\alpha_1 \pmod{2p}, \\ -\frac{n\mp\alpha_k}{4p}(\zeta^{\frac{\mp n+\alpha_k}{2p}} - \zeta^{\frac{\pm n-\alpha_k}{2p}}) & n \equiv \pm\alpha_k \pmod{2p},\ k=2,3 \\ \frac{n\mp(\alpha_4-2p)}{4p}(\zeta^{\frac{\mp n+(\alpha_4-2p)}{2p}} - \zeta^{\frac{\pm n-(\alpha_4-2p)}{2p}}) & n \equiv \pm\alpha_4 \pmod{2p}, \\ 0 & \textit{otherwise.} \end{cases}$$

Note that we may write $A'_\zeta(\tau)$ as

$$\sum_{n\geq 0} n\psi(n;\zeta) q^{\frac{n^2}{4p}} + \sum_{n\geq 0} \chi(n;\zeta) q^{\frac{n^2}{4p}},$$

where

$$\psi(n;\zeta) := \begin{cases} \frac{1}{4p}(\zeta^{\frac{\mp n+(\alpha_1+2p)}{2p}} - \zeta^{\frac{\pm n-(\alpha_1+2p)}{2p}}) & n \equiv \pm\alpha_1 \pmod{2p}, \\ -\frac{1}{4p}(\zeta^{\frac{\mp n+\alpha_k}{2p}} - \zeta^{\frac{\pm n-\alpha_k}{2p}}) & n \equiv \pm\alpha_k \pmod{2p},\ k=2,3 \\ \frac{1}{4p}(\zeta^{\frac{\mp n+(\alpha_4-2p)}{2p}} - \zeta^{\frac{\pm n-(\alpha_4-2p)}{2p}}) & n \equiv \pm\alpha_4 \pmod{2p}, \\ 0 & \textit{otherwise;} \end{cases}$$

$$\chi(n;\zeta) := \begin{cases} \mp\frac{(\alpha_1+2p)}{4p}(\zeta^{\frac{\mp n+(\alpha_1+2p)}{2p}} - \zeta^{\frac{\pm n-(\alpha_1+2p)}{2p}}) & n \equiv \pm\alpha_1 \pmod{2p}, \\ \pm\frac{\alpha_k}{4p}(\zeta^{\frac{\mp n+\alpha_k}{2p}} - \zeta^{\frac{\pm n-\alpha_k}{2p}}) & n \equiv \pm\alpha_k \pmod{2p},\ k=2,3 \\ \mp\frac{(\alpha_4-2p)}{4p}(\zeta^{\frac{\mp n+(\alpha_4-2p)}{2p}} - \zeta^{\frac{\pm n-(\alpha_4-2p)}{2p}}) & n \equiv \pm\alpha_4 \pmod{2p}, \\ 0 & \textit{otherwise.} \end{cases}$$

Then $\psi(n;\zeta)$ is even and $2pj$-periodic and $\chi(n;\zeta)$ is odd and $2pj$-periodic. Following the same style of argument as Theorem 1.11, one concludes that $\sum_{n\geq 0} \chi(n;\zeta)q^{\frac{n^2}{4p}}$ is a quantum modular form of weight 1/2 on $\Gamma(4pj^2)$.

To analyze $\sum_{n\geq 0} n\psi(n;\zeta)q^{\frac{n^2}{4p}}$, note that the series $\sum_{n\geq 0} \psi(n;\zeta)q^{\frac{n^2}{4p}}$ is modular but may not be a cusp form. This requires us to appeal to a more general result of Goswami and Osburn (Theorem 1.1 of [21]) which gives a careful treatment of this more general case. Their result tells us that

$$\sum_{n\geq 0} n\psi(n;\zeta)q^{\frac{n^2}{4pj}}$$

is a quantum modular form on Q_{2pj} with respect to $\Gamma_1(4pj)$, where

$$Q_{2pj} := \{x \in \mathbb{Q} \ : \ x \text{ is } \Gamma_1(4pj) - \text{equivalent to } i\infty\}.$$

Note that one must still utilize Lemmas 2.22 and 5.7 in order to contend with the supports of these series. This ultimately allows us to conclude that $\sum_{n\geq 0} n\psi(n;\zeta)q^{\frac{n^2}{4p}}$ is a quantum modular form of weight 3/2 as desired. □

Bibliography

[1] R. Akhmechet, P. K. Johnson, and V. Krushkal, *Lattice cohomology and q-series invariants of* 3*-manifolds*, Journal für die reine und angewandte Mathematik (Crelles Journal) **2023** (2023), no. 796, 269–299.

[2] G. Almkvist, *Asymptotics of the number of partitions into p-cores and some trigonometric sums*, arXiv preprint arXiv:0806.3163 (2008).

[3] J. M. Borwein and P. B. Borwein, *Pi and the AGM: A Study in the Analytic Number Theory and Computational Complexity*, Wiley-Interscience, 1987.

[4] K. Bringmann, A. Folsom, K. Ono, and L. Rolen, *Harmonic Maass forms and mock modular forms: theory and applications*, vol. 64, American Mathematical Soc., 2017.

[5] K. Bringmann, K. Mahlburg, and A. Milas, *Higher depth quantum modular forms and plumbed* 3*-manifolds*, Letters in Mathematical Physics **110** (2020), no. 10, 2675–2702.

[6] ______, *Quantum modular forms and plumbing graphs of* 3*-manifolds*, Journal of Combinatorial Theory, Series A **170** (2020), 105145.

[7] K. Bringmann and L. Rolen, *Half-integral weight Eichler integrals and quantum modular forms*, Journal of Number Theory **161** (2016), 240–254.

[8] B. Brown, N. J. Calkin, T. B. Flowers, K. James, E. Smith, and A. Stout, *Elliptic curves, modular forms, and sums of Hurwitz class numbers*, Journal of Number Theory **128** (2008), no. 6, 1847–1863.

[9] J. Bryson, K. Ono, S. Pitman, and Robert C Rhoades, *Unimodal sequences and quantum and mock modular forms*, Proceedings of the National Academy of Sciences **109** (2012), no. 40, 16063–16067.

[10] M. C. N. Cheng, S. Chun, F. Ferrari, S. Gukov, and S. M. Harrison, *3d modularity*, Journal of High Energy Physics **2019** (2019), no. 10, 1–95.

[11] D. Choi, S. Lim, and R. C. Rhoades, *Mock modular forms and quantum modular forms*, Proceedings of the American Mathematical Society **144** (2016), no. 6, 2337–2349.

[12] H. Cohen, *A course in computational algebraic number theory*, vol. 138, Springer Science & Business Media, 2013.

[13] G. Coogan and K. Ono, *A q-series identity and the arithmetic of Hurwitz zeta functions*, Proceedings of the American Mathematical Society **131** (2003), no. 3, 719–724.

[14] S. Das, *Asymptotic properties of maximal p-core p-partitions*, Journal of Combinatorial Theory, Series A **193** (2023), 105685.

[15] M. Deuring, *Die typen der multiplikatorenringe elliptischer funktionenkörper*, Abhandlungen aus dem mathematischen Seminar der Universität Hamburg, vol. 14, Springer Berlin/Heidelberg, 1941, pp. 197–272.

[16] M. Eichler, *On the class number of imaginary quadratic fields and the sums of divisors of natural numbers*, J. Ind. Math. Soc **15** (1955), 153–180.

[17] K. Erdmann and G. Michler, *Blocks for symmetric groups and their covering groups and quadratic forms*, Contributions to algebra and geometry **37** (1996), 103–118.

[18] A. Folsom, K. Ono, and R. C. Rhoades, *Mock theta functions and quantum modular forms*, Forum of mathematics, Pi, vol. 1, Cambridge University Press, 2013, p. e2.

[19] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, International Algorithmic Number Theory Symposium, Springer, 2002, pp. 276–291.

[20] F. Garvan, D. Kim, and D. Stanton, *Cranks and t-cores*, Invent. Math. **101** (1990), 1–17.

[21] A. Goswami and R. Osburn, *Quantum modularity of partial theta series with periodic coefficients*, Forum Mathematicum **33** (2021), no. 2, 451–463.

[22] A. Granville and K. Ono, *Defect zero p-blocks for finite simple groups*, Trans. Amer. Math. Soc. **348** (1996), 331–347.

[23] M. J. Griffin, K. Ono, and L. Rolen, *Ramanujan's mock theta functions*, Proceedings of the National Academy of Sciences **110** (2013), 5765 – 5768.

[24] M. J. Griffin, K. Ono, N. Saikia, and W-L. Tsai, *AGM and jellyfish swarms of elliptic curves*, The American Mathematical Monthly. DOI: 10.1080/00029890.2022.2160157 (2023).

[25] S. Gukov and C. Manolescu, *A two-variable series for knot complements*, Quantum Topol. **12** (2021), no. 1, 1–109.

[26] S. Gukov, D. Pei, P. Putrov, and C. Vafa, *BPS spectra and* 3*-manifold invariants*, J. Knot Theory Ramifications **29** (2020), no. 2.

[27] S. Gukov, P. Putrov, and C. Vafa, *Fivebranes and* 3*-manifold homology*, Journal of High Energy Physics **2017** (2017), no. 7, 1–82.

[28] G. James and A. Kerber, *Representation theory of the symmetric group*, Cambridge Univ. Press, 1984.

[29] A. Klyachko, *Modular forms and representations of symmetric groups, integral lattices, and finite linear groups*, Zap. Nauchn. Sem. Leningrad Otdel. Mat. Inst. Steklov **116** (1982), 74–85.

[30] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*, University of California, Berkeley, 1996.

[31] R. Lawrence and D. Zagier, *Modular forms and quantum invariants of* 3*-manifolds*, Asian Journal of Mathematics **3** (1999), no. 1, 93–108.

[32] L. Liles and E. McSpirit, *Infinite Families of Quantum Modular 3-Manifold Invariants*, Communications in Number Theory and Physics (2024), Accepted for Publication.

[33] E. McDowell, *Large p-core p-partitions and walks on the additive residue graph*, Annals of Combinatorics **27** (2023), no. 4, 857–871.

[34] E. McSpirit and K. Ono, *Hypergeometry and the AGM over finite fields*, Contemporary Mathematics, American Mathematical Society (2023), Accepted for Publication.

[35] ______, *Zeros in the character tables of symmetric groups with an ℓ-core index*, Canadian Mathematical Bulletin **66** (2023), no. 2, 467–476.

[36] M. H. Mertens, *Mock modular forms and class number relations*, Research in the Mathematical Sciences **1** (2014), 1–16.

[37] T. Miyake, *Modular forms*, Springer Science & Business Media, 2006.

[38] A. Némethi, *On the Ozsváth-Szabó invariant of negative definite plumbed* 3*-manifolds*, Geometry & Topology **9** (2005), no. 2, 991–1042.

[39] W. D. Neumann, *A calculus for plumbing applied to the topology of complex surface singularities and degenerating complex curves*, Transactions of the American Mathematical Society **268** (1981), no. 2, 299–344.

[40] W. D. Neumann and F. Raymond, *Seifert manifolds, plumbing, μ-invariant and orientation reversing maps*, Algebraic and Geometric Topology: Proceedings of a Symposium held at Santa Barbara in honor of Raymond L. Wilder, July 25–29, 1977, Springer, 2006, pp. 163–196.

[41] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, no. 102, American Mathematical Soc., 2004.

[42] K. Ono and L. Sze, *4-core partitions and class numbers*, Acta Arith. **80** (1997), 249–272.

[43] Jr. P. Hagis, *Partitions with a restriction on the multiplicity of the summands*, Trans. Amer. Math. Soc. **155** (1971), 375–384.

[44] N. Reshetikhin and V. G. Turaev, *Invariants of* 3*-manifolds via link polynomials and quantum groups*, Inventiones mathematicae **103** (1991), no. 1, 547–597.

[45] R. Schoof, *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory, Series A **46** (1987), no. 2, 183–211.

[46] J.-P. Serre and H. M. Stark, *Modular forms of weight 1/2*, Modular Functions of One Variable VI: Proceedings International Conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik July 2–14, 1976, Springer, 2006, pp. 27–67.

[47] G. Shimura, *Modular forms of half integral weight*, Modular Functions of One Variable I: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972, Springer, 1973, pp. 57–74.

[48] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, vol. 151, Springer Science & Business Media, 1994.

[49] ——, *The arithmetic of elliptic curves*, vol. 106, Springer, 2009.

[50] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones mathematicae **2** (1966), no. 2, 134–144.

[51] W. C. Waterhouse, *Abelian varieties over finite fields*, Annales scientifiques de l'École normale supérieure, vol. 2, 1969, pp. 521–560.

[52] E. Witten, *Quantum field theory and the Jones polynomial*, Communications in Mathematical Physics **121** (1989), no. 3, 351–399.

[53] D. Zagier, *Nombres de classes et formes modulaires de poids 3/2*, Séminaire de Théorie des Nombres de Bordeaux **4** (1974), 1–2.

[54] ——, *Vassiliev invariants and a strange identity related to the dedekind eta-function*, Topology **40** (2001), no. 5, 945–960.

[55] ——, *Quantum modular forms*, Quanta of maths **11** (2010), 659–675.