Distribution Agreement

Signature:

______________________________ __________

Madeline Locus Dawsey Date

New Results on Partitions, Prime Numbers, and Moonshine

By

Madeline Locus Dawsey

Doctor of Philosophy

Mathematics

Ken Ono

Advisor

David Borthwick

Committee Member

John Duncan

Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.

Dean of the James T. Laney School of Graduate Studies

Date

New Results on Partitions, Prime Numbers, and Moonshine

By

Madeline Locus Dawsey

B.S., University of Georgia, 2014

Advisor: Ken Ono, Ph.D.

An abstract of

A dissertation submitted to the Faculty of the

James T. Laney School of Graduate Studies of Emory University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in Mathematics

2019

Abstract

New Results on Partitions, Prime Numbers, and Moonshine

By Madeline Locus Dawsey

In this thesis, we prove new results in combinatorics, analytic number theory, and representation theory. In particular, in combinatorics we prove conjectured inequalities regarding the Andrews smallest parts partition function by first establishing effective estimates using new methods from the theory of quadratic forms. In addition, we provide recurrence relations for the coefficients of conjugacy growth series for wreath products of finitary permutation groups, which essentially measure the algebraic complexity of these groups. In analytic number theory, we apply the Chebotarev Density Theorem in order to generalize a theorem of Alladi on the distribution of primes in arithmetic progressions. More precisely, we reproduce the Chebotarev densities of certain subsets of prime numbers through an infinite sum involving the Möbius function, where we sum over only those integers whose smallest prime divisors fall in the specified subsets. Finally, we refine the theory of moonshine so that the modular forms associated to the representation theory of all finite groups uniquely determine those groups up to isomorphism. We obtain this "higher width moonshine" for all finite groups by employing the classical Frobenius r-characters, which we prove satisfy orthogonality relations analogous to Schur's orthogonality relations for ordinary group characters.

New Results on Partitions, Prime Numbers, and Moonshine

By

Madeline Locus Dawsey

B.S., University of Georgia, 2014

Advisor: Ken Ono, Ph.D.

A dissertation submitted to the Faculty of the

James T. Laney School of Graduate Studies of Emory University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in Mathematics

2019

Acknowledgments

I would like to thank my advisor, Ken Ono, for his advice and constant encouragement. He is a wonderfully inspiring mathematician, teacher, and mentor, and I hope to follow his great example in the years to come. Many others have helped and encouraged me throughout graduate school, including Olivia Beckwith, Lea Beneish, Bree Ettinger, Marie Jameson, Robert Lemke Oliver, Riad Masri, and Jesse Thorner. I especially thank Amanda Folsom for several enriching conversations and for being an advocate of math graduate students and young math professors. Finally, I thank my family and friends for all of their support.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the eighteenth century, Euler played an integral role in the advancement of modern number theory. Among other important works in the mathematical sciences, he discovered the formula, now called an Euler product representation, which relates the Riemann zeta function to the prime numbers. This relationship paved the way for the development of analytic number theory by Dirichlet, who proved the very first result on the distribution of primes in arithmetic progressions in 1837. The impetus for Dirichlet's Theorem was Gauss's 1796 conjecture of the most fundamental density statement regarding the primes: if $\pi(X)$ counts the number of primes up to X, then

$$\lim_{X\to\infty} \frac{\pi(X)\log X}{X} = 1.$$

Riemann's revolutionary ideas and powerful analytic constructions, published in his famous 1859 paper on number theory, were crucial to the progress of mathematicians toward understanding the primes. Gauss's conjecture, now known as the Prime Number Theorem, was proven independently a century after its formulation by Hadamard and de la Vallée Poussin using analysis and special properties of the Riemann zeta function which built on Riemann's work.

These examples demonstrate the advantage of using analytic techniques to study problems in number theory. Over time, number theory has developed into a multifaceted field with branches in many other areas of mathematics. It is clear from the innovative work of Euler, Dirichlet, Riemann, and many others that this amalgamation of fields provides the potential for a deeper understanding of the integers and their building blocks, the primes. Although elementary proof methods remain common, techniques and results from other fields open countless doors in the theory of numbers. Here we focus on number theoretic problems which require combinatorics, algebra and analysis, and representation theory.

1.1 Partitions

The most basic construction in combinatorial number theory is a *partition* of a positive integer n, which is defined as a non-increasing sequence of positive integers which sum to n. The *partition function* $p(n)$ counts the number of partitions of n. For example, the partitions of 4 are

$$4, \quad 3+1, \quad 2+2, \quad 2+1+1, \quad \text{and} \quad 1+1+1+1,$$

and so $p(4) = 5$. Euler proved that the generating function for $p(n)$ can be represented as an infinite product; namely, we have that

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n}, \tag{1.1}$$

where throughout $q := e^{2\pi i\tau}$ with τ in the upper half of the complex plane $\mathbb{H}$. The Euler product representation (1.1) follows from the fundamental theorem of arithmetic, since the coefficients of the right hand side, when expanded as a product of geometric series, count the number of partitions corresponding to each exponent.

Ramanujan offered groundbreaking theorems on partitions in the early 1900s, initially in isolation but eventually at Cambridge with G. H. Hardy. After calculating several values of $p(n)$ by hand, he discovered many interesting arithmetic properties, including the well-known Ramanujan congruences [47–50]:

$$\begin{aligned} p(5n+4) &\equiv 0 \pmod{5}, \\ p(7n+5) &\equiv 0 \pmod{7}, \\ p(11n+6) &\equiv 0 \pmod{11}. \end{aligned}$$

Seeking a general estimate for the size of $p(n)$, Hardy and Ramanujan developed what is now called the circle method, which allows one to calculate an asymptotic formula for a sequence by computing residues of its generating function, carefully choosing a circular contour of integration which avoids singularities at roots of unity. Using this method, they proved the illustrious Hardy–Ramanujan asymptotic [32]:

$$p(n) \sim \frac{1}{4n\sqrt{3}}\, e^{\pi\sqrt{\frac{2n}{3}}}. \tag{1.2}$$

A refinement of the circle method by Rademacher in 1937 produced the following exact formula for $p(n)$ [46], the first term of which gives (1.2):

$$p(n) = \frac{2\pi}{(24n-1)^{3/4}} \sum_{c=0}^{\infty} \frac{A_c(n)}{c} I_{3/2}\left(\frac{\pi\sqrt{24n-1}}{6c}\right), \tag{1.3}$$

where $A_c(n)$ is a Kloosterman sum and I_ν is the weight ν I-Bessel function. All of the above results on partitions depend on the fact that the Euler product (1.1) is essentially (up to a power of q) a modular form (see Section 2.1).

1.1.1 The Andrews smallest parts partition function

We study these types of problems regarding a different kind of partition function introduced by Andrews, which he named the *smallest parts partition function*. This function, spt(n), counts the number of smallest parts among all of the partitions of n. For example, the partitions of 4 with smallest parts underlined are

$$\underline{4}, \quad 3+\underline{1}, \quad \underline{2}+\underline{2}, \quad 2+\underline{1}+\underline{1}, \quad \text{and} \quad \underline{1}+\underline{1}+\underline{1}+\underline{1},$$

and so spt(4) = 10. Andrews proved [3] in 2008 that the generating function for spt(n) is given by

$$\sum_{n=1}^{\infty} \operatorname{spt}(n) q^n = \sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2 (q^{n+1};q)_\infty}, \tag{1.4}$$

where $(a;q)_\infty := \prod_{n\geq 0}(1-aq^n)$ is the ordinary infinite q-Pochhammer symbol. The function (1.4) is essentially a mock modular form. In other words, (1.4) is the (non-modular) holomorphic part of a harmonic Maass form, which is a non-holomorphic analogue of a modular form (see Section 2.2). Despite this, spt(n) enjoys many properties similar to those of $p(n)$. For example, spt(n) satisfies Andrews's Ramanujan-like congruences [3]:

$$\begin{aligned} \operatorname{spt}(5n+4) &\equiv 0 \pmod{5}, \\ \operatorname{spt}(7n+5) &\equiv 0 \pmod{7}, \\ \operatorname{spt}(13n+6) &\equiv 0 \pmod{13}. \end{aligned}$$

Also, Bringmann proved the following asymptotic formula [6]:

$$\operatorname{spt}(n) \sim \frac{\sqrt{6n}}{\pi} p(n) \sim \frac{1}{\pi\sqrt{8n}} e^{\pi\sqrt{\frac{2n}{3}}}, \tag{1.5}$$

and in 2016 Ahlgren and Andersen proved [1] the following Rademacher-type formula:

$$\operatorname{spt}(n) = \frac{\pi}{6}(24n-1)^{1/4} \sum_{c=1}^{\infty} \frac{A_c(n)}{c} \left(I_{1/2} - I_{3/2}\right) \left(\frac{\pi\sqrt{24n-1}}{6c}\right). \tag{1.6}$$

Recently, Chen conjectured [11] six inequalities for $\mathrm{spt}(n)$ which had already been proven true for $p(n)$ using Lehmer's effective bounds [39] of Rademacher's formula.

Conjecture (Chen)**.**

1. *For* $n \geq 5$*, we have that* $\frac{\sqrt{6}}{\pi}\sqrt{n}\, p(n) < \mathrm{spt}(n) < \sqrt{n}\, p(n)$.
2. *For* $(a,b) \neq (2,2)$ *or* $(3,3)$*, we have that* $\mathrm{spt}(a+b) < \mathrm{spt}(a)\,\mathrm{spt}(b)$.
3. *For* $n \geq 36$*, we have that* $\mathrm{spt}(n-1)\,\mathrm{spt}(n+1) < \mathrm{spt}(n)^2$.
4. *For* $n > m > 1$*, we have that* $\mathrm{spt}(n-m)\,\mathrm{spt}(n+m) < \mathrm{spt}(n)^2$.
5. *For* $n \geq 13$*, we have that* $\mathrm{spt}(n)^2 < \mathrm{spt}(n-1)\,\mathrm{spt}(n+1)\left(1+\frac{1}{n}\right)$.
6. *For* $n \geq 73$*, we have that* $\mathrm{spt}(n)^2 < \mathrm{spt}(n-1)\,\mathrm{spt}(n+1)\left(1+\frac{\pi}{\sqrt{24}n^{3/2}}\right)$.

In joint work with Masri [19], we prove all of the above inequalities.

Theorem 1.1.1 (D–Masri)**.** *All of Chen's conjectures are true.*

In order to prove the conjectures, one must first effectively bound $\mathrm{spt}(n)$. The difficulty of this task stems from the conditional convergence of the Ahlgren–Andersen formula (1.6) for $\mathrm{spt}(n)$, which stands in contrast to Rademacher's absolutely convergent formula (1.3) for $p(n)$. We prove [19] an effective bound using new methods.

Theorem 1.1.2 (D–Masri)**.** *Let* $\lambda(n) := \frac{\pi\sqrt{24n-1}}{6}$*. Then for all* $n \geq 1$*, we have that*

$$\mathrm{spt}(n) = \frac{\sqrt{3}}{\pi\sqrt{24n-1}} e^{\lambda(n)} + E_s(n),$$

where

$$|E_s(n)| < \left(3.59 \times 10^{22}\right) 2^{q(n)} (24n-1)^2 e^{\lambda(n)/2}$$

with

$$q(n) := \frac{\log(24n-1)}{|\log(\log(24n-1)) - 1.1714|}.$$

1.1.2 Finitary permutation groups

The ordinary partition function also turns out to have a connection with the so-called infinite finitary permutation groups and their wreath products. For an infinite set X, the *finitary symmetric group* $\mathrm{Sym}(X)$ is the group of permutations of X with finite support. The *symmetric wreath product* of a group H with $\mathrm{Sym}(X)$ is defined as the group $H \wr_X \mathrm{Sym}(X) := H^{(X)} \rtimes \mathrm{Sym}(X)$ with the following properties:

1. The group $H^{(X)}$ is the group of functions from X to H with finite support.

2. The action of permutations $f \in \mathrm{Sym}(X)$ on functions $\psi \in H^{(X)}$ is defined by $\psi \mapsto f(\psi) := \psi \circ f^{-1}$.

3. Multiplication in the semidirect product is defined for functions $\varphi, \psi \in H^{(X)}$ and permutations $f, g \in \mathrm{Sym}(X)$ by $(\varphi, f)(\psi, g) = (\varphi f(\psi), fg)$.

The *finitary alternating group* $\mathrm{Alt}(X)$ is the subgroup of $\mathrm{Sym}(X)$ of even permutations, and the *alternating wreath product* $H \wr_X \mathrm{Alt}(X)$ is defined analogously.

We now define some statistics which are used to analytically measure the algebraic complexity of these groups. Let G be a group generated by a set S. The *word length* $\ell_{G,S}(g)$ of any element $g \in G$ is the minimal positive integer n such that there exist $s_1, \ldots, s_n$ in $S \cup S^{-1}$ with $g = s_1 \cdots s_n$. The *conjugacy length* $\kappa_{G,S}(g)$ is the minimal word length appearing in the conjugacy class of g. For any positive integer n, we define $\gamma_{G,S}(n) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ to be the number of conjugacy classes in G with minimal word length n. If $\gamma_{G,S}(n)$ is finite for all n, then the *conjugacy growth series* of G is

$$C_{G,S}(q) := \sum_{[g] \in \mathrm{Conj}(G)} q^{\kappa_{G,S}(g)} = \sum_{n=0}^{\infty} \gamma_{G,S}(n) q^n,$$

where the first sum is over representatives of conjugacy classes of G.

Bacher and de la Harpe recently proved [4] conjugacy growth series identities for sufficiently large generating sets (see [4] for details) S of $\mathrm{Sym}(X)$, S' of $\mathrm{Alt}(X)$, and

$S^{(W_S)}$ of the symmetric wreath product $W_S := H_S \wr_X \mathrm{Sym}(X)$ which relate these groups to the partition function. Explicitly, they obtained the fascinating identities

$$C_{\mathrm{Sym}(X),S}(q) = \sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n}$$

for the finitary symmetric group,

$$C_{\mathrm{Alt}(X),S'}(q) = \left(\sum_{n=0}^{\infty} p(n)q^n\right)\left(\sum_{m=0}^{\infty} p_e(m)q^m\right) = \frac{1}{2}\prod_{n=1}^{\infty} \frac{1}{(1-q^n)^2} + \frac{1}{2}\prod_{n=1}^{\infty} \frac{1}{1-q^{2n}}$$

for the finitary alternating group, where $p_e(m)$ denotes the number of partitions of m into an even number of parts, and

$$C_{W_S,S^{(W_S)}}(q) = \left(\sum_{n=0}^{\infty} p(n)q^n\right)^{M_S} = \prod_{n=1}^{\infty} \frac{1}{(1-q^n)^{M_S}} \tag{1.7}$$

for wreath products $W_S = H_S \wr_X \mathrm{Sym}(X)$, where M_S is the number of conjugacy classes of H_S. Following their method, we prove [17] an analogous conjugacy growth series identity for alternating wreath products. We omit the proof, since it also appears in [57].

Theorem 1.1.3 (D and Wagner)**.** *Let H_A be a finite group with M_A conjugacy classes, X an infinite set, and W_A an alternating wreath product of H_A generated by a sufficiently large set $S^{(W_A)}$. Then we have that*

$$\begin{aligned} C_{W_A,S^{(W_A)}}(q) &= \left(\sum_{n=0}^{\infty} p(n)q^n\right)^{M_A} \left(\sum_{m=0}^{\infty} p_e(m)q^m\right)^{M_A} \\ &= \left(\frac{1}{2}\prod_{n=1}^{\infty} \frac{1}{(1-q^n)^2} + \frac{1}{2}\prod_{n=1}^{\infty} \frac{1}{1-q^{2n}}\right)^{M_A}. \end{aligned} \tag{1.8}$$

From now on, we assume sufficiently large generating sets, so that we may simply denote the conjugacy growth series for W by $C_W(q)$ and its coefficients by $\gamma_W(n)$.

For symmetric wreath products $W_S = H_S \wr_X \mathrm{Sym}(X)$ and alternating wreath products $W_A = H_A \wr_X \mathrm{Alt}(X)$, the quantities $\gamma_{W_S}(n)$ and $\gamma_{W_A}(n)$ are naturally functions of the number of conjugacy classes of H_S and H_A through (1.7) and (1.8). Using this relationship, we obtain [17] a recursive formula for these numbers. These results require the ordinary divisor function

$$\sigma_k(n) := \sum_{d|n} d^k \tag{1.9}$$

and the *universal polynomial of partitions* $\widehat{F}_n$ defined for $n \geq 2$ by

$$\widehat{F}_n(x_1, \ldots, x_{n-1}) := \sum_{\substack{m_1,\ldots,m_{n-1}\geq 0 \\ m_1+\cdots+(n-1)m_{n-1}=n}} (-1)^{m_1+\cdots+m_{n-1}} \cdot \frac{(m_1+\cdots+m_{n-1}-1)!}{m_1!\cdots m_{n-1}!} \cdot x_1^{m_1}\cdots x_{n-1}^{m_{n-1}}.$$

Remark. The polynomials $\widehat{F}_n$ are fairly straightforward to compute using only the partitions of n. The first three $\widehat{F}_n$ are listed below.

$$\begin{aligned}
\widehat{F}_2(x_1) &= \frac{1}{2}x_1^2, \\
\widehat{F}_3(x_1, x_2) &= -\frac{1}{3}x_1^3 + x_1x_2, \\
\widehat{F}_4(x_1, x_2, x_3) &= \frac{1}{4}x_1^4 - x_1^2x_2 + \frac{1}{2}x_2^2 + x_1x_3.
\end{aligned}$$

Theorem 1.1.4 (D)**.** *Let H_S be a finite group with M_S conjugacy classes, and let W_S be a symmetric wreath product of H_S. Then we have that*

$$\gamma_{W_S}(n) = \widehat{F}_n\big(\gamma_{W_S}(1), \ldots, \gamma_{W_S}(n-1)\big) + \frac{M_S}{n} \cdot \sigma_1(n).$$

Theorem 1.1.4 has an application to the Nekrasov-Okounkov hook length formula (see Section 3.3.2). We also prove [17] a recursion for alternating wreath products.

Theorem 1.1.5 (D)**.** *Let H_A be a finite group with M_A conjugacy classes, and let W_A be an alternating wreath product of H_A. Then we have that*

$$\gamma_{W_A}(n) = \frac{1}{2^{M_A}} \sum_{k=0}^{M_A} \binom{M_A}{k} \Bigg(\widehat{F}_n\big(a_k(1), \ldots, a_k(n-1)\big) - \sum_{\delta | n} \delta \cdot \left[(-1)^{\delta}(k - M_A) - (k + M_A)\right] \Bigg),$$

where the a_k are defined by their generating function

$$\sum_{n=0}^{\infty} a_k(n) q^n := \prod_{n=1}^{\infty} \frac{1}{(1-q^n)^{2k} (1-q^{2n})^{M_A - k}}.$$

In [17], we additionally provide asymptotics for $\gamma_{W_S}(n)$, $\gamma_{W_A}(n)$, and certain ratios using Ingham's Tauberian Theorem. These results are not discussed here.

In Chapter 2, we introduce the theory of modular forms and harmonic Maass forms which is crucial to the proofs in Chapters 3 and 5.

In Chapter 3, we give background information on quadratic forms in Section 3.1. We prove Theorems 1.1.1 and 1.1.2 in Section 3.2. We then prove Theorems 1.1.4 and 1.1.5 and give an application to hook lengths of partitions in Section 3.3.

1.2 Prime numbers

The prime numbers are intimately related to the Riemann zeta function, which is defined for $\mathrm{Re}(s) > 1$ by the Dirichlet series $\zeta(s) := \sum_{n \geq 1} n^{-s}$. Using the Euler product representation $\zeta(s) = \prod_{p,\,\text{prime}} (1 - p^{-s})^{-1}$, it is straightforward to show that

$$\lim_{s \to 1^+} \zeta(s)^{-1} = \prod_{p,\,\text{prime}} \left(1 - \frac{1}{p}\right) = \lim_{X \to \infty} \sum_{n=1}^{X} \frac{\mu(n)}{n}, \tag{1.10}$$

where the Möbius function $\mu(n)$ is defined by

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is not squarefree,} \\ (-1)^r & \text{if } n = p_1 \cdots p_r \text{ for distinct primes } p_1, \ldots, p_r. \end{cases}$$

Since $\zeta(s)$ has a pole at $s = 1$, the relationship (1.10) implies that

$$\lim_{X\to\infty} \sum_{n=1}^{X} \frac{\mu(n)}{n} = 0. \tag{1.11}$$

We now subtract the first term from both sides of (1.11) to obtain

$$-\lim_{X\to\infty} \sum_{n=2}^{X} \frac{\mu(n)}{n} = 1. \tag{1.12}$$

We may interpret (1.12) as a density statement by summing instead over certain natural restrictions of the integers $n \geq 2$. To make sense of this, let $p_{\min}(n)$ $\big($resp. $p_{\max}(n)\big)$ denote the smallest (resp. largest) prime divisor of n. As usual, let $\varphi(k)$ denote Euler's φ-function, which counts the number of positive integers up to k that are relatively prime to k. Alladi proved [2] in 1977 that if $\gcd(\ell, k) = 1$, then

$$-\lim_{X\to\infty} \sum_{\substack{2\leq n\leq X \\ p_{\min}(n)\equiv \ell \pmod{k}}} \frac{\mu(n)}{n} = \frac{1}{\varphi(k)}. \tag{1.13}$$

Alladi's theorem is reminiscent of Dirichlet's famous theorem on primes in arithmetic progressions, which guarantees the existence of infinitely many primes in any arithmetic progression $\ell \pmod{k}$ with $\gcd(\ell, k) = 1$. More precisely, Dirichlet proved that a prime is likely to fall in a fixed allowable arithmetic progression modulo k with probability $1/\varphi(k)$. Alladi also proved [2] a beautiful duality principle: if f is a function defined on integers with $f(1)=0$, then by Möbius inversion we have that

$$\sum_{d|n}\mu(d)f\big(p_{\max}(d)\big)=-f\big(p_{\min}(n)\big) \text{ and } \sum_{d|n}\mu(d)f\big(p_{\min}(d)\big)=-f\big(p_{\max}(n)\big). \tag{1.14}$$

Combined with Dirichlet's Theorem, (1.14) implies that *largest* prime divisors $p_{\max}(n)$ are equidistributed in allowable arithmetic progressions modulo k.

We generalize Alladi's results to reproduce densities of further subsets of the integers $n\geq 2$. To explain, we require some basic algebraic number theory. Suppose that K is a Galois extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$. Let p be a prime unramified in K, i.e. $p\mathcal{O}_K$ is a product of distinct prime ideals in $\mathcal{O}_K$, and let $\mathfrak{p}\subseteq\mathcal{O}_K$ be a prime ideal lying above p. Then the Artin symbol $\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right]$ is defined as the element $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ which maps every $a\in K$ to $a^p \pmod{\mathfrak{p}}$. We define $\left[\frac{K/\mathbb{Q}}{p}\right]$ to be the set $\left\{\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right]:\mathfrak{p}\subseteq\mathcal{O}_K \text{ lies above } p\right\}$. Then $\left[\frac{K/\mathbb{Q}}{p}\right]$ is a conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$.

We prove the following density statement [18].

Theorem 1.2.1 (D)**.** *Let K be a finite Galois extension of $\mathbb{Q}$ with Galois group G, and let $C\subset G$ be a conjugacy class. Then we have that*

$$-\lim_{X\to\infty}\sum_{\substack{2\leq n\leq X\\ \left[\frac{K/\mathbb{Q}}{p_{\min}(n)}\right]=C}}\frac{\mu(n)}{n}=\frac{\#C}{\#G}.$$

Remark. The sum in Theorem 1.2.1 converges conditionally, and the proof gives an explicit convergence rate (see (4.6)).

Remark. The set $\left\{-\frac{\mu(2)}{2},-\frac{\mu(3)}{3},-\frac{\mu(5)}{5},-\frac{\mu(6)}{6},\dots\right\}$ can be viewed as a "signed probability measure" to calculate Chebotarev densities (i.e. $\#C/\#G$) via smallest prime divisors of squarefree integers.

Examples. (1) Alladi's theorem (1.13) is a special case of Theorem 1.2.1 in which K is a cyclotomic field, i.e. $K=\mathbb{Q}(\zeta_k)$ for some primitive kth root of unity ζ_k.

(2) Let $f(x) = x^4+x+1$. Then the Galois group of f is $\mathrm{Gal}(f) = S_4$, so in particular $\#\mathrm{Gal}(f) = 24$. Let K be the splitting field of f, and let S be the set of all primes p unramified in K such that f has no roots in $\mathbb{Z}/p\mathbb{Z}$. For primes $p \in S$, $f \pmod p$ is either an irreducible quartic, which corresponds to the conjugacy class consisting of six 4-cycles in S_4, or a product of two irreducible quadratics, which corresponds to the conjugacy class consisting of products of two transpositions (three elements) in S_4. Then the probability of an irreducible quartic contributes 6/24 to the sum, and the probability of a product of irreducible quadratics contributes 3/24, so the theorem gives

$$- \lim_{X\to\infty} \sum_{\substack{2\leq n\leq X \\ p_{\min}(n)\in S}} \frac{\mu(n)}{n} = \frac{3}{8} = 0.375.$$

Table 1.1 shows the actual values of the above sum for increasing values of X.

Table 1.1: Illustration of Theorem 1.2.1

X	$f \pmod p$ has no roots
20,000	0.3730
40,000	0.3741
60,000	0.3738
80,000	0.3735
100,000	0.3734

In Chapter 4, we explain the Chebotarev Density Theorem [56] in Section 4.1. In Section 4.2, we state and prove some results which help bound error terms in the proof of Theorem 1.2.1, and we prove Theorem 1.2.1. Finally, in Section 4.3, we state a generalization of Theorem 1.2.1 which was proven by Sweeting and Woo in [53].

1.3 Moonshine

Monstrous Moonshine, conjectured by Conway and Norton in 1979 [14], refers to the unexpected relationship between the monster group $\mathbb{M}$, which is the largest sporadic finite simple group, and the normalized modular invariant

$$J(\tau) := j(\tau) - 744 = q^{-1} + 196884q + 21493760q^2 + O\left(q^3\right).$$

Note that $J(\tau)$ is the Hauptmodul for $\mathrm{SL}_2(\mathbb{Z})$, i.e. the unique generator of the modular function field with Fourier expansion beginning with $q^{-1} + O(q)$. The relationship between $\mathbb{M}$ and $J(\tau)$ was initially observed by McKay, who noticed that certain linear combinations of the dimensions of the 194 irreducible representations of $\mathbb{M}$ reproduce the first few coefficients of $J(\tau)$. For example, if χ_1, χ_2, χ_3 are the first three irreducible characters of $\mathbb{M}$ (ordered by dimension), then we see that

$$\chi_1(1) = 1,$$
$$\chi_1(1) + \chi_2(1) = 1 + 196883 = 196884,$$
$$\chi_1(1) + \chi_2(1) + \chi_3(1) = 1 + 196883 + 21296876 = 21493760.$$

Based on these observations, Thompson conjectured [54,55] more generally that there exists a graded, infinite-dimensional $\mathbb{M}$-module

$$V^\natural = \bigoplus_{n \geq -1} V^\natural(n)$$

such that the graded dimensions $\dim V^\natural(n)$ are the Fourier coefficients of $J(\tau)$. Conway and Norton further conjectured [14] that for each element $g \in \mathbb{M}$, there is a genus zero subgroup $\Gamma_g \subseteq \mathrm{SL}_2(\mathbb{R})$ such that the graded trace function

$$T_g(\tau) := \sum_{n \geq -1} \mathrm{Tr}\left(g|V^\natural(n)\right) q^n,$$

called the *McKay–Thompson series*, is also magically the unique normalized Hauptmodul for Γ_g. The Monstrous Moonshine Conjecture was famously proven in 1992 by Borcherds [5], who received the Fields Medal in 1998 for this work.

In recent years, many more examples of moonshine have been established for other distinguished finite groups (for example, see [12, 25–27]). In view of this, it is natural to explore the extent to which dimensions of irreducible representations of finite groups are related to Fourier coefficients of modular functions. In 2017, Dehority, Gonzalez, Vafa, and Van Peski [22] proved that the seemingly rare occurrence of moonshine actually holds for every single finite group, if we relax certain requirements on the the graded trace functions. Namely, for every finite group G, there exists an infinite-dimensional graded G-module

$$V_G = \bigoplus_{n \in \{-d\} \cup \mathbb{Z}^+} V_G(n),$$

for sufficiently large $d > 0$, such that the McKay–Thompson series for each $g \in G$ is a weakly holomorphic modular function, i.e. a meromorphic modular function that is allowed to have poles at cusps. This generalization is now called *weak moonshine*.

By definition, weak moonshine depends only on the character table of a group. Since a moonshine module and its graded trace functions encode identifying information about a finite group, one would think that different groups should have different moonshines. However, it is possible for two non-isomorphic groups to have the same moonshine due to the fact that the character table of a group does not uniquely determine the group. For example, the representation theory of the dihedral group D_4 is identical to that of the quaternion group Q_8. Therefore, it is natural to ask whether one can extend weak moonshine so that it distinguishes non-isomorphic groups. To answer this question, we make use of classical higher dimensional group characters defined by Frobenius [30] in 1896, which we refer to as *Frobenius r-characters.*

Let G be a finite group with irreducible representations $\rho_1, \ldots, \rho_t$ and corresponding irreducible characters $\chi_1, \ldots, \chi_t$. Throughout, for $r \in \mathbb{Z}^+$ we denote by $G^{(r)}$ the direct product $G \times \cdots \times G$ (r copies). If χ is an irreducible character, then its Frobenius r-character generalizations are defined for $r = 1$ by $\chi^{(1)}(g) := \chi(g)$, for $r = 2$ by $\chi^{(2)}(g_1, g_2) := \chi(g_1)\chi(g_2) - \chi(g_1 g_2)$, and for $r \geq 3$ by the recursive formula

$$\begin{aligned} \chi^{(r)}\big(g_1, \ldots, g_r\big) &:= \chi(g_1)\,\chi^{(r-1)}(g_2, \ldots, g_r) \\ &- \chi^{(r-1)}(g_1 g_2, \ldots, g_r) - \chi^{(r-1)}(g_2, g_1 g_3, \ldots, g_r) - \cdots - \chi^{(r-1)}(g_2, \ldots, g_1 g_r)\,. \end{aligned} \tag{1.15}$$

For convenience, we denote the 1-character $\chi^{(1)}$ by χ.

For many years, determining the extent to which the Frobenius r-characters uniquely determine groups up to isomorphism remained an open problem. This problem was solved in the 1990s by Hoehnke and Johnson [34,35], who proved that a group is uniquely determined by its 1, 2, and 3-characters. Therefore, we aim to construct an extension of weak moonshine that also makes use of the 2 and 3-characters. With this goal in mind, we define *higher width moonshine* as follows.

Definition. We say that G has **width $s \geq 1$ weak moonshine** if the following hold:

1. There exists an infinite-dimensional graded G-module

$$V_G := \bigoplus_{n \gg -\infty} V_G(n),$$

   where each $V_G(n)$ is a finite sum of representation spaces arising from the irreducible characters $\chi_1, \ldots, \chi_t$.

2. If $1 \leq r \leq s$ and $\underline{g} := (g_1, \ldots, g_r) \in G^{(r)}$, then we define the *$r$-Frobenius of $\underline{g}$ on $V_G^{(r)}(n) := V_G(n) \times \cdots \times V_G(n)$* ($r$ copies) by

$$\mathrm{Frob}_r\left(\underline{g}; n\right) := \sum_{1 \leq j \leq t} m_i(n) \chi_i^{(r)}\left(\underline{g}\right).$$

   Here $m_i(n)$ denotes the number of copies of the representation space for χ_i in the nth graded component $V_G(n)$ of V_G.

3. For each $1 \leq r \leq s$ and each $\underline{g} \in G^{(r)}$, we define the *McKay–Thompson series*

$$T\left(r, \underline{g}; \tau\right) := \sum_{n \gg -\infty} \mathrm{Frob}_r\left(\underline{g}; n\right) q^n,$$

   which are the generalized graded trace functions for $V_G^{(r)}$.

4. Each $T\left(r, \underline{g}; \tau\right)$ is a weakly holomorphic modular function.

We say that width s weak moonshine is *complete* if for each $1 \leq i \leq t$, we have that $m_i(n)$ is nonzero for some n (and therefore for infinitely many n).

Remark. When $r = 1$, we have that $\mathrm{Frob}_1(g; n) = \mathrm{Tr}\big(g|V_G(n)\big)$. In particular, for the identity element $g = e$ of G, the graded dimensions $\dim V_G(n)$ agree with the coefficients of the McKay–Thompson series $T(1, e; q)$.

In joint work with Ono [20], we obtain the following theorem which extends width 1 weak moonshine.

Theorem 1.3.1 (D–Ono)**.** *Every finite group has width s weak moonshine for every $s \in \mathbb{Z}^+$.*

Thanks to Hoehnke and Johnson [34, 35], we have the following immediate corollary which refines weak moonshine to be a group isomorphism invariant.

Corollary 1.3.2 (D–Ono)**.** *If $s \geq 3$, then complete width s weak moonshine uniquely determines a finite group up to isomorphism.*

It is important to understand the algebraic compatibility of the higher width McKay–Thompson series $\big($i.e. $T\left(r, \underline{g}; \tau\right)$ with $r \geq 2\big)$ under this extension. In particular, these series should satisfy relations which reveal the structure of the seed module V_G. In short, the multiplicity generating functions must be compatible with all of the

McKay–Thompson series. The following theorem [20] illustrates the compatibility of weak moonshine for V_G when extended to width s.

Theorem 1.3.3 (D–Ono)**.** *Consider width s weak moonshine for a finite group G with irreducible characters $\chi_1, \ldots, \chi_t$ and McKay–Thompson series $T\left(r, \underline{g}; \tau\right)$, with $1 \le r \le s$ and $\underline{g} \in G^{(r)}$. If $1 \le r \le s$ and $\dim\chi_i \ge r$, then we have that*

$$\sum_{n \gg -\infty} m_i(n) q^n = \frac{(\dim\chi_i)^{r-1}}{r!|G|^r (\dim\chi_i - 1) \cdots (\dim\chi_i - (r-1))} \sum_{\underline{g} \in G^{(r)}} \overline{\chi_i^{(r)}\left(\underline{g}\right)} T\left(r, \underline{g}; \tau\right).$$

Theorem 1.3.3 follows from a new result on the orthogonality of the Frobenius r-characters [20]. This result is of independent interest in character theory.

Theorem 1.3.4 (D–Ono)**.** *If G is a finite group with irreducible characters $\chi_1, \ldots, \chi_t$ and $1 \le i, j \le t$, then for any $r \ge 1$ we have that*

$$\sum_{\underline{g} \in G^{(r)}} \chi_i^{(r)}\left(\underline{g}\right) \overline{\chi_j^{(r)}\left(\underline{g}\right)} = \frac{r!|G|^r \delta_{ij}}{(\dim\chi_i)^{r-1}} (\dim\chi_i - 1) \cdots (\dim\chi_i - (r-1)).$$

In Chapter 5, we give background on classical representation theory in Section 5.1 and prove Theorem 1.3.4 in Section 5.2. We prove Theorems 1.3.1 and 1.3.3 in Section 5.3, and we provide an example of higher width moonshine in Section 5.4.

Chapter 2

Modular Forms and Harmonic Maass Forms

The notation used here is standard (for example, see [7, 45]).

In order to define modular forms, we must first define the congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and their action on the upper half of the complex plane $\mathbb{H}$. For any matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we have that γ acts on $\mathbb{H}$ by linear fractional transformations

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}, \qquad \tau \in \mathbb{H}.$$

The *fundamental domain* of this action is the region

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

which contains exactly one element from each $\mathrm{SL}_2(\mathbb{Z})$-orbit. For a positive integer N, the *level N congruence subgroup* $\Gamma_0(N)$ is defined by

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

A *cusp* of a congruence subgroup Γ is then defined to be an equivalence class under the Γ-action on $\mathbb{Q} \cup \{\infty\}$. For a cusp x of Γ and a matrix $\gamma \in \Gamma$ with $\gamma x = \infty$, the *width* of x is the smallest number w such that $\left(\begin{smallmatrix} 1 & w \\ 0 & 1 \end{smallmatrix}\right) \in \gamma^{-1}\Gamma\gamma$.

2.1 Modular forms

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be a matrix with real entries and positive determinant, let $k \in \mathbb{Z}$, and let $f : \mathbb{H} \to \mathbb{C}$ be a meromorphic function. The matrix γ acts on f by the *slash operator* $|_k$, which is defined by

$$(f|_k\gamma)(\tau) := (\det\gamma)^{k/2}(c\tau + d)^{-k} f(\gamma\tau).$$

If $N \in \mathbb{Z}^+$ and $k \in \mathbb{Z}$, then a *weight* k *meromorphic modular form on* $\Gamma_0(N)$ is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ with the following properties:

1. We have that $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all $\tau \in \mathbb{H}$ and all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

2. For all $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$, we have that $(f|_k\gamma_0)(\tau)$ has the Fourier expansion

$$(f|_k\gamma_0)(\tau) = \sum_{n \geq n_{\gamma_0}} a_{\gamma_0}(n) q^{n/N},$$

where $a_{\gamma_0}(n_{\gamma_0}) \neq 0$. In other words, f is meromorphic at the cusps of $\Gamma_0(N)$.

If χ is a Dirichlet character modulo N, then we say that a weight k modular form f on $\Gamma_0(N)$ has *Nebentypus character* χ if condition (1) above is replaced by $f(\gamma\tau) = \chi(d)(c\tau + d)^k f(\tau)$.

Choosing γ to be the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, condition (2) of the above definition gives the following transformation properties:

$$f\left(-\frac{1}{\tau}\right) = \tau^k f(\tau) \quad \text{and} \quad f(\tau + 1) = f(\tau). \tag{2.1}$$

It is well known that S and T generate the full modular group $\mathrm{SL}_2(\mathbb{Z})$, and so (2.1) is actually equivalent to condition (2).

If $n_{\gamma_0} \geq 0$ for each matrix $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$, then f is called a *holomorphic modular form* since it is holomorphic at the cusps of $\Gamma_0(N)$. If n_{γ_0} is strictly positive, then f vanishes at the cusps of $\Gamma_0(N)$, and f is called a *cusp form.* A *weakly holomorphic modular form* is a meromorphic modular form whose poles are supported at the cusps. If f is a weight zero modular form on $\Gamma_0(N)$, then f is actually invariant under the action of $\Gamma_0(N)$. In this case, we call f a *modular function* on $\Gamma_0(N)$.

The Fourier expansion of an integer weight meromorphic modular form f at infinity has the form

$$f(\tau) = \sum_{n \geq n_0} a(n) q^n,$$

where as usual $q := e^{2\pi i \tau}$ with $\tau \in \mathbb{H}$.

There are three further modular form operators which are important for understanding Chapter 3: Hecke operators, Atkin–Lehner involutions, and Fricke involutions. If $f(\tau) = \sum_{n=0}^{\infty} a(n) q^n$ is a weight k holomorphic modular form on $\Gamma_0(N)$ with Nebentypus χ, then the *Hecke operator* $T_{p,k,\chi}$ acts on f by

$$f(\tau) \mid T_{p,k,\chi} := \sum_{n=0}^{\infty} \left(a(pn) + \chi(p) p^{k-1} a\left(\frac{n}{p}\right)\right) q^n,$$

where $a(n/p) := 0$ if $p \nmid a$. The Hecke operator preserves spaces of modular forms and in addition sends cusp forms to cusp forms. A modular form f is called a *Hecke eigenform* if $f(\tau) \mid T_{p,k,\chi} = \lambda(p) f(\tau)$ for some $\lambda(p) \in \mathbb{C}$. Now, let p be a prime dividing N with $\mathrm{ord}_p(N) = \ell$. In other words, ℓ is the largest integer for which $p^\ell \big| N$. Then the *Atkin–Lehner involution* $|_k W\left(p^\ell\right)$ acts on the space of weight k modular forms on $\Gamma_0(N)$ by any integer matrix of the form

$$W\left(p^{\ell}\right) := \begin{pmatrix} p^{\ell}\alpha & \beta \\ N_{\gamma} & p^{\ell}\delta \end{pmatrix}$$

with determinant p^{ℓ}, where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. We also define the *Fricke involution* $|_k W(N)$ on weight k modular forms on $\Gamma_0(N)$ by the action of $W(N) := \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. It is well known that the Atkin–Lehner and Fricke involutions commute with all of the Hecke operators.

There is a theory of so-called newforms which describes the relationship between fixed weight modular forms with trivial Nebentypus on different congruence subgroups. A weight k *newform* on $\Gamma_0(N)$ is a weight k normalized cusp form on $\Gamma_0(N)$ which is an eigenform of all of the corresponding Hecke operators, Atkin–Lehner involutions, and Fricke involutions with $p|N$. Atkin and Lehner characterized the eigenvalues of weight k newforms $f(\tau)$ on $\Gamma_0(N)$ as follows:

1. If $p|N$ is prime, then there is a $\lambda_p \in \{\pm 1\}$ for which $f|_k W\left(p^{\ell}\right) = \lambda_p f(\tau)$.

2. There is a $\lambda_N \in \{\pm 1\}$ for which $f|_k W(N) = \lambda_N f(\tau)$, and moreover we have that $\lambda_N = \prod_{p|N} \lambda_p$.

Two of the most important examples of modular forms are the Eisenstein series and the the Dedekind eta-function. Before defining these forms, we require additional notation. For a positive integer k, the ordinary divisor function $\sigma_k(n)$ is given by (1.9), and the Bernoulli numbers B_k are defined by the equation

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

If $k \geq 2$ is an even integer, then the *Eisenstein series* $E_k(\tau)$ are defined in general by

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

These series are weight k modular forms (and Hecke eigenforms) for all even $k \geq 4$, but (2.1) fails for $k = 2$, since $\tau^{-2} E_2(-1/\tau) = E_2(\tau) + \frac{12}{2\pi i \tau}$. It is known that the Eisenstein series $E_4(\tau)$ and $E_6(\tau)$ generate all modular forms on $\mathrm{SL}_2(\mathbb{Z})$. The series $E_4(\tau)$ is related to the modular j-invariant as follows. The *Delta-function* (sometimes called the *discriminant function*) is the unique normalized weight 12 cusp form on $\mathrm{SL}_2(\mathbb{Z})$, and it is given by

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

The Delta-function is also a Hecke eigenform. The *j-function* or *j-invariant*, which is a modular function on $\mathrm{SL}_2(\mathbb{Z})$, is given by

$$j(\tau) := \frac{E_4(\tau)^3}{\Delta(\tau)}.$$

In fact, every modular function on $\mathrm{SL}_2(\mathbb{Z})$ is a rational function in $j(\tau)$.

In order to define the Dedekind eta-function, we must first define half-integer weight modular forms. Let $\left(\frac{c}{d}\right)$ be the usual Kronecker symbol, and for d odd we let

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

If $\lambda \in \mathbb{Z}_{\geq 0}$, $N \in \mathbb{Z}^+$, and χ is a Dirichlet character modulo $4N$, then a *weight $\lambda + \frac{1}{2}$ meromorphic modular form with Nebentypus χ* is a meromorphic function g such that condition (1) in the definition of an integral weight modular form is replaced by

$$g(\gamma\tau) = \chi(d)\left(\frac{c}{d}\right)^{2\lambda+1} \epsilon_d^{-1-2\lambda}(c\tau+d)^{\lambda+\frac{1}{2}}g(\tau)$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4N)$. The adjectives *holomorphic*, *weakly holomorphic*, and *cusp form* have analogous definitions in this setting.

The *Dedekind eta-function* is defined by

$$\eta(\tau) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n),$$

and it is a weight 1/2 modular form. In fact, $\eta(\tau)^{24} = \Delta(\tau)$ is the weight 12 cusp form for $\mathrm{SL}_2(\mathbb{Z})$. The transformation properties analogous to (2.1) for $\eta(\tau)$ are

$$\eta(-1/\tau) = (-i\tau)^{1/2}\eta(\tau) \quad \text{and} \quad \eta(\tau+1) = e^{\pi i/12}\eta(\tau),$$

and so $\eta(24\tau)$ is a weight 1/2 cusp form on $\Gamma_0(576)$ with Nebentypus $\chi_{12}(n) := \left(\frac{12}{n}\right)$. It turns out that the Eisenstein series $E_4(\tau)$ and $E_6(\tau)$ can be expressed as rational functions in $\eta(\tau)$, $\eta(2\tau)$, and $\eta(4\tau)$, and therefore every modular form on $\mathrm{SL}_2(\mathbb{Z})$ can be expressed as a rational function in these three eta-functions.

Define the compact Riemann surface $X_0(N)$ to be the compactification of the quotient $\Gamma_0(N)\backslash\mathbb{H}$, which is obtained by adding suitable cusps. Then $X_0(N)$ is called a *modular curve*. Modular curves are closely related to spaces of elliptic curves, but for our purposes we only need to know that the *modular function field* $\mathbb{C}\left(X_0(N)\right)$ has a single generator, the unique normalized *Hauptmodul* for $\Gamma_0(N)$, whenever the genus of $X_0(N)$ is zero. For example, the modular curve $X_0(1)$ for $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$ has genus zero, and the Hauptmodul for $\mathbb{C}\left(X_0(1)\right)$ is the normalized j-invariant, $J(\tau) := j(\tau) - 744$.

2.2 Harmonic Maass forms

We now turn to harmonic Maass forms. A smooth function $f : \mathbb{H} \to \mathbb{C}$ is a *weight* $k \in \frac{1}{2}\mathbb{Z}$ *harmonic Maass form* on a congruence subgroup $\Gamma = \Gamma_0(N)$, where $4|N$ if $k \in \frac{1}{2} + \mathbb{Z}$, if it has the following properties:

1. For all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and all $\tau \in \mathbb{H}$, we have that

$$f(\gamma\tau) = \begin{cases} (c\tau + d)^k f(\tau) & \text{if } k \in \mathbb{Z}, \\ \left(\frac{c}{d}\right) \epsilon_d^{-2k} (c\tau + d)^k f(\tau) & \text{if } k \in \frac{1}{2} + \mathbb{Z}. \end{cases}$$

   In other words, f transforms like a modular form.

2. We have that $\Delta_k(f) = 0$, where the *weight k hyperbolic Laplacian operator* Δ_k on $\mathbb{H}$ is defined for $\tau = u + iv$ by

$$\Delta_k := -v^2 \left(\frac{\partial^2}{\partial u^2} + \frac{\partial^2}{\partial v^2} \right) + ikv \left(\frac{\partial}{\partial u} + i\frac{\partial}{\partial v} \right).$$

   In other words, f is harmonic.

3. There exists a polynomial $P_f(\tau) \in \mathbb{C}\left[q^{-1}\right]$ such that $f(\tau) - P_f(\tau) = O\left(e^{-\epsilon v}\right)$ as $v \to \infty$ for some $\epsilon > 0$. Analogous conditions are required at all cusps, and the polynomial P_f is called the *principal part* of f at the corresponding cusp.

Condition (1) has an analogous statement for harmonic Maass forms with Nebentypus χ. If instead f is an eigenfunction of Δ_k with nonzero eigenvalue, then f is called a *weak Maass form*. If condition (3) above is replaced by the growth condition $f(\tau) = O\left(e^{\epsilon v}\right)$ as $v \to \infty$ for some $\epsilon > 0$, then we say f has *manageable growth*.

In order to give the Fourier expansion of a harmonic Maass form, we require additional notation. The *incomplete Gamma function* $\Gamma(s, z)$ for $\mathrm{Re}(s) > 0$ and

$z \in \mathbb{C}$ is defined by

$$\Gamma(s,z) := \int_z^\infty e^{-t}\, t^s \,\frac{dt}{t}.$$

This function has an analytic continuation to $\mathbb{C}$, and for $x \in \mathbb{R}$ it satisfies the asymptotic formula $\Gamma(s,x) \sim x^{s-1}e^{-x}$ as $|x| \to \infty$.

Now, let $k \in \mathbb{Z} \setminus \{1\}$ and $N \in \mathbb{Z}^+$. If f is a weight k harmonic Maass form on $\Gamma_0(N)$, then f has a Fourier expansion of the form

$$f(\tau) = \sum_{n \gg -\infty} c_f^+(n) q^n + \sum_{n<0} c_f^-(n)\Gamma(1-k, -4\pi n v) q^n,$$

and similar expansions hold at other cusps. We call the component

$$f^+(\tau) := \sum_{n \gg -\infty} c_f^+(n) q^n$$

the *holomorphic part* of f, and

$$f^-(\tau) := \sum_{n<0} c_f^-(n)\Gamma(1-k, -2\pi n v) q^n$$

the *nonholomorphic part*. The holomorphic part of a harmonic Maass form is called a *mock modular form*, because it is holomorphic but not quite modular.

To make this precise, we must define the differential operator

$$\xi_k := 2iv^k \overline{\frac{\partial}{\partial \overline{\tau}}}.$$

This operator maps weight $2-k$ harmonic Maass forms to weight k cusp forms:

$$\begin{aligned} \xi_{2-k} : H_{2-k}(\Gamma_0(N)) &\to S_k(\Gamma_0(N)) \\ f(\tau) &\mapsto -(4\pi)^{k-1} \sum_{n=1}^{\infty} \overline{c_f^-(-n)} n^{k-1} q^n. \end{aligned}$$

The image of f under the ξ-operator above is called the *shadow* of the mock modular form f^+. If f is a weight $2-k$ harmonic Maass form on $\Gamma_0(N)$ and f^+ has shadow $g(\tau) = \sum_{n=1}^{\infty} c_g(n)q^n$, then the nonholomorphic part f^- has the form

$$f^-(\tau) = 2^{1-k} i \int_{-\overline{\tau}}^{i\infty} \frac{\overline{g\left(-\overline{\tau}\right)}}{(-i(w+\tau))^{2-k}}\, dw.$$

In other words, f^+ is holomorphic but not modular, and adding the above integral (essentially a *period integral*) to f^+ makes it modular but not holomorphic.

Chapter 3

Partitions

The most important results related to the partition function $p(n)$ are theorems that address two questions: what is the size of $p(n)$, and what special arithmetic properties do the values of this function satisfy? Together with Wagner, we studied arithmetic properties in the form of congruences for powers of the partition function in [40], but this work is not included here. In this section, we focus on log concavity and related results for the smallest parts partition function $\mathrm{spt}(n)$ of Andrews, as well as formulas involving partition functions which measure the algebraic complexity of the finitary permutation groups and their wreath products. In order to state our results, we must first introduce the theory of quadratic forms.

3.1 The theory of quadratic forms

Let $N \geq 1$ be a positive integer, and let $D < 0$ be a negative discriminant coprime to N. Let $\mathcal{Q}_{D,N}$ be the set of positive definite, integral binary quadratic forms

$$Q(X,Y) = [a_Q, b_Q, c_Q](X,Y) = a_Q X^2 + b_Q XY + c_Q Y^2$$

of discriminant $b_Q^2 - 4a_Q c_Q = D < 0$ with $a_Q \equiv 0 \pmod{N}$. There is a (right) action of $\Gamma_0(N)$ on $\mathcal{Q}_{D,N}$ defined by

$$Q = [a_Q, b_Q, c_Q] \mapsto Q \circ \sigma = \left[a_Q^\sigma, b_Q^\sigma, c_Q^\sigma\right],$$

where for $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma_0(N)$ we have that

$$\begin{aligned} a_Q^\sigma &= a_Q\alpha^2 + b_Q\alpha\gamma + c_Q\gamma^2, \\ b_Q^\sigma &= 2a_Q\alpha\beta + b_Q(\alpha\delta + \beta\gamma) + 2c_Q\gamma\delta, \\ c_Q^\sigma &= a_Q\beta^2 + b_Q\beta\delta + c_Q\delta^2. \end{aligned}$$

Given a solution $r \pmod{2N}$ of $r^2 \equiv D \pmod{4N}$, we define the subset of forms

$$\mathcal{Q}_{D,N,r} := \{Q = [a_Q, b_Q, c_Q] \in \mathcal{Q}_{D,N} :\ b_Q \equiv r \pmod{2N}\}.$$

Then the group $\Gamma_0(N)$ also acts on $\mathcal{Q}_{D,N,r}$. The number of $\Gamma_0(N)$-equivalence classes in $\mathcal{Q}_{D,N,r}$ is given by the Hurwitz–Kronecker class number $H(D)$.

The preceding facts remain true if we restrict to the subset $\mathcal{Q}_{D,N}^{\text{prim}}$ of primitive forms in $\mathcal{Q}_{D,N}$; i.e. those forms with $(a_Q, b_Q, c_Q) = 1$. In this case, the number of $\Gamma_0(N)$ equivalence classes in $\mathcal{Q}_{D,N,r}^{\text{prim}}$ is given by the class number $h(D)$.

To each form $Q \in \mathcal{Q}_{D,N}$, we associate a *CM point* (also called a *Heegner point*) τ_Q, which is the root of $Q(X, 1)$ in $\mathbb{H}$ given by

$$\tau_Q = \frac{-b_Q + \sqrt{D}}{2a_Q}.$$

The CM points τ_Q are compatible with the action of $\Gamma_0(N)$: if $\sigma \in \Gamma_0(N)$, then

$$\sigma\tau_Q = \tau_{Q\circ\sigma^{-1}}. \tag{3.1}$$

3.2 The smallest parts partition function

The smallest parts partition function $\mathrm{spt}(n)$ has many arithmetic properties which resemble those of the ordinary partition function $p(n)$. The most well-known examples include the Ramanujan-type congruences of Andrews for the moduli 5, 7, and 13 [3], Bringmann's asymptotic formula [6], and the Rademacher-type exact formula of Ahlgren and Andersen [1]. Based on extensive numerical calculations, Chen predicted [11] that the inequalities listed in Section 1.1.1, (2)–(6) of which were proven true for $p(n)$ in [23] and [10], also hold for $\mathrm{spt}(n)$.

In fact, we prove a more precise version of Theorem 1.1.1 regarding Conjecture (1). Note that this version is a refinement of Bringmann's asymptotic (1.5).

Theorem 3.2.1 (Refined Theorem 1.1.1 (1), D–Masri)**.** *For each $\epsilon > 0$, there is an effectively computable constant $N(\epsilon) > 0$ such that for all $n \geq N(\epsilon)$, we have that*

$$\frac{\sqrt{6}}{\pi}\sqrt{n}\,p(n) < \mathrm{spt}(n) < \left(\frac{\sqrt{6}}{\pi} + \epsilon\right)\sqrt{n}\,p(n).$$

Remark. The constant $N(\epsilon)$ of Theorem 3.2.1 can be computed in practice. For example, by letting $\epsilon = 1 - \frac{\sqrt{6}}{\pi}$ in Theorem 3.2.1, we obtain Theorem 1.1.1 (1) for $n \geq N\left(1 - \frac{\sqrt{6}}{\pi}\right)$ with $N\left(1 - \frac{\sqrt{6}}{\pi}\right) = 5310$. We then use a computer to verify Theorem 1.1.1 (1) in the exceptional range $5 \leq n < 5310$.

To prove Theorems 1.1.1 and 3.2.1, we make use of classic work of Lehmer [39] which gives effective bounds for the partition function, recent work of Desalvo and Pak [23] and Chen, Wang, and Xie [10], and a formula different from (1.6) by Ahlgren and Andersen [1] for $\mathrm{spt}(n)$. In order to give an effective bound on the error term for $p(n)$, Lehmer [39] truncated the absolutely convergent sum (1.3) and applied bounds for the Kloosterman sum $A_c(n)$. On the other hand, since the formula (1.6) is only conditionally convergent, bounding $\mathrm{spt}(n)$ is a much more delicate matter. In fact, to resolve the difficult problem of proving that (1.6) converges, Ahlgren and Andersen used advanced methods from the spectral theory of automorphic forms.

There are now different types of formulas for $p(n)$ and $\mathrm{spt}(n)$ that are useful in this situation. For example, Bruinier and Ono [8] proved that the coefficients of certain weight $-1/2$ harmonic Maass forms are essentially traces of singular moduli for weak Maass forms, from which they obtained a formula for the partition function as a finite sum of algebraic numbers. More precisely, consider the weight zero weak Maass form for $\Gamma_0(6)$ defined by

$$P(z) := -\left(\frac{1}{2\pi i}\frac{d}{dz} + \frac{1}{2\pi y}\right) g(z), \quad z = x + iy \in \mathbb{H},$$

where $g(z)$ is the weight -2 weakly holomorphic modular form for $\Gamma_0(6)$ defined by

$$g(z) := \frac{1}{2}\frac{E_2(z) - 2E_2(2z) - 3E_2(3z) + 6E_2(6z)}{\big(\eta(z)\eta(2z)\eta(3z)\eta(6z)\big)^2}.$$

Bruinier and Ono [8] proved that for all $n \geq 1$, we have that

$$p(n) = \frac{1}{24n-1} \sum_{Q \in \mathcal{Q}_{-24n+1,6,1}} P\left(\tau_Q\right). \tag{3.2}$$

Similarly, let $f(z)$ be the weakly holomorphic modular function for $\Gamma_0(6)$ defined by

$$f(z) := \frac{1}{24}\frac{E_4(z) - 4E_4(2z) - 9E_4(3z) + 36E_4(6z)}{\big(\eta(z)\eta(2z)\eta(3z)\eta(6z)\big)^2}.$$

Ahlgren and Andersen [1] proved the following analogue of (3.2) for $\mathrm{spt}(n)$: for all $n \geq 1$, we have that

$$\mathrm{spt}(n) = \frac{1}{12} \sum_{Q \in \mathcal{Q}_{-24n+1,6,1}} \big(f\left(\tau_Q\right) - P\left(\tau_Q\right)\big). \tag{3.3}$$

We prove Theorem 1.1.2 by effectively bounding this finite formula (3.3). The bound is then used to verify Chen's conjectured inequalities for sufficiently large n, and we complete the proofs of Theorems 1.1.1 and 3.2.1 by checking the exceptional range with a computer.

Before proving Theorem 1.1.2, we must define the Kloosterman sum $A_c(n)$ and the I-Bessel function which appear in the formula of Ahlgren and Andersen (1.6). The Kloosterman sum $A_c(n)$ is defined by

$$A_c(n) := \sum_{\substack{d \pmod{c} \\ (d,c)=1}} e^{\pi i s(d,c)} e^{-\frac{2\pi i d n}{c}},$$

where $s(d,c)$ is the classical Dedekind sum

$$s(d,c) := \sum_{r=1}^{c-1} \frac{r}{c} \left(\frac{dr}{c} - \left\lfloor \frac{dr}{c} \right\rfloor - \frac{1}{2} \right).$$

The weight ν I-Bessel function is given by the sum

$$I_\nu(x) := \sum_{m=0}^{\infty} \frac{1}{m!\Gamma(m+\nu+1)} \left(\frac{x}{2} \right)^{2m+\nu}, \tag{3.4}$$

where the Gamma-function $\Gamma(z)$ is defined for $\mathrm{Re}(z) > 0$ by

$$\Gamma(z) := \int_0^\infty x^{z-1} e^{-x}\, dx.$$

Note that the Gamma-function can be analytically continued to $\mathbb{C} \setminus \{0, -1, -2, \ldots\}$.

3.2.1 Effective estimates for spt(n)

Using (3.2), the formula (3.3) can be written as

$$\operatorname{spt}(n) = \frac{1}{12}S(n) - \frac{24n-1}{12}p(n), \tag{3.5}$$

where $S(n)$ is the trace of singular moduli for $f(z)$ given by

$$S(n) := \sum_{[Q]} f\left(\tau_Q\right).$$

By applying Lehmer's effective error bounds for $p(n)$ in (3.5), we reduce the proof of Theorem 1.1.2 to the following asymptotic formula for the trace $S(n)$ with an effective bound on the error term.

Theorem 3.2.2 (D–Masri)**.** *Let* $\lambda(n) := \frac{\pi\sqrt{24n-1}}{6}$*, and define* $q(n)$ *as in Theorem 1.1.2. Then for all* $n \geq 1$*, we have that*

$$S(n) = 2\sqrt{3}\, e^{\lambda(n)} + E(n),$$

where

$$|E(n)| < \left(4.30 \times 10^{23}\right) 2^{q(n)} (24n-1)^2 e^{\lambda(n)/2}.$$

In order to prove Theorem 3.2.2, we first must establish some notation and prove an intermediate lemma. Let $D_n := -24n+1$ for $n \in \mathbb{Z}^+$, and define the trace of $f(z)$,

$$S(n) := \sum_{[Q] \in \mathcal{Q}_{D_n,6,1}/\Gamma_0(6)} f\left(\tau_Q\right).$$

First, we decompose $S(n)$ as a linear combination of traces involving primitive forms. Let $\Delta < 0$ be any discriminant with $\Delta \equiv 1 \pmod{24}$, and define the class polynomials

$$H_n(X) := \prod_{[Q]\in \mathcal{Q}_{D_n,6,1}/\Gamma_0(6)} (X - f(\tau_Q)) \quad \text{and} \quad \widehat{H}_\Delta(X) := \prod_{[Q]\in \mathcal{Q}^{\text{prim}}_{\Delta,6,1}/\Gamma_0(6)} (X - f(\tau_Q)).$$

Let $\{W_\ell\}_{\ell|6}$ be the group of Atkin-Lehner involutions for $\Gamma_0(6)$. Since $f|_0 W_\ell = \lambda_\ell f$ with $\lambda_\ell = 1$ for $\ell = 1, 6$ and $\lambda_\ell = -1$ for $\ell = 2, 3$, arguing exactly as in the proof of [9, Lemma 3.7] we get the identity

$$H_n(X) = \prod_{\substack{u>0 \\ u^2|D_n}} \varepsilon(u)^{h(D_n/u^2)} \widehat{H}_{D_n/u^2}(\varepsilon(u)X), \tag{3.6}$$

where $\varepsilon(u) = 1$ if $u \equiv \pm 1 \pmod{12}$ and $\varepsilon(u) = -1$ otherwise. Comparing terms on both sides of (3.6) yields the class number relation

$$H(D_n) = \sum_{\substack{u>0 \\ u^2|D_n}} h\left(\frac{D_n}{u^2}\right)$$

and the decomposition

$$S(n) = \sum_{\substack{u>0 \\ u^2|D_n}} \varepsilon(u) S_u(n), \tag{3.7}$$

where

$$S_u(n) := \sum_{[Q]\in \mathcal{Q}^{\text{prim}}_{D_n/u^2,6,1}/\Gamma_0(6)} f(\tau_Q).$$

Next, following [24] we express $S_u(n)$ as a trace involving primitive forms of level 1. The group $\Gamma_0(6)$ has index 12 in $SL_2(\mathbb{Z})$. We choose the following 12 right coset representatives:

$$\gamma_\infty := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\gamma_{1/3,r} := \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \quad r = 0, 1;$$

$$\gamma_{1/2,s} := \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}, \quad s = 0, 1, 2;$$

$$\gamma_{0,t} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad t = 0, 1, 2, 3, 4, 5.$$

We denote this set of coset representatives by $\mathbf{C}_6$. Each matrix $\gamma \in \mathbf{C}_6$ maps the cusp ∞ to one of the four cusps $\{\infty, 1/3, 1/2, 0\}$ of the modular curve $X_0(6)$, which have widths 1, 2, 3, and 6, respectively. In particular, we have $\gamma_\infty\infty = \infty$, $\gamma_{1/3,r}\infty = 1/3$, $\gamma_{1/2,s}\infty = 1/2$, and $\gamma_{0,t}\infty = 0$.

Recall that a form $Q = [a_Q, b_Q, c_Q] \in \mathcal{Q}_{\Delta,1}$ is reduced if $|b_Q| \leq a_Q \leq c_Q$, and if either $|b_Q| = a_Q$ or $a_Q = c_Q$, then $b_Q \geq 0$. Let $\mathcal{Q}_\Delta$ denote a set of primitive, reduced forms representing the equivalence classes in $\mathcal{Q}_{\Delta,1}^{\text{prim}}/SL_2(\mathbb{Z})$. For each $Q \in \mathcal{Q}_\Delta$, there is a unique choice of coset representative $\gamma_Q \in \mathbf{C}_6$ such that $[Q \circ \gamma_Q^{-1}] \in \mathcal{Q}_{\Delta,6,1}^{\text{prim}}/\Gamma_0(6)$. This induces a bijection

$$\begin{aligned} \mathcal{Q}_\Delta &\longrightarrow \mathcal{Q}_{\Delta,6,1}^{\text{prim}}/\Gamma_0(6) \\ Q &\longmapsto [Q \circ \gamma_Q^{-1}]; \end{aligned} \tag{3.8}$$

see the Proposition on page 505 in [31], or more concretely [24, Lemma 3], for an explicit list of the matrices $\gamma_Q \in \mathbf{C}_6$. Using the bijection (3.8) and the compatibility relation (3.1) for CM points, the trace $S_u(n)$ can be expressed as

$$S_u(n) = \sum_{[Q]\in\mathcal{Q}^{\text{prim}}_{D_n/u^2,6,1}/\Gamma_0(6)} f\left(\tau_Q\right) = \sum_{Q\in\mathcal{Q}_{D_n/u^2}} f\left(\gamma_Q\tau_Q\right). \tag{3.9}$$

Therefore, to study the asymptotic distribution of $S_u(n)$, we need the Fourier expansion of $f(z)$ with respect to the matrices $\gamma_\infty, \gamma_{1/3,r}, \gamma_{1/2,s}$, and $\gamma_{0,t}$.

In [1, Section 4], Ahlgren and Andersen computed the Fourier expansion of $f(z)$ at the cusp ∞. The basic idea is as follows. The weakly holomorphic modular form $f(z)$ has a Fourier expansion of the form

$$f(z) = e(-z) + b(0) + \sum_{m=1}^{\infty} b(m)e(mz), \quad e(z) := e^{2\pi iz}$$

for some integers $b(m)$ for $m \geq 0$. One can construct a weight zero weak Maass form $f(z,s)$ for $\Gamma_0(6)$ with eigenvalue $s(1-s)$ whose analytic continuation at $s=1$ is a harmonic function on $\mathbb{H}$ with the Fourier expansion

$$f(z,1) = e(-z) + a(0) + \sum_{m=1}^{\infty} \frac{a(m)}{\sqrt{m}} e(mz) - e(-\overline{z}) + \sum_{m=1}^{\infty} \frac{a(-m)}{\sqrt{m}} e(-m\overline{z}),$$

where

$$a(0) = 4\pi^2 \sum_{\ell|6} \frac{\mu(\ell)}{\ell} \sum_{\substack{0<c\equiv 0 \pmod{6/\ell} \\ (c,\ell)=1}} \frac{S\left(-\overline{\ell},0;c\right)}{c^2},$$

$$a(m) = 2\pi \sum_{\ell|6} \frac{\mu(\ell)}{\sqrt{\ell}} \sum_{\substack{0<c\equiv 0 \pmod{6/\ell} \\ (c,\ell)=1}} \frac{S\left(-\overline{\ell},m;c\right)}{c} I_1\left(\frac{4\pi\sqrt{m}}{\sqrt{\ell}c}\right), \quad m \geq 1,$$

$$a(-m) = 2\pi \sum_{\ell|6} \frac{\mu(\ell)}{\sqrt{\ell}} \sum_{\substack{0<c\equiv 0 \pmod{6/\ell} \\ (c,\ell)=1}} \frac{S\left(-\overline{\ell},-m;c\right)}{c} J_1\left(\frac{4\pi\sqrt{m}}{\sqrt{\ell}c}\right), \quad m \geq 1.$$

Here $\mu(\ell)$ is the Möbius function, $S(a,b;c)$ is the Kloosterman sum

$$S(a,b;c) := \sum_{\substack{d \pmod c \\ (c,d)=1}} e\left(\frac{a\overline{d}+bd}{c}\right),$$

and I_1, J_1 are the Bessel functions of order 1 (note that $\overline{d}$ is the multiplicative inverse of $d \pmod c$). The weight ν J-Bessel function is defined by the sum

$$J_\nu(x) := \sum_{m=0}^{\infty} \frac{(-1)^m}{m!\Gamma(m+\nu+1)} \left(\frac{x}{2}\right)^{2m+\nu}.$$

From these Fourier expansions, one can see that the functions $f(z)$ and $f(z,1)$ have the same principal parts at the cusps $\{\infty, 1/3, 1/2, 0\}$, and hence $f(z) - f(z,1)$ is bounded on the compact Riemann surface $X_0(6)$. Since a bounded harmonic function on a compact Riemann surface is constant, the function $f(z) - f(z,1)$ is constant.

Now, using the Fourier expansions of $E_4(z)$ and $\eta(z)$, we use `SageMath` to compute

$$f(z) = q^{-1} + 12 + 77q + 376q^2 + 1299q^3 + 4600q^4 + 12025q^5 + \cdots.$$

In particular, $b(0) = 12$. On the other hand, in Lemma 3.2.3 we will show by a direct calculation that $a(0) = 12$. Since $f(z) - f(z,1)$ is constant, we have

$$f(z) - f(z,1) = b(0) - a(0) = 12 - 12 = 0.$$

Finally, we have that $f(z) = f(z,1)$, so by uniqueness of Fourier expansions we have that $b(m) = m^{-1/2}a(m)$ for $m \geq 1$, $a(-1) = 1$, and $a(-m) = 0$ for $m \geq 2$.

We next use the Fourier expansion

$$f|_0\gamma_\infty(z) = e(-z) + 12 + \sum_{m=1}^{\infty} \frac{a(m)}{\sqrt{m}} e(mz)$$

to compute the Fourier expansion of f with respect to $\gamma_\infty, \gamma_{1/3,r}, \gamma_{1/2,s}, \gamma_{0,t}$.

The Atkin-Lehner involutions for $\Gamma_0(6)$ are given by

$$W_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad W_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 2 & -1 \\ 6 & -2 \end{pmatrix},$$

$$W_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 3 & 1 \\ 6 & 3 \end{pmatrix}, \quad W_6 = \frac{1}{\sqrt{6}} \begin{pmatrix} 0 & -1 \\ 6 & 0 \end{pmatrix}.$$

For each $\ell | 6$ and $v = 6/\ell$, let $V_\ell = \sqrt{\ell}\, W_\ell$ and

$$A_\ell = \begin{pmatrix} \frac{1}{\text{width of the cusp } 1/v} & 0 \\ 0 & 1 \end{pmatrix}.$$

Then we compute the following matrices:

Table 3.1: Evaluations of the Matrices V_ℓ and A_ℓ

cusp $1/v$	$\infty \simeq 1/6$	$1/3$	$1/2$	$0 \simeq 1$
ℓ	1	2	3	6
V_ℓ	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ 6 & -2 \end{pmatrix}$	$\begin{pmatrix} 3 & 1 \\ 6 & 3 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 6 & 0 \end{pmatrix}$
A_ℓ	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1/3 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1/6 & 0 \\ 0 & 1 \end{pmatrix}$
$V_\ell A_\ell$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Note that $V_\ell A_\ell \in SL_2(\mathbb{Z})$ and $V_\ell A_\ell(\infty) = 1/v$. Let $\gamma \in SL_2(\mathbb{Z})$ be any matrix such that $\gamma\infty = 1/v$. Then $(V_\ell A_\ell)^{-1}(\gamma\infty) = \infty$, so that $(V_\ell A_\ell)^{-1}\gamma \in \Gamma_\infty$, where $\Gamma_\infty := \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\}$ is the stabilizer of the cusp ∞. In particular, there is an integer $n \in \mathbb{Z}$ such that $\gamma = V_\ell A_\ell \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$. Solving for n for each cusp, we have that

$$\gamma_\infty = V_1 A_1, \qquad \gamma_{1/3,r} = V_2 A_2 \begin{pmatrix} 1 & r+1 \\ 0 & 1 \end{pmatrix},$$
$$\gamma_{1/2,s} = V_3 A_3 \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}, \qquad \gamma_{0,t} = V_6 A_6 \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

Now, since f is an eigenfunction of the Atkin-Lehner involutions $\{W_\ell\}_{\ell|6}$, we have that $f(V_\ell z) = f(z)$ for $\ell = 1, 6$ and $f(V_\ell z) = -f(z)$ for $\ell = 2, 3$. Therefore, we have

$$f|_0\gamma_\infty(z) = f(z),$$
$$f|_0\gamma_{1/3,r}(z) = f\left(V_2 A_2 \begin{pmatrix} 1 & r+1 \\ 0 & 1 \end{pmatrix} z\right) = f\left(V_2\left(\frac{z+r+1}{2}\right)\right) = -f\left(\frac{z+r+1}{2}\right),$$
$$f|_0\gamma_{1/2,s}(z) = f\left(V_3 A_3 \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} z\right) = f\left(V_3\left(\frac{z+s}{3}\right)\right) = -f\left(\frac{z+s}{3}\right),$$
$$f|_0\gamma_{0,t}(z) = f\left(V_6 A_6 \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} z\right) = f\left(V_6\left(\frac{z+t}{6}\right)\right) = f\left(\frac{z+t}{6}\right).$$

The Fourier expansion of $f(z)$ with respect to the matrices $\gamma_{1/3,r}, \gamma_{1/2,s}, \gamma_{0,t}$ can now be determined from the Fourier expansion at ∞ using these identities. In particular, if $\zeta_6 := e(1/6)$ is a primitive sixth root of unity, then we have that

$$f|_0\gamma_{1/3,r}(z) = \zeta_6^{3r} e\left(-\frac{z}{2}\right) - 12 + \sum_{m=1}^{\infty} \zeta_6^{3+3m(r+1)} \frac{a(m)}{\sqrt{m}} e\left(\frac{mz}{2}\right),$$
$$f|_0\gamma_{1/2,s}(z) = \zeta_6^{3-2s} e\left(-\frac{z}{3}\right) - 12 + \sum_{m=1}^{\infty} \zeta_6^{3+2ms} \frac{a(m)}{\sqrt{m}} e\left(\frac{mz}{3}\right),$$
$$f|_0\gamma_{0,t}(z) = \zeta_6^{-t} e\left(-\frac{z}{6}\right) + 12 + \sum_{m=1}^{\infty} \zeta_6^{mt} \frac{a(m)}{\sqrt{m}} e\left(\frac{mz}{6}\right).$$

Given a quadratic form $Q \in Q_\Delta$ and corresponding coset representative $\gamma_Q \in \mathbf{C}_6$, let $h_Q \in \{1, 2, 3, 6\}$ be the width of the cusp $\gamma_Q\infty$, and let ζ_Q and $\phi_{m,Q}$ be the sixth roots of unity defined as follows:

Table 3.2: Roots of Unity

cusp $\gamma_Q\infty$	$\infty \simeq 1/6$	$1/3$	$1/2$	$0 \simeq 1$
ζ_Q	1	ζ_6^{3r}	ζ_6^{3-2s}	ζ_6^{-t}
$\phi_{m,Q}$	1	$\zeta_6^{3+3m(r+1)}$	ζ_6^{3+2ms}	ζ_6^{mt}

Then we can write

$$f|_0\gamma_Q(z) = \zeta_Q e\left(-\frac{z}{h_Q}\right) + 12\mu\left(h_Q\right) + \sum_{m=1}^{\infty} \phi_{m,Q}\frac{a(m)}{\sqrt{m}} e\left(\frac{mz}{h_Q}\right). \tag{3.10}$$

In the following lemma, we evaluate $a(0)$ and give effective bounds for the Fourier coefficients $a(m)$ for $m \geq 1$.

Lemma 3.2.3. *We have that $a(0) = 12$ and*

$$|a(m)| \leq C\sqrt{m}\exp\left(4\pi\sqrt{m}\right), \quad m \geq 1,$$

where

$$C := 8\sqrt{6}\pi^{3/2} + 16\pi^2\zeta^2\left(\frac{3}{2}\right).$$

Proof of Lemma 3.2.3. We first evaluate $a(0)$. Recall that

$$a(0) = 4\pi^2 \sum_{\ell|6} \frac{\mu(\ell)}{\ell} \sum_{\substack{0<c\equiv 0 \pmod{6/\ell} \\ (c,\ell)=1}} \frac{S\left(-\overline{\ell}, 0; c\right)}{c^2}.$$

Since $(\ell, c) = 1$, we can evaluate the Kloosterman sum as

$$S\left(-\overline{\ell}, 0; c\right) = \sum_{\substack{d \pmod c \\ (c,d)=1}} e\left(\frac{-\overline{\ell}d}{c}\right) = \sum_{\substack{d \pmod c \\ (c,d)=1}} e\left(\frac{\overline{\ell}d}{c}\right) = \mu(c)$$

where the last equality follows from [36, Equation (3.4)]. Therefore,

$$a(0) = 4\pi^2 \sum_{\ell | 6} \frac{\mu(\ell)}{\ell} \sum_{\substack{0<c\equiv 0 \pmod{6/\ell} \\ (c,\ell)=1}} \frac{\mu(n)}{c^2}.$$

Now, if $\ell = 1$, then we have that

$$\begin{aligned}
\sum_{\substack{0<c\equiv 0 \pmod{6/\ell} \\ (c,\ell)=1}} \frac{\mu(n)}{c^2} &= \sum_{n=1}^{\infty} \frac{\mu(6n)}{(6n)^2} \\
&= \frac{1}{36} \sum_{\substack{n=1 \\ (n,6)=1}}^{\infty} \frac{\mu(n)}{n^2} \\
&= \frac{1}{36} \frac{1}{\zeta(2)} (1-2^{-2})^{-1}(1-3^{-2})^{-1} \\
&= \frac{1}{24} \frac{1}{\zeta(2)}.
\end{aligned}$$

A similar calculation yields

$$\sum_{\substack{0<c\equiv 0 \pmod{6/\ell} \\ (c,\ell)=1}} \frac{\mu(n)}{c^2} = \frac{1}{\zeta(2)} \begin{cases} -1/6, & \ell = 2 \\ -3/8, & \ell = 3 \\ 3/2, & \ell = 6. \end{cases}$$

Using $\zeta(2) = \pi^2/6$, we get

$$a(0) = 24\left(\frac{1}{24} + \frac{1}{12} + \frac{1}{8} + \frac{1}{4}\right) = 12.$$

We next estimate $|a(m)|$ for $m \geq 1$. From (3.4), we have that

$$|I_1(x)| \leq x \quad \text{for} \quad 0 < x < 1. \tag{3.11}$$

Also, using the asymptotic expansion (see `dlmf.nist.gov/10.40.1`) and the error bounds (see `dlmf.nist.gov/10.40.(ii)`), we have that

$$|I_1(x)| \leq \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{x}} \exp(x) \quad \text{for} \quad x \geq 1. \tag{3.12}$$

Let $M = 4\pi\sqrt{m}/\sqrt{\ell}$. Then using the classical Weil bound

$$|S(a,b;c)| \leq \tau(c)(a,b,c)^{1/2} c^{1/2}$$

where $\tau(c)$ is the number of divisors of c, and the estimates (3.11) and (3.12), we have

$$\begin{aligned} |a(m)| &\leq 2\pi \sum_{\ell|6} \frac{|\mu(\ell)|}{\sqrt{\ell}} \sum_{\substack{0<c\equiv 0 \pmod{6/\ell} \\ (c,\ell)=1}} \frac{\left|S\left(-\bar{\ell}, m; c\right)\right|}{c} \left| I_1\left(\frac{M}{c}\right)\right| \\ &\leq \frac{1}{\sqrt{2}} m^{-1/4} S_1 + 8\pi^2 m^{1/2} S_2, \end{aligned}$$

where

$$S_1 := \sum_{\ell|6} \ell^{-1/4} \sum_{\substack{0<c\leq M \\ (c,\ell)=1}} \tau(c) \exp\left(\frac{4\pi\sqrt{m}}{\sqrt{\ell}\, c}\right)$$

and

$$S_2 := \sum_{\ell|6} \ell^{-1} \sum_{\substack{c>M \\ (c,\ell)=1}} \frac{\tau(c)}{c^{3/2}}.$$

Using the bound (see [43])

$$\tau(n) \le n^{1.538\frac{\log(2)}{\log(\log(n))}}, \quad n \ge 2,$$

which implies that $\tau(n) \le \sqrt{3}\, n^{1/2}$ for $n \ge 1$, we get

$$\begin{aligned} |S_1| &\le \sqrt{3} \exp\left(4\pi\sqrt{m}\right) \sum_{\ell \mid 6} \ell^{-1/4} \sum_{0<c\le M} c^{1/2} \\ &\le 2\sqrt{3}(4\pi)^{3/2} m^{3/4} \exp\left(4\pi\sqrt{m}\right). \end{aligned}$$

Also, we have that

$$|S_2| \le 2\sum_{c=1}^{\infty} \frac{\tau(c)}{c^{3/2}} = 2\zeta^2\left(\frac{3}{2}\right).$$

Then combining estimates yields $|a(m)| \le Cm^{1/2}\exp\left(4\pi\sqrt{m}\right)$ for $m \ge 1$, where $C := 8\sqrt{6}\pi^{3/2} + 16\pi^2\zeta^2\left(\frac{3}{2}\right)$. □

We now turn to the proof of Theorem 3.2.2.

Proof of Theorem 3.2.2. By (3.7), (3.9), and (3.10), we have that

$$\begin{aligned} S(n) &= \sum_{\substack{u>0 \\ u^2 \mid D_n}} \varepsilon(u) S_u(n) \\ &= \sum_{\substack{u>0 \\ u^2 \mid D_n}} \varepsilon(u) \sum_{Q \in \mathcal{Q}_{D_n/u^2}} f|_0 \gamma_Q\left(\tau_Q\right) \\ &= \sum_{\substack{u>0 \\ u^2 \mid D_n}} \varepsilon(u) \sum_{Q \in \mathcal{Q}_{D_n/u^2}} \zeta_Q e\left(-\frac{\tau_Q}{h_Q}\right) + E_1(n), \end{aligned}$$

where

$$E_1(n) := 12\mu\left(h_Q\right) \sum_{\substack{u>0 \\ u^2|D_n}} \varepsilon(u) h\left(\frac{D_n}{u^2}\right) + \sum_{m=1}^{\infty} \frac{a(m)}{\sqrt{m}} \sum_{\substack{u>0 \\ u^2|D_n}} \varepsilon(u) \sum_{Q \in \mathcal{Q}_{D_n/u^2}} \phi_{m,Q} e\left(\frac{m\tau_Q}{h_Q}\right).$$

We have that

$$\left| 12\mu\left(h_Q\right) \sum_{\substack{u>0 \\ u^2|D_n}} \varepsilon(u) h\left(\frac{D_n}{u^2}\right) \right| \leq 12 \sum_{\substack{u>0 \\ u^2|D_n}} h\left(\frac{D_n}{u^2}\right) = 12 H\left(D_n\right).$$

Next, we observe that

$$e\left(\frac{m\tau_Q}{h_Q}\right) = \zeta_{2a_Q h_Q}^{-b_Q m} \exp\left(-\frac{\pi m \sqrt{|D_n|/u^2}}{a_Q h_Q}\right),$$

where $\zeta_{2a_Q h_Q}$ is the primitive $2a_Q h_Q$-th root of unity defined by $\zeta_{2a_Q h_Q} := e\left(1/2a_Q h_Q\right)$. Since $Q \in \mathcal{Q}_{D_n/u^2}$ is reduced, the corresponding CM point τ_Q lies in the standard fundamental domain $\mathcal{F}$ for $SL_2(\mathbb{Z})$. In particular, we have that

$$\operatorname{Im}\left(\tau_Q\right) = \frac{\sqrt{|D_n|/u^2}}{2a_Q} \geq \frac{\sqrt{3}}{2},$$

which implies that

$$a_Q \leq \frac{\sqrt{|D_n|/u^2}}{\sqrt{3}}.$$

Since $h_Q \leq 6$, we have that

$$-\frac{\pi m \sqrt{|D_n|/u^2}}{a_Q h_Q} \leq -\frac{\pi m}{2\sqrt{3}}. \tag{3.13}$$

Then using (3.13) and Lemma 3.2.3, we obtain

$$\begin{aligned}\left|\sum_{m=1}^{\infty}\frac{a(m)}{\sqrt{m}}\sum_{\substack{u>0\\u^2|D_n}}\varepsilon(u)\sum_{Q\in\mathcal{Q}_{D_n/u^2}}\phi_{m,Q}e\left(\frac{m\tau_Q}{h_Q}\right)\right|&\\
\leq\sum_{m=1}^{\infty}\frac{|a(m)|}{\sqrt{m}}\sum_{\substack{u>0\\u^2|D_n}}\sum_{Q\in\mathcal{Q}_{D_n/u^2}}\left|e\left(\frac{m\tau_Q}{h_Q}\right)\right|&\\
\leq CH(D_n)\sum_{m=1}^{\infty}\exp\left(4\pi\sqrt{m}-\frac{\pi m}{2\sqrt{3}}\right).&\end{aligned}$$

Combining the preceding estimates yields

$$|E_1(n)|\leq 12H(D_n)+CH(D_n)\sum_{m=1}^{\infty}\exp\left(4\pi\sqrt{m}-\frac{\pi m}{2\sqrt{3}}\right).$$

To estimate the infinite sum, we write

$$4\pi\sqrt{m}-\frac{\pi m}{2\sqrt{3}}=-m\left(\frac{\pi}{2\sqrt{3}}-\frac{4\pi}{\sqrt{m}}\right),$$

and we observe that $\frac{\pi}{2\sqrt{3}}-\frac{4\pi}{\sqrt{m}}>0$ if and only if $m\geq 193$, in which case we have that

$$-m\left(\frac{\pi}{2\sqrt{3}}-\frac{4\pi}{\sqrt{m}}\right)\leq -m\left(\frac{\pi}{2\sqrt{3}}-\frac{4\pi}{\sqrt{193}}\right).$$

We then split the infinite sum into appropriate ranges and use the preceding bound to obtain

$$\begin{aligned}\sum_{m=1}^{\infty}\exp\left(4\pi\sqrt{m}-\frac{\pi m}{2\sqrt{3}}\right)&\\
\leq\sum_{m=1}^{192}\exp\left(4\pi\sqrt{m}-\frac{\pi m}{2\sqrt{3}}\right)+\sum_{m=193}^{\infty}\exp\left(-m\left(\frac{\pi}{2\sqrt{3}}-\frac{4\pi}{\sqrt{193}}\right)\right).&\end{aligned}$$

A calculation shows that

$$\sum_{m=1}^{192} \exp\left(4\pi\sqrt{m} - \frac{\pi m}{2\sqrt{3}}\right) < 2.08 \times 10^{20}$$

and

$$\sum_{m=193}^{\infty} \exp\left(-m\left(\frac{\pi}{2\sqrt{3}} - \frac{4\pi}{\sqrt{193}}\right)\right) < 426.$$

We have now shown that $|E_1(n)| \le C_1 H(D_n)$, where

$$C_1 := 12 + C\left(2.08 \times 10^{20} + 426\right) < 2.47 \times 10^{23}.$$

It remains to analyze the main term. We write the main term as

$$\sum_{\substack{u>0\\u^2|D_n}} \varepsilon(u) \sum_{Q\in\mathcal{Q}_{D_n/u^2}} \zeta_Q e\left(-\frac{\tau_Q}{h_Q}\right) = \sum_{Q\in\mathcal{Q}_{D_n}} \zeta_Q e\left(-\frac{\tau_Q}{h_Q}\right) + E_2(n),$$

where

$$E_2(n) := \sum_{\substack{u\ge 2\\u^2|D_n}} \varepsilon(u) \sum_{Q\in\mathcal{Q}_{D_n/u^2}} \zeta_Q e\left(-\frac{\tau_Q}{h_Q}\right).$$

We observe that for any form $Q = [a_Q, b_Q, c_Q] \in \mathcal{Q}_{D_n/u^2}$, we have that

$$a_Q h_Q \equiv 0 \pmod 6 \tag{3.14}$$

and

$$e\left(-\frac{\tau_Q}{h_Q}\right) = \zeta_{2a_Q h_Q}^{b_Q} \exp\left(\frac{\pi\sqrt{|D_n|/u^2}}{a_Q h_Q}\right). \tag{3.15}$$

Now, by [24, (4.2)] there are exactly four forms $Q \in \mathcal{Q}_{D_n}$ with $a_Q h_Q = 6$, and these are given by $Q_1 = [1, 1, 6n]$, $Q_2 = [2, 1, 3n]$, $Q_3 = [3, 1, 2n]$, $Q_4 = [6, 1, n]$. The corresponding coset representatives $\gamma_{Q_i} \in \mathbf{C}_6$ such that $\left[Q_i \circ \gamma_{Q_i}^{-1}\right] \in \mathcal{Q}^{\text{prim}}_{D_n,6,1}/\Gamma_0(6)$ are given by $\gamma_{Q_1} = \gamma_{0,1}$, $\gamma_{Q_2} = \gamma_{1/2,-1}$, $\gamma_{Q_3} = \gamma_{1/3,0}$, $\gamma_{Q_4} = \gamma_{\infty}$.. We may now write

$$\sum_{Q \in \mathcal{Q}_{D_n}} \zeta_Q e\left(-\frac{\tau_Q}{h_Q}\right) = \sum_{i=1}^{4} \zeta_{Q_i} e\left(-\frac{\tau_{Q_i}}{h_{Q_i}}\right) + E_3(n),$$

where

$$E_3(n) := \sum_{\substack{Q \in \mathcal{Q}_{D_n} \\ Q \neq Q_i}} \zeta_Q e\left(-\frac{\tau_Q}{h_Q}\right).$$

By (3.14), we have that $a_Q h_Q \geq 12$ for all $Q \neq Q_i$. Therefore, using (3.15), we get

$$\begin{aligned} |E_3(n)| &\leq \sum_{\substack{Q \in \mathcal{Q}_{D_n} \\ Q \neq Q_i}} \exp\left(\frac{\pi\sqrt{|D_n|}}{a_Q h_Q}\right) \\ &\leq h\left(D_n\right) \exp\left(\frac{\pi\sqrt{|D_n|}}{12}\right). \end{aligned}$$

Similarly, by (3.14) we have that $a_Q h_Q \geq 6$ for all $Q \in \mathcal{Q}_{D_n/u^2}$, and therefore for $u \geq 2$ we have that

$$\frac{\sqrt{|D_n|/u^2}}{a_Q h_Q} \leq \frac{\sqrt{|D_n|}}{12}.$$

Then by (3.15) we have

$$\begin{aligned} |E_2(n)| &\leq \sum_{\substack{u \geq 2 \\ u^2 | D_n}} \sum_{Q \in \mathcal{Q}_{D_n/u^2}} \exp\left(\frac{\pi\sqrt{|D_n|/u^2}}{a_Q h_Q}\right) \\ &\leq H(D_n) \exp\left(\frac{\pi\sqrt{|D_n|}}{12}\right). \end{aligned}$$

Since $a_{Q_i}h_{Q_i} = 6$ and $b_{Q_i} = 1$ for $i = 1, 2, 3, 4$, using (3.15) we get

$$\sum_{i=1}^{4} \zeta_{Q_i} e\left(-\frac{\tau_{Q_i}}{h_{Q_i}}\right) = \exp\left(\frac{\pi i}{6}\right)\sum_{i=1}^{4} \zeta_{Q_i} \cdot \exp\left(\frac{\pi\sqrt{|D_n|}}{6}\right).$$

Also, from the Fourier expansion of $f(z)$ with respect to $\gamma_{0,1}, \gamma_{1/2,-1}, \gamma_{1/3,0}$, and γ_∞ given previously, we have that $\zeta_{Q_1} = \zeta_6^{-1}$, $\zeta_{Q_2} = \zeta_6^{3-2(-1)}$, $\zeta_{Q_3} = \zeta_6^0$, $\zeta_{Q_4} = 1$. Hence,

$$\exp\left(\frac{\pi i}{6}\right)\sum_{i=1}^{4} \zeta_{Q_i} = 2\sqrt{3}.$$

By combining the preceding results, we get

$$S(n) = 2\sqrt{3}\exp\left(\frac{\pi\sqrt{|D_n|}}{6}\right) + E(n),$$

where $E(n) := E_1(n) + E_2(n) + E_3(n)$ with

$$\begin{aligned}|E(n)| &\leq |E_1(n)| + |E_2(n)| + |E_3(n)| \\ &< 2H(D_n)\exp\left(\frac{\pi\sqrt{|D_n|}}{12}\right) + \left(2.47 \times 10^{23}\right) H\left(D_n\right) \\ &< \left(2.48 \times 10^{23}\right) H\left(D_n\right)\exp\left(\frac{\pi\sqrt{|D_n|}}{12}\right).\end{aligned}$$

To complete the proof, we require only a crude effective upper bound for the Hurwitz–Kronecker class number $H\left(D_n\right)$.

Write $D_n = d_n f_n^2$, with $d_n < 0$ a fundamental discriminant and $f_n \in \mathbb{Z}^+$. Then we have the class number relation

$$H(D_n) = \sum_{\substack{u>0 \\ u^2|D_n}} h\left(\frac{D_n}{u^2}\right) = \sum_{\substack{u>0 \\ u|f_n}} h\left(u^2 d_n\right). \tag{3.16}$$

Inserting the formula (see e.g. [13, p. 233])

$$h(u^2 d_n) = u \prod_{p|u} \left(1 - \frac{\chi_{d_n}(p)}{p}\right) h(d_n)$$

into (3.16) yields $H(D_n) = \delta(n)h(d_n)$, where

$$\delta(n) := \sum_{\substack{u>0 \\ u|f_n}} u \prod_{p|u} \left(1 - \frac{\chi_{d_n}(p)}{p}\right).$$

Now, a simple estimate gives $|\delta(n)| \leq \sqrt{|D_n|}\, \tau(|D_n|) 2^{\omega(|D_n|)}$, where $\omega(|D_n|)$ is the number of prime divisors of $|D_n|$. We have that $\tau(|D_n|) < \sqrt{3}\sqrt{|D_n|}$, and by [51, Théorème 13], we have that

$$\omega(|D_n|) \leq \max\left\{1, \frac{\log(|D_n|)}{\log(\log(|D_n|)) - 1.1714}\right\} \leq \frac{\log(|D_n|)}{|\log(\log(|D_n|)) - 1.1714|} =: q(n).$$

Therefore, $|\delta(n)| \leq \sqrt{3}\, 2^{q(n)}|D_n|$. Using the class number formula

$$h(d_n) = \frac{\sqrt{|d_n|}}{\pi} L(1, \chi_{d_n}),$$

where the L-function $L(s, \chi)$ is defined by $L(s, \chi) := \sum_{n=1}^{\infty} \chi(n)n^{-s}$, and the evaluation

$$L(1, \chi_{d_n}) = -\frac{\pi}{|d_n|^{3/2}} \sum_{t=1}^{|d_n|-1} \chi_{d_n}(t)t,$$

another simple estimate yields $h(d_n) \leq |d_n|$. Then combining the preceding estimates gives $H(D_n) \leq \sqrt{3}\, 2^{q(n)}|D_n|^2$.

Finally, using the above class number bound, we obtain

$$|E(n)| < \left(4.30 \times 10^{23}\right) 2^{q(n)}|D_n|^2 \exp\left(\frac{\pi\sqrt{|D_n|}}{12}\right).$$

This completes the proof. □

Now, we must apply an effective bound for $p(n)$ in order to prove Theorem 1.1.2. Using Rademacher's formula (1.3), Lehmer [39] proved the following result.

Theorem 3.2.4 (Lehmer)**.** *For all $n \geq 1$, we have that*

$$p(n) = \frac{\sqrt{12}}{24n-1} \sum_{c=1}^{N} \frac{A_c(n)}{\sqrt{c}} \left\{ \left(1 - \frac{c}{\lambda(n)}\right) e^{\lambda(n)/c} + \left(1 + \frac{c}{\lambda(n)}\right) e^{-\lambda(n)/c} \right\} + R_2(n, N),$$

where

$$|R_2(n, N)| < \frac{N^{-2/3}\pi^2}{\sqrt{3}} \left\{ \frac{N^3}{2\lambda(n)^3} \left(e^{\lambda(n)/N} - e^{-\lambda(n)/N}\right) + \frac{1}{6} - \frac{N^2}{\lambda(n)^2} \right\}.$$

We use Theorem 3.2.4 to deduce the following effective bound.

Lemma 3.2.5. *For all $n \geq 1$, we have that*

$$p(n) = \frac{2\sqrt{3}}{24n-1} \left(1 - \frac{1}{\lambda(n)}\right) e^{\lambda(n)} + E_p(n),$$

where $|E_p(n)| \leq 1313\, e^{\lambda(n)/2}$.

Proof of Lemma 3.2.5. Using the identity

$$I_{3/2}(x) = \frac{1}{2}\sqrt{\frac{2}{\pi x}} \left[\left(1 - \frac{1}{x}\right) e^{x} + \left(1 + \frac{1}{x}\right) e^{-x} \right], \tag{3.17}$$

we may write Theorem 3.2.4 (with the choice $N = 2$) as

$$p(n) = \frac{2\pi}{(24n-1)^{3/4}} \sum_{c=1}^{2} \frac{A_c(n)}{c} I_{3/2}\left(\frac{\lambda(n)}{c}\right) + R_2(n, 2), \tag{3.18}$$

where

$$|R_2(n,2)| < \frac{\pi^2}{\sqrt{3}\,2^{2/3}}\left[\left(\frac{2}{\lambda(n)}\right)^3\left\{\frac{e^{\lambda(n)/2}-e^{-\lambda(n)/2)}}{2}\right\}+1/6-\left(\frac{2}{\lambda(n)}\right)^2\right].$$

Now, using (3.17) and (3.18), we have that

$$\begin{aligned} p(n) &= \frac{2\pi}{(24n-1)^{3/4}} I_{3/2}\left(\lambda(n)\right) + \frac{2\pi}{(24n-1)^{3/4}}\frac{A_2(n)}{2} I_{3/2}\left(\frac{\lambda(n)}{2}\right) + R_2(n,2) \\ &= \frac{2\sqrt{3}}{24n-1}\left(1-\frac{1}{\lambda(n)}\right)e^{\lambda(n)} + E_p(n), \end{aligned}$$

where

$$\begin{aligned} E_p(n) := \frac{2\pi}{(24n-1)^{3/4}}&\left[\frac{1}{2}\sqrt{\frac{2}{\pi\lambda(n)}}\left(1+\frac{1}{\lambda(n)}\right)e^{-\lambda(n)} + \frac{A_2(n)}{2} I_{3/2}\left(\frac{\lambda(n)}{2}\right)\right] \\ &+ R_2(n,2). \end{aligned}$$

Using (3.17), we have the bound

$$I_{3/2}(x) < x^{-1/2}e^x, \quad x \geq 1. \tag{3.19}$$

Then an estimate using the trivial bound $|A_c(n)| < c$ and (3.19) yields

$$\left|\frac{2\pi}{(24n-1)^{3/4}}\frac{A_2(n)}{2} I_{3/2}\left(\frac{\lambda(n)}{2}\right)\right| \leq e^{\lambda(n)/2}.$$

Similarly, two straightforward estimates yield

$$\left|\frac{2\pi}{(24n-1)^{3/4}}\frac{1}{2}\sqrt{\frac{2}{\pi\lambda(n)}}\left(1+\frac{1}{\lambda(n)}\right)e^{-\lambda(n)}\right| \leq 16\,e^{\lambda(n)/2}$$

and $|R_2(n,2)| < 1296\,e^{\lambda(n)/2}$. Therefore, $|E_p(n)| \leq 1313\,e^{\lambda(n)/2}$. □

Using all of the tools established above, the proof of Theorem 1.1.2 is immediate.

Proof of Theorem 1.1.2. Using (3.2), the formula (3.3) can be written as

$$\operatorname{spt}(n) = \frac{1}{12}\left[S(n) - (24n-1)p(n)\right]. \tag{3.20}$$

Then using (3.20), Theorem 3.2.2, and Lemma 3.2.5, a straightforward calculation yields

$$\operatorname{spt}(n) = \frac{\sqrt{3}}{\pi\sqrt{24n-1}}e^{\lambda(n)} + E_s(n),$$

where the error term

$$E_s(n) := \frac{E(n)}{12} - \frac{24n-1}{12}E_p(n)$$

satisfies the bound

$$|E_s(n)| < \left(3.59 \times 10^{22}\right) 2^{q(n)}(24n-1)^2 e^{\lambda(n)/2}.$$

□

3.2.2 Inequalities satisfied by $\operatorname{spt}(n)$

We begin by proving the refined version of Theorem 1.1.1 (1).

Proof of Theorem 3.2.1. By Theorem 1.1.2 and Lemma 3.2.5, we may write

$$\operatorname{spt}(n) = \alpha(n)e^{\lambda(n)} + E_s(n) \tag{3.21}$$

and

$$p(n) = \beta(n)e^{\lambda(n)} + E_p(n), \tag{3.22}$$

where

$$\alpha(n) := \frac{\sqrt{3}}{\pi\sqrt{24n-1}} \quad \text{and} \quad \beta(n) := \frac{2\sqrt{3}}{24n-1}\left(1 - \frac{6}{\pi\sqrt{24n-1}}\right).$$

Also, for $\epsilon > 0$ we define

$$\gamma(n) := \frac{\sqrt{6}}{\pi}\sqrt{n} \quad \text{and} \quad \gamma(n,\epsilon) := \left(\frac{\sqrt{6}}{\pi} + \epsilon\right)\sqrt{n}.$$

We must prove that there exists an effectively computable positive constant $N(\epsilon) > 0$ such that for all $n \geq N(\epsilon)$, we have that

$$\gamma(n)p(n) < \mathrm{spt}(n) < \gamma(n,\epsilon)p(n). \tag{3.23}$$

Using (3.21) and (3.22) we find that the lower bound in (3.23) is equivalent to

$$c_1(n)e^{\lambda(n)} > \gamma(n)E_p(n) - E_s(n), \tag{3.24}$$

where $c_1(n) := \alpha(n) - \beta(n)\gamma(n)$. Now, the error bounds in Theorem 1.1.2 and Lemma 3.2.5 imply that

$$|\gamma(n)E_p(n) - E_s(n)| \leq c_2(n)e^{\lambda(n)/2},$$

where

$$c_2(n) := 1313\,\gamma(n) + \left(3.59 \times 10^{22}\right) 2^{q(n)}(24n-1)^2.$$

Then, noting that $c_1(n) > 0$ for all $n \geq 1$, we find that (3.24) follows from the bound

$$e^{\lambda(n)/2} > c_3(n) := \frac{c_2(n)}{c_1(n)},$$

or equivalently, the bound

$$n > \frac{1}{24}\left[\left(\frac{12}{\pi}\log(c_3(n))\right)^2 + 1\right]. \tag{3.25}$$

A calculation shows that (3.25) holds for all $n \geq N := 5310$.

Similarly, using (3.21) and (3.22), we find that the upper bound in (3.23) is equivalent to

$$c_4(n,\epsilon)e^{\lambda(n)} > E_s(n) - \gamma(n,\epsilon)E_p(n), \tag{3.26}$$

where $c_4(n,\epsilon) := \beta(n)\gamma(n,\epsilon) - \alpha(n)$. The error bounds in Theorem 1.1.2 and Lemma 3.2.5 imply that

$$|E_s(n) - \gamma(n,\epsilon)E_p(n)| \leq c_5(n,\epsilon)e^{\lambda(n)/2},$$

where

$$c_5(n,\epsilon) := 1313\,\gamma(n,\epsilon) + \left(3.59 \times 10^{22}\right)2^{q(n)}(24n-1)^2.$$

Moreover, there exists an effectively computable positive constant $N_1(\epsilon) > 0$ such that $c_4(n,\epsilon) > 0$ for all $n \geq N_1(\epsilon)$. Arguing as above, we find that if $n \geq N_1(\epsilon)$, the bound (3.26) follows from the bound

$$n > \frac{1}{24}\left[\left(\frac{12}{\pi}\log(c_6(n,\epsilon))\right)^2 + 1\right], \tag{3.27}$$

where $c_6(n,\epsilon) := c_5(n,\epsilon)/c_4(n,\epsilon)$. Clearly, there exists an effectively computable positive constant $N_2(\epsilon) \geq N_1(\epsilon)$ such that (3.27) holds for all $n \geq N_2(\epsilon)$. Define $N(\epsilon) := \max\{N, N_2(\epsilon)\}$. Then the inequalities (3.23) hold for all $n \geq N(\epsilon)$. $\square$

We require a preliminary lemma before we can prove Theorem 1.1.1. As pointed out by Bessenrodt and Ono [8], it is straightforward to see from Theorem 3.2.4 that

$$\frac{\sqrt{3}}{12n}\left(1-\frac{1}{\sqrt{n}}\right)e^{\lambda(n)} < p(n) < \frac{\sqrt{3}}{12n}\left(1+\frac{1}{\sqrt{n}}\right)e^{\lambda(n)}$$

for all $n \geq 1$.

We will use Theorem 1.1.2 to prove the following analogous statement for $\mathrm{spt}(n)$, where $\sqrt{n}$ is replaced by any positive integral power of n.

Lemma 3.2.6. *For each $\alpha \in \mathbb{Z}^+$ and $k \in \mathbb{Z}^+$, there is an effectively computable positive integer $B_k(\alpha)$ such that for all $n \geq B_k(\alpha)$, we have that*

$$\frac{\sqrt{3}}{\pi\sqrt{24n-1}}\left(1-\frac{1}{\alpha n^k}\right)e^{\lambda(n)} < \mathrm{spt}(n) < \frac{\sqrt{3}}{\pi\sqrt{24n-1}}\left(1+\frac{1}{\alpha n^k}\right)e^{\lambda(n)}.$$

Proof of Lemma 3.2.6. By Theorem 1.1.2, we have the bounds

$$\frac{\sqrt{3}}{\pi\sqrt{24n-1}}e^{\lambda(n)} - |E_s(n)| < \mathrm{spt}(n) < \frac{\sqrt{3}}{\pi\sqrt{24n-1}}e^{\lambda(n)} + |E_s(n)|,$$

where

$$|E_s(n)| < \left(3.59 \times 10^{22}\right) 2^{q(n)}(24n-1)^2 e^{\lambda(n)/2}.$$

Clearly, there is an effectively computable positive integer $B_k(\alpha)$ such that

$$\left(3.59 \times 10^{22}\right) 2^{q(n)}(24n-1)^2 e^{\lambda(n)/2} < \frac{\sqrt{3}}{\pi\sqrt{24n-1}} \cdot \frac{1}{\alpha n^k} e^{\lambda(n)}$$

holds for all $n \geq B_k(\alpha)$. For instance, if $\alpha = k = 1$, then $B_1(1) = 5729$. This completes the proof. □

We may now prove Theorem 1.1.1 (1) and (2).

Proof of Theorem 1.1.1 (1). Let $\epsilon = 1 - \frac{\sqrt{6}}{\pi}$ in Theorem 3.2.1. We need to determine the constant $N\left(1-\frac{\sqrt{6}}{\pi}\right)$. A calculation shows that $c_4\left(n,1-\frac{\sqrt{6}}{\pi}\right)>0$ holds if $n\geq N_1\left(1-\frac{\sqrt{6}}{\pi}\right)$, where $N_1\left(1-\frac{\sqrt{6}}{\pi}\right)=4$. Next, we need to find the smallest positive integer $N_2\left(1-\frac{\sqrt{6}}{\pi}\right)\geq 4$ such that the bound

$$n>\frac{1}{24}\left[\left(\frac{12}{\pi}\log\left(c_6\left(n,1-\frac{\sqrt{6}}{\pi}\right)\right)\right)^2+1\right]$$

holds for all $n\geq N_2\left(1-\frac{\sqrt{6}}{\pi}\right)$. A calculation shows that this constant is given by $N_2\left(1-\frac{\sqrt{6}}{\pi}\right)=4845$. We now have

$$N\left(1-\frac{\sqrt{6}}{\pi}\right):=\max\left\{N,N_2\left(1-\frac{\sqrt{6}}{\pi}\right)\right\}=\max\{5310,4845\}=5310.$$

Therefore, the inequalities

$$\frac{\sqrt{6}}{\pi}\sqrt{n}p(n)<\operatorname{spt}(n)<\sqrt{n}p(n)$$

hold for all $n\geq 5310$. Finally, one can verify with a computer that these inequalities also hold for $5\leq n<5310$. □

Proof of Theorem 1.1.1 (2). We follow closely the proof of [8, Theorem 2.1]. By taking $\alpha=k=1$ in Theorem 3.2.6 (recall that $B_1(1)=5729$), we find that

$$\frac{\sqrt{3}}{\pi\sqrt{24n-1}}\left(1-\frac{1}{n}\right)e^{\lambda(n)}<\operatorname{spt}(n)<\frac{\sqrt{3}}{\pi\sqrt{24n-1}}\left(1+\frac{1}{n}\right)e^{\lambda(n)}\tag{3.28}$$

holds for all $n\geq 5729$. One can verify with a computer that (3.28) also holds for $1\leq n<5729$.

Now, assume that $1<a\leq b$, and let $b=Ca$ where $C\geq 1$. From (3.28) we have

$$\operatorname{spt}(a)\operatorname{spt}(Ca)>\frac{3}{\pi^2\sqrt{24a-1}\sqrt{24Ca-1}}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{Ca}\right)e^{\lambda(a)+\lambda(Ca)}$$

and

$$\operatorname{spt}(a+Ca) < \frac{\sqrt{3}}{\pi\sqrt{24(a+Ca)-1}}\left(1+\frac{1}{a+Ca}\right)e^{\lambda(a+Ca)}.$$

Therefore, for all but finitely many cases, it suffices to find conditions on $a > 1$ and $C \geq 1$ such that

$$e^{\lambda(a)+\lambda(Ca)-\lambda(a+Ca)} > \frac{\pi\sqrt{24a-1}\sqrt{24Ca-1}}{\sqrt{3}\sqrt{24(a+Ca)-1}} \cdot \frac{\left(1+\frac{1}{a+Ca}\right)}{\left(1-\frac{1}{a}\right)\left(1-\frac{1}{Ca}\right)}. \tag{3.29}$$

For convenience, we define

$$T_a(C) := \lambda(a)+\lambda(Ca)-\lambda(a+Ca) \quad \text{and} \quad S_a(C) := \frac{\left(1+\frac{1}{a+Ca}\right)}{\left(1-\frac{1}{a}\right)\left(1-\frac{1}{Ca}\right)}.$$

Then by taking logarithms, we find that (3.29) is equivalent to

$$T_a(C) > \log\left(\frac{\pi\sqrt{24a-1}\sqrt{24Ca-1}}{\sqrt{3}\sqrt{24(a+Ca)-1}}\right) + \log(S_a(C)). \tag{3.30}$$

As functions of C, it can be shown that $T_a(C)$ is increasing and $S_a(C)$ is decreasing for $C \geq 1$, and thus $T_a(C) \geq T_a(1)$ and $\log(S_a(1)) \geq \log(S_a(C))$. Hence, it suffices to show that

$$T_a(1) > \log\left(\frac{\pi\sqrt{24a-1}\sqrt{24Ca-1}}{\sqrt{3}\sqrt{24(a+Ca)-1}}\right) + \log(S_a(1)).$$

Moreover, since

$$\frac{\sqrt{24Ca-1}}{\sqrt{24(a+Ca)-1}} \leq 1$$

for all $C \geq 1$ and all $a > 1$, it suffices to show that

$$T_a(1) > \log\left(\frac{\pi\sqrt{24a-1}}{\sqrt{3}}\right) + \log(S_a(1)). \tag{3.31}$$

By computing the values $T_a(1)$ and $S_a(1)$, we find that (3.31) holds for all $a \geq 6$.

To complete the proof, we assume that $2 \leq a \leq 5$. For each such integer a, we calculate the real number C_a for which

$$T_a\left(C_a\right) = \log\left(\frac{\pi\sqrt{24a-1}}{\sqrt{3}}\right) + \log(S_a\left(C_a\right)).$$

The values C_a are listed in the table below.

Table 3.3: Exceptional Cases of Theorem 1.1.1 (2)

a	C_a
2	27.87...
3	3.54...
4	1.79...
5	1.20...

By the discussion above, if $b = Ca \geq a$ is an integer for which $C > C_a$, then (3.30) holds, which in turn gives the theorem in these cases. Only finitely many cases remain: namely, the pairs of integers where $2 \leq a \leq 5$ and $1 \leq b/a \leq C_a$. We compute $\operatorname{spt}(a), \operatorname{spt}(b)$, and $\operatorname{spt}(a+b)$ in these cases to complete the proof. □

We require some results analogous to those of Desalvo and Pak [23] in order to prove the remaining conjectures. The following is [23, Lemma 2.1]; we omit the proof.

Lemma 3.2.7. *Suppose $h(x)$ is a positive, increasing function with two continuous derivatives for all $x > 0$, and that $h'(x) > 0$ is decreasing, and $h''(x) < 0$ is increasing for all $x > 0$. Then for all $x > 0$, we have that*

$$h''(x-1) < h(x+1) - 2h(x) + h(x-1) < h''(x+1).$$

By Theorem 1.1.2, we may write $\operatorname{spt}(n) = f(n) + E_s(n)$, where

$$f(n) := \frac{\sqrt{3}}{\pi\sqrt{24n-1}}e^{\lambda(n)} \tag{3.32}$$

and

$$|E_s(n)| < \left(3.59 \times 10^{22}\right) 2^{q(n)}(24n-1)^2 e^{\lambda(n)/2}.$$

Lemma 3.2.8. *Let $F(n) := 2\log(f(n)) - \log(f(n+1)) - \log(f(n-1))$. Then for all $n \geq 4$, we have that*

$$\frac{24\pi}{\left(24(n+1)-1\right)^{3/2}} - \frac{1}{n^2} < F(n) < \frac{24\pi}{\left(24(n-1)-1\right)^{3/2}} - \frac{288}{\left(24(n+1)-1\right)^2}.$$

Proof of Lemma 3.2.8. We can write $f(n)$ from (3.32) as

$$f(n) = \frac{1}{2\sqrt{3}\lambda(n)} e^{\lambda(n)},$$

so that $\log(f(n)) = \lambda(n) - \log(\lambda(n)) - \log\left(2\sqrt{3}\right)$. Then we have that

$$F(n) = 2\lambda(n) - \lambda(n+1) - \lambda(n-1) - 2\log(\lambda(n)) + \log(\lambda(n+1)) + \log(\lambda(n-1)).$$

Since the functions $\lambda(x)$ and $\widetilde{\lambda}(x) := \log(\lambda(x))$ satisfy the hypotheses of Lemma 3.2.7, we obtain $-\lambda''(n+1) + \widetilde{\lambda}''(n-1) < F(n) < -\lambda''(n-1) + \widetilde{\lambda}''(n+1)$. Computing derivatives gives

$$\frac{24\pi}{\left(24(n+1)-1\right)^{3/2}} - \frac{288}{\left(24(n-1)-1\right)^2} < F(n)$$

and

$$F(n) < \frac{24\pi}{\left(24(n-1)-1\right)^{3/2}} - \frac{288}{\left(24(n+1)-1\right)^2}$$

for all $n \geq 2$, from which we deduce that

$$\frac{24\pi}{\left(24(n+1)-1\right)^{3/2}} - \frac{1}{n^2} < F(n) < \frac{24\pi}{\left(24(n-1)-1\right)^{3/2}} - \frac{288}{\left(24(n+1)-1\right)^2}$$

for all $n \geq 4$. □

Lemma 3.2.9. *Define the functions* $y_n := |E_s(n)|/f(n)$,

$$M(n) := 2\sqrt{3}\left(3.59 \times 10^{22}\right)\lambda(n) 2^{q(n)}(24n-1)^2 e^{-\lambda(n)/2},$$

and $g(n) := M(n)/(1-M(n))$. *Then for all* $n \geq 2$, *we have that*

$$\log\left[\frac{(1-y_n)^2}{(1+y_{n+1})(1+y_{n-1})}\right] > -2g(n) - M(n+1) - M(n-1),$$
$$\log\left[\frac{(1+y_n)^2}{(1-y_{n+1})(1-y_{n-1})}\right] < 2M(n) + g(n+1) + g(n-1).$$

Proof of Lemma 3.2.9. First, we observe that for all $n \geq 1$, we have

$$0 < y_n = \frac{|E_s(n)|}{f(n)} < \frac{\left(3.59 \times 10^{22}\right) 2^{q(n)}(24n-1)^2 e^{\lambda(n)/2}}{\frac{1}{2\sqrt{3}\lambda(n)} e^{\lambda(n)}} = M(n). \tag{3.33}$$

The bound $M(n) < 1$ is equivalent to the bound

$$2\sqrt{3}\left(3.59 \times 10^{22}\right)\lambda(n) 2^{q(n)}(24n-1)^2 < e^{\lambda(n)/2}. \tag{3.34}$$

Clearly, there is an effectively computable positive integer M_0 such that the inequality (3.34) holds for all $n \geq M_0$. A calculation shows that (3.34) holds for all $n \geq M_0$ with $M_0 = 4698$. On the other hand, one can verify with a computer that $\max_{1 \leq n < 4698} y_n < 1$. Hence $y_n < 1$ for all $n \geq 1$. Then using (3.33) and the inequalities

$$\log(1-x) \geq -\frac{x}{1-x} \quad \text{for} \quad 0 < x < 1$$

and $\log(1+x) < x$ for $x > 0$, we obtain

$$\begin{aligned}\log\left[\frac{(1-y_n)^2}{(1+y_{n+1})(1+y_{n-1})}\right] &= 2\log(1-y_n) - \log(1+y_{n+1}) - \log(1+y_{n-1})\\ &> -\frac{2y_n}{1-y_n} - y_{n+1} - y_{n-1}\\ &> -2g(n) - M(n+1) - M(n-1)\end{aligned}$$

for all $n \geq 2$. Similarly, for all $n \geq 2$ we obtain

$$\begin{aligned}\log\left[\frac{(1+y_n)^2}{(1-y_{n+1})(1-y_{n-1})}\right] &= 2\log(1+y_n) - \log(1-y_{n+1}) - \log(1-y_{n-1})\\ &< 2y_n + \frac{y_{n+1}}{1-y_{n+1}} + \frac{y_{n-1}}{1-y_{n-1}}\\ &< 2M(n) + g(n+1) + g(n-1).\end{aligned}$$

□

Proposition 3.2.10. *Let*

$$\operatorname{spt}_2(n) := 2\log(\operatorname{spt}(n)) - \log(\operatorname{spt}(n+1)) - \log(\operatorname{spt}(n-1)).$$

Then we have $\operatorname{spt}_2(n) > \frac{1}{(24n)^{3/2}}$ *for all* $n \geq 6553$ *and* $\operatorname{spt}_2(n) < \frac{2}{n^{3/2}}$ *for all* $n \geq 6445$.

Proof of Proposition 3.2.10. We first bound $\operatorname{spt}(n)$ by

$$f(n)\left(1 - \frac{|E_s(n)|}{f(n)}\right) < \operatorname{spt}(n) < f(n)\left(1 + \frac{|E_s(n)|}{f(n)}\right).$$

Then, using $F(n) := 2\log(f(n)) - \log(f(n+1)) - \log(f(n-1))$ and $y_n := |E_s(n)|/f(n)$, we take logarithms in the preceding inequalities to get

$$F(n) + \log\left[\frac{(1-y_n)^2}{(1+y_{n+1})(1+y_{n-1})}\right] < \operatorname{spt}_2(n) < F(n) + \log\left[\frac{(1+y_n)^2}{(1-y_{n+1})(1-y_{n-1})}\right].$$

It follows immediately from Lemmas 3.2.8 and 3.2.9 that for all $n \geq 4$, we have that

$$\mathrm{spt}_2(n) > \frac{24\pi}{\big(24(n+1)-1\big)^{3/2}} - \frac{1}{n^2} - 2g(n) - M(n+1) - M(n-1)$$

and

$$\mathrm{spt}_2(n) < \frac{24\pi}{\big(24(n-1)-1\big)^{3/2}} - \frac{288}{\big(24(n+1)-1\big)^{2}} + 2M(n) + g(n+1) + g(n-1). \tag{3.35}$$

Then a calculation shows that

$$\frac{24\pi}{\big(24(n+1)-1\big)^{3/2}} - \frac{1}{n^2} - 2g(n) - M(n+1) - M(n-1) > \frac{1}{(24n)^{3/2}}$$

for all $n \geq 6553$ and

$$\frac{24\pi}{\big(24(n-1)-1\big)^{3/2}} - \frac{288}{\big(24(n+1)-1\big)^{2}} + 2M(n) + g(n+1) + g(n-1) < \frac{2}{n^{3/2}}$$

for all $n \geq 6445$. This completes the proof. □

We now prove the remaining conjectures.

Proof of Theorem 1.1.1 (3). To prove Theorem 1.1.1 (3), we must show that the inequality $\mathrm{spt}(n)^2 > \mathrm{spt}(n-1)\mathrm{spt}(n+1)$ holds for all $n \geq 36$. Taking logarithms, we see that this is equivalent to $\mathrm{spt}_2(n) > 0$, where $\mathrm{spt}_2(n)$ is defined as in Proposition 3.2.10. By the lower bound in Proposition 3.2.10, we have $\mathrm{spt}_2(n) > 0$ for all $n \geq 6553$. Finally, one can verify with a computer that $\mathrm{spt}_2(n) > 0$ for all $36 \leq n < 6553$. This completes the proof. □

Proof of Theorem 1.1.1 (4). We follow closely the proof of [23, Theorem 5.1]. It is known that log-concavity implies strong log-concavity $a(\ell - i)a(k+i) \geq a(k)a(\ell)$ for all $0 \leq k \leq \ell \leq n$ and $0 \leq i \leq \ell - k$ (see e.g. [52]).

Now, we have proved that $\mathrm{spt}(n)^2 > \mathrm{spt}(n-1)\mathrm{spt}(n+1)$ for all $n \geq 36$. Therefore, if we take $k = n - m$, $\ell = n + m$, and $i = m$, then $\mathrm{spt}(n)^2 > \mathrm{spt}(n-m)\mathrm{spt}(n+m)$ for all $n > m > 1$ with $n - m > 36$.

We next consider the case $n > m > 1$ with $1 \leq n - m \leq 36$. We will prove that

$$\mathrm{spt}(n)^2 \geq \mathrm{spt}(m+1)^2 > \mathrm{spt}(36)\mathrm{spt}(36+2m) \geq \mathrm{spt}(n-m)\mathrm{spt}(n+m) \tag{3.36}$$

for all $1 \leq n - m \leq 36$ with $m \geq 6244$. On the other hand, one can verify with a computer that $\mathrm{spt}(n)^2 > \mathrm{spt}(n-m)\mathrm{spt}(n+m)$ for all $1 \leq n-m \leq 36$ with $m < 6244$. This completes the proof of Conjecture (4), subject to verifying the inequalities (3.36).

Since $n \geq m+1$, we have that $\mathrm{spt}(n)^2 \geq \mathrm{spt}(m+1)^2$. Moreover, since $n-m \leq 36$ we have that $\mathrm{spt}(n-m) < \mathrm{spt}(36)$, and thus $\mathrm{spt}(36)\mathrm{spt}(36+2m) \geq \mathrm{spt}(n-m)\mathrm{spt}(n+m)$. This verifies the first and third inequalities in (3.36).

It remains to prove that

$$\mathrm{spt}(m+1)^2 > \mathrm{spt}(36)\mathrm{spt}(36+2m) \tag{3.37}$$

for all $m \geq 6244$. Taking logarithms in (3.37), we see that it suffices to prove

$$2\log(\mathrm{spt}(m+1)) - \log(\mathrm{spt}(36)) - \log(\mathrm{spt}(36+2m)) > 0 \tag{3.38}$$

for all $m \geq 6244$. By [32, Section 2] and [28, (4)], respectively, we have the bounds

$$\frac{e^{2\sqrt{m}}}{2\pi m e^{1/6m}} < p(m) < e^{\pi\sqrt{\frac{2m}{3}}}$$

for all $m \geq 1$. Then by the inequality in Theorem 1.1.1 (1), we have

$$\frac{\sqrt{6}}{\pi}\sqrt{m}\frac{e^{2\sqrt{m}}}{2\pi m e^{1/6m}} < \mathrm{spt}(m) < \sqrt{m}e^{\pi\sqrt{\frac{2m}{3}}} \tag{3.39}$$

for all $m \geq 5$. Using the inequalities (3.39) and $\mathrm{spt}(36) < 90000$, we see that the left hand side of (3.38) is bounded below by the function

$$2\log\left(\frac{\sqrt{6(m+1)}}{2\pi^2(m+1)e^{1/6(m+1)}}\right) + 4\sqrt{m+1} - \log(90000) \\ - \log\left(\sqrt{36+2m}\right) - \frac{\pi\sqrt{2(36+2m)}}{\sqrt{3}}$$

for all $m \geq 4$. A calculation shows that this function is positive for all $m \geq 6244$. □

Proof of Theorem 1.1.1 (5). Taking logarithms, we find that Theorem 1.1.1 (5) is equivalent to

$$\mathrm{spt}_2(n) < \log\left(1 + \frac{1}{n}\right)$$

for all $n \geq 13$. By the upper bound in Proposition 3.2.10 and some straightforward estimates, we have that

$$\mathrm{spt}_2(n) < \frac{2}{n^{3/2}} < \frac{1}{n+1} < \log\left(1 + \frac{1}{n}\right)$$

for all $n \geq 6445$. Finally, one can verify with a computer that the conjectured inequality holds for all $13 \leq n < 6445$. This completes the proof. □

Proof of Theorem 1.1.1 (6). We follow closely the proof of [10, Conjecture 1.3]. Taking logarithms, we find that Theorem 1.1.1 (6) is equivalent to

$$\mathrm{spt}_2(n) < \log\left(1 + \frac{\pi}{\sqrt{24}n^{3/2}}\right)$$

for all $n \geq 73$. By (3.35), we have that

$$\mathrm{spt}_2(n) < \frac{24\pi}{\big(24(n-1)-1\big)^{3/2}} - \frac{288}{\big(24(n+1)-1\big)^{2}} + 2M(n) + g(n+1) + g(n-1)$$

for all $n \geq 4$. On the other hand, by [10, (2.3)], we have that

$$\frac{24\pi}{\big(24(n+1)-1\big)^{3/2}} < \frac{24\pi}{(24n)^{3/2}} - \left(\frac{24\pi}{(24n)^{3/2}}\right)^2 + \frac{3}{2n^{5/2}}$$

for all $n \geq 50$, and by [10, (2.23)], we have that

$$-\frac{288}{\big(24(n+1)-1\big)^2} < \frac{1}{6n^{5/2}} - \frac{1}{2n^2}$$

for all $n \geq 50$. Therefore, for all $n \geq 50$, we have that

$$\mathrm{spt}_2(n) < \frac{24\pi}{(24n)^{3/2}} - \left(\frac{24\pi}{(24n)^{3/2}}\right)^2 + \frac{5}{3n^{5/2}} - \frac{1}{2n^2} + 2M(n) + g(n+1) + g(n-1).$$

Now, a calculation shows that

$$\frac{5}{3n^{5/2}} - \frac{1}{2n^2} + 2M(n) + g(n+1) + g(n-1) < 0$$

for all $n \geq 7211$. Hence,

$$\mathrm{spt}_2(n) < \frac{24\pi}{(24n)^{3/2}} - \left(\frac{24\pi}{(24n)^{3/2}}\right)^2 = \frac{24\pi}{(24n)^{3/2}}\left(1 - \frac{24\pi}{(24n)^{3/2}}\right)$$

for all $n \geq 7211$. Then using the inequality $x(1-x) < \log(1+x)$ for $x > 0$, we obtain

$$\mathrm{spt}_2(n) < \log\left(1 + \frac{24\pi}{(24n)^{3/2}}\right) = \log\left(1 + \frac{\pi}{\sqrt{24}n^{3/2}}\right)$$

for all $n \geq 7211$. Finally, one can verify with a computer that this inequality also holds for all $73 \leq n < 7211$. This completes the proof. □

3.3 Conjugacy growth series for finitary permutation groups

The coefficients of the conjugacy growth series corresponding to an infinite group G generated by a set S reveal some information about the algebraic complexity of G. In particular, they measure the number of elements of S required to fully generate the various conjugacy classes of G. Bacher and de la Harpe discovered [4] that the values of the partition function determine this information for the finitary symmetric group $\mathrm{Sym}(X)$ on an infinite set X. This relationship may not come as a surprise, since it is well known that the number of partitions of a positive integer n agrees with the number of conjugacy classes of the ordinary finite symmetric group S_n. It is more interesting that the complexity of the finitary alternating group $\mathrm{Alt}(X)$ is determined by products of values of the usual partition function $p(n)$ with values of the function $p_e(n)$ that counts partitions into an even number of parts. The most intriguing of the q-series identities in [4] is the identity that relates wreath products of $\mathrm{Sym}(X)$ to powers of the partition function. It is natural to seek an analogous statement for wreath products of $\mathrm{Alt}(X)$. This statement is given by Theorem 1.1.3, and the proof is omitted here (see [17] and [57]).

It turns out that the coefficients of the conjugacy growth series for symmetric and alternating wreath products actually satisfy recursive formulas depending on the number of conjugacy classes. These formulas are the content of Theorems 1.1.4 and 1.1.5, and they give another measure of the complexity of these groups.

3.3.1 Recurrence relations

Here we prove recurrence relations for the coefficients of the conjugacy growth series for symmetric and alternating wreath products.

Proof of Theorem 1.1.4. Define the q-series identity

$$F_r(q) := \sum_{n=0}^{\infty} p_n(r)q^n := \prod_{n=1}^{\infty}(1-q^n)^r,$$

so that $p_n(r) = \gamma_{W_S}(n)$ and $r = -M_S$. We take logarithms of both sides to obtain

$$\log\left(1+\sum_{n=1}^{\infty} p_n(r)q^n\right) = \sum_{n=1}^{\infty} r\log(1-q^n) = -\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{rq^{kn}}{k}.$$

Taking the derivatives of both sides, we see that

$$\frac{\sum\limits_{n=1}^{\infty} np_n(r)q^{n-1}}{1+\sum\limits_{n=1}^{\infty} p_n(r)q^n} = -\sum_{n=1}^{\infty}\sum_{d|n} rdq^{n-1} = -\sum_{n=1}^{\infty} r\sigma_1(n)q^{n-1},$$

and so we have that

$$\sum_{n=1}^{\infty} np_n(r)q^n = \left(-\sum_{n=1}^{\infty} r\sigma_1(n)q^n\right)\left(1+\sum_{n=1}^{\infty} p_n(r)q^n\right).$$

For convenience, we define $b(n) := r\sigma_1(n)$. Equating coefficients, we see that

$$0 = b(n) + b(n-1)p_1(r) + b(n-2)p_2(r) + \cdots + b(1)p_{n-1}(r) + np_n(r).$$

The symmetric power functions $s_i := X_1^i + \cdots + X_n^i$ and the elementary symmetric functions $\sigma_i = \sum\limits_{1\le j_1\le\cdots\le j_i\le n} X_{j_1}\cdots X_{j_i}$ exhibit a similar relationship; namely, we have the identity

$$0 = s_n - s_{n-1}\sigma_1 + s_{n-2}\sigma_2 - \cdots + (-1)^{n-1}s_1\sigma_{n-1} + (-1)^n\sigma_n. \tag{3.40}$$

Evaluating equation (3.40) at $(X_1,\ldots,X_n) = (\ell(1,n),\ldots,\ell(n,n))$, where $\ell(j,n)$ are the roots of the polynomial $X^n + p_1(r)X^{n-1} + \cdots + p_{n-1}(r)X + p_n(r)$, we have that

$p_n(r) = \sigma_n$ for $n \geq 1$, and so $b(n) = (-1)^n s_n$. Using the classical fact that

$$s_n = n \sum_{\substack{m_1,\ldots,m_n \geq 0 \\ m_1+\cdots+nm_n=i}} (-1)^{m_2+m_4+\cdots} \cdot \frac{(m_1+\cdots+m_n-1)!}{m_1!\cdots m_n!} \cdot \sigma_1^{m_1}\cdots\sigma_n^{m_n},$$

we arrive at the desired recursion: $p_n(r) = \widehat{F}_n\big(p_1(r),\ldots,p_{n-1}(r)\big) - \dfrac{r}{n}\sigma_1(n)$. □

Proof of Theorem 1.1.5. Define the q-series identity

$$F_{M_A}(q) := \sum_{n=0}^{\infty} P_n(M_A)q^n := \left(\frac{1}{2}\prod_{n=1}^{\infty}\frac{1}{(1-q^n)^2} + \frac{1}{2}\prod_{n=1}^{\infty}\frac{1}{1-q^{2n}}\right)^{M_A},$$

so that $P_n(M_A) = \gamma_{W_A}(n)$. By the binomial theorem, we have that

$$\sum_{n=0}^{\infty} P_n(M_A)q^n = \frac{1}{2^{M_A}}\sum_{k=1}^{M_A}\binom{M_A}{k}\prod_{n=1}^{\infty}\frac{1}{(1-q^n)^{2k}(1-q^{2n})^{M_A-k}}.$$

It suffices to find recurrence relations for each summand. Define

$$F_{M_A,k}(q) := \sum_{n=0}^{\infty} a_k(n)q^n := \prod_{n=1}^{\infty}\frac{1}{(1-q^n)^{2k}(1-q^{2n})^{M_A-k}}.$$

We take the logarithmic derivative as above and simplify to obtain

$$\sum_{n=1}^{\infty} na_k(n)q^n = \left(-\sum_{n=1}^{\infty}\sum_{d|n} d\cdot\left[(-1)^{\frac{n}{d}}(k-M_A)-(k+M_A)\right]q^n\right)\left(1+\sum_{n=1}^{\infty}a_k(n)q^n\right),$$

and then we equate coefficients and use (3.40) as in the proof of Theorem 1.1.4 to obtain the desired recursion:

$$a_k(n) = \widehat{F}_n\big(a_k(1),\ldots,a_k(n-1)\big) - \sum_{\delta|n}\delta\cdot\left[(-1)^{\delta}(k-M_A)-(k+M_A)\right].$$

□

3.3.2 An application to hook lengths

We now discuss an application to hook lengths of partitions. The *hook length* of a partition $\lambda = (\lambda_1, \ldots, \lambda_n)$ of a positive integer L, i.e. $\lambda_1 + \cdots + \lambda_n = L$, is defined using a Ferrers diagram. For example, Figure 3.1 below is a Ferrers diagram of the partition $\lambda = (6, 4, 3, 1, 1)$ of 15, Figure 3.2 shows a hook of length 4, and Figure 3.3 shows all hook lengths associated to λ.

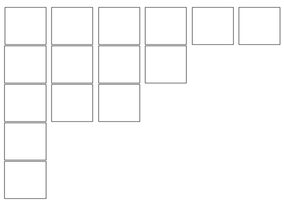

Figure 3.1: Partition

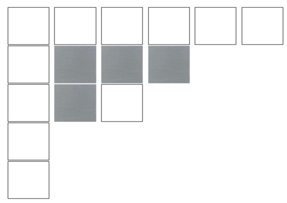

Figure 3.2: Hook

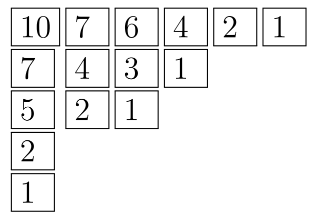

Figure 3.3: Hook Lengths

More generally, for each box v in the Ferrers diagram of a partition λ, its *hook length* $h_v(\lambda)$ is defined as the number of boxes u such that

1. $u = v$,

2. u is in the same column as v and below v, or

3. u is in the same row as v and to the right of v.

The *hook length multi-set* $\mathcal{H}(\lambda)$ is the set of all hook lengths of λ.

Consider the more general infinite product $\prod_{n \geq 1} (1 - q^n)^r$ for any $r \in \mathbb{C}$. In recent work, Nekrasov and Okounkov obtained a different formula for this type of infinite product in terms of hook lengths [42]:

$$\sum_{\lambda \in \mathcal{P}} x^{|\lambda|} \prod_{h \in \mathcal{H}(\lambda)} \left(1 - \frac{z}{h^2}\right) = \prod_{k \geq 1} \left(1 - x^k\right)^{z-1}, \tag{3.41}$$

where $\mathcal{P}$ denotes the set of all partitions and $|\lambda|$ denotes the sum of the parts of λ. Theorem 1.1.4 applies to the coefficients of the Nekrasov–Okounkov formula (3.41) if we make the following changes of variable: $z \mapsto 1 + r$ and $x \mapsto q := e^{2\pi i\tau}$ with $\tau \in \mathbb{H}$. The coefficients $\prod_{h \in \mathcal{H}(\lambda)} \left(1 - \frac{1+r}{h^2}\right)$ of the product $\prod_{n \geq 1} (1 - q^n)^r$ then satisfy the recurrence relation

$$\prod_{h \in \mathcal{H}(\lambda)} \left(1 - \frac{1+r}{h^2}\right) = \gamma_{W_S}(n) = \widehat{F}_n\big(\gamma_{W_S}(1), \ldots, \gamma_{W_S}(n-1)\big) - \frac{r}{n}\sigma_1(n).$$

Although for $r \in \mathbb{C} \setminus \mathbb{Z}^+$ we can no longer observe the relationship between the number of conjugacy classes and the coefficients of the conjugacy growth series of $H_S \wr_X \operatorname{Sym}(X)$, we do obtain a simple recursion for the famous Nekrasov–Okounkov hook length formula which is independent of complex analysis and hook lengths.

Chapter 4

Prime Numbers

The density of the set of prime numbers within the set of all positive integers is given by the Prime Number Theorem. Namely, if $\pi(X) := \#\{p \leq X : p \text{ is prime}\}$ denotes the prime counting function, then we have that $\pi(X) \sim X/\log X$. It is then natural to study densities of subsets of prime numbers within the set of all prime numbers. Dirichlet's Theorem on primes in arithmetic progressions was the first result in this area: if ℓ and k are relatively prime integers, then the density of the set of primes $p \equiv \ell \pmod{k}$ within the set of all primes is $1/\varphi(k)$, where $\varphi(k) := \#\{1 \leq a \leq k : \gcd(a, k) = 1\}$ is Euler's φ-function. In other words, the primes are equidistributed in allowable arithmetic progressions modulo any given integer k. One can view Dirichlet's Theorem as the special case of the more general Chebotarev Density Theorem corresponding to a cyclotomic extension $K = \mathbb{Q}(\zeta_k)$, where ζ_k is some primitive kth root of unity.

Inspired by work of Alladi [2], we reproduce Chebotarev densities of certain subsets of prime numbers through an infinite sum involving the Möbius function. In order to prove this result, we first recall the Chebotarev Density Theorem.

4.1 Some algebraic number theory

Our main result on prime numbers depends on the Chebotarev Density Theorem, which we carefully state here. We must first give all of the machinery required to define the most general form of the Artin symbol. Let L/K be a finite Galois extension of number fields with Galois group $G := \mathrm{Gal}(L/K)$, and let $\mathcal{O}_L$ and $\mathcal{O}_K$ be the corresponding rings of integers. Let $\mathfrak{p}$ be any nonzero prime (maximal) ideal in $\mathcal{O}_K$. The ideal generated in $\mathcal{O}_L$ by $\mathfrak{p}$ uniquely splits into distinct maximal ideals $\mathfrak{P}_j$ lying over $\mathfrak{p}$ in the following way: there exists an integer $g \geq 1$ such that $\mathfrak{p}\mathcal{O}_L = \prod_{j=1}^{g} \mathfrak{P}_j^{e_j}$. We say the ideal $\mathfrak{p}$ is *unramified* in L if $e_j = 1$ for all $1 \leq j \leq g$, which occurs for all but finitely many prime ideals. We must also define the *absolute norm* of a nonzero ideal $\mathfrak{a}$ of the ring of integers $\mathcal{O}_F$ of some number field F by $\mathrm{Nm}(\mathfrak{a}) := [\mathcal{O}_F : \mathfrak{a}] = |\mathcal{O}_F/\mathfrak{a}|$.

For any prime ideal $\mathfrak{P}$ lying over $\mathfrak{p}$, the *Artin symbol* $\left[\frac{L/K}{\mathfrak{P}}\right]$ is defined as the unique element $\sigma \in G$ such that $\sigma(\alpha) = \alpha^{\mathrm{Nm}(\mathfrak{p})} \pmod{\mathfrak{P}}$ for all $\alpha \in L$. All of the prime ideals $\mathfrak{P}_j$ lying over $\mathfrak{p}$ are isomorphic by elements of G, and $\left[\frac{L/K}{\tau(\mathfrak{P}_j)}\right] = \tau \left[\frac{L/K}{\mathfrak{P}_j}\right] \tau^{-1}$ for $\tau \in G$, so there exists a conjugacy class C associated to $\mathfrak{p}$ such that each $\left[\frac{L/K}{\mathfrak{P}_j}\right]$ lies in C. We define the Artin symbol $\left[\frac{L/K}{\mathfrak{p}}\right]$ to be the conjugacy class $C = \left\{\left[\frac{L/K}{\mathfrak{P}_j}\right] : 1 \leq j \leq g\right\}$.

We now define density. Let K be a number field. Let $Q(K)$ be some set of prime ideals of $\mathcal{O}_K$, and let $P(K)$ be the set of all prime ideals of $\mathcal{O}_K$. The *natural density* of $Q(K)$ is defined by

$$\lim_{X\to\infty} \frac{\#\{\mathfrak{p} \in Q(K) : \mathrm{Nm}(\mathfrak{p}) \leq X\}}{\#\{\mathfrak{p} \in P(K) : \mathrm{Nm}(\mathfrak{p}) \leq X\}},$$

provided the limit exists.

For a conjugacy class $C \subset G$, we define P_C to be the set of prime ideals defined by $P_C := \left\{\mathfrak{p} \in P(K) : \mathfrak{p} \text{ is unramified in } L, \left[\frac{L/K}{\mathfrak{p}}\right] = C\right\}$. For convenience, we define the prime ideal counting function

$$\pi_C(X, L/K) \;\; := \;\; \#\{\mathfrak{p} \in P_C : \mathrm{Nm}(\mathfrak{p}) \leq X\}.$$

In other words, $\pi_C(X, L/K)$ counts the number of prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ unramified in L which have Artin symbol C and bounded norm $\mathrm{Nm}(\mathfrak{p}) \leq X$.

We now recall the Chebotarev Density Theorem [56]. Let L/K be a finite Galois extension of number fields, and let C be a conjugacy class of $G := \mathrm{Gal}(L/K)$. Then, as $X \to \infty$, we have that

$$\pi_C(X, L/K) = \frac{\#C}{\#G} \cdot \frac{X}{\log X} + o\left(\frac{X}{\log X}\right).$$

Specifically, the density of P_C within the set of all unramified prime ideals of $\mathcal{O}_K$ exists and equals $\#C/\#G$. For this reason, a density of the form $\#C/\#G$ is referred to as *Chebotarev density*.

We require a more precise formulation of the Chebotarev Density Theorem which was proven by Lagarias and Odlyzko [38, Theorems 1.3 and 1.4].

Theorem 4.1.1 (Lagarias–Odlyzko)**.** *For sufficiently large $X \geq c_1\,(D_L, n_L)$, where the constant c_1 depends on both the discriminant D_L and the degree n_L of L, we have*

$$\left|\pi_C(X, L/K) - \frac{\#C}{\#G}\,\mathrm{Li}(X)\right| \leq 2c_2\, X \exp\left\{-c_3\,(n_L)^{-1/2}\,\sqrt{\log X}\right\}$$

for constants c_2 and c_3.

Note that $\mathrm{Li}(X) := \int_2^X dt/\log t$, and that $\mathrm{Li}(X) = \frac{X}{\log X} + o\left(\frac{X}{\log X}\right)$.

Remark. The constant c_1 can be made explicit using Theorems 1.3 and 1.4 of [38].

4.2 Chebotarev densities of subsets of primes

We require several tools in order to prove Theorem 1.2.1. We must first give estimates for relevant counting functions.

4.2.1 Intermediate estimates

We first prove an intermediate theorem about largest prime divisors of integers.

Theorem 4.2.1 (D). *Let K be a finite Galois extension of $\mathbb{Q}$ with Galois group G, and let $C \subset G$ be a conjugacy class. Then we have that*

$$\sum_{\substack{2 \leq n \leq X \\ \left[\frac{K/\mathbb{Q}}{p_{\max}(n)}\right] = C}} 1 = \frac{\#C}{\#G} \cdot X + O\left(X \exp\left\{-k(\log X)^{1/3}\right\}\right), \tag{4.1}$$

where k is a positive constant.

To set up the proofs of Theorems 1.2.1 and 4.2.1, we define the function

$$\Psi(X, Y) := \sum_{\substack{n \leq X \\ p_{\max}(n) \leq Y}} 1,$$

which counts the number of integers $n \leq X$ with largest prime divisor $p_{\max}(n) \leq Y$. Let $\mathcal{S}(X, Y)$ denote the set of such integers $n \leq X$ with $p_{\max}(n) \leq Y$, so that clearly $|\mathcal{S}(X, Y)| = \Psi(X, Y)$.

We now state a theorem of Hildebrand [33] which improves an asymptotic bound for $\Psi(X, Y)$ given by de Bruijn [21]. We must first define the *Dickman function* $\rho(\beta)$ as the continuous solution of the system

$$\begin{aligned} \rho(\beta) &= 1 \quad \text{for } 0 \leq \beta \leq 1, \\ -\beta\rho'(\beta) &= \rho(\beta - 1) \quad \text{for } \beta > 1. \end{aligned}$$

Theorem 4.2.2 (Hildebrand)**.** *We have that*

$$\Psi(X,Y) = X\rho(\beta)\left(1 + O_\epsilon\left(\frac{\beta\log(\beta+1)}{\log X}\right)\right)$$

uniformly in the range $X \geq 3, 1 \leq \beta \leq \log X/(\log\log X)^{5/3+\epsilon}$, *for any fixed* $\epsilon > 0$.

The following unpublished theorem of Maier [41] can be recognized as a corollary of Hildebrand's Theorem, and this corollary will be sufficient to prove our results.

Corollary 4.2.3 (Maier)**.** *If* $\beta = \frac{\log X}{\log Y}$, *then for* X *sufficiently large (where* β *varies with* X*) we have that* $\Psi(X,Y) \sim X\rho(\beta)$ *uniformly in the range* $1 \leq \beta \leq (\log X)^{1-\epsilon}$ *for any fixed* $\epsilon > 0$.

It turns out that for $1 \leq \beta \leq (\log X)^{1-\epsilon}$, we have that

$$\Psi(X,Y) = O_\epsilon\left(X\exp\left\{-\beta\log\beta/2\right\}\right). \tag{4.2}$$

The O-constant depends on ϵ, and we choose $\epsilon = 2/3$ in the proof of Theorem 4.2.1. To obtain (4.2), we require Norton's upper bound $\rho(\beta) \leq \frac{1}{\Gamma(\beta+1)}$ [44, Lemma 4.7]. Applying Stirling's formula, we see that

$$\rho(\beta) \sim \frac{1}{\sqrt{2\pi\beta}}\exp\left\{-\beta\log\beta/e\right\}. \tag{4.3}$$

From (4.3) and Corollary 4.2.3, it is straightforward to see that (4.2) holds.

These estimates will be useful in bounding error terms in the proof of Theorem 1.2.1. The following lemma will also be useful in obtaining estimates.

Lemma 4.2.4. *For* $a \leq X$ *and* $\mathcal{S}(X,Y)$ *defined as above, we have that*

$$\int_a^X \left(\sum_{n\in\mathcal{S}(X/t,t)} 1\right)dt = \sum_{\substack{1\leq n\leq X/a \\ p_{\max}(n)\leq X/n}} \int_{\max\left\{p_{\max}(n),a\right\}}^{X/n} dt.$$

Proof. Looking at the (Stieltjes) integral on the left hand side, a given integer n occurs whenever t is in the range $t \geq a$, $t \geq p_{\max}(n)$, and $t \leq X/n$. Therefore, the integer n contributes to the integral the length of the interval from $\max\left\{p_{\max}(n), a\right\}$ to X/n, provided that $\max\left\{p_{\max}(n), a\right\} \leq X/n$. This is precisely the contribution of n to the sum on the right hand side. $\square$

We now turn to the proof of Theorem 4.2.1. The proof closely follows the proof of the corresponding theorem in [2]. Note that $c_4, \ldots, c_9$ are positive constants which will not be specified in the following proof.

Proof of Theorem 4.2.1. We first rewrite the desired sum in terms of the function $\Psi(X, Y)$, for which we have asymptotic bounds.

$$\sum_{\substack{2 \leq n \leq X \\ \left[\frac{K/\mathbb{Q}}{p_{\max}(n)}\right] = C}} 1 = \sum_{\substack{p \leq X \\ \left[\frac{K/\mathbb{Q}}{p}\right] = C}} \sum_{\substack{n \leq X \\ p_{\max}(n) = p}} 1 = \sum_{\substack{p \leq X \\ \left[\frac{K/\mathbb{Q}}{p}\right] = C}} \Psi\left(\frac{X}{p}, p\right).$$

Notice that this sum can be broken up into a sum over small primes and a sum over large primes, so that

$$\sum_{\substack{2 \leq n \leq X \\ \left[\frac{K/\mathbb{Q}}{p_{\max}(n)}\right] = C}} 1 = \sum_{\substack{p \leq \exp\left\{(\log X)^{2/3}\right\} \\ \left[\frac{K/\mathbb{Q}}{p}\right] = C}} \Psi\left(\frac{X}{p}, p\right) + \sum_{\substack{\exp\left\{(\log X)^{2/3}\right\} < p \leq X \\ \left[\frac{K/\mathbb{Q}}{p}\right] = C}} \Psi\left(\frac{X}{p}, p\right).$$

Let

$$S_1 := \sum_{\substack{p \leq \exp\left\{(\log X)^{2/3}\right\} \\ \left[\frac{K/\mathbb{Q}}{p}\right] = C}} \Psi\left(\frac{X}{p}, p\right) \quad \text{and} \quad S_2 := \sum_{\substack{\exp\left\{(\log X)^{2/3}\right\} < p \leq X \\ \left[\frac{K/\mathbb{Q}}{p}\right] = C}} \Psi\left(\frac{X}{p}, p\right).$$

We now estimate S_1 and show that it is much smaller than S_2. This implies that S_1 is not the main term in the asymptotic formula (4.1), so we only need to obtain an upper bound. We see that

$$S_1 = \sum_{\substack{p \le \exp\left\{(\log X)^{2/3}\right\} \\ \left[\frac{K/\mathbb{Q}}{p}\right]=C}} \Psi\left(\frac{X}{p}, p\right) \le \sum_{p \le \exp\left\{(\log X)^{2/3}\right\}} \Psi\left(\frac{X}{p}, p\right).$$

Let $Y = \exp\left\{(\log X)^{2/3}\right\}$. Then we have that $S_1 \le \Psi(X, Y) - 1$. If $Y = X^{1/\beta}$ for some β, then $\beta = (\log X)^{1/3}$. Thus, by (4.2) we have that

$$S_1 = O\left(X \exp\left\{-(\log X)^{1/3} \log\log X\right\}\right).$$

We now estimate S_2, which will provide the main term in the asymptotic formula (4.1). To obtain the main term, it will be convenient to define

$$S_3 := \sum_{\substack{\exp\left\{(\log X)^{2/3}\right\} < p \le X \\ \left[\frac{K/\mathbb{Q}}{p}\right]=C}} \Psi\left(\frac{X}{p}, p\right) - \frac{\#C}{\#G} \int_{\exp\left\{(\log X)^{2/3}\right\}}^{X} \Psi\left(\frac{X}{t}, t\right) \frac{dt}{\log t},$$

which means that

$$S_2 = \frac{\#C}{\#G} \int_{\exp\left\{(\log X)^{2/3}\right\}}^{X} \Psi\left(\frac{X}{t}, t\right) \frac{dt}{\log t} - S_3.$$

Our goal now is to show that S_3 is small compared to S_2. By the definition of $\Psi\left(\frac{X}{t}, t\right)$, we replace it with a function counting elements of $\mathcal{S}\left(\frac{X}{t}, t\right)$ to obtain

$$S_3 = \sum_{\substack{\exp\left\{(\log X)^{2/3}\right\} < p \le X \\ \left[\frac{K/\mathbb{Q}}{p}\right]=C}} \left(\sum_{n \in \mathcal{S}(X/p, p)} 1\right) - \frac{\#C}{\#G} \int_{\exp\left\{(\log X)^{2/3}\right\}}^{X} \left(\sum_{n \in \mathcal{S}(X/t, t)} 1\right) \frac{dt}{\log t}.$$

Applying Lemma 4.2.4 and switching the order of summation in the first term, we then have that

$$S_3 = \sum_{\substack{1\le n\le X\exp\left\{-(\log X)^{2/3}\right\}\\ p_{\max}(n)\le X/n}} \left(\sum_{\substack{p_{\max}(n)\le p\le X/n\\ p>\exp\left\{(\log X)^{2/3}\right\}\\ \left[\frac{K/\mathbb{Q}}{p}\right]=C}} 1 - \frac{\#C}{\#G}\int_{\max\left\{p_{\max}(n),\exp\{(\log X)^{2/3}\}\right\}}^{X/n} \frac{dt}{\log t} \right)$$

$$= \sum_{\substack{1\le n\le X\exp\left\{-(\log X)^{2/3}\right\}\\ p_{\max}(n)\le X/n}} \Bigg(\pi_C\left(\frac{X}{n}, K/\mathbb{Q}\right) - \pi_C\left(\max\left\{p_{\max}(n), \exp\left\{(\log X)^{2/3}\right\}\right\}, K/\mathbb{Q}\right) - \frac{\#C}{\#G}\,\mathrm{Li}\left(\frac{X}{n}\right) + \frac{\#C}{\#G}\,\mathrm{Li}\left(\max\left\{p_{\max}(n), \exp\left\{(\log X)^{2/3}\right\}\right\}\right) \Bigg).$$

Here we apply the explicit reformulation of the Chebotarev Density Theorem by Lagarias and Odlyzko [38] to obtain

$$|S_3| \le \sum_{\substack{1\le n\le X\exp\left\{-(\log X)^{2/3}\right\}\\ p_{\max}(n)\le X/n}} c_4\left(\frac{X}{n}\right)\exp\left\{-c_5\sqrt{\log\left(\frac{X}{n}\right)}\right\}.$$

Since each summand satisfies

$$c_4\left(\frac{X}{n}\right)\exp\left\{-c_5\sqrt{\log\left(\frac{X}{n}\right)}\right\} \le c_4\left(\frac{X}{n}\right)\exp\left\{-c_6(\log X)^{1/3}\right\},$$

we have that

$$S_3 = O\left(X\,\exp\left\{-c_7(\log X)^{1/3}\right\}\right).$$

We have used the fact that an absolute value upper bound of the remainder term in the Chebotarev Density Theorem is an increasing function of X, so we have replaced the terms $p_{\max}(n)$ and $\exp\left\{(\log X)^{2/3}\right\}$ by X/n. In order to get the main term of the asymptotic formula from S_2, we must show that the integral

$$\int_{\exp\{(\log X)^{2/3}\}}^{X} \Psi\left(\frac{X}{t}, t\right) \frac{dt}{\log t}$$

contributes a factor of X. Let $[X]$ denote the largest integer part of X. We see that

$$[X] - 1 = \sum_{2 \le n \le X} 1 = \sum_{p \le X} \Psi\left(\frac{X}{p}, p\right),$$

which we break up into a sum over small primes and a sum over large primes so that

$$[X] - 1 \quad = \sum_{p \le \exp\{(\log X)^{2/3}\}} \Psi\left(\frac{X}{p}, p\right) + \sum_{\exp\{(\log X)^{2/3}\} < p \le X} \Psi\left(\frac{X}{p}, p\right).$$

Let

$$S_1{}' := \sum_{p \le \exp\{(\log X)^{2/3}\}} \Psi\left(\frac{X}{p}, p\right) \quad \text{and} \quad S_2{}' := \sum_{\exp\{(\log X)^{2/3}\} < p \le X} \Psi\left(\frac{X}{p}, p\right).$$

By similar estimates, we have that

$$S_1{}' = O\left(X \, \exp\left\{-(\log X)^{1/3}(\log\log X)\right\}\right)$$

and

$$S_2{}' = \int_{\exp\{(\log X)^{2/3}\}}^{X} \Psi\left(\frac{X}{t}, t\right) \frac{dt}{\log t} + S_3{}',$$

where

$$S_3{}' = O\left(X \, \exp\left\{-c_8(\log X)^{1/3}\right\}\right).$$

Combining these estimates gives

$$\int_{\exp\{(\log X)^{2/3}\}}^{X} \Psi\left(\frac{X}{t}, t\right) \frac{dt}{\log t} = [X] + O(S_1{}' + S_3{}').$$

Thus, we obtain the desired asymptotic formula

$$\sum_{\substack{2\le n\le X\\ \left[\frac{K/\mathbb{Q}}{p_{\max}(n)}\right]=C}} 1 = \frac{\#C}{\#G}\cdot X + O\left(S_1+S_3+{S_1}'+{S_3}'\right)$$
$$= \frac{\#C}{\#G}\cdot X + O\left(X\exp\left\{-c_9(\log X)^{1/3}\right\}\right).$$

□

As a consequence of Theorem 4.2.1, we have the following lemma.

Lemma 4.2.5. *Assume the notation and hypotheses from Theorem 1.2.1. Then we have that*

$$\sum_{\substack{2\le n\le X\\ \left[\frac{K/\mathbb{Q}}{p_{\max}(n)}\right]=C}} \frac{1}{n} = \frac{\#C}{\#G}\cdot \log X + O\left(\exp\left\{-k(\log X)^{1/3}\right\}\right)$$

where k is a positive constant.

Proof of Lemma 4.2.5. Define the function f by

$$f(n) := \begin{cases} 1 & \text{if } \left[\frac{K/\mathbb{Q}}{p}\right]=C, \quad n=p>1,\\ 0 & \text{otherwise,}\end{cases} \tag{4.4}$$

and set

$$\psi_f(X) := \sum_{n\le X} f\big(p_{\max}(n)\big).$$

Then $\psi_f(X)$ counts the number of integers $n\le X$ such that $\left[\frac{K/\mathbb{Q}}{p_{\max}(n)}\right]=C$, so by Theorem 4.2.1 we have that

$$\psi_f(X) = \frac{\#C}{\#G}\cdot X + e_f(X),$$

where $e_f(X) = O\left(X\exp\left\{-k(\log X)^{1/3}\right\}\right)$. The function $\psi_f(X)$ is a type of stair-step function, meaning it oscillates as (the integral part of) X increases depending on the values of $p_{\max}(n)$ for $n \le X$. Then we can rewrite

$$\sum_{\substack{2\le n\le X \\ \left[\frac{K/\mathbb{Q}}{p_{\max}(n)}\right]=C}} \frac{1}{n} = \int_1^X \frac{d\psi_f(t)}{t},$$

which by Theorem 4.2.1 is

$$\begin{aligned} \int_1^X \frac{d\psi_f(t)}{t} &= \frac{\#C}{\#G}\int_1^X \frac{dt}{t} + \int_1^X \frac{de_f(t)}{t} \\ &= \frac{\#C}{\#G}\cdot \log X + \frac{e_f(t)}{t}\bigg|_1^X + \int_1^X \frac{e_f(t)\,dt}{t^2} \\ &= \frac{\#C}{\#G}\cdot \log X + c_1 - \int_X^\infty \frac{e_f(t)\,dt}{t^2} + \frac{e_f(X)}{X}, \end{aligned}$$

where

$$c_1 = \frac{-e_f(1)}{1} + \int_1^\infty \frac{e_f(t)\,dt}{t^2}.$$

Note that the number c_1 exists by Theorem 4.2.1, and that Lemma 4.2.5 now follows because

$$\frac{e_f(X)}{X} = O\left(\exp\left\{-k(\log X)^{1/3}\right\}\right),$$

where k is a positive constant. □

4.2.2 Densities of subsets of smallest prime divisors

We now prove Theorem 1.2.1 using all of the above tools. Again, the proof closely follows the proof of the analogous theorem in [2]. Note that c_{10}, c_{11}, and c_{12} are positive constants which will not be specified.

Proof of Theorem 1.2.1. Let f be defined as in (4.4). By Alladi's duality principle

(1.14), we have that

$$\begin{aligned}
\sum_{\substack{n\le X\\ \left[\frac{K/\mathbb{Q}}{p_{\min}(n)}\right]=C}} \frac{\mu(n)}{n} &= \sum_{n\le X} \frac{\mu(n)f(p_{\min}(n))}{n} \\
&= -\sum_{n\le X} \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) f(p_{\max}(d)) \\
&= -\sum_{n\le X} \sum_{d|n} \frac{\mu(n/d)}{n/d} \cdot \frac{f(p_{\max}(d))}{d}.
\end{aligned}$$

To more easily obtain estimates, we delicately split the double sum into two double sums by introducing the variable $m := n/d$. For each such m, the allowed values of d with $dm = n < X$ are exactly $1 \le d \le X/m$, so we have that

$$\begin{aligned}
&-\sum_{n\le X} \sum_{d|n} \frac{\mu(n/d)}{n/d} \cdot \frac{f(p_{\max}(d))}{d} \\
&\qquad = -\sum_{1\le m\le\sqrt{X}} \frac{\mu(m)}{m} \sum_{d\le X/m} \frac{f(p_{\max}(d))}{d} - \sum_{\sqrt{X}<m\le X} \frac{\mu(m)}{m} \sum_{d\le X/m} \frac{f(p_{\max}(d))}{d}.
\end{aligned}$$

Now we change the order of summation in the second sum. We use the fact that $m > \sqrt{X}$ and $md = n \le X$ implies $d < \sqrt{X}$ to obtain

$$\begin{aligned}
&-\sum_{n\le X} \sum_{d|n} \frac{\mu(n/d)}{n/d} \cdot \frac{f(p_{\max}(d))}{d} \\
&\qquad = -\sum_{1\le m\le\sqrt{X}} \frac{\mu(m)}{m} \sum_{d\le X/m} \frac{f(p_{\max}(d))}{d} - \sum_{d<\sqrt{X}} \frac{f(p_{\max}(d))}{d} \sum_{\sqrt{X}<m\le X/d} \frac{\mu(m)}{m}.
\end{aligned}$$

We estimate the two sums separately, reverting back to the variable n. Let

$$S_6 := -\sum_{n\le\sqrt{X}} \frac{\mu(n)}{n} \sum_{d\le X/n} \frac{f(p_{\max}(d))}{d} \quad \text{and} \quad S_7 := -\sum_{n<\sqrt{X}} \frac{f(p_{\max}(n))}{n} \sum_{\sqrt{X}<d\le X/n} \frac{\mu(d)}{d}.$$

We will show that S_6 gives the main term of the desired asymptotic formula, and we will bound S_7. By Lemma 4.2.5, we have that

$$\begin{aligned} S_6 &= -\sum_{n\le\sqrt{X}} \frac{\mu(n)}{n}\left[\frac{\#C}{\#G}\cdot\log\left(\frac{X}{n}\right)+O\left(\exp\left\{-k\left(\log\left(\frac{X}{n}\right)\right)^{1/3}\right\}\right)\right] \\ &= -\left(\frac{\#C}{\#G}\cdot\log X\right)\sum_{n\le\sqrt{X}}\frac{\mu(n)}{n}+\frac{\#C}{\#G}\sum_{1\le n\le\sqrt{X}}\frac{\mu(n)\,\log n}{n} \\ &\qquad + O\left(\exp\left\{-k(\log X)^{1/3}\right\}\right). \end{aligned}$$

We now apply well-known bounds for

$$\sum_{n\le\sqrt{X}}\frac{\mu(n)}{n} \quad \text{and} \quad \sum_{1\le n\le\sqrt{X}}\frac{\mu(n)\,\log n}{n}$$

which are consequences of the standard zero-free region for $\zeta(s)$ (for example, see [16, Chapter 13]). Namely, we have that

$$\sum_{n\le\sqrt{X}}\frac{\mu(n)}{n} = O\left(\exp\left\{-c_{10}(\log X)^{1/2}\right\}\right) \tag{4.5}$$

and

$$\sum_{1\le n\le\sqrt{X}}\frac{\mu(n)\,\log n}{n} = -1+O\left(\exp\left\{-c_{11}(\log X)^{1/2}\right\}\right).$$

Therefore, we have that

$$S_6 = -\frac{\#C}{\#G}+O\left(\exp\left\{-k(\log X)^{1/3}\right\}\right)$$

for some positive constant k. By equation (4.5), we also have that

$$S_7 \;=\; O\left(\sum_{n\le\sqrt{X}}\frac{1}{n}\exp\left\{-c_{10}\left(\log\left(\frac{X}{n}\right)\right)^{1/2}\right\}\right) = O\left(\exp\left\{-c_{12}(\log X)^{1/2}\right\}\right).$$

Now we see that

$$\sum_{\substack{2\leq n\leq X\\ \left[\frac{K/\mathbb{Q}}{p_{\min}(n)}\right]=C}} \frac{\mu(n)}{n} = -\frac{\#C}{\#G} + S_6 + S_7,$$

and therefore we have that

$$\sum_{\substack{2\leq n\leq X\\ \left[\frac{K/\mathbb{Q}}{p_{\min}(n)}\right]=C}} \frac{\mu(n)}{n} = -\frac{\#C}{\#G} + O\left(\exp\left\{-k(\log X)^{1/3}\right\}\right). \tag{4.6}$$

As $X \to \infty$, the error term $1/\exp\left\{k(\log X)^{1/3}\right\} \to 0$. This completes the proof. □

4.3 Generalization to arbitrary number field extensions

Since the Chebotarev Density Theorem applies to arbitrary number field extensions, it is natural to extend Theorem 1.2.1 to this more general setting. In order to state the generalization of Theorem 1.2.1 in [53], we must establish some notation. Let L/K be a finite Galois extension of number fields with Galois group $G := \mathrm{Gal}(L/K)$. One can define a Möbius-type function for ideals I of $\mathcal{O}_K$ by

$$\mu_K(I) := \begin{cases} 1 & \text{if } I = \mathcal{O}_K, \\ 0 & \text{if } I \subset \mathfrak{p}^2 \text{ for some prime ideal } \mathfrak{p} \subset \mathcal{O}_K, \\ (-1)^k & \text{if } I = \mathfrak{p}_1 \cdots \mathfrak{p}_k \text{ for distinct prime ideals } \mathfrak{p}_1, \ldots, \mathfrak{p}_k. \end{cases}$$

The function $\mu_K(I)$ satisfies a duality principle analogous to (1.14). An ideal $I \subset \mathcal{O}_K$ is called *salient* if it has a unique prime divisor of smallest norm, which is denoted $\mathfrak{p}_{\min}(I)$. For a conjugacy class $C \subset G$, we define the set $S(L/K;C)$ by

$$S(L/K;C) := \left\{ I \subset \mathcal{O}_K \text{ salient} : \mathfrak{p}_{\min}(I) \text{ is unramified, } \left[\frac{L/K}{\mathfrak{p}_{\min}(I)}\right] = C \right\}.$$

Then we have the following theorem [53].

Theorem 4.3.1 (Sweeting–Woo)**.** *Let L/K be a finite Galois extension of number fields with Galois group $G := \mathrm{Gal}(L/K)$. If C is a conjugacy class of G, then we have that*

$$-\lim_{X\to\infty} \sum_{\substack{2\le \mathrm{Nm}(I)\le X\\ I\in S(L/K;C)}} \frac{\mu_K(I)}{\mathrm{Nm(I)}} = \frac{\#C}{\#G}.$$

Chapter 5

Moonshine

The beautiful theory of moonshine guarantees a deep connection between the representation theory of finite groups and the Fourier coefficients of modular functions. The recent generalization of moonshine to all finite groups by Dehority, Gonzalez, Vafa, and Van Peski [22] raises the natural question of whether moonshine can be refined to distinguish non-isomorphic groups. Since character tables do not uniquely determine groups, one solution to this problem is to use the classical higher dimensional Frobenius r-characters in the construction of the moonshine module. It is known from the 1990s [34, 35, 37] that 1, 2, and 3-characters uniquely determine groups up to isomorphism. Therefore, a refinement of moonshine which takes into account 1, 2, and 3-character tables would suffice to distinguish groups. Here we prove a more general refinement, which is the content of Theorem 1.3.1. In addition, we prove Theorem 1.3.4 on new orthogonality relations for r-characters. These relations are required to prove Theorem 1.3.3, which guarantees the compatibility of the higher width graded trace functions with the multiplicity generating functions of the original moonshine module.

5.1 Classical representation theory

Let G be a finite group, and let $\rho_1, \ldots, \rho_t$ be the irreducible representations of G. In particular, each ρ_i is a group homomorphism $\rho_i : G \to \mathrm{GL}(V)$ for some $\mathbb{C}$-vector space V. Let $\chi_1, \ldots, \chi_t$ be the irreducible characters of G, which are the class functions $\chi_i : G \to \mathbb{C}$ defined by $\chi_i(g) := \mathrm{Tr}\left(\rho_i(g)\right)$ for all $g \in G$. Classical work of Schur (for example, see [15]) asserts that if χ is nontrivial, then

$$\sum_{g \in G} \chi(g) = 0, \tag{5.1}$$

and offers the following orthogonality relations:

$$\sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = |G|\delta_{ij}, \tag{5.2}$$

where δ_{ij} is the usual Kronecker delta function.

We require the following auxiliary orthogonality relations to prove Theorem 1.3.4.

Lemma 5.1.1. *Let χ_i be an irreducible character of G, and fix elements $h_1, h_2 \in G$. Then the following are true.*

1. *We have that*
$$\sum_{g \in G} \chi_i\left(g h_1 g^{-1} h_2^{-1}\right) = \frac{\chi_i\left(h_1\right)\overline{\chi_i\left(h_2\right)}|G|}{\dim \chi_i}.$$

2. *If χ_j is an irreducible character of G, then we have that*
$$\sum_{g \in G} \chi_i\left(h_1 g\right)\overline{\chi_j\left(g h_2\right)} = \frac{\chi_i\left(h_1 h_2^{-1}\right)|G|\delta_{ij}}{\dim \chi_i}.$$

Lemma 5.1.1 (1) was proved by Feit [29, (5.5)]. We now recall a classical result of Schur which will aid in the proof of Lemma 5.1.1 (2). For each $1 \leq i \leq t$, let m_i be the dimension of the representation ρ_i. Namely, for each $1 \leq i \leq t$ and each $g \in G$, the matrix corresponding to ρ_i is

$$\rho_i(g) =: \left[a_{jk}^{(i)}(g)\right]_{1\le j,k\le m_i}.$$

In particular, the image of the character χ_i for all $g \in G$ is the trace

$$\chi_i(g) = \sum_{1\le j\le m_i} a_{jj}^{(i)}(g).$$

The following famous result of Schur (see, for example, Chapter 5 of [15]) gives an important relationship between two representations which ultimately leads to all of the orthogonality relations between two characters.

Lemma 5.1.2 (Schur's Lemma)**.** *Let G be a finite group, and let V and W be vector spaces over $\mathbb{C}$ with corresponding irreducible representations ρ_V and ρ_W of G. If $f : V \to W$ is a G-linear map, then f is a scalar multiple of the identity map if $V \cong W$ and $f = 0$ if $V \ncong W$.*

Returning to the proof of Lemma 5.1.1 (2), we let χ_i and χ_j be irreducible characters of G, and we let C be an arbitrary $m_i \times m_j$ matrix. We define the matrix

$$B_C := \sum_{g\in G} \rho_i(g) C \rho_j\left(g^{-1}\right). \tag{5.3}$$

Since ρ_i and ρ_j are homomorphisms, it follows easily from (5.3) that for all $h \in G$, we have $\rho_i(h)B_C = B_C\rho_j(h)$. Therefore, by Schur's Lemma we have that

$$B_C = \begin{cases} 0, & \text{if } i \neq j, \\ b_i(C)\cdot I & \text{if } i = j, \end{cases}.$$

where $b_i(C) \in \mathbb{C}$, and I is the identity matrix of rank $\dim\chi_i$.

Proof of Lemma 5.1.1 (2). To prove the claim, we shall make repeated use of (5.3).

Given a matrix $C := [c_{st}]$, we observe that the (w,z) entry of (5.3) is

$$\sum_{g\in G}\sum_{1\le s\le m_i}\sum_{1\le t\le m_j} a^{(i)}_{ws}(g)c_{st}a^{(j)}_{tz}\left(g^{-1}\right) = b_i(C)\delta_{ij}\delta_{wz}.$$

Since B_C is diagonal, if $x \le m_i$, $y \le m_j$ and $C = C_{x,y}$ is chosen so that $c_{st} := \delta_{sx}\delta_{ty}$, then we have that

$$\sum_{g\in G} a^{(i)}_{wx}(g)a^{(j)}_{yz}\left(g^{-1}\right) = b_i\left(C_{x,y}\right)\delta_{ij}\delta_{wz}. \tag{5.4}$$

Obviously, if $i \ne j$, then this expression vanishes. We consider the case where $i = j$, and this becomes

$$\sum_{g\in G} a^{(i)}_{wx}(g)a^{(i)}_{yz}\left(g^{-1}\right) = b_i\left(C_{x,y}\right)\delta_{wz}.$$

The constant $b_i\left(C_{x,y}\right)$ seems to depend on the choice of x and y. However, notice that by replacing g by h^{-1}, this gives

$$\sum_{h\in G} a^{(i)}_{yz}(h)a^{(i)}_{wx}\left(h^{-1}\right) = b_i\left(C_{x,y}\right)\delta_{wz} = b_i\left(C_{w,z}\right)\delta_{xy},$$

which holds for all x, y, w, and z. Therefore, it follows that $b_i(C)$ is a constant which depends only on χ_i.

We now return to the general case where i might not equal j. Since ρ_i is a homomorphism, it is clear that

$$a^{(i)}_{sx}\left(h_1 g\right) = \sum_{1\le w\le m_i} a^{(i)}_{sw}\left(h_1\right)a^{(i)}_{wx}(g). \tag{5.5}$$

We multiply (5.4) by $a^{(i)}_{sw}\left(h_1\right)$ and sum on w to obtain

$$\sum_{g\in G} a^{(j)}_{yz}\left(g^{-1}\right)\sum_{1\le w\le m_i} a^{(i)}_{sw}\left(h_1\right)a^{(i)}_{wx}(g) = b_i(C)\delta_{ij}\delta_{xy}\sum_{1\le w\le m_i}\delta_{wz}a^{(i)}_{sw}\left(h_1\right),$$

which by (5.5) gives

$$\sum_{g\in G} a_{sx}^{(i)}(h_1 g)\, a_{yz}^{(j)}\left(g^{-1}\right) = a_{sz}^{(i)}(h_1)\, b_i(C)\delta_{ij}\delta_{xy}. \tag{5.6}$$

Similarly, we observe that

$$a_{tz}^{(j)}\left(h_2^{-1}g^{-1}\right) = \sum_{1\leq y\leq m_j} a_{ty}^{(j)}\left(h_2^{-1}\right) a_{yz}^{(j)}\left(g^{-1}\right),$$

so we multiply (5.6) by $a_{ty}^{(j)}\left(h_2^{-1}\right)$ and sum on y to obtain

$$\sum_{g\in G} a_{sx}^{(i)}(h_1 g)\, a_{tz}^{(j)}\left(h_2^{-1}g^{-1}\right) = a_{sz}^{(i)}(h_1)\, a_{tx}^{(j)}\left(h_2^{-1}\right) b_i(C)\delta_{ij}.$$

Now we choose $x = s$ and $z = t$ so that we have

$$\sum_{g\in G} a_{ss}^{(i)}(h_1 g)\, a_{tt}^{(j)}\left(h_2^{-1}g^{-1}\right) = a_{st}^{(i)}(h_1)\, a_{ts}^{(j)}\left(h_2^{-1}\right) b_i(C)\delta_{ij}.$$

It is apparent that this becomes a statement about the group characters if we sum on both s and t to obtain

$$\sum_{\substack{1\leq s\leq m_i\\ 1\leq t\leq m_j}} \sum_{g\in G} a_{ss}^{(i)}(h_1 g)\, a_{tt}^{(j)}\left(h_2^{-1}g^{-1}\right) = \sum_{g\in G}\left[\sum_{1\leq s\leq m_i} a_{ss}^{(i)}(h_1 g)\right]\left[\sum_{1\leq t\leq m_j} a_{tt}^{(j)}\left(h_2^{-1}g^{-1}\right)\right]$$

on the left hand side and

$$\begin{aligned}\sum_{\substack{1\leq s\leq m_i\\ 1\leq t\leq m_j}} a_{st}^{(i)}(h_1)\, a_{ts}^{(j)}\left(h_2^{-1}\right) b_i(C)\delta_{ij} &= b_i(C)\delta_{ij}\sum_{1\leq s\leq m_i}\left[\sum_{1\leq t\leq m_j} a_{st}^{(i)}(h_1)\, a_{ts}^{(j)}\left(h_2^{-1}\right)\right]\\ &= b_i(C)\delta_{ij}\sum_{1\leq s\leq m_i} a_{ss}^{(i)}\left(h_1 h_2^{-1}\right)\end{aligned}$$

on the right. By definition, since $\chi(g)^{-1} = \overline{\chi(g)}$, we obtain

$$\sum_{g\in G} \chi_i\left(h_1 g\right) \overline{\chi_j\left(g h_2\right)} = \chi_i\left(h_1 h_2^{-1}\right) b_i(C)\delta_{ij}. \tag{5.7}$$

Finally, we determine the value of $b_i(C)$. If $i \neq j$, then $b_i(C) = 0$ by Schur's Lemma. If $i = j$, then we set $h_1 = h_2 = 1$ in (5.7) and apply (5.2) to obtain

$$|G| = \sum_{g\in G} \chi_i(g)\overline{\chi_i(g)} = b_i(C)m_i.$$

Therefore $b_i(C) = |G|/\dim\chi_i$, and this completes the proof. □

5.2 Orthogonality of r-characters

It is a natural problem to determine the complete orthogonality relations of the Frobenius r-characters for $r > 1$. Frobenius, Hoehnke, and Johnson [30, 34, 35, 37] obtained some parts of this theory. In particular, they proved the vanishing relation analogous to (5.2) for distinct r-characters $\chi_i^{(r)} \neq \chi_j^{(r)}$. Here we obtain the remaining relations in the case where $\chi_i^{(r)} = \chi_j^{(r)}$, which provide what one can think of as the norms of the Frobenius r-characters. These results are of independent interest in character theory.

If $r \geq 2$, then (1.15) offers a recursive formula for r-characters. For $r = 2$ and 3, if χ is an irreducible character, then we find that

$$\begin{aligned}
\chi^{(2)}\left(g_1, g_2\right) &= \chi\left(g_1\right)\chi\left(g_2\right) - \chi\left(g_1 g_2\right), \\
\chi^{(3)}\left(g_1, g_2, g_3\right) &= \chi\left(g_1\right)\chi\left(g_2\right)\chi\left(g_3\right) - \chi\left(g_1\right)\chi\left(g_2 g_3\right) - \chi\left(g_3\right)\chi\left(g_1 g_2\right) \\
&\quad - \chi\left(g_2\right)\chi\left(g_1 g_3\right) + \chi\left(g_1 g_2 g_3\right) + \chi\left(g_2 g_1 g_3\right).
\end{aligned}$$

For dimension $r \geq 2$, these characters can be trivial (see [35, p. 244]).

Lemma 5.2.1. *Let G be a finite group. If χ is an irreducible character of G and $r > \dim\chi$, then $\chi^{(r)}\left(\underline{g}\right) = 0$ for all $\underline{g} \in G^{(r)}$.*

Generalizing (5.1), we obtain the following lemma.

Lemma 5.2.2. *Let G be a finite group. If χ is a nontrivial irreducible character of G, then for any integer $r \geq 1$, we have that*

$$\sum_{\underline{g} \in G^{(r)}} \chi^{(r)}\left(\underline{g}\right) = 0.$$

Proof of Lemma 5.2.2. We prove Lemma 5.2.2 by induction. When $r = 1$, the result is simply (5.1). Now, assume for $r \geq 1$ that

$$\sum_{g_1,\ldots,g_r \in G} \chi_i^{(r)}\left(g_1,\ldots,g_r\right) = 0.$$

Since $G^{(r+1)} = G \times G^{(r)}$, (1.15) implies that

$$\sum_{(g_1,\ldots,g_{r+1}) \in G^{(r+1)}} \chi_i^{(r+1)}\left(g_1,\ldots,g_{r+1}\right) = \sum_{g_1 \in G} \chi_i\left(g_1\right) \sum_{(g_2,\ldots,g_{r+1}) \in G^{(r)}} \chi_i^{(r)}\left(g_2,\ldots,g_{r+1}\right)$$
$$- \sum_{g_1 \in G} \left[\sum_{(g_2,\ldots,g_{r+1}) \in G^{(r)}} \chi_i^{(r)}\left(g_1 g_2, g_3, \ldots, g_{r+1}\right) - \sum_{(g_2,\ldots,g_{r+1}) \in G^{(r)}} \chi_i^{(r)}\left(g_2, g_1 g_3, \ldots, g_{r+1}\right) \right.$$
$$\left. - \cdots - \sum_{(g_2,\ldots,g_{r+1}) \in G^{(r)}} \chi_i^{(r)}\left(g_2, g_3, \ldots, g_1 g_{r+1}\right) \right].$$

The bracketed expression inside the sum over g_1 is the sequential shift of the location of g_1 through the elements $g_2, \ldots, g_{r+1}$. The result then follows from the induction hypothesis and the observation that $g_1 g_j$ varies over G as g_j varies over G. □

We now prove the general orthogonality relations in Theorem 1.3.4.

Proof of Theorem 1.3.4. If $i \neq j$, then it follows from [37, Theorem 2.1] that the sum is zero. Also, if G is abelian, then G has only one-dimensional characters, so the sum is zero for all $r > 1$ by Lemma 5.2.1.

For the remainder of the proof, we assume that G is non-abelian and that $i = j$. We prove Theorem 1.3.4 by writing the r-character $\chi^{(r)}$ in terms of the action of the symmetric group S_r on products of χ-values. For $\sigma \in S_r$, let $n(\sigma)$ be the number of disjoint cycles in σ, including 1-cycles, and denote

$$\sigma = \left(a_1^\sigma(1), \dots, a_1^\sigma\left(k_1^\sigma\right)\right)\left(a_2^\sigma(1), \dots, a_2^\sigma\left(k_2^\sigma\right)\right) \cdots \left(a_{n(\sigma)}^\sigma(1), \dots, a_{n(\sigma)}^\sigma\left(k_{n(\sigma)}^\sigma\right)\right). \tag{5.8}$$

The cycles have order $k_1^\sigma, k_2^\sigma, \dots, k_{n(\sigma)}^\sigma$, and as sets we have that

$$\{1, 2, \dots, r\} = \left\{a_1^\sigma(1), \dots, a_1^\sigma\left(k_1^\sigma\right), a_2^\sigma(1), \dots, a_2^\sigma\left(k_2^\sigma\right), \dots, a_{n(\sigma)}^\sigma(1), \dots, a_{n(\sigma)}^\sigma\left(k_{n(\sigma)}^\sigma\right)\right\}.$$

With this notation, it is easy to see that (1.15) can be iterated to obtain the following formulas for values of r-characters as products of χ-values. We abuse notation and write a for g_a in the formula below.

$$\chi^{(r)}\left(g_1, \dots, g_r\right) = \sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) \chi\left(a_1^\sigma(1) \cdots a_1^\sigma\left(k_1^\sigma\right)\right) \cdots \chi\left(a_{n(\sigma)}^\sigma(1) \cdots a_{n(\sigma)}^\sigma\left(k_{n(\sigma)}^\sigma\right)\right).$$

Using the notation in (5.8), the sum in Theorem 1.3.4 can now be rewritten as

$$\begin{aligned}
\Omega := \sum_{\underline{g} \in G^{(r)}} \chi^{(r)}\left(\underline{g}\right) \overline{\chi^{(r)}\left(\underline{g}\right)} &= \sum_{\underline{g}=(g_1,\dots,g_r) \in G^{(r)}} \chi^{(r)}\left(g_1, \dots, g_r\right) \overline{\chi^{(r)}\left(g_1, \dots, g_r\right)} \\
= \sum_{\sigma, \tau \in S_r} \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) &\sum_{\underline{g} \in G^{(r)}} \chi\left(a_1^\sigma(1) \cdots a_1^\sigma\left(k_1^\sigma\right)\right) \cdots \chi\left(a_{n(\sigma)}^\sigma(1) \cdots a_{n(\sigma)}^\sigma\left(k_{n(\sigma)}^\sigma\right)\right) \\
&\times \overline{\chi\left(a_1^\tau(1) \cdots a_1^\tau\left(k_1^\tau\right)\right)} \cdots \overline{\chi\left(a_{n(\tau)}^\tau(1) \cdots a_{n(\tau)}^\tau\left(k_{n(\tau)}^\tau\right)\right)}.
\end{aligned}$$

Next, we observe that without loss of generality we may order the cycles so that g_r appears in the last cycles $\left(a_{n(\sigma)}^\sigma(1), \dots, a_{n(\sigma)}^\sigma\left(k_{n(\sigma)}^\sigma\right)\right)$ and $\left(a_{n(\tau)}^\tau(1), \dots, a_{n(\tau)}^\tau\left(k_{n(\tau)}^\tau\right)\right)$.

It follows that

$$\Omega = \sum_{\sigma,\tau\in S_r} \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$$
$$\times \sum_{g_1,\ldots,g_{r-1}\in G} \left[\chi\left(a_1^{\sigma}(1)\cdots a_1^{\sigma}\left(k_1^{\sigma}\right)\right)\cdots\chi\left(a_{n(\sigma)-1}^{\sigma}(1)\cdots a_{n(\sigma)-1}^{\sigma}\left(k_{n(\sigma)-1}^{\sigma}\right)\right)\right.$$
$$\left.\times\,\overline{\chi\left(a_1^{\tau}(1)\cdots a_1^{\tau}\left(k_1^{\tau}\right)\right)}\cdots\overline{\chi\left(a_{n(\tau)-1}^{\tau}(1)\cdots a_{n(\tau)-1}^{\tau}\left(k_{n(\tau)-1}^{\tau}\right)\right)}\right]$$
$$\times \sum_{g_r\in G}\chi\left(a_{n(\sigma)}^{\sigma}(1)\cdots a_{n(\sigma)}^{\sigma}\left(k_{n(\sigma)}^{\sigma}\right)\right)\overline{\chi\left(a_{n(\tau)}^{\tau}(1)\cdots a_{n(\tau)}^{\tau}\left(k_{n(\tau)}^{\tau}\right)\right)}.$$

This last inner sum on g_r can be evaluated by either (5.2) or Lemma 5.1.1 (2). If g_r is the only element of G which appears in the sum over g_r, then we apply (5.2) to eliminate g_r from the sum and to get a factor of $|G|$. If not, then we assume without loss of generality that the sum over g_r is of the form $\sum_{g_r}\chi\left(A(\sigma)\cdot g_r\right)\overline{\chi\left(g_r\cdot A(\tau)\right)}$. We use $A(\sigma), A(\tau)$ to denote the products of the remaining elements of G in this particular sum, which of course depend on σ and τ (respectively). Lemma 5.1.1 (2) then eliminates g_r from the sum and results in $\chi\left(A(\sigma)\cdot A(\tau)^{-1}\right)$ multiplied by $|G|/\dim\chi$. This leaves a sum on $g_1,\ldots,g_{r-1}$, where each of these elements appears in exactly one χ and exactly one $\overline{\chi}$, before possible cancellations. If applying Lemma 5.1.1 results in the cancellation of a group element (for example, if the rightmost element of $A(\sigma)$ is the inverse of the leftmost element of $A(\tau)^{-1}$), then the sum over that group element is simply the sum of 1 over all elements in the group, so it contributes $|G|$. Repeating this process by applying the appropriate 1-character orthogonality relation for each of the remaining inner sums, we find that if we write the product $\sigma\tau^{-1} = x_1x_2x_3\cdots$ as a product of disjoint cycles, and if we define

$$m(\sigma,\tau) := \sum_{1\le j\le n(\sigma\tau^{-1})}\left[\operatorname{ord}_{S_r}\left(x_j\right)-1\right],$$

where $\text{ord}_{S_r}(x_j)$ denotes the length of the cycle x_j, then we have that

$$\Omega = \sum_{\sigma,\tau\in S_r} \text{sgn}(\sigma)\text{sgn}(\tau)\frac{|G|^r}{(\text{dim}\chi)^{m(\sigma,\tau)}}.$$

It remains to show that

$$\sum_{\sigma,\tau\in S_r} \text{sgn}(\sigma)\text{sgn}(\tau)\frac{|G|^r}{(\text{dim}\chi)^{m(\sigma,\tau)}} = \frac{r!|G|^r}{(\text{dim}\chi)^{r-1}}(\text{dim}\chi - 1)\cdots\big(\text{dim}\chi - (r-1)\big)$$

by a simple counting argument. If $1 \leq i \leq r$, then it is straightforward to see that the coefficient of $(\text{dim}\chi)^{r-i}$ on the right hand side is

$$(-1)^{i-1}\cdot\frac{r!|G|^r}{(\text{dim}\chi)^{r-1}}\cdot\frac{r(r-1)\cdots(r-(i-1))}{i}.$$

We will now show that the left hand sum gives the same coefficient. Clearly, if we fix an element $g \in S_r$, then $\{gh : h \in S_r\} = S_r$ as sets. Then the number of i-cycles in $\{\sigma\tau^{-1} : \sigma, \tau \in S_r\}$ equals the product of the number of i-cycles in S_r with the total number of elements in S_r. Since $\text{sgn}(\sigma)\text{sgn}(\tau)$ contributes $(-1)^{i-1}$ for each i-cycle appearing in $\sigma\tau^{-1}$, and since

$$\frac{1}{(\text{dim}\chi)^{i-1}} = \frac{1}{(\text{dim}\chi)^{r-1}}\cdot(\text{dim}\chi)^{r-i},$$

we see that the coefficient of $(\text{dim}\chi)^{r-i}$ on the left hand side is

$$(-1)^{i-1}\cdot\frac{r!|G|^r}{(\text{dim}\chi)^{r-1}}\cdot\frac{r(r-1)\cdots(r-(i-1))}{i}.$$

This completes the proof. $\square$

5.3 Higher width moonshine

We now prove Theorems 1.3.1 and 1.3.3. Theorem 1.3.1 guarantees that weak moonshine can be extended to width $s \geq 1$. Theorem 1.3.3 shows that the general orthogonality relations for Frobenius r-characters are compatible with width s weak moonshine. Namely, we show how to determine the multiplicity generating functions for the representation space for each nontrivial χ_i in the graded G-module V_G using the higher width McKay–Thompson series.

Proof of Theorem 1.3.1. By the Schur orthogonality relations for 1-characters, the multiplicity generating functions $\mathcal{M}_i(\tau) := \sum_{n \gg -\infty} m_i(n) q^n$ are given by

$$\mathcal{M}_i(\tau) = \sum_{n \gg -\infty} \frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \mathrm{Frob}_1(g; n) q^n = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} T(1, g; \tau). \tag{5.9}$$

It follows from [22] that width 1 weak moonshine exists for all finite groups, so that the G-module $V_G = \bigoplus_n V_G(n)$ exists, the graded trace functions $T(1, g; \tau)$ are modular functions for all $g \in G$, and the multiplicities $m_i(n)$ are positive integers for infinitely many $n \gg -\infty$ for each $1 \leq i \leq t$. We build the McKay–Thompson series for $V_G^{(r)}$ for $r > 1$ as follows. By the definitions of the generalized graded trace functions and the r-Frobenius of $\underline{g} \in G^{(r)}$ at $V_G^{(r)}(n)$, for each $1 \leq r \leq s$ we have that

$$\begin{aligned} T\left(r, \underline{g}; \tau\right) &= \sum_{n \gg -\infty} \mathrm{Frob}_r\left(\underline{g}; n\right) q^n \\ &= \sum_{n \gg -\infty} \sum_{1 \leq j \leq t} m_j(n) \chi_j^{(r)}\left(\underline{g}\right) q^n \\ &= \sum_{1 \leq j \leq t} \chi_j^{(r)}\left(\underline{g}\right) \mathcal{M}_j(\tau). \end{aligned}$$

Since all of the $\mathcal{M}_j(\tau)$ are modular functions by (5.9), we must have that the $T\left(r, \underline{g}; \tau\right)$ are modular functions as well for each $\underline{g} \in G^{(r)}$. □

Proof of Theorem 1.3.3. We now compute the multiplicity generating functions $\mathcal{M}_i(\tau)$ in terms of the McKay–Thompson series $T\left(r, \underline{g}; \tau\right)$ for each possible $r > 1$ using the r-character orthogonality relations. By Theorem 1.3.4, we have that

$$\begin{aligned}
\mathcal{M}_i(\tau) &= \sum_{n \gg -\infty} m_i(n) q^n \\
&= \sum_{n \gg -\infty} \frac{(\dim\chi_i)^{r-1}}{r!|G|^r (\dim\chi_i - 1) \cdots (\dim\chi_i - (r-1))} \sum_{\underline{g} \in G^{(r)}} \overline{\chi_i^{(r)}\left(\underline{g}\right)} \sum_{1 \le j \le t} m_j(n) \chi_j^{(r)}\left(\underline{g}\right) q^n \\
&= \sum_{n \gg -\infty} \frac{(\dim\chi_i)^{r-1}}{r!|G|^r (\dim\chi_i - 1) \cdots (\dim\chi_i - (r-1))} \sum_{\underline{g} \in G^{(r)}} \overline{\chi_i^{(r)}\left(\underline{g}\right)} \mathrm{Frob}_r\left(\underline{g}; n\right) q^n \\
&= \frac{(\dim\chi_i)^{r-1}}{r!|G|^r (\dim\chi_i - 1) \cdots (\dim\chi_i - (r-1))} \sum_{\underline{g} \in G^{(r)}} \overline{\chi_i^{(r)}\left(\underline{g}\right)} T\left(r, \underline{g}; \tau\right).
\end{aligned}$$

Therefore, the number of copies of the representation space for χ_i in all of the graded components $V_G^{(r)}(n)$ for all $1 \le r \le \dim\chi_i$ are given as the Fourier coefficients of the above linear combination of the modular McKay–Thompson series. □

5.4 An example of higher width moonshine

The common character table of D_4 and Q_8 is displayed below, with the following presentations of the groups in question:

$$D_4 = \left\{1, r, r^2, r^3, s, rs, r^2s, r^3s\right\} \quad \text{and} \quad Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

We abuse notation and let C_1, C_2, C_3, C_4, and C_5 denote the five conjugacy classes of both D_4 and Q_8, as indicated by the table below.

Table 5.1: Character Table of D_4 and Q_8

$\mathbf{D_4}$	$\{1\}$	$\{r^2\}$	$\{r, r^3\}$	$\{s, r^2 s\}$	$\{rs, r^3 s\}$
$\mathbf{Q_8}$	$\{1\}$	$\{-1\}$	$\{i, -i\}$	$\{j, -j\}$	$\{k, -k\}$
	C_1	C_2	C_3	C_4	C_5
χ_1	1	1	1	1	1
χ_2	1	1	−1	1	−1
χ_3	1	1	−1	−1	1
χ_4	1	1	1	−1	−1
χ_5	2	−2	0	0	0

The McKay–Thompson series for both D_4 and Q_8 are the Hauptmoduln f_1, f_2, and f_4 for $\Gamma_0(1)$, $\Gamma_0(2)$, and $\Gamma_0(4)$ (respectively) given by

$$
\begin{aligned}
f_1(\tau) &:= J(\tau) = q^{-1} + 196884q + 21493760q^2 + O\left(q^3\right), \\
f_2(\tau) &:= \left(\frac{\eta(\tau)}{\eta(2\tau)}\right)^{24} = q^{-1} + 276q - 2048q^2 + 11202q^3 - 49152q^4 + O\left(q^5\right), \\
f_4(\tau) &:= \left(\frac{\eta(\tau)}{\eta(4\tau)}\right)^{8} = q^{-1} + 20q - 62q^3 + 216q^5 - 641q^7 + 1636q^9 + O\left(q^{11}\right).
\end{aligned}
$$

The multiplicity generating functions for both D_4 and Q_8 are

$$
\begin{aligned}
\mathcal{M}_1(\tau) &= q^{-1} + 24788q + 2685440q^2 + 108044482q^3 + O\left(q^4\right), \\
\mathcal{M}_2(\tau) &= 26460q + 2686464q^2 + 108038912q^3 + O\left(q^4\right), \\
\mathcal{M}_3(\tau) &= 24640q + 2686464q^2 + 108038912q^3 + O\left(q^4\right), \\
\mathcal{M}_4(\tau) &= 24512q + 2687488q^2 + 108033280q^3 + O\left(q^4\right), \\
\mathcal{M}_5(\tau) &= 49152q + 5373952q^2 + 216072192q^3 + O\left(q^4\right).
\end{aligned}
$$

Therefore, D_4 and Q_8 have the same width 1 weak moonshine.

To illustrate Theorem 1.3.1, we extend to width 2 weak moonshine. All of the

2-character values of D_4 and Q_8 are identical except eight corresponding pairs:

$$\begin{aligned} \chi_5^{(2)}(s, r^2 s) &= 2, & \chi_5^{(2)}(j, -j) &= -2, \\ \chi_5^{(2)}(s, s) &= -2, & \chi_5^{(2)}(j, j) &= 2, \\ \chi_5^{(2)}(r^2 s, s) &= 2, & \chi_5^{(2)}(-j, j) &= -2, \\ \chi_5^{(2)}(r^2 s, r^2 s) &= -2, & \chi_5^{(2)}(-j, -j) &= 2, \\ \chi_5^{(2)}(rs, r^3 s) &= 2, & \chi_5^{(2)}(k, -k) &= -2, \\ \chi_5^{(2)}(rs, rs) &= -2, & \chi_5^{(2)}(k, -k) &= 2, \\ \chi_5^{(2)}(r^3 s, rs) &= 2, & \chi_5^{(2)}(k, -k) &= -2, \\ \chi_5^{(2)}(r^3 s, r^3 s) &= -2, & \chi_5^{(2)}(k, -k) &= 2. \end{aligned}$$

Consider, for example, the corresponding pairs of elements $(r^3 s, rs) \in D_4^{(2)}$ and $(-k, k) \in Q_8^{(2)}$. The McKay–Thompson series for $V_{D_4}^{(2)}$ is given by

$$T\left(2, \left(r^3 s, rs\right); \tau\right) = 98304q + 10747904q^2 + 432144384q^3 + O\left(q^4\right),$$

while the McKay–Thompson series for $V_{Q_8}^{(2)}$ is given by

$$T\left(2, (-k, k); \tau\right) = -98304q - 10747904q^2 - 432144384q^3 + O\left(q^4\right).$$

Therefore, width 2 weak moonshine distinguishes D_4 and Q_8.

The theory of *Brauer pairs*, i.e. non-isomorphic groups with isomorphic character tables including equivalent power maps, guarantees infinitely many examples of non-isomorphic groups whose width 1 and width 2 moonshines are equal. Therefore, the extension of weak moonshine to width 3 is required in order to uniquely determine all groups up to isomorphism.

Bibliography

[1] S. Ahlgren and N. Andersen. Algebraic and transcendental formulas for the smallest parts function. *Adv. Math.*, 289:411–437, 2016.

[2] K. Alladi. Duality between prime factors and an application to the prime number theorem for arithmetic progressions. *J. Number Theory*, 9(4):436–451, 1977.

[3] G. E. Andrews. The number of smallest parts in the partitions of n. *J. Reine Angew. Math.*, 624:133–142, 2008.

[4] R. Bacher and P. de la Harpe. Conjugacy growth series of some infinitely generated groups. *International Math. Res. Notices*, 2018(5):1532–1584, 2016.

[5] R. Borcherds. Monstrous Moonshine and Monstrous Lie Superalgebras. *Invent. Math.*, 109:405–444, 1992.

[6] K. Bringmann. On the explicit construction of higher deformations of partition statistics. *Duke Math J.*, 144:195–233, 2008.

[7] K. Bringmann, A. Folsom, K. Ono, and L. Rolen. *Harmonic Maass Forms and Mock Modular Forms: Theory and Applications*, volume 64. AMS Colloquium Publications, 2017.

[8] J. H. Bruinier and K. Ono. Algebraic formulas for the coefficients of half-integral weight harmonic weak Maass forms. *Adv. Math.*, 246:198–219, 2013.

[9] J. H. Bruinier, K. Ono, and A. V. Sutherland. Class polynomials for nonholomorphic modular functions. *J. Number Theory*, 161:204–229, 2016.

[10] W. Y. Chen, L. X. Wang, and G. Y. Xie. Finite differences of the logarithm of the partition function. *Math. Comp.*, 85:825–847, 2015.

[11] W. Y. C. Chen. The spt-function of Andrews, 2017.

[12] M. C. N. Cheng, J. F. R. Duncan, and J. A. Harvey. Umbral Moonshine and the Niemeier Lattices. *Res. Math. Sci.*, 1:3, 2014.

[13] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1996.

[14] J. H. Conway and S. P. Norton. Monstrous Moonshine. *Bull. London Math. Soc.*, 11:308–339, 1979.

[15] C. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras*. AMS Chelsea Publishing, Providence, RI, 1962.

[16] H. Davenport. *Multiplicative Number Theory*, volume 74 of *Graduate Texts in Mathematics*. Springer, New York, 1980.

[17] M. L. Dawsey. Conjugacy growth series for finitary wreath products. *Res. Number Theory*, 3(7), 2017.

[18] M. L. Dawsey. A new formula for Chebotarev densities. *Res. Number Theory*, 3(27):1–13, 2017.

[19] M. L. Dawsey and R. Masri. Effective bounds for the Andrews spt-function. *Forum Math. (accepted)*.

[20] M. L. Dawsey and K. Ono. Higher width moonshine. *Submitted.*

[21] N. J. de Bruijn. On the number of integers $\leq x$ free of prime factors $> y$. *Indag. Math.*, pages 50–60, 1951.

[22] S. Dehority, X. Gonzalez, N. Vafa, and R. Van Peski. Moonshine for all finite groups. *Res. Math. Sci.*, 5:14, 2018.

[23] S. Desalvo and I. Pak. Log-concavity of the partition function. *Ramanujan J.*, 38:61–73, 2015.

[24] M. Dewar and R. Murty. A derivation of the Hardy–Ramanujan formula from an arithmetic formula. *Proc. Amer. Math. Soc.*, 141:1903–1911, 2012.

[25] J. F. R. Duncan, M. Griffin, and K. Ono. Moonshine. *Res. Math. Sci.*, 2(11), 2015.

[26] J. F. R. Duncan, M. Griffin, and K. Ono. Proof of the Umbral Moonshine Conjecture. *Res. Math. Sci.*, 8(26), 2015.

[27] J. F. R. Duncan, M. H. Mertens, and K. Ono. Pariah Moonshine. *Nature, Ser. Communications*, 8(670), 2017.

[28] P. Erdös. On an elementary proof of some asymptotic formulas in the theory of partitions. *Ann. Math.*, 43:437–450, 1942.

[29] W. Feit. *Characters of Finite Groups.* W. A. Benjamin, Inc., New York, Amsterdam, 1967.

[30] G. Frobenius. Über die Primfaktoren der Gruppendeterminante. *S'ber. Akad. Wiss. Berlin*, pages 1343–1382, 1896.

[31] B. Gross, W. Kohnen, and D. Zagier. Heegner points and derivatives of L-series. ii. *Math. Ann.*, 278:497–562, 1987.

[32] G. H. Hardy and S. Ramanujan. Asymptotic Formulæ in Combinatory Analysis. *Proc. London Math. Soc.*, XVII(s2):75–115, 1918.

[33] A. Hildebrand. On the Number of Positive Integers $\leq x$ and Free of Prime Factors $> y$. *Journal of Number Theory*, 22:289–307, 1986.

[34] H. J. Hoehnke and K. W. Johnson. The 1-, 2-, and 3-characters determine a group. *Bulletin of the AMS*, 27(2), 1992.

[35] H. J. Hoehnke and K. W. Johnson. K-characters and group invariants. *Communications in Algebra*, 26(1):1–27, 1998.

[36] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[37] K. W. Johnson. On the group determinant. *Math. Proc. Camb. Phil. Soc.*, 109:299, 1991.

[38] J. C. Lagarias and A. M. Odlyzko. *Effective versions of the Chebotarev Density Theorem*. Algebraic Number Fields, L-Functions, and Galois Properties. Academic Press, New York, London, 1977.

[39] D. H. Lehmer. On the remainders and convergence of the series for the partition function. *Trans. Amer. Math. Soc.*, 46:362–373, 1939.

[40] M. Locus and I. Wagner. Congruences for powers of the partition function. *Annals of Combinatorics*, 21:83–93, 2017.

[41] H. Maier. On integers free of large prime divisors.

[42] N. Nekrasov and A. Okounkov. Seiberg–Witten theory and random partitions. *The Unity of Mathematics*, 244:525–596, 2003.

[43] J. L. Nicolas and G. Robin. Majorations explicites pour le nombre de diviseurs de n. *Canad. Math. Bull.*, 26:485–492, 1983.

[44] K. K. Norton. *Numbers with small prime factors, and the least k-th power non-residue*. Number 106 in Memoirs of the Amer. Math. Soc. Providence, RI, 1971.

[45] K. Ono. *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series.* AMS and CBMS, Providence, RI, 2004.

[46] H. Rademacher. A Convergent Series for the Partition Function $p(n)$. *Proc. Natl. Acad. Sci. U. S. A.*, 23(2):78–84, 1937.

[47] S. Ramanujan. On certain arithmetical functions. *Trans. Cambridge Philos. Soc.*, 22:159–184, 1916.

[48] S. Ramanujan. Congruence properties of partitions. *Proc. London Math. Soc.*, 18:xix, 1920.

[49] S. Ramanujan. Congruence properties of partitions. *Math. Z.*, 9:147–153, 1921.

[50] S. Ramanujan. *Collected papers.* Cambridge University Press, 1927.

[51] G. Robin. Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs de n. *Acta. Arith.*, 42:367–389, 1983.

[52] B. E. Sagan. Inductive and injective proofs of log concavity results. *Discret. Math.*, 68:281–292, 1988.

[53] N. Sweeting and K. Woo. Formulas for Chebotarev densities of Galois extensions of number fields. *Res. Number Theory*, 5(4), 2019.

[54] J. G. Thompson. Finite groups and modular functions. *Bull. London Math. Soc.*, 11(3):347–351, 1979.

[55] J. G. Thompson. Some numerology between the Fischer–Griess Monster and the elliptic modular function. *Bull. London Math. Soc.*, 11(3):352–353, 1979.

[56] N. Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.*, 95:191–228, 1926.

[57] I. Wagner. Conjugacy growth series for wreath product finitary symmetric groups. *Res. Number Theory*, 3(17), 2017.