Distribution Agreement

Signature:

Olivia Beckwith   Date

Harmonic Maass forms and modular forms:

Applications to class numbers and partitions

By

Olivia Beckwith

Doctor of Philosophy

Mathematics

Ken Ono

Advisor

John Duncan

Committee Member

David Zureick-Brown

Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.

Dean of the James T. Laney School of Graduate Studies

Date

Harmonic Maass forms and modular forms:

Applications to class numbers and partitions

By

Olivia Beckwith

B.S., Harvey Mudd College, 2013

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

2018

Abstract

This thesis is about analytic number theory. In particular, I prove theorems about class numbers, L-functions, and partitions, by using methods from the theory of modular forms and a generalization of modular forms called harmonic Maass forms.

Class numbers of quadratic number fields count classes of quadratic forms, and information about their arithmetic properties percolates into many areas of number theory. I quantified a recent theorem of Wiles, who proved the existence of imaginary quadratic fields with prescribed local conditions whose class numbers are indivisible by a given odd prime. I extended Wiles' result by proving a lower bound on the number of such fields with discriminant down to a given bound. I used this estimate to count rank 0 twists of certain elliptic curves.

Partition numbers are given by a simple combinatorial definition, but are connected to deep ideas in math. I proved Hardy-Ramanujan-type effective estimates for the number of k-regular partitions for low k. With Bessenrodt, I used these estimates to prove formulas for multiplicative partition functions arising in group theory.

I studied parts of partitions lying in given residue classes with respect to a fixed modulus. For large n, how many parts of a partition of n should one expect to be equivalent to $r \pmod m$? Mertens and I used the Circle Method, a technique for estimating the coefficients of modular forms that have a pole, to answer this question.

The theory of modular forms is the two-dimensional case of a larger body of work called the Langlands Program. A challenge in this area is studying the analytic properties of L-functions for automorphic forms; the Rankin-Selberg method allows one to do this in certain settings. Recent work to extend this technique has led to the development by Hoffstein and Hulse of shifted convolution L-series. Making use of mock modular properties of a class of these series, I proved bounds for special values of symmetrizations of the shifted convolution series.

Harmonic Maass forms and modular forms:

Applications to class numbers and partitions

By

Olivia Beckwith

B.S., Harvey Mudd College, 2013

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

2018

Acknowledgments

I am extremely grateful to my adviser Ken Ono for his fantastic guidance throughout my time at Emory.

I would like to thank the NSF and Emory University for supporting me financially. Emory has provided a wonderful environment for learning and for research, and I want to thank the professors there who have taught and mentored me.

I am grateful to my fellow graduate students who have provided me with invaluable friendship and emotional support throughout graduate school, especially Victor Manuel Aricheta, Lea Beneish, Adele Lopez, Robert Schneider, Sarah Trebat Leder, and Alex Viguerie.

I am also grateful to the mathematicians who have helped me with this thesis. Specifically, I wish to thank Michael Mertens for many helpful conversations about harmonic Maass forms, Michael Griffin for some helpful conversations about modular forms and for assistance with the partitions computations in Chapter 5, and Jesse Thorner for some helpful conversations about L-functions. I also thank John Duncan for his valuable comments on an earlier version of this thesis. The results proved in Chapter 5 were done with Christine Bessenrodt, and the results of Chapter 6 were proved with Michael Mertens.

Finally, I am forever indebted to Ken and Laura Beckwith, and Hudson Carpenter, for their relentless love and support that I depend on in all areas of my life, including math.

Contents

List of Tables

Chapter 1

Introduction

1.1 Class numbers, partitions, and L-functions

In this thesis, I present original results in the areas of class numbers, L-functions, and partitions. Each of these areas played a major role in the some of the most important developments in number theory of the twentieth century. Before I delve into the details of my work, let me give a brief overview of these three areas and their significance.

Class numbers were defined by Gauss to count classes of binary quadratic forms up to matrix equivalence. At first glance this may seem boring, but it turns out that class numbers are also the orders of groups which describe the obstruction to unique factorization for rings of integers of number fields, and consequences of deep knowledge about these groups percolate through virtually every important question in algebraic number theory.

Dirichlet found that although algebraic in their definition, class numbers are produced by special values of L-functions, giving class numbers an analytic interpretation. So, the theory of L-functions can be used to study class numbers. This idea also connects class numbers to the group structure of elliptic curves through the work of

Birch and Swinnerton-Dyer, who conjectured an important relationship between the analytic and algebraic approaches to studying elliptic curves. Moving forward, the Langlands philosophy connects the behavior of automorphic L-functions to the structure of number fields and important ideas in representation theory and arithmetic geometry.

Partition numbers were first studied by Euler and Ramanujan for their combinatorial properties. They seem like child's play: they simply count the nonincreasing sequences of positive integers with a fixed sum. This elementary idea has played a role in the representation theory of finite groups through the use of Young diagrams and in mathematical physics through the work of Okounkov. Partitions have also served as a testing ground throughout the development of the entire theory of modular forms. Hardy and Ramanujan developed the Circle Method to estimate the partition numbers, and this technique has been used throughout the study of modular forms and beyond it to classical problems in analytic number theory, including Waring's problem and the Odd Goldbach Conjecture. The Ramanujan Congruences were proved years before Atkin realized that they are the manifestations for the Dedekind eta-function of the action of the $U(p)$ operator on modular forms. This led to Atkin and Lehner's extension of this work to the theory of Hecke operators and the theory of newforms, which are necessary for understanding the structure of spaces of modular forms and for stating the most well-known formulation of the Modularity Theorem. The Ramanujan Congruences can also be viewed as consequences of properties of the Deligne-Serre Galois representations for modular forms, which played a central role in the proof of Fermat's Last Theorem.

I describe my results in Sections 2-5 of the present chapter, and present their proofs in Chapters 3 - 6. Chapter 2 introduces the primary objects used in these proofs: modular forms and harmonic Maass forms.

1.2 Class Numbers

Ideal class numbers of imaginary quadratic fields have been studied since Gauss, who conjectured that for any given h, there are only finitely many negative fundamental discriminants D such that $h(D) = h$. The history of Gauss' Conjecture is rich. The conjecture was shown to be true by work of Heilbronn [Hei34], who did not show how to find the imaginary quadratic fields with a given class number. Siegel [Sie35] proved that $h(-D)$ grows like $|D|^{1/2}$, but did so ineffectively. In other words, for each $\epsilon > 0$ he proved that for sufficiently large D that there are positive constants c_1 and c_2 for which

$$c_1 D^{1/2-\epsilon} < h(-D) < c_2 D^{1/2+\epsilon}$$

While explicit upper bounds for $h(-D)$ are known, the constants c_1 are ineffective for all ϵ. Baker [Bak66] and Heegner [Hee52]and Stark [Sta67] computed the complete finite list of negative fundamental discriminants D for which $h(D) = 1$. The works Gross and Zagier [GZ86] and Goldfeld [Gol85] produce a lower bound for $h(D)$ which is asymptotically smaller than Siegel's bound, but is effective and allows one (in principle) to compute the complete list of imaginary quadratic fields with any given class number.

It is natural to ask what else can be said about the structure of ideal class groups. For example, how often should we expect the ℓ-torsion subgroup of the class group to be trivial for a given odd prime ℓ? The *Cohen-Lenstra heuristics* [CL84] predict an answer:

$$\lim_{X\to\infty} \frac{\#\{-X < D < 0 : \ell \nmid h(D)\}}{X} = \prod_{n=1}^{\infty}\left(1 - \frac{1}{\ell^n}\right) = 1 - \frac{1}{\ell} - \frac{1}{\ell^2} + \frac{1}{\ell^5} \cdots \qquad (1.1)$$

Here the numbers D are fundamental discriminants. Note that the Cohen-Lenstra heuristics actually predict much more about the structure of the class groups, give similar predictions for real quadratic fields, and have been generalized by others to other number fields. For a concise description for the quadratic number field case, the reader is encouraged to read Chapter 5 Section 10 of [Coh93].

Numerical data provides some evidence for the Cohen-Lenstra heuristics, and for $\ell = 3$, strong theorems supporting equation (1.1) are known. Gauss' *genus theory* says that the number of order 2 elements of the class group is $2^{t-1} - 1$, where t is the number of distinct prime divisors of the discriminant (see Proposition 3.11 of [Cox97]). For $\ell = 3$, a theorem of Davenport and Heilbronn [DH71] says that if $\epsilon > 0$, then for X sufficiently large we have

$$\frac{\#\{-X < D < 0 : 3 \nmid h(D)\}}{\#\{-X < D < 0\}} \geq \frac{1}{2} - \epsilon.$$

They proved this by showing that the cubic number fields are in a discriminant preserving correspondence with a certain set of classes of binary cubic forms, and they used this fact to count the order 3 elements of class groups of quadratic number fields.

For $\ell > 3$ much less is known about the ℓ-torsion of class groups. Soundararajan [Sou00] used analytic techniques to count ℓ-torsion points of class groups, and showed

$$\#\{-X < D < 0 : \ell | h(D)\} \gg X^{\frac{1}{2}+\epsilon(\ell)},$$

where $\epsilon(\ell) > 0$ approaches 0 as $\ell \to \infty$. Kohnen and Ono [KO99] used the theory of modular forms to study the occurrence of class groups with trivial ℓ-torsion for $\ell > 3$. They proved for any $\epsilon > 0$, for sufficiently large X we have

$$\#\{-X < D < 0 : \ell \nmid h(D)\} \geq \left(\frac{2(\ell - 2)}{\sqrt{3}(\ell - 1)} - \epsilon \right) \frac{\sqrt{X}}{\log X}.$$

Information about the structure of class groups of quadratic fields can be used to study questions about Mordell-Weil groups of elliptic curves in families of quadratic twists, however, additional information about the splitting and ramification data of the quadratic number fields is often required for such applications. For $E : y^2 = p(x)$ an elliptic curve over $\mathbb{Q}$ with $p(x)$ in Weierstrass form, we define the twist of E by a fundamental discriminant D to be the elliptic curve defined by

$$E_D : y^2 D = p(x).$$

Note that E_D is isomorphic to E over $\mathbb{Q}(\sqrt{D})$, but not over $\mathbb{Q}$. The *Heegner hypotheses* are a set of conditions about how the rational primes of bad reduction of an elliptic curve split in an imaginary quadratic field. The work of Kolyvagin on the Birch and Swinnerton-Dyer Conjecture (see [Kol89a], [Kol89b]) is based on the existence of suitable quadratic twists of elliptic curves in which the twisting discriminant satisfy prescribed Heegner hypotheses. Combining his work with an important theorem of Gross and Zagier, who showed that the height of the Heegner point is a multiple of the derivative of the L-series of the elliptic curve at 1, it follows that the Birch and Swinnerton-Dyer Conjecture holds when the analytic rank is at most 1.

Heegner points have played an important role in studying Goldfeld's Conjecture, which concerns the ranks of the twists as D varies over the set of fundamental discriminants. Define $M_E^r(X) := \#\{D : |D| < X : \mathrm{ord}_{s=1} L(s, E_D) = r\}$. If $E/\mathbb{Q}$ is an elliptic curve and r is 0 or 1, then

$$M_E^r(X) \sim \frac{X}{2}, \quad X \to \infty.$$

The best general results on Goldfeld's Conjecture were, until recently, due to Perelli, Pomykala, and Skinner (see [OS98] and [PP97]). For the rank 0 case, Ono and Skinner [OS98] showed that

$$M_E^0(X) \gg \frac{X}{\log X}. \tag{1.2}$$

For the rank 1 case, Perelli and Pomykala [PP97] showed

$$M_E^1(X) \gg_\epsilon X^{1-\epsilon} \tag{1.3}$$

for any $\epsilon > 0$.

Recently, Kriz and Li [KL17] showed for a large class of elliptic curves,

$$M^r(X) \gg \frac{X}{\log^{\frac{5}{6}}(X)}.$$

Strong results on Goldfeld's conjecture have been obtained for special elliptic curves by making use of the aformentioned theorem of Davenport and Heilbronn on the 3-indivisibility of class numbers. Using the half-integral weight modular forms established by Waldspurger and a theorem of Frey [Fre88], James [Jam98] showed that the elliptic curve with Cremona label 14B satisfies $M_E^0(X) \gg X$.

Showing that an elliptic curve has a positive proportion of twists with rank one requires more than Waldspurger's modular forms. Vatsal [Vat98] used a theorem of Gross and Zagier [GZ86] to show that the elliptic curve $E = X_0(19)$ has $M_E^r(X) \gg X$ for $r = 0, 1$. Vatsal's argument was extended by Byeon [Bye12] to elliptic curves in the isogeny class of an elliptic curve with a nontrivial cuspidal 3-torsion point and square-free conductor.

The results toward Goldfeld's conjecture described above apply to certain elliptic curves with residually reducible mod 3 Galois representations, and rely on a refinement of the theorem of Davenport and Heilbronn due to Horie and Nakagawa [HN88]. Their refinement showed that a positive proportion of imaginary quadratic fields have trivial ℓ-torsion and satisfy prescribed local conditions. One might hope to extend the work of Horie and Nakagawa to a theorem on ℓ-indivisibility of class groups for $\ell > 3$ by refining the work of Kohnen and Ono [KO99] in an analogous way.

A barrier to refining Kohnen and Ono's theorem is showing that the modular forms arising in their argument have Fourier coefficients which are supported on prescribed arithmetic progressions and are nontrivial modulo ℓ. This is difficult because for many modular forms this property doesn't hold. For example, the values of the partition function $p(n)$ are the Fourier coefficients for the modular form $1/\eta(z)$, and the Ramanujan congruences tell us $p(5n+4) \equiv 0 \pmod{5}$, and so sieving the Fourier expansion of this form can return a modular form which is trivial modulo 5. Here $\eta(z) := q^{1/24} \prod_{n=1}^{\infty}(1-q^n)$ (throughout we use the notation $q := e^{2\pi i z}$) is Dedekind's eta-function, a weight 1/2 holomorphic modular form.

Recently, Wiles [Wil15] established the existence of imaginary quadratic fields with prescribed local data whose class numbers are indivisible by a given odd prime ℓ.

Theorem. *(Wiles) Let $\ell \geq 5$ be prime, and let S_0, S_+, S_- be finite disjoint sets of distinct odd primes not containing ℓ such that the following are true:*

1. *S_0 does not contain any primes which are $1 \pmod{\ell}$*
2. *S_+ does not contain any primes which are $-1 \pmod{\ell}$*
3. *S_- does not contain any primes which are $1 \pmod{\ell}$ and $-1 \pmod{4}$.*

Then there exists a negative fundamental discriminant D such that $\ell \nmid h(D)$, and $\mathbb{Q}(\sqrt{D})$ splits at every prime in S_+, is inert at every prime in S_-, and ramifies at every prime in S_0.

In view of the work of Horie and Nakagawa when $\ell = 3$ [HN88], I prove a quantified version of the theorem of Wiles for the $\ell > 3$ case by obtaining an estimate for the number of imaginary quadratic fields which satisfy the conclusion of Wiles' theorem, similar to the estimate of Kohnen and Ono.

Define the following:

$$M_\Sigma := \frac{1}{8}[\Gamma_0(1) : \Gamma_0(N_\Sigma)] \tag{1.4}$$

and

$$N_\Sigma := 4Q_\Sigma^6 \Big(\prod_{q \in S_0 \cup S_- \cup S_+} q^6 \Big), \tag{1.5}$$

where Q_Σ is equal to 1 if S_- is nonempty and otherwise is the smallest odd prime not contained in $S_+ \cup S_- \cup S_0$ which is not congruent to 1 modulo ℓ and -1 modulo 4.

In Chapter 3, I prove the following estimate for the smallest discriminant divisible by a given prime p lying in a certain arithmetic progression which satisfies the conclusion of Wiles' theorem.

Theorem 1.2.1. *Suppose $p > M_\Sigma$ is a prime such that the following are true:*

1. *We have that $\left(\frac{p}{\ell}\right) = 1$ and $p \not\equiv 1 \pmod{\ell}$,*

2. *We have that $p \equiv 1 \pmod 8$,*

3. *For odd primes $q \leq M_\Sigma$, $q \neq \ell$, we have $\left(\frac{p}{q}\right) = 1$.*

Then there is some $k_p \leq pM_\Sigma$ such that $p \nmid k_p$ and $\ell \nmid h(-k_p p)$ and $\mathbb{Q}(\sqrt{-k_p p})$ ramifies at all primes of S_0, splits at every prime in S_+, and is inert at every prime in S_-.

Combining this result with Dirichlet's Theorem on primes in arithmetic progressions, I obtained the following corollary, which can viewed as an extension of [KO99] to allow for local conditions. To state it, let $T_{\Sigma,\ell}$ denote the set of all fundamental discriminants which satisfy the conclusions of Theorem 1.2.1. That is, $T_{\Sigma,\ell}$ contains the set of negative fundamental discriminants D of quadratic fields K which ramify at all primes of S_0, split at every prime in S_+, and are inert at every prime in S_-, and have $\ell \nmid h(D)$. Also, let r_Σ be the number of odd primes less than M_Σ, excluding ℓ. Then we have the following:

Corollary 1.2.2. *Let ℓ be an odd prime. If $\epsilon > 0$, then for sufficiently large X we* *have*

$$\#\{-X < D < 0 : \ell \nmid h(D), D \in T_{\Sigma,\ell}\} \geq \left(\frac{\ell - 2}{(\ell-1)2^{r_\Sigma+4}\sqrt{M_\Sigma}} - \epsilon \right) \frac{\sqrt{X}}{\log X}.$$

One can apply Corollary 1.2.2 to count quadratic twists of certain elliptic curves which have Mordell-Weil rank 0 over $\mathbb{Q}$ and trivial ℓ-Selmer group. To state this result, it is convenient to define the following subsets of primes dividing the conductor N_E. Let $\tilde{S}_E$ be the subset of odd primes dividing the conductor N_E of E defined by

$$\widetilde{S}_E := \{p | N_E : p \equiv -1 \pmod{\ell}, \ell \nmid ord_p(\Delta_E)\}, \tag{1.6}$$

where Δ_E is the discriminant of E. Also, we set

$$T_+ = \{p | N_E, ord_p(j_E) < 0; E/\mathbb{Q}_p \text{ is not a Tate Curve}\}, \tag{1.7}$$

and

$$T_- = \{p | N_E : p \notin T_+, p \equiv 3 \pmod{4}\}. \tag{1.8}$$

A Tate curve $E/\mathbb{Q}_p$ is such that $E/\overline{\mathbb{Q}}_p \simeq \overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$ for some $q \in \mathbb{Q}_p$, for details see Appendix C of [Sil86].

Corollary 1.2.3. *Suppose $E/\mathbb{Q}$ is an elliptic curve with odd conductor N_E, and suppose E has a $\mathbb{Q}$-rational torsion point P of odd prime order ℓ, and suppose P is not contained in the kernel of reduction modulo ℓ. Assume $ord_\ell(j(E)) \geq 0$. Also assume $\widetilde{S}_E = \emptyset$ and neither T_+ nor T_- contain a prime which is $1 \pmod{\ell}$. Then we have*

$$\#\{-X < D < 0 : Sel_\ell(E_D) = \{1\}\} \gg \frac{\sqrt{X}}{\log X}.$$

1.3 Shifted Convolution L-functions

Let $f_1, f_2 \in S_k(\Gamma_0(N))$ be cusp forms with L-series given by

$$L(f_i, s) = \sum_{n=1}^{\infty} \frac{a_i(n)}{n^s}, \quad i = 1, 2.$$

Rankin and Selberg independently defined the *Rankin-Selberg convolution series* $L(f_1 \otimes f_2, s)$ as

$$L(f_1 \otimes f_2, s) := \sum_{n=1}^{\infty} \frac{a_1(n)\overline{a_2(n)}}{n^s}$$

for $\Re(s) > k$ and by analytic continuation elsewhere. Rankin-Selberg convolution series were first used to bound Fourier coefficients of cusp forms in the direction of the Ramanujan conjecture, and the idea has also been important in studying the Langlands program. Selberg [Sel65] later defined *shifted convolution L-functions*, which have been important in studying the Lindelöf hypothesis.

In [HH16] Hoffstein and Hulse defined *shifted convolution series* as follows:

$$D(f_1, f_2, h; s) := \sum_{n=1}^{\infty} \frac{a_1(n+h)\overline{a_2(n)}}{n^s}. \tag{1.9}$$

Hoffstein and Hulse established meromorphic continuation for this series and used it to prove strong estimates for certain shifted sums (see Theorem 1.3 of [HH16]). From these estimates a subconvexity bound for Dirichlet character twists of modular L-functions was obtained.

Shifted convolution sums such as the ones in [HH16] arise frequently in the theory of automorphic L-function and have been studied by many authors, who often use them to prove subconvexity bounds. Duke, Friedlander, and Iwaniec [DFI93] were the first to study bounds for shifted convolution sums of Hecke eigenvalues for holomorphic forms and their applications to subconvexity estimates. Harcos [Har03] extended their work to similar results for Maass forms. Works of Blomer, Harcos, and Michel [Blo04] [BHM07] extended the work of [Har03], proving a Burgess-type estimate in the latter paper. Note that Blomer [Blo04] showed, as a corollary of his main result, that if $\epsilon > 0$ is fixed, and $h \leq M^{\frac{64}{39}-\epsilon}$, there exists $\delta > 0$ such that

$$\sum_{m \leq M} a_1(m)\overline{a_1(m+h)} \ll_\epsilon M^{1-\delta}. \tag{1.10}$$

Remark 1.3.1. *The convergence of the sum considered in the present work (see equation 1.11) is implied by equation (1.10). Although Blomer only states his result for the case that $f_1 = f_2$, his argument can be extended to the case that $f_1 \neq f_2$.*

These results were extended using automorphic spectral decomposition by Blomer and Harcos in [BH08] and [BH10]. In [BH08], a sum very similar to the one studied in [HH16] and in the present work was considered. In [BH10], a Burgess-type estimate was obtained. Maga [Magar] [Mag13] generalized the bound and Burgess-type bound of [BH10] to automorphic GL_2 twisted L-functions over general number fields (note that Maga was not the first to obtain a Burgess-type estimate in this generality, but the first to do so using shifted convolution sums). For an overview of these results and their applications to quadratic forms, see [Har14].

We consider *symmetrized shifted convolution series* $\hat{D}(f_1, f_2, h; s)$ for $f_1, f_2 \in S_k(\Gamma_0(N))$, which were first defined by Mertens and Ono [MO16]. They are defined as follows:

$$\hat{D}(f_1, f_2, h; s) := D(f_1, f_2, h; s) - D(\overline{f_1}, \overline{f_2}, -h; s). \tag{1.11}$$

This symmetrized series has conditional convergence at $s = k - 1$.

In view of the works described above, it is natural to ask for bounds for the L-values in h-aspect. In Chapter 4, I use the theory of harmonic Maass forms to obtain a polynomial bound in h aspect for $\hat{D}(f_1, f_2, h, k-1)$ as $h \to \infty$.

Theorem 1.3.2. *Let $f_1, f_2 \in S_k(2(\mathbb{Z}))$. Then*

$$|\hat{D}(f_1, f_2, h, k-1)| \ll_{f_1,f_2} h^{\frac{k}{2}}, \quad h \to \infty.$$

Remark 1.3.3. *These methods would probably also work for forms of higher level, but for simplicity I only do the level 1 case here. By making use of the full strength of theorem of Mertens and Ono which involves the Rankin-Cohen bracket, these methods could probably be generalized to the case that the weight of f_1 is greater than the weight of f_2, rather than their weights being equal.*

1.4 Multiplicative Partition Functions

A partition of a natural number n is a finite weakly decreasing sequence of positive integers that sums to n. For $k \in \mathbb{N}$, $k > 1$, let $p_k(n)$ count the k-regular partitions of n, i.e., partitions of n for which no part is divisible by k. These generating functions arise in many different contexts, in particular in connection with the representation theory of the symmetric groups, Hecke algebras, and related groups and algebras; for a long time, this has been studied both in combinatorics and number theory.

For the classical (unrestricted) partition function $p(n)$, explicit formulae are known due to the work of Hardy, Ramanujan and Rademacher, and more recent work of Bruinier and Ono [BO13]. Based on a result due to Lehmer, the following inequality was shown in a recent article by the Bessendrodt and Ono [BO16]:

For any integers a, b such that $a, b > 1$ and $a + b > 9$, we have $p(a)p(b) > p(a + b)$.

Also the cases of equality were determined in [BO16]. The inequality above was then used to study an "extended partition function", given by defining for a partition $\mu = (\mu_1, \mu_2, \ldots)$:

$$p(\mu) = \prod_{j \geq 1} p(\mu_j).$$

With $P(n)$ denoting the set of all partitions of n, the maximum

$$\mathrm{maxp}(n) = \max(p(\mu) \mid \mu \in P(n))$$

was determined explicitly in [BO16]; see Chapter 5 for the complete statement.

In Chapter 5, I present the results of a joint project with Christine Bessenrodt, in which we obtain results analogous to the theorems [BO16] for $p_k(n)$. My contribution to this project was proving a result corresponding to the inequality above for an extension of the generating function $p_k(n)$ to a function on the set $P_k(n)$ of all k-regular partitions of n, defined for $\mu = (\mu_1, \mu_2, \ldots) \in P_k(n)$ by:

$$p_k(\mu) = \prod_{j \geq 1} p_k(\mu_j).$$

We then determine on which partitions the maximum

$$\mathrm{maxp}_k(n) = \max(p_k(\mu) \mid \mu \in P_k(n))$$

is attained, and we use this to give an explicit formula for the maximum.

By the work of Bessenrodt and Ono [BO16], for $k > 6$ nothing new happens, as all the partitions providing the maximal values $\mathrm{maxp}(n)$ are already k-regular; hence we may restrict our considerations to the cases where $2 \leq k \leq 6$. For this case, we first show in Theorem 1.4.1 that $p_k(n)$ satisfies a similar inequality as the one given for $p(n)$ above, where again we specify the corresponding bounds explicitly.

For the maximum problem, we found that the behavior is quite similar to the one observed in [BO16], though we lose uniqueness for small k; see Theorem 5.3.2 in Chapter 5 for the detailed results.

The key to understanding the maximal values is the following analytic inequality for the generating function $p_k(n)$. As mentioned above, Theorem 1.4.1 is the analogue of a result for the ordinary partition function $p(n)$ in recent work by Bessenrodt and Ono [BO16].

Theorem 1.4.1. *For $k \in \mathbb{N}$, $2 \leq k \leq 6$, we define parameters n_k, m_k by the following table:*

k	2	3	4	5	6
n_k	3	2	2	2	2
m_k	22	17	9	9	9

Then for any $a, b \in \mathbb{N}$ with $a, b \geq n_k$ and $a + b \geq m_k$ we have

$$p_k(a)p_k(b) > p_k(a+b).$$

Furthermore, all the pairs (a, b) with $2 \leq a \leq b$ for which this inequality fails are given in the table below.

k	(a,b) *with* $p_k(a)p_k(b) = p_k(a+b)$	(a,b) *with* $p_k(a)p_k(b) < p_k(a+b)$
2	$(3,3), (3,5), (3,6), (3,7), (3,8), (4,15), (4,16), (4,17), (5,6), (5,7), (5,8)$	$(2,*), (3,4), (4,4), (4,5), (4,6), (4,7), (4,8), (4,9), (4,10), (4,11), (4,12), (4,13), (4,14), (5,5)$
3	$(2,2), (2,3), (3,3), (3,4), (3,5), (3,6), (3,7), (3,8), (3,9), (3,10)$	$(3,11), (3,13)$
4	$(2,2), (2,3), (2,5), (3,3)$	$(2,4), (3,5)$
5	$(2,3), (2,4)$	$(2,2), (2,5), (3,3), (3,5)$
6	$(2,4), (2,5), (2,6)$	$(2,2), (2,3), (3,3)$

My main tool for deriving Theorem 1.4.1 was an analogue of a classical result of D. H. Lehmer [Leh38]. In particular, I derive precise approximations for $p_k(n)$ which have effectively bounded error, which we obtain using work of Hagis [Hag71]. I present these proofs in Chapter 5.

Remark 1.4.2. *Recently, Alanazi, Gagola, and Munagi [AGM17] gave a combinatorial proof of Theorem 1.4.1 and of the analogous partition inequality of [BO16].*

1.5 Parts of partitions in given residue classes

The Circle Method, certainly one of the most important techniques in analytic number theory, originates in the investigation of the partition function. Exploiting the modularity of the generating function of partition function, Hardy and Ramanujan [HR18] found their famous asymptotic formula for the number $p(n)$ of partitions of a natural number n,

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

Later, Rademacher [Rad37] was able to refine the method of Hardy-Ramanujan to obtain his exact formula

$$p(n) = \frac{2\pi}{(24n-1)^{\frac{3}{4}}} \sum_{k=1}^{\infty} \frac{A_k(n)}{k} I_{\frac{3}{2}}\left(\frac{\pi\sqrt{24n-1}}{6k}\right), \tag{1.12}$$

where $I_{\frac{3}{2}}$ is the modified Bessel function of the first kind and $A_k(n)$ is a certain Kloosterman sum (see Chapter 6).

In Chapter 6, I present results on the number of parts in all partitions in certain congruence classes. These results are joint with Michael Mertens. The first work addressing the related question of how many parts does a "generic" partition of an integer n contain, is the seminal work by Erdős and Lehner [EL41]. To be more precise, they showed that for large n, almost all partitions of n contain

$$(1+o(1))\frac{\sqrt{6n}}{2\pi}\log n$$

parts.

If $\lambda = (\lambda_0, \dots, \lambda_k)$ is a partition, i.e. a non-increasing sequence of positive integers, we let

$$T_{r,N}(\lambda) = |\{\lambda_j : \lambda_j \equiv r \pmod{N}\}|. \tag{1.13}$$

For a positive integer n we then define

$$\widehat{T}_{r,N}(n) = \sum_{|\lambda|=n} T_{r,N}(\lambda), \tag{1.14}$$

where the summation runs over all partitions of size n. The quantity $\widehat{T}_{r,N}(n)$ counts the number of parts congruent to $r \pmod{N}$ in all partitions of n. For example, all partitions of 5 are

$$(5),\ (4,1),\ (3,2),\ (3,1,1),\ (2,2,1),\ (2,1,1,1),\ (1,1,1,1,1),$$

hence $\widehat{T}_{1,3}(5) = 13$ and $\widehat{T}_{2,3}(5) = 5$. We will study differences between these functions for $N \geq 3$ and $\gcd(r, N) = 1$.

A formula giving a lower bound for the number of parts of a partition of n in a residue class $r \pmod{d}$ for a proportion of partitions was proved by Dartyge, Sarkozy, and Szalay [DSS05] for $d < n^{\frac{1}{2}-\epsilon}$. The same authors in [DSS06] proved a formula for the expected number of parts of a partition in a residue class when the parts must be distinct.

In [DS05a] Dartyge and Sarkozy proved an inequality that suggests that some residue classes occur as parts in a partition more frequently than others. They showed that for sufficiently large n and $1 \leq r < s \leq N$, a positive proportion of the partitions of n satisfy

$$T_{r,N}(\lambda) - T_{s,N}(\lambda) > \frac{(r+s)\sqrt{n}}{50rs}.$$

In Chapter 6, I use the Circle Method to prove an asymptotic formula for $\widehat{T}_{r,N}(n) - \widehat{T}_{N-r,N}(n)$ for $\gcd(r, N) = 1$. I prove the following:

Theorem 1.5.1. *Let r, N be coprime positive integers with $N \geq 3$ and $1 \leq r < \frac{N}{2}$. Then we have that*

$$\widehat{T}_{r,N}(n) - \widehat{T}_{N-r,N}(n) = \frac{1}{2\sqrt{2}\varphi(N)N}\left(\sum_{\psi(-1)=-1}\psi(r')\sum_{c=1}^{N-1}\psi(c)\cot\left(\frac{\pi c}{N}\right)\right)\frac{e^{\left(\pi\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)}}{\sqrt{\left(n-\frac{1}{24}\right)}}$$
$$-\frac{1}{4\sqrt{3}\varphi(N)}\sum_{\psi(-1)=-1}\psi(r')L(0,\psi)\frac{e^{\left(\pi\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)}}{n-\frac{1}{24}} + O\left(n^2 e^{\left(\frac{\pi}{2}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)}\right),$$

where ψ runs through all odd Dirichlet characters modulo N, $L(s,\psi)$ denotes the Dirichlet L-series associated to ψ, and r' denotes the multiplicative inverse of r modulo N.

Remark 1.5.2. *In the proof of 1.5.1, we also give further terms of an asymptotic expansion of $\widehat{T}_{r,N}(n) - \widehat{T}_{N-r,N}(n)$.*

Example 1.5.3. *Let $N = 3$ and $r = 1$. Then the formula in 1.5.1 simplifies to*

$$\widehat{T}_{1,3}(n) - \widehat{T}_{2,3}(n) \sim \frac{1}{6\sqrt{6}}\left(\frac{1}{\sqrt{n-\frac{1}{24}}} - \frac{1}{2\sqrt{2}\left(n-\frac{1}{24}\right)}\right)e^{\pi\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}}.$$

We denote by $Q(n)$ the quotient of the left-hand side of the above asymptotic equation by its right-hand side. Table 1.1 contains numerical values of $Q(n)$ for various n, illustrating that the above asymptotic is a relatively good approximation for large n.

n	10	100	1,000	10,000	100,000
$Q(n)$	1.00417	1.00142	1.00013	1.00001	1.00000

Table 1.1: Numerics for Theorem 1.5.1

As it turns out, the generating function of $\widehat{T}_{r,N}(n) - \widehat{T}_{N-r,N}(n)$ is a weakly holomorphic modular form of weight $\frac{1}{2}$ for $\Gamma_1(N)$ so that we can essentially follow Rademacher's proof for his exact formula for $p(n)$.

The generating function of $\widehat{T}_{r,N}(n)$ is not modular, but we use a variant of the circle method due to Wright to prove the following asymptotic formula for $\widehat{T}_{r,N}(n)$. This is possible due to the fact that $\widehat{T}_{r,N}(n)$ is monotonically increasing in n.

Theorem 1.5.4. *For fixed numbers $r, N \in \mathbb{N}$, $r \leq N$, we have the asymptotic*

$$\widehat{T}_{r,N}(n) = e^{\pi\sqrt{\frac{2n}{3}}} n^{-\frac{1}{2}} \frac{1}{4\pi N\sqrt{2}} \left[\log n - \log\left(\frac{\pi^2}{6}\right) - 2\left(\psi\left(\frac{r}{N}\right) + \log N\right) + O\left(n^{-\frac{1}{2}}\log n\right)\right],$$

where $\psi(z) = \frac{\Gamma'(z)}{\Gamma(z)}$ denotes Euler's digamma function, as $n \to \infty$.

Remark 1.5.5. *Since the digamma function $\psi(x)$ is monotonically increasing and negative for real arguments $x \leq 1$, we see at once that for $1 \leq r < s \leq N$ we have the inequality*

$$\widehat{T}_{r,N}(n) \geq \widehat{T}_{s,N}(n)$$

for all sufficiently large N.

Example 1.5.6. *Let $N = 3$. We want to illustrate the asymptotic formula from Theorem 1.5.4 for $\widehat{T}_{r,3}(n)$ for $r = 1, 2, 3$. Let $Q_r(n)$ denote the quotient of $\widehat{T}_{r,3}(n)$ by the respective main term. Table 1.2 gives the numerical values (decimal expansions are truncated, not rounded).*

n	10	100	1,000	10,000	100,000
$Q_1(n)$	0.982155	0.992241	0.997608	0.999273	0.999778
$Q_2(n)$	1.149645	1.017114	1.003063	1.000592	1.000115
$Q_3(n)$	1.792248	1.067095	1.011771	1.002470	1.000563

Table 1.2: Numerics for Theorem 1.5.4

Chapter 2

Background

This chapter introduces objects which are vital tools for the proofs presented in the subsequent chapters. First, we introduce classical modular forms and some of their important properties, and then we introduce harmonic Maass forms. As an example of a harmonic Maass form, in Section 2.3 we introduce a harmonic Maass form discovered by Zagier whose Fourier coefficients are Hurwitz class numbers. This form will be important in Chapter 3.

We present only a few of the important and interesting properties and examples of these functions. The reader is encouraged to see other sources for more complete treatments of these theories, including [Ono00] or [DS05b] for modular forms, and [BFOR17] or [BF04] for harmonic Maass forms.

2.1 Modular Forms

Famous for their important role in proving Fermat's Last Theorem in the 1990s, modular forms are connected to many areas of mathematics, including number theory, representation theory, combinatorics, and mathematical physics. A recent example of their relevance in mathematics is Viazovska's solution to the sphere packing problem in $\mathbb{R}^8$ [Via17] and its extension by several authors to the dimension 24 sphere packing problem [CKM+17].

Modular forms are holomorphic functions on the upper-half plane which transform nicely under discrete groups of isometries of the hyperbolic plane. Every modular form has a weight, and the set of modular forms of the same weight satisfying certain nice asymptotic properties form finite-dimensional vector spaces. Modular forms are periodic, and their Fourier coefficients are often full of arithmetic meaning. The following sections make these ideas precise. In Section 2.1.1, the important subgroups of $SL_2(\mathbb{R})$ are introduced. In Section 2.1.2, modular forms are defined and a few of their important properties are stated. In Section 2.1.3, a few well-known examples of modular forms are presented.

2.1.1 The Modular Group

Here, we introduce some important matrix groups and state some of their properties. The modular group and its finite-indexed subgroups arise naturally in the study of geometry of the Poincaré half plane model for the hyperbolic plane $\mathbb{H}$ as discrete subgroups of the group of isometries of $\mathbb{H}$. While this may seem far removed from number theory at first glance, these groups give rise to moduli spaces for complex elliptic curves and are foundational objects in the theory of modular forms.

Throughout the rest of this thesis, let $\mathbb{H} := \{x+iy \in \mathbb{C} : y > 0\}$ denote the upper half plane. The group $SL_2(\mathbb{R})$ of 2×2 determinant one matrices with real entries acts on $\mathbb{H}$ by Möbius transformation. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{R})$, we have the following action on $\mathbb{H}$:

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

These transformations act isometrically on $\mathbb{H}$ with with respect to the Poincaré metric, which is given by

$$(ds)^2 := y^{-2}\left((dx)^2 + (dy)^2\right).$$

With respect to this metric, $\mathbb{H}$ is a Riemannian manifold. Its geodesics are given by half circles centered on the real line and the vertical lines (Euclidean lines which are orthogonal to $\mathbb{R}$).

The *modular group* $SL_2(\mathbb{Z})$ is the subgroup of $SL_2(\mathbb{R})$ consisting of two by two determinant one matrices with integer entries. This group has many nice properties. The modular group (and any finite index subgroup of the modular group) acts on $\mathbb{H}$ in a nice way, in particular, it acts *discontinuously* in that for any $x \in \mathbb{H}$, the orbit of x under $SL_2(\mathbb{Z})$ has no limit points. Consequently, one can find a set of representatives for the orbits of $\mathbb{H}$ under the $SL_2(\mathbb{Z})$ action which is finite in volume and is actually polygonal (the edges are geodesics with respect to the hyperbolic metric, not the euclidean metric). One can use these facts and a few other properties to show that the quotient $SL_2(\mathbb{Z})\backslash\mathbb{H}$ when compactified is a genus zero Riemann surface. Its points parametrize the isomorphism classes of complex elliptic curves via $\tau \to \mathbb{C}/\{\mathbb{Z} + \tau\mathbb{Z}\}$.

The modular group has a family of important subgroups known as *congruence subgroups*, which also satisfy the interesting properties discussed in the last paragraph.

The *principal congruence subgroup of level* N, where $N \geq 1$, is given by

$$\Gamma(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\}.$$

More generally, a congruence subgroup of level N is a subgroup of $SL_2(\mathbb{Z})$ that contains $\Gamma(N)$. Here are two important families of level N congruence subgroups:

$$\Gamma_1(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\},$$

and

$$\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{N}\}.$$

The action of a congruence subgroup on $\mathbb{H}$ extends to an action on $\mathbb{Q} \cup \{i\infty\}$. The orbit classes of $\mathbb{Q} \cup \{i\infty\}$ under the action of a congruence subgroup Γ are called the *cusps* of Γ. For example, $SL_2(\mathbb{Z})$ has just a single cusp $i\infty$, because every reduced rational $-\frac{d}{c}$ is mapped to $i\infty$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

Similar to the modular group, the compactifications of the quotients $\Gamma\backslash\mathbb{H}$ are Riemann surfaces (although the genus is rarely zero). It turns out that these quotients are also algebraic curves whose points parametrize isomorphism classes of elliptic curves enhanced with torsion data.

Congruence subgroups and cusps are needed to define modular forms, which we'll do in the next section.

2.1.2 What is a modular form?

For each integer k and each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, we define the operator $|_k\gamma$ on smooth functions $f : \mathbb{H} \to \mathbb{C}$ by

$$(f|_k\gamma)(z) := (cz + d)^{-k} f(\gamma z).$$

Let k be an integer, and let Γ be a congruence subgroup.

Definition 2.1.1. *Let $f : \mathbb{H} \to \mathbb{C}$ be holomorphic. Then f is a* weight k modular form with respect to Γ *if the following are true:*

(i) f is weight k invariant under Γ, that is, for all $\gamma \in \Gamma$, $(f|_k\gamma) = f$.

(ii) $f(\tau)$ has at most polynomial growth in $Im(\tau)$ as $\tau \to i\infty$, and analogous conditions hold at the other cusps of Γ.

When k is an even integer, condition (i) basically says that we can interpret a modular form of weight k as an order $k/2$ differential form on $\mathbb{H}/SL_2(\mathbb{Z})$.

If Γ contains $\Gamma(N)$, then we say that a modular form with respect to Γ has level N. Since $\Gamma(N)$ always contains $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$, condition (i) ensures that all modular forms are periodic. The second condition then ensures that f has a Fourier expansion of the form $\sum_{n=0}^{\infty} a_n q^{n/N}$, and $(f|_k\gamma)$ for $\gamma \in SL_2(\mathbb{Z})$ have similar expansions, where through $q := e^{2\pi i z}$.

A modular form that vanishes at every cusp of Γ is called a *cusp form.* Cusp forms are an important family of examples of these functions.

We let $M_k(\Gamma)$ (resp. $S_k(\Gamma)$) denote the complex vector space of modular (resp. cusp) forms of weight k with respect to Γ. The spaces $M_k(\Gamma)$ and $S_k(\Gamma)$ are both finite dimensional for all congruence subgroups.

The spaces $M_k(\Gamma_1(N))$ each admit a useful decomposition as a direct sum of subspaces. Let χ be a character modulo N. We let $M_k(\Gamma_0(N), \chi)$ denote the space of holomorphic functions $f : \mathbb{H} \to \mathbb{C}$ which satisfy $(f|_k\gamma) = \chi(d)f$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ as well as condition (ii) from the definition above. Then we have

$$M_k(\Gamma_1(N)) = \oplus_\chi M_k(\Gamma_0(N), \chi),$$

where the sum is over all Dirichlet characters modulo N. The eigenspaces $M_k(\Gamma_0(N), \chi)$ will be important in Chapters 3 and 6, where we will use them to construct modular forms with Fourier coefficients supported on specific residue classes.

Note that while we only define integral weight modular forms here, the definitions above can be modified to allow for half-integer values of k. Many important modular forms are of half integral weight, including the generating function for the partition numbers $p(n)$.

Another space that is important is the space of *weakly holomorphic modular forms*, which is denoted $M_k^!(\Gamma)$. The difference between weakly holomorphic modular forms and ordinary modular forms is that weakly holomorphic modular forms are allowed to have poles at the cusps of Γ. The vector space $M_k^!(\Gamma)$ is infinite dimensional.

Remarks on the structure of $M_k(\Gamma)$: The remainder of this subsection is not essential for understanding this thesis, but is included to provide a more complete summary of the theory of modular forms.

The weight k cusp forms are endowed with a Hilbert space structure given by the Petersson inner product, $< f, g >_{Petersson}$, which can be viewed as a hyperbolic analogue of the $L^2(\mathbb{R})$ inner product. While $< f, g >_{Petersson}$ does not extend to an inner product on all of $M_k(\Gamma)$, it is well defined if the product fg vanishes at all cusps. We can therefore decompose $M_k(\Gamma)$ as

$$M_k(\Gamma) = S_k(\Gamma)^{\perp} \oplus S_k(\Gamma).$$

The orthogonal complement of $S_k(\Gamma)$ consists of the *Eisenstein series* of $M_k(\Gamma)$. When $k \geq 3$, the space of Eisenstein series can be described explicitly by constructing, for each cusp α of Γ, a modular form which is nonvanishing at α and vanishes at all other cusps. When $k = 2$, this construction produces functions which do not satisfy the modular transformation law (it turns out that they are *quasi-modular*), and the weight two Eisenstein series are obtained by taking the linear combinations of these forms for which the sum of the constant terms in the Fourier expansions is zero. There is also an analogous construction of Eisenstein series when $k = 1$. The weight one Eisenstein series are used extensively in Chapter 6.

Bases for $S_k(\Gamma)$ are less straightforward to construct. One can quickly see that, as $\Gamma(dN) \subseteq \Gamma(N)$, the space $S_k(\Gamma)$ can be decomposed as the direct sum of the space of *old forms* of cusp forms of lower level, and the space of *newforms* $S_k(\Gamma_0(N))^{new}$.

The Hecke operators T_n are a family of commuting operators on $M_k(\Gamma)$ that act on Fourier series in a nice way. It turns out that the Hecke operators form an algebra of linear operators acting on $M_k(\Gamma)$ which are fundamental for understanding many of the arithmetic properties of modular forms, such as the famous Ramanujan Congruences for $p(n)$. The Hecke operators are self-adjoint with respect to the Petersson inner product on the space of newforms, and it follows that $S_k(\Gamma_0(N))^{new}$ has a basis of simultaneous eigenforms for the Hecke operators.

A typical feature of modular forms is for their Fourier coefficients to encode various kinds of arithmetically important information. In the next subsection, we give some examples of this.

2.1.3 Examples

Here, we give three examples of classical modular forms.

Modular forms can often be constructed by averaging some function over the action of modular group. Here is the simplest example:

$$E_k(z) = \frac{1}{2\zeta(k)} \sum_{(m,n)\in\mathbb{Z}^2 \ (0,0)} \frac{1}{(mz+n)^k}.$$

For even $k > 2$, this is a modular form of weight k with respect to the full modular group. Its Fourier series is given as follows:

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

where B_k is the kth Bernoulli number and $\sigma_{k-1}(n)$ is the well known sum of divisors function given by:

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

An important half weight modular form is the Jacobi theta function, which is defined by

$$\Theta(z) := \sum_{n\in\mathbb{Z}} q^{n^2}.$$

This is a weight 1/2 modular form with respect to $\Gamma_0(4)$. By taking its cube, we obtain the weight 3/2 modular form $\Theta(z)^3 =: \sum_{n=0}^{\infty} r(n)q^n$. This modular form is intimately tied to class numbers for imaginary quadratic fields. It is well known that the $r(n)$ are given by Hurwitz class numbers $H(n)$ (see Section 2.3).

Theorem 2.1.2 (Gauss)**.**

$$r(n) = \begin{cases} 12\frac{h(-m)}{w(-m)} \sum_{d|f} \mu(d) \left(\frac{-m}{d}\right) \sigma_1(\frac{f}{d}) & n \equiv 1, 2 \pmod 4 \\ 24\frac{h(-m)}{w(-m)} \sum_{d|f} \mu(d) \left(\frac{-m}{d}\right) \sigma_1(\frac{f}{d}) & n \equiv 3 \pmod 8 \\ r(n/4) & n \equiv 0 \pmod 4 \\ 0 & n \equiv 7 \pmod 8 \end{cases}$$

I conclude the chapter with a famous example arising in the study of partitions. Let $\eta(z)$ be defined by

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

This is a weight $\frac{1}{2}$ modular form on $SL_2(\mathbb{Z})$ and consequently $1/\eta(z)$ is a weight $-\frac{1}{2}$ modular form on $SL_2(\mathbb{Z})$. It is easily seen that $q^{1/24}/\eta(z)$ is the generating function for the partition numbers $p(n)$.

The proofs in Chapter 6 rely on the Circle Method. We record here, for later use, the explicit transformation formula for $\eta(z)$, in a form that is convenient for ascertaining the behavior of η near a cusp $\frac{h}{k}$. Assuming $(h, k) = 1$, there is an element of $SL_2(\mathbb{Z}$ given by $\alpha_{h,k} := \begin{pmatrix} -h & \frac{hH+1}{k} \\ -k & H \end{pmatrix}$.

For $\tau' = \frac{H}{k} + \frac{i}{z}$ and $\tau = \frac{h}{k} + \frac{iz}{k^2}$, where z is complex, we have $\alpha_{h,k}^{-1}(\tau) = \tau'$.

Theorem 2.1.3. *Let h, k, H, τ, τ' be as described above. Then we have*

$$\frac{q^{\frac{1}{24}}}{\eta(\tau)} = \frac{e^{2\pi i \frac{\tau'}{24}}}{\eta(\tau')} \left(\frac{z}{k}\right)^{\frac{1}{2}} e^{-\frac{\pi z}{12k^2} + \frac{\pi}{12z} + \pi i s(-H,k)},$$

where $s(h,k)$ denotes the Dedekind sum,

$$s(h,k) = \sum_{r=1}^{k-1} \frac{r}{k}\left(\frac{hr}{k} - \left\lfloor \frac{hr}{k} \right\rfloor - \frac{1}{2}\right). \tag{2.1}$$

See Theorem 5.1 in [Apo90] for a proof.

2.2 Harmonic Maass Forms

A harmonic Maass form is a certain kind of nonholomorphic modular form that has a natural decomposition into a holomorphic and nonholomorphic part. The holomorphic part of a harmonic Maass form is called a mock modular form, and every mock modular form naturally has a cusp form associated to it called its shadow. In this section, we define level 1 harmonic Maass forms (harmonic Maass forms of level greater than 1 are defined as the natural generalization of the definition given here) and state some of their important properties. For more on mock modular forms and harmonic Maass forms, see references such as [BF04], [Ono09], and [BFOR17]. Throughout, the variable z lies in $\mathbb{H}$ with $z = x + iy$, where $x, y \in \mathbb{R}$.

The *weight k hyperbolic Laplacian operator* Δ_k is defined as follows:

$$\Delta_k := -y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right) + iky\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right).$$

Bruinier and Funke in [BF04] first defined harmonic weak Maass forms.

Definition 2.2.1. *Let $F : \mathbb{H} \to \mathbb{C}$ be real-analytic, and assume that $k \geq 2$ is an even integer. Then F is a* weight $2-k$ harmonic weak Maass form *if the following hold:*

(i) F is weight $2-k$ invariant under $SL_2(\mathbb{Z})$, that is, for all $\gamma \in SL_2(\mathbb{Z})$, $(F|_{2-k}\gamma) = F$.

(ii) The weight $2-k$ hyperbolic Laplacian operator annihilates F, that is, $\Delta_{2-k}F = 0$.

(iii) There is a polynomial $P_F(q) \in \mathbb{C}[q^{-1}]$ *such that* $F(z) - P_F(q) = O(e^{-\epsilon y})$ *as* $y \to \infty$.

We let H_{2-k} denote the vector space of weight $2-k$ harmonic weak Maass forms. For convenience, we refer to harmonic weak Maass forms as *harmonic Maass forms*, and omit the word "weak".

The following fact is straightforward from the definition.

Theorem 2.2.2. *Every* $F \in H_{2-k}$ *can be written in the following way:*

$$F(z) = F^+(z) + \frac{(4\pi y)^{1-k}}{k-1}\overline{c_0(y)} + F^-(z),$$

where F^+ *and* F^- *have Fourier expansions as follows, for some* $m_0 \in \mathbb{Z}$*:*

$$F^+(z) = \sum_{n=m_0}^{\infty} c_F^+(n)q^n,$$

and

$$F^-(\tau) = \sum_{n>0} \overline{c_F^-(n)}\Gamma(1-k, 4\pi n y)q^{-n}.$$

In the theorem, F^+ is called the *holomorphic part* of F, and $\frac{(4\pi y)^{1-k}}{k-1}\overline{c_0(y)} + F^-(\tau)$ is called the *nonholomorphic part* of F. When the nonholomorphic part is nonzero, F^+ is called a *mock modular form.*

The following theorem, due to Bruinier and Funke [BF04], explains why we conjugate the coefficients of the nonholomorphic part in Theorem 2.2.2.

Theorem 2.2.3 (Bruinier, Funke)**.** *The operator* $\xi_{2-k} : H_{2-k} \to S_k$ *given by* $\xi_{2-k} = 2iy^{2-k}\frac{\overline{\partial}}{\partial \overline{\tau}}$ *is well defined and surjective. Moreover, for* $F \in H_{2-k}$,

$$\xi_{2-k}(F) = -(4\pi)^{k-1}\sum_{n>0} c_F^-(n)n^{k-1}q^n \in S_k,$$

where $c_F^-(n)$ *and* n_0 *are as in Theorem 2.2.2.*

For any $F \in H_{2-k}$, the cusp form $(-4\pi)^{k-1}\sum_{n=n_0}^{\infty} c_F^-(n)q^n \in S_k$ is called the *shadow* of the mock modular form F^+.

2.3 Hurwitz Eisenstein Series

In this section, we give an example of a harmonic Maass form that will be useful in the next chapter.

For nonzero integers D, we let $h(D)$ be the class number of $\mathbb{Q}(\sqrt{D})$. In other words, $h(D)$ is the size of the index of the group of fractional ideals for $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ over its subgroup of principal fractional ideals. Recall that $h(D) = 1$ precisely when $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a Unique Factorization Domain.

The class numbers $h(D)$ count classes of binary quadratic forms with discriminant D up to matrix equivalence. The *Hurwitz class numbers* $H(n)$ come from counting equivalence classes of binary quadratic forms inversely weighted by the size of their stabilizer in $SL_2(\mathbb{Z})$. Specifically, we define $H(n)$ as follows for positive integers n. Suppose $-n = Df^2$, where $D < 0$ is a square-free fundamental discriminant.

$$H(n) = \frac{h(D)}{w(D)} \sum_{d|f} \mu(d) \left(\frac{D}{d}\right) \sigma_1(\frac{f}{d}),$$

where $w(-n)$ is half the number of units in the integer ring of $\mathbb{Q}(\sqrt{-n})$, that is

$$w(-m) = \begin{cases} 4 & m = 1 \\ 3 & m = 3 \\ 2 & m = 2, n > 3 \end{cases}$$

Let $\mathcal{H}(z)$ be defined by

$$\mathcal{H}(z) := -\frac{1}{12} + \sum_{n=1}^{\infty} H(n)q^n + \frac{1}{4\sqrt{\pi}} \sum_{n=1}^{\infty} \Gamma(-\frac{1}{2}, 4\pi n^2 y) q^{-n^2} + \frac{1}{8\pi\sqrt{y}}.$$

Zagier showed that $\mathcal{H}(z)$ is a harmonic Maass form [Zag75].

Theorem 2.3.1. *(Zagier) $\mathcal{H}(z)$ is a weight $\frac{3}{2}$ harmonic Maass form of moderate growth on $\Gamma_0(4)$. Moreover, $\xi_{3/2}(H) = -\frac{1}{16\pi}\Theta$.*

By "moderate growth", I mean that instead of (iii) in the definition of harmonic Maass form, we have $\mathcal{H}(z) = O(y^r)$ as $y \to \infty$ for some real value r, and analogous conditions hold at all cusps. We have to modify condition (iii) due to the presence of the third term in the definition of $\mathcal{H}(z)$. Harmonic Maass forms which satisfy certain weakened or altered growth conditions have shadows which are modular forms but are not cusp forms, as we see in Theorem 2.3.1.

In the next chapter, I show how one can use $\mathcal{H}(z)$ to construct modular forms whose coefficients are the Hurwitz class number for fields with desired splitting conditions.

Chapter 3

Indivisibility of Class Numbers of Imaginary Quadratic Fields

This chapter is devoted to the proof of Theorem 1.2.1, Corollary 1.2.2, and Corollary 1.2.3.

Theorem 1.2.1 gives a bound on the smallest discriminant satisfying Wiles' theorem. The proof relies on Zagier's weight 3/2 harmonic Maass form $\mathcal{H}(z)$, which is discussed in Chapter 2.3. The idea is to take linear combinations of twists of $\mathcal{H}(z)$ to construct a modular form that is only supported on discriminants satisfying the desired local data. Then we use the theory of modular forms to bound the smallest Fourier coefficient that is indivisible by p.

Corollary 1.2.2 follows from using Dirichlet's Theorem on primes in arithmetic progression to count discriminants given by Theorem 1.2.1. Specifically, one obtains an imaginary quadratic field whose discriminant is divisible by p for every p in a certain arithmetic progression.

Corollary 1.2.3 follows from using the primes of bad reduction of an elliptic curve to generate the local conditions, and applying Corollary 1.2.2. A theorem of Frey relates the indivisibility of the class numbers to that of Selmer groups of quadratic twists.

Remark on the necessity of harmonic Maass forms: The Θ^3 modular form was used in most modular forms results on indivisibility of class numbers, such as [KO99]. However, it is insufficient for our result, because its Fourier coefficients are not supported on all arithmetic progressions. For the square free n with $n \equiv 7 \pmod 8$, the class numbers $h(-n)$ are not represented. We do not have this problem when working with $\mathcal{H}(z)$, because its Fourier coefficients represent all class numbers.

3.1 Sieving Zagier's Harmonic Maass Form

We require the following result, which shows that we can define holomorphic modular forms whose coefficients are supported on fundamental discriminants satisfying local conditions and are given by class numbers. Given sets S_+, S_-, S_0 as in Theorem 1.2.1, we let A_Σ be defined as the set of positive integers n such that the following hold:

1. For $p \in S_+ \cup S_- \cup S_-$, $p^2 \nmid n$.

2. $\mathbb{Q}(\sqrt{-n})$ splits at the primes in S_+, ramifies at the primes in S_0, and is inert at the primes in S_-.

Lemma 3.1.1. *Let S_+, S_-, S_0 be sets as in Theorem 1.2.1, and assume that S_- is nonempty.*

Then there is a weight $\frac{3}{2}$ modular form $H^\Sigma(z) = \sum_{n=1}^{\infty} a(n)q^n$ on $\Gamma_0(N_\Sigma)$, where N_σ is as in equation (1.5), such that

$$a(n) = \begin{cases} H(n) & n \in A_\Sigma \\ 0 & \textit{otherwise} \end{cases}$$

The idea is to take combinations of twists of Zagier's function $\mathcal{H}(z)$ to obtain holomorphic modular form. The key properties of $\mathcal{H}(z)$ that allow us to do this are

1. The Fourier expansion of the non-holomorphic part is supported on terms of the form q^{-n^2}, which allows us to use twisting to annihilate the non-holomorphic part of $\mathcal{H}(z)$, and

2. $\mathcal{H}(z)$ has moderate growth at poles, which ensures that any linear combination of twists of $\mathcal{H}(z)$ will not have any exponential singularities, as a weakly holomorphic modular form would.

For χ, ψ Dirichlet characters modulo m and N, the twist of $\mathcal{G}(z) := \sum_{n=0}^{\infty} a(n,y)q^n \in H_k(\Gamma_0(N), \psi)$ by χ is given by

$$\mathcal{G}_\chi(z) = \sum_{n \in \mathbb{Z}} \chi(n)a(n,y)q^n.$$

If d is a positive integer, the operators $U(d), V(d)$ are defined, as one does when working with holomorphic modular forms, by

$$(\mathcal{G}|U(d))(z) := \sum_{n \in \mathbb{Z}} a(dn,y)q^n$$

and

$$(\mathcal{G}|V(d))(z) := \sum_{n \in \mathbb{Z}}^{\infty} a(n,y)q^{dn}.$$

It is well known that a twist of a modular form is itself a modular form, for a proof, see Proposition 17 on page 127 of [Kob93]. The same proof shows that twists of harmonic Maass forms are also harmonic Maass forms. Specifically, for $\mathcal{G}(z) \in H^{mg}_{k+\frac{1}{2}}(\Gamma_0(4N), \psi)$, the form $\mathcal{G}_\chi(z)$ belongs to $H^{mg}_{k+\frac{1}{2}}(\Gamma_0(4Nm^2), \psi \cdot \chi^2)$, and $(\mathcal{G}|V(d))$ and $(\mathcal{G}|U(d))$ lie in $H^{mg}_{k+\frac{1}{2}}(\Gamma_0(4Nd), \psi \cdot \left(\frac{4d}{\cdot}\right))$.

Proof of Lemma 3.1.1: First, we take a combination of twists for which the nonholomorphic part of $\mathcal{H}(z)$ is annihilated. Let p be in S_-. We have

$$\begin{aligned} f(z) &:= \frac{1}{2}(\mathcal{H}(z) - \left(\frac{-1}{p}\right)\mathcal{H}_{\left(\frac{\cdot}{p}\right)}(z)) \\ &= \sum_{n=1}^{\infty} \frac{1}{2}\left(1 - \left(\frac{-n}{p}\right)\right) H(n)q^n + \frac{1}{16\sqrt{\pi}} \sum_{p|n} \Gamma(-\frac{1}{2}, 4\pi n^2 y)q^{-n^2}. \end{aligned}$$

Note that the coefficient of q^n in the holomorphic part of $f(z)$is $\frac{1}{2}H(n)$ if $p|n$, $H(n)$ if $(\frac{-n}{p}) = -1$, and 0 if $\left(\frac{-n}{p}\right) = 1$. The nonholomorphic part of f is supported on multiples of p, because twisting the nonholomorphic part by the Legendre symbol annihilates those coefficients. To eliminate what remains of the nonholomorphic part and the multiples of p in the holomorphic part, we take the twist $f_{\left(\frac{\cdot}{p}\right)^2}$.

Repeating the above steps for every $p \in S_+ \cup S_-$, we obtain a form which is supported on n for which the primes in $S_+ \cup S_-$ split or are inert in $\mathbb{Q}(\sqrt{-n})$ as desired.

To obtain a modular form which is supported on coefficients which are multiples of the primes in S_0, let d be the product of the primes in S_0. We apply the $U(d)$, operator, then twist by $\left(\frac{-n}{q}\right)^2$ for each $q \in S_0$, and then apply the $V(d)$ operator.

□

3.2 Proof of Theorem 1.1

The proof of Theorem 1.2.1 requires a well known result of Sturm [Stu80], which says that if a modular form with integer Fourier coefficients is nonvanishing modulo a prime ℓ, then there is a bound on the index of the first coefficient which is nonzero modulo ℓ. To state his theorem, for a rational prime ℓ and a modular form $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$ with coefficients in $\mathbb{Z}$, we define

$$ord_\ell(f) := min_n\{n : \ell \nmid a(n)\},$$

and we say $ord_\ell(f) := \infty$ if $\ell | a(n)$ for all n.

Theorem 3.2.1 (Sturm). *For a modular form $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$ with integer Fourier coefficients, if*

$$ord_\ell(f) > \frac{k}{12}[\Gamma_0(1) : \Gamma_0(N)],$$

then $ord_\ell(f) = \infty$.

Remark 3.2.2. *Note that Sturm's theorem was originally only formulated for holomorphic modular forms of integer weight, but the proof carries over to half-integral weight modular forms by raising half-integral weight forms to even powers.*

Proof of Theorem 1.2.1: Let $H^\Sigma(z)$ be the modular form from Lemma 3.1.1 for S_+, S_-, and S_0, replacing $S-$ with $\{Q_\Sigma\}$ if $S_- = \emptyset$. Let

$$\mathcal{F}(z) := \left(H^\Sigma | U(p)\right) - p\left(H^\Sigma | V(p)\right).$$

By Lemma 3.1.1, the form $\mathcal{F}(z)$ is a modular form of weight $\frac{3}{2}$ on $\Gamma_0(pN_\Sigma)$. By Theorem 1 of Wiles [Wil15], $\mathcal{F}(z)$ has a Fourier coefficient which is indivisible by ℓ. Therefore Sturm's Theorem tells us that we have

$$n_p := ord_\ell(\mathcal{F}) \leq \frac{3}{24}[\Gamma_0(1) : \Gamma_0(pN_\Sigma)].$$

It follows from a well-known formula for $[\Gamma_0(1) : \Gamma_0(N)]$ (see for example [Ono00]) that we have

$$n_p \leq M_\Sigma(p+1).$$

We have that n_p must be of the form $f_p^2 k_p$, with k_p square free. It follows from conditions (1)-(3) in Theorem 1.2.1 that for all $n \leq M_\Sigma$, the np^{th} Fourier coefficient of $\mathcal{F}(z)$ is divisible by ℓ, so $p \nmid k_p$. Therefore either $-pk_p$ or $-4pk_p$ is a fundamental discriminant for an imaginary quadratic field satisfying the desired local conditions and whose class number is indivisible by ℓ. $\square$

3.3 Proof of Theorem 1.2

Note that at least half of the values $k_p p$ from the main theorem must be distinct as p varies over the primes greater than M_Σ satisfying the conditions of Theorem 1.2.1. If instead we had $k_p p = k_q q = k_r r$ with $p < q < r$, we would have $qr | k_p$, which would violate the bound on k_p.

To count the fundamental discriminants down to $-X$ which satisfy the desired conditions, it suffices to count the primes which satisfy the conditions of Theorem 1.2.1 for which the fundamental discriminant from Theorem 1.2.1 is greater than $-X$.

The primes p that satisfy the third condition of Theorem 1.2.1 are those for which for each q up to M_Σ, p lies one of $\frac{q-1}{2}$ arithmetic progressions modulo q, which correspond to p being a quadratic residue modulo q. Similarly, the other two conditions amount to restricting p to certain arithmetic progressions modulo 2 and ℓ.

For the fundamental discriminant corresponding to p obtained from Theorem 1.2.1 to be guaranteed to be greater than $-X$, it suffices to require

$$4pM_\Sigma(p+1) \leq X.$$

It follows from Dirichlet's Theorem for primes in arithmetic progressions that given $\epsilon > 0$ for sufficiently large X, we have

$$\#\{-X < D < 0 : \ell \nmid h(D), D \in T_\Sigma\} \geq \left(\frac{\ell-2}{\ell-1}\frac{1}{2^{r_\Sigma+4}\sqrt{M_\Sigma}} - \epsilon\right)\frac{\sqrt{X}}{\log X}.$$

3.4 Twists of Elliptic Curves

First we recall a theorem of Frey [Fre88], which gives a relationship between Selmer groups of quadratic twists of certain elliptic curves E and the ideal class group of the quadratic field associated with the twisting discriminant. For the quadratic fields $\mathbb{Q}(\sqrt{D})$ appearing in Frey's result, all of the primes of bad reduction of E factor (i.e. split, ramify, or remain inert) in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ in a prescribed way depending on their reduction type.

To state Frey's conditions precisely, we must define Tate curves, which are a class of elliptic curves over local fields. The local fields we will refer to are simply the p-adic completions of $\mathbb{Q}$, denoted by $\mathbb{Q}_p$. Tate curves admit a uniformizing map (which here means a complex analytic isomorphism of Riemann surfaces that also preserves the group structure) that is analogous to one admitted by all elliptic curves over $\mathbb{C}$. We recall the analogous facts for elliptic curves over $\mathbb{C}$ in the next paragraph.

Every elliptic curve over $\mathbb{C}$ admits a uniformization $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where Λ is an additive discrete subgroup of $\mathbb{C}$ which can be taken to be of the form $\Lambda = \mathbb{Z}+\tau\mathbb{Z}$, with $\tau \in \mathbb{H}$. The map $z \to e^{2\pi i z}$ applied to $\mathbb{C}/\Lambda$ yields the uniformization $E(\mathbb{C}) \cong \mathbb{C}/e^{2\pi i \tau \mathbb{Z}}$, where $\mathbb{C}^*$ is the multiplicative subgroup of $\mathbb{C}$ and $e^{2\pi i \tau \mathbb{Z}}$ denotes the subgroup of $\mathbb{C}^*$ generated by $e^{2\pi i \tau}$.

Now let K be a local field which is complete with respect to a discrete valuation v. A Tate curve over K is an elliptic curve E over K which admits a uniformization $K^*/q^{\mathbb{Z}} \cong E(K)$ for some $q \in K^*$with $|q|_v < 1$, where $q^{\mathbb{Z}}$ is the subgroup of K^* (the multiplicative subgroup of K) generated by q. A Weierstrass form and uniformizing map for such curves can be defined explicitly by series expansions in terms of q. The j-invariant and discriminant Δ are given by $\frac{1}{q}+744+196884q+\cdots$ and $q\prod_{n\geq 1}(1-q^n)^{24}$ respectively, which are identical to the formulas in the complex case. See Appendix C.14 of [Sil86] for a much more detailed introduction to Tate curves.

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E, j-invariant j_E, and discriminant Δ_E, and suppose that E contains a point P of odd prime order ℓ. We let S_E denote the set of primes q dividing N_E such that $q \equiv -1 \pmod{\ell}$, and $v_q(\Delta_E) \not\equiv 0 \pmod{\ell}$, and $v_q(j_E) < 0$. Let $Sel_\ell(E_D, \mathbb{Q})_\ell$ denote the elements of order ℓ in the Selmer group of E_D.

Theorem 3.4.1 (Frey). *Suppose $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational torsion point P of odd prime order ℓ, and suppose P is not contained in the kernel of reduction modulo ℓ. Suppose $\widetilde{S}_E = \emptyset$. Suppose that D is a negative square-free integer coprime to ℓN_E and satisfies*

1. *If $2|N_E$ then $d \equiv 3 \pmod 4$*
2. *If $ord_\ell(j(E)) < 0$, then $\left(\frac{D}{\ell}\right) = -1$,*
3. *If $p|N_E$ is an odd prime, then*

$$\left(\frac{d}{p}\right) = \begin{cases} -1 & \text{if } ord_p(j_E) \geq 0 \\ -1 & \text{if } ord_p(j_E) < 0 \text{ and } E/\mathbb{Q}_p \text{ is a Tate curve} \\ 1 & \text{otherwise} \end{cases}$$

Then $Sel_\ell(E_D, \mathbb{Q})_p$ is nontrivial if and only if $\ell | h(D)$.

Now to prove the corollary, note that the twists E_D have trivial ℓ torsion over $\mathbb{Q}$. We set

$$S_+ = \{p|N_E, ord_p(j_E) < 0 : E/\mathbb{Q}_l \text{ is not a Tate Curve}\},$$

and

$$S_- = \{p|N_E : p \notin S_+\},$$

and $S_0 = \emptyset$. It follows from Corollary 1.2.2 that there are at least $O(\frac{\sqrt{X}}{\log X})$ fundamental discriminants down to $-X$ which satisfy Frey's conditions, and so the result follows from Theorem 3.4.1.

3.5 Examples

Here we illustrate Theorem 1.2.1 and Corollary 1.2.3.

Example 3.5.1. *Suppose that* $\ell = 5$ *and that the sets are* $S_+ = \{3\}$, $S_- = S_0 = \emptyset$.

The smallest prime which satisfies the conditions of Theorem 1.2.1 is 394969. The smallest discriminant bounded by Theorem 1.2.1 is a multiple of this prime, however, it is clear that one shouldn't need to look at numbers that large to find imaginary quadratic fields which split at 3 and have a class number which is not divisible by 5. By direct calculation, we see that for the primes p *less than 100, for all but 79 we have* $5 \nmid h(-p)$, *out of which 11 of the 21 corresponding imaginary quadratic fields split at 3. This discrepancy between the bounds predicted by Theorem 1.2.1 and the actual fundamental discriminants we observe is typical of these theorems, and it illustrates the main obstacles which remain in attacking the original Cohen-Lenstra conjectures.*

Example 3.5.2. *Let* $E : y^2 + y = x^3 - x^2 + 20x - 8$ *be the elliptic curve with Cremona label 203.a1. Then* $E(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$. *The conductor of* E *is* $7 \cdot 29$. *It follows from Corollary 1.2.3 that we have*

$$\#\{-X < D < 0 : rk(E_D) = 0, Sel_5(E_D) = \{1\}\} \gg \frac{\sqrt{X}}{\log X}.$$

Chapter 4

Shifted Convolution L-functions

The goal of this chapter is to prove Theorem 1.3.2.

The main ingredients of the proof, in addition to many basic facts about harmonic Maass forms which are discussed in Chapter 2, are a theorem of Mertens and Ono [MO16], which says that the generating function for the symmetrized shifted convolution L-values is nearly the product of a mock modular and modular form, and the Eichler-Shimura isomorphism theorem which we use to describe the obstruction to modularity for our generating functions.

This chapter is organized into three subsections. The first subsection describes the theory of period polynomials and the Eichler-Shimura theorem, the second describes the work of Mertens and Ono [MO16], and the third proves Theorem 1.3.2.

4.1 Period Functions

We require some facts about period polynomials and their relationship to the obstructions to modularity for mock modular forms. We first recall the definition and important properties of periods polynomials.

Definition 4.1.1 (Period Polynomial). *Let $f \in S_k(\Gamma_0(N))$ be a cusp form where*

$k \geq 2$ is even. We define the nth period of f *by*

$$r_n(f) := \int_0^\infty f(it)t^n dt.$$

The period polynomial of f is defined by

$$r(f;z) := r^+(f,z) + ir^-(f,z),$$

where

$$r^-(f,z) = \sum_{\substack{0 \leq n \leq k-2 \\ 2 \nmid n}} (-1)^{\frac{n-1}{2}} \binom{k-2}{n} r_n(f) z^{k-2-n}$$

and

$$r^+(f,z) = \sum_{\substack{0 \leq n \leq k-2 \\ 2 \mid n}} (-1)^{\frac{n}{2}} \binom{k-2}{n} r_n(f) z^{k-2-n}.$$

Remark 4.1.2. *One can show that $L(f, n+1) = \frac{(2\pi)^{n+1}}{n!} r_n(f)$, where $L(f,s)$ is the L-series for f.*

The Eichler-Shimura isomorphism theorem and the work of Kohnen and Zagier [KZ84] imply that the maps r^+ and r^- define correspondences between $S_k(\Gamma_0(N))$ and explicitly defined subspaces of the vector space of degree $k-2$ polynomials with coefficients in $\mathbb{C}$. These important bijections can be used to efficiently compute spaces of cusp forms.

Bringmann, Guerzhoy, Kent, and Ono in [BGKO13] connected period polynomials to the theory of harmonic Maass forms. They showed that the obstruction to modularity for a mock modular form can be described in terms of the periods of its shadow.

Definition 4.1.3 (Period Function)**.** *Let $F^+(\tau)$ be a mock modular form of weight $2-k$ with respect to $SL_2(\mathbb{Z})$, and $\gamma \in SL_2(\mathbb{Z})$. The* period function of F^+ with respect to γ *is defined as follows:*

$$\mathbb{P}(F^+, \gamma; \tau) := \frac{(4\pi)^{k-1}}{\Gamma(k-1)}(F^+ - F^+|_{2-k}\gamma))(\tau).$$

Theorem 4.1.4 (Bringmann, Guerzhoy, Kent, Ono)**.** *Let* $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$*. Then we have that the period function with respect to* S *is given by*

$$\overline{\mathbb{P}(F^+, S; \tau)} = \sum_{n=0}^{k-2} \frac{L(f, n+1)}{(k-2-n)!}(2\pi i\tau)^{k-2-n}.$$

We require a generalization of this result due to Bringmann, Fricke, and Kent in [BFK14]. Among other results, they proved that the period functions corresponding to other modular transformations are also polynomials whose coefficients are essentially values of additive twists of $L(f, s)$.

Let $L(f, e^{-2\pi id/c}; s)$ be defined for $c \neq 0$, $c, d \in \mathbb{Z}$ by

$$L(f, e^{-2\pi id/c}, s) := \sum_{n=1}^{\infty} \frac{e^{-2\pi idn/c}a_n}{n^s}$$

for $\Re(s)$ sufficiently large and by analytic continuation elsewhere. The analytic continuation is given by

$$L(f, e^{-2\pi id/c}; s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^{\infty} f\left(iy - \frac{d}{c}\right) dy.$$

Theorem 4.1.5 (Bringmann, Fricke, Kent)**.** *Let* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ *satisfy* $c \neq 0$*. Then*

$$\mathbb{P}(F^+, \gamma, z) = \sum_{n=0}^{k-2} \frac{\overline{L(f, e^{-2\pi id/c}, n+1)}}{(k-2-n)!}(-2\pi i)^{k-2-n}\left(\frac{cz+d}{c}\right)^{k-2-n}. \tag{4.1}$$

4.2 Work of Mertens and Ono

Mertens and Ono related the values $\hat{D}(f_1, f_2, h; k-1)$ to the theory of harmonic Maass forms by studying the generating function

$$\mathbb{L}(f_1, f_2; \tau) := \sum_{h=1}^{\infty} \hat{D}(f_1, f_2, h; k-1) q^h,$$

where $q = e^{2\pi i\tau}$ for $\tau \in \mathbb{H}$. They proved that $\mathbb{L}(f_1, f_2; \tau)$ is the sum of a a weakly holomorphic modular or quasimodular form and the product of a mock modular form and a cusp form.

To state their theorem, we need to define a few spaces. Let $\widetilde{M_k}(\Gamma_0(N))$ be as follows for even $k \geq 2$:

$$\widetilde{M_k}(\Gamma_0(N)) := \left\{ \begin{array}{ll} M_k(\Gamma_0(N)) & \text{if } k \geq 4 \\ M_2(\Gamma_0(N)) \oplus \mathbb{C}E_2 & \text{if } k = 2 \end{array} \right\} \tag{4.2}$$

Moreover, let $\widetilde{M_k^!}(\Gamma_0(N))$ be the extension of $\widetilde{M_k}(\Gamma_0(N))$ by the weight k weakly holomorphic modular forms on $\Gamma_0(N)$. A weakly holomorphic modular form is a meromorphic modular form whose poles are supported at cusps.

We say that a harmonic Maass form F is *good* for a cusp form f if f is the shadow of F^+ and $F(\tau)f(\tau)$ is bounded at all cusps. Note that there are cusp forms f for which there is no mock modular form that is good for f.

Theorem 4.2.1. *For $f_1, f_2 \in S_k(\Gamma_0(N))$, we have*

$$\mathbb{L}(f_1, f_2; \tau) = -\frac{1}{(k-1)!} M_{f_1}^+(\tau) f_2(\tau) + F(\tau), \tag{4.3}$$

where $M_{f_1}^+$ is a mock modular form whose shadow is f_1 and $F(\tau) \in \widetilde{M_2^!}(\Gamma_0(N))$. If M_{f_1} is good *for f_2, then $F \in \widetilde{M_2}(\Gamma_0(N))$.*

Remark 4.2.2. *They actually prove a more general result for when f_1 and f_2 are cusp forms of weight k_1 and k_2 respectively with $k_1 \geq k_2$. In this case, the formula involves the Rankin-Cohen bracket $[M^+_{f_1}(\tau), f_2(\tau)]_{\frac{k_1-k_2}{2}}$, and the form F lies in $\widetilde{M}^!_{\frac{k_1-k_2}{2}}(\Gamma_0(N))$.*

The form $F(\tau)$ in Theorem 4.2.1 can be described as the image of $M_{f_1} f_2$ under a modified holomorphic projection operator. Recall that if f is a smooth (that is, analytic in the variables $Re(\tau)$ and $Im(\tau)$, and not necessarily holomorphic) weight $k \geq 2$ modular form for $\Gamma_0(N)$ with moderate growth at cusps, then its holormorphic projection $\pi_{hol} f$ lies in $\widetilde{M}_k(\Gamma_0(N))$. For more on the classical holomorphic projection operator, see [Stu80], [IRR14], [Mer] and [GZ86].

The regularized holormorphic projection operator π^{reg}_{hol} is an extension of π_{hol} to an operator on smooth modular forms with certain exponential singularities at cusps. This definition is due to Mertens and Ono [MO16] who based it on Borcherds' [Bor98] regularized Petersson inner product.

Definition 4.2.3. *Regularized Holomorphic Projection Let $f : \mathbb{H} \to \mathbb{C}$ be real-analytic, weight $k \geq 2$ modular with respect to $\Gamma_0(N)$, and have Fourier series $\sum_{n\in\mathbb{Z}} a_f(n, y)q^n$. Let the cusps of $\Gamma_0(N)$ be denoted $\kappa_1, \cdots, \kappa_s$ where $\kappa_1 = i\infty$. For each κ_j, fix some $\gamma_j \in 2(\mathbb{Z})$ with $\gamma_j \kappa_j = i\infty$. Suppose that for each κ_j, there is a polynomial $H_{\kappa_j}(X) \in \mathbb{C}[X]$ such that*

$$(f|_k \gamma_j^{-1})(\tau) - H_{\kappa_j}(q^{-1}) = O(v^{-\epsilon}),$$

for some $\epsilon > 0$. Also, suppose $a_f(n, y) = O(y^{2-k})$ as $y \to 0$ for all $n > 0$. Then we define the regularized holomorphic projection *of f by*

$$(\pi^{reg}_{hol} f) = H_{i\infty}(q^{-1}) + \sum_{n=1}^{\infty} c(n)q^n,$$

where

$$c(n) = \lim_{s\to 0} \frac{(4\pi n)^{k-1}}{(k-2)!} \int_0^\infty a_f(n,y) e^{-4\pi n y} y^{k-2-s} dy.$$

It turns out that if f is a real analytic modular form, $\pi_{hol}^{reg} f$ is a weakly holomorphic modular or quasimodular form.

Theorem 4.2.4 (Mertens, Ono)**.** *Suppose f is as in the previous definition. Then $\pi_{hol}^{reg}(f)$ lies in $\widetilde{M}_k^!(\Gamma_0(N))$.*

Remark 4.2.5. *In Theorem 4.2.1, we have*

$$F(\tau) = \frac{1}{(k_1-1)!} \pi_{hol}^{reg}(M_{f_1}^+ \cdot f_2)(\tau).$$

4.3 Proof of Theorem 1.3.2

In this section we prove Theorem 1.3.2. First we prove a lemma which gives a bound for the obstruction to modularity for a mock modular form. Throughout the section, let $\mathcal{F}$ denote the usual fundamental domain for $\mathbb{H}$, given by

$$\mathcal{F} := \{\tau \in \mathbb{H} : |\tau| > 1, -1 \le \Re(\tau) < 1\}.$$

4.3.1 Lemma

We prove an estimate for $\mathbb{P}(M_f^+, \alpha; \tau)$ (defined in Section 4.1).

Lemma 4.3.1. *Let $f \in S_k$ be a cusp form, and M_f^+ be a harmonic Maass form whose shadow is f. Then there exists a constant $C(f) > 0$ such that for all $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in 2(\mathbb{Z})$ with $c \neq 0$ and $\tau \in \mathcal{F}$, we have*

$$|\mathbb{P}(M_f^+, \alpha; \tau)| \le C(f) |c\tau + d|^{k-2}.$$

Proof. By Theorem 4.1.5, we have

$$\frac{\mathbb{P}(M_f^+, \alpha; \tau)}{(c\tau + d)^{k-2}} = \sum_{n=0}^{k-2} \frac{\overline{L(f, e^{-2\pi i d/c}, n+1)}}{(k-2-n!)} (-2\pi i)^{k-2-n} \left(\frac{1}{c^{k-2-n}(c\tau + d)^n} \right). \tag{4.4}$$

One can show that $\int_0^\infty f(iy - x) y^{s-1} dy$ is a periodic continuous function in x, thus for fixed n the values $L(f, e^{-2\pi i d/c}; n+2)$ can be bounded independently of c and d. Since $|c| \geq 1$ and $|c\tau + d| \geq \frac{\sqrt{3}}{2}$ for $\tau \in \mathcal{F}$, the right hand side of equation (4.4) is bounded uniformly in α and $\tau \in \mathcal{F}$. $\square$

4.3.2 Proof of Theorem 1.3.2

Let $F(\tau) := \pi_{hol}^{reg}(M_{f_1} f_2) - M_{f_1}^+ f_2 = \pi_{hol}^{reg}(M_{f_1}^- f_2)$. By Theorem 4.2.1, we have $F(\tau) = (k-1)! \cdot \mathbb{L}(f_1, f_2; \tau)$.

Since F is holomorphic, by Cauchy's integral formula the coefficients of $\mathbb{L}(f_1, f_2, \tau)$ are given by a contour integral as follows.

$$\begin{aligned} (k-1)! \hat{D}(f_1, f_2, h; k-1) &= \frac{1}{2\pi i} \int_C \frac{F(\tau)}{q^{h+1}} dq \\ &= \int_0^1 F\left(x + \frac{i}{h}\right) e^{-2\pi i h(x + (i/h))} dx. \end{aligned}$$

Choose $\beta \in \mathbb{C}$ so that $G(\tau) := \pi_{hol}^{reg}(M_{f_1}^- f_2) - \beta E_2(\tau)$ lies in $M_2^!(SL_2(\mathbb{Z}))$, and let $E_2^*(\tau)$ be the completed weight 2 nonholomorphic modular form $E_2^*(\tau) = E_2(\tau) -$

$\frac{3}{\pi\Im(\tau)}$. We rewrite the integral in the previous expression as follows:

$$\begin{aligned}(k-1)!\hat{D}(f_1, f_2, h; k-1) = &\int_0^1 e^{-2\pi ih(x+(i/h))}\left(\beta E_2^*\left(x+\frac{i}{h}\right)+G\left(x+\frac{i}{h}\right)\right)dx \\ &-\int_0^1 e^{-2\pi ih(x+(i/h))}M_{f_1}\left(x+\frac{i}{h}\right)f_2\left(x+\frac{i}{h}\right)dx \\ &+\int_0^1 M_{f_1}^-\left(x+\frac{i}{h}\right)f_2\left(x+\frac{i}{h}\right)e^{-2\pi ih(x+(i/h))}dx \\ &-\beta\int_0^1 e^{-2\pi ih(x+(i/h))}\frac{3}{\Im(x+\frac{i}{h})\pi}dx.\end{aligned}$$

By direct evaluation, the fourth integral is 0.

The difference of the first and second integrals satisfies an $O(h)$ estimate. This follows from the fact that the difference of the integrands is a smooth weight 2 modular form which vanishes as $e^{2\pi i\tau}$ as $\tau \to i\infty$.

To complete the proof, it is sufficient to show that the third integral satisfies an $O(h^{\frac{k}{2}})$ estimate, and for this it is sufficient to establish that $h(\tau) := M_{f_1}^-(\tau)f_2(\tau)y^{\frac{k}{2}}$ is bounded on $\mathbb{H}$.

As $\tau \to i\infty$, $h(\tau)$ has exponential decay because of the exponential decay of f_2. Thus, h is bounded on the fundamental domain $\mathcal{F}$.

It is sufficient to show that for $\alpha = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, $h(\alpha\tau)$ is bounded on $\mathcal{F}$ uniformly with respect to α. Rewriting $|h(\alpha\tau)|$ using the modular invariance of $|f_2(\tau)\Im(\tau)^{\frac{k}{2}}|$, we have

$$|h(\alpha\tau)| = |f_2(\tau)M_{f_1}^-(\alpha\tau)||\Im(\tau)|^{\frac{k}{2}}.$$

Substituting

$$M_{f_1}^-(\tau) + \mathbb{P}(f, \alpha, \tau) = M_{f_1}^-|_{2-k}(\alpha)(\tau)$$

gives

$$|h(\alpha\tau)| \leq |f_2(\tau)\Im(\tau)|^{\frac{k}{2}} \left(|\frac{M^-_{f_1}(\tau)}{(c\tau+d)^{k-2}}| + |\frac{1}{(c\tau+d)^{k-2}}\mathbb{P}(f,\alpha;\tau)| \right).$$

The second factor is bounded on $\mathcal{F}$ because of Lemma 4.3.1, the fact that $|c\tau+d| \geq \frac{\sqrt{3}}{2}$ on $\mathcal{F}$, and the exponential decay of $M^-_{f_1}(\tau)$ as $\tau \to i\infty$. On the other hand, $f_2(\tau)|\Im(\tau)|^{\frac{k}{2}}$ has exponential decay at $i\infty$. Thus, $|h(\alpha\tau)|$ is bounded for $\tau \in \mathcal{F}$. This completes the proof.

4.3.3 Example

When $f_1 = f_2 = \Delta$, where $\Delta(\tau)$ is the modular discriminant, that is, the unique normalized cusp form of weight 12, Theorem 4.2.1 says

$$\mathbb{L}(\Delta,\Delta;\tau) = \frac{Q^+(-1,12,1;\tau)\Delta(\tau)}{11!\beta} - \frac{E_2(\tau)}{\beta} = 33.38465...q + 266.447...q^2 + \cdots,$$

where $Q^+(-1,12,1;\tau)$ is the holomorphic part of the Maass-Poincare series of weight 12 and level 1 with a simple pole at $i\infty$. It follows from Theorem 1.3.2 that the Fourier coefficients of $\mathbb{L}(\Delta,\Delta;\tau)$ grow as $O(n^6)$. The following table illustrates the significant cancellation that occurs. Here, $c^+_\Delta(n)$ denotes nth Fourier coefficient of $Q^+(-1,12,1;\tau)$, which grows exponentially with n.

n	1	10	100	1000
$c^+_\Delta(n)/11!$	$-1842.89....$	$4.94...10^{10}$	$5.19...10^{42}$	$1.30...10^{155}$
$\hat{D}(\Delta,\Delta,n;11)$	33.384...	538192.6...	80949379532.2...	$5.4234...10^{15}$

Table 4.1: Numerics for Theorem 1.3.2

Chapter 5

Multiplicative Partition Functions

The purpose of this chapter is to describe the $maxp_k(n)$ functions, which were introduced in Chapter 1.6. The values of $maxp_k(n)$ are given explicitly in the third section of this chapter for all k and n. The key to determining these values is an effective estimate for $p_k(n)$, which we obtain in Section 5.1. The estimate that we show allows us to prove inequality Theorem 1.4.1, and the complete finite list of the pairs (a, b) for which the inequality fails, which are necessary for understanding the $maxp_k(n)$ values. We prove Theorem 1.4.1 in 5.2.

This was joint work with Christine Bessenrodt.

5.1 Explicit estimates for $p_k(n)$

Hagis [Hag71] proved an explicit formula for $p_k(n)$ that is analogous to Rademacher's formula for $p(n)$. Before describing his theorem, we introduce several necessary quantities, most importantly the Kloosterman-type sums $A(m, t, n, s, D)$ and the expressions $L(m, t, n, s, D)$.

Let D divide $t + 1$, let $J = J(t, D) := \frac{(t/D)-D}{24D}$, and let $a = a(t) := \frac{t}{24}$. Let I_1 be the order one modified Bessel function of the first kind, and let $L(m, t, n, s, D)$ be given by

$$L(m,t,n,s,D) := D^{\frac{3}{2}} m^{-1} \left(\frac{J-s}{n+a}\right)^{\frac{1}{2}} I_1 \left(4\pi D m^{-1} \left(\frac{(J-s)(n+a)}{(t+1)}\right)^{\frac{1}{2}}\right). \qquad (5.1)$$

Several definitions are needed to define the modified Kloosterman sums $A(t,m,n,s,D)$. First $g = g(m)$ is defined to be $\gcd(3,m)$ when m is odd, and $8\gcd(3,m)$ when m is even. We define $M = M(m,D) := \frac{m}{D}$. Additionally, we define $f = f(m) := \frac{24}{g}$, and define $r = r(m)$ to be any integer such that $fr \equiv 1 \pmod{gm}$. Further, G is defined to be analogous to g, in that $G = G(m,D) := \gcd(3,M)$ when M is odd and $G := 8\gcd(3,M)$ when M is even. Then we also let $B = B(m,D) := \frac{g}{G}$, and we define A to be any integer such that $AB \equiv 1 \pmod{GM}$. We also let $T = T(t,D) := \frac{t+1}{D}$, and choose $T' = T'(t,D)$ to satisfy $TT' \equiv 1 \pmod{GM}$. More importantly:

$$U = U(t,m,D) := 1 - AB(t+1), V = V(t,m,D) := ABT'D - 1.$$

Hagis defines special roots of unity, $w(h,t,m,D)$, which satisfy the following:

$$w(h,t,m,D) = C(h,t,m,D)\exp(2\pi i(rUh + rVh')/gm).$$

The $C(h,t,m,D)$ satisfy $|C(h,t,m,D)| = 1$, and are independent of h if m is odd, or if m is even and we restrict to $h \equiv d \pmod 8$ for some odd d. In what follows we will not explicitly use the definitions of $C(h,t,m,D)$.

Then we define $A(m,t,n,s,D)$ to be the Kloosterman sum with multiplier system given by

$$A(m,t,n,s,D) = \sum_{\substack{h \pmod m, \\ \gcd(h,m)=1}} w(h,t,m,D)\exp(-2\pi i(nh - DT'sh')/m), \qquad (5.2)$$

where $hh' \equiv 1 \pmod{gm}$.

Let $p'(s)$ be the number of partitions of s into an even number of distinct parts minus the number of partitions of s into an odd number of distinct parts; by Euler's pentagonal number theorem, $p'(s)$ is ± 1 if s is a pentagonal number, and 0 otherwise. Recall Glaisher's partition identity saying that the number $p_k(n)$ of k-regular partitions of n is equal to the number of partitions of n where no part has a multiplicity $\geq k$. Using the previous notation, Hagis proved the following for the numbers $p_k(n)$ in [Hag71, Theorem 3].

Theorem 5.1.1. *For all $k \geq 2$, the number of k-regular partitions of $n \in \mathbb{N}$ is given by*

$$p_k(n) = \frac{2\pi}{k} \sum_{\substack{D|k \\ D<k^{\frac{1}{2}}}} \sum_{\substack{m \\ \gcd(k,m)=D}}^{\infty} \sum_{s<J(k,D)} p'(s) A(m, k-1, n, s, D) L(m, k-1, n, s, D). \tag{5.3}$$

For $2 \leq k \leq 6$, in the summations above, we only have $s = 0$ and $D \leq 2$. Thus, the formulae needed for Theorem 1.4.1 consist of one or two of the inner sums in Theorem 5.1.1.

5.1.1 Estimates in the theorem of Hagis

In this section, we obtain an asymptotic for $p_k(n)$ with an explicitly bounded error term.

Let α_k be defined as follows:

$$\alpha_k := \begin{cases} 1.8 & \text{if } k = 2 \\ 9.84 & \text{if } k = 3 \\ 1.8 \cdot 3^{\frac{1}{2}} & \text{if } k = 4 \\ 14.37 & \text{if } k = 5 \\ 1.23 \cdot 5^{\frac{1}{2}} & \text{if } k = 6 \end{cases} \tag{5.4}$$

We also let $\alpha_6' := 19.68$.

Theorem 5.1.2. *For $n \in \mathbb{N}$, let $\mu = \mu(n,k) := \frac{\pi((k-1)^2+24n(k-1))^{\frac{1}{2}}}{6k^{\frac{1}{2}}}$.*

1. *For $2 \le k \le 5$ we have:*

$$p_k(n) = \frac{2\pi}{k}\left(\frac{k-1}{k-1+24n}\right)^{\frac{1}{2}} I_1(\mu) + E_k(n)$$

where

$$|E_k(n)| < \frac{\alpha_k \pi}{k}\left(\frac{k-1}{(k-1)+24n}\right)^{\frac{1}{2}} \frac{1}{\mu} e^{\mu}(1+5\mu^2 e^{-\mu}).$$

2. *For $k = 6$ we have:*

$$p_6(n) = \frac{\pi}{3}\left(\frac{5}{24n+5}\right)^{\frac{1}{2}} I_1(\mu) + E_6(n)$$

where

$$|E_6(n)| < \frac{\pi}{3}\left(\frac{5}{24n+5}\right)^{\frac{1}{2}} \frac{\alpha_6}{2}\frac{e^{\mu}}{\mu}(1+\delta(n)) + \frac{\pi}{3}\left(\frac{1}{24n+5}\right)^{\frac{1}{2}} I_1\left(\frac{\mu}{10^{\frac{1}{2}}}\right),$$

where $\delta(n) := 5\mu^2 e^{-\mu} + \frac{2^{\frac{4}{3}}\alpha_6'}{\alpha_6} e^{\mu\left(\frac{1}{\sqrt{10}}-1\right)}\left(1 + e^{-\frac{\mu}{\sqrt{10}}}\frac{\mu^2}{2}\right)$.

Remark 5.1.3. *Theorem 5.1.2 is analogous to [Leh38, (4.14)] in the case of $p(n)$.*

To prove this theorem, we need some preparations. The first is a bound on the divisor counting function $d(n)$.

Lemma 5.1.4. *Let $d(n)$ denote the number of positive divisors of a positive integer n.*

1. *For all n, $d(n) \le 3.57n^{\frac{1}{3}}$.*

2. *If n is odd, then $d(n) \le 1.8n^{\frac{1}{3}}$.*

3. *If* $\gcd(n,3)=1$*, then* $d(n) \leq 2.46n^{\frac{1}{3}}$*.*

4. *If* $\gcd(n,5)=1$*, then* $d(n) \leq 3.05n^{\frac{1}{3}}$*.*

5. *If* $\gcd(n,6)=1$*, then* $d(n) \leq 1.23n^{\frac{1}{3}}$*.*

Proof. Let $n = \prod_{i=1}^{M} p_i{}^{a_i}$, where each p_i is prime. Then $d(n) = \prod_{i=1}^{M}(1+a_i)$. We follow the classical method in [HW08] of bounding $\prod_{i=1}^{M} \frac{a_i+1}{p_i^{\frac{a_i}{3}}}$. For $p_i \geq 11$, we have $\frac{a_i+1}{p_i^{\frac{a_i}{3}}} \leq 1$ for $a_i \geq 1$. For the remaining p_i, the quantity $\frac{a_i+1}{p_i^{\frac{a_i}{3}}}$ is maximized when a_i is equal to $3, 2, 1$ and 1 for p_i equal to $2, 3, 5$ and 7, respectively. The lemma follows by maximizing $\prod_{i=1}^{M} \frac{a_i+1}{p_i^{\frac{a_i}{3}}}$ over n which respect each of the given divisibility constraints. □

The next lemma is a bound on $A(m, k-1, n, 0, D)$, which is related to the classical Kloosterman sums defined below; it is a slight modification of [Leh38, Theorem 12].

Definition 5.1.5. *Let* $a, b, m \in \mathbb{N}$*. The Kloosterman sum* $S(a,b,m)$ *is defined by*

$$S(a,b,m) := \sum_{\substack{1 \leq h \leq m-1 \\ \gcd(h,m)=1}} e^{2\pi i(ah+bh')/m},$$

where h' *is the multiplicative inverse of* h *modulo* m*.*

Weil proved the following bound (see [Iwa97, Theorem 4.5]):

Theorem 5.1.6. *Let* $a, b, m \in \mathbb{N}$*.*

$$|S(a,b,m)| \leq d(m)m^{\frac{1}{2}} \gcd(a,b,m)^{\frac{1}{2}}.$$

We will use this bound in the following lemma.

Lemma 5.1.7. 1. *For* $2 \leq k \leq 6$*, and for all* $n, m \geq 1$ *with* $\gcd(k,m)=1$*, we have*

$$|A(m, k-1, n, 0, 1)| < \alpha_k m^{\frac{5}{6}}.$$

2. For all $n, m \geq 1$ with $\gcd(6, m) = 2$, we have

$$|A(m, 5, n, 0, 2)| < \alpha_6' m^{\frac{5}{6}}.$$

Proof. We will follow Hagis' argument in [Hag71, Theorem 2]. Our strategy is to rewrite $A(m, k-1, n, 0, D)$ as a sum of ordinary Kloosterman sums and apply Theorem 5.1.6.

In order to bound the ordinary Kloosterman sums, we will need to be able to bound certain greatest common divisors. We use the notation introduced at the beginning of the section, and we begin by stating a series of bounds for $\gcd(Ur - gn, rV, gm)$ and $\gcd(Ur - gn, rV + \frac{wgm}{8}, gm)$ which depend on k and D. These are straightforward to verify from their definitions.

For $D = 1$, $2 \leq k \leq 6$ we have $\gcd(r, gm) = 1$ and $\gcd(k, gm) = 1$, thus $\gcd(rV, gm) = \gcd(kV, gm)$. Then since $kV = k(T' - 1) \equiv 1 - k \pmod{gm}$, we have

$$\gcd(rV, gm) = (1 - k, gm) \leq k - 1.$$

Let $k = 3, 5$, let $D = 1$, and let m be even. Note that $\gcd(r, g) = 1$ and $U = k - 1$, which implies $\gcd(Ur - gn, g) = \gcd(k - 1, g)$. Also for $1 \leq w \leq 8$, we have

$$\gcd(rV + \frac{wgm}{8}, m) = \gcd(V, m) = \gcd(1 - k, m).$$

Therefore $\gcd(Ur - gn, rV + \frac{wgm}{8}, gm)$ divides $(k-1)^2$, so it must be $1, 2, 4, 8$, or 16. However, the highest power of 2 that $Ur - gn$ can be divisible by is $k - 1$, because g is divisible by 8, and r is odd, and $Ur - gn = r(1 - k) - gm$. Thus we have:

$$\gcd(Ur - gn, Vr + \frac{wgm}{8}, gm) \leq k - 1.$$

For the last bound, we let $k = 6$ and $D = 2$. Then we have $g = 8$, $T = 3$, $M = \frac{m}{2}$, and $\gcd(6, m) = 2$. So $\gcd(rV + \frac{wgm}{8}, m) = \gcd(V, m) = \gcd(2ABT' - 1, m)$. Now we have $2AB \equiv 2 \pmod{m}$ and $6T' \equiv 2 \pmod{m}$, thus

$$\gcd(V, m) = \gcd(2T' - 1, m) = \gcd(3(2T' - 1), m) = 1.$$

Therefore we have $\gcd(rU - gn, rV + \frac{wgm}{8}, gm) \leq g = 8$.

To use these bounds, we rewrite $A(m, k-1, n, 0, D)$ as a sum over a reduced residue class modulo gm:

$$A(m, k{-}1, n, 0, D) = \frac{1}{g} \sum_{\substack{h \mod m \\ \gcd(h,m)=1}} C(h, k{-}1, m, D) \exp\left(2\pi i((Ur - gn)h + rVh')/gm)\right).$$

For odd m, $C(h, k-1, m, D)$ does not depend on h. Therefore we have

$$A(m, k-1, n, 0, 1) = C(1, k-1, m, 1)\frac{1}{g} \sum_{\substack{h \mod m \\ \gcd(h,m)=1}} \exp(2\pi i((rU - gn)h + rVh')/gm).$$

The sum on the right is an ordinary Kloosterman sum, so by Theorem 5.1.6 we have, for all odd m:

$$|A(m, k-1, n, 0, 1)| = |S(Ur - gn, rV, gm)| \leq \frac{1}{g} d(gm) \gcd(Ur - gn, rV, gm)^{\frac{1}{2}} (gm)^{\frac{1}{2}}.$$

Then by Lemma 5.1.4 and the bounds at the beginning of the proof, it follows that for all m such that $2 \nmid m$ and $\gcd(k, m) = 1$, we have:

$$|A(m, k-1, n, 0, 1)| \leq (k-1)^{\frac{1}{2}} \cdot 1.8 \cdot m^{\frac{5}{6}}.$$

This proves the lemma for $k = 2, 4$, and for $k = 3, 5$ in the case of m being odd.

Similarly, for $k=6$, by Lemma 5.1.4, we have:

$$|A(m,5,n,0,1)| \leq (k-1)^{\frac{1}{2}} \cdot 1.23 \cdot m^{\frac{5}{6}}.$$

For $k=6$, $D=1$, the proof is complete.

If m is even, we write

$$A(m,k-1,n,0,D)$$
$$= A_1(m,k-1,n,0,D) + A_3(m,k-1,n,0,D) + A_5(m,k-1,n,0,D) + A_7(m,k-1,n,0,D),$$

where

$$A_d(m,k-1,n,0,D) = \frac{1}{g} \sum_{\substack{h \mod gm, \\ h\equiv d \mod 8, \\ \gcd(h,m)=1}} C(h,k-1,m,D) \exp\left(2\pi i((rU-gn)h + rVh')/gm\right).$$

Over each d, the coefficient $C(h,k-1,m,D)$ does not depend on h, so

$$A_d(m,k-1,n,0,D) = C(d,k-1,m,D)\frac{1}{g} \sum_{\substack{h \pmod{gm}, \\ h\equiv d \pmod 8, \\ \gcd(h,m)=1}} \exp\left(2\pi i((rU-gn)h + rVh')/gm\right).$$

By the formula on page 266 of [Sal33], for $dd' \equiv 1 \pmod 8$, we have:

$$A_d(k-1,m,n,0,D) = \frac{1}{8g} C(d,k-1,m,D) \sum_{w=1}^{8} e^{2\pi i \frac{d'w}{8}} S(Ur-gn, Vr + \frac{wgm}{8}; gm).$$

By Theorem 5.1.6,

$$A_d(m,k-1,n,0,D) =$$
$$\frac{1}{8g} C(d,k-1,m,D) \sum_{w=1}^{8} e^{-\frac{2\pi i}{8} d'w} \gcd(Ur-gn, Vr + \frac{wgm}{8}, gm)^{\frac{1}{2}} d(gm)(gm)^{\frac{1}{2}}.$$

For $k = 3$, by the bounds at the beginning of the proof we have:

$$A_d(m, 2, n, 0, 1) \leq 8 \cdot \frac{1}{8g} \cdot 2^{\frac{1}{2}} \cdot 2.46(gm)^{\frac{1}{3}} \cdot (gm)^{\frac{1}{2}} \leq 2.46m^{\frac{5}{6}}.$$

Similarly for $k = 5$, if $3|m$, by our previous bounds we have:

$$A_d(m, 4, n, 0, 1) \leq 8 \cdot \frac{1}{8 \cdot 24} \cdot 4^{\frac{1}{2}} \cdot 3.05 \cdot (24m)^{\frac{1}{3}} \cdot (24m)^{\frac{1}{2}} \leq 3.592m^{\frac{5}{6}}.$$

If $3 \nmid m$, then we have:

$$|A_d(m, 4, n, 0, 1)| \leq 8 \cdot \frac{1}{8 \cdot 8} \cdot 4^{\frac{1}{2}} \cdot 2.46 \cdot (8m)^{\frac{1}{3}} \cdot (8m)^{\frac{1}{2}} \leq 3.48m^{\frac{5}{6}}.$$

We note that $|A(m, k-1, n, 0, D)| \leq 4|A_d(m, k-1, n, 0, D)|$. Comparing these bounds to the bounds in the odd m case, we conclude that for $k = 3, 5$, the desired bound holds whenever $\gcd(m, k) = 1$.

For $\gcd(6, m) = 2$, we have:

$$|A(m, 5, n, 0, 2)| \leq 4|A_d(m, 5, n, 0, 2)| \leq 4 \cdot (8 \cdot 8^{\frac{1}{2}} \cdot \frac{1}{8g} \cdot 2.46(gm)^{\frac{1}{3}} \cdot (gm)^{\frac{1}{2}}) \leq 19.6m^{\frac{5}{6}}.$$

This completes the proof. $\square$

Now we come to the **proof of Theorem 5.1.2**. For $2 \leq k \leq 5$, Theorem 5.1.1 says

$$p_k(n) = \frac{2\pi}{k} \sum_{\substack{m=1 \\ \gcd(k,m)=1}}^{\infty} m^{-1} \left(\frac{k-1}{(k-1) + 24n} \right)^{\frac{1}{2}} A(m, k-1, n, 0, 1) I_1 \left(\frac{\mu}{m} \right), \tag{5.5}$$

and for $k = 6$, Theorem 5.1.1 says

$$\begin{aligned} p_6(n) =& \frac{\pi}{3}\frac{5^{1/2}}{(5+24n)^{\frac{1}{2}}}\sum_{m=1}^{\infty}\frac{1}{m}A(m,5,n,0,1)I_1\left(\frac{\mu}{m}\right) \\ &+\frac{\pi}{3}\frac{1}{(5+24n)^{\frac{1}{2}}}\sum_{(3,a)=1}^{\infty}\frac{1}{a}A(2a,5,n,0,2)I_1\left(\frac{\mu}{10^{\frac{1}{2}}a}\right). \end{aligned} \tag{5.6}$$

Let $\alpha = \frac{1}{6}$. Our proof works by bounding the sums in (5.5) and (5.6). We have, for any $\nu \neq 0$,

$$\begin{aligned} \left|\sum_{m=N+1}^{\infty} m^{-1}A(m,k-1,n,0,1)I_1\left(\frac{\nu}{m}\right)\right| &\leq \sum_{m=N+1}^{\infty}\alpha_k m^{-\alpha}\sum_{j=0}^{\infty}\frac{(\frac{\nu}{2m})^{2j+1}}{j!(j+1)!} \\ &< \alpha_k\int_N^{\infty}x^{-\alpha}\sum_{j=0}^{\infty}\frac{(\frac{\nu}{2x})^{2j+1}}{j!(j+1)!}dx. \end{aligned}$$

We substitute $t = \frac{\nu}{2x}$.

$$\begin{aligned} \left|\sum_{m=N+1}^{\infty} m^{-1}A(m,k-1,n,0,1)I_1\left(\frac{\nu}{m}\right)\right| &\leq \alpha_k\int_0^{\frac{\nu}{2N}}(\frac{\nu}{2t})^{-\alpha}\sum_{j=0}^{\infty}\frac{t^{2j+1}}{j!(j+1)!}\frac{\nu}{2t^2}dt \\ &= \alpha_k(\frac{\nu}{2})^{1-\alpha}\int_0^{\frac{\nu}{2N}}\sum_{j=0}^{\infty}\frac{(t^{2j-1+\alpha})}{j!(j+1)!}dt \\ &\leq \alpha_k\ (\frac{\nu}{2})^{1-\alpha}\sum_{j=0}^{\infty}\frac{(\frac{\nu}{2N})^{2j+\alpha}}{j!(j+1)!(2j+\alpha)} \\ &\leq \alpha_k(\frac{\nu}{2})^{1-\alpha}\left(\frac{(\frac{\nu}{N})^{\alpha}}{2\alpha}+\sum_{j=2}^{\infty}\frac{((\frac{\nu}{N})^{2j-2+\alpha})}{(2j)!}\right)2^{1-\alpha} \\ &\leq \alpha_k N^{2+\alpha}\frac{1}{\nu}\left(\cosh(\nu/N)-1+\frac{5}{2}\left(\frac{\nu}{N}\right)^2\right). \end{aligned}$$

To bound $\sum_{a=N+1}^{\infty}(2a)^{-1}A(2a,5,n,0,2)I(\frac{\nu}{2a})$, we replace α_6 with α_6' in the previous argument. To complete the proof, we let $N = 1$, and apply the above inequality to the sums in Theorem 5.1.1, where $\nu = \mu$ for $2 \leq k \leq 5$, and for $k = 6$, ν is set to be μ and $\frac{\mu}{\sqrt{10}}$ in the first and second sum, respectively. $\square$

5.2 Proof of Theorem 1.4.1

This proof is analogous to the proof of [BO16, Theorem 2.1].

By well known properties of Bessel functions, such as the bounds in (9.8.4) of [AS72], for $x \geq 37.5$ the modified Bessel function $I_1(x)$ is bounded by

$$N \leq x^{\frac{1}{2}} e^{-x} I_1(x) \leq M$$

where $N = 0.394$, $M = 0.399$.

First, let $2 \leq k \leq 5$, and let $\beta := \frac{\alpha_k}{2}$. Then by Theorem 5.1.2, for $n \geq 450$ we have:

$$\frac{2\pi}{k}\left(\frac{k-1}{k-1+24n}\right)^{\frac{1}{2}}\left(N - \frac{\beta}{\sqrt{\mu}}\left(1+5\mu^2 e^{-\mu}\right)\right)\frac{e^{\mu}}{\sqrt{\mu}} < p_k(n)$$
$$< \frac{2\pi}{k}\left(\frac{k-1}{k-1+24n}\right)^{\frac{1}{2}}\frac{e^{\mu}}{\sqrt{\mu}}\left(M + \frac{\beta}{\sqrt{\mu}}\left(1+5\mu^2 e^{-\mu}\right)\right).$$

We assume $a \leq b$ and write $b = \lambda a$ for some $\lambda \geq 1$. Then it is sufficient to show

$$e^{\mu(a)+\mu(\lambda a)-\mu(\lambda a+a)} > S_{a,k}(\lambda)(k-1+24a)^{\frac{3}{4}},$$

where

$$S_{a,k}(\lambda) := C_k \frac{\left(M + \frac{\beta}{\sqrt{\mu(\lambda a+a)}}\left(1+5\mu(\lambda a+a)^2 e^{-\mu(\lambda a+a)}\right)\right)}{\left(N - \frac{\beta}{\sqrt{\mu(\lambda a)}}\left(1+5\mu(\lambda a)^2 e^{-\mu(\lambda a)}\right)\right)\left(N - \frac{\beta}{\sqrt{\mu(a)}}\left(1+5\mu(a)^2 e^{-\mu(a)}\right)\right)},$$

for $C_k := \frac{k^{\frac{3}{4}}}{2(\pi(k-1))^{\frac{1}{2}}}$. For a fixed a, the left-hand side of the inequality is increasing for all $\lambda \geq 1$, and the right-hand side is decreasing. Thus, for any given a, to prove Theorem 1.4.1 for $b \geq a$, it suffices to verify the inequality for $\lambda = 1$. Taking the natural logarithm of each side, it is straightforward to verify that the inequality holds for $a \geq 1000$ for $k = 2, 4$, and holds for $a \geq 5 \cdot 10^4$ for $k = 3, 5$. Then for each of the remaining a, we wish to find $\lambda_{a,k}$ such that for $\lambda \geq \lambda_{a,k}$:

$$p_k(a)\frac{2\pi}{k}\left(\frac{k-1}{k-1+24\lambda a}\right)^{\frac{1}{2}}\left(N - \frac{\beta}{\sqrt{\mu(\lambda a)}}\left(1+5\mu(\lambda a)^2 e^{-\mu(\lambda a)}\right)\right)\frac{e^{\mu(\lambda a)}}{\sqrt{\mu(\lambda a)}} >$$
$$\frac{2\pi}{k}\left(\frac{k-1}{k-1+24(\lambda a+a)}\right)^{\frac{1}{2}}\frac{e^{\mu(\lambda a+a)}}{\sqrt{\mu(\lambda a+a)}}\left(M + \frac{\beta}{\sqrt{\mu(\lambda a+a)}}\left(1+5\mu(\lambda a+a)^2 e^{-\mu(\lambda a+a)}\right)\right).$$

For $a \geq 20$, $k = 2, 4$, $\lambda_{a,k} = \frac{1000}{a}$ suffices. For $a \leq 20$, $k = 3, 5$, $\lambda_{a,k} = \frac{50000}{a}$ suffices. For smaller a, the needed $a\lambda_{a,k}$ values can be as large as $4 \cdot 10^5$, except when $k = 5$ and $a = 2$, where the larger bound in Theorem 5.1.7 for $k = 5$ causes the needed $\lambda_{a,k}$ values to be much larger. All other cases are reduced to checking a large but finite number of pairs (a, b), where $a \leq 5 \cdot 10^4$ and $b \leq \lambda_{a,k} a$. We carried out these calculations using Sage mathematical software [S$^+$14]. To ease our calculation, we proved the inequality $p_5(2) \cdot p_5(b) > p_5(b+2)$ for $b \geq 75$ with a combinatorial argument (see the end of the section), and used Sage [S$^+$14] to check the remaining pairs.

Now we handle the $k = 6$ case. This case is very similar to the cases for $2 \leq k \leq 5$, but because of the second summation in (5.6), we have additional, non-dominant terms in our expressions. Using Theorem 5.1.2 and factoring out the leading term, we obtain

$$\frac{\pi}{3}\frac{\sqrt{5}}{\sqrt{24n+5}}\frac{e^{\mu}}{\sqrt{\mu_6}}\left(N\left(1-\eta(n)\right) - \frac{\beta}{\sqrt{\mu}}\left(1+\delta(n)\right)\right) < p_6(n)$$
$$< \frac{\pi}{3}\frac{\sqrt{5}}{\sqrt{24n+5}}\frac{e^{\mu}}{\sqrt{\mu_6}}\left(M\left(1+\eta(n)\right) + \frac{\beta}{\sqrt{\mu}}\left(1+\delta(n)\right)\right),$$

where $\eta(n) := \left(\frac{2}{5}\right)^{\frac{1}{4}} e^{\mu\left(10^{-\frac{1}{2}}-1\right)}$. The desired inequality is implied by

$$e^{\mu(a)+\mu(\lambda a)-\mu(\lambda a+a)} > S_{a,k}(\lambda)(k-1+24a)^{\frac{3}{4}},$$

where

$$S_a(\lambda) = C_6 \frac{\left(M(1+\eta(\lambda a + a)) + \frac{\beta}{\sqrt{\mu((\lambda+1)a)}}(1+\delta(\lambda a + a))\right)}{\left(N(1-\eta(a)) - \frac{\beta}{\sqrt{\mu(\lambda a)}}(1+\delta(\lambda a))\right)\left(N(1-\eta(a)) - \frac{\beta}{2\sqrt{\mu_6(a)}}(1+\delta(a))\right)},$$

and $C_6 = \frac{3}{\pi\sqrt{5}}(\frac{6^{\frac{3}{2}}}{\sqrt{5}\pi})^{\frac{1}{2}}$. As before, it suffices to verify that this is true for $\lambda = 1$, which is straightforward for $a \geq 3500$. Then for each $a \leq 3500$, we wish to find $\lambda_{a,6}$ such that for all $\lambda \geq \lambda_{a,6}$,

$$p_6(a)\frac{\pi}{3}\frac{\sqrt{5}}{\sqrt{24(\lambda a)+5}}\frac{e^{\mu(\lambda a)}}{\sqrt{\mu(\lambda a)}}\left(N(1-\eta(\lambda a)) - \frac{\beta}{\sqrt{\mu(\lambda a)}}(1+\delta(\lambda a))\right) >$$
$$\frac{\pi}{3}\frac{\sqrt{5}}{\sqrt{24(\lambda a + a)+5}}\frac{e^{\mu(\lambda a + a)}}{\sqrt{\mu((\lambda+1)a)}}\left(M(1+\eta(\lambda a + 1)) + \frac{\beta}{\sqrt{\mu(\lambda a + a)}}(1+\delta(\lambda a + a))\right).$$

It is straightforward to verify that the inequality holds for $\lambda \geq \frac{3500}{a}$ for all $a \geq 4$. For $a = 2, 3, 4$, the inequality holds for $\lambda \geq \frac{50000}{a}$. This reduces the $k = 6$ case to a finite number of pairs (a, b) to check, which we computed with Sage [S+14].

Finally, we prove that for $b \geq 75$, we have $p_5(b+2) < 2\,p_5(b)$. To do this, we separate the 5-regular partitions of $b+2$ into two disjoint sets. Let S_1 be the set of 5-regular partitions of $b+2$ which contain 1 as a part with multiplicity at least two. Let S_2 contain all the other 5-regular partitions of $b+2$. Let S be the set of 5-regular partitions of b. We map S_1 and S_2 each injectively into S. To map S_1 injectively into S, for each partition in S_1, simply remove two parts 1.

Next, we define an injective map from S_2 into S. Let $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_\ell)$ be a partition in S_2. If $\gamma_\ell \geq 2$ and $\gamma_1 \geq 7$, then γ is mapped to $(\gamma_2, \ldots, \gamma_\ell, 1^{\gamma_1 - 2})$ (here, we use exponential notation for multiplicities). If $\gamma_\ell \geq 2$ and $\gamma_1 < 7$, then if 2 has multiplicity at least 5 in γ, replace five parts 2 with eight parts 1. Otherwise, if γ has five parts 3, we replace them with thirteen parts 1. If γ has five parts 4, then we replace them with eighteen parts 1. Otherwise, γ must have at least five parts 6, which we replace with 28 parts 1. Finally, assume $\gamma_\ell = 1$. If $\gamma_{\ell-1} \equiv 1 \pmod 5$, then we map γ to $(\gamma_1, \ldots, \gamma_{\ell-2}, \gamma_{\ell-1} - 4, 1^3)$. Otherwise, γ is mapped to $(\gamma_1, \ldots, \gamma_{\ell-2}, \gamma_{\ell-1} - 1)$. Note that the mapping from S_2 to S is not onto by considering any 5-regular partition of b which contains exactly two ones. Thus we obtain the inequality $p_5(b+2) < 2p_5(b)$ for $b \geq 75$.

This completes the proof of the inequality stated in Theorem 1.4.1.

The exceptional pairs given in the table are then easily obtained by direct computations. $\square$

5.3 The maximum property

We first recall [BO16, Theorem 1.1].

Theorem 5.3.1. *Let $n \in \mathbb{N}$. For $n \geq 4$ and $n \neq 7$, the maximal value* $\operatorname{maxp}(n)$ *of the partition function on $P(n)$ is attained exactly at the partitions (in exponential notation)*

$$\begin{array}{ll} (4^{\frac{n}{4}}) & \textit{when } n \equiv 0 \pmod 4 \\ (5, 4^{\frac{n-5}{4}}) & \textit{when } n \equiv 1 \pmod 4 \\ (6, 4^{\frac{n-6}{4}}) & \textit{when } n \equiv 2 \pmod 4 \\ (6, 5, 4^{\frac{n-11}{4}}) & \textit{when } n \equiv 3 \pmod 4 \end{array}$$

For $n = 7$, the maximal value is $\operatorname{maxp}(7) = 15$, *attained at the two partitions* (7) *and* $(4, 3)$.

In particular, if $n \geq 8$, then

$$\operatorname{maxp}(n) = \begin{cases} 5^{\frac{n}{4}} & \text{if } n \equiv 0 \pmod 4, \\ 7 \cdot 5^{\frac{n-5}{4}} & \text{if } n \equiv 1 \pmod 4, \\ 11 \cdot 5^{\frac{n-6}{4}} & \text{if } n \equiv 2 \pmod 4, \\ 11 \cdot 7 \cdot 5^{\frac{n-11}{4}} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Since the partitions where the maximum of $p(n)$ is attained on $P(n)$ are k-regular for any $k > 6$, in the following it suffices to consider the cases $k \in \{2, 3, 4, 5, 6\}$.

Theorem 5.3.2. *Let $k \in \mathbb{N}$, $k > 1$. Let $n \in \mathbb{N}$.*

(i) $k = 2$. For $n \geq 9$ and $n \neq 11$, the maximal value $\mathrm{maxp}_2(n)$ of $p_2(n)$ on $P_2(n)$ is attained exactly at the partitions

$$\begin{array}{ll} (9^a, 3^b) & \text{when } n \equiv 0 \pmod 3 \\ (9^a, 7, 3^b) & \text{when } n \equiv 1 \pmod 3 \\ (9^a, 7, 7, 3^b) & \text{when } n \equiv 2 \pmod 3 \end{array}$$

where $a, b \in \mathbb{N}_0$ may be chosen arbitrarily as long as we have partitions of n. In particular, we have

$$\mathrm{maxp}_2(n) = \begin{cases} 2^{\frac{n}{3}} & \text{when } n \equiv 0 \pmod 3 \\ 5 \cdot 2^{\frac{n-7}{3}} & \text{when } n \equiv 1 \pmod 3 \\ 5^2 \cdot 2^{\frac{n-14}{3}} & \text{when } n \equiv 2 \pmod 3 \end{cases}$$

(ii) $k = 3$. For $n \geq 2$ and $n \neq 3$, the maximal value $\mathrm{maxp}_3(n)$ of $p_3(n)$ on $P_3(n)$ is attained exactly at the partitions

$$\begin{array}{ll} (4^a, 2^b) & \text{when } n \equiv 0 \pmod 2 \\ (5, 4^a, 2^b) & \text{when } n \equiv 1 \pmod 2 \end{array}$$

where $a, b \in \mathbb{N}_0$ may be chosen arbitrarily as long as we have partitions of n. In particular, we have

$$\mathrm{maxp}_3(n) = \begin{cases} 2^{\frac{n}{2}} & \text{when } n \equiv 0 \pmod 2 \\ 5 \cdot 2^{\frac{n-5}{2}} & \text{when } n \equiv 1 \pmod 2 \end{cases}$$

(iii) $k = 4$. For $n \geq 2$, the maximal value $\mathrm{maxp}_4(n)$ of $p_4(n)$ on $P_4(n)$ is attained

exactly at the partitions

$$\begin{array}{ll} (6^a, 3^b) & \textit{when } n \equiv 0 \pmod 3 \\ (6^a, 3^b, 2, 2), (7, 6^a, 3^b), (6^a, 5, 3^b, 2), (6^a, 5, 5, 3^b) & \textit{when } n \equiv 1 \pmod 3 \\ (6^a, 3^b, 2), (6^a, 5, 3^b) & \textit{when } n \equiv 2 \pmod 3 \end{array}$$

where $a, b \in \mathbb{N}_0$ *may be chosen arbitrarily as long as we have partitions of* n, *and with the understanding that partitions with given parts* $2, 5, 7$ *of positive multiplicity do not occur when* n *is too small.*

In particular, we have

$$\operatorname{maxp}_4(n) = \begin{cases} 3^{\frac{n}{3}} & \textit{when } n \equiv 0 \pmod 3 \\ 4 \cdot 3^{\frac{n-4}{3}} & \textit{when } n \equiv 1 \pmod 3 \\ 2 \cdot 3^{\frac{n-2}{3}} & \textit{when } n \equiv 2 \pmod 3 \end{cases}$$

(iv) $k = 5$. *For* $n \geq 2$, *the maximal value* $\operatorname{maxp}_5(n)$ *of* $p_5(n)$ *on* $P_5(n)$ *is attained exactly at the partitions*

$$\begin{array}{ll} (4^{\frac{n}{4}}) & \textit{when } n \equiv 0 \pmod 4 \\ (4^{\frac{n-5}{4}}, 3, 2), (6, 4^{\frac{n-9}{4}}, 3) & \textit{when } n \equiv 1 \pmod 4 \\ (4^{\frac{n-2}{4}}, 2), (6, 4^{\frac{n-6}{4}}) & \textit{when } n \equiv 2 \pmod 4 \\ (4^{\frac{n-3}{4}}, 3) & \textit{when } n \equiv 3 \pmod 4 \end{array}$$

with the understanding that partitions with given parts $2, 3, 6$ *of positive multiplicity do not occur when* n *is too small.*

In particular, we have

$$\operatorname{maxp}_5(n) = \begin{cases} 5^{\frac{n}{4}} & \textit{when } n \equiv 0 \pmod 4 \\ 6 \cdot 5^{\frac{n-5}{4}} & \textit{when } n \equiv 1 \pmod 4 \\ 2 \cdot 5^{\frac{n-2}{4}} & \textit{when } n \equiv 2 \pmod 4 \\ 3 \cdot 5^{\frac{n-3}{4}} & \textit{when } n \equiv 3 \pmod 4 \end{cases}$$

(v) $k = 6$*. For* $n \geq 2$*, the maximal value* $\operatorname{maxp}_6(n)$ *of* $p_6(n)$ *on* $P_6(n)$ *is attained exactly at the partitions*

$$\begin{array}{ll} (4^{\frac{n}{4}}) & \textit{when } n \equiv 0 \pmod 4 \\ (5, 4^{\frac{n-5}{4}}) & \textit{when } n \equiv 1 \pmod 4 \\ (4^{\frac{n-2}{4}}, 2) & \textit{when } n \equiv 2 \pmod 4 \\ (4^{\frac{n-3}{4}}, 3) & \textit{when } n \equiv 3 \pmod 4 \end{array}$$

In particular, we have

$$\operatorname{maxp}_6(n) = \begin{cases} 5^{\frac{n}{4}} & \textit{when } n \equiv 0 \pmod 4 \\ 7 \cdot 5^{\frac{n-5}{4}} & \textit{when } n \equiv 1 \pmod 4 \\ 2 \cdot 5^{\frac{n-2}{4}} & \textit{when } n \equiv 2 \pmod 4 \\ 3 \cdot 5^{\frac{n-3}{4}} & \textit{when } n \equiv 3 \pmod 4 \end{cases}$$

Proof. (i) We will need the partitions where $\operatorname{maxp}_2(n)$ is attained for $n \leq 22$; these are given in Table 5.1 (computed by Maple [Map]). We see that the assertion holds as stated up to $n = 22$.

Now take $n > 22$. Let $\mu \in P_2(n)$ be such that $p_2(\mu)$ is maximal; let m_j be the multiplicity of a part j in μ. Suppose μ has a part $j = 2h + 1 \geq 19$; let $\{h, h+1\} = \{2l, h'\}$. Then by Theorem 1.4.1 and Table 5.1, replacing j by the parts

Table 5.1: Maximum value partitions μ for $k = 2$

n	$p_2(n)$	$\mathrm{maxp}_2(n)$	μ
1	1	1	(1)
2	1	1	(1,1)
3	2	2	(3)
4	2	2	(3,1)
5	3	3	(5)
6	4	4	(3^2)
7	5	5	(7)
8	6	6	(5,3)
9	8	8	$(9), (3^3)$
10	10	10	(7,3)
11	12	12	$(11), (5, 3^2)$
12	15	16	$(9, 3), (3^4)$
13	18	20	$(7, 3^2)$
14	22	25	(7^2)
15	27	32	$(9, 3^2), (3^5)$
16	32	40	$(9, 7), (7, 3^3)$
17	38	50	$(7^2, 3)$
18	46	64	$(9^2), (9, 3^3), (3^6)$
19	54	80	$(9, 7, 3), (7, 3^4)$
20	64	100	$(7^2, 3^2)$
21	76	128	$(9^2, 3), (9, 3^4), (3^7)$
22	89	160	$(9, 7, 3^2), (7, 3^5)$

$h', 2l-3, 3$ in μ would produce a partition $\nu \in P_2(n)$ such that $p_2(\nu) > p_2(\mu)$. Thus μ has no parts $j \geq 19$. By Table 5.1, a part $j \in \{13, 15, 17\}$ could be replaced in μ by a partition in $P_2(j)$ giving a partition $\nu \in P_2(n)$ of larger p_2-value. Thus μ only has odd parts $j \leq 11$.

Any two parts (11^2), $(11, 9)$, $(11, 7)$, $(11, 5)$, $(11, 3)$, $(11, 1)$ can be replaced by a 2-regular partition to obtain a higher p_2-value, see Table 5.1; thus $m_{11} = 0$. Also (7^3), $(7, 5)$, $(7, 1)$ can be replaced to obtain a higher p_2-value. Thus $m_7 \leq 2$, and the part 7 can only occur when μ is of the form $(9^a, 7, 3^b)$ or $(9^a, 7^2, 3^b)$; in the first case $n \equiv 1 \mod 3$, in the second case we have $n \equiv 2 \mod 3$. Also (5^2) can be replaced by $(7, 3)$ to obtain a higher p_2-value, so $m_5 \leq 1$; then replacing $(9, 5)$ or $(5, 3^3)$ by (7^2), and $(5, 1)$ by (3^2) shows that μ has no part 5. Hence if μ has no part 7, then μ is of the form $(9^a, 3^b)$, and $n \equiv 0 \mod 3$. As $p_2((9)) = p_2((3^3))$, the part 9 and the parts $3, 3, 3$ can always be used interchangeably. Now for $n \geq 19$ and any congruence $n \equiv c \mod 3$, $c \in \{0, 1, 2\}$, we have found just one type of 2-regular partition maximizing the p_2-value, namely $(9^a, 7^c, 3^b)$, with $a, b \in \mathbb{N}_0$ such that $(3a+b)\cdot 3 + c \cdot 7 = n$, where $p_2((9^a, 7^c, 3^b)) = 2^{3a+b}5^c = \mathrm{maxp}_2(n)$. This proves the claim for $k = 2$.

(ii) By Table 5.2 the claim holds for $n \leq 16$. So we assume now that $n > 16$.

Table 5.2: Maximum value partitions μ for $k = 3$

n	$p_3(n)$	$\mathrm{maxp}_3(n)$	μ
1	1	1	(1)
2	2	2	(2)
3	2	2	(2,1)
4	4	4	$(4), (2^2)$
5	5	5	(5)
6	7	8	$(4, 2), (2^3)$
7	9	10	(5,2)
8	13	16	$(4^2), (4, 2^2), (2^4)$
9	16	20	$(5, 4), (5, 2^2)$
10	22	32	$(4^2, 2), (4, 2^3), (2^5)$
11	27	40	$(5, 4, 2), (5, 2^3)$
12	36	64	$(4^3), (4^2, 2^3), (4, 2^4), (2^6)$
13	44	80	$(5, 4^2), (5, 4, 2^2), (5, 2^4)$
14	57	128	$(4^3, 2), (4^2, 2^3), (4, 2^5), (2^7)$
15	70	160	$(5, 4^2, 2), (5, 4, 2^3), (5, 2^5)$
16	89	256	$(4^4), (4^3, 2^2), (4^2, 2^4), (4, 2^6), (2^8)$

Let $\mu \in P_3(n)$ be such that $p_3(\mu)$ is maximal. Suppose μ has a part $j \geq 17$. Replace j by $\nu_j = (j-2, 2)$ if $j \equiv 1 \mod 3$, and by $\nu_j = (j-4, 4)$ if $j \equiv 2 \mod 3$. By Theorem 1.4.1 we have $p_3(j) < p_3(\nu_j)$. Thus μ only has parts ≤ 16. By Table 5.2, any of these can be replaced by a partition of the form $(5^a, 4^b, 2^c, 1^d)$ to increase the p_3-value, and we note that the parts 4 and $2, 2$ can be used interchangeably. Hence only parts $1, 2, 4, 5$ can appear in μ. By Table 5.2, the following replacements would increase the p_3-value: $(5^2) \to (2^5)$, $(5, 1) \to (2^3)$, $(4, 1), (2^2, 1) \to (5)$, $(1^2) \to (2)$. This implies that μ can only have one of the forms $(4^a, 2^b)$ or $(5, 4^a, 2^b)$, where in the first case $n \equiv 0 \mod 2$, in the second case $n \equiv 1 \mod 2$. Hence $\mathrm{maxp}_3(n) = 2^{\frac{n}{2}}$ when n is even, and $\mathrm{maxp}_3(n) = 5 \cdot 2^{\frac{n-5}{2}}$ when n is odd.

(iii) By Table 5.3 the claim holds for $n \leq 15$, so now take $n \geq 16$. Let $\mu \in P_4(n)$ be such that $p_4(\mu)$ is maximal. Note that by Table 5.3, we may always exchange a part 6 against the parts $3, 3$ without changing the p_4-value. Suppose μ has a part $j \geq 9$. Replace j by $\nu_j = (j-2, 2)$, when $j \not\equiv 2 \mod 4$, or by $\nu_j = (j-3, 3)$ when $j \equiv 2 \mod 4$. By Theorem 1.4.1, $p_4(j) < p_4(\nu_j)$; hence μ only has parts ≤ 7. Replacing (7^2) by $(6^2, 2)$, $(7, 5)$ by (6^2), $(7, 2)$ by $(6, 3)$, $(7, 1)$ by $(6, 2)$ shows that μ can have a part 7 only when it is of the form $(7, 6^a, 3^b)$, and then $n \equiv 1 \mod 3$. By Table 5.3, in these partitions we may exchange 7 with $(5, 2)$ or $(3, 2^2)$, and $(7, 3)$ with (5^2) without changing the p_4-value.

Now assume that μ has no part 7. Replacing (5^3) by $(6^2, 3)$, $(5^2, 2)$ by (6^2), $(5, 1)$ by 6, shows that μ can have a part 5 only when $n \equiv 1 \mod 3$ and it is of the form $(6^a, 5, 3^b, 2)$ or $(6^a, 5^2, 3^b)$ already discussed above, or $n \equiv 2 \mod 3$ and it is of the form $(6^a, 5, 3^b)$. Note that 5 can be exchanged with $(3, 2)$ without changing the p_4-value.

Finally, when μ has no parts 5 and 7, the replacements of $(6, 1)$ by 7, (2^3) by 6, $(3, 1)$ by (2^2), $(2, 1)$ by 3, (1^2) by 2 show that μ can have no part 1 and $m_2 \leq 2$. Then μ has one of the forms $(6^a, 3^b)$, $(6^a, 3^b, 2)$ or $(6^a, 3^b, 2^2)$, when n is congruent to $0, 2, 1$ mod 3, respectively.

Together with the remarks above, we then have $\mathrm{maxp}_4(n) = 3^{\frac{n}{3}}$ when $n \equiv 0 \mod 3$, $\mathrm{maxp}_4(n) = 4 \cdot 3^{\frac{n-4}{3}}$ when $n \equiv 1 \mod 3$, and $\mathrm{maxp}_4(n) = 2 \cdot 3^{\frac{n-2}{3}}$ when $n \equiv 2 \mod 3$, attained at the partitions as stated in the claim for $k = 4$.

(iv) Table 5.4 shows that the assertion is true for $n \leq 12$. Take $n \geq 13$, and let $\mu \in P_5(n)$ be such that $p_5(\mu)$ is maximal. Note that by Table 5.4 we may always exchange a part 6 against the parts $4, 2$ without changing the p_5-value. Suppose μ has a part $j \geq 7$. Replace j by $\nu_j = (j-3, 3)$, when $j \not\equiv 3 \mod 5$, or by $\nu_j = (j-4, 4)$

Table 5.3: Maximum value partitions μ for $k = 4$

n	$p_4(n)$	$\mathrm{maxp}_4(n)$	μ
1	1	1	(1)
2	2	2	(2)
3	3	3	(3)
4	4	4	(2,2)
5	6	6	(5), (3,2)
6	9	9	$(6), (3^2)$
7	12	12	$(7), (5,2), (3,2^2)$
8	16	18	$(6,2), (5,3), (3^2,2)$
9	22	27	$(6,3), (3^3)$
10	29	36	$(7,3), (6,2^2), (5^2), (5,3,2)(3^2,2^2)$
11	38	54	$(6,5), (6,3,2), (5,3^2), (3^3,2)$
12	50	81	$(6^2), (6,3^2), (3^4)$
13	64	108	$(7,6), (7,3^2), (6,5,2), (6,3,2^2), (5^2,3), (5,3^2,2), (3^3,2^2)$
14	82	162	$(6^2,2), (5^2,3), (6,3^2,2), (5,3^3), (3^4,2)$
15	105	243	$(6^2,3), (6,3^3), (3^5)$

when $j \equiv 3 \mod 5$. By Table 5.4 and Theorem 1.4.1 $p_5(j) < p_5(\nu_j)$; hence μ only has parts ≤ 6.

Replacing (6^2) by (4^3), $(6,2)$ by (4^2), $(6,1)$ by $(4,3)$, (3^2) by 6, $(3,1)$ or (2^2) by 4, $(2,1)$ by 3 and (1^2) by 2 increases the p_5-value. Hence μ can only have the forms stated in (iv), and the assertion about the maxp_5-value also follows.

(v) Table 5.5 shows that the assertion is true for $n \leq 10$. Let $n \geq 11$, and let $\mu \in P_6(n)$ be such that $p_6(\mu)$ is maximal. Suppose μ has a part $j \geq 7$. Replace j by $\nu_j = (j-3,3)$, when $j \equiv 4 \mod 6$, or by $\nu_j = (j-4,4)$ when $j \not\equiv 4 \mod 6$. By Table 5.5 and Theorem 1.4.1 $p_6(j) < p_6(\nu_j)$; hence μ only has parts ≤ 5. Replacing (5^2) by $(4^2,2)$, $(5,1)$ by $(4,2)$, $(5,2)$ by $(4,3)$, $(5,3)$ by (4^2), (3^2) by $(4,2)$, $(3,2)$ by 5, $(3,1)$ or (2^2) by 4, $(2,1)$ by 3 and (1^2) by 2 increases the p_6-value. Hence μ can only have the forms stated in (v), and the assertion about the maxp_6-value also follows in this final case.

□

Table 5.4: Maximum value partitions μ for $k = 5$

n	$p_5(n)$	$\mathrm{maxp}_5(n)$	μ
1	1	1	(1)
2	2	2	(2)
3	3	3	(3)
4	5	5	(4)
5	6	6	(3,2)
6	10	10	(6), (4,2)
7	13	15	(4,3)
8	19	25	(4^2)
9	25	30	(6,3), (4,3,2)
10	34	50	$(6,4), (4^2,2)$
11	44	75	$(4^2,3)$
12	60	125	(4^3)

Table 5.5: Maximum value partitions μ for $k = 6$

n	$p_6(n)$	$\mathrm{maxp}_6(n)$	μ
1	1	1	(1)
2	2	2	(2)
3	3	3	(3)
4	5	5	(4)
5	7	7	(5)
6	10	10	(4,2)
7	14	15	(4,3)
8	20	25	(4^2)
9	27	35	(5,4)
10	37	50	$(4^2,2)$

Chapter 6

Parts of partitions in residue classes

The purpose of this chapter is to prove Theorems 1.5.1 and 1.5.4.

This is joint work with Michael Mertens.

6.1 Generating function

We prove a formula for the generating function for $\widehat{T}_{r,N}(n)$.

Lemma 6.1.1. *$\widehat{T}_{r,N}$ has the following generating function,*

$$\sum_{n=1}^{\infty} \widehat{T}_{r,N}(n) q^n = \left(\prod_{n \geq 1} \frac{1}{(1-q^n)} \right) \left(\sum_{n=1}^{\infty} \left(\sum_{\substack{d|n \\ d \equiv r \pmod{N}}} q^n \right) \right).$$

Proof. Note that

$$\frac{q^m}{(1-q^m)^2} = \sum_{k=1}^{\infty} k q^{km}.$$

Then, modifying the proof of Euler's formula for the generating function of $p(n)$, we have that

$$\sum_{n=0}^{\infty} a(n)q^n = \frac{q^m}{(1-q^m)^2} \cdot \prod_{\substack{n\geq 1\\ n\neq m}} \frac{1}{1-q^n},$$

where $a(n)$ equals the number of times m appears as a part in a partition of n.

Thus, summing over $m \equiv r \pmod{N}$, we have

$$\begin{aligned}
\sum_{n=1}^{\infty} \widehat{T}_{r,N}(n)q^n &= \sum_{\substack{m\geq 1\\ m\equiv r \pmod{N}}} \frac{q^m}{(1-q^m)^2} \cdot \prod_{\substack{n\geq 1\\ n\neq m}} \frac{1}{1-q^n} \\
&= \left(\prod_{n\geq 1} \frac{1}{1-q^n}\right) \sum_{\substack{m\geq 1\\ m\equiv r \pmod{N}}} \left(\sum_{k=1}^{\infty} q^{km}\right) \\
&= \left(\prod_{n\geq 1} \frac{1}{(1-q^n)}\right) \left(\sum_{n=1}^{\infty} \left(\sum_{\substack{d\mid n\\ d\equiv r \mod N}} q^n\right)\right).
\end{aligned}$$

This proves the lemma. $\square$

6.2 Odd Dirichlet Characters

In the next section, we relate the generating function for $\widehat{T}_{r,N}(n) - \widehat{T}_{N-r,N}(n)$ to modular forms. We begin by showing that the odd Dirichlet characters satisfy the same orthogonality relations as the usual Dirichlet characters.

Lemma 6.2.1. *Let G be a finite abelian group containing an element $u \in G \setminus \{1\}$ with $u^2 = 1$. Fix such a u, then we have the following equality,*

$$\frac{2}{n} \sum_{\substack{\psi\in\widehat{G}\\ \psi(u)=-1}} \psi(g) = \begin{cases} 1 & g = 1 \\ -1 & g = u \\ 0 & \text{otherwise.} \end{cases},$$

where $n := |G|$ and $\widehat{G} := \mathrm{Hom}(G, \mathbb{C}^*)$ denotes the dual group of G.

Proof. Since G is finite and abelian, it is a direct product of cyclic groups

$$G \cong C_{d_1} \times \ldots \times C_{d_\ell}$$

with $d_1|\ldots|d_\ell$. Since we can define characters on each component separately, we can assume without loss of generality that $G = \langle g \rangle$ is cyclic. Note that the existence of an element u of order 2 in G assures that at least one of the cyclic factors above has even order. Now if ζ_n is a primitive nth root of unity, each character ψ of G is uniquely determined by setting

$$\psi(g) = \zeta_n^k$$

for some $k \in \{0, \ldots, n-1\}$. Since $u = g^{\frac{n}{2}}$, we see that the condition $\psi(u) = -1$ forces k to be odd. Thus we have for any $j \in \{0, \ldots, n-1\}$ that

$$\sum_{\substack{\psi \in \widehat{G} \\ \psi(u)=-1}} \psi(g^j) = \sum_{\substack{k=0 \\ k \text{ odd}}}^{n} \zeta_n^{jk} = \zeta^j \sum_{k=0}^{\frac{n}{2}} \zeta_n^{2jk} = \zeta^j \sum_{k=0}^{\frac{n}{2}} \zeta_{\frac{n}{2}}^{jk}.$$

Now, unless j is a multiple of $\frac{n}{2}$, the last sum vanishes because it ranges over all dth roots of unity, where $d = \gcd(jk, \frac{n}{2})$. For $j = 0$, the whole expression obviously becomes $\frac{n}{2}$, for $j = \frac{n}{2}$, we obtain $-\frac{n}{2}$, proving the assertion. $\square$

Corollary 6.2.2. *Let* $\gcd(r, N) = 1$. *Then*

$$\phi_{r,N}(n) := \frac{2}{\varphi(N)} \sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(n \cdot r') = \begin{cases} 1, & \textit{if } n \equiv r \pmod N \\ -1, & \textit{if } n \equiv -r \pmod N \\ 0 & \textit{otherwise} \end{cases}$$

where $\varphi(N) := |(\mathbb{Z}/N\mathbb{Z})^*|$ *denotes Euler's totient function. The summation over* ψ *runs over all odd characters modulo* N *and* r' *is any integer such that* $rr' \equiv 1 \pmod N$.

Proof. This is an immediate consequence of 6.2.1. □

6.3 Weight one Eistenstein series

In this section, we recall the relevant facts about Eisenstein series of weight 1. For a general reference, the reader is referred to Section 4.8. in [DS05b].

For $v = (c_v, d_v) \in ((\mathbb{Z}/N\mathbb{Z})^*)^2$ with order N we define

$$g_1^v(\tau) = \delta(c_v)\zeta^{d_v}(1) + \frac{2\pi i}{N}\left(\frac{\overline{c_v}}{N} - \frac{1}{2}\right) - \frac{2\pi i}{N}\sum_{n=1}^{\infty}\left(\sum_{\substack{m|n \\ \frac{n}{m}\equiv c_v \pmod N}} sign(m)e^{\frac{2\pi i d_v m}{N}}\right)q^{\frac{n}{N}}.$$

In this formula, $\overline{c_v}$ denotes the integer such that $0 \le \overline{c_v} < N$ and $c_v \equiv \overline{c_v} \pmod N$. We also define

$$\delta(c_v) := \begin{cases} 1 & \overline{c_v} = 0, \\ 0 & \text{otherwise}, \end{cases}$$

and the function $\zeta^d(k)$ by

$$\zeta^d(s) := \sum_{\substack{n\in\mathbb{Z} \\ n\equiv d \pmod N}} \frac{1}{n^s}$$

for $\Re(s) > 1$ and otherwise by analytic continuation. We shall mainly need the special value (see [DS05b], Equation (4.22) and Exercise 4.4.5)

$$\zeta^d(1) = \frac{\pi i}{N} + \frac{\pi}{N}\cot\left(\frac{\pi d}{N}\right) \qquad (\gcd(d, N) = 1). \tag{6.1}$$

The formula for $g_1^v(\tau)$ is very similar to the typical Eisenstein series for $k \ge 3$, but contains a correction term. One can show that $g_1^v(\tau)$ is a weight 1 modular form with respect to the principal congruence subgroup $\Gamma(N)$, and satisfies the equation

$$g_1^v[\gamma]_1(\tau) = g_1^{\gamma(v)}(\tau),$$

with

$$\gamma(v) = (ac_v + cd_v, bc_v + dd_v).$$

for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

To obtain forms which are weight 1 invariant with respect to $\Gamma_1(N)$, one generally takes special linear combinations of the g_1^v functions as follows: Let ψ, χ be Dirichlet characters modulo u and v respectively with $uv = N$ such that χ is primitive and $\psi\chi$ is odd. Define $G_1^{\psi,\chi}$ as follows:

$$G_1^{\psi,\chi}(\tau) = \sum_{c=0}^{u-1} \sum_{d=0}^{v-1} \sum_{e=0}^{u-1} \psi(c)\overline{\chi}(d) g_1^{(cv,d+ev)}(\tau). \tag{6.2}$$

In our arguments, we choose to take v to be 1 so that χ is trivial and ψ is an odd character with respect to modulus N. We let $E_1^{\psi}(\tau)$ denote the normalized series given by $-\frac{1}{2\pi i} G_1^{\psi,1}(\tau)$. The Fourier series of $E_1^{\psi}(\tau)$ is given by (see [DS05b], p. 140)

$$E_1^{\psi}(\tau) = L(0,\psi) + 2\sum_{n=1}^{\infty} \left(\sum_{d|n} \psi(d) \right) q^n. \tag{6.3}$$

The next result connects the E_1^{ψ} series to the generating function for $\widehat{T}_{r,N}(n) - \widehat{T}_{N-r,N}(n)$.

Proposition 6.3.1. *If* $N \geq 3$ *and* $\gcd(r,N) = 1$, *then*

$$G_{r,N}(q) := \sum_{n\geq 1} \left(\widehat{T}_{r,N}(n) - \widehat{T}_{N-r,N}(n) \right) q^n$$

$$= \frac{1}{\varphi(N)} \frac{q^{\frac{1}{24}}}{\eta(\tau)} \left(c_{r,N} + \sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(r') E_1^{\psi}(\tau) \right),$$

where

$$c_{r,N} = -\sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(r')L(0,\psi)$$

and $L(s,\psi)$ denotes the Dirichlet L-series associated to ψ.

Proof. First, we rewrite $G_{r,N}(q)$ using Lemma 6.1.1.

$$G_{r,N}(q) = \prod_{n=1}^{\infty} \frac{1}{1-q^n} \left(\sum_{m=1}^{\infty} \left(\sum_{\substack{d|m \\ d\equiv r \pmod N}} - \sum_{\substack{d|m \\ d\equiv -r \pmod N}} \right) q^m \right).$$

By 6.2.2 we see that the coefficient of q^m is $\sum_{d|m} \phi_{r,N}(d)$, so that we can write

$$G_{r,N}(q) = \frac{1}{\varphi(N)} \prod_{n=1}^{\infty} \frac{1}{1-q^n} \left(\sum_{n=1}^{\infty} \left(\sum_{d|n} \sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(d)\psi(r') \right) q^n \right).$$

Finally, we write this expression in terms of the Eisenstein series given in (6.3).

$$\begin{aligned} G_{r,N}(q) &= \frac{1}{\varphi(N)} \frac{q^{\frac{1}{24}}}{\eta(\tau)} \left(\sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \Big(\psi(r')E_1^{\psi}(\tau) - \psi(r')L(0,\psi) \Big) \right) \\ &= \frac{1}{\varphi(N)} \frac{q^{\frac{1}{24}}}{\eta(\tau)} \left(c_{r,N} + \sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(r')E_1^{\psi}(\tau) \right). \end{aligned}$$

□

Our proof will also require some information about the behavior of the Eisenstein series in 6.3.1 near the cusps, that is, near $\tau = \frac{h}{k}$.

Let $E_{r,N}(\tau)$ denote the Eisenstein series in 6.3.1, that is

$$E_{r,N}(\tau) := \sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(r')E_1^{\psi}(\tau).$$

Lemma 6.3.2. *Let r, N be fixed positive integers with $\gcd(r, N) = 1$. Let h, k be integers with $h \leq k$ and $\gcd(h, k) = 1$. Let H be such that $1 \leq H \leq k$ and $hH \equiv -1 \pmod k$. As introduced in Chapter 2, we let*

$$\alpha_{h,k} := \begin{pmatrix} -h & \frac{hH+1}{k} \\ -k & H \end{pmatrix}$$

Then

$$E_{r,N}[\alpha]_1(\tau) = \sum_{n=0}^{\infty} a_n(h,k)q^{\frac{n}{N}}$$

where the following are true:

$$a_0(h,k) = \sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} c_{\psi}(h,k)\psi(r') \tag{6.4}$$

where

$$c_{\psi}(h,k) =$$
$$-\frac{1}{2\pi i}\sum_{c=0}^{N-1}\sum_{e=0}^{N-1}\psi(c)\left(\delta(-hc-ke)\zeta^{(\frac{hH+1}{k})c+He}(1) + \frac{2\pi i}{N}\left(\frac{\overline{(-hc-ke)}}{N} - \frac{1}{2}\right)\right)$$

and $rr' \equiv 1 \pmod N$.

Also, we have the following:

$$|a_0(h,k)| \leq C_0,$$

and for all $n \geq 1$*,*

$$|a_n(h,k)| \leq C_1 n,$$

where C_0, C_1*, depend on* N *but do not depend on* h *or* k*.*

Proof. Recall that

$$E_{r,N}[\alpha_{h,k}]_1(\tau) = \sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(r') E_1^{\psi}[\alpha_{h,k}]_1(\tau).$$

We have

$$E_1^{\psi}[\alpha_{h,k}]_1(\tau) = -\frac{1}{2\pi i} \sum_{c=0}^{N-1} \sum_{e=0}^{N-1} \psi(c) g_1^{\alpha_{h,k}(c,e)}(\tau)$$

where

$$\alpha_{h,k}(c,e) = \left(-hc - ke, \left(\frac{hH+1}{k}\right) c + He\right).$$

Using the Fourier expansion for $g_1^v(\tau)$, we obtain the following expressions for the coefficients of $E_1^{\psi}[\alpha](\tau)$:

$$a_0(h,k) = \sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(r') c_{\psi}(h,k)$$

where

$$c_{\psi}(h,k) = -\frac{1}{2\pi i} \sum_{c=0}^{N-1} \sum_{e=0}^{N-1} \psi(c) \left(\delta(-hc-ke) \zeta^{(\frac{hH+1}{k})c + He}(1) + \frac{2\pi i}{N} \left(\frac{\overline{(-hc-ke)}}{N} - \frac{1}{2} \right) \right).$$

and for $n \geq 1$:

$$a_n(h,k) = \sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(r') \left(\sum_{c=0}^{N-1} \sum_{e=0}^{N-1} \left(\sum_{\substack{d \mid n \\ \frac{n}{d} \equiv -hc-ke \pmod N}} sign(d) e^{\frac{2\pi i}{N} d (\frac{hH+1}{k} c + He)} \right) \right).$$

The inner sum is bounded by the divisor counting function $2d(n)$ which is less than

$2n$, so the whole expression is bounded by $\varphi(N)N^2 n$. Note that much stronger bounds for $d(n)$ exist, in fact $d(n) = O(n^\epsilon)$ for any $\epsilon > 0$, however we require only the crude bound $d(n) \leq n$. This proves the second inequality in the proposition. $\square$

6.4 Proof of Theorem 1.5.1

We will follow the proof of Rademacher's formula for the partition function, as described by Apostol in Chapter 5 of [Apo90]. Throughout the proof, let r and N be fixed coprime integers with $N \geq 3$.

By Cauchy's integral formula, we have:

$$\widehat{T}_{r,N}(n) - \widehat{T}_{N-r,N}(n) = \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{G_{r,N}(q)}{q^{n+1}}dq,$$

where $\mathcal{C}$ is any positively oriented contour lying inside the unit circle, which contains the origin in its interior. By Proposition 6.3.1, we can decompose this integral into two integrals, as follows,

$$\widehat{T}_{r,N}(n) - \widehat{T}_{N-r,N}(n) = T_1 + T_2 := \tag{6.5}$$

$$\frac{1}{2\pi i\varphi(N)}c_{r,N}\int_{\mathcal{C}} \frac{q^{\frac{1}{24}}}{\eta(\tau)}\frac{1}{q^{n+1}}dq + \frac{1}{2\pi i\varphi(N)}\int_{\mathcal{C}} \frac{q^{\frac{1}{24}}E_{r,N}(\tau)}{\eta(\tau)q^{n+1}}dq. \tag{6.6}$$

The first integral is basically the one Rademacher considered, which yields (see (1.12))

$$T_1 = \frac{c_{r,N}}{\varphi(N)}\frac{2\pi}{(24)^{\frac{3}{4}}}\left(n - \frac{1}{24}\right)^{-\frac{3}{4}}\sum_{k=1}^{\infty} A_k(n)k^{-1}I_{\frac{3}{2}}\left(\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right),$$

where $I_{\frac{3}{2}}$ is the order $\frac{3}{2}$ modified Bessel function of the first kind,

$$A_k(n) = \sum_{\substack{0 \le h < k \\ (h,k)=1}} e^{\pi i s(h,k) - 2\pi i n \frac{h}{k}}, \tag{6.7}$$

and $s(h,k)$ is as in (2.1).

For the rest of the subsection, we will use Rademacher's technique to obtain an asymptotic formula for T_2. We define the contour $\mathcal{C}$ to be given by $q = e^{2\pi i \tau}$ where τ follows Rademacher's path of integration $P(n)$ which takes τ from i to $i+1$ by going along the upper arcs of the Farey circles $C_{h,k}$ where $\frac{h}{k}$ is in the Farey sequence of order n. That is, $\gcd(h,k) = 1$, and $1 \le h \le k \le n$. Let $\gamma(h,k)$ denote the upper arc of the Ford circle $C_{h,k}$. Changing variables from q to τ, we have:

$$T_2 = \frac{1}{\varphi(N)} \sum_{\substack{0 \le h \le k \le n \\ \gcd(h,k)=1}} \int_{\gamma(h,k)} \frac{q^{\frac{1}{24}} E_{r,N}(\tau)}{\eta(\tau) q^n} d\tau.$$

As in [Apo90], we make the change of variables $z = -ik^2 \left(\tau - \frac{h}{k}\right)$, so that $\tau = \frac{h}{k} + \frac{iz}{k^2}$. This maps $\gamma(h,k)$ to an arc of the circle of radius $\frac{1}{2}$ centered at $\frac{1}{2}$. The contour goes in the clockwise direction from the image of the left end point of $\gamma_(h,k)$ to the image of the right endpoint of $\gamma(h,k)$. It is well-known (see Theorem 5.8 in [Apo90]) that if $\frac{h_1}{k_1} < \frac{h}{k} < \frac{h_2}{k_2}$ are adjacent in the Farey sequence of order M, then the image under the change of variables from τ to z of the point where $\gamma(h_1,k_1)$ and $\gamma(h,k)$ intersect is given by

$$z_1(h,k) = \frac{k^2}{k^2 + k_1^2} + i\frac{kk_1}{k^2 + k_1^2}.$$

Similarly, the point where $\gamma(h,k)$ meets $\gamma(h_2,k_2)$ is mapped to

$$z_2(h,k) = \frac{k^2}{k^2 + {k_2}^2} - \frac{ikk_2}{k^2 + {k_2}^2}.$$

This gives us the following:

$$T_2 = \frac{i}{\varphi(N)} \sum_{h,k} \frac{1}{k^2} \int_{z_1(h,k)}^{z_2(h,k)} \frac{q^{\frac{1}{24}} E_{r,N}(\tau)}{\eta(\tau) q^n} dz.$$

Now we will estimate the integrand by its behavior near the cusps. Let $a_n(h,k)$ be as in 6.3.2. First we decompose the integrand,

$$\begin{aligned}
&\frac{\left(q^{\frac{1}{24}} E_{r,N}(\tau)\right)}{\eta(\tau) q^n} = \Psi_1(\tau) + \Psi_2(\tau) := \\
&- i \left(\frac{z}{k}\right)^{-\frac{1}{2}} \frac{1}{q^n} e^{-\frac{\pi z}{12k^2} + \frac{\pi}{12z} + \pi i s(-H,k)} a_0(h,k) \\
&+ \left(\frac{\left(q^{\frac{1}{24}} E_{r,N}(\tau)\right)}{\eta(\tau) q^n} + i \left(\frac{z}{k}\right)^{-\frac{1}{2}} \frac{1}{q^n} e^{-\frac{\pi z}{12k^2} + \frac{\pi}{12z} + \pi i s(-H,k)} a_0(h,k) \right).
\end{aligned}$$

Now we show that $\Psi_2(\tau)$ is negligible. We can adjust to the contour of integration so that we are integrating along the chord adjoining $z_1(h,k)$ and $z_2(h,k)$ instead of the arc. This yields

$$\begin{aligned}
|\Psi_2(\tau)| &= \left| \left(\frac{z}{k}\right)^{-\frac{1}{2}} e^{-\frac{\pi z}{12k^2} + \frac{\pi}{12z} + \pi i s(h,k)} \frac{1}{q^n} \left(\sum_{m=1}^{\infty} (\sum_{Nj+\ell=m} a_\ell(h,k) p(j)) e^{2\pi i \frac{m}{N}(\frac{H}{k} + \frac{i}{z})} \right) \right| \\
&\le \frac{\sqrt{k}}{\sqrt{|z|}} e^{2\pi \Re(z) n/k^2} \left(\sum_{m=1}^{\infty} (\sum_{Nj+\ell=m}^{\infty} a_\ell(h,k) p(j)) e^{-2\pi \Re\left(\frac{1}{z}\right)(\frac{m}{N} - \frac{1}{24})} \right).
\end{aligned}$$

For z inside the circle, $\Re\left(\frac{1}{z}\right) \ge 1$ ([Apo90], page 107). By Lemma 6.3.2, we have $|a_n(h,k)| \le C_1 n$ for $n \ge 1$. Thus:

$$\sum_{m=1}^{\infty} \left(\sum_{i+j=m}^{\infty} a_i(h,k) p(j) \right) e^{-2\pi \Re\left(\frac{1}{z}\right)\left(m - \frac{1}{24}\right)} \le \sum_{m=1}^{\infty} C_1 m^2 p(m) e^{-2\pi(m - \frac{1}{24})}$$

The known asymptotics for $p(n)$ ensure that the sum is convergent.

By Theorem 5.9 in [Apo90], we have $\Re(z) \le |z| \le \frac{\sqrt{2}k}{n}$ on the chord, thus we have

$e^{2\pi\Re(z)n/k^2} \leq e^{8\pi}$. Using the formulas for $z_1(h,k), z_2(h,k)$, we have that for z on the chord,

$$|z| \geq \min\{\mathrm{Re}(z_1(h,k)), \mathrm{Re}(z_2(h,k))\} \geq \frac{1}{2n^2}.$$

Thus we have the following:

$$|\Psi_2(\tau)| \leq Ck^{\frac{1}{2}}n,$$

for some constant C, independent of h, k, or n. The length of the chord at most $\frac{2\sqrt{2}k}{n}$, so we have

$$\int_{z_1(h,k)}^{z_2(h,k)} \Psi_2(\tau)dz \leq C2\sqrt{2}k^{\frac{3}{2}}.$$

Considering all the integrals over Ψ_2 that contribute the calculation of T_2, we estimate:

$$\left|\frac{i}{\varphi(N)} \sum_{h,k} \frac{1}{k^2} \int_{z_1(h,k)}^{z_2(h,k)} \Psi_2(\tau)dz\right| \leq \frac{C2\sqrt{2}}{\varphi(N)} n^{\frac{3}{2}}.$$

This allows us to approximate T_2 as follows:

$$\begin{aligned} T_2 &= \frac{i}{\varphi(N)} \sum_{h,k} \frac{1}{k^2} \int_{z_1(h,k)}^{z_2(h,k)} -i\left(\frac{z}{k}\right)^{-\frac{1}{2}} \frac{1}{q^n} e^{-\frac{\pi z}{12k^2}+\frac{\pi}{12z}+\pi i s(-H,k)} a_0(h,k)dz \\ &+ \frac{i}{\varphi(N)} \sum_{h,k} \frac{1}{k^2} \int_{z_1(h,k)}^{z_2(h,k)} \Psi_2(\tau)dz \\ &= \frac{1}{\varphi(N)} \sum_{h,k} \frac{1}{k^2} \int_{z_1(h,k)}^{z_2(h,k)} \left(\frac{z}{k}\right)^{-\frac{1}{2}} \frac{1}{q^n} e^{-\frac{\pi z}{12k^2}+\frac{\pi}{12z}+\pi i s(-H,k)} a_0(h,k)dz + O(n^{\frac{3}{2}}). \end{aligned}$$

To evaluate the integral, we adjust the contour of integration.Let $x_1(n)$ be the point on the upper half of the circle K with $|x_1(n)| = \frac{1}{n}$, and let $x_2(n)$ be the point on the lower half of the circle with $|x_2(n)| = \frac{1}{n}$, and we rewrite the integral as $\int_{z_1(h,k)}^{z_2(h,k)} = \int_{x_1(n)}^{x_2(n)} - \int_{x_1(n)}^{z_1(h,k)} - \int_{z_2(h,k)}^{x_2(n)}$.

We will show that the second two integrals are negligible. On the arc between $x_1(n)$ and $z_1(h,k)$, and on the arc between $z_2(h,k)$ and $x_2(n)$, we have $\frac{1}{n} \leq |z| \leq \frac{\sqrt{2}k}{n}$. For z on the circle, $\Re\left(\frac{1}{z}\right) = 1$. Combining these facts, we have that the integrand is bounded as follows:

$$\left|\frac{1}{k^2}\left(\frac{k}{z}\right)^{\frac{1}{2}} a_0(h,k)e^{-\frac{2\pi inh}{k}} e^{\frac{2\pi nz}{k^2}} e^{-\frac{\pi z}{12k^2}+\frac{\pi}{12z}+\pi is(h,k)}\right| \leq$$

$$\frac{1}{k^2}\sqrt{k}|z|^{-\frac{1}{2}}|a_0(h,k)|e^{2\pi n\Re(z)/k^2-\frac{\pi\Re(z)}{12k^2}+\frac{\pi\Re\left(\frac{1}{z}\right)}{12}}$$

$$\leq k^{-\frac{3}{2}}\sqrt{n}C_0 k e^{2\pi\sqrt{2}/k+\frac{\pi}{12}}$$

$$\leq C_0 e^{2\sqrt{2}\pi+\frac{\pi}{12}} k^{-\frac{1}{2}} n^{\frac{1}{2}}$$

Thus, making use of the fact that the length of both arcs is bounded by π, we have the following bound for the integral over these two arcs:

$$\left|\left(\int_{x_1(n)}^{z_1(h,k)} + \int_{z_2(h,k)}^{x_2(n)}\right)\left(\frac{1}{k^2}\left(\frac{k}{z}\right)^{\frac{1}{2}} a_0(h,k)e^{-\frac{2\pi inh}{k}} e^{\frac{2\pi nz}{k^2}} e^{-\frac{\pi z}{12k^2}+\frac{\pi}{12z}+\pi is(h,k)}\right)\right| \leq C_0\pi e^{2\sqrt{2}\pi+\frac{\pi}{12}}.$$

Summing over h,k, we get the total contribution to the asymptotic from these arcs,

$$\left|\frac{1}{\varphi(N)}\sum_{h,k}\left(\int_{x_1(n)}^{z_1(h,k)} + \int_{z_2(h,k)}^{x_2(n)}\right)\left(\frac{1}{k^2}\left(\frac{k}{z}\right)^{\frac{1}{2}} a_0(h,k)e^{-\frac{2\pi inh}{k}} e^{\frac{2\pi nz}{k^2}} e^{-\frac{\pi z}{12k^2}+\frac{\pi}{12z}+\pi is(h,k)}\right)\right|$$
$$\leq C_0\pi e^{2\sqrt{2}\pi+\frac{\pi}{12}} n^2.$$

Therefore, we can rewrite T_2 as follows:

$$T_2 = \frac{1}{\varphi(N)}\sum_{h,k} B_k(n)\int_{x_1(n)}^{x_2(n)} \frac{1}{k^{\frac{3}{2}}}\left(\frac{1}{z}\right)^{\frac{1}{2}} e^{\frac{2\pi nz}{k^2}-\frac{\pi z}{12k^2}+\frac{\pi}{12z}} dz + O(n^2),$$

where

$$B_k(n) = \sum_{\substack{1\leq h\leq k\\ \gcd(h,k)=1}} a_0(h,k)e^{\pi is(h,k)-\frac{2\pi inh}{k}}.$$

We change variables by taking $t = \frac{\pi}{12z}$. This yields the following:

$$T_2 = -\left(\frac{\pi}{12}\right)^{\frac{1}{2}} \frac{1}{\varphi(N)} \sum_{h,k} B_k(n) k^{-\frac{3}{2}} \int_{\frac{\pi}{12} - i\frac{\pi}{12}\sqrt{n^2-1}}^{\frac{\pi}{12} + i\frac{\pi}{12}\sqrt{n^2-1}} t^{-\frac{3}{2}} e^{\frac{2\pi^2 n}{12tk^2} - \frac{\pi^2}{t12^2k^2} + t} dt + O(n^2).$$

Finally, we rewrite all this in terms of modified I Bessel functions. We have the following well-known description of the I-Bessel function of order ν in terms of contour integrals (see [Apo90], p. 109)

$$I_\nu(z) = \frac{\left(\frac{1}{2}z\right)^\nu}{2\pi i} \int_{c-i\infty}^{c+i\infty} t^{-\nu-1} e^{t + \frac{z^2}{4t}} dt. \tag{6.8}$$

Furthermore, one can express the I-Bessel functions whose order is half of an odd integer as an elementary function, e.g.,

$$I_{\frac{1}{2}}(z) = \sqrt{\frac{2}{\pi z}} \sinh(z) = \frac{1}{\sqrt{2\pi z}}(e^z - e^{-z}).$$

It is straightforward to show

$$\left| \int_{\frac{\pi}{12} + i\frac{\pi}{12}\sqrt{n^2-1}}^{\frac{\pi}{12} + i\infty} t^{-\frac{3}{2}} e^{\frac{2\pi^2 n}{12tk^2} - \frac{\pi^2}{t12^2k^2} + t} dt \right| = O(n^{-\frac{1}{2}})$$

and

$$\left| \int_{\frac{\pi}{12} - i\infty}^{\frac{\pi}{12} - i\frac{\pi}{12}\sqrt{n^2-1}} t^{-\frac{3}{2}} e^{\frac{2\pi^2 n}{12tk^2} - \frac{\pi^2}{t12^2k^2} + t} dt \right| = O(n^{-\frac{1}{2}}).$$

Applying the trivial bound $|B_k(n)| \leq C_0 k$, we have the following:

$$\begin{aligned} T_2 &= -\left(\frac{\pi}{12}\right)^{\frac{1}{2}} \frac{1}{\varphi(N)} \sum_{h,k} B_k(n) k^{-\frac{3}{2}} \left(\int_{\frac{\pi}{12} - i\infty}^{\frac{\pi}{12} + i\infty} t^{-\frac{3}{2}} e^{\frac{2\pi^2 n}{12tk^2} - \frac{\pi^2}{t12^2k^2} + t} dt + O(n^{-\frac{1}{2}}) \right) + O(n^2) \\ &= -\left(\frac{\pi}{12}\right)^{\frac{1}{2}} \frac{1}{\varphi(N)} \sum_{h,k} B_k(n) k^{-\frac{3}{2}} \int_{\frac{\pi}{12} - i\infty}^{\frac{\pi}{12} + i\infty} t^{-\frac{3}{2}} e^{\frac{2\pi^2 n}{12tk^2} - \frac{\pi^2}{t12^2k^2} + t} dt + O(n^2). \end{aligned}$$

We take $z = 2\sqrt{\frac{\pi^2}{6k^2}\left(n - \frac{1}{24}\right)}$ in (6.8) and find

$$T_2 = \tag{6.9}$$

$$-2\pi i \frac{1}{\varphi(N)}\left(\frac{\pi}{12}\right)^{\frac{1}{2}}\left(\frac{\pi^2}{6}\left(n-\frac{1}{24}\right)\right)^{-\frac{1}{4}}\sum_{k=1}^{n} B_k(n)k^{-1}I_{\frac{1}{2}}\left(\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)+O(n^2). \tag{6.10}$$

To compute the asymptotic, we need the $k = 1$ term of this sum. We find with (6.1) and 6.3.2 the following formula for $B_1(n)$,

$$B_1(n) = a_0(0,1) = -\frac{1}{2Ni}\sum_{\substack{\psi \pmod N \\ \psi(-1)=-1}} \psi(r')\sum_{c=0}^{N-1}\psi(c)\cot\left(\frac{\pi c}{N}\right).$$

We compute the error:

$$\begin{aligned} &2\pi\frac{1}{\varphi(N)}\left(\frac{\pi}{12}\right)^{\frac{1}{2}}\left(\frac{\pi^2}{6}\left(n-\frac{1}{24}\right)\right)^{-\frac{1}{4}}\sum_{k=2}^{n}\left|B_k(n)k^{-1}I_{\frac{1}{2}}\left(\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)\right| \\ &\le \frac{\pi}{\varphi(N)}\left(n-\frac{1}{24}\right)^{-\frac{1}{2}}C_0\left(n^{\frac{5}{2}}e^{\frac{\pi}{2}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}}+O(1)\right)\end{aligned}$$

Thus we have:

$$T_2 = \tag{6.11}$$

$$\frac{1}{2\sqrt{2}\varphi(N)N}\left(\sum_{\psi(-1)=-1}\psi(r')\sum_{c=0}^{N-1}\psi(c)\cot\left(\frac{\pi c}{N}\right)\right)\frac{e^{\left(\pi\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)}}{\sqrt{\left(n-\frac{1}{24}\right)}} \tag{6.12}$$

$$+O\left(n^2 e^{\left(\frac{\pi}{2}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)}\right). \tag{6.13}$$

6.5 Euler-Maclaurin Summation

In this subsection we recall a maybe not too widely known version of the Euler-Maclaurin summation formula. For asymptotic exansions in the strong sense, we use the notation

$$h(t) \sim \sum_{k=-1}^{\infty} a_k t^k, \quad (t \to 0).$$

This means that for every $M \geq 0$ we have

$$h(t) - \sum_{k=-1}^{M-1} a_k t^k = O(t^M), \quad (t \to 0).$$

In the following, we will often encounter *Bernoulli polynomials* $B_n(x)$ for n a non-negative integer, which can be defined via their generating function

$$\sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!} = \frac{te^{xt}}{e^t - 1}, \quad |t| < 2\pi,$$

and the *Bernoulli numbers* $B_n := B_n(0)$.

The Bernoulli polynomials are also given explicitly in terms of the Bernoulli numbers as follows:

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} x^k \tag{6.14}$$

and they satisfy the following relations,

$$B_n(x+1) - B_n(x) = nx^{n-1} \tag{6.15}$$

and

$$B_n(1-x) = (-1)^n B_n(x), \tag{6.16}$$

see e.g. equations (24.4.1) and (24.4.3) in [OLBC10].

In Proposition 3 in [Zag75], Zagier gives the following formula, which we use.

He proves a slightly more restrictive version of the following theorem, but states the version displayed here[1]. The reader is also referred to formula 23.1.32 in [AS] as well as [Lam01] and the references therein.

Proposition 6.5.1. *Let f be a C^∞ function on the positive real line which has an asymptotic expansion $f(t) \sim \sum_{n=0}^{\infty} b_n t^n$ as $t \to 0$, and satisfies the property that it and all of its derivatives are of rapid decay at infinity. Then we have the asymptotic expansion*

$$\sum_{m=0}^{\infty} f((m+a)t) \sim \frac{1}{t}\int_0^\infty f(t)dt - \sum_{n=0}^{\infty} b_n \frac{B_{n+1}(a)}{n+1} t^n, \quad (t \to 0).$$

for every $a > 0$.

Remark 6.5.2. *An inspection of the proof of Proposition 6.5.1 shows that the given asymptotic expansion is actually valid whenever t is a complex variable with $|\arg(t)| < \frac{\pi}{2} - \delta$ for some $\delta > 0$ provided that $f^{(n)}(e^{i\theta}x)$ is of rapid decay for real $x \to \infty$, $|\theta| < \frac{\pi}{2} - \delta$ and all non-negative integers n.*

For the convenience of the reader, we give a proof of 6.5.1.

Proof. For some t, Let $g(x) := f((a+x)t)$. Note that g is still smooth and has derivatives of rapid decay at infinity. Applying the first formula on page 13 of [Zag75] to $g(x)$ gives us the following:

$$\sum_{m=1}^{\infty} f((m+a)t) = \frac{\int_{at}^{\infty} f(x)dx}{t} + \sum_{n=1}^{N-1} \frac{(-1)^n B_{n+1}}{(n+1)!} g^{(n)}(0) - (-1)^N \int_0^\infty g^{(N)}(x) \frac{\widehat{B}_N(x)}{N!} dx.$$

where $\widehat{B}_N(x) := B_n(x - \lfloor x \rfloor)$.

[1]The equation he gives (see eq. (44) in [Zag75]), however, contains a slight typo, the + sign in front of the sum should be a - sign.

We notice that the first term is given by

$$\frac{\int_{at}^{\infty} f(x)dx}{t} = \frac{\int_0^{\infty} f(x)dx}{t} - \frac{\int_0^{at} f(x)dx}{t}$$

Using the asymptotic expansion for f, we have

$$\frac{\int_0^{at} f(x)dx}{t} = \sum_{n=0}^{N-1} \frac{b_n a^{n+1} t^n}{n+1} + O(t^N), \quad (t \to 0).$$

We notice that the last integral is $O(t^N)$ as $t \to 0$, since

$$-(-1)^N \int_0^{\infty} g^{(N)}(x) \frac{\widehat{B}_N(x)}{N!} dx = (-t)^{N-1} \int_0^{\infty} f^{(N)}(x+a) \frac{\widehat{B}_N(\frac{x}{t})}{N!} dx,$$

and since $\widehat{B}_N(x)$ is bounded and $f^{(N)}$ is of rapid decay.

Now we consider the second sum. We have $g^{(n)}(0) = t^n f^{(n)}(at)$, which has the following expansion:

$$g^{(n)}(0) = t^n \left(\sum_{m=0}^{N-1-n} b_{m+n} \frac{(m+n)!}{m!} a^m t^m + O(t^{N-n}) \right), \quad (t \to 0).$$

Substituting this formula and switching the order of summation, we find the asymptotic expansion as $t \to 0$ for the middle sum:

$$\begin{aligned}
&\sum_{n=1}^{N-1} \frac{(-1)^n B_{n+1}}{(n+1)!} g^{(n)}(0) \\
&\quad = \sum_{n=1}^{N-1} \frac{(-1)^n B_{n+1}}{(n+1)!} t^n \left(\sum_{m=0}^{N-1-n} b_{m+n} \frac{(m+n)!}{m!} a^m t^m + O(t^{N-n}) \right), \quad (t \to 0) \\
&\quad = \sum_{k=0}^{N-1} \frac{b_k t^k}{k+1} \sum_{n=0}^{k} (-1)^n B_{n+1} a^{k-n} \binom{k+1}{n+1} + O(t^N), \quad (t \to 0).
\end{aligned}$$

Now we can put everything together to obtain

$$\begin{aligned}\sum_{m=0}^{\infty} f((m+a)t) &= f(at) + \sum_{m=1}^{\infty} f((m+a)t)\\ &= \sum_{n=0}^{N-1} b_n a^n t^n + \frac{\int_0^\infty f(x)dx}{t} - \sum_{n=0}^{N-1} \frac{b_n a^{n+1}}{n+1} t^n\\ &\qquad + \sum_{n=0}^{N-1} \frac{b_n}{n+1}\left[\sum_{k=0}^{n} (-1)^k B_{k+1} a^{n-k} \binom{n+1}{k+1}\right] t^n + O(t^N)\\ &= \frac{\int_0^\infty f(x)dx}{t} + \sum_{n=0}^{N-1} b_n a^n t^n + \sum_{n=0}^{N-1} \frac{b_n}{n+1}\left[\sum_{k=0}^{n+1} \binom{n+1}{k} B_k (-a)^{n+1-k}\right](-t)^n\\ &\quad + O(t^N).\end{aligned}$$

By (6.14) we recognize the sum in square brackets as the Bernoulli polynomial $B_{n+1}(-a)$. Then using (6.15) and (6.16), one easily sees that the coefficient of t^n $(n \geq 0)$ in the above expansion is given by $-\frac{B_{n+1}(a)}{n+1}$, which is what we claimed. $\square$

6.6 Wright's Circle Method

In this section, we briefly recall two propositions from [NR], based on Wright's version of the Circle Method [Wri71], that allow to obtain asymptotic results for products of functions in a fairly general setting.

Suppose $\xi(q)$ and $L(q)$ are analytic functions for complex arguments $|q| < 1$ and $q \notin \mathbb{R}_{\leq 0}$, such that

$$\xi(q)L(q) =: \sum_n a(n)q^n$$

is analytic for $|q| < 1$. Further assume the following hypotheses, where $0 < \delta < \frac{\pi}{2}$ and $c > 0$ are fixed constants.

1. As $t \to 0$ in the cone $|\arg(t)| < \frac{\pi}{2} - \delta$ and $|\Im(t)| \leq \pi$ we have, for some $B \in \mathbb{R}$,

either

$$L(e^{-t}) = t^{-B}\left(\sum_{\ell=0}^{k-1} \alpha_\ell t^\ell + O_\delta(t^k)\right), \tag{6.17}$$

in which case we say that L is *of polynomial type near* 1, or

$$L(e^{-t}) = \frac{\log t}{t^B}\left(\sum_{\ell=0}^{k-1} \alpha_\ell t^\ell + O_\delta(t^k)\right), \tag{6.18}$$

in which case we call L *of logarithmic type near* 1.

2. As $t \to 0$ in the cone $|\arg(t)| < \frac{\pi}{2} - \delta$ and $|\Im(t)| \leq \pi$ we have

$$\xi(e^{-t}) = t^\beta e^{\frac{c^2}{t}}\left(1 + O_\delta(e^{-\frac{\gamma}{t}})\right) \tag{6.19}$$

for real constants $\beta \geq 0$ and $\gamma > c^2$.

3. As $t \to 0$ in the cone $\frac{\pi}{2} - \delta \leq |\arg(t)| < \frac{\pi}{2}$ and $|\Im(t)| \leq \pi$ one has

$$|L(e^{-t})| \ll_\delta |t|^{-C}, \tag{6.20}$$

where $C = C(\delta) > 0$.

4. As $t \to 0$ in the cone $\frac{\pi}{2} - \delta \leq |\arg(t)| < \frac{\pi}{2}$ and $|\Im(t)| \leq \pi$ one has

$$|\xi(e^{-t})| \ll_\delta \xi(|e^{-t}|)e^{-K\Re\left(\frac{1}{t}\right)}, \tag{6.21}$$

where $K = K(\delta) > 0$.

These hypotheses in (6.17)–(6.19) ensure the asymptotics of L and ξ on the so-called *major arc*, those in (6.20)–(6.21) their asymptotics on the so-called *minor arc* of the unit circle.

For our purposes, we require the following two propositions (see Propositions 1.8 and 1.10 in [NR]).

Proposition 6.6.1. *Suppose the hypotheses (1)–(4) are satisfied and that L has polynomial type near* 1*. Then there is an asymptotic expansion*

$$a(n) = e^{2c\sqrt{n}} n^{\frac{1}{4}(2B-2\beta-3)} \left(\sum_{r=0}^{M-1} p_r n^{-\frac{r}{2}} + O(n^{-\frac{M}{2}}) \right), \tag{6.22}$$

where

$$p_r = \sum_{s=0}^{r} \alpha_s w_{s,r-s} \tag{6.23}$$

with α_s as in (6.17) *and*

$$w_{s,r} = \frac{c^{s+\beta-B+\frac{1}{2}}}{(-4c)^r 2\pi^{\frac{1}{2}}} \cdot \frac{\Gamma\left(s+\beta-B+r+\frac{3}{2}\right)}{r!\Gamma\left(s+\beta-B-r+\frac{3}{2}\right)} \tag{6.24}$$

for the coefficients $a(n)$ of $\xi(q)L(q)$ as $n \to \infty$.

Note that Proposition 6.6.1 is originally due to Wright [Wri71].

Proposition 6.6.2. *Suppose hypotheses (1)–(4) are satisfied and that L has logarithmic type near* 1 *such that $B - \beta = \frac{1}{2}$, with B and β as in equations* (6.18) *and* (6.19) *respectively. Then we have*

$$a(n) = -e^{2c\sqrt{n}} n^{-\frac{1}{2}} \frac{\alpha_0}{4\pi^{\frac{1}{2}}} \left(\log n - 2\log c + O(n^{-\frac{1}{2}} \log n) \right)$$

as $n \to \infty$.

6.6.1 A Preliminary Lemma

Here we prove a preliminary result that will be the key step towards the proof of Theorem 1.5.4. For the rest of this thesis, let

$$f(t) = \frac{1}{e^t - 1}, \quad \Re(t) > 0$$

Lemma 6.6.3. *Let r, N be greater than zero. Then we have for $|\arg(t)| < \frac{\pi}{2} - \delta$ for some $0 < \delta < \frac{\pi}{2}$:*

$$\sum_{m=0}^{\infty} f\left(\left(m + \frac{r}{N}\right) t\right) \sim -\frac{\log(t) + \psi\left(\frac{r}{N}\right)}{t} + O(\log t), , \quad (t \to 0),$$

where $\psi(z) = \frac{\Gamma'(z)}{\Gamma(z)}$ denotes Euler's digamma function.

Proof. From the definition of the Bernoulli numbers we have

$$f(t) = \sum_{k=0}^{\infty} \frac{B_k}{k!} t^{k-1}.$$

Let $f^*(t) := f(t) - t^{-1}e^{-t}$. Then we have for $\Re(t) > 0$,

$$\sum_{m=0}^{\infty} f\left(\left(m + \frac{r}{N}\right) t\right) = \sum_{m=0}^{\infty} \frac{1}{\left(m + \frac{r}{N}\right) t} e^{-\left(m + \frac{r}{N}\right)t} + \sum_{m=0}^{\infty} f^*\left(\left(m + \frac{r}{N}\right) t\right). \quad (6.25)$$

To find the asymptotic expansion of the second sum in the right hand side of 6.25, we note that

$$f^*(t) \sim \sum_{k=0}^{\infty} b_k t^k, \quad (t \to 0),$$

where

$$b_k := (B_{k+1} - 1)\frac{1}{(k+1)!}.$$

Then it follows from Proposition 6.5.1 that we have

$$\sum_{m=0}^{\infty} f^*\left(\left(m + \frac{r}{N}\right) t\right) \sim \frac{\int_0^{\infty} f^*(t)dt}{t} - \sum_{n=0}^{\infty} b_n \frac{B_{n+1}\left(\frac{r}{N}\right)}{n+1} t^n, \quad (t \to 0).$$

Next we consider the first sum of the right hand side of (6.25).

First, since

$$\frac{1}{m + \frac{r}{N}} = \left(\frac{1}{m + \frac{r}{N}} - \frac{1}{m}\right) + \frac{1}{m},$$

we have the following:

$$\sum_{m=0}^{\infty} \frac{1}{m+\frac{r}{N}} e^{-mt} = \frac{N}{r} + \sum_{m=1}^{\infty} \frac{e^{-mt}}{m} - \sum_{m=1}^{\infty} \frac{\frac{r}{N}}{m(m+\frac{r}{N})} e^{-mt}.$$

The first sum is equal to $-\log(1-e^{-t})$. Differentiating once with respect to t, we see that the following holds:

$$-\log\left(1-e^{-t}\right) \sim \log\left(\frac{1}{t}\right) - \sum_{n=1}^{\infty} \frac{B_n}{n \cdot n!} t^n, \quad (t \to 0).$$

The second sum is absolutely and uniformly convergent for $\Re(t) \geq 0$ and we have

$$\lim_{t\to 0} \sum_{m=1}^{\infty} \frac{1}{m(m+\frac{r}{N})} e^{-mt} = \sum_{m=1}^{\infty} \frac{1}{m(m+\frac{r}{N})} = \frac{N}{r}\left(\gamma_E + \psi\left(\frac{r}{N}\right)\right) + \frac{N^2}{r^2}$$

by equation (5.7.6) in [OLBC10], where γ_E denotes the Euler-Mascheroni constant. We have that in fact

$$\sum_{m=1}^{\infty} \frac{1}{m(m+\frac{r}{N})} e^{-mt} = \frac{N}{r}\left(\gamma_E + \psi\left(\frac{r}{N}\right)\right) + \frac{N^2}{r^2} + O(t\log t), \quad (t \to 0),$$

or, equivalently, that

$$\lim_{t\to 0} \sum_{m=1}^{\infty} \frac{1}{m(m+\frac{r}{N})} \frac{e^{-mt}-1}{t\log t}$$

exists, which can easily be seen by applying de l'Hôpital's Rule (since the series is still absolutely and locally uniformly convergent for $\Re(t) > 0$, we can differentiate each summand).

Assembling all of this gives the following:

$$\sum_{m=0}^{\infty} f\left(\left(m+\frac{r}{N}\right)t\right) \sim \frac{e^{-\frac{r}{N}t}}{t}\left(\frac{N}{r}+\log\left(\frac{1}{t}\right)-\sum_{n=1}^{\infty}\frac{B_n}{n\cdot n!}t^n+\sum_{m=1}^{\infty}\frac{-\frac{r}{N}}{m(m+\frac{r}{N})}e^{-mt}\right)$$
$$+\frac{\int_0^{\infty} f^*(t)dt}{t}-\sum_{n=0}^{\infty} b_n \frac{B_{n+1}(\frac{r}{N})}{n+1}t^n, \quad (t \to 0).$$

Simplifying, we have

$$\sum_{m=0}^{\infty} f\left(\left(m+\frac{r}{N}\right)t\right) \sim -\frac{\log(t)+\psi\left(\frac{r}{N}\right)}{t}+O(\log t), \quad (t \to 0).$$

Here we used the fact (see eq. (5.9.18) in [OLBC10]) that

$$\int_0^{\infty} f^*(t)dt = \int_0^{\infty} \frac{1}{e^t-1}-\frac{e^{-t}}{t}dt = \gamma_E.$$

□

6.7 Proof of Theorem 1.5.4

Now we prove the Theorem 1.5.4.

Proof. By Lemma 6.1.1 we have

$$\sum_{n=1}^{\infty} \hat{T}_{r,N}(n)q^n = \left(\prod_{n\geq 1}\frac{1}{1-q^n}\right)\left(\sum_{n=1}^{\infty}\left(\sum_{\substack{d|n \\ d\equiv r \pmod N}} q^n\right)\right)$$

Letting f be as defined in the previous section and setting $q=e^{-t}$, we simplify this as follows:

$$\sum_{n=1}^{\infty}\hat{T}_{r,N}(n)q^n = \left(\prod_{n\geq 1}\frac{1}{1-q^n}\right)\sum_{m\equiv r \pmod N}\frac{q^m}{1-q^m}$$
$$= \left(\prod_{n\geq 1}\frac{1}{1-q^n}\right)\sum_{m=0}^{\infty} f\left(\left(m+\frac{r}{N}\right)Nt\right).$$

Now we wish to apply the method outlined in Section 6.6 with $\xi(e^{-t}) = \frac{(2\pi)^{\frac{1}{2}}}{\eta(\frac{it}{2\pi})}$ and $L(e^{-t}) = (2\pi)^{-\frac{1}{2}}q^{\frac{1}{24}}\sum_{m=0}^{\infty} f\left(\left(m+\frac{r}{N}\right)Nt\right)$. The function $\xi(q)$ is known to satisfies hypotheses 2 and 4 in Section 6.6 with $c^2 = \frac{\pi^2}{6}$, $\beta = \frac{1}{2}$, and $\gamma = 4\pi^2$ (see Theorem 4.1 in [NR]).

From Lemma 6.6.3 we see that $L(q)$ satisfies hypothesis 1. By the straightforward estimate

$$\left|\sum_{m\equiv r \pmod N}\frac{q^m}{1-q^m}\right| \leq \sum_{m=1}^{\infty}\frac{|q|^m}{1-|q|^m}$$

and Corollary 4.5 in [NR] we see that

$$\sum_{m\equiv r \pmod N}\frac{q^m}{1-q^m} \ll_\delta t^{-\frac{3}{2}}$$

in the bounded cone $\frac{\pi}{2}-\delta \leq |\arg(t)| < \frac{\pi}{2}$ and $|\Im(t)| \leq \pi$, so that $L(q)$ also satisfies hypothesis 3 so that we can apply Propositions 6.6.1 and 6.6.2.

To be more precise, the asymptotic expansion as $t \to 0$ has both a polynomial and logarithmic asymptotic component. The logarithmic component is as follows:

$$L_1(e^{-t}) = -\frac{\log(t)}{(2\pi)^{\frac{1}{2}}Nt}(1+O(1)),$$

to which we can apply Proposition 6.6.2, with $B = 1$ and $\alpha_0 = -\frac{1}{(2\pi)^{\frac{1}{2}}N}$.

For the polynomial part, we have the following:

$$L_2(e^{-t}) = -\frac{\log N}{Nt(2\pi)^{\frac{1}{2}}} - \frac{\psi\left(\frac{r}{N}\right)}{Nt(2\pi)^{\frac{1}{2}}}.$$

For L_2, we apply Proposition 6.6.1, with $B = 1$, $M = 1$, $\alpha_0 = -\frac{1}{N(2\pi)^{\frac{1}{2}}}\left(\psi\left(\frac{N}{r}\right) + \log N\right)$. Putting these results together completes the proof. $\square$

Bibliography

[AGM17] A. Alanazi, S. Gagola, and A. Munagi. Combinatorial proof of a partition inequality of bessenrodt-ono. volume 21, pages 331–337. Ann. Comb., 2017.

[Apo90] T. Apostol. Modular functions and dirichlet series in number theory. In *Springer-Verlag New York, Graduate Texts in Mathematics*, volume 41, 1990.

[AS] M. Abramovitz and I. Stegun. Handbook of mathematical functions. In *10th printing*. online, `http://people.math.sfu.ca/~cbm/aands/`.

[AS72] M. Abramovitz and I. Stegun. Handbook of mathematical functions with formulas, graphs, and mathematical tables. page 378. Courier Dover Publications, 1972.

[Bak66] A. Baker. Linear forms in the logarithms of algebraic numbers. i. In *Mathematika. A Journal of Pure and Applied Mathematics*, volume 13, pages 204–216, 1966.

[BF04] J.H. Bruinier and J. Funke. On two geometric theta lifts. volume 1, pages 45–90. Duke Math J., 2004.

[BFK14] K. Bringmann, K.H. Fricke, and Z. Kent. Special l-values and periods of weakly holomorphic modular forms. In *Proc. AMS*, volume 142, pages 3425–3439, 2014.

[BFOR17] K. Bringmann, A. Folsom, K. Ono, and L. Rolen. Harmonic maass forms. In *AMS Colloquium Series*, 2017.

[BGKO13] K. Bringmann, P. Guerzhoy, Z. Kent, and K. Ono. Eichler shimura theory for mock modular forms. In *Mathematische Annalen*, volume 355, pages 1085–1121, 2013.

[BH08] V. Blomer and G Harcos. The spectral decomposition of shifted convolution sums. volume 144, pages 321–339. Duke Math. J., 2008.

[BH10] V. Blomer and G Harcos. Twisted l-functions over number fields and hilbert's eleventh problem. volume 20, pages 1–52. Geom. Funct. Anal., 2010.

[BHM07] V. Blomer, G. Harcos, and P. Michel. A burgess-like subconvex bound for twisted l-functions (with appendix 2 by z. mao). volume 19, pages 61–105. Forum Math., 2007.

[Blo04] V. Blomer. Shifted convolution sums and subconvexity bounds for automorphic l-functions. volume 73, pages 3905–3926. Int. Math. Res. Notes, 2004.

[BO13] J. Bruinier and K. Ono. Algebraic formulas for the coefficients of half-integral weight harmonic weak maass forms. In *Adv. in Math.*, volume 246, pages 198–219, 2013.

[BO16] C. Bessenrodt and K. Ono. Maximal multiplative properties of partitions. In *Annals of Combinatorics*, volume 20, pages 59–64, 2016.

[Bor98] R.E. Borcherds. Automorphic forms with singularities on grassmanians. volume 132, pages 491–562. Invent. Math., 1998.

[Bye12] D. Byeon. Indivisibility of class numbers and iwasawa invariants of real quadratic fields. In *J. Num. Theory*, volume 132, pages 3029–3036, 2012.

[CKM+17] H. Cohn, A. Kumar, S.D. Miller, D. Radchenko, and M. Viazovska. The sphere packing problem in dimension 24. volume 185, pages 1017 – 1033. Annals of Mathematics, 2017.

[CL84] H. Cohen and H.W. Lenstra. Heuristics on class groups of number fields. In *Springer Lect. Notes in Math.*, volume 1068, pages 33–62, 1984.

[Coh93] H. Cohen. A course in computational number theory. In *Springer-Verlag Berlin Heidelberg*, pages 1–536, 1993.

[Cox97] D. Cox. Primes of the form $x^2 + ny^2$. In *Wiley-Interscience*, pages 1–368, 1997.

[DFI93] W. Duke, D.B. Friedlander, and H. Iwaniec. Bounds for automorphic l-functions. volume 112, pages 1–8. Invent. Math., 1993.

[DH71] H. Davenport and H. Heilbronn. On the density of the discriminants of cubic fields, ii. In *Proc. Roy. Soc. London A*, volume 322, pages 405–420, 1971.

[DS05a] N. Dartyge and A. Sarkozy. Arithmetic properties of summands of partitions. ii. In *Ramanujan J.*, volume 10, pages 383–394, 2005.

[DS05b] F. Diamon and J. Shurman. A first course in modular forms. In *Springer-Verlag New York, Graduate Texts in Mathematics*, volume 228, 2005.

[DSS05] N. Dartyge, A. Sarkozy, and M. Szalay. On the distribution of the summands of partitions in residue classes. In *Acta Math. Hungar.*, volume 109, pages 215–237, 2005.

[DSS06] N. Dartyge, A. Sarkozy, and M. Szalay. On the distribution of the summands of unequal partitions in residue classes. In *Acta Math. Hungar.*, volume 110, pages 323–335, 2006.

[EL41] P. Erdös and J. Lehner. The distribution of the number of summands in the partitions of a postive integer. In *Duke Math Journal*, volume 8, pages 335–345, 1941.

[Fre88] G. Frey. On the selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points. In *Canad. J. Math.*, volume 15, pages 449–655, 1988.

[Gol85] D. Goldfeld. Gauss' class number problem for imaginary quadratic fields. In *Bulletin of the AMS*, volume 13, pages 23–37, 1985.

[GZ86] B.H. Gross and D. Zagier. Heegner points and derivatives of l-series. In *Invent. Math.*, volume 84, pages 225–320, 1986.

[Hag71] P. Hagis. Partitions with a restriction on the multiplicity of the summands. In *Trans. Amer. Math. Soc*, volume 155, pages 375–384, 1971.

[Har03] G. Harcos. An additive problem in the fourier coefficients of cusp forms. volume 326, pages 347–365. Math. Ann., 2003.

[Har14] G. Harcos. Twisted hilbert modular l-functions and spectral theory. In *Adv. Lect. Math.*, volume 30, pages 49–67, 2014.

[Hee52] K. Heegner. Diophantische analysis und modulfunktionen. In *Math. Z*, volume 56, pages 227–253, 1952.

[Hei34] H. Heilbronn. On the class number in imaginary quadratic fields. In *Quart. J. Math. Oxford Ser. 2*, volume 5, pages 150–160, 1934.

[HH16] J. Hoffstein and T.A. Hulse. Multiple dirichlet series and shifted convolutions. In *J. of Number Theory*, volume 162, pages 255–274, 2016.

[HN88] K. Horie and J. Nakagawa. Elliptic curves with no torsion points. In *Proc. A.M.S.*, volume 104, pages 20–25, 1988.

[HR18] G.H. Hardy and S. Ramanujan. Asymptotic formulae in combinatory analysis. In *Proc. London Math. Soc.*, volume 17, pages 75–115, 1918.

[HW08] G.H. Hardy and E.M. Wright. An introduction to the theory of numbers. volume 6. Oxford Press, 2008.

[IRR14] Ö Imamoglu, M. Raum, and O. Richter. Holomorphic projections and ramanujan's mock theta functions. In *Proc. Nat. Acad. Sci. U.S.A.*, volume 111.11, pages 3961–3967, 2014.

[Iwa97] H. Iwaniec. Topics in classical automorphic forms. In *Trans. Amer. Math. Soc*, 1997.

[Jam98] K. James. l-series with nonzero central critical value. In *J. AMS*, volume 11, pages 635–691, 1998.

[KL17] D. Kriz and C. Li. Goldfeld's conjecture and congruenes between heegner points. 2017.

[KO99] W. Kohnen and K. Ono. Indivisibility of class numbers of imaginary quadratic fields and orders tate-shafarevich groups of elliptic curves with complex multiplication. In *Inventiones Mathematicae*, volume 135, pages 387–398, 1999.

[Kob93] N. Koblitz. Introduction to elliptic curves and modular forms. Springer-Verlag, Edition 2, 1993.

[Kol89a] V. Kolyvagin. Finiteness of $e(\mathbb{Q})$ and shafarevich-tate groups for a subclass of weil curves. In *Math USSR-Izv.*, volume 32, pages 523–541, 1989.

[Kol89b] V. Kolyvagin. Finiteness of mordell-weil and shafarevich-tate groups for weil elliptic curves. In *Math USSR-Izv.*, volume 33, pages 473–499, 1989.

[KZ84] W. Kohnen and D. Zagier. Modular forms with rational periods. In *Ellis Horwood Ser. Math. Applr.:Statist. Oper. Res. Horwood Chichester*, pages 197–249, 1984.

[Lam01] V. Lampret. The euler-maclaurin and taylor formulas: Twin, elementary derivations. In *Math. Mag.*, volume 74, pages 109–122, 2001.

[Leh38] D. Lehmer. On the series for the partition. In *Trans. Amer. Math. Soc*, volume 43, pages 271–395, 1938.

[Mag13] P. Maga. Subconvexity and shifted convolution sums over number fields. In *PhD Thesis*, page 89. Central European University, 2013.

[Magar] P. Maga. Shifted convolution sums and burgess type convexity over number fields. In *J. Reine Angew. Math.*, to appear.

[Map] Maple. Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

[Mer] M. Mertens. Eichler-selberg type identities for mixed modular forms. In *Advances in Mathematics*.

[MO16] M. Mertens and K. Ono. Special values of shifted convolution dirichlet series. In *Mathematika*, volume 62, pages 47–66, 2016.

[NR] T.H. Ngo and R.C. Rhoades. Integer partitions, probabilities and quantum modular forms. preprint, available at `http://math.stanford.edu/~rhoades/RESEARCH/papers.html`.

[OLBC10] F.W.J. Olver, D. W. Lozier, R.F. Boisvert, and C.W. Clark. Nist handbook of mathematical functions. In *Print companion to NIST*. Cambridge University Press, New York, NY, 2010.

[Ono00] K. Ono. The web of modularity: arithmetic of the coefficients of modular forms and q-series. AMS, 2000.

[Ono09] K. Ono. Unearthing the visions of a master: harmonic maass forms and number theory. In *Somerville, MA*, pages 347–454. Proceedings of the 2008 Harvard-MIT Current Developments in Mathematics Conference, 2009.

[OS98] K. Ono and C. Skinner. Nonvanishing of quadratic twists of modular l-functions. In *Inventiones Mathematicae*, volume 134, pages 651–660, 1998.

[PP97] A. Perelli and J. Pomykala. Averages of twisted l-functions. In *Acta Arithmetica*, pages 149–163, 1997.

[Rad37] H. Rademacher. On the partition function $p(n)$. volume 43, pages 241–254. Proc. London Math. Soc., 1937.

[S+14] W.A. Stein et al. Sage Mathematics Software. The Sage Development Team, 2014. `http://www.sagemath.org`.

[Sal33] H. Salie. Zur abscätzung der fourierkoeffizenten ganzer modulformen. In *Math. Z.*, volume 36, pages 263–278, 1933.

[Sel65] A. Selberg. On the estimation of fourier coefficients of modular forms. In *Proc. Sympos. Pure Math. Vol VIII*, pages 1–15, 1965.

[Sie35] C. Siegel. Über die classenzahl quadratischer zahlkörper. In *Acta Arithmetica*, volume 1, pages 83–86, 1935.

[Sil86] J. Silverman. The arithmetic of elliptic curves. page 513 p. Springer, 1986.

[Sou00] K. Soundararajan. Divisibility of class numbers of imaginary quadratic fields. In *J. London Math Soc.*, volume 61, pages 681–690, 2000.

[Sta67] H.M. Stark. A complete determination of the complex quadratic fields of class number one. volume 14, pages 1–27. Michigan Math. J., 1967.

[Stu80] J. Sturm. Projections of c^∞ automorphic forms. In *Bull. Amer. Math. Soc.*, volume 2, pages 435 – 439, 1980.

[Vat98] V. Vatsal. Rank-one twists of a certain elliptic curve. In *Math. Ann.*, volume 311, pages 791–794, 1998.

[Via17] M. Viazovska. The sphere packing problem in dimension 8. In *Ann. Math.*, volume 185, pages 991–1015, 2017.

[Wil15] A. Wiles. On class groups of imaginary quadratic fields. In *J. London Math. Soc. (2)*, volume 92, pages 411–426, 2015.

[Wri71] E. M. Wright. Stack ii. volume 22, pages 107–116. Quart. J. Math. Oxford Ser., 1971.

[Zag75] D. Zagier. Nombres de classes et formes modulaires do poids 3/2. In *C.R. Acad. Sci. Paris (A)*, volume 281, pages 883–886, 1975.