IMPERIAL

Imperial College London

Department of Mathematics

MSci Research Project

Viazovska’s Magic Function in Dimension 8: A Formalisation in Lean

Author:
Sidharth Hariharan

Supervisor(s):
Bhavik Mehta

Submitted in partial fulfillment of the requirements for the MSci in Mathematics at Imperial College London

June 8, 2025

Abstract

Hi

Acknowledgments

Plagiarism statement

The work contained in this thesis is my own work unless otherwise stated.

Signature: Sidharth Hariharan
Date: June 8, 2025

Contents

Chapter 1

Introduction

On 5 July, 2022, in Helsinki, Finland, the International Mathematical Union announced the names of the four mathematicians who were to be awarded the Fields Medal, the most coveted prize in the world of mathematics: Hugo Duminil-Copin, June Huh, James Maynard and Maryna Viazovska. Duminil-Copin, Huh and Maynard received this most prestigious honour for making several outstanding contributions to their specific fields of expertise—respectively, statistical physics, geometric combinatorics, and analytic number theory. Viazovska, on the other hand, was awarded the Fields Medal for a distinct, outstanding conceptual brilliancy: proving the optimality of the E_8 sphere packings in $\mathbb{R}^8$. Her solution [1] exploited the myriad symmetries of the theory of modular forms to construct a special function—the so-called Magic Function—that, in combination with a previous result by Cohn and Elkies, solves the problem. Very shortly afterwards, Cohn, Kumar, Miller, Radchenko and Viazovska were able to use similar ideas to prove that the Leech lattice packing is the densest possible sphere packing in $\mathbb{R}^{24}$ [2].

Before Viazovska's remarkable breakthrough, the optimal sphere packing density was only known in dimensions 1, 2 and 3 [3]. Furthermore, Thomas Hales' solution in dimension 3 [4] was lengthy and involved extensive computer-assisted calculations. In contrast, Viazovska's proof in dimension 8 is elegant and concise. Even before Viazovska was awarded the Fields Medal, her work received wide acclaim from eminent mathematicians across the world: Peter Sarnak described it as "stunningly simple, as all great things are," and Akshay Venkatesh remarked that her Magic Function is very likely "part of some richer story" that connects to other areas of mathematics and physics [5]. Viazovska's work is a truly remarkable achievement in modern mathematics, with its elegance coming from the manner in which the many pieces of the puzzle fit perfectly together. In this project, we offer a detailed exposition of one of those pieces—namely, the construction of the so-called 'Magic Function'—and discuss current progress in formalising Viazovska's breakthrough in the Lean Theorem Prover.

1.1 The Sphere Packing Problem

The Sphere Packing problem is a classical optimisation problem in mathematics. It goes as follows.

Problem 1.1.1 (The Sphere Packing Problem in Dimensinon n). *For some $n \in \mathbb{N}$, what is the densest non-overlapping arrangement of n-spheres of equal radius in $\mathbb{R}^n$?*

Despite its straightforward formulation, Problem 1.1.1 is notoriously difficult to solve. A key challenge in high dimensions is the fact that proceeding inductively is not always helpful: 'stacking' the optimal n-dimensional sphere packing onto itself is not guaranteed to yield the optimal sphere packing in $n+1$ dimensions [3]. In fact, this appraoch is known to fail in dimensions as low as 10 [6]. This is not obvious, not least because the approach does, in fact, succeed in the visualisable dimensions of 1, 2 and 3.

The 1-dimensional case is uninteresting. Visually, one can easily see that the densest possible arrangement of disjoint intervals of the form $(-r, r)$ on the real line consists of intervals centred at all points $2rm$ for $m \in \mathbb{Z}$. Indeed, one can fix r to be $\frac{1}{2}$ by rescaling the real line. The optimal packing therefore consists of open intervals of unit length centred at points on the lattice $\mathbb{Z} \subset \mathbb{R}$.

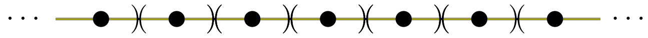
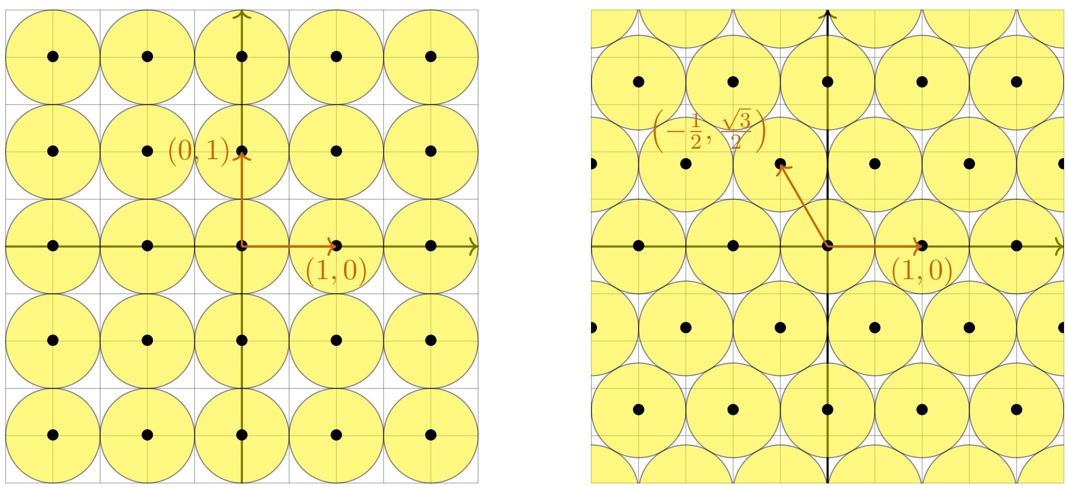


Figure 1.1: The $\mathbb{Z}$ lattice packing in dimension 1.

In dimension 2, Problem 1.1.1, also known as the circle packing problem, turns out to be more interesting. A reasonable strategy for finding the densest packing is to 'stack' the $\mathbb{Z}$ lattice packing from dimension 1 onto itself in some manner, turning these intervals into circles of the same radius. The question remains how to do this optimally.

One natural way of doing this is to stack the circles on top of themselves, turning $\mathbb{Z}$ into the lattice $\mathbb{Z}^2$, where circles are centred at points with integer coordinates: see Figure 1.2a. Unfortunately, this packing turns out to be sub-optimal. A better candidate is the A_2 lattice packing: see Figure 1.2b. This packing is sometimes referred to as the *honeycomb packing* due to the fact that every circle has six neighbours, whose centres form the vertices of a regular hexagon.

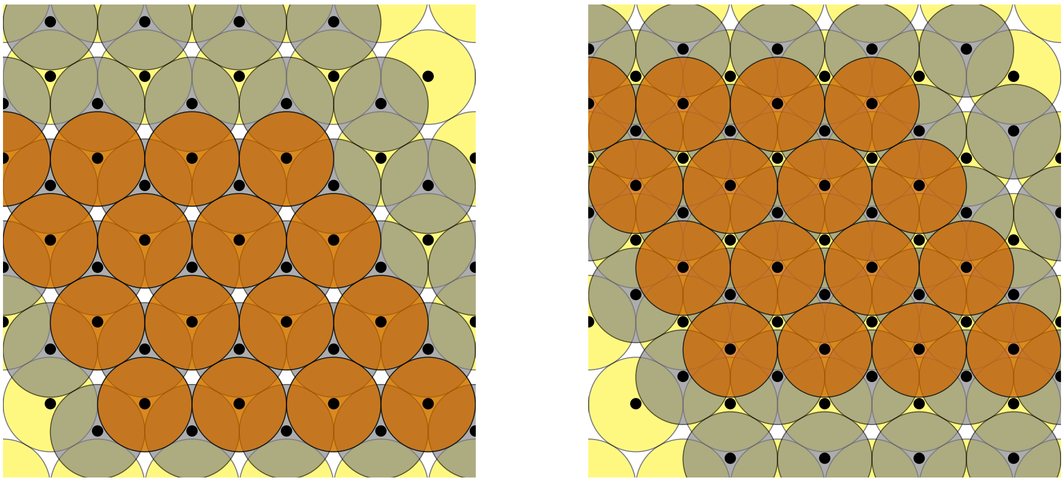
It is well-known that the honeycomb packing is optimal in $\mathbb{R}^2$. The original proof of this fact is attributed to Thue [7], but there are many proofs in the literature. One is outlined by Hales in [8, p. 442]. An intuitive way of convincing oneself of Thue's theorem is that it is not possible for a circle in a given row to be in contact with more than 2 circles in the rows above and below, meaning the A_2 packing cannot be improved. See Figure 1.3a.



(a) The $\mathbb{Z}^2$ lattice packing. **(b)** The A_2 lattice packing.

Figure 1.2: Circle packings covering the square $\{(x, y) \subset \mathbb{R}^2 \mid -2.5 \leq x, y \leq 2.5\}$.

In dimension 3, too, it is tempting to replicate this strategy: we can stack the A_2 packing on top of itself, in layers instead of rows, attempting to maximise the number of neighbours of a



(a) (b)

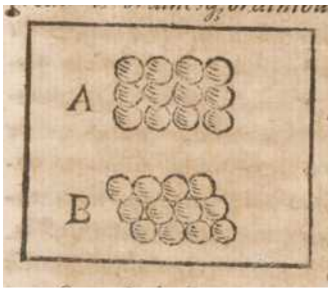
Figure 1.4: Two different ways of stacking the honeycomb packing on itself.

sphere. From trial and error, we see that a sphere cannot be in contact with more than three neighbours from the layer below. This suggests that the optimal sphere packing in dimension 3 is given by stacking honeycomb arrangements on top of each other with spheres in each layer being nestled in the gaps between three spheres in the layer below.

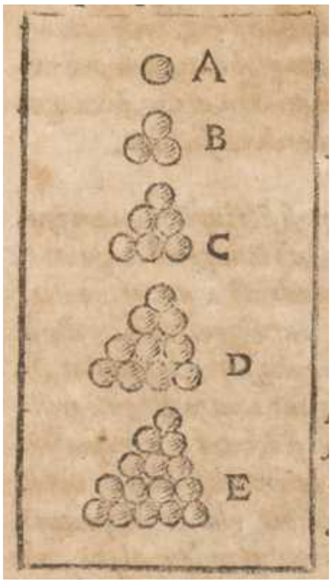
As it turns out, unlike dimension 2, this characterisation not describe a unique packing: spheres are simply too large! See Figure 1.4. One can construct infinitely many locally similar, globally different sphere packings in $\mathbb{R}^3$, all of which are as dense as possible, by varying how successive layers are placed.

This observation is not novel. In a 1611 essay whose title has been translated from Latin as *The Six-Cornered Snowflake* [9], Johannes Kepler asserted that spheres cannot be more tightly packed together than they are in a tetrahedral arrangement: see Figure 1.3b. This result became known as the Kepler Conjecture, and it went unproven for over three centuries, until 2005 that a paper proving it, written by Thomas Hales, was published [4].

The complexity of the sphere packing problem in dimension 3 is illustrated not only by the time elapsed between Kepler's original assertion and a proof being published but also by the length of Hales's paper. Indeed, in an expository account of his proof published in 2000, five years before the publication of the full paper in the Annals, Hales recounted how a jury of twelve referees, despite having been in deliberation for over a year, had yet to make a "thorough, independent check of the computer code" he had written to perform the elaborate calculations on which "every aspect of [his proof] is based" [8]. In January 2003, at the Joint Math Meetings in Baltimore, USA, Hales announced that he intended to formally verify his proof [10], in what he termed the Flyspeck project. The paper authored by Hales and his collaborators on their successful formalisation of his argument was only published in 2017. Therefore, not only did the Kepler Conjecture take close to 400 years to solve, but



(a)



(b)

Figure 1.3: Diagrams from an essay written by Johannes Kepler in Latin in 1611 [9].

it took nearly two decades to eliminate any doubt as to the correctness of the solution. This project aims to formalise a result of a similar flavour in a significantly shorter timeframe.

1.2 The Formalisation Movement

While Hales announced his intent to formally verify his proof of the Kepler Conjecture in 2003, it was not till 2006, after Hales's solution appeared in the *Annals*, that a formal description of Hales's formalisation project was published. Of his motivations, Hales wrote:

> *In response to the lingering doubt about the correctness of the proof, at the beginning of 2003, I launched the* Flyspeck *project, whose aim is a complete formal verification of the Kepler Conjecture. In truth, my motivations for the project are far more complex than a simple hope of removing residual doubt from the minds of few referees. Indeed, I see formal methods as fundamental to the long-term growth of mathematics.* [11]

Formal theorem proving was not unheard of in 2006. Interactive theorem provers, such as Coq and PRL, have existed since the 1980s. However, it was a relatively young field, and the amount of mathematics that had been formalised was limited. Hales's project was immensely ambitious, and the fact that it succeeded, despite taking over a decade, is impressive.

There is something prophetic about Hales's "far more complex" motivations for launching the Flyspeck project. The field of formal theorem proving has grown rapidly in the last decade, and interactive theorem provers like Lean are slowly making their way into mainstream mathematics. An excellent example of this is the formal verification of Gowers, Green, Manners and Tao's proof of Marton's Conjecture [12], which was formally verified in Lean in just three weeks. In particular, their proof was formally verified *before* their paper was submitted for publication. The paper appeared in the *Annals* in March 2025.

While this project has its similarities to Flyspeck, the objectives are slightly different. There is significant consensus in the mathematical community as to the correctness of Viazovska's result, and suspicions that E_8 is optimal in $\mathbb{R}^8$ existed long before her paper was published. The project is instead a challenge to the formalisation community—an attempt to push the capabilities of modern interactive theorem proving by formalising a Fields Medal-winning result mere years after its publication and sooner still after it was given this most prestigious recognition. While cutting-edge mathematics has been formalised [13] previously, formalising a result of the prestige, nuance, and beauty of Viazovska's would be a landmark achievement.

Associated to this project are a blueprint [14] and a GitHub repository. The first version of the blueprint was written by Viazovska herself, and read as a more detailed version of the original paper. Sections of the blueprint have been modified by Birkbeck, Hariharan, Lee and Ma, but the section describing the construction of the magic function, which will be the focus of this project, remains nearly identical to Viazovska's original blueprint.

There primary purpose of a blueprint is to offer a detailed exposition of the mathematics, reflecting a vision of the proof strategies to be used in the formalisation. One objective of this project is to offer a more detailed exposition still that can serve as an improvement of the blueprint that more closely resembles the actual state of the formalisation. The project blueprint was built using the Lean blueprint software [15], which has become an important part of modern, large-scale formalisation projects in Lean. It offers two extremely useful features: linking the definitions and theorems in the exposition to those in the code, and displaying the progress of the formalisation via a dependency graph. The dependency graph is colour-coded to reflect the state of the formalisation, and we invite the interested reader to view it here.

1.3 The Scope of this Project

In November 2023, the author had the privilege of meeting Maryna Viazovska while pursuing an exchange programme at the Swiss Federal Institute of Technology, Lausanne, where she is based. A discussion soon led to the initiation of a collaboration with Christopher Birkbeck, Seewoo Lee, and Gareth Ma, with invaluable assistance from Kevin Buzzard, Utensil Song, and Patrick Massot. On 31 May 2024, Viazovska formally announced at the ICMS workshop *Formalisation of Mathematics: Workshop for Women and Mathematicians of Minority Gender* that a formalisation of her groundbreaking paper was in the works.

Viazovska's original paper [1] is divided into five sections. The first section introduces sphere packings and develops basic theory; the second discusses linear programming bounds discovered by Cohn and Elkies [16, Theorem 3.1]; the third offers some background on the theory of modular forms; the fourth constructs two radial, Schwartz Fourier eigenfunctions with double zeroes at almost all points on the E_8 lattice; and finally, the fifth uses these eigenfunctions to construct the "Magic Function", a Schwartz function that satisfies the conditions of Cohn and Elkies's theorem to give an upper bound for all sphere packings in $\mathbb{R}^8$ that is equal to the density of the E_8 packing. Significant portions of the first two sections were formalised collaboratively in July and August 2024, and the third is actively being worked on by Birkbeck and Lee. This project focuses on formalising the fourth section of Viazovska's paper. The code written for this section is primarily my own, and the author have credited the contributions of others where appropriate.

The primary objective of this thesis is to offer a mathematical exposition of the fourth section of Viazovska's original paper and explore how the choices she made over the course of her construction can be adapted in Lean. We offer an overview of the author's contributions to the formalisation and discuss successes, roadblocks, and future challenges.

Viazovska's construction is based heavily on the theory of modular forms. While we will briefly discuss this rich subject at the intersection of analysis, algebra and number theory, we will not state more than what we need to understand the construction of Viazovska's magic function in [1, §4], keeping the focus of the informal and formal aspects of this project to the author's own contributions and expository insights. Furthermore, we will not discuss any more of general sphere packing than is necessary for general understanding. While we will study Cohn and Elkies's intermediate result in some detail, we will only do so to motivate Viazovska's construction, and progress in formalising it should not be viewed as being a part of this M4R.

Apart from references in the literature, given that this M4R is part of a formalisation project, we will make free and confident use of formalised code, particularly code found in `mathlib` [17]. Such code is usually linked to in this fashion. We explicitly describe results that were not formalised by the author for the purposes of this projects as being previous formalisations, or otherwise make clear the distinction between the author's own contributions and those of others.

We end by reiterating that the formalisation is active, dynamic research. Significant developments are set to unfold immediately after the submission of this thesis, at the *Big Proof 2025: Formalising Mathematics at Scale* event at Cambridge. The author has taken every effort to ensure the contents of this thesis are up-to-date, but points the reader to the blueprint, which is public, and the GitHub Repository, which is set to be made public on 13 June, 2025, for the latest information.

Chapter 2

The Ingredients of Viazovska's Solution

The purpose of this chapter is to offer background information that will be essential to understanding the rest of this exposition. We will begin by providing precise mathematical definitions for sphere packings, densities, and the sphere packing constant. We will then discuss the variation of the linear programming bound proven by Cohn and Elkies [16, Theorem 3.1] used by Viazovska [1, Theorem 2]. Finally, we will include a small discussion on the theory of modular forms and establish its relevance to the subsequent chapters of this thesis, which will focus on the construction of the Magic Function.

We will be minimalistic in our discussions, and focus on motivating new concepts and their relevance to the sphere packing problem in dimension 8. This section is not intended to offer an exhaustive treatment of the mathematics we will encounter, which is as vast as it is rich.

2.1 Sphere Packing Fundamentals

This section is divided into two subsections. The first defines fundamental notions about general sphere packings, lattice packings and periodic packings. The third subsection studies the sphere packing of our interest: the E_8 lattice packing.

2.1.1 The General Theory of Sphere Packings

We begin by defining a sphere packing.

Definition 2.1.1 (Sphere Packing). Fix $d \in \mathbb{N}$ and $X \subset \mathbb{R}^d$. Assume that there exists a real number $r > 0$, known as the **separation radius**, such that

$$\|x - y\| \geq r$$

for all distinct $x, y \in X$. We define the **sphere packing with centres at** X to be

$$\mathcal{P}(X) := \bigcup_{x \in X} B_d(x, r)$$

The density of a sphere packing is the limit superior of an indicator of how much of a bounded region of space a sphere packing covers.

Definition 2.1.2 (Density). Let $\mathcal{P}$ be a sphere packing. Define the **density** of $\mathcal{P}$ to be

$$\Delta(\mathcal{P}) := \limsup_{R\to\infty} \frac{\mathrm{Vol}(\mathcal{P}\cap B_d(0,R))}{\mathrm{Vol}(B_d(0,R))}$$

As one might expect, finite density and density are invariant under scaling. We now define lattice and periodic packings.

Definition 2.1.3 (Lattice and Periodic Sphere Packings). A **lattice** in a Euclidean space $\mathbb{R}^n$ is a discrete $\mathbb{Z}$-submodule of $\mathbb{R}^n$ such that its $\mathbb{R}$-span contains every element in $\mathbb{R}^n$. We say a sphere packing $\mathcal{P}(X)$ is

1. a lattice packing if X is a lattice.
2. Λ-periodic if for all $\lambda \in \Lambda$ and $x \in X$, we have that $\lambda + x \in X$, where Λ is a lattice.

The periodicity property of a periodic sphere packing can be exploited to derive a more convenient formula for its density.

Proposition 2.1.4. *Let $\mathcal{P}(X)$ be a sphere packing with centres at $X \subset \mathbb{R}^d$ and separation r that is periodic with respect to some lattice $\Lambda \subset \mathbb{R}^d$. We have that*

$$\Delta_{\mathcal{P}(X)} = \left|{}^{X}\!/_{\Lambda}\right| \frac{\mathrm{Vol}\left(B_d(0,\frac{r}{2})\right)}{\mathrm{Vol}\left({}^{\mathbb{R}^d}\!/_{\Lambda}\right)} \tag{2.1.1}$$

where $\left|{}^{X}\!/_{\Lambda}\right|$ is the number of orbits of the additive Λ-action on X and $\mathrm{Vol}\left({}^{\mathbb{R}^d}\!/_{\Lambda}\right)$ is the volume of the fundamental domain of the Λ-action on $\mathbb{R}^d$.

Interestingly, one can show that the supremum of densities taken over all sphere packings in $\mathbb{R}^n$ is the same as the supremum taken over all periodic packings in $\mathbb{R}^n$. A proof can be found in [16, Appendix A]. We denote this quantity by Δ_n, n being the dimension of the ambient space.

We will end by defining dual lattices. Viewing a lattice in $\mathbb{R}^d$ as a free $\mathbb{Z}$-submodule of $\mathbb{R}^d$, we can view its dual lattice as the corresponding submodule of $(\mathbb{R}^d)^*$. We offer a slightly more convenient definition.

Definition 2.1.5 (Dual Lattice). Fix $d > 0$ and let $\Lambda \subset \mathbb{R}^d$ be a lattice. We define the **dual lattice** of Λ to be

$$\Lambda^* := \left\{ y \in \mathbb{R}^d \;\middle|\; \langle x, y\rangle \in \mathbb{Z} \text{ for all } x \in \Lambda \right\}$$

We are now ready to discuss a special sphere packing in $\mathbb{R}^8$: the E_8 sphere packing.

2.1.2 The E_8 Lattice Packing

It is quite remarkable that E_8 should show up when discussing sphere packings. At its core, E_8 is an irreducible root system. It shows up in the classification of important classes of objects like irreducible Coxeter groups, crystallographic Coxeter groups, and semi-simple Lie algebras over $\mathbb{C}$. E_8 is not a classical root system but an *exceptional* root system, meaning that the geometric properties of its roots cannot be found in irreducible root systems in all dimensions.

The E_8 root system consists of 240 vectors in $\mathbb{R}^8$ that are permuted by a certain finite subgroup of the 8-dimensional orthogonal group. This group is sometimes referred to as the E_8 Coxeter group or as the Weyl group of the E_8 lattice. These roots can be divided into 8 orbits, each of which corresponds to one of the 'layers' of concentric circles in Figure 2.1. The dots in the figure correspond to projections of the roots onto a plane on which a specific type of element of the Coxeter group, known as a Coxeter element, acts as a rotation. This visualisation offers a convenient—and aesthetically pleasing—means of visualising this collection of 8-dimensional vectors and appreciating some of its symmetry.

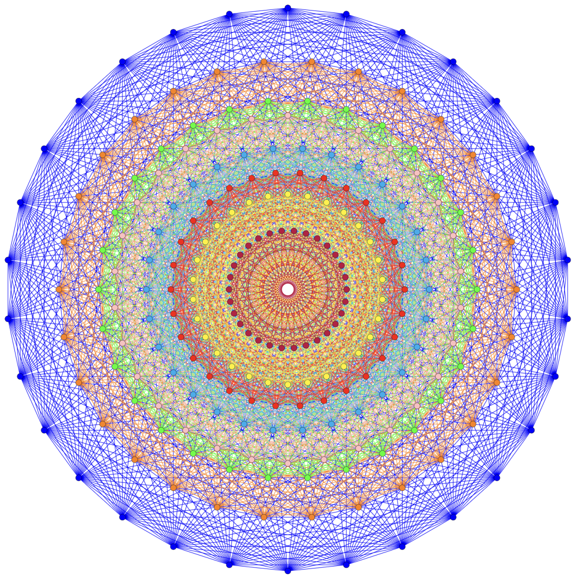


Figure 2.1: The Coxeter projection of the E_8 root system. [18]

The E_8 lattice is characterised in many ways. One is as the $\mathbb{Z}$-span of the so-called *simple roots* of the E_8 root system, the simple roots being a distinguished basis of $\mathbb{R}^8$ that is contained in the E_8 root system. Another is that up to isomorphism, the E_8 lattice is the unique positive-definite, even, unimodular lattice in $\mathbb{R}^8$. We instead give the following explicit definition of the E_8 lattice, which we attempted to reconcile with the '`Zspan`' characterisation in Lean.

Definition 2.1.6 (The E_8 Lattice). The E_8 lattice consists of all vectors in $\mathbb{R}^8$ such that either all coordinates are integers or all coordinates are half-integers and the sum of all coordinates is even. That is,

$$\Lambda_8 := \left\{ (x_1, \ldots, x_8) \in \mathbb{Z}^8 \cup \left(\mathbb{Z} + \frac{1}{2}\right)^8 \;\middle|\; \sum_{i=1}^{8} x_i \equiv 0 \pmod 2 \right\}$$

For the construction of the magic function, we will primarily rely on the following facts.

Proposition 2.1.7 (Properties of the E_8 Lattice). *The following are true of the E_8 lattice.*

1. *For all $x, y \in \Lambda_8$, $\|x - y\| \geq \sqrt{2}$.*
2. *The density of the sphere packing centred at points in Λ_8 with separation $\sqrt{2}$ is*

$$\frac{\pi^4}{384} \approx 0.2536695$$

3. *The elements of Λ_8 all have norm $\sqrt{2n}$ for some $n \in \mathbb{N}$.*
4. *The dual lattice of Λ_8 is Λ_8.*
5. *The covolume of Λ_8 is 1. Ie, $\mathrm{Vol}\left(\mathbb{R}^8 / \Lambda_8\right) = 1$.*

The sphere packing to which we refer in the second point of the above theorem is precisely the E_8 sphere packing. We are now ready to examine Cohn and Elkies's groundbreaking intermediate result that Viazovska uses to construct her Magic Function.

2.2 The Cohn-Elkies Linear Programming Bounds

The linear programming bounds constructed by Henry Cohn and Noam Elkies was a profound and powerful discovery that transformed the inherently geometric sphere packing problem into an analytic one. For all $d \in \mathbb{N}$, it posits the existence of a family of upper-bounds on the sphere packing constant Δ_d, indexed by functions $f : \mathbb{R}^d \to \mathbb{R}$ that satisfy certain conditions. Solving the sphere packing problem then amounts to finding a function such that the corresponding upper-bound on sphere packing densities is exactly the density of a known sphere packing.

Cohn and Elkies's result depends directly on the **Poisson Summation Formula over Lattices**. The formula, and hence, Cohn and Elkies's linear programming bound, deals with a special class of functions, a subset of which will be of interest to us. This subset consists of smooth, rapidly decaying functions first described by Laurent Schwartz in his book *Théorie des Distributions* [19, Ch VII, §3] and since named after him. Such functions are particularly well-behaved under the Fourier transform. We say a few words about Fourier transforms before discussing the Poisson Summation Formula and the Cohn-Elkies Linear Programming Bound in detail.

2.2.1 Fourier Transforms and the Poisson Summation Formula

The subject of Fourier analysis is deep, and has applications to a number of areas in pure and applied mathematics. There are deeper undertones to the role of the Fourier transform in Viazovska's proof of the optimality of the E_8 lattice packing in $\mathbb{R}^8$: much of the underlying motivation comes from broader Fourier interpolation results that are beyond the scope of this thesis and this formalisation project. In this subsection, we merely define the Fourier transform and its inverse. We will also very briefly discuss the formalisation of these definitions in Lean.

We begin by defining the Fourier transform of a function.

Definition 2.2.1 (Fourier Transform). Fix $m, n \in \mathbb{N}$ and let $f : \mathbb{R}^m \to \mathbb{C}^n$. We define the **Fourier transform** of f to be the function

$$\mathcal{F}(f) : \mathbb{R}^m \to \mathbb{C}^n : \xi \mapsto \int_{\mathbb{R}^d} f(x)\, e^{-2\pi i \langle x, \xi \rangle}\, \mathrm{d}x$$

We adopt the following alternative notation for the Fourier transform, in line with general literature as well as Viazovska's original paper. We will use both notations interchangeably.

Notation. We denote the Fourier transform $\mathcal{F}(f)$ of a function f by $\widehat{f}$.

We can also define the inverse Fourier transform.

Definition 2.2.2 (Inverse Fourier Transform). Fix $m, n \in \mathbb{N}$ and let $f : \mathbb{R}^m \to \mathbb{C}^n$ be an L^1 function. We define the **inverse Fourier transform** of f to be the function

$$\mathcal{F}^{-1}(f) : \mathbb{R}^m \to \mathbb{C}^n : x \mapsto \int_{\mathbb{R}^d} f(\xi)\, e^{2\pi i \langle x, \xi \rangle}\, \mathrm{d}\xi$$

Confusingly, the inverse Fourier transform is not always the inverse of the Fourier transform. For instance, the Fourier integral may not converge. For integrable functions with integrable Fourier transforms, though, the inverse Fourier transform does invert the Fourier transform. Regardless, we have the following result, which has been previously formalised in `mathlib`.

Lemma 2.2.3. *For all $m, n \in \mathbb{N}$ and $f : \mathbb{R}^m \to \mathbb{C}^n$,*

$$\mathcal{F}^{-1}(f)(x) = \mathcal{F}(f)(-x)$$

We can now state the Poisson Summation Formula. Here, Λ^* is as in Definition 2.1.5.

Theorem 2.2.4 (Poisson Summation Formula over Lattices). *Let $d > 0$ and let $\Lambda \subset \mathbb{R}^d$ be a lattice. Let $f : \mathbb{R}^d \to \mathbb{R}$ be a Schwartz function. For all vectors $v \in \mathbb{R}^d$, we have*

$$\sum_{\ell \in \Lambda} f(\ell + v) = \frac{1}{\mathrm{Vol}\left(\mathbb{R}^d / \Lambda\right)} \sum_{m \in \Lambda^*} \widehat{f}(y) e^{-2\pi i \langle v, m \rangle}$$

Variants of this classical result and its proof can be found in several sources, such as [20, Chapter VII, §6, Proposition 15] and [19, Chapter VII, §7, Equation (VII, 7:5)]. While it has been stated in Lean, it has not been proven yet for lattices other than $\mathbb{Z} \subset \mathbb{R}$ due to a multitude of challenges associated with generalising the argument to higher dimensions.

Armed with this important result, we are ready to state and prove the Cohn-Elkies Linear Programming Bound for Schwartz functions.

2.2.2 The Cohn-Elkies Linear Programming Bound

We now state the most important intermediate result in the proof of the optimality of the E_8 lattice packing in $\mathbb{R}^8$.

Theorem 2.2.5 (Cohn and Elkies, 2003 [16, Theorem 3.1]). *If $f : \mathbb{R}^d \to \mathbb{R}$ is a Schwartz function satisfying the conditions*

(CE1) *f is not identically zero.*

(CE2) *For all $x \in \mathbb{R}^d$, if $\|x\| \geq 1$ then $f(x) \leq 0$.*

(CE3) *For all $x \in \mathbb{R}^d$, $\widehat{f}(x) \geq 0$.*

then we have the following bound on the sphere packing constant Δ_d:

$$\Delta_d \leq \frac{f(0)}{\widehat{f}(0)} \cdot \mathrm{Vol}\left(B_d\left(0, \frac{1}{2}\right)\right)$$

Proof. Let $f : \mathbb{R}^d \to \mathbb{R}$ be a Schwartz function satisfying the conditions (CE1)-(CE3). Fix a sphere packing $\mathcal{P}$. Without loss of generality, we may assume that $\mathcal{P}$ is periodic with respect to some lattice Λ and has separation radius 1. Denote the set of centres of $\mathcal{P}$ by X. By Proposition 2.1.4, we need to show that

$$\frac{\left| X / \Lambda \right|}{\mathrm{Vol}\left(\mathbb{R}^d / \Lambda\right)} \cdot \mathrm{Vol}\left(B_d\left(0, \frac{1}{2}\right)\right) \leq \frac{f(0)}{\widehat{f}(0)} \cdot \mathrm{Vol}\left(B_d\left(0, \frac{1}{2}\right)\right) \tag{2.2.1}$$

It turns out to be easier to show the equivalent inequality

$$\frac{\left|X/\Lambda\right|^2}{\mathrm{Vol}\left(\mathbb{R}^d/\Lambda\right)} \cdot \widehat{f}(0) \leq \left|X/\Lambda\right| \cdot f(0) \tag{2.2.2}$$

Applying (CE2) to our assumption that $\|x - y\| \geq 1$ for all distinct $x, y \in X$, one can show that

$$\left|X/\Lambda\right| \cdot f(0) \geq \sum_{x \in X} \sum_{y \in X/\Lambda} f(x - y) \tag{2.2.3}$$

Applying Theorem 2.2.4, we can show that

$$\sum_{x \in X} \sum_{y \in X/\Lambda} f(x - y) = \frac{1}{\mathrm{Vol}\left(\mathbb{R}^d/\Lambda\right)} \sum_{m \in \Lambda^*} \widehat{f}(m) \cdot \left| \sum_{x \in X/\Lambda} e^{2\pi i \langle x, m \rangle} \right|^2$$

(CE3) tells us this is a sum of non-negative real numbers. We can therefore bound this sum below by the term corresponding to $m = 0$. Therefore,

$$\begin{aligned} \frac{1}{\mathrm{Vol}\left(\mathbb{R}^d/\Lambda\right)} \sum_{m \in \Lambda^*} \widehat{f}(m) \cdot \left| \sum_{x \in X/\Lambda} e^{2\pi i \langle x, m \rangle} \right|^2 &\geq \frac{1}{\mathrm{Vol}\left(\mathbb{R}^d/\Lambda\right)} \widehat{f}(0) \cdot \left| \sum_{x \in X/\Lambda} e^{2\pi i \langle x, 0 \rangle} \right|^2 \\ &= \frac{\left|X/\Lambda\right|^2}{\mathrm{Vol}\left(\mathbb{R}^d/\Lambda\right)} \cdot \widehat{f}(0) \end{aligned} \tag{2.2.4}$$

Putting these computations together gives us the desired result. □

While the formalisation of Theorem 2.2.5 is beyond the scope of this thesis, the details we have included will give us important conditions that the magic function should obey. We will revisit this argument in Section 3.2.

We are now ready to discuss a key ingredient in the construction of the magic function: the theory of modular forms. Since much of the theory is beyond the scope of this thesis, we will not venture too far beyond the fundamentals.

2.3 A Word on Modular Forms

The theory of modular forms is a rich subject lying at the intersection of complex analysis, algebra and number theory. Among other things, it describes symmetries and relations between an important and well-behaved class of functions and gives us algebraic ways of manipulating and composing these relations. In Section 3.3, we discuss why this is useful for Viazovska's argument. The primary reference for the contents of this section is [21, Chapter 1].

Several results in the theory of modular forms have been formalised by Birkbeck, Loeffler and others, and a significant portion of their work has been merged into `mathlib`. Definitions and results from this section that pertain to Viazovska's solution to the sphere packing problem in $\mathbb{R}^8$ that do not feature in `mathlib` are being actively formalised by Birkbeck and Lee. We freely reference previously formalised code and provide links.

First, we introduce the following useful notation, which corresponds to `mathlib` notation.

Notation. For the remainder of this paper, denote the Complex upper half-plane by $\mathbb{H}$. That is, define $\mathbb{H} := \{z \in \mathbb{C} \mid 0 < \operatorname{Im}(z)\}$.

A key motivating idea in the study of modular forms is the study of the action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathbb{H}$ by Möbius transformations via

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

That matrix multiplication corresponds to the composition of Möbius transformations is a well-known fact in Complex Analysis. One can hence show that the above is indeed a group action. In essence, a modular form is a holomorphic $\mathbb{H} \to \mathbb{C}$ function that exhibits some invariance under composition with this action.

A modular form is usually described using a *weight* and a *level*. The *weight* can be thought of as the *extent* of its invariance, that is, the amount of correction needed after composition with the $\mathrm{SL}(2,\mathbb{Z})$-action. The *level* can be thought of as the *scope* of its invariance, that is, it describes the elements of $\mathrm{SL}(2,\mathbb{Z})$ under composition with which we have invariance. The composition itself is described using *slash actions*, which are defined below.

Definition 2.3.1 (Automorphy Factors and Slash Actions). Fix $k \in \mathbb{Z}$, $z \in \mathbb{H}$ and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. Define the **automorphy factor of weight** k to be

$$j_k(z,\gamma) := (cz+d)^{-k} \tag{2.3.1}$$

For any function $f : \mathbb{H} \to \mathbb{C}$, with k and γ as above, the **slash operator** maps f to a new function $f \mid_k \gamma : \mathbb{H} \to \mathbb{C}$ given by

$$(f \mid_k \gamma)(z) := j_k(z,\gamma)\, f(\gamma \cdot z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) \tag{2.3.2}$$

The action of γ mapping f to $f \mid_k \gamma$ via the weight k slash operator is sometimes referred to as a **slash action**.

It is clear, from the above definition, that $f \mid_0 \gamma = f \circ \gamma$ for al $\gamma \in \mathrm{SL}(2,\mathbb{Z})$. That is, if $f = f \mid_0 \gamma$, then $f = f \circ \gamma$, that is, f is invariant under composition with (the action of) γ. If $f = f \mid_k \gamma$ for some $k \in \mathbb{Z}$ and $\gamma \in \mathrm{SL}(2,\mathbb{Z})$, we can view the weight k as indicating the 'extent of invariance' of f under composition with γ.

Note that slash actions compose nicely, due to the nature of the Möbius action of $\mathrm{SL}(2,\mathbb{Z})$ as well as the definition of the automorphy factor. A slightly more general version of this has been previously formalised in `mathlib`.

Lemma 2.3.2. *For all $k \in \mathbb{Z}$, $f : \mathbb{H} \to \mathbb{C}$ and $\gamma_1, \gamma_2 \in \mathrm{SL}(2,\mathbb{Z})$,*

$$(f \mid_k \gamma_1) \mid_k \gamma_2 = f \mid_k (\gamma_1\gamma_2)$$

where $\gamma_1\gamma_2$ is the product of γ_1 and γ_2 as matrices.

We are now ready to define congruence subgroups, which will tell us under precisely which elements of $\mathrm{SL}(2,\mathbb{Z})$ a modular form is slash-invariant. We express this notion in the language of modular arithmetic.

Definition 2.3.3 (Congruence Subgroup). Fix $N \in \mathbb{N}$. The **level** N **principal congruence subgroup** of $\mathrm{SL}(2,\mathbb{Z})$, denoted $\Gamma(N)$, is defined to be the kernel of the surjective group homomorphism from $\mathrm{SL}(2,\mathbb{Z})$ to $\mathrm{SL}\left(2, \mathbb{Z}/N\mathbb{Z}\right)$ that comes from reducing modulo N. That is,

$$\Gamma(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod N \right\} \tag{2.3.3}$$

More generally, a subgroup Γ of $\mathrm{SL}(2,\mathbb{Z})$ is called a **congruence subgroup** if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{N}$.

We now have enough to define what it means for a holomorphic function to be invariant under the slash action of a congruence subgroup. In the definition of modular forms, however, we include an additional condition that is often referred to as *holomorphicity at* $i\infty$, the purpose of which is to ensure that spaces of modular forms, which turn out to admit $\mathbb{C}$-vector space structures, are, in fact, finite-dimensional [22].

Definition 2.3.4 (Holomorphicity at $i\infty$). We say a function $f : \mathbb{H} \to \mathbb{C}$ is **holomorphic at** $i\infty$ if f admits a Fourier expansion of the form

$$f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}$$

That is, f admits a Fourier expansion with no negative powers of $e^{2\pi i z}$.

The holomorphicity of f at $i\infty$ essentially means that the Fourier expansion of f is a holomorphic function in $e^{2\pi i z}$ from the open, punctured unit disc, with the added constraint that $|f(z)|$ remains bounded as $\mathrm{Im}(z) \to \infty$, that is, the corresponding $D \to \mathbb{C}$ function in $q(z)$ extends to a holomorphic function that is defined and bounded at 0. There is a rich theory of functions where $c_0 = 0$, but we will not explore that theory here.[1]

We are now ready to define modular forms. Intuitively, a modular form is a function that satisfies the above definitions in a slash-invariant manner. More precisely, we have the following.

Definition 2.3.5 (Modular Form). Fix $k \in \mathbb{Z}$ and let Γ be a congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$. We say a function $f : \mathbb{H} \to \mathbb{C}$ is a **modular form of weight** k **with respect to** Γ if f is **invariant** under the slash action of Γ and **holomorphic at** $i\infty$ under the slash action of $\mathrm{SL}(2,\mathbb{Z})$. That is,

1. For all $\gamma \in \Gamma$, $f \mid_k \gamma = f$ (cf. Definition 2.3.1).
2. For all $\gamma \in \mathrm{SL}(2,\mathbb{Z})$, $f \mid_k \gamma$ is holomorphic at $i\infty$ (cf. Definition 2.3.4).

We denote by $M_k(\Gamma)$ the space of modular forms of weight k and congruence subgroup Γ. If $\Gamma = \Gamma(N)$ for some $N \in \mathbb{N}$, we say an element of $M_k(\Gamma)$ has **level** N.

There is an immensely rich theory of modular forms, and for the purposes of practicality, it

[1] Modular forms with this property are known as **cusp forms**. One modular form we will need to construct the magic function is the discriminant form, which will turn out to be a cusp form.

was decided not to explore this theory in great detail in this project, particularly because the formalisation of the aspects of Viazovska's proof that stem from this theory is being led by Birkbeck and Lee. We will instead use the remainder of this section to discuss three specific families of modular forms and those of their properties that Viazovska uses to construct her magic function.

2.3.1 The Eisenstein Series

The Eisenstein Series are an important family of slash-invariant forms that will prove essential to the construction of the magic function. The Eisenstein Series whose *weight* is an even integer that is at least 4 are modular forms, though we will also need to work with the Eisenstein Series of weight 2, which, despite not being a modular form, is sufficiently well-behaved for our purposes. We will define it separately from those Eisenstein Series that are modular forms.

Let $k \geq 4$ be an even integer. We denote by E_k the weight k Eisenstein Series. There is more than one way to define E_k. We give below the definitions formalised by Birkbeck for this project, which are particular cases of the `mathlib` definition.

Definition 2.3.6 (The Eisenstein Series of Even Weight ≥ 4). For $k \geq 4$ even, define the **weight k Eisenstein Series** to be the function $E_k : \mathbb{H} \to \mathbb{C}$ given by

$$E_k(z) := \frac{1}{2} \sum_{\substack{(m,n) \in \mathbb{Z}^2 \\ \gcd(m,n)=1}} \frac{1}{(mz+n)^k} \tag{2.3.4}$$

with the defining summation converging absolutely.

Note that the Eisenstein Series can also be defined as

$$E_k(z) = \frac{1}{2\zeta(k)} \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{0\}} \frac{1}{(mz+n)^k} \tag{2.3.5}$$

with ζ here denoting the Riemann zeta function. It is shown in [21, Equation (4.1), pp. 109-110] that this definition matches the definition formalised by Birkbeck in the project repository and stated informally in Definition 2.3.6.

It is shown in [21, pp. 4-5] that E_k is a weight k, level 1 modular form for even integers $k \geq 4$. That is, E_k is invariant under the weight k slash-action of every element of $\mathrm{SL}(2, \mathbb{Z})$. As important special cases of this, E_k satisfies two important functional equations.

Proposition 2.3.7. *For all even $k \geq 4$ and $z \in \mathbb{H}$, the following both hold:*

$$E_k(z+1) = E_k \tag{2.3.6}$$

$$E_k\left(-\frac{1}{z}\right) = z^k E_k(z) \tag{2.3.7}$$

The functional equations (2.3.6) and (2.3.7) yield similar results for an important function that will be used in constructing the magic function. We will explore this idea in Chapter 4.

One of the most important properties of the Eisenstein Series—at least, for our purposes—is that their Fourier coefficients grow polynomially. We will be particularly interested in E_4 and E_6, which are defined as above, and their cousin E_2, which is not a modular form but is nonetheless well-behaved. These functions show up in the definition of Viazovska's magic function, and the polynomial growth property allows us to prove that the magic function is Schwartz.

Theorem 2.3.8. *For all even $k \geq 4$ and $z \in \mathbb{H}$, $E_k(z)$ can be expressed as the Fourier series*

$$E_k(z) = 1 + C_k \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, e^{2\pi i n z} \tag{2.3.8}$$

where

$$C_k = \frac{1}{\zeta(k)} \cdot \frac{(-2\pi i)^k}{(k-1)!} \tag{2.3.9}$$

and

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

In particular, $C_4 = 240$ and $C_6 = -504$. That is, E_4 and E_6 have the following Fourier expansions:

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) e^{2\pi i n z} \tag{2.3.10}$$

$$E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) e^{2\pi i n z} \tag{2.3.11}$$

The statement and proof of the general Fourier expansion of E_k for even $k \geq 4$ have been formalised by Birkbeck in the Sphere Packing repository. Substituting $k = 4$ and $k = 6$ in the expression for C_k and evaluating it using software like Wolfram|Alpha gives the desired result. Now, it is immediate that the Fourier coefficients exhibit polynomial growth: for all $k, n \in \mathbb{N}$, $\sigma_k(n)$ is a sum of at most n numbers that are each at most n^k, meaning $\sigma_k(n) \leq n^{k+1}$.

For the remainder of this subsection, we will focus on a cousin of the weight ≥ 4 Eisenstein Series: the weight 2 Eisenstein Series, denoted E_2. The reason why we treat E_2 separately is that it is not a modular form. Furthermore, it cannot be defined via the summation used in Equation (2.3.4) or Equation (2.3.5): unfortunately, when $k = 2$, these sums do not converge absolutely.

For the purpose of this report, we define E_2 in the following manner. We note that this differs from the definition in the repository, and that we are choosing this definition for expository convenience.

Definition 2.3.9. For all $z \in \mathbb{H}$, define $E_2(z)$ as the Fourier series

$$E_2(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) e^{2\pi i n z} \tag{2.3.12}$$

Interestingly, substituting $k = 2$ in (2.3.9) yields precisely -24. Moreover, the same argument we used earlier demonstrates that the Fourier coefficients of E_2 also grow polynomially. We will mention this result again in Chapter 4, where we will prove that the magic function is Schwartz.

We end our discussion on the Eisenstein Series by giving an explicit counterexample to weight 2, level 1 slash-invariance that shows that E_2 is not a weight 2, level 1 modular form.

Lemma 2.3.10. *For all* $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z})$*, we have*

$$E_2 \mid_2 \gamma = (cz+d)^{-2} \, E_2\left(\frac{az+b}{cz+d}\right) = E_2(z) - \frac{6ic}{\pi \, (cz+d)}$$

The proof uses results about the discriminant form, which we define in the next subsection. We do not prove it here.

2.3.2 The Discriminant Form

The discriminant form is a weight 12, level 1 modular form. As was briefly alluded to earlier, it is a cusp form. It is defined in terms of the Eisenstein series E_4 and E_6.

Definition 2.3.11 (The Discriminant Form). The **discriminant form** Δ is defined by

$$\Delta := \frac{E_4^3 - E_6^2}{1728} \tag{2.3.13}$$

The discriminant form is expressible as the following infinite product.

Theorem 2.3.12 (Product Formula for Δ). *For all $z \in \mathbb{H}$, $\Delta(z)$ is expressible as the following infinite product:*

$$\Delta(z) = e^{2\pi i z} \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n z}\right)^{24} \tag{2.3.14}$$

A proof can be found in [20, Chapter VII, §4, Theorem 6, p. 95]. Birkbeck has shown formally that the above product converges for all $z \in \mathbb{H}$.

We now state important positivity and nonvanishing properties of Δ that we will use when constructing the magic function.

Corollary 2.3.13. *The discriminant form has the following important properties.*
1. *For all $t > 0$, we have $\Delta(it) > 0$.*
2. *For all $z \in \mathbb{H}$, $\Delta(z) \neq 0$.*

We now discuss the last family of functions used in Viazovska's construction.

2.3.3 The Theta Functions

In this subsection, we define and state some basic properties of the Theta functions Θ_2, Θ_3 and Θ_4, the fourth powers of which define the corresponding H-functions.

Definition 2.3.14 (The Θ- and H-Functions). Define $\Theta_2, \Theta_3, \Theta_4 : \mathbb{H} \to \mathbb{C}$ by

$$\Theta_2(z) = \sum_{n\in\mathbb{Z}} e^{\pi i \left(n+\frac{1}{2}\right)^2 z} \qquad \Theta_3(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z} \qquad \Theta_4(z) = \sum_{n\in\mathbb{Z}} (-1)^n e^{\pi i n^2 z}$$

for all $z \in \mathbb{H}$. Define $H_2, H_3, H_4 : \mathbb{H} \to \mathbb{C}$ by

$$H_2 = \Theta_2^4 \qquad H_3 = \Theta_3^4 \qquad H_4 = \Theta_4^4$$

It can be shown that the H-functions are modular forms of weight 2 and level 2.

Given the manner in which the H-functions are defined, it is tedious to compute their Fourier expansions explicitly. However, the purpose of computing the Fourier expansions of the Eisenstein Series was to determine that their Fourier coefficients grow polynomially. It turns out that in the case of the H-functions, we can do this without explicitly computing their Fourier series.

The Fourier coefficients of H_3 and H_4 grow polynomially because those of Θ_3 and Θ_4 grow polynomially (see Proposition 4.2.2). Unfortunately, due to the fractional term in the exponents of the summands in the definition of Θ_2, it is not possible to use the same technique to show that its Fourier coefficients grow polynomially. Fortunately, we can still prove the result for H_2, because raising Θ_2 to the fourth power gets rid of the fractional exponent. That is,

$$H_2 = \Theta_2^4 = \left(2 \sum_{n=0}^{\infty} e^{\pi i \left(n+\frac{1}{2}\right)^2 z}\right)^4 = 16 e^{\pi i z} \left(\sum_{n=0}^{\infty} e^{\pi i \left(n^2+n\right) z}\right)^4 \tag{2.3.15}$$

This can be explicitly computed as an iterated sum with coefficients that grow polynomially.

Finally, we mention some important slash action relations that we will take advantage of when proving properties about the magic function. We define some notation first.

Notation. Denote by S, T, I the following elements of $\mathrm{SL}(2, \mathbb{Z})$:

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

We now state important properties of the H-functions. These have been taken from [1, (13)-(19)] and [14, §6], though the notation used in [1] is slightly different (Θ_2, Θ_3 and Θ_4 are denoted θ_{10}, θ_{00} and θ_{01} respectively).

Proposition 2.3.15. *The following slash action relations hold.*

$$\begin{aligned} H_2 \mid_2 S &= -H_4 & \qquad H_3 \mid_2 S &= -H_3 & \qquad H_4 \mid_2 S &= -H_2 \\ H_2 \mid_2 T &= -H_2 & \qquad H_3 \mid_2 T &= H_4 & \qquad H_4 \mid_2 T &= H_3 \end{aligned}$$

Furthermore, the H-functions are invariant under the weight 0 slash action of $\Gamma(2)$. Finally, *the H-functions are related to each other, E_4, E_6 and Δ in the following manner.*

$$0 = H_2 - H_3 + H_4 \tag{2.3.16}$$

$$E_4 = \frac{1}{2}\left(H_2^2 + H_3^2 + H_4^2\right) \tag{2.3.17}$$

$$E_6 = \frac{1}{2}\left(H_2 + H_3\right)\left(H_3 + H_4\right)\left(H_4 - H_2\right) \tag{2.3.18}$$

$$\Delta = \frac{1}{256}\left(H_2\, H_3\, H_4\right)^2 \tag{2.3.19}$$

Further relations can be obtained by writing $H_3 = H_2 + H_4$ in (2.3.17) and (2.3.18).

Combining the relations listed above with Lemma 2.3.2 allows us to show that several more relations hold. In Section 4.1.2, we will use this technique to provide a comprehensive list of transformations that will be essential to Viazovska's construction.

Chapter 3

A Roadmap to Constructing the Magic Function

We mentioned, in the introduction, that the scope of this project is to construct Viazovska's Magic Function in Lean and prove that it satisfies certain specific properties, such as satisfying the hypotheses of the Cohn-Elkies Linear Programming Bound. In this chapter, we will outline the steps we will take to achieve this goal. In particular, we will list all the conditions we need to prove that the Magic Function satisfies. Our approach will be to construct the Magic Function in terms of two intermediary functions. Proving it satisfies the necessary conditions will then be a matter of proving that these intermediary functions satisfy certain properties. We will list these properties as well.

3.1 Radial Schwartz Functions

In the statement of Theorem 2.2.5, we require the function in terms of which we bound the sphere packing constant in dimension d to be Schwartz. We have discussed Schwartz functions informally, but give a more formal definition below that is adapted from the `mathlib`definition.

Definition 3.1.1 (Schwartz Function). Let E and F be normed $\mathbb{R}$-vector spaces. We say that $f : E \to F$ is **Schwartz** if it is infinitely continuously differentiable and for all $n, k \in \mathbb{N}$, there exists some $C \in \mathbb{R}$ such that for all $x \in E$,

$$\|x\|^k \cdot \left\| f^{(n)}(x) \right\| \leq C \tag{3.1.1}$$

We define the **Schwartz space** $\mathcal{S}(E, F)$ to be the set of all Schwartz functions from E to F, which admits a vector space structure over $\mathbb{R}$.

At the outset, it might appear that the reason we are interested in Schwartz functions is that this is a requirement of the Poisson Summation Formula (Theorem 2.2.4), which is used in the proof of the Cohn-Elkies Linear Programming Bound (Theorem 2.2.5). However, this turns out to be a sufficient condition for the Poisson Summation Formula to hold, not a necessary condition. There is a deeper reason why we are interested in Schwartz functions: the Cohn-Elkies Conditions immediately show us that we should also consider the properties of the Fourier transform of the magic function, and Fourier transforms of Schwartz functions turn out to be Schwartz. In fact, we can say something stronger when we view the Fourier transform as an operator on the Schwartz space.

Theorem 3.1.2. *Let V be a finite-dimensional inner-product space over $\mathbb{R}$ and let E be a normed vector space over $\mathbb{C}$. The Fourier transform*

$$\mathcal{F} : \mathcal{S}(V, E) \to \mathcal{S}(V, E) : f \mapsto \widehat{f}$$

is a linear isomorphism of $\mathcal{S}(V, E)$.

This is a well-known result that has previously been formalised in `mathlib`.

It turns out that there is another condition we can impose to simplify our hunt for the magic function. The key idea is to find a function satisfying the conditions (CE1)-(CE3). Observe, for $x \in \mathbb{R}^d$, that (CE1) does not depend on x, and (CE2) and (CE3) only depend on $\|x\|$. This allows us to narrow our search to **radial functions**, which we define as follows.

Definition 3.1.3 (Radial Functions). Let E be a normed $\mathbb{R}$-vector space and α an arbitrary set. We say that $f : E \to \alpha$ is **radial** if for all $x, y \in E$, if $\|x\| = \|y\|$, then $f(x) = f(y)$.

Radial Schwartz functions interact with the Fourier Transform in an even nicer way than ordinary Schwartz functions.

Proposition 3.1.4. *Let $f : \mathbb{R}^d \to \mathbb{C}$ be a radial Schwartz function. Then,*

$$\mathcal{F}(\mathcal{F}(f)) = f$$

A key consequence of Proposition 3.1.4 is the following mechanism for constructing radial Schwartz functions, and thereby, the magic function.

Theorem 3.1.5. *If f is a radial Schwartz function, there exist unique functions f_+ and f_- such that $f = f_+ + f_-$ and $\mathcal{F}(f_+) = f_+$ and $\mathcal{F}(f_-) = -f_-$.*

Proof. Observe that if f is a radial Schwartz function, we can write

$$f = \underbrace{\frac{f - \widehat{f}}{2}}_{=:f_-} + \underbrace{\frac{f + \widehat{f}}{2}}_{=:f_+}$$

The functions f_- and f_+ have the properties that

$$\mathcal{F}(f_-) = \frac{1}{2}\left(\mathcal{F}(f) - \mathcal{F}\left(\widehat{f}\right)\right) = \frac{1}{2}\left(\widehat{f} - f\right) = -f_-$$
$$\mathcal{F}(f_+) = \frac{1}{2}\left(\mathcal{F}(f) + \mathcal{F}\left(\widehat{f}\right)\right) = \frac{1}{2}\left(\widehat{f} + f\right) = f_+$$

where we use Proposition 3.1.4 to show that $\widehat{\widehat{f}} = f$. In other words, f_- and f_+ are **eigenfunctions of the Fourier transform** with eigenvalues -1 and $+1$ respectively. Furthermore, if

$f = \lambda f_1 + \mu f_2$ for *any* two functions f_1 and f_2 such that $\widehat{f_1} = -f_1$ and $\widehat{f_2} = f_2$, then one can show, by computing f_- and f_+, that $\lambda f_1 = f_-$ and $\mu b = f_+$. $\square$

By Theorem 3.1.5, we can break down the problem of constructing the magic function into two smaller problems: constructing appropriate ± 1-Fourier eigenfunctions. Before we discuss the properties we seek in our magic function—or its constituent Fourier eigenfunctions—we briefly mention one final ingredient of the utmost import about radial Schwartz functions that we will use repeatedly to simplify the argument.

We usually treat radial functions as $\mathbb{R} \to \mathbb{C}$ functions, because all information about the input that is necessary to compute the corresponding output is captured by a (non-negative) real number: its norm. However, the decaying property (3.1.1) of Schwartz functions is something that, at first glance, makes it a bit tricky to ignore the dimension of the domain when dealing with radial Schwartz functions, particularly because it is stated in terms of higher derivatives. Computing n-dimensional Jacobians is already tedious, and formally, it tends to be very challenging indeed. Fortunately, we have a workaround.

Proposition 3.1.6. *Let $f : \mathbb{R} \to \mathbb{C}$ be a function that is smooth on $[0, \infty)$ and decays faster than any inverse integer or half-integer power of x. Then, for all $d \in \mathbb{N}$, the function*

$$f_d : \mathbb{R}^d \to \mathbb{C} : x \mapsto f\left(\|x\|^2\right)$$

is Schwartz. In particular, if f is Schwartz, f_d is Schwartz.

This is an extremely important result, because it allows us to translate freely between functions with Schwartz-like properties with one- or multiple-dimensional inputs. It has been formalised by the author, and we discuss it further in Section 5.1.2.

The point of Proposition 3.1.6 is that it gives us a criterion to show that radial functions in higher dimensions that are functions not of the norm but of the norm *squared* are Schwartz, purely by considering the corresponding function that takes in a one-dimensional input. This will be instrumental in our argument.

With this, we end our discussion of radial Schwartz functions. The key takeaway is that while Schwartzness is a necessary condition for our magic function to satisfy, we can also impose the condition of radiality to simplify our construction. We will now take a closer look at Cohn and Elkies's groundbreaking result (Theorem 2.2.5) to determine further properties for the magic function to satisfy.

3.2 The Cohn-Elkies Linear Programming Bound, Revisited

So far, we have examined the statement of Theorem 2.2.5 in detail: it immediately tells us that we want the magic function to be Schwartz and satisfy the conditions (CE1)-(CE3), and upon noticing that these conditions only depend on the norm and that radial functions are very well-behaved, we have narrowed our search to radial Schwartz function obeying (CE1)-(CE3). It turns out that we can learn even more about the magic function when we examine the *proof* of Theorem 2.2.5 when we specialise to the case where the function f is optimal. Our examination of the proof of Theorem 2.2.5 is based on an insightful discussion in [3, p. 8].

Specifically, let f be a (radial) Schwartz function satisfying (CE1), (CE2) and (CE3). What it means for f to be optimal is that there exists a sphere packing $\mathcal{P}(X)$ in $\mathbb{R}^d$ such that the Cohn-Elkies bound indexed by f is precisely the density of this sphere packing. This would make $\mathcal{P}(X)$ an optimal sphere packing in $\mathbb{R}^d$ and f an optimal function.

Since it is enough to prove the upper-bound property for periodic sphere packings, we can simplify our search for the right f by assuming the Cohn-Elkies bound corresponding to f is the density of a *periodic* packing. In other words, we can assume there exists some lattice $\Lambda \subset \mathbb{R}^d$ such that the set of centres X is periodic with respect to Λ. This turns out to be helpful because we can then use the exact forms of the inequalities in the proof to deduce properties that f must have if it is optimal, corresponding to some optimal periodic packing.

In our argument, we fix an arbitrary Λ-periodic sphere packing $\mathcal{P}(X)$ of separation 1 and show the inequality (2.2.1). In the case where f is optimal, in the sense that the upper-bound is achieved, we must have that (2.2.1) is, in fact, an **equality**. The same must be true of the equivalent inequality, (2.2.2). This tells us that the intermediate inequalities (2.2.3) and (2.2.4) must *also* be equalities, because the chain of inequalities begins and ends at the same quantity. In particular, we can take a closer look at (2.2.3): the way we prove it is by writing

$$\left|{}^{X}\!/_{\Lambda}\right| \cdot f(0) = \sum_{x \in {}^{X}\!/_{\Lambda}} f(x-x) = \sum_{x \in X} \sum_{\substack{y \in {}^{X}\!/_{\Lambda} \\ y = x}} \geq \sum_{x \in X} \sum_{y \in {}^{X}\!/_{\Lambda}} f(x-y)$$

The terms we discard to prove the inequality are non-positive, as they are of the form $f(x-y)$ for $y \neq x$ (meaning $\|y-x\| \geq 1$, allowing us to apply (CE2)). If this inequality is an equality, then all the terms we discard must not merely be non-positive: they must, in fact, be zero. That is, we need

$$f(x-y) = 0 \text{ for all } \textbf{distinct } x \in X \text{ and } y \in {}^{X}\!/_{\Lambda} \tag{3.2.1}$$

By definition of ${}^{X}\!/_{\Lambda}$, *every* element of Λ is expressible as $x-y$ for some $x \in X$ and $y \in {}^{X}\!/_{\Lambda}$, because X consists of *all* Λ-translates of y. So, all non-zero lattice points are expressible as $x-y$ for x and y as in (3.2.1). We can therefore conclude that **an optimal function f with Cohn-Elkies bound equal to the density of a periodic sphere packing must vanish at all non-zero lattice points**.

It turns out that examining (CE2) gives us an *even stronger* condition on f. First, note that we must have $0 \leq f(0)$: the bound

$$\frac{f(0)}{\widehat{f}(0)} \cdot \mathrm{Vol}\left(B_d\left(0, \frac{1}{2}\right)\right)$$

is greater than or equal to a non-negative constant, and both $\mathrm{Vol}\big(B_d(0, \frac{1}{2})\big)$ (as a volume) and $\widehat{f}(0)$ (by (CE3)) are non-negative, meaning $f(0)$ cannot possibly be negative. Indeed, this is true regardless of whether f is optimal. Since (CE2) tells us that f is non-positive at points with norm at least 1, we can conclude that f not only has zeroes but **double zeroes** at all lattice points with norm at least 1: the behaviour of f, viewed as an $\mathbb{R} \to \mathbb{R}$ function of the norm r of a point on $\mathbb{R}^d$, is such that sign-changes, if any, from non-negative to non-positive cannot occur at zeroes ≥ 1, and thereafter, there are no more sign changes.

There is one final condition we can glean from the statement of the theorem that specifically applies to the eight-dimensional case. Recall that for all $k \in \mathbb{N}$,

$$\mathrm{Vol}(B_{2k}(0, r)) = r^{2k} \cdot \frac{\pi^k}{k!}$$

This fact has previously been formalised. When $k = 4$ and $r = \frac{1}{2}$, we get

$$\mathrm{Vol}\left(B_8\left(0, \frac{1}{2}\right)\right) = \frac{1}{256} \cdot \frac{\pi^4}{24!} = \frac{1}{16} \cdot \frac{\pi^4}{384}$$

which is a factor of $\frac{1}{16}$ away from the density of Λ_8. We thus conclude that the function we seek must satisfy $\widehat{f}(0) = 16\, f(0)$.

We end by saying a few words about scaling. In the proof of Theorem 2.2.5, and by extension, in our discussion above, we assumed that the least distance between points on Λ is 1. This is not true of Λ_8, but we can rescale sphere packings freely without affecting their density. It will be more convenient to rescale the magic function at the very end than to rescale Λ_8 by a factor of $\sqrt{2}$ right away, as Viazovska does in [1]. In fact, this gives us an even nicer condition: if we have a function g that satisfies the conditions we would have if we replaced Λ by Λ_8 in the above discussion, then the function $f(x) = g\left(\sqrt{2}\, x\right)$ satisfies the properties discussed so far on the normalised E_8 lattice, which has separation one. Moreover, $\widehat{f}(0) = 16\, f(0)$ tells us that we require $g(0) = \widehat{g}(0)$. This further makes (CE1) redundant, as we cannot have $g(0) = \widehat{g}(0) = 0$.

Putting these conclusions about single and double zeroes together with our observation about splitting radial Schwartz functions into their constituent ± 1-Fourier eigenfunctions, we can conclude that we need to find **Fourier eigenfunctions with double zeroes at Λ_8 lattice points**. It is no accident that this is precisely the title of [1, §4].

3.3 The Properties Desired of Viazovska's Fourier Eigenfunctions

We begin by summarising the properties we would like the magic function to have. We then examine which of these properties come from the eigenfunctions. Finally, we will mention tools that are used to show that both its ± 1-Fourier eigenfunctions satisfy the conditions we list below.

For the remainder of this thesis, we will fix the following notation.

Notation. Going forward, the magic function for 8-dimensional sphere packing shall be denoted g, its $+1$-eigenfunction shall be denoted a, and its -1-eigenfunction shall be denoted b.

We now list the properties we would require g to have.

1. g needs to be a Schwartz function.

2. It suffices for g to be radial.

3. The scaled function $g\left(\sqrt{2}\, x\right)$ needs to satisfy the Cohn-Elkies conditions (CE1), (CE2) and (CE3). Equivalently, we need $g(x) \leq 0$ for all $x \in \mathbb{R}^8$ with $\|x\| \geq \sqrt{2}$, $\widehat{g}(x) \geq 0$ for all $x \in \mathbb{R}^8$, and $g(0) = \widehat{g}(0) = 1$.

4. g needs to have single zeroes at all non-zero points in Λ_8.

5. g needs to have double zeroes at all but finitely many points in Λ_8.

Of these properties, the following would be inherited from a and b:

1. Schwartzness
2. Radiality
3. Having single zeroes at all non-zero points in Λ_8
4. Having double zeroes at all but finitely many points in Λ_8

That is, if we can construct a and b such that they satisfy the above properties, then g will satisfy them as well. The remaining properties will have to do with the coefficients of the linear combination of a and b that makes up g.

One of the most interesting conceptual breakthroughs in Viazovska's construction is her use of the theory of modular forms. While examining the proof of Theorem 2.2.5 gives us concrete criteria to look for when constructing the magic function, it also presents a fundamental challenge: constructing a function in a manner whereby we have control over both the function itself and its Fourier transform. This is a deceptively challenging task, and is explored in detail by Bourgain et al in [23]. The eigenfunction property offers a way around this problem, but the challenge of constructing ± 1-eigenfunctions remains. Viazovska's approach is to tackle the problem on the integrand level rather than the integral level. If a function is already expressed as an integral, then taking its Fourier transform produces a double-integral. If it is possible to reduce this double-integral to a single integral, it is conceivable that with a clever change of variables, one might be able to express this single integral as being equal to the original function, up to signs. It is not inherently difficult to construct integrals with respect to one variable of functions of two variables such that the double integral reduces to a single integral. Finding integrands with such versatile change-of-variable properties is more difficult. The fact that modular forms, and related functions like E_2, admit numerous functional relations through slash actions is a key motivator for their use in Viazovska's construction: she expresses a and b as sums of integrals whose integrands satisfy such relations because they are expressed in terms of modular forms and associated functions.

There is a deeper story involving the theory of modular forms, but we will no more than scratch the surface in this exposition because the formalisation of the associated details is being handled by other collaborators. We refer the interested reader to Cohn's beautiful reverse-engineering of Viazovska's construction [3], which explores the modular forms connection in greater detail.

Chapter 4

Viazovska's Magic Function, Informally

In this chapter, we will construct the $+1$-eigenfunction a, the -1-eigenfunction b, and the magic function g. The theory developed in Chapter 3 tells us what properties we would like all three functions to satisfy, and in Section 3.3, we summarised those properties concisely. Over the course of this chapter, we prove that they do, indeed, satisfy them.

The content is based heavily on Viazovska's original paper [1, §4] and a more detailed version of her proof that she wrote originally for the project blueprint [14, §7]. However, some details, including the very definitions of a and b, differ slightly from the original paper. While these modifications add numerous computational inconveniences to the argument, they are necessary for the formalisation. The arguments given in this chapter are formulated to correspond either to formalised proofs or to the proof path the author has in mind for eventual formalisation, and every effort has been made to avoid assuming general results, however well-known, that have not previously been formalised. Previously formalised mathematics is assumed and applied freely, and links are provided where appropriate. The similarities and subtle differences between the approach in this report and Viazovska's original approach are discussed in greater detail in Section 5.1.

We begin by defining the functions in question. In each subsequent section of this chapter, we will prove a certain property for each of the eigenfunctions. Finally, in Section 4.6, we will prove that g does, indeed, satisfy the properties outlined in Chapter 3.

4.1 Defining Viazovska's Fourier Eigenfunctions

As we noted in Section 3.3, we construct our Fourier eigenfunctions as sums of integrals whose integrands obey several transformation properties. These transformation properties will be the result of well-known facts about modular forms, which we discussed in Section 2.3. For each eigenfunction, we begin by defining families of functions—the ϕ- and ψ-functions respectively—in terms of modular forms and associated functions. We then list their transformation rules, which we will apply throughout this chapter. We will end each subsection by defining their namesake eigenfunction.

4.1.1 The $+1$-Eigenfunction

We begin by defining the ϕ-functions.

Definition 4.1.1 (The ϕ-Functions). Define the functions $\phi_0, \phi_{-2}, \phi_{-4} : \mathbb{H} \to \mathbb{C}$ by

$$\phi_{-4} := \frac{E_4^2}{\Delta} \tag{4.1.1}$$

$$\phi_{-2} := \frac{E_4\left(E_2 E_4 - E_6\right)}{\Delta} \tag{4.1.2}$$

$$\phi_0 := \frac{\left(E_2 E_4 - E_6\right)^2}{\Delta} \tag{4.1.3}$$

Note first that these functions are holomorphic: their numerators are clearly holomorphic, as one can see from Section 2.3, and we know that Δ does not vanish on the upper half-plane. We now give important transformation properties exhibited by these functions that will later allow us to change variables inside the integrands making up a.

Lemma 4.1.2. *For all $z \in \mathbb{H}$,*

$$\phi_0(z+1) = \phi_0(z) \tag{4.1.4}$$

$$\phi_0\left(\frac{-1}{z}\right) = \phi_0(z) - \frac{12i}{\pi} \cdot \frac{1}{z} \cdot \phi_{-2}(z) - \frac{36}{\pi^2} \cdot \frac{1}{z^2} \cdot \phi_{-4}(z) \tag{4.1.5}$$

We do not prove these here, but mention that they both follow from the weight k slash action formulae on E_k for $k \in \{2, 4, 6\}$. When $k = 4$ and $k = 6$, we have weight k invariance, because E_4 and E_6 are modular forms, but when $k = 2$, we need to use Lemma 2.3.10. A detailed proof of these transformations can be found in [14]. We now define the $+1$-eigenfunction a.

Definition 4.1.3 (Viazovska's $+1$-Fourier Eigenfunction). Define $a_{\text{rad}} : \mathbb{R} \to \mathbb{C}$ by

$$a_{\text{rad}}(r) := I_1(r) + I_2(r) + I_3(r) + I_4(r) + I_5(r) + I_6(r) \tag{4.1.6}$$

where, for all $r \in \mathbb{R}$,

$$I_1(r) := \int_{-1}^{-1+i} \phi_0\left(\frac{-1}{z+1}\right) (z+1)^2 \, e^{\pi i r z} \, \mathrm{d}z \tag{4.1.7}$$

$$I_2(r) := \int_{-1+i}^{i} \phi_0\left(\frac{-1}{z+1}\right) (z+1)^2 \, e^{\pi i r z} \, \mathrm{d}z \tag{4.1.8}$$

$$I_3(r) := \int_{1}^{1+i} \phi_0\left(\frac{-1}{z-1}\right) (z-1)^2 \, e^{\pi i r z} \, \mathrm{d}z \tag{4.1.9}$$

$$I_4(r) := \int_{1+i}^{i} \phi_0\left(\frac{-1}{z-1}\right) (z-1)^2 \, e^{\pi i r z} \, \mathrm{d}z \tag{4.1.10}$$

$$I_5(r) := -2 \int_{0}^{i} \phi_0\left(\frac{-1}{z}\right) z^2 \, e^{\pi i r z} \, \mathrm{d}z \tag{4.1.11}$$

$$I_6(r) := 2 \int_{i}^{i\infty} \phi_0(z) \, e^{\pi i r z} \, \mathrm{d}z \tag{4.1.12}$$

Define the $+1$-Fourier eigenfunction $a : \mathbb{R}^8 \to \mathbb{C}$ by

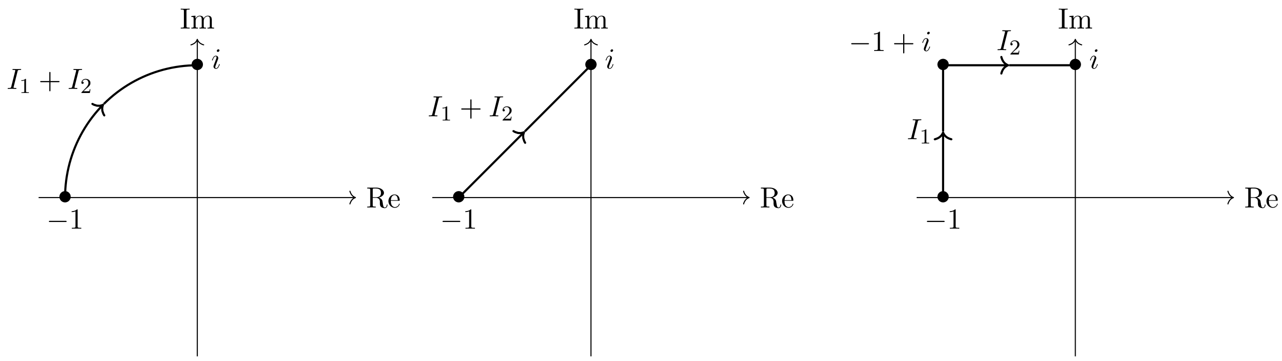
$$a(x) := a_{\text{rad}}\left(\|x\|^2\right) \tag{4.1.13}$$

It is immediate from (4.1.13) that a is radial. All of its properties are determined by its radial part a_{rad}. There are similar definitions in Lean.

There is an important remark that must be made about the definitions in (4.1.7)-(4.1.12): in the original paper [1], the integrals I_1 and I_2 are combined, as are I_3 and I_4, and expressed in the following manner:

$$I_1(r) + I_2(r) = \int_{-1}^{i} \phi_0\left(\frac{-1}{z+1}\right)\,(z+1)^2\, e^{\pi i r z}\,\mathrm{d}z$$
$$I_3(r) + I_4(r) = \int_{1}^{i} \phi_0\left(\frac{-1}{z-1}\right)\,(z-1)^2\, e^{\pi i r z}\,\mathrm{d}z$$

with the contours not specified. The most 'classical' choice would be quarter-circular contours, though the same results can be achieved working with straight and rectangular contours.



(a) Quarter-Circular Contour **(b)** Straight Line Contour **(c)** Rectangular Contour

Figure 4.1: Different contours along which we can integrate the integrand of I_1 and I_2 to get an integral equal to $I_1 + I_2$

The reason the choice of contours does not matter is that the integrands of $I_1, \ldots, I_6$ are holomorphic on the upper half-plane. This is clear for I_6, and for the others, if we multiply terms of the form $\phi_0(\frac{-1}{z})$ by z^2, apply (4.1.5) and multiply through, we end up with a holomorphic function.

The choice of rectangular contours (as in Section 4.1.1) as opposed to quarter-circles or straight lines for $I_1 + I_2$ and $I_3 + I_4$ is motivated by the versions of the Cauchy-Goursat Theorem that have been formalised in Lean. We discuss this further in Section 5.3.

We are now ready to define the -1-eigenfunction b.

4.1.2 The -1-Eigenfunction

Recall the H-functions defined as the fourth powers of the Theta functions in Definition 2.3.14. We begin by defining the h function, in terms of which we define the ψ-functions.

Definition 4.1.4 (The h-Function). Define the function $h : \mathbb{H} \to \mathbb{C}$ by

$$h(z) := 128 \frac{H_3(z) + H_4(z)}{H_2(z)^2} \tag{4.1.14}$$

where H_2, H_3 and H_4 are as defined in Definition 2.3.14.

In [1], the ψ-functions are defined in terms of the h-function via slash actions.

Definition 4.1.5 (The ψ-Functions). Define the functions $\psi_I, \psi_S, \psi_T : \mathbb{H} \to \mathbb{C}$ by

$$\psi_I := h - h \mid_{-2} ST \qquad \psi_T := \psi_I \mid_{-2} T \qquad \psi_S := \psi_I \mid_{-2} S$$

where h is as defined in Definition 4.1.4 and $I, S, T \in \mathrm{SL}(2, \mathbb{Z})$ are as defined just before Proposition 2.3.15.

It is possible to use the weight-2 slash action relations seen in Proposition 2.3.15 to express the ψ-functions explicitly in terms of the H-functions.

Lemma 4.1.6. *The ψ-functions can be expressed in the following manner:*

$$\psi_I = 128\left(\frac{H_3 + H_4}{H_2^2} + \frac{H_4 - H_2}{H_3^2}\right)$$
$$\psi_T = 128\left(\frac{H_3 + H_4}{H_2^2} + \frac{H_2 + H_3}{H_4^2}\right)$$
$$\psi_S = 128\left(\frac{H_4 - H_2}{H_3^2} - \frac{H_2 + H_3}{H_4^2}\right)$$

Proof. We prove the result for ψ_I and sketch how to prove it for the others. Since $\psi_I = h - h \mid_{-2} ST$ and the first summand of ψ_I given above is precisely h, we show that $h \mid_{-2} ST$ gives precisely the second summand.

First, note that $j_{-2}(ST) = (z+1)^2$. Observe that for all $z \in \mathbb{H}$, $(z+1)^2 = \frac{(z+1)^{-2}}{\left((z+1)^{-2}\right)^2}$. Hence,

$$h \mid_{-2} ST = 128\frac{(H_3 \mid_2 ST) + (H_4 \mid_2 ST)}{(H_2 \mid_2 ST)^2} = 128\frac{-(H_3 \mid_2 T) - (H_2 \mid_2 T)}{(-H_2 \mid_2 T)^2} = -128\frac{H_4 - H_2}{H_3^2}$$

with the second equality following from Lemma 2.3.2. Subtracting $h \mid_{-2} ST$ from h then gives the desired result. The explicit expressions for ψ_T and ψ_S can be obtained by performing similar computations on ψ_I. □

The proof of Lemma 4.1.6 shows us that weight -2 slash actions on the ψ-functions come directly from the analogous weight 2 slash operations on the H-functions. We have seen several of these in Proposition 2.3.15 and can combine them with Lemma 2.3.2 to generate the following relations between the ψ-functions.

$$\psi_T = \psi_I \mid_{-2} T \qquad \psi_T(z) = \psi_I(z+1) \tag{4.1.15}$$
$$\psi_I = \psi_T \mid_{-2} T \qquad \psi_I(z) = \psi_T(z+1) \tag{4.1.16}$$
$$\psi_S = \psi_I \mid_{-2} S \qquad \psi_S(z) = z^2\, \psi_I\left(\frac{-1}{z}\right) \tag{4.1.17}$$
$$\psi_I = \psi_S \mid_{-2} S \qquad \psi_I(z) = z^2 \psi_S\left(\frac{-1}{z}\right) \tag{4.1.18}$$
$$\psi_S = \psi_I \mid_{-2} S \qquad \psi_S(z) = z^2 \psi_I\left(\frac{-1}{z}\right) \tag{4.1.19}$$
$$\psi_T = \psi_S \mid_{-2} ST \qquad \psi_T(z) = (z+1)^2\, \psi_S\left(\frac{-1}{z+1}\right) \tag{4.1.20}$$

$$\psi_S = \psi_S \mid_{-2} T \qquad \psi_S(z) = \psi_S(z+1) \tag{4.1.21}$$

$$-\psi_T = \psi_T \mid_{-2} S \qquad -\psi_T(z) = z^2 \psi_T\left(\frac{-1}{z}\right) \tag{4.1.22}$$

$$-\psi_T = \psi_I \mid_{-2} TS \qquad -\psi_T(z) = z^2 \psi_I\left(\frac{z-1}{z}\right) \tag{4.1.23}$$

$$-\psi_T = \psi_S \mid_{-2} STS \qquad -\psi_T(z) = (z-1)^2\, \psi_S\left(\frac{-z}{z-1}\right) \tag{4.1.24}$$

$$-\psi_T = \psi_S \mid_{-2} TSTS \qquad -\psi_T(z) = (z-1)^2\, \psi_S\left(\frac{-1}{z-1}\right) \tag{4.1.25}$$

where we note that

$$ST = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \qquad TS = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$

$$STS = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix} \qquad TSTS = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$

It will be useful, particularly to prove Schwartzness, to express the ψ-functions in an alternate form, as fractions with the discriminant in the denominator. We can therefore express the ψ-functions in yet another form.

Proposition 4.1.7. *We can express ψ_I, ψ_S, ψ_T in the following manner:*

$$\psi_I = \frac{H_4^3\left(2H_4^2 + 5H_4H_2 + 5H_2^2\right)}{2\Delta} \tag{4.1.26}$$

$$\psi_S = \frac{-H_2^3\left(2H_2^3 + 5H_2H_4 + 5H_4^2\right)}{2\Delta} \tag{4.1.27}$$

$$\psi_T = \psi_I - \psi_S \tag{4.1.28}$$

where Δ is the discriminant form.

(4.1.26) and (4.1.27) can be proved by finding common denominators for the expressions in Lemma 4.1.6 and applying (2.3.16) and (2.3.19). (4.1.28) is proved using slash actions, but we include it in Proposition 4.1.7 because this gives us a clear way of seeing that the ψ-functions are holomorphic on the upper half-plane: Δ is holomorphic and non-vanishing, and the numerators are made entirely of holomorphic functions.

We are now ready to define the -1-eigenfunction, denoted b.

Definition 4.1.8 (Viazovska's -1-Fourier Eigenfunction). Define $b_{\text{rad}} : \mathbb{R} \to \mathbb{C}$ by

$$b_{\text{rad}}(r) := J_1(r) + J_2(r) + J_3(r) + J_4(r) + J_5(r) + J_6(r) \tag{4.1.29}$$

where, for all $r \in \mathbb{R}$,

$$J_1(r) := \int_{-1}^{-1+i} \psi_T(z)\, e^{\pi i r z}\, \mathrm{d}z \tag{4.1.30}$$

$$J_2(r) := \int_{-1+i}^{i} \psi_T(z)\, e^{\pi i r z}\, \mathrm{d}z \tag{4.1.31}$$

$$J_3(r) := \int_{1}^{1+i} \psi_T(z)\, e^{\pi i r z}\, \mathrm{d}z \tag{4.1.32}$$

$$J_4(r) := \int_{1+i}^{i} \psi_T(z)\; e^{\pi i r z}\; \mathrm{d}z \tag{4.1.33}$$

$$J_5(r) := -2\int_{0}^{i} \psi_I(z)\; e^{\pi i r z}\; \mathrm{d}z \tag{4.1.34}$$

$$J_6(r) := -2\int_{i}^{i\infty} \psi_S(z)\; e^{\pi i r z}\; \mathrm{d}z \tag{4.1.35}$$

Define the -1-Fourier eigenfunction $a : \mathbb{R}^8 \to \mathbb{C}$ by

$$b(x) := b_{\mathrm{rad}}\left(\|x\|^2\right) \tag{4.1.36}$$

Note that by applying (4.1.20) and (4.1.25), we can express $J_1, \ldots, J_5$ in the following manner:

$$J_1(r) = \int_{-1}^{-1+i} \psi_S\left(\frac{-1}{z+1}\right)\; (z+1)^2\; e^{\pi i r z}\; \mathrm{d}z \tag{4.1.37}$$

$$J_2(r) = \int_{-1+i}^{i} \psi_S\left(\frac{-1}{z+1}\right)\; (z+1)^2\; e^{\pi i r z}\; \mathrm{d}z \tag{4.1.38}$$

$$J_3(r) = -\int_{1}^{1+i} \psi_S\left(\frac{-1}{z-1}\right)\; (z-1)^2\; e^{\pi i r z}\; \mathrm{d}z \tag{4.1.39}$$

$$J_4(r) = -\int_{1+i}^{i} \psi_S\left(\frac{-1}{z-1}\right)\; (z-1)^2\; e^{\pi i r z}\; \mathrm{d}z \tag{4.1.40}$$

$$J_5(r) = -2\int_{0}^{i} \psi_S\left(\frac{-1}{z}\right)\; z^2\, e^{\pi i r z}\; \mathrm{d}z \tag{4.1.41}$$

With $J_1, \ldots, J_5$ expressed in this manner, and J_6 expressed as in (4.1.35), there are striking similarities between the J_j and the I_j, with ψ_S being the analogue of ϕ_0. We can hence use similar approaches to prove properties about both a and b. The differences in the signs between J_3 and I_r, J_4 and I_4, and J_6 and I_6, as well as the differences between the relations between the ϕ- and ψ-functions, will account for the differences in the way we treat a and b.

4.2 Establishing the Schwartzness Property

The magic function is a linear combination of a and b, which are each defined as compositions of a_{rad} and b_{rad} with the norm-squared function. From Proposition 3.1.6, we know that it is enough to establish that a_{rad} and b_{rad} have Schwartz-like properties on $[0, \infty)$ to establish that a and b are Schwartz. In particular, this means the smoothness and decaying conditions need to be satisfied with respect to $\mathbb{R}$ inputs instead of $\mathbb{R}^8$ inputs, a substantial simplification.

To show that a_{rad} and b_{rad} are Schwartz-like, we show that their constituent integrals $I_1, \ldots, I_6$ and $J_1, \ldots, J_6$ are Schwartz-like, as rapid decay and smoothness on $[0, \infty)$ are both compatible with addition. We do this by first bounding the I_j and the J_j and concluding their integrands are integrable, bounded by rapidly decaying functions. This will immediately give us rapid decay. Smoothness will follow from applying the Leibniz Integral Rule to differentiate with respect to r under the integral sign.

It turns out that we can establish a an upper-bound for all functions of the form $\frac{f}{\Delta}$, where Δ is the discriminant form and f admits a Fourier expansion whose coefficients grow polynomially.

Theorem 4.2.1 ([14, Lemma 7.4]). *Let $f : \mathbb{C} \to \mathbb{C}$ be holomorphic. Denote by $c_f(n)$ its nth Fourier coefficient, with $c_f(n_0) \neq 0$, so that*

$$f(z) = \sum_{n=n_0}^{\infty} c_f(n)\, e^{i\pi n z}$$

If there exists $k \in \mathbb{N}$ such that $c_f(n) = \mathrm{O}(n^k)$ as $n \to \infty$, then there exists a constant $C_f > 0$ such that for all $z \in \mathbb{H}$ with $\mathrm{Im}(z) > 1/2$,

$$\left|\frac{f(z)}{\Delta(z)}\right| \leq C_f\, e^{-\pi(n_0-2)\,\mathrm{Im}(z)}$$

Proof. Fix $z \in \mathbb{H}$ and assume $\mathrm{Im}(z) > 1/2$. Recall from Theorem 2.3.12 that Δ can be expressed as a (convergent) infinite product. We can hence write

$$\left|\frac{f(z)}{\Delta(z)}\right| = \left|\frac{\sum_{n=n_0}^{\infty} c_f(n)\, e^{\pi i n z}}{e^{2\pi i z}\prod_{n=1}^{\infty}\left(1-e^{2\pi i n z}\right)^{24}}\right| = \left|e^{\pi i(n_0-2)z}\right| \cdot \frac{\left|\sum_{n=n_0}^{\infty} c_f(n)\, e^{\pi i(n-n_0)z}\right|}{\prod_{n=1}^{\infty}\left|1-e^{2\pi i n z}\right|^{24}}$$

Noting that $\left|e^{iz}\right| = e^{-\mathrm{Im}(z)}$ and $\mathrm{Im}(z) > \frac{1}{2}$, we can see that

$$\left|e^{\pi i(n_0-2)z}\right| \cdot \frac{\left|\sum_{n=n_0}^{\infty} c_f(n)\, e^{\pi i(n-n_0)z}\right|}{\left|\prod_{n=1}^{\infty} 1-e^{2\pi i n z^{24}}\right|} \leq e^{-\pi(n-n_0)\,\mathrm{Im}(z)} \cdot \frac{\sum_{n=0}^{\infty} |c_f(n)|\; e^{-\pi(n-n_0)/2}}{\left|\prod_{n=1}^{\infty} 1-e^{2\pi i n z^{24}}\right|}$$

It has been verified formally that the absolute value of a convergent infinite product is the product of the absolute values, and moreover, that the product of the absolute values is convergent. It has also been verified formally that the infinite product is monotonic on convergent infinite products whose terms are nonnegative. Hence,

$$\left|\prod_{n=1}^{\infty}\left(1-e^{2\pi i n z}\right)^{24}\right| = \prod_{n=1}^{\infty}\left|1-e^{2\pi i n z}\right|^{24} \geq \prod_{n=1}^{\infty}\left(1-e^{-2\pi n\,\mathrm{Im}(z)}\right)^{24} \geq \prod_{n=1}^{\infty}\left(1-e^{-\pi n}\right)^{24}$$

We note that the third and fourth products are convergent because they are expressible, via the product formula, as $e^{2\pi\,\mathrm{Im}(z)}\Delta(i \cdot \mathrm{Im}(z))$ and $e^{\pi}\Delta(i/2)$ respectively. Hence, defining

$$C_f := \frac{\sum_{n=0}^{\infty} |c_f(n)|\; e^{-\pi(n-n_0)/2}}{\prod_{n=1}^{\infty}\left(1-e^{-\pi n}\right)^{24}}$$

we can see that $\left|\frac{f(z)}{\Delta(z)}\right| \leq C_f\, e^{-\pi(n_0-2)\,\mathrm{Im}(z)}$, as desired. $\square$

The purpose of the above is to bound the ϕ- and ψ-functions using Theorem 4.2.1. Since these functions are defined as sums and products of the Eisenstein series and the H-functions, whose Fourier series have the properties that

1. the coefficients grow polynomially

2. there is an index n_0 below which all Fourier coefficients are zero

it is enough to show that sums and products of functions exhibiting this property inherit it.

Proposition 4.2.2. *Let $f_1, f_2 : \mathbb{H} \to \mathbb{C}$ be have (absolutely convergent) Fourier expansions*

$$f_1(z) = \sum_{n=n_1}^{\infty} c_1(n)\, e^{\pi i n z} \qquad f_2(z) = \sum_{n=n_2}^{\infty} c_2(n)\, e^{\pi i n z}$$

such that for $i \in \{1, 2\}$, $c_i(n_i) \neq 0$ and $\exists k_i \in \mathbb{N}$ such that $c_i(n) = \mathrm{O}\big(n^{k_i}\big)$ as $n \to \infty$. Then, their product $f_1 f_2$ is expressible as an absolutely convergent Fourier series

$$f_1(z) f_2(z) = \sum_{n=n_1+n_2}^{\infty} c(n)\, e^{\pi i n z}$$

such that $c(n_1 + n_2) \neq 0$ and $\exists k \in \mathbb{N}$ such that $c(n) = \mathrm{O}\big(n^{k}\big)$ as $n \to \infty$.

The analogous result for sums is clear, with $n_0 \geq \min(n_1, n_2)$ and $k = \max(k_1, k_2)$. Note that for sums, n_0 may not be exactly $\min(n_1, n_2)$ because the Fourier coefficients of smallest index may cancel each other out. For the remainder of this thesis, we use the following notation.

Notation. For a function f with a Fourier expansion, denote by

- $n_0(f)$ the smallest index n such that $c_f(n) \neq 0$ (if it exists)
- $c_f(n)$ the nth Fourier coefficient of f

We will not use this notation for functions for which $n_0(f)$ does not exist.

In the following subsections, we apply the above results and show that a_{rad} and b_{rad} are Schwartz functions. In each case, since the bound in Theorem 4.2.1 is given in terms of n_0, we compute the values of n_0 explicitly.

4.2.1 The $+1$-Eigenfunction

We begin by proving that $I_1, \ldots, I_6$ decay rapidly. As a first step, we show that we can apply Theorem 4.2.1.

Lemma 4.2.3. *There exist real numbers $C_0, C_{-2}, C_{-4} > 0$ such that*

$$|\phi_0(z)| \leq C_0 e^{-2\pi \operatorname{Im}(z)} \tag{4.2.1}$$
$$|\phi_{-2}(z)| \leq C_{-2} \tag{4.2.2}$$
$$|\phi_{-4}(z)| \leq C_{-4} e^{2\pi \operatorname{Im}(z)} \tag{4.2.3}$$

for all $z \in \mathbb{H}$ with $\operatorname{Im}(z) > \frac{1}{2}$.

Proof. Fix $z \in \mathbb{H}$ and assume that $\operatorname{Im}(z) > 1/2$. Since the Fourier coefficients of E_2, E_4 and E_6 grow polynomially (see Definition 2.3.9 and theorem 2.3.8), by Proposition 4.2.2, the Fourier coefficients of the numerators of ϕ_0, ϕ_{-2} and ϕ_{-4} grow polynomially as well. All that remains is to compute n_0 for the numerators of ϕ_0, ϕ_{-2} and ϕ_{-4}. Denote these N_0, N_{-2} and N_{-4} respectively. Note that $n_0(E_2) = n_0(E_4) = n_0(E_6) = 0$, with $c_{E_2}(0) = c_{E_4}(0) = C_{E_6}(0) = 1$.

- $\underline{N_0 = 4.}$ Recall that the numerator of ϕ_0 is $(E_2E_4 - E_6)^2$. Proposition 4.2.2 then tells us that $n_0(E_2E_4) = 0$. So, $n_0(E_2E_4 - E_6) \geq 0$. In fact, the 0th coefficients of both E_2E_4 and

E_6 are 1, so they cancel. Hence, $n_0(E_2E_4 - E_6) = 2$. Hence, by $n_0\left((E_2E_4 - E_6)^2\right) = 4$.

- $\underline{N_{-2} = 2}$. Recall that the numerator of ϕ_{-2} is $E_4\,(E_2E_4 - E_6)$. $n_0(E_2E_4 - E_6) = 2$ as shown above. Hence, $n_0(E_4\,(E_2E_4 - E_6)) = 2$.
- $\underline{N_{-4} = 0}$. Recall that the numerator of ϕ_0 is E_4^2. Hence, $n_0(E_4^2) = 0$.

Substituting these values into Theorem 4.2.1 then gives us the desired bounds. □

We can now bound I_1, I_3 and I_5.

Lemma 4.2.4. *There exists a positive real number C_0 such that for all $r \in \mathbb{R}$,*

$$|I_1(r)|\,,|I_3(r)|\,,|I_5(r)| \leq \int_1^\infty C_0\,e^{-2\pi s}\,e^{-\pi r/s}\;\mathrm{d}s \tag{4.2.4}$$

Proof. For conciseness, we only bound $|I_1|$ explicitly. Parametrise $z = -1 + it$ in (4.1.7). Then, for all $r \in \mathbb{R}$, we can write

$$I_1(r) = -i\int_0^1 \phi_0\left(\frac{-1}{it}\right)\,t^2\,e^{-\pi ir}\,e^{-\pi rt}\;\mathrm{d}t$$

Writing $s = \frac{1}{t}$ and simplifying, we get that

$$I_1(r) = -i\int_1^\infty \phi_0(is)\;s^{-4}\,e^{-\pi ir}\,e^{-\pi r/s}\;\mathrm{d}t$$

Applying the triangle inequality, multiplicativity and monotonicity, we get

$$|I_1(r)| \leq \int_1^\infty \left|\phi_0(is)\;s^{-4}\,e^{-\pi ir}\,e^{-\pi r/s}\right|\mathrm{d}t \leq \int_1^\infty \left|\phi_0(is)\right|\,e^{-\pi r/s}$$

Since $s > \frac{1}{2}$ inside the integral, we know from Lemma 4.2.3 that $\exists C_0 > 0$ such that

$$|I_1(r)| \leq \int_1^\infty C_0\,e^{-2\pi s}\,e^{-\pi r/s}\;\mathrm{d}s$$

as required. The bounds on $|I_3|$ and $|I_5|$ are computed similarly. □

In similar fashion, arguing by parametrising and applying Theorem 4.2.1, we can show that there exist $C_1, C_2 > 0$ such that

$$|I_2(r)|\,,|I_4(r)| \leq C_1\,e^{-\pi r} \tag{4.2.5}$$

$$|I_6(r)| \leq C_2\,\frac{e^{-\pi(r+2)}}{r+2} \tag{4.2.6}$$

We omit the informal proofs, but note that we have formal proofs in the repository. We discuss this in greater detail in Section 5.1.1.

It is clear that the estimates for $|I_2|$, $|I_4|$ and $|I_6|$ have at least exponential decay, making them more rapidly decaying than any inverse power of r for $r \in [0,\infty)$. For $|I_1|$, $|I_3|$ and $|I_5|$, the result is actually a consequence of deeper results involving the Gamma function.

Lemma 4.2.5. *For all $n \in \mathbb{N}$, there exists a constant C' such that for all $r \geq 0$,*

$$r^n \cdot \int_1^\infty e^{-2\pi s}\, e^{-\pi r/s}\, \mathrm{d}s \leq C'$$

Proof. Fix $n \in \mathbb{N}$. We know there exists a constant C such that for all $x \geq 0$, $|x|^n \cdot |e^{-\pi x}| \leq C$. In particular, for all $r \geq 0$ and $s \geq 1$, $r^n \cdot e^{-\pi r/s} \leq Cs^n$. Hence, for all $r \in \mathbb{R}$, we can write

$$r \cdot \int_1^\infty e^{-2\pi s}\, e^{-\pi r/s}\, \mathrm{d}s = \int_1^\infty e^{-2\pi s} \left(|r|^n \cdot e^{-\pi r/s}\right) \mathrm{d}s \leq C \int_1^\infty e^{-2\pi s}\, s^n\, \mathrm{d}s$$

It was previously known in `mathlib` that the Γ function is given by

$$\Gamma(x) = \int_0^\infty e^{-u}\, u^{x-1}\, \mathrm{d}u$$

for all $x > 0$. Hence, writing $u = 2\pi s$ and relating Γ with the factorial, we get

$$C \int_1^\infty e^{-2\pi s}\, s^n\, \mathrm{d}s \leq C \int_0^\infty e^{-2\pi s}\, s^n\, \mathrm{d}s = C \int_0^\infty \frac{1}{(2\pi)^{n+1}} e^{-u}\, u^n\, \mathrm{d}u = \frac{C}{(2\pi)^n}\Gamma(n+1) = \frac{C \cdot n!}{(2\pi)^n}$$

Defining $C' := \frac{C \cdot n!}{(2\pi)^n}$ finishes the proof. □

This proof has not been formalised, but the road to formalising it is clear.

Next, we show that the I_j are smooth and that their derivatives satisfy similar bounds to the ones computed above.

Lemma 4.2.6. *For all $1 \leq j \leq 6$ and $k \in \mathbb{N}$, $I_j(r)$ is k times differentiable.*

The key to proving this is the Leibniz Integral Rule, which has been formalised previously. It is not difficult to prove informally that the I_j satisfy the conditions laid out in the formal statement of the theorem, though there may be some difficulties when arguing formally. We can use this to show that the derivatives of each I_j can be bounded in the same manner as I_j.

Finally, we note that the $\mathbb{R} \to \mathbb{C}$ function $a_{\text{rad}} = I_1 + \cdots + I_6$ satisfies the Schwartz-like properties outlined in Proposition 3.1.6 because $I_1, \ldots, I_6$ satisfy them. Hence, the $+1$-eigenfunction $a : \mathbb{R}^8 \to \mathbb{C}$, defined as in (4.1.13), lies in the Schwartz space $\mathcal{S}(\mathbb{R}^8, \mathbb{C})$.

4.2.2 The -1-Eigenfunction

At the end of Section 4.1.2, we observed striking similarities between the J_j and the I_j. As a result, much of the proof of Schwartzness is quite similar. Our main strategy is the same: we show that $J_1, \ldots, J_6$ are Schwartz-like and conclude that b must be Schwartz by Proposition 3.1.6.

We begin by proving an analogue of Lemma 4.2.3 for the ψ-functions.

Lemma 4.2.7. *There exist real numbers $C_S, C_I, C_T > 0$ such that*

$$|\psi_S(z)| \leq C_S\, e^{-\pi\, \mathrm{Im}(z)} \tag{4.2.7}$$

$$|\psi_I(z)| \leq C_I \, e^{2\pi \operatorname{Im}(z)} \tag{4.2.8}$$

for all $z \in \mathbb{H}$ *with* $\operatorname{Im}(z) > 1/2$.

Proof. For the purposes of this proof, we will consider the ψ-functions to be expressed as in Proposition 4.1.7. We have seen in Section 2.3.3 that the Fourier coefficients of the H-functions have polynomial growth. From Proposition 4.2.2 and the ensuing discussion, we can see that the numerators of the ψ-functions all admit Fourier expansions with polynomially growing coefficients. All that remains is to explicitly compute the value of n_0 for the numerators.

Denote by N_I, N_S and N_T the values of n_0 for the numerators of ψ_I, ψ_S and ψ_T respectively. From (2.3.15), we can see that $n_0(H_2) = 1$. Furthermore, from Definition 2.3.14, we can see that $n_0(\Theta_3) = n_0(\Theta_4) = 0$, from which we can conclude that $n_0(H_3) = n_0(H_4) = 0$. Finally, $c_{H_2}(1) = 16$ from (2.3.15) and $c_{H_2} = c_{H_3} = 1$ from Definition 2.3.14. We are now ready to compute N_S and N_I.

- $\underline{N_S = 3.}$ Note that $n_0\left(H_2^3\right) = 3$ and the smallest n_0 in the numerator of ψ_S is 0, with none of the n_0th coefficients cancelling. Hence, $N_S = n_0\left(H_2^3\right) = 3$.

- $\underline{N_I = 0.}$ Note that $n_0\left(H_4^3\right) = 0$ and the smallest n_0 in the numerator of ψ_I is 0, with none of the n_0th coefficients cancelling. Hence, $N_I = n_0\left(H_r^3\right) = 0$.

Substituting these into Theorem 4.2.1 then yields the desired result. □

We are now ready to compute bounds on the J_j. Observe that the bounding arguments in Equations (4.2.4) and (4.2.5) and **??** do not use any property of ϕ_0 apart from the bound given in (4.2.1). By inspection (cf. (4.1.37)-(4.1.41) and (4.1.35)), it is possible to replicate those arguments almost verbatim to show that there exist constants $C_S, C_S', C_S'' > 0$ such that

$$|J_1(r)|\,, |J_3(r)|\,, |J_5(r)| \leq \int_1^\infty C_S \, e^{-\pi s} \, e^{-\pi r/s} \, \mathrm{d}s \tag{4.2.9}$$

$$|J_2(r)|\,, |J_4(r)| \leq C_S' \, e^{-\pi r} \tag{4.2.10}$$

$$|J_6(r)| \leq C_S'' \, \frac{e^{-\pi(r+1)}}{\pi\,(r+1)} \tag{4.2.11}$$

We note that some occurrences of 2π in the arguments in Section 4.2.1 must be replaced with occurrences of π because of the differences in the n_0 values of the numerators of ϕ_0 and ψ_S, which means the exponents in (4.2.1) and (4.2.7) are different. However, since they are still negative, this does not affect the argument.

Finally, we note that smoothness and boundedness are, once again, analogous to **??**: the assumptions of the Leibniz Integral Rule are satisfied for the same reasons, and the process of reducing higher derivatives to lower derivatives is nearly identical. We can therefore conclude that b, like a, is a Schwartz function.

4.3 Establishing the Eigenfunction Property

In the previous section, we did not work with a and b directly as it was sufficient to work with a_{rad} and b_{rad} instead. In this section, however, we will need the full strength of the Schwartzness property—specifically, linearity of the Fourier transform—and will need to explicitly compute the n-dimensional Fourier transform of the n-dimensional Gaussian. We will therefore be working in $\mathbb{R}^8$ in this section. The analogous result in $\mathbb{R}$ would not hold.

We begin by stating the following well-known fact.

Theorem 4.3.1 (Fourier Transform of a Gaussian). *Fix $n \in \mathbb{N}$ and $b \in \mathbb{C}$, with $\mathrm{Re}(b) > 0$. If $F : \mathbb{R}^n \to \mathbb{C}$ is given by*

$$F(x) = e^{-b\|x\|^2}$$

then for all $\xi \in \mathbb{R}^n$, the Fourier transform of F is given by

$$\widehat{F}(\xi) = \left(\frac{\pi}{b}\right)^{n/2} e^{-\pi^2\|\xi\|^2/b}$$

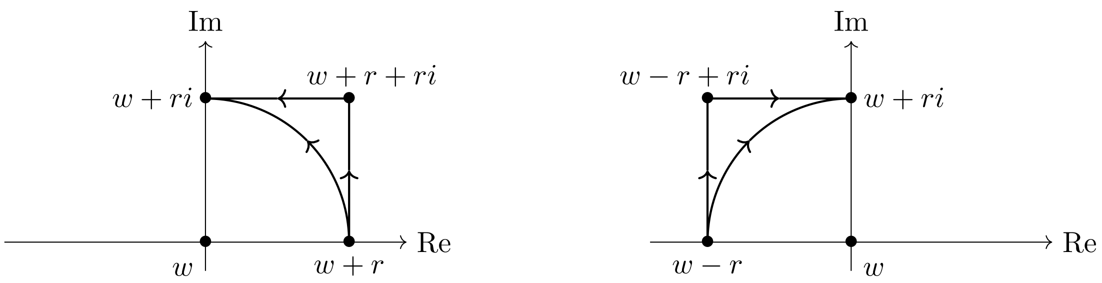
A formal proof exists in `mathlib`.

We will also need the following version of the Cauchy-Goursat Theorem, which allows us to deform contours of integration in the complex plane.

Theorem 4.3.2 (Cauchy-Goursat: Squares and Circles). *Fix $w \in \mathbb{C}$ and $r > 0$. Let γ be the quarter-circle parametrised by $\gamma(t) = w + r\cos(t) + ri\sin(t)$ for $0 \le t \le \pi/2$. For any $f : \mathbb{C} \to \mathbb{C}$ holomorphic in the open region enclosed by γ and the line segments from $w + r$ to $w + r + ir$ and $w + r + ir$ to $w + ir$ and continuous on the corresponding closed region,*

$$\int_\gamma f(z)\ \mathrm{d}z = \int_{w+r}^{w+r+ir} f(z)\ \mathrm{d}z + \int_{w+r+ir}^{w+ir} f(z)\ \mathrm{d}z$$

While this is an immediate consequence of the more general (and well-known) Cauchy-Goursat Theorem from complex analysis, there are numerous challenges involved in formalising this and other versions of the theorem. We will discuss it in Section 5.3. We also note that the above result implies an analogous result that can be proved by a change of variables. See Figure 4.2b.



(a) Contours for which Theorem 4.3.2 holds. **(b)** Contours for which an analogous result holds.

Figure 4.2: The contour deformations permitted by Theorem 4.3.2.

We now prove that a is indeed a $+1$-eigenfunction of the Fourier transform.

4.3.1 The $+1$-Eigenfunction

The Fourier transform acts very interestingly on a. Recall from Theorem 3.1.2 that the Fourier transform is a linear isomorphism of Schwartz spaces. Since $I_1, \ldots, I_6$ are Schwartz, so are their compositions with the norm-squared function. Hence, for all $x \in \mathbb{R}^8$,

$$\mathcal{F}(a(x)) = \mathcal{F}\left(\sum_{j=1}^{6} I_j\left(\|x\|^2\right)\right) = \sum_{j=1}^{6} \mathcal{F}\left(I_j\left(\|x\|^2\right)\right)$$

We will show that $\mathcal{F}$ acts on the $I_j\left(\|x\|^2\right)$ in the following manner:[1]

$$\mathcal{F}\left(I_1\left(\|x\|^2\right) + I_2\left(\|x\|^2\right)\right) = I_3\left(\|x\|^2\right) + I_4\left(\|x\|^2\right) \tag{4.3.1}$$

$$\mathcal{F}\left(I_3\left(\|x\|^2\right) + I_4\left(\|x\|^2\right)\right) = I_1\left(\|x\|^2\right) + I_2\left(\|x\|^2\right) \tag{4.3.2}$$

$$\mathcal{F}\left(I_5\left(\|x\|^2\right)\right) = I_6\left(\|x\|^2\right) \tag{4.3.3}$$

$$\mathcal{F}\left(I_6\left(\|x\|^2\right)\right) = I_5\left(\|x\|^2\right) \tag{4.3.4}$$

Since, in addition to being Schwartz, all the $I_j\left(\|x\|^2\right)$ (and their sums) are radial, Proposition 3.1.4 tells us that (4.3.2) and (4.3.4) follow from (4.3.1) and (4.3.3) respectively. As a preliminary step, though, we need to show that

$$(x, z) \mapsto f\left(\|x\|^2, z\right)$$

admits an absolutely convergent integral over $\mathbb{R}^8 \times X_j$. It has previously been formally verified that proving this is equivalent to proving the following two facts.

1. The integral over X_j of the function $z \mapsto f\left(\|x\|^2, z\right)$ is absolutely convergent for almost every $x \in \mathbb{R}^8$.
2. The integral over $\mathbb{R}^8$ of the function $x \mapsto \int_{X_j} \left|f\left(\|x^2\|, z\right)\right| \mathrm{d}z$ is absolutely convergent.

These easily follow from the arguments in Section 4.2.1. Since the function is also clearly measurable, we can swap integrals freely using Fubini's theorem to prove the eigenfunction property. This has previously been formalised.

Lemma 4.3.3. *The Fourier transform maps* $I_1\left(\|x\|^2\right) + I_2\left(\|x\|^2\right)$ *to* $I_3\left(\|x\|^2\right) + I_4\left(\|x\|^2\right)$.

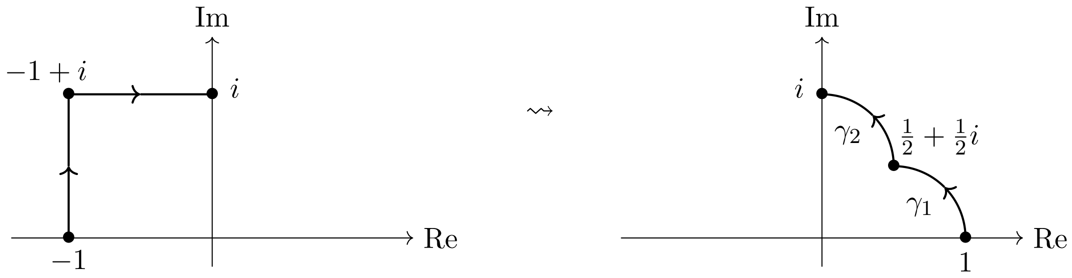
Proof. Since $\mathcal{F}$ acts linearly, we can treat I_1 and I_2 separately. For the purpose of this proof, denote the Fourier transforms of $I_1\left(\|x\|^2\right)$ and $I_2\left(\|x\|^2\right)$ by F_1 and F_2 respectively. Fix $\xi \in \mathbb{R}^8$. Integrability allows us to write

$$F_1(\xi) = \int_{-1}^{-1+i} \phi_0\left(\frac{-1}{z+1}\right) (z+1)^2 \left(\int_{\mathbb{R}^8} e^{\pi i \|x\|^2 z} e^{-2\pi i \langle x, \xi\rangle}\, \mathrm{d}x\right) \mathrm{d}z$$

We may therefore apply Theorem 4.3.1 and write

$$F_1(\xi) = \int_{-1}^{-1+i} \phi_0\left(\frac{-1}{z+1}\right) (z+1)^2\, z^{-4}\, e^{\pi i \|\xi\|^2 \left(\frac{-1}{z}\right)}\, \mathrm{d}z$$

$$F_2(\xi) = \int_{-1+i}^{i} \phi_0\left(\frac{-1}{z+1}\right) (z+1)^2\, z^{-4}\, e^{\pi i \|\xi\|^2 \left(\frac{-1}{z}\right)}\, \mathrm{d}z$$



(a) Before the transformation **(b)** After the transformation

Figure 4.3: The effect of the Möbius transformation $z \mapsto -1/z$ on the contours of F_1 and F_2

We make a change of variables $w = \frac{-1}{z}$ in the above integrals. This Möbius transformation turns the vertical and horizontal contours in F_1 and F_2 into quarter-circular contours that we denote γ_1 and γ_2 respectively. See Figure 4.3.

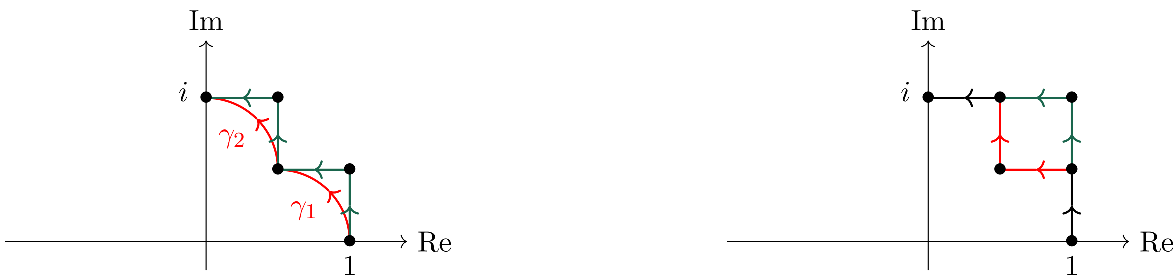
We write

$$f(w,\xi) = \phi_0\left(-1 - \frac{1}{w-1}\right)\left(\frac{-1}{w}+1\right)^2 w^2\, e^{\pi i \|\xi\|^2 w} = \phi_0\left(\frac{-1}{w-1}\right)(w-1)^2\, e^{\pi i \|\xi\|^2 w}$$

by (4.1.4). One can show f to be holomorphic (in w) on $\mathbb{H}$ and continuous on the closed regions in question because of (4.1.5). Applying Theorem 4.3.2, followed by an analogous, previously formalised result, we can show that changing contours as we do in Figure 4.4 then tells us that

$$F_1(\xi) + F_2(\xi) = I_3\left(\|\xi\|^2\right) + I_4\left(\|\xi\|^2\right)$$

as required. □



(a) Changing contours from circles to rectangles **(b)** Changing rectangular contours to get I_3 and I_4

Figure 4.4: Applying the two versions of the Cauchy-Goursat Theorem to prove the result. In the proof, contours were changed from red to green.

The proof that the Fourier transform maps I_5 to I_6 is nearly identical in structure but significantly simpler, because the Möbius transformation $z \mapsto \frac{-1}{z}$ simply maps the contour in I_5 to that in I_6 (and vice-versa). In summary, the Fourier transform permutes the integrals that make up a, thereby not changing a. a is thus an eigenfunction of $\mathcal{F}$ with eigenvalue 1.

We now use similar techniques to show that b is a Fourier eigenfunction with eigenvalue -1.

[1]Note that we are abusing notation by denoting the function $x \mapsto I_j\left(\|x\|^2\right) \in \mathcal{S}(\mathbb{R}^8, \mathbb{C})$ by $I_j\left(\|x\|^2\right)$.

4.3.2 The -1-Eigenfunction

Just as with the integrals of a, the 8-dimensional Fourier transform permutes the integrals that make up b. The difference, however, is that it reverses signs in the process. Specifically,

$$\mathcal{F}\left(J_1\left(\|x\|^2\right) + J_2\left(\|x\|^2\right)\right) = -J_3\left(\|x\|^2\right) - J_4\left(\|x\|^2\right) \tag{4.3.5}$$
$$\mathcal{F}\left(I_5\left(\|x\|^2\right)\right) = -I_6\left(\|x\|^2\right) \tag{4.3.6}$$

with the inverse results following from linearity and Proposition 3.1.4.

First, we note that we have integrability for the same reason we did in Section 4.3.1. We thus prove an analogue of Lemma 4.3.3.

Lemma 4.3.4. *The Fourier transform maps $J_1\left(\|x\|^2\right)+J_2\left(\|x\|^2\right)$ to $-J_3\left(\|x\|^2\right)-J_4\left(\|x\|^2\right)$.*

Proof. Again, since $\mathcal{F}$ acts linearly, we can treat J_1 and J_2 separately. For the purpose of this proof, denote the Fourier transforms of $J_1\left(\|x\|^2\right)$ and $J_2\left(\|x\|^2\right)$ by F_1 and F_2 respectively. As before, we may exchange the order of the integrals and write, for all $\xi \in \mathbb{R}^8$,

$$F_1 = \int_{-1}^{-1+i} \psi_T(z)\, z^{-4}\, e^{\pi i \|\xi\|^2 \left(\frac{-1}{z}\right)}\, \mathrm{d}z$$
$$F_2 = \int_{-1+i}^{i} \psi_T(z)\, z^{-4}\, e^{\pi i \|\xi\|^2 \left(\frac{-1}{z}\right)}\, \mathrm{d}z$$

Again, we change variables via the Möbius transformation $w = \frac{-1}{z}$. Denoting by f the integrand (with respect to w) of F_1 and F_2, we have

$$f(w, \xi) = \psi_T\left(\frac{-1}{w}\right)\, w^2\, e^{\pi i \|\xi\|^2 w} = -\psi_T(w)\, e^{\pi i \|\xi\|^2 w}$$

by (4.1.22). Noting further that f is holomorphic in w because of Proposition 4.1.7, we can prove the result by deforming contours in exactly the same manner as we did in the proof of Lemma 4.3.3. See Figure 4.4. □

An analogous argument shows that $\mathcal{F}\left(J_5\left(\|x\|^2\right)\right) = -J_6\left(\|x\|^2\right)$. The key difference is that we use the fact that $\psi_S = \psi_I \mid_{-2} S$ instead of the fact that $\psi_T \mid_{-2} S = -\psi_T$. Furthermore, the sign change in the case of J_5 comes not from applying a slash relation but from the fact that the Möbius transformation $z \mapsto \frac{-1}{z}$ reverses the direction of the contours.

4.4 Establishing the Double Zeroes Property

The way we prove that a and b have double zeroes at E_8 lattice points with norm $> \sqrt{2}$ is by showing that a_{rad} and b_{rad} agree, for $r > 2$, with functions that have double zeroes at *all* even integers. It will then follow that a and b have double zeroes at all points on the E_8 lattice with norm $> \sqrt{2}$, since all elements of Λ_8 have norm of the form $\sqrt{2n}$ for some $n \in \mathbb{N}$ (cf. Proposition 2.1.7).

The strategy to prove these two equalities will be to perform a change of contours using a version of the Cauchy-Goursat Theorem and use the relations and transformation rules between the ϕ- and ψ-functions to combine integrals so that the result is exactly a_{rad} or b_{rad}.

The version of the Cauchy-Goursat Theorem we use is the following.

Theorem 4.4.1 (Cauchy-Goursat for Unbounded Contours). *Suppose $f : \mathbb{C} \to \mathbb{C}$ is a function such that $f(z) \to 0$ as $\mathrm{Im}(z) \to \infty$. Then, for all $x_1, y_1, x_2, y_2 \in \mathbb{R}$, if f is holomorphic at z for all $z \in \mathbb{C}$ with $x_1 < \mathrm{Re}(z) < x_2$ and $y_1 < \mathrm{Im}(z)$, then*

$$\int_{x_1+iy_1}^{x_1+i\infty} f(z)\,\mathrm{d}z = \int_{x_1+iy_1}^{x_1+iy_2} f(z)\,\mathrm{d}z + \int_{x_1+iy_2}^{x_2+iy_2} f(z)\,\mathrm{d}z + \int_{x_2+iy_2}^{x_2+i\infty} f(z)\,\mathrm{d}z$$

provided that f is integrable on the unbounded vertical contours.

We discuss the informal and formal proofs of this theorem in Section 5.3.

For both a_{rad} and b_{rad}, we begin by their alternate expressions for them. We then make estimates to prove that the integrals in these expressions converge. We finally manipulate the expressions and apply Theorem 4.4.1 to show that they do, indeed, agree with a_{rad} and b_{rad} on inputs > 2.

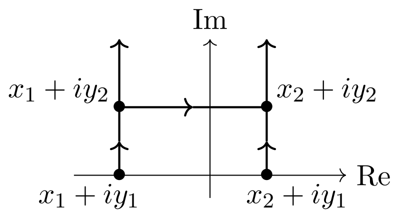


Figure 4.5: Visualising the contours in Theorem 4.4.1.

4.4.1 The $+1$-Eigenfunction

We begin by defining the integral by which we represent a_{rad}.

Definition 4.4.2 (Alternate Representation of a_{rad}). Define $d : (2, \infty) \to \mathbb{C}$ by

$$d(r) = -4\sin^2\left(\frac{\pi r}{2}\right) \int_0^{i\infty} \phi_0\left(\frac{-1}{z}\right) z^2\, e^{\pi i r z}\,\mathrm{d}z$$

for all $r \in (2, \infty)$.

It is clear that we can parametrise the integral in d by $z = it$ for $t \in (0, \infty)$, and write

$$d(r) = 4i\sin^2\left(\frac{\pi r}{2}\right) \int_0^{\infty} \phi_0\left(\frac{i}{t}\right) t^2\, e^{-\pi r t}\,\mathrm{d}t \tag{4.4.1}$$

We now show that this integral converges for $r > 2$. We do this by estimating the integrand.

Lemma 4.4.3. *$\exists C_0 > 0$ such that for $t \in (0, 2)$, $\left|\phi_0\left(\frac{i}{t}\right)\right| \le C_0\, e^{-2\pi/t}$.*

Proof. This follows immediately from (4.2.1), with $z = i/t$. □

We can hence conclude that for $t \in (0, 2)$, the integrand in (4.4.1) is bounded:

$$\left|\phi_0\left(\frac{i}{t}\right) t^2\, e^{-\pi r t}\right| \le 4C_0\, e^{-2\pi/t}\, e^{-\pi r t} \le 4C_0$$

We can also estimate the integrand for $t \ge 2$.

Lemma 4.4.4. *$\exists C > 0$ such that for $t \geq 2$, $\left|\phi_0\left(\frac{i}{t}\right)\right| \leq Ct^{-2}e^{2\pi t}$.*

Proof. From (4.1.5), we know that for all $t \geq 2$,

$$\left|\phi_0\left(\frac{i}{t}\right)\right| = \left|\phi_0\left(\frac{-1}{it}\right)\right| \leq |\phi_{0(it)}| + \frac{12}{\pi t}\left|\phi_{-2}(it)\right| + \frac{36}{\pi^2 t^2}\left|\phi_{-4}(it)\right|$$

Estimating each of these terms using Lemma 4.2.3, we know $\exists C_0, C_{-2}, C_{-4} > 0$ such that

$$|\phi_0(it)| + \frac{12}{\pi t}|\phi_{-2}(it)| + \frac{36}{\pi^2 t^2}|\phi_{-4}(it)| \leq C_0 e^{-2\pi t} + \frac{12}{\pi t}C_{-2} + \frac{36}{\pi^2 t^2}C_{-4}e^{2\pi t}$$

For $t \geq 2$, $C_0 e^{-2\pi t}$ and $\frac{12}{\pi t}C_{-2}$ are clearly bounded by constants, and the growth of the above expression is dominated by $t^{-2}e^{2\pi t}$. Hence, we can conclude that $\exists C > 0$ such that for $t \geq 2$, $\left|\phi_0\left(\frac{i}{t}\right)\right| \leq Ct^{-2}e^{2\pi t}$, as required. $\square$

We can hence conclude that for $t \geq 2$, the integrand in (4.4.1) is bounded by an integrable function:

$$\left|\phi_0\left(\frac{i}{t}\right)\, t^2\, e^{-\pi r t}\right| \leq C\left(t^{-2}e^{2\pi t}\right)\left(t^2 e^{-\pi r t}\right) = Ce^{\pi t(2-r)}$$

Here, we require $r > 2$ so that the exponent is negative. Since d was defined precisely on such r, we can conclude that the integral in the definition of d converges absolutely.

Arguing as above yields another important result.

Lemma 4.4.5. *For all $r > 2$ and $z \in \mathbb{H}$, as $\operatorname{Im}(z) \to \infty$,*

$$\phi_0\left(\frac{-1}{z}\right)\, z^2\, e^{\pi i r z} \to 0$$

The function $z \mapsto \phi_0\left(\frac{-1}{z}\right)\, z^2\, e^{\pi i r z}$ is also holomorphic on $\mathbb{H}$, a fact that is again seen by applying (4.1.5) and the fact that the numerators of the ϕ-function are holomorphic and the denominators are non-vanishing on $\mathbb{H}$.

We are now ready for the main result of this subsection.

Proposition 4.4.6. *For all $r > 2$, $d(r) = a_{\text{rad}}(r)$.*

Proof. Fix $r > 2$. Write $-4\sin^2\left(\frac{\pi r}{2}\right) = e^{i\pi r} - 2 + e^{-i\pi r}$. Then, for all $r > 2$, we can write

$$d(r) = \int_0^{i\infty} \phi_0\left(\frac{-1}{z}\right) z^2 e^{\pi i r(z-1)}\, \mathrm{d}z + \int_0^{i\infty} \phi_0\left(\frac{-1}{z-1}\right)(z-1)^2\, e^{\pi i r z}\, \mathrm{d}z + \int_0^{i\infty} \phi_0\left(\frac{-1}{z}\right) z^2 e^{\pi i r(z+1)}\, \mathrm{d}z \tag{4.4.2}$$

Changing variables, we can express the integrals as follows.

$$\int_0^{i\infty} \phi_0\left(\frac{-1}{z}\right) z^2\, e^{\pi i r(z-1)}\, \mathrm{d}z = \int_{-1}^{-1+i\infty} \phi_0\left(\frac{-1}{z+1}\right)(z+1)^2\, e^{\pi i r z}\, \mathrm{d}z$$

$$\int_0^{i\infty} \phi_0\left(\frac{-1}{z}\right) z^2\, e^{\pi i r(z+1)}\ \mathrm{d}z = \int_1^{1+i\infty} \phi_0\left(\frac{-1}{z-1}\right) (z-1)^2\ e^{\pi i r z}\ \mathrm{d}z$$

$$-2\int_0^{i\infty} \phi_0\left(\frac{-1}{z}\right) z^2\, e^{\pi i r z}\ \mathrm{d}z = \underbrace{-2\int_0^{i} \phi_0\left(\frac{-1}{z}\right) z^2\, e^{\pi i r z}\ \mathrm{d}z}_{I_5} - 2\int_i^{i\infty} \phi_0\left(\frac{-1}{z}\right) z^2\, e^{\pi i r z}\ \mathrm{d}z$$

We can now apply Theorem 4.4.1 to the first and third integrals, noting that the required integrability conditions do hold because the integrals making up d and a_{rad} converge absolutely.

$$\begin{aligned}
\int_{-1}^{-1+i\infty} \phi_0\left(\frac{-1}{z+1}\right) (z+1)^2\ e^{\pi i r z}\ \mathrm{d}z &= \underbrace{\int_{-1}^{-1+i} \phi_0\left(\frac{-1}{z+1}\right) (z+1)^2\ e^{\pi i r z}\ \mathrm{d}z}_{I_1} \\
&\quad + \underbrace{\int_{-1+i}^{i} \phi_0\left(\frac{-1}{z+1}\right) (z+1)^2\ e^{\pi i r z}\ \mathrm{d}z}_{I_2} \\
&\quad + \int_{i}^{i\infty} \phi_0\left(\frac{-1}{z+1}\right) (z+1)^2\ e^{\pi i r z}\ \mathrm{d}z \\
\int_{1}^{1+i\infty} \phi_0\left(\frac{-1}{z-1}\right) (z-1)^2\ e^{\pi i r z}\ \mathrm{d}z &= \underbrace{\int_{1}^{1+i} \phi_0\left(\frac{-1}{z-1}\right) (z-1)^2\ e^{\pi i r z}\ \mathrm{d}z}_{I_3} \\
&\quad + \underbrace{\int_{1+i}^{i} \phi_0\left(\frac{-1}{z-1}\right) (z-1)^2\ e^{\pi i r z}\ \mathrm{d}z}_{I_4} \\
&\quad + \int_{i}^{i\infty} \phi_0\left(\frac{-1}{z-1}\right) (z-1)^2\ e^{\pi i r z}\ \mathrm{d}z
\end{aligned}$$

Hence, we can express $d(r)$ as the sum of the following six integrals:

$$\begin{aligned}
d(r) = & I_1(r) + I_2(r) + I_3(r) + I_4(r) + I_5(r) \\
& + \int_i^{i\infty} \left(\phi_0\left(\frac{-1}{z+1}\right) (z+1)^2\ e^{\pi i r z} + \phi_0\left(\frac{-1}{z-1}\right) (z-1)^2\ e^{\pi i r z} - 2\phi_0\left(\frac{-1}{z}\right) z^2\, e^{\pi i r z}\right) \mathrm{d}z
\end{aligned}$$

One can show, by applying (4.1.5) and simplifying, that

$$\phi_0\left(\frac{-1}{z+1}\right) (z+1)^2 + \phi_0\left(\frac{-1}{z-1}\right) (z-1)^2 + \phi_0\left(\frac{-1}{z}\right) z^2 = 2\phi_0$$

Hence, the sixth integral above is precisely I_6, proving that $d(r) = a_{\mathrm{rad}}(r)$ for all $r > 2$. □

The factor of $-4\sin^2(\pi r/2)$ in the definition of d then ensures that a_{rad} has double zeroes at all even integers except possibly 0 and ± 2, which allows us to conclude that a has double zeroes at all points in $\mathbb{R}^8$—particularly those lying on Λ_8—with norm of the form $\sqrt{2n}$ for $n \in \mathbb{N} \setminus \{0, 1\}$.

4.4.2 The -1-Eigenfunction

We begin by defining the integral by which we represent b_{rad}.

Definition 4.4.7 (Alternate Representation of b_{rad}). Define $c : (2, \infty) \to \mathbb{C}$ by

$$c(r) = -4 \sin^2\left(\frac{\pi r}{2}\right) \int_0^{i\infty} \psi_I(z)\; e^{\pi i r z}\; \mathrm{d}z$$

for all $r \in (2, \infty)$.

It is clear that we can parametrise the integral in d by $z = it$ for $t \in (0, \infty)$, and write

$$d(r) = 4i \sin^2\left(\frac{\pi r}{2}\right) \int_0^{\infty} \psi_T(it)\; e^{-\pi r t}\; \mathrm{d}t \tag{4.4.3}$$

We now show that this integral converges for $r > 2$. We do this by estimating the integrand.

Lemma 4.4.8. *$\exists C_S > 0$ such that for $t \in (0, 2)$, $|\psi_I(it)| \le C_S\, t^2\, e^{\pi/t}$.*

Proof. From (4.1.18), we know that for all $t \in (0, 2)$,

$$|\psi_I(it)| = \left|(it)^2\; \psi_S\left(\frac{-1}{it}\right)\right| = t^2 \left|\psi_S\left(\frac{i}{t}\right)\right|$$

Since $t < 2$, $\frac{1}{t} > \frac{1}{2}$. Hence, Lemma 4.2.7 is applicable and yields exactly the desired result. □

Since $(0, 2)$ is clearly bounded, we can conclude that the integrand in (4.4.3) is bounded for $t \in (0, 2)$.

In similar fashion, we can estimate the integrand for $t \ge 2$.

Lemma 4.4.9. *$\exists C > 0$ such that for all $t \ge 2$, $|\psi_I(it)| \le Ce^{2\pi t}$.*

Proof. This follows immediately from (4.2.8), with $z = it$. □

We can hence conclude that for $t \ge 2$, the integrand in (4.4.3) is bounded by an integrable function:

$$\left|\psi_I(it)\; e^{-\pi r t}\right| \le C\, e^{\pi t (2 - r)}$$

where, as with d in the previous subsection, we require $r > 2$ for the exponent $2 - r$ to be negative. We can hence conclude that c converges absolutely. This gives us the integrability condition that is necessary to apply Theorem 4.4.1. Indeed, this bound also tells us, as it did in Lemma 4.4.5, that

Lemma 4.4.10. *For all $r > 2$ and $z \in \mathbb{H}$, as $\operatorname{Im}(z) \to \infty$,*

$$\psi_I(z)\; e^{\pi i r z} \to 0$$

We end our discussion on the integrand by remarking that it is holomorphic, as was discussed immediately after Proposition 4.1.7. We are now ready for the main result of this subsection.

Proposition 4.4.11. *For all $r > 2$, $c(r) = b_{\text{rad}}(r)$.*

Proof. Fix $r > 2$. As in (4.4.2), we can write

$$c(r) = \int_{-1}^{-1+i\infty} \psi_I(z+1)\, e^{i\pi r z}\, \mathrm{d}z - 2\int_0^{i\infty} \psi_I(z)\, e^{i\pi r z}\, \mathrm{d}z + \int_1^{1+i\infty} \psi_I(z-1)\, e^{i\pi r z}\, \mathrm{d}z$$

We may now apply Theorem 4.4.1 and write

$$\begin{aligned}
\int_{-1}^{-1+i\infty} \psi_I(z+1)\, e^{i\pi r z}\, \mathrm{d}z &= \underbrace{\int_{-1}^{-1+i} \psi_I(z+1)\, e^{i\pi r z}\, \mathrm{d}z}_{J_1} \\
&\quad + \underbrace{\int_{-1+i}^{i} \psi_I(z+1)\, e^{i\pi r z}\, \mathrm{d}z}_{J_2} \\
&\quad + \int_{i}^{i\infty} \psi_I(z+1)\, e^{i\pi r z}\, \mathrm{d}z \\
\int_{1}^{1+i\infty} \psi_I(z-1)\, e^{i\pi r z}\, \mathrm{d}z &= \underbrace{\int_{1}^{1+i} \psi_I(z-1)\, e^{i\pi r z}\, \mathrm{d}z}_{J_3} \\
&\quad + \underbrace{\int_{1+i}^{i} \psi_I(z-1)\, e^{i\pi r z}\, \mathrm{d}z}_{J_4} \\
&\quad + \int_{i}^{i\infty} \psi_I(z-1)\, e^{i\pi r z}\, \mathrm{d}z
\end{aligned}$$

Applying (4.1.15), (4.1.16) and (4.1.28) tells us that $\psi_S = \psi_T - \psi_I$. Hence,

$$c(r) = J_1(r) + J_2(r) + J_3(r) + J_4(r) + J_5(r) + J_6(r) = b_{\text{rad}}(r)$$

for $r > 2$, as required. □

We can therefore conclude that b has double zeroes at all points on Λ_8 with norm $> \sqrt{2}$.

4.5 Another Representation of the Eigenfunctions

At this stage, it is worth consolidating the results proven thus far. In Section 3.3, we mentioned numerous *necessary* conditions for eigenfunctions to satisfy. The fact that it is immensely difficult to find functions satisfying such conditions, juxtaposed with the fact that we have done precisely that, is an indication that we are on the right track. However, it is still not clear how to compute g as a linear combination of a and b and show it satisfies the Cohn-Elkies conditions. We need information about the behaviour of a_{rad} and b_{rad} on specific points in $[0, \infty)$.

It will turn out that (CE2) is a consequence of the alternate representations of a and b constructed in Section 4.4. d and c, however, are only defined on $(2, \infty)$, so they do not provide us with information on what happens closer to 0, which we need for (CE3). Viazovska's solution was to analytically continue d and c to all of $[0, \infty)$. This will help us prove not only (CE3) but also that $g(0) = \widehat{g}(0)$, which, as discussed in Section 3.3, will show us that the bound obtained by applying Theorem 2.2.5 will be the right one.

4.5.1 The $+1$-Eigenfunction

We begin by defining the following integral.

Definition 4.5.1. Define $\widetilde{d} : [0, \infty) \to \mathbb{R}$ by

$$\widetilde{d}(r) := 4i \sin^2\left(\frac{\pi r}{2}\right) \left(-\frac{36}{\pi^3 (r-2)} + \frac{8640}{\pi^3 r^2} - \frac{18144}{\pi^3 r} + \int_0^\infty \left(t^2 \phi_0\left(\frac{i}{t}\right) - \frac{36}{\pi^2} e^{2\pi t} + \frac{8640}{\pi} - \frac{18144}{\pi^2} \right) e^{-\pi r t} \, \mathrm{d}t \right)$$

We note that $\widetilde{d}$ is indeed well-defined at 0 and freely consider it as a $[0, \infty) \to \mathbb{R}$ function. Observe that for $r > 2$

$$\int_0^\infty \left(\frac{36}{\pi^2} e^{2\pi t} - \frac{8640}{\pi} + \frac{18144}{\pi^2} \right) e^{-\pi r t} \, \mathrm{d}t = \frac{36}{\pi^3 (r-2)} - \frac{8640}{\pi^3 r^2} + \frac{18144}{\pi^3 r}$$

Thus, for all $r > 2$, $\widetilde{d} = d$. So, $\widetilde{d}$ is a continuation of d from $(2, \infty)$ to $[0, \infty)$. However, it is not immediately clear that $\widetilde{d}$ is analytic.

Viazovska proceeds by computing the Fourier expansion of $\phi_0(i/t)$ and showing that

$$t^2 \, \phi_0\left(\frac{i}{t}\right) = \frac{36}{\pi^2} e^{2\pi t} - \frac{8640}{\pi} + \frac{18144}{\pi^2} + \mathrm{O}\left(t^2 \, e^{-2\pi t}\right)$$

as $t \to \infty$ [1, (39)]. One can then conclude that the integral in $\widetilde{d}$ converges absolutely for all $r \geq 0$. It is then clear that $\widetilde{d}$ is analytic on $[0, \infty)$. Since a_{rad} is smooth, hence analytic, on $[0, \infty)$ as well, by the identity principle for analytic functions, which has previously been formalised, we can conclude that $a_{\text{rad}} = \widetilde{d}$ on $[0, \infty)$.

Finally, we note that

$$a(0) = a_{\text{rad}}(0) = \widetilde{d}(0) = \frac{-i8640}{\pi}$$

which can be seen by computing the limits as $r \to 0$ in the expression for $\widetilde{d}$.

4.5.2 The -1-Eigenfunction

We proceed analogously.

Definition 4.5.2. Define $\widetilde{c} : [0, \infty) \to \mathbb{R}$ by

$$\widetilde{d}(r) := 4i \sin^2\left(\frac{\pi r}{2}\right) \left(\frac{144}{\pi r} + \frac{1}{\pi (r-2)} + + \int_0^\infty \left(\psi_I(it) - 144 - e^{2\pi t} \right) e^{-\pi r t} \, \mathrm{d}t \right)$$

Observe that for $r > 2$

$$\int_0^\infty \left(144 + e^{2\pi t}\right) e^{-\pi r t} \, \mathrm{d}t = \frac{144}{\pi r} + \frac{1}{\pi (r-2)}$$

Thus, for all $r > 2$, $\widetilde{c} = c$. So, $\widetilde{c}$ is clearly a continuation of c from $(2, \infty)$ to $[0, \infty)$. However, it is not immediately clear that $\widetilde{c}$ is analytic.

Again, Viazovska proceeds by computing the Fourier expansion of $\psi_I(it)$ and showing that

$$\phi_I(it) = 144 + e^{2\pi t} + \mathrm{O}\big(e^{-\pi t}\big)$$

as $t \to \infty$ [1, (39)]. One can then conclude that the integral in $\widetilde{c}$ converges absolutely for all $r \geq 0$. It is then clear that $\widetilde{c}$ is analytic on $[0, \infty)$. We conclude just as we did for a.

Finally, we note that

$$b(0) = b_{\text{rad}}(0) = \widetilde{c}(0) = 0$$

4.6 The Magic of g

In this section, we briefly describe the construction of g. We recall that we want g to satisfy

(Property 1) For all $x \in \mathbb{R}^8$, $g(x) \in \mathbb{R}$

(Property 2) For all $x \in \mathbb{R}^8$, if $\|x\| \geq \sqrt{2}$, then $g(x) \leq 0$

(Property 3) For all $x \in \mathbb{R}^8$, $\widehat{g}(x) \geq 0$

(Property 4) For all $x \in \mathbb{R}^8$, $g(0) = \widehat{g}(0)$

as discussed in Section 3.3. We now define g.

Definition 4.6.1 (Viazovska's Magic Function). Define $g \in \mathcal{S}\big(\mathbb{R}^8, \mathbb{C}\big)$ by

$$g = \frac{\pi i}{8640} a + \frac{i}{240\pi} b$$

and define g_{rad} to be the same linear combination of a_{rad} and b_{rad}.

It is obvious that $g(x) = g_{\text{rad}}\big(\|x\|^2\big)$ for all $x \in \mathbb{R}^8$.

Clearly, g is Schwartz because g is a linear combination of Schwartz functions. Furthermore, (Property 4) is immediate:

$$g(0) = \widehat{g}(0) = \frac{\pi i}{8640} \cdot \frac{-8640 i}{\pi} = 1$$

We now define two auxiliary functions A and B.

Definition 4.6.2 (Auxiliary Functions for Viazovska's Inequalities). For $t \in [0, \infty)$, define

$$A(t) = -t^2\, \phi_0\left(\frac{i}{t}\right) - \frac{36}{\pi^2}\psi_I(it)$$
$$B(t) = -t^2\, \phi_0\left(\frac{i}{t}\right) + \frac{36}{\pi^2}\psi_I(it)$$

Observe that for all $r > 2$, if we write $a_{\text{rad}} = d$ and $b_{\text{rad}} = c$, we have

$$g_{\text{rad}}(r) = \frac{\pi}{2160} \sin^2\left(\frac{\pi r}{2}\right) \int_0^\infty A(t)\, e^{-\pi r t} \,\mathrm{d}t$$

as argued in Section 4.4. Furthermore, observe that

$$\widehat{g} = \frac{\pi i}{8640} a - \frac{i}{240\pi} b \tag{4.6.1}$$

and denote by $\widehat{g}_{\text{rad}}$ the analogous linear combination of a_{rad} and b_{rad}. In similar fashion, as argued in Section 4.5, for all $r \geq 0$,

$$\widehat{g}_{\text{rad}} = \frac{\pi}{2160} \sin^2\left(\frac{\pi r}{2}\right) \int_0^\infty B(t)\, e^{0\pi r t} \,\mathrm{d}t \tag{4.6.2}$$

It is possible to show that for all $t \in (0, \infty)$,

$$A(t) \in \mathbb{R}_{<0} \tag{4.6.3}$$

$$B(t) \in \mathbb{R}_{>0} \tag{4.6.4}$$

There are numerous ways of showing these inequalities, the details of all of which are beyond the scope of this thesis. We briefly discuss three different approaches below, but do not offer further details.

Viazovska's original approach in [1] was to perform asymptotic analyses and interval arithmetic, taking advantage of Fourier coefficient properties of weakly holomorphic modular forms, to estimate A and B to arbitrary precision and show that they are negative. Particularly, Viazovska's proof involved computer calculations. In 2023, Romik [24] proved the inequalities in a manner that did not rely on such calculations: instead, he proved the result using functional equations arising from the theory of modular forms, such as those listed in Section 4.1.2. In 2024, when the collaboration to formalise Viazovska's work was initiated, there was some discussion as to whether this was the best approach. It was ultimately decided that an algebraic proof by Lee [25], which uses the theory of quasimodular forms, particularly the positivity-preservation properties of Serre and anti-Serre derivatives. These fall significantly outside the scope of this project.

We end by noting that (4.6.3) and (4.6.4) imply that g is real-valued, proving (Property 1); that (4.6.3) directly implies (Property 2); and (4.6.4) directly implies (Property 3).

Chapter 5

Viazovska's Magic Function, Formally

In this chapter, we discuss aspects of the formalisation that we alluded to, but did not discuss in detail, in Chapter 4.

Throughout Chapter 4, particularly in Sections 4.1, 4.2 and 4.4, we provided incredibly detailed arguments. The purpose of doing this was to ensure a correspondence between the informal text in this document and the formal proof or proof path written or envisioned by the author. This approach was also intended to pre-empt challenges that would be faced when ultimately formalising Viazovska's proof.

We note that while the formalisation is still actively in progress, over the course of this M4R, the author has made significant progress towards formalising the contents of Chapter 4. These steps are highlighted across this chapter. In Section 5.1, we give a broad overview of the author's contributions and account for the minor but deliberate and carefully considered differences between Viazovska's original proof in [1] and the author's exposition of it in Chapter 4. In Section 5.2, we briefly discuss an innovative approach conceived by Macbeth and the author to simplify computations in $\mathbb{C}$, which has since been implemented with significant contributions by Xie. In Section 5.3, we discuss the nuances that make the Cauchy-Goursat Theorem, an integral part of Viazovska's proof, a challenging theorem to formalise, and outline how some, but not all, of these challenges have been overcome by the author over the course of this M4R.

5.1 The Formalisation Effort: A Broad Overview

As was mentioned in Chapter 1, the formalisation of Viazovska's proof was initiated by Viazovska and Hariharan in March 2024. A public announcement was made in June 2024, following which Birkbeck, Lee, and Ma joined the collaboration. Macbeth and Mehta too have made significant contributions since October 2024.

All code pertaining to the formalisation of the contents of Chapter 4 that does not come from the broader theory of modular forms has been written solely by the author, with advice from Mehta. While the formalisation is not complete, the author's progress is best interpreted as providing important tools and frameworks that will significantly ease the remainder of the formalisation.

The most significant difference between the author's exposition and Viazovska's original proof is that the author uses six defining integrals instead of four, with all contours being rectangular. The reason this is useful is that a formal version of the Cauchy-Goursat Theorem that exists in `mathlib` for rectangular contours. A crucial step in Section 4.4 involves deforming unbounded contours, and the author formalised an appropriate version of the Cauchy-Goursat Theorem to work around this problem. The author's work builds on the `mathlib` version for bounded rectangular contours, and hypothesised that it would be easier to adapt the definitions and proofs preceding that of double zeroes to a function defined using rectangular contours than it would to prove an unbounded version of the Cauchy-Goursat Theorem involving circular or triangular contours. Unfortunately, the proof of the eigenfunction property is not compatible with rectangular contours, but the author remains confident in the possibility of a workaround. We continue this discussion in Section 5.3.

Viazovska's proof is heavy on computation. At the beginning of this M4R, the author was unaccustomed to proving computationally intensive results in Lean. While early attempts involved writing lengthy calculation lemmas, the author soon discovered that breaking computations into several lemmas corresponding to individual steps improved not only readability but also compilation time. The author's formal proof of Theorem 4.2.1, for example, consists of thirteen auxiliary lemmas corresponding to individual steps, and the author's formal proofs of the bounds on each of the $I_1, \ldots, I_6$ are spread across two files: one with alternate expressions for all the I_js and one with bounds on the I_j in question. A further advantage of this approach is its isolation of dependencies that are difficult to formalise, such as convergence results for sums, products and integrals that arise in either the statement or proof of a result. In some cases, one finds workarounds: for instance, when bounding the I_j, the author realised that the proof that the I_j converge absolutely is not necessary because of the way integrals are defined in `mathlib`. The necessity of such excruciating detail in formal proofs was the author's key motivator to provide detailed arguments in Chapter 4: the author's intent is for the proofs in this thesis to be a bridge between the informal and the formal, building on Viazovska's arguments in [14, §7].

For the remainder of this section, we briefly discuss two contributions the author made to the formalisation that account for differences, however minor, between Viazovska's original proof and the author's exposition. We then move onto two dedicated sections that respectively describe the metaprogramming approach implemented by Macbeth, Xie and the author and the challenges associated with the Cauchy-Goursat Theorem and how some, though not all, of them have been overcome.

5.1.1 A Systematic Approach to Bounding Integrals

Before the idea of rectangular contours, the author attempted to express $I_1 + I_2$ using a triangular contour. In fact, the author succeeded in bounding it by following the arguments in [1]. However, once the idea of rectangular contours was conceived, the author realised that six integrals would need to be bounded instead of four, as in [1]. The author hence decided to systematise his approach to maximise reusability of code. Indeed, that the proofs of Equations (4.2.4) and (4.2.5) and **??** are direct informalisations of the formal proofs found in the repository. There is one file per integral in the directory `MagicFunction.a.IntegralEstimates`, but the structure is nearly identical for those integrals bounded using the same techniques, reflecting the systematic nature of the approach. All specific references in this subsection will involve the I_j, though we emphasise, as we did in Section 4.2.2, that the J_j are similar.

Maybe rephrase if we don't finish bounding the Js in time

The integrals are defined using parametrisations involving a real variable, so that API on `intervalIntegral` could be used. To maximise compatibility, the most frequently used versions of the ϕ-functions and the parametrisations are extensions of these functions to $\mathbb{C}$ and $\mathbb{R}$ respectively that are 0 outside of where they are meant to be defined. This is in line with the `mathlib` style of defining constructions like sums, integrals and products to take trivial values outside when these constructions are not well-defined in informal mathematics. We now give a step-by-step breakdown of how the author bounded integrals in Lean.

1. Expressing the integrands in a convenient form.

   Aside from enhancing readability and underscoring the resemblance of the formal integrals to the informal integrals, parametrisations are a way to control the variable of integration. However, they come with a layer of syntax that is unhelpful for bounding. Hence, we define lemmas ending in `_eq` and `_eq'` to overcome them.

   `_eq` lemmas expand the parametrisations and perform basic simplifications, such as separating a term of the form $e^{\pi ir(1+it)}$ into $e^{\pi ir} \cdot e^{-\pi rt}$. `_eq'` lemmas take any scalars arising from this process (such as a factor of i from a parametrisation $z = 1 + it$) outside of the integral, which makes them easier to deal with when bounding the integral. These lemmas are proved in `MagicFunction.a.Basic` for all I_j, whereas the remaining steps are proved in individual files in `MagicFunction.a.IntegralEstimates`.

2. Changing variables (first, third and fifth integrals only).

   Informally and formally, the key to bounding the first, third, and fifth integrals of both eigenfunctions is to perform a change of variables $s = \frac{1}{t}$. We do this by applying a previously formalised `mathlib` result using functions `f`, `f'` and `g`, defined at the top of each file, denoting the variable change, its derivative, and the desired form of the integrand **after** the change of variables. Just as in this thesis, the author applied the convention of using `s` to denote the integration variable after the change and `t` to denote it before. An intermediate lemma navigates syntactic challenges, reconciling the integral in `t` whose integrand is a composition `g` with `f`.

3. Bounding the integrand.

   By inspection, one sees that in Equations (4.2.4) and (4.2.5) and **??**, the bounds on the integrals actually come from bounds on the integrands. This is done formally using two lemmas, the first performing elementary bounds and the second applying Theorem 4.2.1. The application of Theorem 4.2.1 is less straightforward for I_2 and I_4 because the condition $\mathrm{Im}(z) > \frac{1}{2}$ is more difficult to show (as seen in the informal proof of Equation (4.2.5) as well), so there are added helper lemmas for this.

4. Bounding the integral.

   This involves applying the triangle inequality and monotonicity of the integral, which were formalised in `mathlib` well before this project. Applying the former is straightforward, but applying the latter is not, because it requires integrability assumptions on the functions in question. The reason for this is that if $f \leq g$ and f is integrable but g is not, then the integral of g, as defined in Lean, is 0. Fortunately, for nonnegative f and g (such as the absolute values of our integrands and the functions that bound them), only needs g to be integrable. Integrability proofs for some bounding functions are currently `sorry`s.

The systematic nature of this approach makes it easy to reuse: the only differences between the computations for similar integrals are in the `g`s and the `_eq` and `_eq'` lemmas that are invoked at various points. Thus, the overall complexity of the task was reduced substantially.

5.1.2 A Schwartzness Bridge Across Dimensions

Having discussed these general contributions, we discuss two very specific and profound contributions made by the author to the formalisation effort. We begin by discussing the development of a Lean tactic by Macbeth, Xie and the author.

5.2 A Metaprogramming Approach

The formalisation of the solution to the sphere packing problem brought to light a longstanding difficulty faced by the Lean community: a lack of automation for performing computations in $\mathbb{C}$. After a discussion with Heather Macbeth, who is experienced in creating automation for Lean, the author, with Macbeth's guidance and Xie's assistance, embarked on the development of a normalisation-simplification automation procedure for performing computations in $\mathbb{C}$.

Lean, like other interactive theorem provers, primarily interacts with its users through **tactics**. Fundamentally, the proof of a theorem in Lean is given by a **proof term**, which can be thought of as a concise expression that captures the information of how the hypotheses or inputs of the theorem are transformed into its conclusion by giving exactly the conclusion into which these inputs are transformed. A tactic is a command that, when invoked by a Lean user, performs a step in the construction of the proof term for a theorem.

The most basic tactics can be thought of as being 'syntax sugar' rather than invocations of computation or reasoning algorithms. Consider the following code.

```
example (P Q R : Prop) : P ∧ (Q ∧ R) → (P ∧ Q) ∧ R := by
  intro h
  constructor
  · constructor
    · exact h.1
    · exact h.2.1
    · exact h.2.2
```

Listing 5.1: A tactic-mode proof of the associativity of $\wedge$

In this example, the `constructor` tactic is syntax sugar for an *anonymous constructor*; the `intro` tactic is syntax sugar for the input of a function; and the `exact` tactic is syntax sugar for placing an exact term at a specific point in the proof term.

There are more advanced tactics, however, that construct proof terms automatically. For instance, results in intuitionistic propositional logic, such as the associativity of $\wedge$, are handled by `itauto`.

```
example (P Q R : Prop) : P ∧ (Q ∧ R) ↔ (P ∧ Q) ∧ R := by itauto
```

Listing 5.2: A one-line tactic proof for the associativity of $\wedge$

Such tactics have immense utility, resulting in shorter, more readable proofs and a speedier, less vexatious interactive theorem proving experience. The science of writing such tactics is called **metaprogramming**. Given how computationally involved the construction of Viazovska's Magic Function is (as seen in Chapter 4), the author, after a discussions with Macbeth, realised that the most efficient approach to formalising some of the computational aspects of Viazovska's argument was to write a tactic capable of handling them. The first version of this tactic, developed as a collaboration between Macbeth, Xie and the author, with inputs from Mehta, was called `norm_numI`.

In the forthcoming subsections, we explore the motivation and technique used to develop `norm_numI`, and briefly discuss how the tactic maybe further developed and the scope of its applicability expanded.

5.2.1 Complex Computations are Complex

Computations in general are quite challenging to perform in interactive theorem provers. This is because such languages are designed for *proof* rather than *computation*. Indeed, tactics that simplify goals do not do so merely by simplifying expressions: they construct proofs that the simplified expression is, indeed, equal to the original expression. Existing tactics like `norm_num`, `simp` and `field_simp` do not always do this successfully when the expressions in question are in $\mathbb{C}$ because they are not designed to navigate its particularities of the field (such as $i^{-1} = -i = \bar{i}$). Our approach was to create an improvement on `norm_num` designed to work in $\mathbb{C}$. The reason for choosing `norm_num` is that it is currently designed to deal with *numerals* in semirings.

`norm_num` works best in $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$. For example, it handles the following.

```
example : (1 : ℕ) + 2 + 3 + 4 = 10 := by norm_num
example : (-2 : ℚ) * (3 + 8/9) = -70/9 := by norm_num
example : (-9 : ℤ) + 5 * (6 - 20) = -79 := by norm_num
```

Listing 5.3: `norm_num` simplifying expressions in $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$

It is worth mentioning, however, that `norm_num` often has difficulties in $\mathbb{R}$. This is due to the immense technical detail baked into the very definition of $\mathbb{R}$. For example, the following is not handled by `norm_num`.

```
example : (π - 1) / (π - 1) = 1 := by
  have hₐ : (1 : ℝ) < 3 := by norm_num
  have h₂ : 1 ≠ π := ne_of_lt <| hₐ.trans pi_gt_three
  have h₃ : π - 1 ≠ 0 := sub_ne_zero_of_ne h₂.symm
  field_simp [h₃]
```

Listing 5.4: An expression in $\mathbb{R}$ not handled immediately by simplification tactics

Observe, however, that `norm_num` *is* able to prove the inequality $1 < 3$ despite it being an expression in $\mathbb{R}$. The reason is that `norm_num` can navigate the canonical inclusions from $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ into $\mathbb{R}$, meaning that it can simplify expressions in $\mathbb{R}$ that come from expressions it can simplify in $\mathbb{N}$, $\mathbb{Z}$ or $\mathbb{Q}$.[1] It cannot, however, show that $1 < \pi$, because it does not treat π *as a numeral*. In $\mathbb{C}$, `norm_num` faces this challenge not only with real transcendental numbers like π but also with the imaginary constant i. For instance, it does not handle the following.[2]

```
example : (1 + I) * (1 + I * I * I) = 2 := by
  simp only [I_mul_I, neg_mul, one_mul, mul_add, mul_one, mul_neg, add_mul,
    neg_add_rev, neg_neg]
  ring
```

Listing 5.5: A nontrivial computation in $\mathbb{C}$, done formally

Observe that $(1 + i)(1 + i \cdot i \cdot i)$ lies in $\mathbb{Z}[i]$. This means that if it is expressed as $a+bi$, with a and b both being (not necessarily simplified) real expressions, then in fact, a and b are both images of expressions in $\mathbb{Z}$. This means that `norm_num` would be able to individually handle both a and b, resulting in a simplified expression of the form $a' + b'i$, with a' and b' being simplified. This suggests that the key to writing a tactic that can simplify expressions like those in Listing 5.5 is to find a way to separate them into their real and imaginary parts.

[1] We say `norm_num` can handle coercions.

[2] Note that in Lean, the imaginary constant is denoted by an uppercase `I` instead of a lowercase i. We will adhere to standard mathematical conventions and use a lowercase i when referring to the imaginary constant in informal contexts.

5.2.2 Parsing and Normalisation

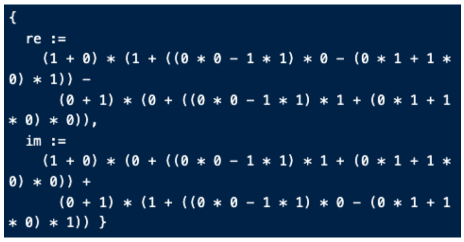
The core idea behind norm_num is that it simplifies expressions by computing normal forms. In its most basic form, norm_num attempts to prove equalities of by putting the left and right hand sides in unique normal forms that can simply be inspected to check if the two sides are equal. As was motived above, the right target normal form for an expression in $\mathbb{C}$ is splitting it into its real and imaginary parts, both of which are real expressions, and normalising them as much as possible.

The key to norm_numI is the parse function. It separates an expression $z \in \mathbb{C}$ into its real and imaginary parts by performing a recursive pattern-match. For example, if the outermost operation is addition—ie, if $z = z_1 + z_2$—then it calls itself on both z_j, obtaining real and imaginary parts $a_j, b_j \in \mathbb{R}$ and proofs that $z_j = a_j + b_j i$, and returns the expression $(a_1 + a_2) + (b_1 + b_2)\, i$ as well as a proof that $z = (a_1 + a_2) + (b_1 + b_2)\, i$, which it obtains via a helper lemma split_add. It performs similar recursive actions if z is of the form $z_1 \cdot z_2$, z_1^{-1}, z_1/z_2, $-z_1$, $z_1 - z_2$, $\overline{z_1}$, z_1^n for some $n \in \mathbb{N}$, i, or a decimal/natural number. The recursion is guaranteed to terminate, because an expression that is fed into the function cannot contain infinitely many characters.

Example 5.2.1. The expression $z = (1 + i)\,(1 + i \cdot i \cdot i)$ (cf. Listing 5.5) would be parsed in the following manner.

1. To parse z, write $z = z_1 \cdot z_2$, where $z_1 = 1 + i$ and $z_2 = 1 + i \cdot i \cdot i$.
2. To parse z_1, write $z_1 = z_{11} + z_{12}$ where $z_{11} = 1$ and $z_{12} = i$.
3. z_{11} is parsed as $1 + 0i$.
4. z_{12} is parsed as $0 + 1i$.
5. By split_add, $z_1 = z_{11} + z_{12}$ is parsed as
$$(1 + 0) + (0 + 1)\, i$$
6. To parse z_2, write $z_2 = z_{21} + z_{22}$, where $z_{21} = 1$ and $z_{22} = i \cdot i \cdot i$.
7. z_{21} is parsed as $1 + 0i$.
8. To parse z_{22}, write $z_{22} = z_{221} \cdot z_{222}$, where $z_{221} = i \cdot i$ and $z_{222} = i$.
9. To parse z_{221}, write $z_{221} = z_{2211} \cdot z_{2212}$, where $z_{2211} = i$ and $z_{2212} = i$.
10. z_{2211} is parsed as $0 + 1i$.
11. z_{2212} is parsed as $0 + 1i$.
12. By split_mul, $z_{221} = z_{2211} \cdot z_{2212}$ is parsed as
$$(0 \cdot 0 - 1 \cdot 1) + (0 \cdot 1 + 0 \cdot 1)\, i$$
13. z_{222} is parsed as $0 + 1i$.
14. By split_mul, $z_{22} = z_{221} \cdot z_{222}$ is parsed as
$$((0 \cdot 0 - 1 \cdot 1) \cdot 0 - (0 \cdot 1 + 1 \cdot 0) \cdot 1) + ((0 \cdot 0 - 1 \cdot 1) \cdot 1 + 0 \cdot (0 \cdot 1 + 1 \cdot 0))\, i$$
15. By split_add, $z_2 = z_{21} + z_{22}$ is parsed as
$$\begin{gathered}(1 + ((0 \cdot 0 - 1 \cdot 1) \cdot 0 - (0 \cdot 1 + 1 \cdot 0) \cdot 1)) \\ + (0 + ((0 \cdot 0 - 1 \cdot 1) \cdot 1 + 0 \cdot (0 \cdot 1 + 1 \cdot 0)))\, i\end{gathered}$$
16. By split_mul, $z = z_1 + z_2$ is parsed as
$$\Big((1 + 0) \cdot (1 + ((0 \cdot 0 - 1 \cdot 1) \cdot 0 - (0 \cdot 1 + 1 \cdot 0) \cdot 1)) \\ - (0 + 1) \cdot (0 + ((0 \cdot 0 - 1 \cdot 1) \cdot 1 + 0 \cdot (0 \cdot 1 + 1 \cdot 0))) \Big)$$

$$
\begin{aligned}
&+\Big((1+0)\cdot(0+((0\cdot 0-1\cdot 1)\cdot 1+0\cdot(0\cdot 1+1\cdot 0)))\\
&\quad+(1+((0\cdot 0-1\cdot 1)\cdot 0-(0\cdot 1+1\cdot 0)\cdot 1))\cdot(0+1)\Big)i
\end{aligned}
$$



```
{
  re :=
    (1 + 0) * (1 + ((0 * 0 - 1 * 1) * 0 - (0 * 1 + 1 *
0) * 1)) -
      (0 + 1) * (0 + ((0 * 0 - 1 * 1) * 1 + (0 * 1 + 1
* 0) * 0)),
  im :=
    (1 + 0) * (0 + ((0 * 0 - 1 * 1) * 1 + (0 * 1 + 1 *
0) * 0)) +
      (0 + 1) * (1 + ((0 * 0 - 1 * 1) * 0 - (0 * 1 + 1
* 0) * 1)) }
```

Figure 5.1: The Lean output of the steps shown in Example 5.2.1.

Clearly, despite being mathematically valid, the result of parsing can be long and uninformative, making it an unsuitable choice of normal form for our purposes. However, by separating complex expressions into their real and imaginary parts, `parse` perfectly sets us up to use an existing, highly effective normalisation procedure: `norm_num` itself. Since `parse` expresses any complex expression as a combination of two real expressions, the normalisation procedure simply makes calls to `norm_num` to express each of them in a *real* normal form. The result is a complex number in a normal form $a + bi$ (or, in Lean notation, `{re := a, im := b}`) with a and b both simplified to the greatest extent possible (as expressions in $\mathbb{R}$) by applying `norm_num`.

`norm_numI` is currently implemented as a `conv` tactic rather than a full tactic, meaning that it is only capable of modifying expressions and providing a proof that the modification is valid. It is not currently capable of proving goals, which are necessarily logical statements, such as equalities. It can be used as follows.

```
example : (1 + I) * (1 + I * I * I) = 2 := by
  conv_lhs => norm_numI
  conv_rhs => norm_numI
```

Listing 5.6: Using `norm_numI` as a `conv` tactic

After Macbeth, Xie and the author's initial success with this `conv` tactic, Macbeth created an *extension* of the existing `norm_num` tactic that uses the parsing technique outlined above to handle complex expressions. This tactic is still being developed, but is being tested on active code from the project with immensely promising results.

5.3 The Cauchy-Goursat Theorem

There are some areas of mathematics that are notoriously difficult to formalise. Algebra, for example, tends to be easier to formalise than analysis. Within analysis, it tends to be particularly difficult to formalise geometric ideas, and few are as deceptively challenging as the innocent-sounding Jordan Curve Theorem. It was not until 2007 that this theorem, proposed in the late 19th Century, was formalised by Tom Hales [26] in HOL Light, and to this day, no formalisation exists in Lean. The author had the privilege of meeting Hales in Pittsburgh, USA, in March 2025 to discuss the formalisation of 8-dimensional sphere packing in Lean, and the very first question Hales asked was what the strategy was to overcome the challenges of not having a Lean formalisation of the Jordan Curve Theorem.

The Jordan Curve Theorem states that a simple closed curve $C \subset \mathbb{R}^2$, given as the image of a continuous injection from $\mathbb{S}^1$, divides $\mathbb{R}^2 \setminus C$ into a bounded region, known as the *interior* of C, and an unbounded region, known as the *exterior* of C. This gives us a clear way of stating the all-important holomorphicity condition of the Cauchy-Goursat Theorem: a path of integration can usually only be deformed if the integrand is holomorphic in the region enclosed by the two paths, and the Jordan Curve Theorem defines this region. Viazovska uses versions of the Cauchy-Goursat Theorem to prove the eigenfunction property and the double zero property (see Sections 4.3 and 4.4. Fortunately, in both instances, we have explicit contours. Hence, the regions where we require holomorphicity can both be defined, and it is easy to show the integrands are holomorphic in those regions.

This is a significant simplification because it means we have all the ingredients to *state* the results we require. However, there are still challenges involved in proving them. We give a brief overview of the two cases of interest in the forthcoming subsections.

5.3.1 Rectangles

The following version of the Cauchy-Goursat Theorem had been formalised prior to this project.

Theorem 5.3.1 (Cauchy-Goursat for Rectangles). *Suppose $f : \mathbb{C} \to \mathbb{C}$ is a function such that $f(z) \to 0$ as $\mathrm{Im}(z) \to \infty$. Then, for all $x_1, y_1, x_2, y_2 \in \mathbb{R}$, if f is holomorphic at all but countably many $z \in \mathbb{C}$ with $x_1 < \mathrm{Re}(z) < x_2$ and $y_1 < \mathrm{Im}(z) < y_2$ and continuous on the corresponding closed rectangle, then*

$$\int_{x_1}^{x_2} f(x + y_1 i)\,\mathrm{d}x - \int_{x_1}^{x_2} f(x + y_2 i)\,\mathrm{d}x + i\int_{y_1}^{y_2} f(x_2 + yi)\,\mathrm{d}y - i\int_{y_1}^{y_2} f(x_1 + yi)\,\mathrm{d}y = 0$$

The author was able to adapt this to the following unbounded version.

Theorem 5.3.2 (Cauchy-Goursat for Unbounded Contours). *Suppose $f : \mathbb{C} \to \mathbb{C}$ is a function such that $f(z) \to 0$ as $\mathrm{Im}(z) \to \infty$. Then, for all $x_1, x_2, y \in \mathbb{R}$, if f is holomorphic at all but countably many $z \in \mathbb{C}$ with $x_1 < \mathrm{Re}(z) < x_2$ and $y < \mathrm{Im}(z)$ and then*

$$\int_{y}^{\infty} f(x_1 + ti)\ \mathrm{d}t = \int_{x_1}^{x_2} f(t + yi)\ \mathrm{d}t + \int_{y}^{\infty} f(x_2 + ti)\ \mathrm{d}t$$

provided that the integrals along the vertical contours exist.

It is immediate that this implies Theorem 4.4.1.

We briefly sketch a proof of Theorem 5.3.2. Writing the integrals along both vertical contours as limits as $m \to \infty$ of the integrals from y to m, we can apply Theorem 5.3.1 to each rectangle with vertices $x_1 + yi$, $x_2 + yi$, $x_1 + mi$ and $x_2 + mi$ gives us two different expressions for the integral along x_1, one of which agrees with the integral along x_2 as $m \to \infty$ because the integrals along the blue contours in Figure 5.2 can be shown to vanish using the property that $f(z) \to 0$ as $\mathrm{Im}(z) \to \infty$.

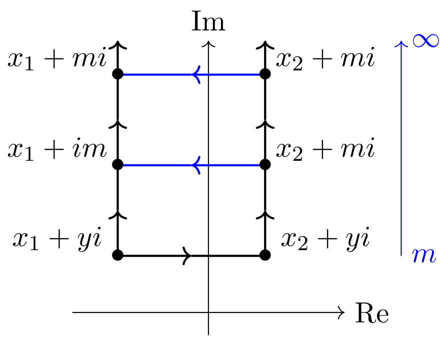


Figure 5.2: The contours in Theorem 5.3.2.

The author has `sorry`-free versions of this in the repository as well as one version with a `sorry`. This is because the author is trying to minimise the number of assumptions required for Theorem 5.3.2. For instance, integrability is stronger than the existence of the integrals, because integrability (in Lean) is a combination of absolute convergence and measurability. In the repository, these contours are currently referred to as open, not in a topological sense but in the sense that they do not consist of closed curves. Perhaps unbounded is a better term.

It was the fact that such a simple and elegant solution existed for deforming unbounded contours that motivated the definition of the I_j and J_j using rectangular contours. While circular contours would make the eigenfunction proof easier, the challenge of proving Theorem 5.3.2 would either involve reconciling circles and rectangles, which we discuss in the next subsection, or a direct proof, which the author expects would be immensely difficult to formalise.

We end this discussion by noting that the rectangles in Theorems 5.3.1 and 5.3.2 have a particular orientation that makes it easier to define their interior. For rectangles oriented differently, it is conceivable that a proof involving variable changes can be formalised when an orientation is specified, but it will require effort.

5.3.2 Squares and Circles

To prove Section 4.3, we effectively need the following.

Theorem 5.3.3 (Cauchy-Goursat: Squares and Circles). *Fix $w \in \mathbb{C}$ and $r > 0$. Let γ be the quarter-circle parametrised by $\gamma(t) = w + r\cos(t) + ri\sin(t)$ for $0 \leq t \leq \pi/2$. Let*

$$S = \left\{x + yi \in \mathbb{C} \;\middle|\; \left(x^2 + y^2 > r^2\right) \wedge (0 < x < r) \wedge (0 < y < r)\right\}$$

For any $f : \mathbb{C} \to \mathbb{C}$ that is holomorphic on all but countably many points in S and continuous on the closure $\bar{S}$ of S,

$$\int_\gamma f(z)\ \mathrm{d}z = \int_{w+r}^{w+r+ir} f(z)\ \mathrm{d}z + \int_{w+r+ir}^{w+ir} f(z)\ \mathrm{d}z$$

Again, we are saved from the difficulties of applying the Jordan Curve Theorem because we are working in a very specific situation where we can explicitly describe S. However, proving this result, formally and informally, is significantly more complicated than proving Theorem 4.4.1. One proof would be to arbitrarily approximate γ by squares of exponentially decaying side lengths. For any contour defined in this way, we can show, by inductively applying Theorem 5.3.1, that the integral along it equals the integral along the rectangular contour in Figure 5.3. Since these contours converge to γ pointwise, it should be possible to show, by dominated convergence, that the (constant) sequence of integrals along the square contours converges to the integrals along γ.

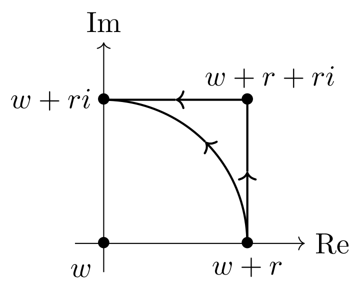


Figure 5.3: The contours in Theorem 5.3.3.

Unfortunately, these ideas are incredibly difficult to formalise, not least because it is difficult to define such a sequence of parametrisations in Lean. Other possible approaches include formalising a version for triangles and subsequently approximating the circle using triangles. Regardless of the approach, formalising Theorem 5.3.3 will be a challenge. If done successfully, however, it will be a significant achievement in itself as well as a valuable contribution to this project.

Chapter 6

Conclusion

Over the course of this thesis, we have explored a revolutionary approach to a classical problem that has since led to deeper insights into the mysteries of the E_8 lattice, its 24-dimensional counterpart, the Leech lattice, and the broader theory of radial Schwartz functions. Previously unexplored links to the theory of modular forms are revealing deep symmetries that lead to fascinating results, such as Cohn, Kumar, Miller, Radchenko and Viazovska's universal optimality and Fourier interpolation formulas [27] that reconstruct radial Schwartz functions f from the values and radial derivatives of f and $\widehat{f}$, generalising Viazovska's approach to solving the sphere packing problem in $\mathbb{R}^8$.

6.1 Viazovska's Monumental Breakthrough

6.2 The Road to Formalising Sphere Packing

6.3 A Glance Ahead

Bibliography

[1] M. S. Viazovska. The sphere packing problem in dimension 8. *Annals of Mathematics*, 185 (3):991–1015, 2017.

[2] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska. The sphere packing problem in dimension 24. *Annals of Mathematics*, 185(3):1017–1033, 2017.

[3] H. Cohn. The work of Maryna Viazovska. In *Proceedings of the International Congress of Mathematicians*, volume 1, pages 82–105. EMS Press, 2023. Presented at ICM, July 6–14, 2022.

[4] T. C. Hales. A Proof of the Kepler Conjecture. *Annals of Mathematics*, 162(3):1065–1185, 2005.

[5] E. Klarreich. Sphere Packing Solved in Higher Dimensions. *Quanta Magazine*, March 2016.

[6] H. Cohn. A Conceptual Breakthrough in Sphere Packing. *Notices of the American Mathematical Society*, 64(02):102–115, Feb. 2017.

[7] A. Thue. Om nogle geometrisk-taltheoretiske Theoremer. *Forhandlingerne ved de Skandinaviske Naturforskeres*, 14, 1892. Zbl 24.0259.01.

[8] T. C. Hales. Cannonballs and Honeycombs. *Notices of the American Mathematical Society*, 47(4):440–449, Apr. 2000.

[9] J. Kepler. *Strena seu de nive sexangula*. Francofurti ad Moenum : apud Godefridum Tampach, 1611. ETH-Bibliothek Zürich, Rar 4342: 2, https://doi.org/10.3931/e-rara-478.

[10] T. C. Hales et al. A Formal Proof of the Kepler Conjecture. *Forum of Mathematics, Pi*, 5: e2, 2017.

[11] T. C. Hales. Introduction to the Flyspeck Project. In T. Coquand, H. Lombardi, and M.-F. Roy, editors, *Mathematics, Algorithms, Proofs*, volume 5021 of *Dagstuhl Seminar Proceedings (DagSemProc)*, pages 1–11, Dagstuhl, Germany, 2006. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[12] W. Gowers, B. Green, F. Manners, and T. Tao. On a conjecture of Marton. *Annals of Mathematics*, 201(2):515 – 549, 2025.

[13] P. Scholze, D. Clausen, J. Commelin, and P. Massot. Blueprint for the Liquid Tensor Experiment, September 2023. https://leanprover-community.github.io/liquid/.

[14] C. Birkbeck, S. Hariharan, S. Lee, G. Ma, B. Mehta, and M. Viazovska. Sphere Pack-

ing in Lean - Project Blueprint, 2025. https://thefundamentaltheor3m.github.io/Sphere-Packing-Lean/blueprint/index.html.

[15] P. Massot and et al. leanblueprint. https://github.com/PatrickMassot/leanblueprint.

[16] H. Cohn and N. Elkies. New Upper Bounds on Sphere Packings I. *Annals of Mathematics*, 157(2):689–714, 2003.

[17] The mathlib Community. The lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP 2020, page 367–381, New York, NY, USA, 2020. Association for Computing Machinery.

[18] T. F. Görbe. Exceptionally Beautiful Symmetries. https://tamasgorbe.com/symmetry.

[19] L. Schwartz. *Théorie des distributions*. Hermann, Paris, 1978. Nouvelle édition.

[20] J.-P. Serre. *A Course in Arithmetic*. Springer-Verlag, New York, 1973.

[21] F. Diamond and J. Shurman. *A First Course in Modular Farms*. Number 228 in Graduate Texts in Mathematics. Springer New York, NY, New York, first edition, March 2006.

[22] K. Buzzard. Families of modular forms. *Journal de Théorie des Nombres de Bordeaux*, 13 (1):43–52, 2001.

[23] J. Bourgain, L. Clozel, and J.-P. Kahane. Principe d'Heisenberg et fonctions positives. *Annales de l'Institut Fourier*, 60(4):1215–1232, 2010.

[24] D. Romik. On Viazovska's modular form inequalities. *Proceedings of the National Academy of Science*, 120(43):e2304891120, Oct. 2023.

[25] S. Lee. Algebraic proof of modular form inequalities for optimal sphere packings, 2024.

[26] T. C. Hales. The Jordan Curve Theorem, Formally and Informally. *The American Mathematical Monthly*, 114(10):882–894, 2007.

[27] H. Cohn, A. Kumar, S. Miller, D. Radchenko, and M. Viazovska. Universal optimality of the E_8 and Leech lattices and interpolation formulas. *Annals of Mathematics*, 196(3):983 – 1082, 2022.