TOPICS IN ANALYTIC NUMBER THEORY

By

G. KASI VISWANADHAM

MATH08200904004

Harish-Chandra Research Institute, Allahabad

A thesis submitted to the

Board of Studies in Mathematical Sciences

In partial fulfillment of requirements

for the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

April, 2015

STATEMENT BY THE AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgement the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Date: **G. Kasi Viswanadham**

DECLARATION

I, G. Kasi Viswanadham, hereby declare that the investigation presented in this thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree or diploma at this or any other Institution or University.

Date: **G. Kasi Viswanadham**

List of Publications arising from the thesis

Journal

1. Set of uniqueness of shifted Gaussian primes, Jay Mehta and G.K. Viswanadham, *Funct. Approx. Comm. Math.*, To appear.

2. A short note on sign changes, Jaban Meher, Karam Deo Shankhadar and G.K. Viswanadham, *Proc. Indian Acad. Sci. Math. Sci.* **2013**, *Vol. 123*, no.3, 315-320.

G. Kasi Viswanadham

Dedicated to my Grand Parents

Sri L. Kameswararao

&

Smt. L. Kameswaramma

Acknowledgments

First and foremost, I wish to thank my thesis advisor Prof. D. S. Ramana for his support throughout my Ph.D. studies and research work. I am very grateful to Prof. Imre Kátai for a suggestion that lead to my collaboration with Jay Mehta.

I thank the members of my doctoral committee, Prof. S. D. Adhikari and Dr. Gyan Prakash, for their helpful comments and encouragement throughout my work on this thesis. I would also like to thank all faculty members of HRI for the courses they gave during my years of study here.

I am indebted to my collaborators for liberally sharing their time and talent. My special thanks to Jay Mehta, Jaban Meher and Karam Deo Shankhadar for collaborating on projects that resulted in this thesis. I would also like to thank Prof. R. Thangadurai and Prof. Anirban Mukhopadhyay for a number of useful discussions.

I thank all the staff of the Administration of HRI for making my stay comfortable. I am especially thankful to the staff of the library who were helpful at all times.

I thank all my friends at HRI, seniors, batch mates and juniors alike, for their support and encouragement. I would like to especially thank Pradip, Pradeep and Akhilesh for their understanding and constant encouragement.

I am deeply thankful to my family and my in-laws for their love, support, and sacrifices. I reserve these last words for my dear wife Padma, who has been with me all these years and made them the best years of my life so far.

G. Kasi Viswanadham

Contents

Notations

Symbol	Meaning/Description
$\mathbf{N}$	The set of integers ≥ 0
$\mathbf{N}^*$	The set of integers ≥ 1
$\mathbf{Z}$	The set of all integers
$\mathbf{Z}^*$	The set of all non-zero integers
$\mathbf{Q}$	The set of all rational numbers
$\mathbf{R}$	The set of all real numbers
$\mathbf{C}$	The set of all complex numbers
$\mathbf{C}^*$	The set of all non-zero complex numbers
$\mathcal{H}$	The upper half plane of $\mathbf{C}$
$\mathbf{U}$	The set of complex numbers with absolute value 1
$\mathbf{Z}[i]$	The ring of Gaussian integers
$\mathcal{G}$	The set of non-zero Gaussian integers
$\mathcal{P}[i]$	A fixed system of representatives for Gaussian primes modulo units
$\mathcal{S}[i]$	The set of π^k, $\pi \in \mathcal{P}[i]$, k any integer ≥ 1

$\mathcal{G}^*$	Multiplicative set generated by $\mathcal{P}[i]$
$\mathcal{N}(z)$	The norm of the Gaussian integer z
$\mathrm{SL}_2(\mathbf{Z})$	Group of all 2×2 integer matrices of determinant 1
$\Gamma_0(N)$	Hecke congruence subgroup of level N
$\hat{\psi}$	Fourier transform of $\psi : \mathbf{R} \to \mathbf{R}$
$f * g$	Convolution of the arithmetical functions f and g
$e(z)$	$e^{2\pi iz}$
$\mathrm{dia}(X)$	The maximum distance between any two points of a set X
$\|A\|$	Cardinality of the set A

Synopsis

This thesis comprises three chapters divided into two parts. The theme of the first part, comprising the first two chapters, is sets of uniqueness of arithmetical functions on the Gaussian integers. A description of the contents of this part of the thesis is given in Sections 1 and 2 below. The third chapter of this thesis forms the second part. This part records some results on sign changes of Fourier coefficients of modular forms. These results are summarised in Section 3 below.

1 Quasi-Uniqueness of Shifted Gaussian Primes

Let $\mathcal{B}$ denote the family of all complex valued additive functions and $\mathcal{B}^*$ denote the family of all complex valued completely additive functions on $\mathbb{N}$, the set of all integers $n \geq 1$. It is clear that an additive function is determined by its values at the prime powers and that a completely additive function is determined by its values at the primes. Thus, an additive (respectively completely additive) function that vanishes at all prime powers (respectively at all primes) necessarily vanishes on all of $\mathbb{N}$. A natural notion in this context is that of a set of uniqueness.

Definition 1.1. A subset A of $\mathbb{N}$ is said to be a *set of uniqueness* for $\mathcal{B}$ (resp. $\mathcal{B}^*$) if *every* $f \in \mathcal{B}$ (resp. $f \in \mathcal{B}^*$) that vanishes on A necessarily vanishes on all of $\mathbb{N}$.

We also have the following more general notion.

Definition 1.2. A subset A of $\mathbb{N}$ is said to be a *set of quasi-uniqueness* for $\mathcal{B}$ (resp. $\mathcal{B}^*$) if there is a finite subset B of $\mathbb{N}$ such that $A \cup B$ is a set of uniqueness for $\mathcal{B}$ (resp. $\mathcal{B}^*$).

I. Kátai proved that the set $\mathcal{P}+1$ of all integers of the form $p+1$, with p a prime number, is a set of quasi-uniqueness for $\mathcal{B}^*$. This is shown in [22] under the General Riemann Hypothesis for Dirichlet L-functions and later in [23] without assuming any unproved hypothesis.

The notions of sets of quasi-uniqueness and sets of uniqueness have evident extensions to additive functions and completely additive functions on the non-zero Gaussian integers $\mathbb{Z}[i]^*$. Also, one may ask if the set $\mathcal{P}[i]+1$ of all Gaussian integers of the form $p+1$, with p a Gaussian prime number, is a set of uniqueness for $\mathcal{A}^*$, the family of all completely additive functions on $\mathbb{Z}[i]^*$. Our first result affirms that this is the case. More precisely, we have the following theorem.

Theorem 1.1. *There exists a real number K_0 such that any complex valued completely additive function on $\mathbb{Z}[i]^*$ that vanishes at each Gaussian prime of norm not exceeding K_0 and at every element of $\mathcal{P}[i]+1$ in fact vanishes on all of $\mathbb{Z}[i]^*$.*

The above theorem is the main conclusion of the paper [33], authored jointly with Jay Mehta. The proof of Theorem 1.1 is the content of Chapter 1 of this thesis.

2 Set of Uniqueness of Shifted Gaussian Primes

The second chapter of the thesis gives a strong form of Theorem 1.1. Indeed, Katai conjectured in [22] that $\mathcal{P}+1$ is a set of uniqueness for $\mathcal{B}^*$. This conjecture was settled by P.D.T.A. Elliott [9]. More precisely, it follows from the main theorem of [9] that $\mathcal{P}+1$ is a set of uniqueness for $\mathcal{B}$ and hence for $\mathcal{B}^*$ as well.

D. Wolke [44] showed that if a set A is a set of uniqueness for $\mathcal{B}^*$ then every $n \in \mathbb{N}$ can be written as a finite product of rational powers of elements of A. Consequently, Elliott's result implies that every positive integer can be written as a finite product of rational powers of elements of $\mathcal{P}+1$.

In Chapter 2 of the thesis we extend these assertions to the Gaussian integers by generalising the method of Elliott [9] to this setting. Our main result is the following theorem.

Theorem 2.1. *Every complex valued additive function on $\mathbb{Z}[i]^*$ that vanishes on the complement of a finite subset of $\mathcal{P}[i]+1$ in fact vanishes on all of $\mathbb{Z}[i]^*$.*

Thus we certainly have that $\mathcal{P}[i]+1$ is a set of uniqueness for $\mathcal{A}^*$, in analogy with Katai's conjecture. Further, it is shown in Chapter 2 that the method of Wolke [44] may be modified to yield the following corollary to Theorem 2.1.

Corollary 2.1. *Every non-zero Gaussian integer can be written as a finite product of rational powers of elements of $\mathcal{P}[i]+1$.*

Both the above theorem and corollary were originally obtained in the paper [34], again, authored jointly with Jay Mehta.

3 Sign Changes

3.1 Fourier Coefficients of Cusp Forms

For N in $\mathbb{N}$, let f be a modular form of weight k on $\Gamma_0(N)$, the Hecke congruence subgroup of level N. Further, let $f(z)=\sum_{n\geq 0} a_n e^{2\pi i n z}$ be the Fourier expansion of f at infinity.

A number of authors have studied the behavior of sign changes of Fourier coefficients a_n of modular forms when they are real numbers. A standard application of the classical theorem of Landau on Dirichlet series with positive coefficients shows that the Fourier coefficients of a cusp form change sign infinitely often when they are real numbers. It is natural to ask if this phenomenon persists when one considers a subsequence $\{a_n | n \in S\}$ of the Fourier coefficients of a given cusp form with S a *sparse* subset of $\mathbb{N}$. The case when S is the set of prime numbers was studied by M. Ram Murty [39].

In Chapter 3 of this thesis we begin with a simple quantitative result on the sign change problem for the case when the sparse set S is one of $\{n^2 : n \in \mathbb{N}\}$, $\{n^3 : n \in \mathbb{N}\}$ or $\{n^4 : n \in \mathbb{N}\}$. Thus, suppose that $f(z) = \sum_{n\geq 1} a(n)e^{2\pi i n z}$ is a Hecke eigenform of weight k on the full modular group $\mathrm{SL}_2(\mathbb{Z})$. Let $\lambda(n) = \frac{a(n)}{n^{\frac{k-1}{2}}}$ and, further, let δ_j be $2/11, 1/9, 2/27$ when $j = 2, 3, 4$ respectively. Then we have the following theorem.

Theorem 3.1. *Suppose that j is 2,3 or 4. Then for any $\epsilon > 0$, there is a real number $C(\epsilon)$ such that the sequence $\{\lambda(n^j)\}_{n\geq 1}$ has at least $C(\epsilon)x^{\delta_j - \epsilon}$ sign changes in the interval $(x, 2x]$, for all sufficiently large x.*

The proof of this theorem relies on an elementary argument taken together with the results O. M. Fomenko [14], G. S. Lü [31] and H. Lao and A. Sankaranarayanan [29]. Theorem 3.1 was originally obtained in a joint work with Jaban Meher and Karam Deo Shankhadar [35].

3.2 q-exponents of Generalised Modular Forms

A generalized modular function (GMF) of weight k and character χ on $\Gamma_0(N)$ is a holomorphic function f on the upper half plane $\mathcal{H}$ satisfying the relation

$$f(\gamma.z) = \chi(\gamma)(cz+d)^k f(z)$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma_0(N)$ and z in $\mathcal{H}$. Here χ is a character of the group $\Gamma_0(N)$ such that $\chi(\gamma) = 1$ for every parabolic element of $\Gamma_0(N)$ of trace 2 and, as usual, $\gamma.z = \frac{az+b}{cz+d}$.

Suppose that f is a generalised modular function and that h is the order of f at $i\infty$. Then it can be shown that there is a complex number a and a sequence of complex numbers c_n such that we have

$$f(z) = a\, e^{2\pi i h z} \prod_{n\geq 1} \left(1 - e^{2\pi i n z}\right)^{c_n}$$

for all z in some neighbourhood of $i\infty$. The c_n are called the q-exponents of f.

Suppose that f is a generalised modular function with $\mathrm{div}(f) = 0$, that is, suppose that f does not vanish on $\mathcal{H}$ and that it is holomorphic at $i\infty$. Then its logarithmic derivative is a cusp form of weight 2 for $\Gamma_0(N)$. Moreover, if a_n are the Fourier coefficients of this cusp form then the c_n are given by $nc_n = -\sum_{d|n} \mu(n/d) a_d$. In view of this relation, it is natural to ask if the q-coefficients c_n of a generalised modular function with $\mathrm{div}(f) = 0$ change sign infinitely often when they are real. Assuming the weight of f to be 0, W. Kohnen and J. Meher [25] show that this is indeed the case. Their argument is qualitative and depends on Landau's theorem.

In the joint work [35], with Jaban Meher and Karam Deo Shankhadar, the following theorem is proved.

Theorem 3.2. *Let N be a square-free integer. Then for every non-constant generalized modular function f of weight 0 on $\Gamma_0(N)$ with div$(f) = 0$ such that $\frac{1}{2\pi i}\frac{f'}{f}$ is* *a normalized new form, the sequence c_p, with p varying over the primes, has atleast $Ae^{B\sqrt{\log x}}$ sign changes in the interval $[x, 2x]$ for sufficiently large x, where A and B are absolute constants.*

A proof of this theorem is given in Chapter 3 of the thesis. This theorem was subsequently much improved by N. Kumar [28], who used the Sato-Tate conjecture, proved by Barnet-Lamb, Geraghty, Harris and Taylor.

CHAPTER 1

Introduction

This thesis comprises two parts. The first part is concerned with sets of uniqueness of arithmetical functions on the Gaussian integers. Section 1 of this chapter provides an introduction to the contents of this part of the thesis. Section 2 of this chapter gives an overview of the second part of this thesis, which records some results on sign changes of Fourier coefficients of modular forms and q-exponents of generalised modular forms.

1 Sets of Uniqueness

Let $\mathbf{N}^*$ be the set of integers $n \geq 1$. An additive function on $\mathbf{N}^*$ is a complex valued function f on $\mathbf{N}^*$ satisfying $f(mn) = f(m) + f(n)$ for all coprime m and n in $\mathbf{N}^*$. An additive function f on $\mathbf{N}^*$ such that $f(mn) = f(m) + f(n)$ holds for all m and n in $\mathbf{N}^*$ is called a completely additive function on $\mathbf{N}^*$.

A subset A of $\mathbf{N}^*$ is called a set of uniqueness for a family $\mathcal{F}$ of complex valued functions on $\mathbf{N}^*$ if for any f, g in $\mathcal{F}$ the relation $f(n) = g(n)$ holds for all $n \in A$

only if the relation $f(n) = g(n)$ holds for all $n \in \mathbf{N}^*$. The set A is called a set of quasi-uniqueness for $\mathcal{F}$ if there is a finite subset B of $\mathbf{N}^*$ such that $A \cup B$ is a set of uniqueness for $\mathcal{F}$.

A completely additive function is determined by its values on the set of prime numbers $\mathcal{P}$. Therefore, $\mathcal{P}$ is a set of uniqueness for the family of completely additive functions on $\mathbf{N}^*$. Following popular heuristics in number theory, one may ask if additive translates of the set $\mathcal{P}$ are still sets of uniqueness for completely additive functions on $\mathbf{N}^*$. To the extent we are aware, investigations around this theme were first carried out by I. Kátai.

Kátai proved that the set $\mathcal{P} + 1$ of all $n \in \mathbf{N}^*$ such that $n - 1$ is a prime number is a set of quasi-uniqueness for the family of completely additive functions on $\mathbf{N}^*$. This was shown in [22] under the Generalized Riemann Hypothesis for Dirichlet L-functions and later in [23] without assuming any unproved hypothesis. Kátai also conjectured in [22] that $\mathcal{P}+1$ is in fact a set of uniqueness for the family of completely additive functions on $\mathbf{N}^*$. This conjecture was settled by P.D.T.A. Elliott [9]. More precisely, it follows from the main theorem of [9] that $\mathcal{P} + 1$ is a set of uniqueness for the family of additive functions, and not just completely additive functions, on $\mathbf{N}^*$.

D. Wolke [44] showed that if a subset A of $\mathbf{N}^*$ is a set of uniqueness for the family of completely additive functions on $\mathbf{N}^*$ then every $n \in \mathbf{N}$ can be written as a finite product of rational powers of elements of A. Consequently, Elliott's result implied that every $n \in \mathbf{N}$ can be written as a finite product of rational powers of elements of $\mathcal{P} + 1$.

In Chapter 2 of this thesis, which is based on the joint paper [34] with Jay Mehta, we rework Elliott's and Wolke's methods to obtain extensions of their results to the non-zero Gaussian integers $\mathbf{Z}[i]^*$, which we shall hereafter denote by $\mathcal{G}$. Our precise conclusions are stated in Section 8 of Chapter 2. We refer the reader to Section 9 of Chapter 2 for an outline of the proof of these results.

2 Changes in Sign

For N in $\mathbf{N}^*$, let f be a modular form of weight k on $\Gamma_0(N)$, the Hecke congruence subgroup of level N. Further, let $f(z) = \sum_{n\geq 0} a(n)e^{2\pi inz}$ be the Fourier expansion of f at infinity.

A number of authors have studied the changes in sign of the Fourier coefficients a_n of modular forms when they are real numbers. A standard application of the classical theorem of Landau on Dirichlet series with positive coefficients shows that the Fourier coefficients of a cusp form change sign infinitely often when they are real numbers. It is natural to ask if this phenomenon persists when one considers a subsequence $\{a(n)|n \in S\}$ of the Fourier coefficients of a given cusp form with S a *sparse* subset of $\mathbf{N}^*$. The case when S is the set of prime numbers was studied by M. Ram Murty [39].

In Chapter 3 of this thesis we begin with a simple quantitative result on the sign change problem for the case when the sparse set S is one of $\{n^2 \mid n \in \mathbf{N}^*\}$, $\{n^3 \mid n \in \mathbf{N}^*\}$ or $\{n^4 \mid n \in \mathbf{N}^*\}$. Thus, suppose that $f(z) = \sum_{n\geq 1} a(n)e^{2\pi inz}$ is a Hecke eigenform of weight k on the full modular group $\mathrm{SL}_2(\mathbf{Z})$ and set $\lambda(n) = \frac{a(n)}{n^{\frac{k-1}{2}}}$. Then Theorem 5.1 of Chapter 3 gives lower bounds for the number of sign changes in the terms of the sequences $\{\lambda(n^j)\}_{n\geq 1}$, for $j = 2, 3$ or 4, when n varies in the interval

$[x, 2x]$, for x sufficiently large.

The proof of this theorem relies on an elementary argument taken together with the results O. M. Fomenko [14], G. S. Lü [31], and H. Lao and A. Sankaranarayanan [29].

A generalized modular function (GMF) of weight k and character χ on $\Gamma_0(N)$ is a holomorphic function f on the upper half plane $\mathcal{H}$ satisfying the relation

$$f(\gamma.z) = \chi(\gamma)(cz+d)^k f(z)$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma_0(N)$ and z in $\mathcal{H}$. Here χ is a character of the group $\Gamma_0(N)$ such that $\chi(\gamma) = 1$ for every parabolic element of $\Gamma_0(N)$ of trace 2 and, as usual, $\gamma.z = \frac{az+b}{cz+d}$.

Suppose that f is a generalised modular function and that h is the order of f at $i\infty$. Then it can be shown that there is a complex number a and a sequence of complex numbers $\{c(n)\}_{n\geq 1}$ such that we have

$$f(z) = a\, e^{2\pi i h z} \prod_{n\geq 1} \left(1 - e^{2\pi i n z}\right)^{c(n)}$$

for all z in some neighbourhood of $i\infty$. The $c(n)$ are called the q-exponents of f.

Let f be a generalised modular function with $\mathrm{div}(f) = 0$, that is, suppose that f does not vanish on $\mathcal{H}$ and that it is holomorphic at all cusps. Then its logarithmic derivative is a cusp form of weight 2 for $\Gamma_0(N)$. Moreover, if $a(n)$ are the Fourier coefficients of this cusp form then the c_n are given by $nc(n) = -\sum_{d|n} \mu(n/d)a(d)$. In view of the presence of the Möbius function in this relation, it is natural to ask if the q-exponents $c(n)$ of a generalised modular function with $\mathrm{div}(f) = 0$ change sign infinitely often when they are real. Assuming the weight of f to be 0, W. Kohnen and J. Meher [25] show that this is indeed the case. Their argument is qualitative and depends on Landau's theorem.

Theorem 5.2 of Chapter 3 gives a first quantitative result for the number of sign changes of the sequence of q-exponents over prime numbers. This theorem was subsequently much improved by N. Kumar [28], who used the Sato-Tate conjecture, proved by Barnet-Lamb, Geraghty, Harris and Taylor. Chapter 3 is based on the paper [35], joint authored with Jaban Meher and Karam Deo Shankhadar.

3 Notations

Throughout this thesis, we will use Vinogradov's well-known symbols $\ll$ and $\gg$, in addition to the O and o symbols. Also, when it is convenient to express $f \ll g$ in words, we will say f is majorised by g or that g majorises f. Similarly, we will say f is minorised by g if $f \gg g$. Any dependencies on certain parameters of the constants implicit in Vinogradov's notations will be denoted by indicating these parameters as subscripts to the symbols $\ll$ and $\gg$. When we write $f(x) \sim g(x)$ as $x \to a$, we mean $\lim_{x\to a} \frac{f(x)}{g(x)} = 1$. When a is $+\infty$, we often only write $f(x) \sim g(x)$. When we say $c(\, , \, , \ldots)$ is real number, it means that this real number depends on the parameters in the brackets. Finally, we will write $e(z)$ to denote $e^{2\pi i z}$ for any complex number z. A list of notations used in this thesis is given on page xvii.

CHAPTER 2

Shifted Gaussian Primes as Sets of Uniqueness

1 Introduction

By a shifted Gaussian prime we shall mean a Gaussian integer of the form $\pi + 1$, where π is a Gaussian prime. The main results of this chapter are Theorem 9.1, which states that the complement of any finite subset of the set of shifted Gaussian primes is a set of uniqueness for the family of complex valued additive functions on the non-zero Gaussian integers, and Corollary 8.1 to this theorem, which tells us that for each non-zero Gaussian integer x there is a finite set of rational powers of shifted Gaussian primes whose product is x. A summary of the proofs of these results is given in Section 9 below. In sections 2 and 3 we recall basic facts on multiplicative sets and the Gaussian integers principally to fix terminology that is used throughout this chapter. In sections 4 through 7 we collect together a number of preliminaries used in the proofs of the main results. This chapter is based on the paper [34], jointly authored with Jay Mehta.

2 Multiplicative Sets

We call a subset X of $\mathbf{C}^*$, the multiplicative group of non-zero complex numbers, a *multiplicative set* if it contains the product of any finite subset of its elements. This is equivalent to saying that 1 is in X and the product of any two elements of X belongs to it.

Evidently, $\mathbf{C}^*$ is a multiplicative set. Also, the intersection of any family of multiplicative sets is a multiplicative set. In particular, for any subset A of $\mathbf{C}^*$, the intersection of the multiplicative sets containing A is the smallest multiplicative set containing A. This is called the multiplicative set generated by A. Its elements are all those complex numbers that can be written as a finite product of complex numbers of the form z^k with z in A and an integer $k \geq 0$.

Definition 2.1. *Let A be a subset of a multiplicative set X. Then A is called a set of uniqueness for a family $\mathcal{F}$ of complex valued functions on X if for any functions f, g in $\mathcal{F}$ the relation $f(z) = g(z)$ holds for all $z \in A$ only if the relation $f(z) = g(z)$ holds for all $z \in X$. The set A is called a set of quasi-uniqueness for $\mathcal{F}$ if there is a finite subset B of X such that $A \cup B$ is a set of uniqueness for $\mathcal{F}$.*

Let y and z be elements of a multiplicative set X. Then we write $y|z$ if the complex number $\frac{z}{y}$ belongs to X. This is equivalent to saying that there is a v in X such that $z = yv$. We say that y and z are associates in X if $y|z$ and $z|y$. An associate of 1 in X is called a unit of X. The set of units of X forms a subgroup of $\mathbf{C}^*$ contained in X, called the unit group of X. On the other hand, y and z called coprime if for any v in X the relations $v|y$ and $v|z$ imply that v is a unit of X. Any pair of units of X are associates in X and are coprime.

An additive function on a multiplicative set X is a complex valued function f on X such that the relation $f(yz) = f(y) + f(z)$ holds when y and z are coprime elements of X. An additive function f on X for which $f(yz) = f(y) + f(z)$ holds for all y and z in X is called a completely additive function on X.

Any additive function f on a multiplicative set X vanishes on any finite subgroup of $\mathbf{C}^*$ contained in X. Indeed, we have from $f(1) = f(1 \cdot 1)$ that $f(1) = 0$ and if any z in X belongs to a finite subgroup of $\mathbf{C}^*$, then there is an integer $k > 0$ such that $z^k = 1$. Thus z is a unit of X and hence coprime to itself. This implies that $kf(z) = f(z^k) = f(1)$ from which we get $f(z) = 0$.

A multiplicative function on X is a complex valued function f on X with $f(u) = 1$ for every unit u of X and such that the relation $f(yz) = f(y)f(z)$ holds when y and z are coprime elements of X. A multiplicative function on X for which $f(yz) = f(y)f(z)$ holds for all y and z in X is called a completely multiplicative function on X.

3 Gaussian Integers

The subring of $\mathbf{C}$ consisting of all complex numbers of the form $a + bi$, with a and b integers, is called the ring of Gaussian integers. We denote this ring by $\mathbf{Z}[i]$.

The set of non-zero Gaussian integers is a multiplicative set. Following notation introduced in Chapter 1, we will always write $\mathcal{G}$ to denote this set. The units of the multiplicative set $\mathcal{G}$ are $1, -1, i$ and $-i$.

For any Gaussian integer z, let us write $\mathcal{N}(z)$ to denote $z\bar{z}$, where $\bar{z}$ is the complex conjugate of z. We call $\mathcal{N}(z)$ the norm of z. It can be shown that

$$\mathcal{N}(z) = |\mathbf{Z}[i]/z\mathbf{Z}[i]| \tag{2.1}$$

for all Gaussian integers z. The function $z \mapsto \mathcal{N}(z)$ is a completely multiplicative function on $\mathcal{G}$.

The triangle inequality in the complex plane applied to the Gaussian integers takes the form $\sqrt{N(z+y)} \leq \sqrt{N(z)} + \sqrt{N(y)}$ for any Gaussian integers z, y. On squaring and using the inequality of the arithmetic and geometric means we obtain

$$N(z+y) \leq 2(N(z) + N(y)) \; . \tag{2.2}$$

A Gaussian prime is an element of $\mathcal{G}$ that can be written as uz, where u is a unit of $\mathcal{G}$ and z is one of $1+i$, a prime number $p \equiv -1$ modulo 4 or an element of $\mathcal{G}$ with norm a prime number $p \equiv 1$ modulo 4. We shall normally use the letter π to denote a Gaussian prime hoping that this will not lead to any confusion when we also use π for the numerical constant $3.141\ldots$.

A system of representatives for the set of Gaussian primes is a set of Gaussian primes containing exactly one associate of each Gaussian prime. We shall hereafter write $\mathcal{P}[i]$ to denote such a system of representatives containing $1+i$, fixed once and for all. Also, we shall write $\mathcal{G}^*$ to denote the multiplicative set generated by $\mathcal{P}[i]$. Then $\mathcal{G}^*$ contains exactly one associate of each element of $\mathcal{G}$. Finally, we denote the set of elements of $\mathcal{G}^*$ of the form π^k for a π in $\mathcal{P}[i]$ and an integer $k \geq 1$ by $\mathcal{S}[i]$.

The ring $\mathbf{Z}[i]$ is an integral domain each of whose ideals is principal. For a non-zero ideal of $\mathbf{Z}[i]$ to be a prime ideal it is necessary and sufficient that it is generated by a Gaussian prime. When $\mathfrak{a}$ is an ideal of $\mathbf{Z}[i]$, we define its norm, written $\mathcal{N}(\mathfrak{a})$, to be $|\mathbf{Z}[i]/\mathfrak{a}|$. Since $\mathcal{G}^*$ contains exactly one associate of each element of $\mathcal{G}$, it follows from the formula (2.1) that the map that associates an element of $\mathcal{G}^*$ to the ideal generated by it is a norm preserving bijection from $\mathcal{G}^*$ to the set of non-zero ideals of $\mathbf{Z}[i]$. Its restriction to $\mathcal{P}[i]$ is also a norm preserving bijection from $\mathcal{P}[i]$ to the set of non-zero prime ideals of $\mathbf{Z}[i]$.

Every element z of $\mathcal{G}$ can be written in a unique manner as

$$z = u \prod_{\pi \in \mathcal{P}[i]} \pi^{v_\pi(z)} \ , \tag{2.3}$$

where u is a unit of $\mathcal{G}$ and each $v_\pi(z) = 0$ except for finitely many π, for which $v_\pi(z)$ is an integer > 0. For any y, z in $\mathcal{G}$ the relation $y|z$ is equivalent to $v_\pi(y) \leq v_\pi(z)$ for all $\pi \in \mathcal{P}[i]$.

If f is an additive function on $\mathcal{G}$ then $f(u) = 0$ for any unit u in $\mathcal{G}$, since the unit group of $\mathcal{G}$ is finite. It then follows from the existence and the uniqueness of the factorisation (2.3) that for any map $\tilde{f} : \mathcal{S}[i] \mapsto \mathbf{C}$ there exists a unique additive (resp. multiplicative) function f on $\mathcal{G}$ such that $f(z) = \tilde{f}(z)$ for all z in $\mathcal{S}[i]$. In particular, $\mathcal{S}[i]$ is a set of uniqueness for the family of additive (resp. multiplicative) functions on $\mathcal{G}$.

A complex valued function f on $\mathcal{G}$ is said to be totally additive if for all $z \in \mathcal{G}$

$$f(z) = \sum_{\substack{\pi \in \mathcal{P}[i], \\ \pi | z.}} f(\pi) \ . \tag{2.4}$$

This is equivalent to saying that f is an additive function on $\mathcal{G}$ satisfying the condition $f(\pi) = f(\pi^k)$ for all $\pi \in \mathcal{P}[i]$ and integers $k \geq 1$. Similarly, a complex valued function f on $\mathcal{G}$ is said to be totally multiplicative if for all $z \in \mathcal{G}$

$$f(z) = \prod_{\substack{\pi \in \mathcal{P}[i], \\ \pi | z.}} f(\pi) \ , \tag{2.5}$$

which is the same thing as requiring that f be a multiplicative function on $\mathcal{G}$ such that $f(\pi) = f(\pi^k)$ for all $\pi \in \mathcal{P}[i]$ and integers $k \geq 1$.

We denote by 1 the multiplicative function on $\mathcal{G}$ that takes the constant value 1 on all of $\mathcal{G}$. For each π^k in $\mathcal{S}[i]$ we set $\mu(\pi^k) = -1$ if $k = 1$ and to be 0 for all other k. Further, we set $\mu(u) = 1$ for every unit in $\mathcal{G}$. These relations define a multiplicative function on $\mathcal{G}$, which we denote by μ. This function is the analogue for the Gaussian integers of the usual Möbius function and for any $z \in \mathcal{G}$ we have

$$\sum_{\substack{y|z, \\ y \in \mathcal{G}^*.}} \mu(y) \ = \ \delta(z) \ , \tag{2.6}$$

where $\delta(z) = 1$ if z is a unit in $\mathcal{G}$ and $\delta(z) = 0$ for all other z in $\mathcal{G}$.

When f and g are multiplicative functions on $\mathcal{G}$ and z is any element of $\mathcal{G}$ we define

$$f * g(z) = \sum_{\substack{y|z, \\ y \in \mathcal{G}^*.}} f(y) g\left(\frac{z}{y}\right) \ . \tag{2.7}$$

Then we have that $f * g(z) = g * f(z)$ and $f * g(u) = 1$ for any unit u of $\mathcal{G}$. Moreover, the function $z \mapsto f * g(z)$ is a multiplicative function on $\mathcal{G}$. If f and g are multiplicative functions such that $f = 1 * g$ then we have $\mu * f = g$. This and

(2.6) are called the the Möbius inversion formulae for the Gaussian integers.

For any z in $\mathcal{G}$ we define $\phi(z)$ by the relation

$$\phi(z) = \mathcal{N}(z) \prod_{\substack{\pi \in \mathcal{P}[i], \\ \pi | z.}} \left(1 - \frac{1}{\mathcal{N}(\pi)}\right) . \tag{2.8}$$

Note that $\phi(u) = 1$ for every unit of $\mathcal{G}$, since the product on the right hand side of (2.8) is empty when z is a unit in $\mathcal{G}$. Then $z \mapsto \phi(z)$ is a multiplicative function on $\mathcal{G}$, the analogue of the usual Euler totient function for the Gaussian integers. Moreover, we have the bounds

$$\frac{\mathcal{N}(z)}{\log\log \mathcal{N}(z)} \ll \phi(z) \leq \mathcal{N}(z) , \tag{2.9}$$

for all z in $\mathcal{G}$. Also, it can be seen by means of the Chinese remainder theorem that $\phi(z)$ is equal to the cardinality of the set of invertible elements of the quotient ring $\mathbf{Z}[i]/\mathfrak{a}$, where $\mathfrak{a}$ is the ideal generated by z in $\mathbf{Z}[i]$.

For any real number $X \geq 1$, we write $\mathcal{L}(X)$ to denote the number of $z \in \mathcal{G}^*$ with $\mathcal{N}(z) \leq X$. Then $\mathcal{L}(X)$ is finite for all $X \geq 1$. In fact, we have

$$|\mathcal{L}(X) - \alpha_0 X| \leq \alpha_1 X^{\frac{1}{2}} , \tag{2.10}$$

for all $X \geq 1$, where $\alpha_0 = \frac{\pi}{4}$ and $\alpha_1 = \frac{\pi}{\sqrt{2}}$, with π denoting the numerical constant. It follows from (2.10) that $\mathcal{L}(X) \leq 3X$ for all $X \geq 1$.

More generally, let $\mathcal{L}(X; a, z)$ denote the number of x in $\mathcal{G}^*$ with $\mathcal{N}(x) \leq X$ and such that $x - a$ is divisible by z, where z is in $\mathcal{G}$ and a is a given Gaussian integer with $\mathcal{N}(a) \leq \mathcal{N}(z)$ and $X \geq 1$. Then for any such x the triangle inequality (2.2) gives

$$\mathcal{N}(x-a) \leq 2(\mathcal{N}(x)+\mathcal{N}(a)) \leq 2(X+\mathcal{N}(z)) \ . \tag{2.11}$$

Thus if $x \neq a$ and $w = \frac{x-a}{z}$, then there is a unique associate w^* of w in $\mathcal{G}^*$ and it satisfies $\mathcal{N}(w^*) \leq \left(\frac{2X}{\mathcal{N}(z)}+2\right)$. It follows that for any $X \geq 1$ and any $z \in \mathcal{G}$ we have

$$\mathcal{L}(X;a,z) \leq \mathcal{L}\left(\frac{2X}{\mathcal{N}(z)}+2\right)+1 \ll \frac{X}{\mathcal{N}(z)}+1 \ , \tag{2.12}$$

for all Gaussian integers a with $\mathcal{N}(a) \leq \mathcal{N}(z)$.

The finiteness of $\mathcal{L}(X)$ allows us to measure the size of subsets of $\mathcal{G}$. Thus, for any subset $\mathcal{A}$ of $\mathcal{G}$, let $\mathcal{A}(X)$ be the set of z in $\mathcal{A}$ with $\mathcal{N}(z) \leq X$, for any real number $X \geq 1$. Then $\mathcal{A}(X)$ is a finite set and we define the upper asymptotic density $\overline{\mathbf{d}}(\mathcal{A})$ of $\mathcal{A}$ by the relation

$$\overline{\mathbf{d}}(\mathcal{A}) = \limsup_{X\to+\infty} \frac{|\mathcal{A}(X)|}{X} \ . \tag{2.13}$$

We bring this section to a close with a simple but useful bound. For positive real numbers X, Y and σ with $X < Y$ and $\sigma > 0$ we have

$$\sum_{\substack{z\in\mathcal{G}^*,\\ X<\mathcal{N}(z)\leq Y.}} \frac{1}{\mathcal{N}(z)^\sigma} \ \leq \sum_{\sqrt{X}<k\leq\sqrt{2Y}} \frac{2}{k^{2\sigma-1}} \ , \tag{2.14}$$

where k in the sum on the right hand side varies over the usual integers. To see this, let $|z| = |a|+|b|$ if $z = a+ib$ for any z in $\mathcal{G}$. Then we have $\frac{|z|}{2} \leq \sqrt{\mathcal{N}(z)} \leq |z|$ for all z in $\mathcal{G}$. Moreover, for any integer $k \geq 0$, the number of $z \in \mathcal{G}^*$ such that $|z| = k$ is at most k. The inequality (2.14) follows from these remarks. From (2.14) with

$\sigma = 1$ we have for any $Y \geq 1$ that

$$\sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\leq Y.}} \frac{1}{\mathcal{N}(z)} \leq \sum_{k\leq\sqrt{2Y}} \frac{2}{k} \ll \log 2Y \; . \tag{2.15}$$

Also, for $\sigma > 1$ and any $X \geq 1$ we have

$$\sum_{\substack{z\in\mathcal{G}^*,\\ X<\mathcal{N}(z).}} \frac{1}{\mathcal{N}(z)^\sigma} \leq \sum_{X^{\frac{1}{2}}<k} \frac{2}{k^{2\sigma-1}} \ll_\sigma \frac{1}{X^{\sigma-1}} \; . \tag{2.16}$$

4 Dirichlet Series

Throughout this chapter by a Dirichlet series we shall mean a series of the form

$$\sum_{z\in\mathcal{G}} \frac{a(z)}{\mathcal{N}(z)^s} \; , \tag{2.17}$$

where the $a(z)$ and $s = \sigma + it$ are complex numbers. We say that a Dirichlet series $A(s) = \sum_{z\in\mathcal{G}} \frac{a(z)}{\mathcal{N}(z)^s}$ is *dominated* by the Dirichlet series $B(s) = \sum_{z\in\mathcal{G}} \frac{b(z)}{\mathcal{N}(z)^s}$ if the inequality $|a(z)| \leq b(z)$ holds for all z in $\mathcal{G}$. This means, in particular, that all coefficients $b(z)$ of $B(s)$ are positive real numbers.

If $A(s)$, $B(s)$, $C(s)$ and $D(s)$ are Dirichlet series such that $A(s)$ is dominated by $B(s)$ and $C(s)$ by $D(s)$ then it follows that $A(s) + C(s)$ and $A(s)C(s)$ are dominated by $B(s) + D(s)$ and $B(s)D(s)$ respectively, as follows by writing down the expressions for the coefficients of these series and using the triangle inequality.

A series of complex valued functions $\sum_{i\in I} f_i(s)$ on a set X is said to converge normally on X if the series of positive terms $\sum_{i\in I} \sup_{s\in X} |f_i(s)|$ converges. When a series of functions holomorphic on a non-empty open subset U of the complex plane is normally convergent on each compact subset of U, then the sum of this series is a holomorphic function on U as well.

If $A(s)$ is a Dirichlet series that is absolutely convergent for $s = \sigma_0$, a real number, then it converges normally in each closed half-plane in $\sigma > \sigma_0$. Thus $s \mapsto A(s)$ is a holomorphic function on the half-plane $\sigma > \sigma_0$.

Suppose that the Dirichlet series $A(s) = \sum_{z\in\mathcal{G}} \frac{a(z)}{\mathcal{N}(z)^s}$ is dominated by the Dirichlet series $B(s) = \sum_{z\in\mathcal{G}} \frac{b(z)}{\mathcal{N}(z)^s}$ and that $B(s)$ converges for all $\sigma > 1$. Then $A(s)$ is normally convergent in every closed half plane contained in $\sigma > 1$.

Lemma 4.1. *Let $B(s)$ be a Dirichlet series with positive coefficients and let $A(s)$ be a Dirichlet series that is dominated by $B(s)$. Suppose further that $\{c_n\}_{n\geq 0}$ is a sequence of positive real numbers such that $D(s) = \sum_{n\geq 0} c_n B(s)^n$ is convergent in $\sigma > 1$. Then $D(s)$ is a Dirichlet series and $E(s) = \sum_{n\geq 0} c_n A(s)^n$ is a Dirichlet series that is normally convergent in each closed half-plane in $\sigma > 1$ and is dominated by $D(s)$.*

Proof. For each integer $n \geq 0$, the Dirichlet series $A(s)^n$ is dominated by $B(s)^n$. Let $a_n(z)$ and $b_n(z)$ denote respectively the coefficients of these Dirichlet series. Then for any $s = \sigma + it$ with $\sigma > 1$ we have

$$\sum_{n\geq 0} c_n \sum_{z\in\mathcal{G}} \frac{b_n(z)}{\mathcal{N}(z)^\sigma} = \sum_{n\geq 0}\sum_{z\in\mathcal{G}} \frac{c_n b_n(z)}{|\mathcal{N}(z)^s|} = \sum_{z\in\mathcal{G}} \frac{\sum_{n\geq 0} c_n b_n(z)}{\mathcal{N}(z)^\sigma}, \qquad (2.18)$$

where the equalities are justified by the positivity of the terms. Since the first double sum in (2.18) is convergent, so are all the sums. In particular, $d(z) = \sum_{n\geq 0} c_n b_n(z)$ converges for each z in $\mathcal{G}$ and we have

$$D(s) = \sum_{n\geq 0} c_n B(s)^n \;=\; \sum_{n\geq 0} c_n \sum_{z\in\mathcal{G}} \frac{b_n(z)}{\mathcal{N}(z)^s} = \sum_{z\in\mathcal{G}} \frac{\sum_{n\geq 0} c_n b_n(z)}{\mathcal{N}(z)^s} \;, \tag{2.19}$$

where the last equality is justified by the convegence of the second double sum in (2.18). Thus $D(s)$ is a Dirichlet series with positive coefficients $d(z)$ and converges in $\sigma > 1$. Further, since $|a_n(z)| \leq b_n(z)$ for all $n \geq 0$ and all z, we see that

$$\sum_{n\geq 0} \sum_{z\in\mathcal{G}} \frac{c_n |a_n(z)|}{|\mathcal{N}(z)^s|} \tag{2.20}$$

is convergent. It then follows that

$$E(s) = \sum_{n\geq 0} c_n A(s)^n \;=\; \sum_{n\geq 0} c_n \sum_{z\in\mathcal{G}} \frac{a_n(z)}{\mathcal{N}(z)^s} = \sum_{z\in\mathcal{G}} \frac{\sum_{n\geq 0} c_n a_n(z)}{\mathcal{N}(z)^s} \;. \tag{2.21}$$

Thus $E(s)$ is a Dirichlet series with coefficients $e(z) = \sum_{n\geq 0} c_n a_n(z)$ and converges for $\sigma > 1$. Since we have $|e(z)| \leq d(z)$ for each z, we conclude that $E(s)$ is dominated by $D(s)$ and therefore that $E(s)$ converges normally in each closed half-plane in $\sigma > 1$.

□

Let f be a multiplicative function on $\mathcal{G}$. The Dirichlet series associated to f is defined by

$$F(s) = \sum_{z\in\mathcal{G}*} \frac{f(z)}{\mathcal{N}(z)^s} \;. \tag{2.22}$$

When for all $z \in \mathcal{G}$ we have $|f(z)| \leq 1$, the right hand side of (2.22) is normally convergent on any closed half plane in $\sigma > 1$ and defines a holomorphic function in $\sigma > 1$. Further, we have

$$F(s) = \prod_{\pi \in \mathcal{P}[i]} \sum_{k \geq 0} \frac{f(\pi^k)}{\mathcal{N}(\pi^k)^s} \,. \tag{2.23}$$

The product on the right hand side is called the Euler product associated to f and is normally convergent in any closed half plane in $\sigma > 1$.

We shall write $G(s)$ to denote the Dirichlet series associated to the multiplicative function g that is 1 on all $z \in \mathcal{G}$. Then $G(s)$ is the same as the Dedekind zeta function of the number field $\mathbf{Q}(i)$. The function $G(s)$ has a meromorphic continuation to the entire complex plane that is analytic outside the point $s = 1$, where it has a simple pole. Moreover, $G(s)$ is non-zero on the closed half-plane $\sigma \geq 1$.
By logarithmic differentiation of the Euler product associated to g we obtain

$$\frac{G'}{G}(s) \;=\; \sum_{\pi \in \mathcal{P}[i]} \sum_{k \geq 1} \frac{\log \mathcal{N}(\pi)}{\mathcal{N}(\pi^k)^s} \,, \tag{2.24}$$

where the Dirichlet series on the right hand side is normally convergent on every closed half plane in $\sigma > 1$. Since $G(s) \neq 0$ on the half plane $\sigma \geq 1$, we see that $\frac{G'}{G}(s)$ extends as a meromorphic function in a neighbourhood of $\sigma \geq 1$, which is analytic in this neighbourhood except for a simple pole at $s = 1$. In particular, we have that $(s-1)\frac{G'}{G}(s)$ is bounded on the rectangle $1 \leq \sigma \leq 4$ and $|t| \leq \frac{1}{2}$.

5 Counting Gaussian Primes

Let $\Pi(X)$ be the number of $\pi \in \mathcal{P}[i]$ with $\mathcal{N}(\pi) \leq X$. Then it follows from the prime ideal theorem (see page 358 of [37]) that there is a real number $c > 0$ such that the asymptotic formula

$$\Pi(X) = \mathrm{li}(X) + O(X \exp(-c\sqrt{\log X})) \tag{2.25}$$

holds, where $\mathrm{li}(X) = \int_2^X \frac{dt}{\log t}$. Since $\mathrm{li}(X) \sim \frac{X}{\log X}$, we obtain from (2.25) that

$$\Pi(X) \sim \frac{X}{\log X} . \tag{2.26}$$

An integration by parts now shows that

$$\sum_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) \leq X.}} \frac{1}{\mathcal{N}(\pi)} \sim \log\log X \quad \text{and} \quad \sum_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) \leq X.}} \frac{\log \mathcal{N}(\pi)}{\mathcal{N}(\pi)} \sim \log X . \tag{2.27}$$

Let $Y = Y(X)$ satisfy $Y(X) \sim \frac{X}{\log^m X}$ for an integer $m \geq 1$. Then by (2.25) we have

$$\Pi(X+Y) - \Pi(X) \sim \frac{Y}{\log X} , \tag{2.28}$$

since $X \exp(-c\sqrt{\log X}) = o(Y)$ and $\int_X^{X+Y} \frac{dt}{\log t} \sim \frac{Y}{\log X}$.

Let z be an element of $\mathcal{G}$ and a denote an invertible residue class in $\mathbf{Z}[i]/z\mathbf{Z}[i]$. We shall write $\Pi(X; a, z)$ for the number of $\pi \in \mathcal{P}[i]$ belonging to the class of a modulo z and such that $\mathcal{N}(\pi) \leq X$. Then generalising (2.25) we have the asymptotic formula

$$\Pi(X; a, z) = \frac{\mathrm{li}(X)}{\phi(z)} + O(X \exp(-c\sqrt{\log X})) , \tag{2.29}$$

where $c > 0$ is a real number that depends on z. This is Corollary 1 (i), page 358 of [37] applied to $K = \mathbf{Q}(i)$.

We now record a certain number of facts that allow us to circumvent the lack of uniformity in z in the error term of (2.29). The first is the trivial estimate for $\Pi(X; a, z)$. That is, on choosing a^* to be a Gaussian integer with $\mathcal{N}(a^*) \leq \mathcal{N}(z)$ lying in the residue class a modulo z we have from (2.12) that

$$\Pi(X; a, z) \ \leq \ \mathcal{L}(X; a^*, z) \ \ll \ \frac{X}{\mathcal{N}(z)} + 1 \tag{2.30}$$

for all $X \geq 2$. The second is the Brun-Titchmarsh theorem which says that for any α in $(0, 1)$ there is a real number $c(\alpha)$ such for all $X \geq 2$ and all $z \in \mathcal{G}$ with $\mathcal{N}(z) \leq X^\alpha$ we have

$$\Pi(X; a, z) \ \leq \ \frac{c(\alpha)X}{\phi(z) \log X} \tag{2.31}$$

for all invertible residue classes a modulo z. This follows from Theorem 4 of [17] applied with $K = \mathbf{Q}(i)$ and $\mathfrak{N}\mathfrak{q} \leq X^\alpha$.

The final fact we will need is the Bombieri-Vinogradov Theorem. For any z in $\mathcal{G}$ and an invertible residue class a modulo z we define $E(X; a, z)$ for all real $X \geq 1$ by the relation

$$E(X; a, z) \ = \ \Pi(X; a, z) - \frac{\mathrm{li}(X)}{\phi(z)} \ . \tag{2.32}$$

By means of the trivial estimate (2.30) and the lower bound in (2.9) we have

$$|E(X; a, z)| \ \leq \ \Pi(X; a, z) + \frac{\mathrm{li}(X)}{\phi(z)} \ll \frac{X \log \log \mathcal{N}(z)}{\mathcal{N}(z)} + 1 \ , \tag{2.33}$$

using the triangle inequality and since li(X) $\ll$ X. Therefore, if we set

$$E^*(X;z) = \sup_{a \bmod^* z} \sup_{Y \le X} |E(Y;a,z)| \ , \tag{2.34}$$

where $a \bmod^* z$ means that a varies over the invertible residue classes in $\mathbf{Z}[i]/z\mathbf{Z}[i]$, then we have from (2.33) that

$$E^*(X;z) \ \ll \ \frac{X \log\log \mathcal{N}(z)}{\mathcal{N}(z)} + 1 \ . \tag{2.35}$$

A version of the very non-trivial Bombieri-Vinogradov theorem is the assertion that

$$\sum_{\mathcal{N}(z) \le X^{\frac{1}{5}} (\log X)^3} E^*(X,z) \ll \frac{X}{(\log X)^5} \tag{2.36}$$

for all $X \ge 1$. In fact, on taking $I = [0, 2\pi)$ and $K = \mathbf{Q}(i)$ in the corollary on page 203 of [21], we obtain a sharper conclusion than we have stated. However, (2.36) is adequate for us and corresponds to the result used by Elliott [9] in the case of $\mathbf{N}^*$.

6 Turán-Kubilius For Gaussian Integers

For any totally additive function f on $\mathcal{G}$ and a real number $X \ge 1$, we set

$$E(f,X) = \sum_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) \le X.}} \frac{f(\pi)}{\mathcal{N}(\pi)} \ \text{ and } \ B(f,X) = \sum_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) \le X.}} \frac{|f(\pi)|^2}{\mathcal{N}(\pi)} \ . \tag{2.37}$$

The proposition below is a special case of a general Turán-Kubilius inequality given by O. Ramaré and G. Bhowmik, [3], Theorem 2, page 61. See also Lemma 1, page 269 of [2]. For the proof of the proposition, we follow [3] and [10], which, in turn, rely on the well-known method of P. Turán.

Proposition 6.1. *For any complex valued totally additive function f on $\mathcal{G}$ and any $X \geq 4$ we have*

$$\sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} |f(z) - E(f, X)|^2 \ll B(f, X)X . \tag{2.38}$$

Proof. Let us first remark that it suffices to prove the proposition for any positive real valued totally additive function. Indeed, for a given $X \geq 4$, and any complex valued totally additive function f, let $L(f)$ and $R(f)$ denote the left and right hand sides of (2.38), respectively. Further, let $f_1 = \mathrm{Re}(f)$ and $f_2 = \mathrm{Im}(f)$. Then f_1, f_2 are real valued totally additive functions. Moreover, we have

$$L(f) = L(f_1) + L(f_2) \text{ and } R(f) = R(f_1) + R(f_2) . \tag{2.39}$$

For $i = 1, 2$, let us set $f_i^+(z) = f_i(z)$ when $f_i(z) \geq 0$ and $f_i^+(z) = 0$ otherwise. Let us also set $f_i^- = f_i^+ - f_i$. Then f_i^+, f_i^- are positive real valued totally additive functions on $\mathcal{G}$. Further, on squaring both sides of the relation $f_i = f_i^+ - f_i^-$ we see that $|f_i|^2 = |f_i^+|^2 + |f_i^-|^2$, since $f_i^+ f_i^- = 0$. It follows that we have

$$R(f_i^+) + R(f_i^-) = R(f_i) . \tag{2.40}$$

Also, on using the elementary inequality $(|a| + |b|)^2 \leq 2(|a|^2 + |b|^2)$, we obtain that

$$L(f_i) = L(f_i^+ - f_i^-) \leq 2(L(f_i^+) + L(f_i^-)) . \tag{2.41}$$

We then conclude from (2.39), (2.40) and (2.41) that it suffices to prove (2.38) for f_i^+ and f_i^- for $i = 1, 2$, thus justifying our remark.

Suppose now that f is a totally additive function on $\mathcal{G}$ with $f(z) \geq 0$ for all z in $\mathcal{G}$. For brevity we shall write E, B and L for $E(f,X)$ and $B(f,X)$ and $L(f)$, respectively. Then we are to show that $L \ll BX$, for all $X \geq 4$. We begin by opening the square in the summand on the left hand side of (2.38) to obtain

$$L = \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} f(z)^2 - 2E \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} f(z) + E^2 \mathcal{L}(X) \,, \tag{2.42}$$

where $\mathcal{L}(X)$ is as in (2.10). We shall presently estimate each term on the right hand side of (2.42). To this end, let us first note that

$$E^2 \;\leq\; B \sum_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) \leq X.}} \frac{1}{\mathcal{N}(\pi)} \;\ll\; B \log\log X \,, \tag{2.43}$$

on writing $\frac{f(\pi)}{\mathcal{N}(\pi)}$ as $\frac{f(\pi)}{\mathcal{N}(\pi)^{\frac{1}{2}}} \cdot \frac{1}{\mathcal{N}(\pi)^{\frac{1}{2}}}$ and applying the Cauchy-Schwarz inequality together with (2.27).

Let us now estimate the first sum on the right hand side of (2.42). Thus on squaring both sides of (2.4) and rearranging the terms we get

$$f(z)^2 \;=\; \sum_{\substack{\pi \neq \pi' \in \mathcal{P}[i], \\ \pi, \pi' | z.}} f(\pi) f(\pi') \;+\; \sum_{\substack{\pi \in \mathcal{P}[i], \\ \pi | z.}} f(\pi)^2 \,, \tag{2.44}$$

for any z in $\mathcal{G}^*$. Summing both sides of (2.44) over z with $\mathcal{N}(z) \leq X$ we obtain

$$\sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} f(z)^2 \;=\; \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} \sum_{\substack{\pi \neq \pi' \in \mathcal{P}[i], \\ \pi, \pi' | z.}} f(\pi) f(\pi') \;+\; \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} \sum_{\substack{\pi \in \mathcal{P}[i], \\ \pi | z.}} f(\pi)^2 \,. \tag{2.45}$$

The relations $\pi \neq \pi'$ and $\pi, \pi' | z$ imply $\pi\pi' | z$. This remark together with an interchange of summations shows that the first term on the right hand side of (2.45) does not exceed the first term of

$$\sum_{\substack{\pi,\pi' \in \mathcal{P}[i], \\ \mathcal{N}(\pi\pi') \leq X.}} f(\pi) f(\pi') \mathcal{L}\left(\frac{X}{\mathcal{N}(\pi\pi')}\right) + \sum_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) \leq X.}} f(\pi)^2 \mathcal{L}\left(\frac{X}{\mathcal{N}(\pi)}\right) . \tag{2.46}$$

A further interchange of summations shows that the second term on the right hand side of (2.45) is the same as the second term of (2.46).

The estimate $\mathcal{L}(t) \leq 3t$ for all $t \geq 1$ yields the upper bound $3BX$ for the second term of (2.46). Using the more precise bound $\mathcal{L}(t) \leq \alpha_0 t + \alpha_1 t^{\frac{1}{2}}$, given by (2.10), we see that the first term in (2.46) does not exceed

$$\alpha_0 X \sum_{\substack{\pi,\pi' \in \mathcal{P}[i], \\ \mathcal{N}(\pi\pi') \leq X.}} \frac{f(\pi) f(\pi')}{\mathcal{N}(\pi\pi')} + \alpha_1 X^{\frac{1}{2}} \sum_{\substack{\pi,\pi' \in \mathcal{P}[i], \\ \mathcal{N}(\pi\pi') \leq X.}} \frac{f(\pi) f(\pi')}{\mathcal{N}(\pi\pi')^{\frac{1}{2}}} . \tag{2.47}$$

The first term in (2.47) is at most $\alpha_0 E^2 X$. Let us momentarily write S for the sum in the second term of (2.47). By means of the Cauchy-Schwarz inequality we then see that

$$S^2 \leq \sum_{\substack{\pi,\pi' \in \mathcal{P}[i], \\ \mathcal{N}(\pi\pi') \leq X.}} \frac{f(\pi)^2 f(\pi')^2}{\mathcal{N}(\pi)\mathcal{N}(\pi')} \sum_{\substack{\pi,\pi' \in \mathcal{P}[i], \\ \mathcal{N}(\pi\pi') \leq X.}} 1 \leq 2B^2 \Pi_2(X) , \tag{2.48}$$

where $\Pi_2(X)$ is the number of $z \in \mathcal{G}^*$ with $\mathcal{N}(z) \leq X$ that can be written as $\pi\pi'$ for some $\pi, \pi' \in \mathcal{P}[i]$. Gathering together our estimates and using the trivial bounds $\Pi_2(X) \leq \mathcal{L}(X) \leq 3X$, we conclude that

$$\sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le X.}} f(z)^2 \le \alpha_0 E^2 X + (\sqrt{6}\alpha_1 + 3)BX \ . \tag{2.49}$$

Let us now consider the second term on the right hand side of (2.42). On using (2.5) we have

$$\sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le X.}} f(z) = \sum_{\substack{\pi\in\mathcal{P}[i],\\ \mathcal{N}(\pi)\le X.}} f(\pi)\mathcal{L}\left(\frac{X}{\mathcal{N}(\pi)}\right) \ , \tag{2.50}$$

after an interchange of summations. From (2.10) we have $\mathcal{L}(t) \ge \alpha_0 t - \alpha_1 t^{\frac{1}{2}}$ and consequently

$$-2E \sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le X.}} f(z) \le -2\alpha_0 E^2 X + 2\alpha_1 E X^{\frac{1}{2}} \sum_{\substack{\pi\in\mathcal{P}[i],\\ \mathcal{N}(\pi)\le X.}} \frac{f(\pi)}{\mathcal{N}(\pi)^{\frac{1}{2}}} \ . \tag{2.51}$$

Denoting the sum on the right hand side of the above relation by T we have

$$T^2 \le B \sum_{\substack{\pi\in\mathcal{P}[i],\\ \mathcal{N}(\pi)\le X.}} 1 \ll \frac{BX}{\log X} \ , \tag{2.52}$$

by the Cauchy-Schwarz inequality and (2.26). Thus on combining (2.52), (2.51) and (2.43) we conclude that

$$-2E \sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le X.}} f(z) \le -2\alpha_0 E^2 X + CBX\sqrt{\frac{\log\log X}{\log X}} \tag{2.53}$$

for some $C > 0$. Finally, using (2.10) with (2.43), we have for some $C_1 > 0$ that

$$E^2\mathcal{L}(X) \le \alpha_0 E^2 X + C_1\alpha_1 B X^{\frac{1}{2}} \log\log X \ . \tag{2.54}$$

The inequality $L \ll BX$, with an absolute implied constant, results on combining (2.42) with (2.49), (2.53) and (2.54).

$\square$

The proof of the proposition in fact gives an explicit value for the implied constant in (2.38); we shall, however, not have much use for this value.

Corollary 6.1. *Let f be a complex valued totally additive function on $\mathcal{G}$. Further, for any $\lambda > 0$, let $\mathcal{E}(\lambda, f, X)$ be the set of $z \in \mathcal{G}^*$ satisfying the conditions*

$$\mathcal{N}(z) \ \leq \ X \ \text{ and } \ \lambda < |f(z) - E(f, X)| \ . \tag{2.55}$$

Then we have $|\mathcal{E}(\lambda, f, X)| \ll \frac{B(f,X)X}{\lambda^2}$ for all $X \geq 4$.

Proof. Indeed, we have

$$\lambda^2 |\mathcal{E}(\lambda, f, X)| \ < \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} (f(z) - E(f, X))^2 \ . \tag{2.56}$$

The corollary follows on using (2.38) to estimate the right hand side of (2.56). $\square$

7 Thin Sets

We call a $\mathcal{Z} \subseteq \mathcal{G}$ a *thin set* if $\sum_{z \in \mathcal{Z}} \frac{1}{\mathcal{N}(z)}$ converges. The empty subset of $\mathcal{G}$ is a thin set. Every subset of a thin set is a thin set. Any finite union of thin sets is a thin set. For any subset $\mathcal{A}$ of $\mathcal{G}$, a thin set contained in $\mathcal{A}$ is called a *thin subset* of $\mathcal{A}$. By an abuse of terminology, a thin subset of $\mathcal{P}[i]$ is called a *thin set of primes*.

With π denoting, as before, an element of $\mathcal{P}[i]$ we have the following simple but useful proposition, which is a minor variation on Lemma 11.1 of Elliott [11], Volume 2. Intuitively speaking, this proposition asserts that large subsets of $\mathcal{G}$ contain a large number of nearly square-free Gaussian integers almost all of whose prime divisors lie outside a given thin set of primes.

Proposition 7.1. *Let $\mathcal{Z}$ be a thin set of primes and $X \geq 1$. Then for each $c > 0$ there is an integer $l(c)$ such that any subset U of $\mathcal{G}^*$, with $\mathcal{N}(z) \leq X$ for all $z \in U$ and $|U| \geq cX$, there is a subset V of U with $|V| \geq \frac{cX}{2}$ and the property that every $z \in V$ satisfies the following conditions.*

(i) $\pi | z$ and $\mathcal{N}(\pi) > l(c)$ implies $\pi \notin \mathcal{Z}$ and π^2 does not divide z.

(ii) $\pi | z$ and $\mathcal{N}(\pi) \leq l(c)$ implies $v_\pi(z) \leq l(c)$.

Proof. Let $\mathcal{Q}$ be the set of π^2 as π runs through $\mathcal{P}[i]$. Then $\mathcal{X} = \mathcal{Z} \cup \mathcal{Q}$ is a thin set. For any integer $l \geq 1$, let $\mathcal{E}_l$ be the set of $z \in \mathcal{G}^*$ with $\mathcal{N}(z) \leq X$ that are a multiple of some $x \in \mathcal{X}$ with $\mathcal{N}(x) \geq l$. Then we have

$$|\mathcal{E}_l| \leq \sum_{\substack{x \in \mathcal{X}, \\ l \leq \mathcal{N}(x) \leq X.}} \mathcal{L}\left(\frac{X}{\mathcal{N}(x)}\right) \leq X \sum_{\substack{x \in \mathcal{X}, \\ \mathcal{N}(x) \geq l.}} \frac{1}{\mathcal{N}(x)}\,, \tag{2.57}$$

by means of the trivial estimate $\mathcal{L}(t) \leq 3t$.

Now let $\mathcal{E}'_l$ be the set of $z \in \mathcal{G}^*$ with $\mathcal{N}(z) \leq X$ that are a multiple of π^m, for some $\pi \in \mathcal{P}[i]$ with $1 \leq \mathcal{N}(\pi) \leq l$ and an integer $m > l$. Then we have

$$|\mathcal{E}'_l| \leq \sum_{\substack{\pi \in \mathcal{P}[i], \\ 1 \leq \mathcal{N}(\pi) \leq l.}} \sum_{m > l} \mathcal{L}\left(\frac{X}{\mathcal{N}(\pi^m)}\right)\,. \tag{2.58}$$

Since $\mathcal{L}(t) \leq 3t$ and $\mathcal{N}(\pi) \geq 2$ for any $\pi \in \mathcal{P}[i]$, the inner sum on the right hand side of (2.58) does not exceed $\frac{X}{2^l}$. Therefore, we have $|\mathcal{E}_l'| \leq \frac{lX}{2^l}$. Since $\sum_{x\in\mathcal{X}} \frac{1}{\mathcal{N}(x)}$ converges, there is an integer $l = l(c)$ such that

$$\sum_{\substack{x\in\mathcal{X},\\ \mathcal{N}(x)\geq l.}} \frac{1}{\mathcal{N}(x)} + \frac{l}{2^l} \leq \frac{c}{2}\,. \tag{2.59}$$

Then for $l = l(c)$ we have $|\mathcal{E}_l \cup \mathcal{E}_l'| \leq \frac{cX}{2}$ and on setting $V = U \setminus (\mathcal{E}_l \cup \mathcal{E}_l')$, we see that the requirements of the proposition are met.

□

The following corollary to Proposition 7.1 will allow us to restrict our attention to totally additive functions in a number of instances.

Corollary 7.1. *Let $X \geq 1$ and suppose that f and g are additive functions on $\mathcal{G}$ such that the set $\mathcal{Z}$ of all $\pi \in \mathcal{P}[i]$ for which $f(\pi) \neq g(\pi)$ is a thin set of primes. Then for each $c > 0$ there is a $d > 0$ such that every subset U of $\mathcal{G}$, with $\mathcal{N}(z) \leq X$ for all $z \in U$ and $|U| \geq cX$, contains a subset W with $|W| \geq dX$ and the property that*

$$f(z) - f(z') = g(z) - g(z') \text{ for all } z \text{ and } z' \text{ in } W. \tag{2.60}$$

Proof. For $l = l(c)$ as in the proposition, let $\mathcal{A}$ be the set of $a \in \mathcal{G}^*$ with prime factorisation $a = \prod_{\pi\in\mathcal{P}[i]} \pi^{v_\pi(a)}$, where $v_\pi(a) \leq l$ when $\mathcal{N}(\pi) \leq l$ and $v_\pi(a) = 0$ for all other π. Also, let $\mathcal{D}$ be the set of all $s \in \mathcal{G}^*$, with s square-free and such that $\pi|s \implies \pi \notin \mathcal{Z}$ and $\mathcal{N}(\pi) > l$. Let V be the subset of U supplied by Proposition 7.1. Then every $z \in V$ can be uniquely written as $z = as$ with $a \in \mathcal{A}$ and $s \in \mathcal{D}$ with s satisfying the condition

(γ) $\pi | s \implies \pi \nmid a, \pi \notin \mathcal{Z}, \pi^2 \nmid s$.

For each $a \in \mathcal{A}$, let $V_a \subset V$ consists of all $z \in V$ of the form $z = as$ for some $s \in \mathcal{D}$. Since f and g are additive, we have using the condition (γ) that

$$f(z) = f(a) + f(s) = f(a) + g(s) = f(a) - g(a) + g(z) \tag{2.61}$$

for all z in V_a. Since V is the union of the sets V_a, there is an $a \in \mathcal{A}$ with $|V_a| \geq \frac{|V|}{|\mathcal{A}|}$. Let us set $W = V_a$ for such an a. Since $|V| \geq \frac{cX}{2}$ by Proposition 7.1 and $|\mathcal{A}| \leq l^l$ by a trivial estimate, we have $|W| \geq dX$ with $d = \frac{c}{2l^l}$. Moreover, (2.61) implies (2.60). □

8 Main Results

At the suggestion of Professor I. Kátai we showed, in the joint work [33] with Jay Mehta, that the set of shifted Gaussian primes is a set of quasi-uniqueness for the family of completely additive functions on $\mathcal{G}$, the set of non-zero Gaussian integers. Our proof of this result is detailed in Jay Mehta's thesis. In a subsequent joint work [34], we gave a proof of the following much stronger theorem and its corollary below.

Theorem 8.1. *The complement in the shifted Gaussian primes of any finite subset is a set of uniqueness for the family of complex valued additive functions on $\mathcal{G}$.*

For a non-zero complex number x we shall call a complex number of the form $\exp(rz)$, where r is a rational number and z satisfies $\exp(z) = x$, an r-th power of x or, less precisely, a rational power of x. When r is an integer, every r-th power of x is the same as x^r. We now have the following corollary to Theorem 8.1.

Corollary 8.1. *Every element of $\mathcal{G}$ can be expressed as a product of finitely many rational powers of shifted Gaussian primes.*

This expression of non-zero Gaussian integers as products of rational powers of shifted Gaussian primes is plainly non-unique. For instance, $-1+2i$ and $-3+2i$ are Gaussian primes that are not even associates and we have

$$(1+i)^6 = ((-1+2i)+1)^3 = ((-3+2i)+1)^2 . \tag{2.62}$$

9 Summary of the Proofs

Here we summarise the proofs of Theorem 8.1 and its corollary. We take up the theorem first, for which we have followed Elliott [9] closely.

If f and g are complex valued additive functions on $\mathcal{G}$ then so is $f-g$. Thus a subset $\mathcal{A}$ of $\mathcal{G}$ is a set of uniqueness for the family of complex valued additive functions on $\mathcal{G}$ if and only if any such function vanishing on $\mathcal{A}$ in fact vanishes on all of $\mathcal{G}$. Also, if $\mathcal{A}$ is the complement in the shifted Gaussian primes of a finite subset, then there are only finitely many $\pi \in \mathcal{P}[i]$ such that $\pi+1 \notin \mathcal{A}$. Therefore, the proof of Theorem 8.1 reduces to that of the following theorem.

Theorem 9.1. *Let f be a complex valued additive function on $\mathcal{G}$ and $\mathcal{X}$ be a finite subset of $\mathcal{P}[i]$ such that $f(\pi+1)=0$ for each π in the complement of $\mathcal{X}$ in $\mathcal{P}[i]$. Then we have that $f(z)=0$ for all $z \in \mathcal{G}$.*

The proof of Theorem 9.1 rests on the assertion that any subset $\mathcal{A}$ of $\mathcal{G}$ with $\overline{\mathbf{d}}(\mathcal{A})>0$ is "nearly" a set of uniqueness for the family of complex valued additive functions f on $\mathcal{G}$. More precisely, if such an f vanishes on $\mathcal{A}$ then there is a thin set of primes

$\mathcal{Z}$ (see Section 7) such that $f(\pi) = 0$ for any $\pi \in \mathcal{P}[i]$ that does not belong to $\mathcal{Z}$. This is Corollary 14.1 to Theorem 14.1. This theorem is an analogue for additive functions on $\mathcal{G}$ of a deep result of P. Erdös [13] for additive functions on $\mathbf{N}^*$. The original proof of Erdös' result is elementary but rather complicated. This result and the key theorems leading to it have been revisited by C. Ryavec [40] and Elliott and Ryavec [12], the latter from a probabilistic point of view.

We prove Theorem 14.1 by a combination of methods from the aforementioned sources and Tenenbaum [43]. We have, however, avoided using the probabilistic language for the sake of simplicity. The proof of Theorem 14.1 is the content of sections 10 to 14. We have given a complete proof of Theorem 14.1 in this chapter partly because it is stated without proof in the paper [34]. Corollary 14.1 is an immediate consequence of the theorem. Theorem 14.1 is itself a consequence of Theorem 13.1 characterising the analogue for $\mathcal{G}$ of what Erdös has called finitely distributed additive functions (see Definition 13.1). The principle of the proof of these theorems is to observe that if f is a real valued additive function on $\mathcal{G}$ then, for any real number θ, the function $z \mapsto e^{2\pi i\theta f(z)}$ is a multiplicative function on $\mathcal{G}$ taking values in $\mathbf{U}$, the set of complex numbers with absolute value 1, and then to exploit this by letting θ vary over $\mathbf{R}$. For this reason, we begin with sections 10 and 11 on mean values of multiplicative functions and the analogue for the Gaussian integers of the central part of the well-known theorem of G. Hálasz for multiplicative functions on $\mathbf{N}^*$.

Let $\mathcal{E}$ be the set of z in $\mathcal{G}^*$ such that $\pi'+1 = z(\pi+1)$ for some $\pi, \pi' \in \mathcal{P}[i]$, with $\pi+1$ coprime to z. If f is a complex value additive function on $\mathcal{G}$ such that $f(\pi+1) = 0$ for all $\pi \in \mathcal{P}[i]$ then evidently f vanishes on $\mathcal{E}$. Taking account of Corollary 14.1, it is natural to ask if $\overline{\mathbf{d}}(\mathcal{E}) > 0$. Proposition 16.1 of Section 16 tells us that this is indeed the case. We prove this proposition by means of an application of the Cauchy-Schwarz inequality that is typical in additive representation problems. This requires two inputs. The first is a lower bound for the number of pairs (π', π), where π' and π in $\mathcal{P}[i]$ are such that $\mathcal{N}(\pi') \le X$ and $\pi + 1 | \pi' + 1$ with $\pi + 1$ coprime to $\frac{\pi'+1}{\pi+1}$. With suitable size restrictions on π as well, the required lower bound is an easy consequence of the prime ideal theorem and the Bombieri-Vinogradov Theorem for the Gaussian integers given by (2.25) and (2.36) respectively, together with the trivial estimate (2.35). The second input required is an upper bound for the number of pairs (π', π) with π' and π in $\mathcal{P}[i]$ satisfying $\pi' + 1 = z(\pi + 1)$ for a given z in $\mathcal{G}$ but subject to the same size restrictions as before. For the analogous problem in the natural numbers in [9], Elliott appeals to a classical bound obtained by means of the Selberg Sieve. However, the extension of the Selberg Sieve to number fields seems cumbersome to apply in our context. For this reason, we use the Large Sieve for number fields in the manner described in Section 15.

With Proposition 16.1 and Corollary 14.1 in place, it is easily seen that for any complex valued additive function f on $\mathcal{G}$ satisfying the hypothesis of Theorem 9.1 there is a thin set of primes $\mathcal{Z}$ such that $f(\pi) = 0$ for any $\pi \in \mathcal{P}[i]$ that does not belong to $\mathcal{Z}$. To obtain the conclusion of the theorem from this, we use Proposition 16.2 which tells us that given any y in $\mathcal{G}$ there are infinitely many π' in $\mathcal{P}[i]$ satisfying

$$\pi' + 1 = (1 + i)yw \; , \tag{2.63}$$

where w is a square-free element of $\mathcal{G}$ such that w is coprime to $(1 + i)y$ and none of its prime divisors in $\mathcal{P}[i]$ belong to $\mathcal{Z}$. We prove Proposition 16.2 by obtaining a positive lower bound for the density of such π' in $\mathcal{P}[i]$. This leads us, naturally, to obtain upper bounds for the number of π' with $\mathcal{N}(\pi') \leq X$ such that $\pi'+1$ is divisible by $(1+i)yz$ with $\mathcal{N}(z)$ suitably large and z in $\mathcal{Z} \cup \mathcal{Q}$, where $\mathcal{Q} = \{\pi^2 \mid \pi \in \mathcal{P}[i]\}$. The required upper bounds in this case are supplied by the Brun-Titchmarsh theorem for number fields given by (2.31) and Proposition 15.1 of Section 15, together with some trivial estimates.

Since there are infinitely many π' in $\mathcal{P}[i]$ satisfying (2.63), there is certainly one such that $f(\pi' + 1) = 0$. Taking account of the properties of w we have that $f(w) = 0$ and therefore $f((1 + i)y) = 0$ from (2.63). Since y is any element of $\mathcal{G}$, we have that f vanishes on the set of all multiples of the prime element $1 + i$ in $\mathcal{G}$. On remarking that this set is a set of uniqueness for the family of complex valued additive functions on $\mathcal{G}$, we obtain Theorem 9.1.

Theorem 8.1 tells us in particular that the set of shifted Gaussian primes is a set of uniqueness for the family of completely additive functions on $\mathcal{G}$. In Section 17 we show by a generalisation of an argument of Wolke [44] that this means that the sets of logarithms of all shifted Gaussian primes generate the $\mathbf{Q}$-vector space generated by the sets of logarithms of all elements of $\mathcal{G}$ in $\mathbf{C}$. On passing to the exponential we then obtain the conclusion of Corollary 8.1.

The following figure gives a schematic diagram of the interdependencies of the various sections of this chapter.

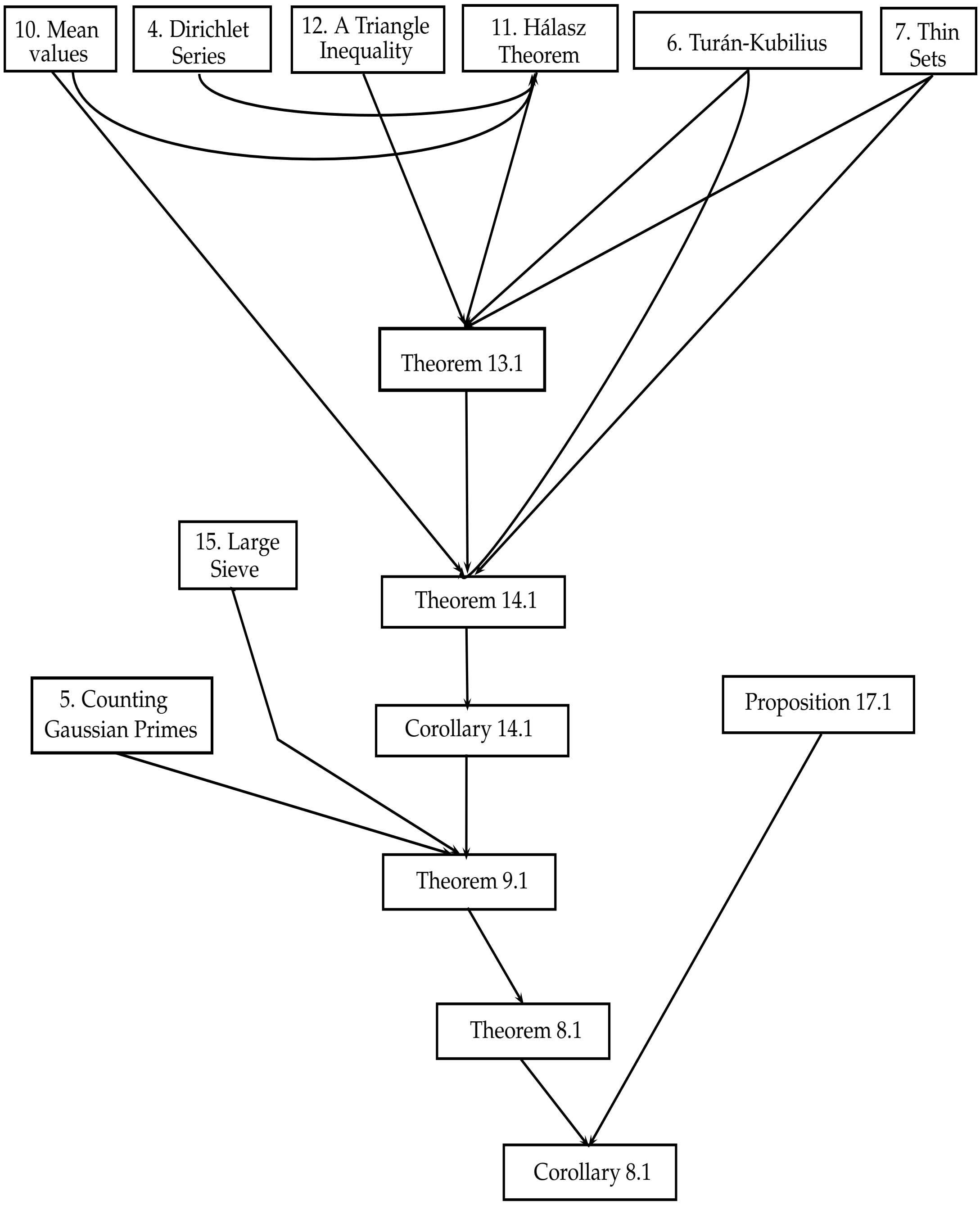
10. Mean values
4. Dirichlet Series
12. A Triangle Inequality
11. Hálasz Theorem
6. Turán-Kubilius
7. Thin Sets
Theorem 13.1
15. Large Sieve
Theorem 14.1
5. Counting Gaussian Primes
Corollary 14.1
Proposition 17.1
Theorem 9.1
Theorem 8.1
Corollary 8.1

Figure 2.1

10 Mean Values of Multiplicative Functions

Definition 10.1. Let f be a complex valued multiplicative function on $\mathcal{G}$. We say that f has a *mean value* if

$$\mathcal{M}(f) = \lim_{X \to +\infty} \frac{1}{X} \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} f(z) \tag{2.64}$$

exists. When this is so we call $\mathcal{M}(f)$ the mean value of f.

Here is a simple but fundamental example.

Proposition 10.1. *Let A be a finite subset of $\mathcal{P}[i]$ and let f be a totally multiplicative function on $\mathcal{G}$ such that $f(\pi) = 1$ when $\pi \notin A$. Then $\mathcal{M}(f)$ exists and it is given by*

$$\mathcal{M}(f) = \alpha_0 \prod_{\pi \in A} \left(1 + \frac{f(\pi) - 1}{\mathcal{N}(\pi)}\right) , \tag{2.65}$$

where α_0 is as in (2.10).

Proof. To see this, let $h = \mu * f$. Then $h(\pi^k) = f(\pi^k) - f(\pi^{k-1})$ for all π in $\mathcal{P}[i]$ and $k \geq 1$. It follows that $h(\pi) = f(\pi) - 1$ when $\pi \in A$ and $h(\pi) = 0$ for all other π. Moreover, $h(\pi^k) = 0$ for all $\pi \in \mathcal{P}[i]$ when $k \geq 2$. Since h is multiplicative, we conclude that $h(z) = 0$ when z lies outside the *finite subset* $F(A)$ of $\mathcal{G}^*$ consisting of all square-free $z \in \mathcal{G}^*$ satisfying $\pi | z \implies \pi \in A$. The Möbius inversion formula (2.6) gives

$$f(z) = \sum_{\substack{y|z,\\ y\in\mathcal{G}^*.}} h(y) \tag{2.66}$$

for all z in $\mathcal{G}$. For a given real number $X \geq 1$ we sum both sides of this relation over z in $\mathcal{G}^*$ with $\mathcal{N}(z) \leq X$. A familiar interchange of summations now tells us that

$$\sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\leq X.}} \sum_{\substack{y|z,\\ y\in\mathcal{G}^*.}} h(y) = \sum_{\substack{y\in\mathcal{G}^*,\\ \mathcal{N}(y)\leq X.}} h(y) \sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\leq X,\\ y|z.}} 1\ . \tag{2.67}$$

The inner sum in the right hand term of the above relation is the same as $\mathcal{L}\left(\frac{X}{\mathcal{N}(y)}\right)$. We then obtain

$$\sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\leq X.}} f(z) = \sum_{\substack{y\in\mathcal{G}^*,\\ \mathcal{N}(y)\leq X.}} h(y)\mathcal{L}\left(\frac{X}{\mathcal{N}(y)}\right) = \sum_{y\in F(A)} h(y)\mathcal{L}\left(\frac{X}{\mathcal{N}(y)}\right)\ , \tag{2.68}$$

for all large enough X. The estimate (2.10) shows that $\frac{1}{X}\mathcal{L}\left(\frac{X}{\mathcal{N}(y)}\right)$ tends to $\frac{\alpha_0}{\mathcal{N}(y)}$, for a given y as X tends to $+\infty$. Thus on dividing the above relation throughout by X and passing to the limit, we conclude that

$$\mathcal{M}(f) \ = \ \alpha_0 \sum_{y\in F(A)} \frac{h(y)}{\mathcal{N}(y)} = \alpha_0 \prod_{\pi\in A}\left(1 + \frac{h(\pi)}{\mathcal{N}(\pi)}\right)\ , \tag{2.69}$$

which gives (2.65) since $h(\pi) = f(\pi) - 1$ for $\pi \in A$. □

11 Hálasz's Theorem

The following theorem is an analogue for the Gaussian integers of the central part of the well-known theorem of G. Hálasz [16] on mean values of multiplicative functions on the $\mathbf{N}^*$ taking values in the closed unit disc..

Theorem 11.1. *Let f be a multiplicative function on $\mathcal{G}$ satisfying $|f(z)| \leq 1$ for all z in $\mathcal{G}$. If for each $t \in \mathbf{R}$ the series of positive terms*

$$\sum_{\pi \in \mathcal{P}[i]} \frac{1 - \mathrm{Re}\,(f(\pi)\mathcal{N}(\pi)^{-it})}{\mathcal{N}(\pi)} \tag{2.70}$$

diverges then f has a mean value and it is 0.

Our account of the proof of Theorem 11.1 is based on the proof of Hálasz's theorem in the classical setting given by G. Tenenbaum on pages 337 to 343 of [43]. The proof comprises three main steps which are detailed in the following five subsections. Unless otherwise stated, f shall denote a given multiplicative function satisfying the hypotheses of the theorem. For any real number X, let $A(X)$ denote the sum

$$A(X) = \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} f(z) \tag{2.71}$$

so that $A(X) = 0$ when $X < 1$.

The assertion that will be proved is $\limsup_{X \to +\infty} \frac{|A(X)|}{X} = 0$, from which the conclusion of the theorem follows.

11.1 Passage to a Mean

We shall show here that the following inequality holds for all $X \geq e^2$.

$$A(X) \ll \frac{X}{\log X} \int_1^X \frac{|A(t)|}{t^2}\, dt + \frac{X \log\log X}{\log X}\ . \tag{2.72}$$

This inequality is in fact an averaged form of the following simple identity.

$$A(t)\log t \; = \; \sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le t.}} f(z)\log\mathcal{N}(z) \; + \; \sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le t.}} f(z)\log\left(\frac{t}{\mathcal{N}(z)}\right)\ . \tag{2.73}$$

The identity (2.73) is an immediate consequence of the additivity of the logarithm and is valid for all $t > 0$. Let us first show that for any $X \ge 1$ and all t in $(0, 2X]$, the identity (2.73) implies the inequality

$$A(t)\log t \; \ll \; \sum_{\pi\in\mathcal{P}[i]} \left| A\left(\frac{t}{\mathcal{N}(\pi)}\right)\right| \log\mathcal{N}(\pi) \; + \; X\ , \tag{2.74}$$

where the sum on the right hand side is finite because $A(u) = 0$ when $u < 1$.

We begin by remarking that the second sum on the right hand side of (2.73) is majorised by X. Indeed, the absolute value of this term does not exceed

$$\sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le t.}} \log\left(\frac{t}{\mathcal{N}(z)}\right) = \sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le t.}} \int_{\mathcal{N}(z)}^t \frac{du}{u} \; = \int_1^t \frac{\mathcal{L}(u)}{u}\, du \; \ll t, \tag{2.75}$$

where the last estimate uses (2.10). Our assertion now follows since $t \le 2X$.

Let us recall that $\mathcal{S}[i]$ denotes the set of Gaussian integers of the form π^k for a π in $\mathcal{P}[i]$ and an integer $k \ge 1$. Then for all $z \in \mathcal{G}^*$ we have

$$\log \mathcal{N}(z) = \sum_{\substack{s\in\mathcal{S}[i],\\ s||z.}} \log \mathcal{N}(s) \ , \tag{2.76}$$

where $s||z$ stands for $s|z$ and $(s, \frac{z}{s}) = 1$. Inserting this into the first sum on the right hand side of (2.73) we see, after an interchange of summations, that this sum is the same as

$$\sum_{s\in\mathcal{S}[i]} \log \mathcal{N}(s) \sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le t,\\ s||z.}} f(z) = \sum_{s\in\mathcal{S}[i]} f(s) \log \mathcal{N}(s) \sum_{\substack{x\in\mathcal{G}^*,\\ \mathcal{N}(x)\le \frac{t}{\mathcal{N}(s)},\\ (s,x)=1.}} f(x) \ , \tag{2.77}$$

by the multiplicativity of f. Now if $s = \pi^k$ then we have

$$A\left(\frac{t}{\mathcal{N}(s)}\right) = \sum_{\substack{x\in\mathcal{G}^*,\\ \mathcal{N}(x)\le \frac{t}{\mathcal{N}(s)},\\ (s,x)=1.}} f(x) + \sum_{\substack{x\in\mathcal{G}^*,\\ \mathcal{N}(x)\le \frac{t}{\mathcal{N}(s)},\\ \pi|x.}} f(x), \tag{2.78}$$

where the absolute value of the second sum does not exceed $\mathcal{L}\left(\frac{t}{\mathcal{N}(\pi s)}\right)$. Thus on combining the two preceding relations with an application of the triangle inequality we infer that the first sum on the right hand side of (2.73) is majorised by

$$\sum_{s\in\mathcal{S}[i]} \left|A\left(\frac{t}{\mathcal{N}(s)}\right)\right| \log \mathcal{N}(s) \ + \sum_{\substack{\pi\in\mathcal{P}[i],\\ k\ge 1.}} \log \mathcal{N}(\pi^k) \mathcal{L}\left(\frac{t}{\mathcal{N}(\pi^{k+1})}\right) \ . \tag{2.79}$$

Estimating trivially the contribution to the first sum in (2.79) from those s that *do not* belong to $\mathcal{P}[i]$, we see that this contribution does not exceed

$$\sum_{\substack{\pi \in \mathcal{P}[i], \\ k \geq 1.}} \log \mathcal{N}(\pi^{k+1}) \mathcal{L}\left(\frac{t}{\mathcal{N}(\pi^{k+1})}\right) \ll t \sum_{\substack{\pi \in \mathcal{P}[i], \\ k \geq 1.}} \frac{\log \mathcal{N}(\pi^{k+1})}{\mathcal{N}(\pi^{k+1})} \ll X \ , \tag{2.80}$$

using (2.10), and since $t \leq 2X$ and the second sum in (2.80) is convergent. We then conclude that the first sum on the right hand side of (2.73) is majorised by

$$\sum_{\pi \in \mathcal{P}[i]} \left| A\left(\frac{t}{\mathcal{N}(\pi)}\right) \right| \log \mathcal{N}(\pi) \ + \ X \ . \tag{2.81}$$

On now recalling that the second sum on the right hand side of (2.73) is majorised by X, we obtain (2.74) from (2.73).

It remains to deduce (2.72) from (2.74). This is done by means of an averaging argument. Thus, let us set $Y = X/\log X$. Then for any t in the interval $I = (X - Y, X + Y]$ we write

$$A(X)\log X - A(t)\log t = (A(X) - A(t))\log X + A(t)(\log X - \log t) \ . \tag{2.82}$$

Since $|f(z)| \leq 1$, an application of the triangle inequality together with (2.10) shows that the first term on the right hand side of the preceding relation is majorised by $Y \log X$. Since $X \geq e^2$, we have $\log(X/t) \leq 2$ for $t \in I$ and hence the second term on the right hand side of (2.82) is majorised by X. Therefore we see that

$$|A(X)| \log X \leq |A(t)| \log t + O(X) \tag{2.83}$$

for all t in the interval I. We now integrate both sides of this relation with t varying over this interval. Writing $\chi_I(t)$ for the characteristic function of I we then obtain from (2.83) that

$$|A(X)|\log X \;\leq\; \frac{1}{2Y}\int_{\mathbf{R}} \chi_I(t)|A(t)|\log t\, dt + O(X)\;. \tag{2.84}$$

On using (2.74) to bound $|A(t)|\log t$ in the integral on the right hand side of (2.84) we get

$$|A(X)|\log X \;\ll\; \frac{1}{Y}\int_{\mathbf{R}} \sum_{\pi\in\mathcal{P}[i]} \chi_I(t)\log\mathcal{N}(\pi)\left|A\left(\frac{t}{\mathcal{N}(\pi)}\right)\right|\, dt \;+X. \tag{2.85}$$

By means of the change of variable $t \mapsto N(\pi)t$ and a rearrangment of terms we then deduce that the integral on the right hand side of (2.85) is the same as

$$\int_{\mathbf{R}} |A(t)| \sum_{\pi\in\mathcal{P}[i]} \chi_I\left(\mathcal{N}(\pi)t\right)\mathcal{N}(\pi)\log\mathcal{N}(\pi)\, dt. \tag{2.86}$$

We now set $Z = X/(\log X)^2$ and bound the contribution to the integral (2.86) from $t < Z$. To this end, note that for any t in $\mathbf{R}$ we have

$$\sum_{\pi\in\mathcal{P}[i]} \chi_I\left(\mathcal{N}(\pi)t\right)\mathcal{N}(\pi)\log\mathcal{N}(\pi) \;=\; \sum_{\substack{\pi\in\mathcal{P}[i],\\ \frac{X-Y}{t}<\mathcal{N}(\pi)\leq\frac{X+Y}{t}\cdot}} \mathcal{N}(\pi)\log\mathcal{N}(\pi)\;. \tag{2.87}$$

When $t < Z$, we have $2Y/t \geq 2$, since $X \geq e^2$. The Brun-Titchmarsh theorem now shows that the right hand side of (2.87) is majorised by

$$\frac{X+Y}{t}\log\left(\frac{X+Y}{t}\right)\frac{\frac{4Y}{t}}{\log\left(\frac{2Y}{t}\right)}=\frac{4(X+Y)Y}{t^2}\left(\frac{\log\left(\frac{X+Y}{t}\right)}{\log\left(\frac{2Y}{t}\right)}\right)\leq\frac{24XY}{t^2}\ , \qquad (2.88)$$

since $Y \leq X$ and since the expression in the brackets on the right hand side of (2.88) does not exceed 3 when $t < Z$. Consequently, the contribution to the integral (2.86) from $t < Z$ is majorised by

$$XY\int_{-\infty}^{Z}\frac{|A(t)|}{t^2}\,dt\ \leq\ XY\int_{1}^{X}\frac{|A(t)|}{t^2}\,dt\ , \qquad (2.89)$$

since $A(t) = 0$ when $t < 1$ and $Z \leq X$. Turning to the contribution to the integral (2.86) from $t \geq Z$, we see that after an interchange of the sum and the integral it can be written as

$$\sum_{\pi\in\mathcal{P}[i]}\mathcal{N}(\pi)\log\mathcal{N}(\pi)\int_{Z}^{+\infty}|A(t)|\,\chi_I\left(\mathcal{N}(\pi)t\right)\,dt. \qquad (2.90)$$

The integral in (2.90) is 0 when $\mathcal{N}(\pi) > (X+Y)/Z$, since then $\chi_I\left(\mathcal{N}(\pi)t\right) = 0$ for $t \geq Z$. When $\mathcal{N}(\pi) \leq (X+Y)/Z$, we estimate this integral trivially as

$$\int_{Z}^{+\infty}|A(t)|\,\chi_I\left(\mathcal{N}(\pi)t\right)\,dt \ll \int_{\frac{X-Y}{\mathcal{N}(\pi)}}^{\frac{X+Y}{\mathcal{N}(\pi)}} t\,dt \ll \frac{XY}{\mathcal{N}(\pi)^2} \qquad (2.91)$$

using (2.10). We conclude that the contribution to the integral (2.86) from $t \geq Z$ is majorised by

$$XY\sum_{\substack{\pi\in\mathcal{P}[i],\\ \mathcal{N}(\pi)\leq\frac{X+Y}{Z}}}\frac{\log\mathcal{N}(\pi)}{\mathcal{N}(\pi)} \ll XY\log\left(\frac{X+Y}{Z}\right) \ll XY\log\log X. \qquad (2.92)$$

In summary, we have verified that the integral (2.86) is majorised by

$$XY \int_1^X \frac{|A(t)|}{t^2}\, dt \; + XY \log\log X \; .$$

We now obtain (2.72) on combining this conclusion with (2.85) and dividing throughout the resulting relation by $\log X$.

11.2 Exploiting the Slow Growth of the Logarithm

For any $X \geq 1$ we shall hereafter write $B(X)$ to denote the sum

$$\sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X.}} f(z) \log \mathcal{N}(z) \; . \tag{2.93}$$

In this subsection we shall use the inequality (2.72) to show that for any θ in $(0, 1]$ we have

$$\limsup_{X \to +\infty} \frac{A(X)}{X} \; \ll \; \frac{1}{\theta} \left(\limsup_{X \to +\infty} \frac{1}{\log^2 X} \int_1^X \frac{|B(t)|}{t^2}\, dt \right) \; + \; \theta. \tag{2.94}$$

Thus, let θ denote a real number in $(0, 1]$ and for a given $X \geq e^2$ we write Y to denote X^θ. Then we have

$$\int_1^X \frac{|A(t)|}{t^2}\, dt \; \leq \; \int_1^Y \frac{|A(t)|}{t^2}\, dt + \frac{1}{\log Y} \int_Y^X \frac{|A(t)| \log t}{t^2}\, dt \; . \tag{2.95}$$

Since $A(t) \ll t$ by (2.10), the first term on the right hand side of the above relation is majorised by $\log Y$. On combining this remark with (2.95) and (2.72) we see that

$$\frac{A(X)}{X} \ll \theta + \frac{1}{\theta(\log X)^2} \int_Y^X \frac{|A(t)| \log t}{t^2}\, dt + \frac{\log\log X}{\log X}\,. \tag{2.96}$$

It follows from (2.73) and (2.75) that we have

$$|A(t)| \log t \ll |B(t)| + t \tag{2.97}$$

for all $t > 0$. Extending the range of integration in the integral on the right hand side of (2.96) to $[1, X]$ and inserting (2.97) into the resulting integral we obtain

$$\frac{A(X)}{X} \ll \theta + \frac{1}{\theta \log^2 X} \int_1^X \frac{|B(t)|}{t^2}\, dt + \frac{1}{\theta \log X} + \frac{\log\log X}{\log X}\,, \tag{2.98}$$

from which (2.94) follows on taking the limsup as $X \to +\infty$ of both sides.

11.3 Plancherel Theorem and Cauchy-Schwarz

In this subsection we will obtain, for any $\sigma > 1$, an upper bound for the integral

$$\int_1^{+\infty} \frac{|B(t)|}{t^{2\sigma}}\, dt \tag{2.99}$$

by means of the Plancherel formula from the theory of the Fourier transform. Note that the estimate $|B(t)| \ll t \log t$ shows that the above integral is convergent for all $\sigma > 1$. Let us write e_+^u to denote the function on $\mathbf{R}$ which is 0 for $u < 0$ and is e^u for $u \geq 0$. Then our starting point is the observation that

$$\int_1^{+\infty} \frac{B(t)}{t^{2\sigma}}\, dt = \int_{\mathbf{R}} B(e^u) e_+^{-\sigma u} e_+^{(1-\sigma)u}\, du \tag{2.100}$$

as follows from the change of variable $t \mapsto e^u$ in the integral on the left hand side.

Further, for any $t \in \mathbf{R}$ and all $\sigma > 1$ we have

$$\int_{\mathbf{R}} B(e^u) e_+^{-\sigma u} e^{-itu} du \;=\; \frac{-F'(\sigma + it)}{\sigma + it}\;, \tag{2.101}$$

where $F(s)$ is the Dirichlet series associated to f (see Section 4). Indeed, on interchanging the sum in the definition of $B(u)$ (see (2.93)) with the integral on the left hand side of (2.101), we see this integral is the same as

$$\sum_{z \in \mathcal{G}^*} f(z) \log \mathcal{N}(z) \int_{\log \mathcal{N}(z)}^{+\infty} e^{-(\sigma+it)u}\, du \;=\; \frac{1}{\sigma + it} \sum_{z \in \mathcal{G}^*} \frac{f(z) \log \mathcal{N}(z)}{N(z)^{\sigma+it}}\;, \tag{2.102}$$

which is the right hand side of (2.101). The required interchange of sum and integral is justified by the fact that

$$\int_0^{+\infty} |B(e^u)| e^{-\sigma u}\, du \tag{2.103}$$

converges, since $\sigma > 1$ and $B(u) \ll u \log u$. Thus, if for any integrable function $u \mapsto \phi(u)$ on $\mathbf{R}$, we define its Fourier transform to be the function $t \mapsto \widehat{\phi}(t)$ given by

$$\widehat{\phi}(t) = \int_{\mathbf{R}} \phi(u) e^{-itu}\, du \tag{2.104}$$

then (2.101) expresses the fact that, for a given $\sigma > 1$, the Fourier transform of the function $u \mapsto B(e^u) e_+^{-\sigma u}$ is the right hand side of (2.101). Further, the Fourier transform of the function $u \mapsto e_+^{(1-\sigma)u}$ is $t \mapsto (\sigma + it - 1)^{-1}$. Let us recall that the Plancherel formula tells us that

$$\int_{\mathbf{R}} \phi(u)\overline{\psi}(u)\, du \ = \ \frac{1}{2\pi} \int_{\mathbf{R}} \widehat{\phi}(t)\overline{\widehat{\psi}}(t)\ dt \tag{2.105}$$

for any square integrable complex valued functions ϕ and ψ on $\mathbf{R}$. Since, for $\sigma > 1$, the functions $\phi(u) = B(e^u)e_+^{-\sigma u}$ and $\psi(u) = e_+^{(1-\sigma)u}$ are bounded integrable functions on $\mathbf{R}$, they are in particular square-integrable on $\mathbf{R}$. Therefore, on applying (2.105) and recalling (2.100) we deduce that

$$\int_1^{+\infty} \frac{B(t)}{t^{2\sigma}}\, dt \ = \ \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\sigma} \frac{-F'(s)}{s(\overline{s}-1)}\, ds\ , \tag{2.106}$$

for any given $\sigma > 1$. Finally, on writing $F' = F \cdot \frac{F'}{F}$ and applying the triangle inequality together with the Cauchy-Schwarz inequality we obtain from (2.106) for all $\sigma > 1$ the bound

$$\int_1^{+\infty} \frac{|B(t)|}{t^{2\sigma}}\, dt \ \leq \ \frac{1}{2\pi} \left(\int_{\mathrm{Re}(s)=\sigma} \left| \frac{F(s)}{s-1} \right|^2 dt \right)^{\frac{1}{2}} \left(\int_{\mathrm{Re}(s)=\sigma} \left| \frac{\frac{F'}{F}(s)}{s} \right|^2 \ dt \right)^{\frac{1}{2}} \ , \tag{2.107}$$

which lies at the heart of Hálasz's method.

11.4 An application of Montgomery's Lemma

We shall show here that for any σ satisfying $1 < \sigma \leq 2$ we have the bound

$$\int_{\mathrm{Re}(s)=\sigma} \left| \frac{\frac{F'}{F}(s)}{s} \right|^2 dt \ \ll \ \frac{1}{(\sigma-1)}\ . \tag{2.108}$$

We will prove (2.108) with the aid of the following proposition, which relies on a well-known lemma due to H. Montgomery. We recall the notion of domination in the context of Dirichlet series introduced in Section 4.

Proposition 11.1. *Let $C(s)$ and $D(s)$ be Dirichlet series that are normally convergent in every closed half plane in $\sigma > 1$ and suppose that the following conditions hold.*

(i) $D(s)$ dominates $C(s)$.

(ii) $|(s-1)D(s)| \leq M$ for $1 \leq \sigma \leq 2$, $|t| \leq \frac{1}{2}$ and a positive real M.

When $1 < \sigma \leq 2$ we have the inequality

$$\int_{\mathrm{Re}(s)=\sigma} \left| \frac{C(s)}{s} \right|^2 dt \ll \frac{1}{(\sigma - 1)} , \tag{2.109}$$

where the implied constant depends only on M.

Proof. Let I denote the interval $(-\frac{1}{2}, \frac{1}{2}]$. Then the left hand side of (2.109) is the same as

$$\sum_{k \in \mathbf{Z}} \int_{I+k} \left| \frac{C(\sigma + it)}{\sigma + it} \right|^2 dt \leq \sum_{k \in \mathbf{Z}} \frac{2}{1+k^2} \int_{I+k} |C(\sigma + it)|^2 dt , \tag{2.110}$$

on noting that for any integer k we have $|\sigma + it|^2 \geq \frac{1+k^2}{2}$ when $t \in I + k$ and $\sigma \geq 1$. For any integer k we also have

$$\int_{I+k} |C(\sigma + it)|^2 dt = \int_I \left| \sum_{z \in \mathcal{G}^*} \frac{c(z)\mathcal{N}(z)^{-ik}}{\mathcal{N}(z)^{\sigma+it}} \right|^2 dt = \int_I \left| \sum_{n \geq 1} \frac{n^{-ik} h(n)}{n^{\sigma + it}} \right|^2 dt, \tag{2.111}$$

where $h(n) = \sum c(z)$ with $\mathcal{N}(z) = n$. Thus if $j(n) = \sum d(z)$ with $\mathcal{N}(z) = n$, then $|n^{-ik}h(n)| \leq j(n)$ for all $n \geq 1$, by the condition (i) and the triangle inequality. It now follows from Montgomery's lemma (see Lemma 6.1, page 338 of [43]) that for any $k \in \mathbf{Z}$ the last term in (2.111) does not exceed

$$3\int_I \left|\sum_{n\geq 1} \frac{j(n)}{n^{\sigma+it}}\right|^2 dt \;=\; 3\int_I \left|\sum_{z\in\mathcal{G}^*} \frac{d(z)}{\mathcal{N}(z)^{\sigma+it}}\right|^2 dt \;=\; 3\int_I |D(\sigma+it)|^2\, dt\,. \qquad (2.112)$$

Finally, the condition (ii) tells us that the last term in (2.112) does not exceed

$$\int_I \frac{3M^2\, dt}{(\sigma-1)^2+t^2} \leq \int_{\mathbf{R}} \frac{3M^2\, dt}{(\sigma-1)^2+t^2} \;=\; \frac{3\pi M^2}{(\sigma-1)}\,. \qquad (2.113)$$

The inequality (2.109) now results on combining (2.110) through (2.113). □

To prepare for an application of the preceding proposition let us set, for each $\pi \in \mathcal{P}[i]$ and $s = \sigma + it$ with $\sigma > 0$,

$$F_\pi(s) = \sum_{k\geq 1} \frac{f(\pi^k)}{\mathcal{N}(\pi^k)^s}\,. \qquad (2.114)$$

Then since $\mathcal{N}(\pi) \geq 5$ when $\pi \neq 1+i$, we have for all such $\pi \in \mathcal{P}[i]$ the estimate

$$|F_\pi(s)| \leq \sum_{k\geq 1} \frac{1}{\mathcal{N}(\pi)^{k\sigma}} \;\leq\; \frac{1}{\mathcal{N}(\pi)^\sigma - 1} \;<\; 1 \qquad (2.115)$$

for any $\sigma \geq \frac{1}{2}$ and all $t \in \mathbf{R}$. If for any $s = \sigma + it$ with $\sigma \geq 1$ we write $\Lambda(s)$ to denote the (properly) oriented circle of radius $\frac{1}{2}$ centered at s, then we have

$$F'_\pi(s) \;=\; \frac{1}{2\pi i} \int_{\Lambda(s)} \frac{F_\pi(u)}{(u-s)^2}\, du\,, \qquad (2.116)$$

and an application of the triangle inequality together with (2.115) then gives

$$|F'_\pi(s)| \;\le\; \frac{2}{(\mathcal{N}(\pi)^{\sigma-\frac{1}{2}}-1)} \tag{2.117}$$

for all $\sigma \ge 1$ and $t \in \mathbf{R}$. Further, by logarithmic differentiation of the Euler product formula (2.23) we get

$$\frac{F'(s)}{F(s)} = \sum_{\pi\in\mathcal{P}[i]} \frac{F'_\pi(s)}{1+F_\pi(s)}\ , \tag{2.118}$$

where the series on the right converges normally in any closed half plane in $\sigma > 1$. Let us introduce the function $H(s)$ defined by

$$H(s) \;=\; \sum_{\substack{\pi\in\mathcal{P}[i],\\ \pi\ne 1+i\ .}} \sum_{k\ge 2} \frac{f(\pi^k)\log\mathcal{N}(\pi^k)}{\mathcal{N}(\pi^k)^s} - \sum_{\substack{\pi\in\mathcal{P}[i],\\ \pi\ne 1+i\ .}} \frac{F_\pi(s)F'_\pi(s)}{1+F_\pi(s)}\ . \tag{2.119}$$

Then $H(s)$ is a holomorphic function in the open half plane $\sigma > 1$ and bounded on the closed half plane $\sigma \ge 1$. This follows on noting that by (2.115) and (2.117) we have

$$|H(s)| \ll \sum_{\substack{\pi\in\mathcal{P}[i],\\ \pi\ne 1+i\ .}} \sum_{k\ge 2} \frac{\log\mathcal{N}(\pi^k)}{\mathcal{N}(\pi^k)^\sigma} + \sum_{\substack{\pi\in\mathcal{P}[i],\\ \pi\ne 1+i\ .}} \frac{1}{\mathcal{N}(\pi)^{2\sigma}}\ , \tag{2.120}$$

and that the right hand side converges for $\sigma \ge 1$. Also, we get on subtracting (2.119) from (2.118) that

$$\frac{F'(s)}{F(s)} \;=\; \frac{F'_{1+i}(s)}{1+F_{1+i}(s)} \;+\; \sum_{\substack{\pi\in\mathcal{P}[i],\\ \pi\ne 1+i\ .}} \frac{f(\pi)\log\mathcal{N}(\pi)}{\mathcal{N}(\pi)^s} + H(s)\ , \tag{2.121}$$

with the series on the right hand side uniformly convergent in any half plane in $\sigma > 1$. Let us recall from Section 4 that if $G(s) = \sum_{z\in\mathcal{G}} \frac{1}{\mathcal{N}(z)^s}$ then we have

$$-\frac{G'(s)}{G(s)} \;=\; \sum_{\pi\in\mathcal{P}[i]}\sum_{k\geq 1}\frac{\log\mathcal{N}(\pi)}{\mathcal{N}(\pi^k)^s} \tag{2.122}$$

and that $|(s-1)\frac{G'(s)}{G(s)}|$ is bounded on the rectangle $1\leq\sigma\leq 4$ and $|t|\leq\frac{1}{2}$. Thus with $C(s)$ as the series on the right hand side of (2.121) and $D(s)$ as the left hand side of (2.122), we see the conditions of Proposition 11.1 are met. Consequently, this proposition gives

$$\int_{\mathrm{Re}(s)=\sigma}\frac{1}{|s|^2}\left|\sum_{\substack{\pi\in\mathcal{P}[i],\\ \pi\neq 1+i.}}\frac{f(\pi)\log\mathcal{N}(\pi)}{\mathcal{N}(\pi)^s}\right|^2 dt \;\ll\; \frac{1}{(\sigma-1)} \tag{2.123}$$

for any $1<\sigma\leq 2$. Finally, let us consider the first term on the right hand side of (2.121). Since $\mathcal{N}(1+i)=2$ we have

$$F_{1+i}(s) \;=\; \sum_{k\geq 1}\frac{f((1+i)^k)}{2^{ks}}\ . \tag{2.124}$$

Thus if we denote $\sum_{k\geq 1}\frac{1}{2^{ks}}$ by $G_{1+i}(s)$ then $-F_{1+i}(s)$ is dominated by $G_{1+i}(s)$. Since $|G_{1+i}(s)|<1$ for $\sigma>1$ we have $|F_{1+i}(s)|<1$ for $\sigma>1$ as well. Further, Lemma 4.1 tells us that

$$\frac{1}{1+F_{1+i}(s)} = \sum_{m\geq 0}(-F_{1+i}(s))^m \tag{2.125}$$

is a Dirichlet series that is normally convergent in any closed half plane in $\sigma>1$ and is dominated by

$$\frac{1}{1-G_{1+i}(s)} = \sum_{m\geq 0}(G_{1+i}(s))^m\ . \tag{2.126}$$

Also we have that

$$\frac{1}{1 - G_{1+i}(s)} = \frac{2^s - 1}{2^s - 2} \,. \tag{2.127}$$

Thus if we set $C(s)$ to be the left hand side of (2.125) and $D(s)$ to be the left hand side of (2.126) then we see conditions of Proposition 11.1 are met and this proposition yields the second inequality in

$$\int_{\mathrm{Re}(s)=\sigma} \left| \frac{F'_{1+i}(s)}{s(1 + F_{1+i}(s))} \right|^2 dt \ \ll \ \int_{\mathrm{Re}(s)=\sigma} \left| \frac{1}{s(1 + F_{1+i}(s))} \right|^2 dt \ll \frac{1}{(\sigma - 1)} \,, \tag{2.128}$$

where the first inequality follows on remarking that $F'_{1+i}(s)$ is bounded on $\sigma \geq 1$. Since $H(s)$ is bounded for $\sigma \geq 1$ we have

$$\int_{\mathrm{Re}(s)=\sigma} \left| \frac{H(s)}{s} \right|^2 dt \ \ll \ 1 \,. \tag{2.129}$$

The inequality (2.108) now follows from (2.121) together with the estimates (2.123), (2.128) and (2.129).

11.5 End of Proof

Let us recall for any $1 \leq \sigma \leq 2$ we have that $G(\sigma) \neq 0$ and that $(\sigma - 1)G(\sigma)$ is bounded. Moreover, we have that

$$|F(\sigma + it)| \leq G(\sigma) \quad \text{for all } \sigma > 1 \text{ and all } t \in \mathbf{R} \,. \tag{2.130}$$

We shall presently deduce from the hypothesis that the series (2.70) diverges for all

$t \in \mathbf{R}$ that, given any $T \geq 0$ and any $\epsilon > 0$, there is a $\sigma_0 = \sigma_0(\epsilon, T)$ such that

$$\left|\frac{F(\sigma+it)}{G(\sigma)}\right| \leq \epsilon \text{ for all } 1 < \sigma \leq \sigma_0 \text{ and } |t| \leq T\,. \tag{2.131}$$

Let us first detail how the proof of Theorem 11.1 may be completed once (2.131) is verified. Indeed, given $\epsilon > 0$ we set $T = \frac{1}{\epsilon}$ and choose σ with $1 < \sigma \leq \sigma_0$. Then we get using (2.131) and (2.130) that

$$\int_{\mathrm{Re}(s)=\sigma} \left|\frac{F(s)}{(s-1)G(\sigma)}\right|^2 dt \;\leq\; \epsilon \int_{|t|\leq T} \frac{dt}{|s-1|^2} \;+\; \int_{|t|>T} \frac{dt}{|s-1|^2}\,. \tag{2.132}$$

Since $|s-1|^2 = (\sigma-1)^2 + t^2 \geq t^2$, the right hand side of (2.132) does not exceed

$$\epsilon \int_{\mathbf{R}} \frac{dt}{(\sigma-1)^2+t^2} \;+\; \int_{|t|>T} \frac{dt}{t^2} \;=\; \frac{\pi\epsilon}{(\sigma-1)} + 2\epsilon. \tag{2.133}$$

When $\sigma \leq 2$ we conclude from (2.133) that the left hand side of (2.132) is majorised by $\frac{\epsilon}{\sigma-1}$. Since $(\sigma-1)G(\sigma)$ is bounded for $1 \leq \sigma \leq 2$ we then deduce that

$$\int_{\mathrm{Re}(s)=\sigma} \left|\frac{F(s)}{s-1}\right|^2 dt \;\ll\; \frac{\epsilon}{(\sigma-1)^3} \tag{2.134}$$

for $1 < \sigma \leq \min(\sigma_0, 2)$. On combining (2.134) with (2.108) and (2.107) we obtain that

$$\int_1^{+\infty} \frac{|B(t)|}{t^{2\sigma}}\, dt \;\ll\; \frac{\sqrt{\epsilon}}{(\sigma-1)^2} \tag{2.135}$$

for $1 < \sigma \leq \min(\sigma_0, 2)$. For any X large enough so that $\sigma = 1 + \frac{1}{\log X}$ satisfies these conditions we then have that

$$\int_1^X \frac{|B(t)|}{t^2}\, dt \le e^2 \int_1^{+\infty} \frac{|B(t)|}{t^{2\sigma}}\, dt \ \ll \log^2 X \sqrt{\epsilon}\,, \tag{2.136}$$

where the first inequality follows on noting that $t^2 \ge e^{-2} t^{2\sigma}$ for $1 \le t \le X$. On dividing throughout the above relation by $\log^2 X$ and taking limsup as $X \to +\infty$, and recalling that $\epsilon > 0$ is arbitrary, we conclude that

$$\limsup_{x \to +\infty} \frac{1}{\log^2 X} \int_1^X \frac{|B(t)|}{t^2}\, dt \ = \ 0\,. \tag{2.137}$$

Finally, we substitute the above conclusion into (2.94) and recall that θ in that relation is an aribitrary real number in $(0, 1]$. It then follows that $\limsup_{x \to +\infty} \frac{|A(X)|}{X} = 0$, as was to be shown.

We shall now prove (2.131). To this end, let f be any multiplicative function on $\mathcal{G}$ satisfying $|f(z)| \le 1$ for all $z \in \mathcal{G}$ and $F(s)$ be the associated Dirichlet series. Also, for any $\sigma > 1$ and $\pi \in \mathcal{P}[i]$, let us set

$$u_\pi(\sigma) = \frac{\mu * f(\pi)}{\mathcal{N}(\pi)^\sigma} \ \text{ and } \ v_\pi(\sigma) = \sum_{k \ge 2} \frac{\mu * f(\pi^k)}{\mathcal{N}(\pi^k)^\sigma}\,. \tag{2.138}$$

Note that $\mu * f(\pi^k) = f(\pi^k) - f(\pi^{k-1})$, for any $k \ge 1$. In particular, we have

$$u_\pi(\sigma) = \frac{f(\pi) - 1}{\mathcal{N}(\pi)^\sigma}\,. \tag{2.139}$$

The Euler product formula for the Dirichlet series associated to $\mu * f$ gives us

$$\frac{F(\sigma)}{G(\sigma)} = \prod_{\pi \in \mathcal{P}[i]} \left(1 + u_\pi(\sigma) + v_\pi(\sigma)\right)\,, \tag{2.140}$$

where the product on the right hand side is absolutely convergent for all $\sigma > 1$, as follows from the estimates

$$|u_\pi(\sigma)| \le \frac{2}{\mathcal{N}(\pi)^\sigma} \quad \text{and} \quad |v_\pi(\sigma)| \le \frac{4}{\mathcal{N}(\pi)^{2\sigma}} \ . \tag{2.141}$$

It is also immediate from (2.141) that when $\pi \neq 1+i$ we have $|u_\pi(\sigma)| + |v_\pi(\sigma)| \le \frac{2}{3}$ for all $\sigma \ge 1$, since $\mathcal{N}(\pi) \ge 5$ for such π.

For any complex number $|s| \le \frac{2}{3}$ we have the inequality $|\log(1+s) - s| \le 3|s|^2$, obtained from the Taylor expansion of $s \mapsto \log(1+s)$ about $s = 0$. On passing to the exponential and using $|\exp(z)| = \exp(\mathrm{Re}(z)) \le \exp(|z|)$, valid for any complex number z, we then obtain

$$|1+s| \le \exp(\mathrm{Re}(s)) \exp(3|s|^2) \quad \text{when } |s| \le \frac{2}{3} \ . \tag{2.142}$$

Applying this with $s = u_\pi(\sigma) + v_\pi(\sigma)$ we see that for any $\sigma \ge 1$ and $\pi \neq 1+i$ we have

$$|1 + u_\pi(\sigma) + v_\pi(\sigma)| \le \exp(\mathrm{Re}(u_\pi(\sigma))) \exp\left(\frac{32}{\mathcal{N}(\pi)^2}\right) \ , \tag{2.143}$$

since for such σ and π, the triangle inequality and (2.141) give

$$\mathrm{Re}(v_\pi(\sigma)) + 3|u_\pi(\sigma) + v_\pi(\sigma)|^2 \le \frac{32}{\mathcal{N}(\pi)^{2\sigma}} \ . \tag{2.144}$$

For $\pi = 1+i$ and any $\sigma \ge 1$ we easily verify that

$$1 + |u_{1+i}(\sigma)| + |v_{1+i}(\sigma)| \ \le \ 3e \exp(\mathrm{Re}(u_{1+i}(\sigma))) \ . \tag{2.145}$$

From (2.143) and (2.145) we then conclude that

$$\left| \prod_{\pi \in \mathcal{P}[i]} (1 + u_\pi(\sigma) + v_\pi(\sigma)) \right| \ll \prod_{\pi \in \mathcal{P}[i]} \exp(\mathrm{Re}(u_\pi(\sigma))) \tag{2.146}$$

for all $\sigma > 1$. For such σ it now follows from (2.146) together with (2.139) and (2.140) that

$$\left| \frac{F(\sigma)}{G(\sigma)} \right| \ll \exp\left(- \sum_{\pi \in \mathcal{P}[i]} \frac{1 - \mathrm{Re}(f(\pi))}{\mathcal{N}(\pi)^\sigma} \right) . \tag{2.147}$$

For a given multiplicative function f and a $t \in \mathbf{R}$ we apply (2.147) to the multiplicative function $h(z) = f(z)\mathcal{N}(z)^{-it}$. If $H(s)$ is the Dirichlet series associated to h, then $H(\sigma) = F(\sigma + it)$ and we then conclude that

$$\left| \frac{F(\sigma + it)}{G(\sigma)} \right| \ll \exp\left(- \sum_{\pi \in \mathcal{P}[i]} \frac{1 - \mathrm{Re}(f(\pi)\mathcal{N}(\pi)^{-it})}{\mathcal{N}(\pi)^\sigma} \right) \tag{2.148}$$

for all $t \in \mathbf{R}$ and all $\sigma > 1$. For an f that satisfies (2.70), let us denote the right hand side by $\phi_\sigma(t)$. Then for each σ, the functions $\phi_\sigma(t)$ are continuous on $\mathbf{R}$ and for each $t \in \mathbf{R}$, we have that $\phi_\sigma(t)$ decreases to 0. By the classical theorem of Dini (see Theorem 7.2.2., page 135 of [6]), the family of functions ϕ_σ converges to 0 uniformly on compact subsets of $\mathbf{R}$. Applying this conclusion to the compact interval $[-T, T]$ and using (2.148), we obtain (2.131).

12 A Triangle Inequality

Let $\mathbf{U}$ denote the set of complex numbers with absolute value 1. For any $s \in \mathbf{U}$ we set $\eta(s) = +\sqrt{1 - \mathrm{Re}(s)}$. Then we have the inequality

$$\eta(uw) \le \eta(u) + \eta(w) \tag{2.149}$$

for all u, w in $\mathbf{U}$. Indeed, when $|s| = 1$ we have $\sqrt{2}\eta(s) = |1 - s|$ so that (2.149) follows from the triangle inequality

$$|1 - uw| = |\overline{u} - w| \le |1 - u| + |1 - w|. \tag{2.150}$$

For any u, v and w in $\mathbf{U}$ we have $\eta(u\overline{w}) = \eta(u\overline{v}v\overline{w})$ and an application of (2.149) gives

$$\eta(u\overline{v}v\overline{w}) \le \eta(u\overline{v}) + \eta(v\overline{w}) \ . \tag{2.151}$$

Thus if we define $K(u, w) = \eta(u\overline{w})$ for any u, w in $\mathbf{U}$, we have the inequality

$$K(u, w) \le K(u, v) + K(v, w) \tag{2.152}$$

for all u, v, w in $\mathbf{U}$. Further, we evidently have the relations

$$K(u, v) = K(v, u) \ \text{ and } \ K(u, v) = K(uw, wv) \tag{2.153}$$

for all u, v, w in $\mathbf{U}$. Thus if u_1, u_2, v_1, v_2 are in $\mathbf{U}$, then on taking $u = u_1u_2$, $v = u_2v_1$ and $w = v_1v_2$ we obtain from (2.152) that

$$K(u_1u_2, v_1v_2) \le K(u_1, v_1) + K(u_2, v_2) \ . \tag{2.154}$$

On squaring both sides of (2.152) and using the inequality of the arithmetic-geometric mean, we get with $K(z, y) = +\sqrt{1 - \mathrm{Re}(z\overline{y})}$ for any z and y in $\mathbf{U}$, the inequality

$$K(u,w)^2 \leq 2(K(u,v)^2 + K(v,w)^2) \tag{2.155}$$

for all u, v, w in $\mathbf{U}$. Similarly, we obtain from (2.154) that

$$K(u_1u_2, v_1v_2)^2 \leq 2(K(u_1,v_1)^2 + K(u_2,v_2)^2) \tag{2.156}$$

for all u_1, u_2, v_1, v_2 in $\mathbf{U}$. Let us write down explicitly the form in which we will often use (2.155). Let a, b, c, x, y and z be real numbers with a, b, c positive and $c \leq \min(a,b)$. Then

$$c(1 - \mathrm{Re}(e(x-y))) \leq 2a(1 - \mathrm{Re}(e(x-z))) + 2b(1 - \mathrm{Re}(e(y-z))) \ , \tag{2.157}$$

which follows from (2.155) on taking $u = e(x)$, $v = e(z)$ and $w = e(y)$. A similar inequality obtains from (2.156) as well.

As observed by A. Granville and K. Soundararajan, the inequalities ((2.149)), ((2.152)) and ((2.154)) in fact extend to all complex numbers in the closed unit disc and these extensions lead to the triangle inequality for the Granville - Soundararajan distance between multiplicative functions taking values in this disc.

We will give a sample application of (2.155) by proving the following proposition, which complements Theorem 11.1 and the classical version of which is often stated as a part of Hálasz's Theorem.

Proposition 12.1. *For any multiplicative function f on $\mathcal{G}$ with values in $\mathbf{U}$ there exists at most one real number t such that the series*

$$\sum_{\pi \in \mathcal{P}[i]} \frac{1 - \operatorname{Re}\left(f(\pi)\mathcal{N}(\pi)^{-it}\right)}{\mathcal{N}(\pi)} \tag{2.158}$$

converges.

Proof. Let t_0 and t_1 be real numbers satisfying the hypothesis of the proposition. Then an application of (2.155) with $u = \mathcal{N}(\pi)^{it_0}$, $v = f(\pi)$ and $w = \mathcal{N}(\pi)^{it_1}$ for each π in $\mathcal{P}[i]$ shows that the series

$$\sum_{\pi \in \mathcal{P}[i]} \frac{1 - \operatorname{Re}\left(\mathcal{N}(\pi)^{i(t_0 - t_1)}\right)}{\mathcal{N}(\pi)} \tag{2.159}$$

converges. The proposition now follows from the conclusion of the lemma below. □

Lemma 12.1. *The unique real number t for which the series*

$$\sum_{\pi \in \mathcal{P}[i]} \frac{1 - \operatorname{Re}\left(\mathcal{N}(\pi)^{it}\right)}{\mathcal{N}(\pi)} \tag{2.160}$$

converges is 0.

Proof. Plainly, it suffices to show that the series (2.160) diverges when $t \neq 0$. Given such a t, let $\mathcal{P}'$ be the set of integral primes $p \equiv 1$ modulo 4 and satisfying the condition

$$1 - \operatorname{Re}\left(p^{it}\right) \geq \frac{1}{2}\,. \tag{2.161}$$

Then on recalling that for each $p \equiv 1$ modulo 4 there are two $\pi \in \mathcal{P}[i]$ with $\mathcal{N}(\pi) = p$, we have that

$$\sum_{\pi\in\mathcal{P}[i]} \frac{1-\mathrm{Re}\,(\mathcal{N}(\pi)^{it})}{\mathcal{N}(\pi)} \;\geq\; \sum_{p\in\mathcal{P}'} \frac{1}{p}\,, \tag{2.162}$$

and it remains to verify that the series on the right hand side of (2.162) diverges. Let us set $2\pi\theta = t$, where π in this instance is the numerical constant. Then for any p satisfying (2.161) we have $\mathrm{Re}(e(\theta\log p)) \leq \frac{1}{2}$. This is the same as saying that

$$n+\frac{1}{6} \;\leq\; \theta\log p \;\leq\; n+\frac{5}{6} \tag{2.163}$$

for some integer n. Since $\theta \neq 0$, it then follows that

$$\sum_{p\in\mathcal{P}'} \frac{1}{p} \;=\; \sum_{n\geq 1} \sum_{\substack{p\equiv 1 \bmod 4,\\ e^{\frac{n}{\theta}+\frac{1}{6\theta}} \leq p \leq e^{\frac{n}{\theta}+\frac{5}{6\theta}}.}} \frac{1}{p}\;. \tag{2.164}$$

Since the inner sum on the right hand side of (2.164) is asymptotic to

$$\frac{1}{2}\left(\log\left(\frac{n}{\theta}+\frac{5}{6\theta}\right) - \log\left(\frac{n}{\theta}+\frac{1}{6\theta}\right)\right) \;\sim\; \frac{2}{3n}, \tag{2.165}$$

we conclude that $\sum_{p\in\mathcal{P}'}\frac{1}{p}$ is a divergent series.

□

We note here that by extending (2.155) to all u, v and w in the closed unit disc rather than $\mathbf{U}$, the same proof as above shows Proposition 12.1 to be valid for multiplicative functions taking values in the closed unit disc.

13 Finitely Distributed Additive Functions

For $\mathcal{X} \subseteq \mathbf{C}$, $\mathrm{dia}(\mathcal{X})$ denotes $\sup|z - z'|$, with (z, z') varying over $\mathcal{X} \times \mathcal{X}$. For a complex valued function f on $\mathcal{X}$, the image of f is denoted by $f(\mathcal{X})$.

Definition 13.1. A complex valued additive function f on $\mathcal{G}$ is said to be *finitely distributed* if there exist real numbers c_1, $c_2 > 0$ and a sequence $\{X_k\}_{k\geq 1}$ of real numbers $X_k \to +\infty$ such that for each $k \geq 1$ there is a subset A_k of $\mathcal{G}^*$ with $\mathcal{N}(z) \leq X_k$ for all $z \in A_k$ and

(i) $|A_k| \geq c_1 X_k$,

(ii) $\mathrm{dia}(f(A_k)) \leq c_2$.

When we wish to emphasise the roles of the real numbers c_1 and c_2, we will say that f is (c_1, c_2)*-finitely distributed.*

Thus, an additive function on $\mathcal{G}$ is finitely distributed if there are large subsets of $\mathcal{G}^*$ on which its values lie close to each other. Our principal aim in this section is to obtain the characterisation of finitely distributed additive functions on $\mathcal{G}$ given by Theorem 13.1.

Definition 13.2. A complex valued function ϕ on the set $\mathcal{P}[i]$ is called *small function* if there is a thin set of primes $\mathcal{Z}$ such that the series

$$\sum_{\pi\in\mathcal{Z}^c} \frac{|\phi(\pi)|^2}{\mathcal{N}(\pi)} \tag{2.166}$$

converges, where $\mathcal{Z}^c$ is the complement of $\mathcal{Z}$ in $\mathcal{P}[i]$. A complex valued additive function on $\mathcal{G}$ is called small if its restriction to $\mathcal{P}[i]$ is a small function.

A small function indeed takes only small values on $\mathcal{P}[i]$ outside a thin set of primes. More precisely, if ϕ is a small function and $\eta > 0$ a real number then the set $\mathcal{Z}(\eta)$ of $\pi \in \mathcal{P}[i]$ such that $|\phi(\pi)| > \eta$ is a thin set of primes. For if $\mathcal{Z}$ is a thin set of primes such that (2.166) converges, then we have

$$\eta^2 \sum_{\pi \in \mathcal{Z}(\eta) \cap \mathcal{Z}^c} \frac{1}{\mathcal{N}(\pi)} \leq \sum_{\pi \in \mathcal{Z}^c} \frac{|\phi(\pi)|^2}{\mathcal{N}(\pi)} . \tag{2.167}$$

Therefore $\mathcal{Z}(\eta) \cap \mathcal{Z}^c$ is a thin set of primes and since $\mathcal{Z}(\eta) \cap \mathcal{Z} \subseteq \mathcal{Z}$ is evidently a thin set of primes, so is $\mathcal{Z}(\eta)$.

Theorem 13.1. *For a complex valued additive function f on $\mathcal{G}$ to be finitely distributed it is necessary and sufficient that there exist a $\kappa \in \mathbf{C}$ and a small additive function ϕ such that $f(z) = \kappa \log \mathcal{N}(z) + \phi(z)$, for all z in $\mathcal{G}$.*

The analogue of Theorem 13.1 for additive functions on $\mathbf{N}^*$, with slightly more restricted hypotheses, is originally due P. Erdös and is contained in his fundamental paper [13].

13.1 Smallness and Finite Distribution

As the statement of Theorem 13.1 tells us, small additive functions are finitely distributed. At several points in [13], Erdös implicitly uses the fact that the analogues of these functions for $\mathbf{N}^*$ in fact enjoy a stronger property. The following lemma extends this property to small additive functions on $\mathcal{G}$.

Lemma 13.1. *Let $X \geq 4$ be a real number and let ϕ be a small additive function on $\mathcal{G}$. Then for each real number $c > 0$ there are real numbers $\gamma > 0$ and $\lambda > 0$*

such that any subset A of $\mathcal{G}^*$ with $\mathcal{N}(z) \leq X$ for all $z \in A$ and $|A| \geq cX$ contains a subset B with $|B| \geq \gamma X$ and $\mathrm{dia}(\phi(B)) \leq \lambda$.

Proof. Let $\mathcal{Z}$ be a thin set of primes such that the series (2.166) converges. Let $S = S(\mathcal{Z}, \phi)$ denote sum of this series. Define the totally additive function ψ on $\mathcal{G}$ by $\psi(\pi) = \phi(\pi)$ when $\pi \notin \mathcal{Z}$ and $\psi(\pi) = 0$ when $\pi \in \mathcal{Z}$. Then by Corollary 7.1 there is a $d > 0$ corresponding to c such that A contains a subset W with $|W| \geq dX$ and

$$\phi(z) - \phi(z') = \psi(z) - \psi(z') \text{ for all } z,\, z' \text{ in } W. \tag{2.168}$$

We have that $\sum_{\pi \in \mathcal{P}[i]} \frac{|\psi(\pi)|^2}{\mathcal{N}(\pi)} = S$. From this and Corollary 6.1 applied to ψ we have $|\mathcal{E}(\frac{\lambda}{2}, \psi, X)| \ll \frac{SX}{\lambda^2} \leq \frac{dX}{2}$, for any $\lambda \gg \sqrt{\frac{S}{d}}$ and all $X \geq 4$. Let us set $B = W \setminus \mathcal{E}(\frac{\lambda}{2}, \psi, X)$ and $\gamma = \frac{d}{2}$. Then

$$|B| \;\geq\; dX - \frac{dX}{2} = \gamma X\;. \tag{2.169}$$

Also, the definition of $\mathcal{E}(\frac{\lambda}{2}, \psi, X)$ tells us that $|\psi(z) - E(\psi, X)| \leq \frac{\lambda}{2}$ for all z in B, where $E(\psi, X)$ is as in (2.37). This implies that

$$|\psi(z) - \psi(z')| \leq \lambda \text{ for all } z, z' \text{ in } B. \tag{2.170}$$

Since $B \subseteq W$, it follows from (2.170) and (2.168) that $\mathrm{dia}(\phi(B)) \leq \lambda$, which when taken together with (2.169) provides the conclusion of the lemma. □

Proposition 13.1. *Suppose that f and ϕ are complex valued additive functions on $\mathcal{G}$ and that ϕ is small. Then for f to be finitely distributed it is necessary and sufficient that $f + \phi$ be so.*

Proof. It suffices to prove that the condition of the proposition is necessary. For then, on replacing f with $f + \phi$ and ϕ with $-\phi$, we obtain that it is sufficient as well. Suppose now that f satisfies the conditions of Definition 13.1 for c_1, c_2. Then Lemma 13.1 shows that there are $\gamma > 0$ and $\lambda > 0$ corresponding to c_1 such that for each $k \geq 1$, the set A_k contains a subset B_k with $|B_k| \geq \gamma X_k$ and $\mathrm{dia}(\phi(B_k)) \leq \lambda$. Since $\mathrm{dia}(f(B_k)) \leq c_2$, we obtain $\mathrm{dia}(g(B_k)) \leq \lambda + c_2$, where $g = f + \phi$. Thus g is $(\gamma, \lambda + c_2)$-finitely distributed. □

The proofs of Lemma 13.1 and Proposition 13.1 yield the following explicit version of Proposition 13.1.

Proposition 13.2. *Suppose that f and ϕ are as in Proposition 13.1. Let $\mathcal{Z}$ be a thin set of primes so that the series (2.166) converges, with $S = S(\mathcal{Z}, \phi)$ denoting its sum. Then for each $c_1 > 0$ there is a $c_1' > 0$ such that if f is (c_1, c_2)-finitely distributed for some $c_2 > 0$ then $f + \phi$ is $(c_1', \lambda + c_2)$-finitely distributed, for any $\lambda \gg \sqrt{\frac{S}{c_1'}}$.*

As an immediate consequence we have :

Corollary 13.1. *Let f and g be complex valued additive functions on $\mathcal{G}$ such that the subset $\mathcal{Z}$ of $\pi \in \mathcal{P}[i]$ with $f(\pi) \neq g(\pi)$ is a thin set of primes. Then for each $c_1 > 0$ there is a $c_1' > 0$ such that if f is (c_1, c_2)-finitely distributed for some $c_2 > 0$ then g is (c_1', c_2)-finitely distributed.*

Proof. Indeed, $\phi = f - g$ vanishes on the complement of $\mathcal{Z}$ in $\mathcal{P}[i]$ and is thus a small additive function with $S(\mathcal{Z}, \phi) = 0$. The corollary now follows from Proposition 13.2. □

13.2 Sufficiency

Here we shall show that the condition of Theorem 13.1 is sufficient. If f is a finitely distributed additive function on $\mathcal{G}$ then so is κf, for any complex number κ. By Proposition 13.1 then so is $\kappa f + \phi$, where ϕ is a small additive function. Thus to show that the condition of Theorem 13.1 is sufficient it is enough to verify that the function $z \mapsto \log \mathcal{N}(z)$ for all z in $\mathcal{G}$ is finitely distributed. To see this, let $\{X_k\}_{k\geq 1}$ be any increasing sequence of real numbers with $X_k \to +\infty$ and $X_1 \geq \frac{4\alpha_1^2}{\alpha_0}$, with α_i as in (2.10). For any $k \geq 1$, let A_k be the set of z in $\mathcal{G}^*$ with $\frac{X_k}{2} < \mathcal{N}(z) \leq X_k$. Then

$$|A_k| = \mathcal{L}(X_k) - \mathcal{L}\left(\frac{X_k}{2}\right) \geq \frac{\alpha_0 X_k}{2} \tag{2.171}$$

for all $k \geq 1$, by (2.10). Also, for all k, we have $\text{dia}(\log \mathcal{N}(A_k)) \leq \log 2$, since for any z, z' in A_k we have $\frac{1}{2} \leq \frac{\mathcal{N}(z)}{\mathcal{N}(z')} \leq 2$. Thus the additive function $z \mapsto \log \mathcal{N}(z)$ is $(\frac{\alpha_0}{2}, \log 2)$-finitely distributed.

13.3 Necessity

We now pass to the proof of the necessity of the condition in statement of Theorem 13.1. If f is a additive function that is finitely distributed then $\text{Re}(f)$ and $\text{Im}(f)$ are real valued finitely distributed functions. Also, any complex linear combination of small additive functions is a small additive function, since a finite union of thin sets of primes is a thin set of primes. Consequently, it suffices for us to prove the following theorem.

Theorem 13.2. *If f is a real valued additive function on $\mathcal{G}$ that is finitely distributed* *then there is a $\kappa \in \mathbf{R}$ and a small additive function ϕ such that for all z in $\mathcal{G}$ we have $f(z) = \kappa \log \mathcal{N}(z) + \phi(z)$.*

The analogue of Theorem 13.2 for additive functions on $\mathbf{N}^*$ is, of course, also contained in Erdös' paper [13]. His proof of this theorem relies on an elementary but complicated argument. Later, C. Ryavec [40] gave an elegant analytic proof of Erdös' theorem. Here we adapt Ryavec's method, with some simplifications, to prove Theorem 13.2. The proof of this theorem occupies subsections through, below.

The principle of Ryavec's method is to observe that for each θ in $\mathbf{R}$, the function $z \mapsto e(\theta f(z))$ is a multiplicative function on $\mathcal{G}$ and then to exploit this observation by varying θ. The starting point is a simple relation between these multiplicative functions and the finite distribution property of f given by Proposition 13.3 below.

13.4 Finite Distribution and the Fourier Transform

Hereafter we will use a normalisation for the Fourier transform different from that given earlier in (2.104). That is, when α is an integrable function on $\mathbf{R}$, we take for its Fourier transform the function $t \mapsto \widehat{\alpha}(t)$ on $\mathbf{R}$, where

$$\widehat{\alpha}(t) \;=\; \int_{\mathbf{R}} \alpha(u) e(-tu)\, du \;, \tag{2.172}$$

for all $t \in \mathbf{R}$.

Proposition 13.3. *For real numbers $c_1, c_2 > 0$, let f be a real valued (c_1, c_2)-finitely distributed additive function on $\mathcal{G}$. Further, for any integer $k \geq 1$ and with X_k as in Definition 13.1, let*

$$F_k(\theta) \;=\; \frac{1}{X_k} \sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le X_k.}} e(\theta f(z)) \;\; \textit{for all } \theta \textit{ in } \mathbf{R}. \tag{2.173}$$

When ϕ *is an integrable function on* $\mathbf{R}$ *such that* $\widehat{\phi}$ *is a positive real valued function with* $\widehat{\phi}(t) \ge 1$ *for* $|t| \le c_2$*, we then have*

$$\liminf_{k\to+\infty} \int_{\mathbf{R}} \phi(\theta)|F_k(\theta)|^2 \, d\theta \;\ge\; c_1^2 \,. \tag{2.174}$$

Proof. For each $k \ge 1$ we have

$$\int_{\mathbf{R}} \phi(\theta)|F_k(\theta)|^2 \, d\theta \;=\; \frac{1}{X_k^2} \sum_{\substack{z,z'\in\mathcal{G}^*,\\ \mathcal{N}(z),\mathcal{N}(z')\le X_k.}} \widehat{\phi}(f(z) - f(z')) \,. \tag{2.175}$$

To see this, we first note using (2.173) that for all θ in $\mathbf{R}$ we have

$$|F_k(\theta)|^2 \;=\; F_k(\theta)\, \overline{F_k(\theta)} \;=\; \frac{1}{X_k^2} \sum_{\substack{z,z'\in\mathcal{G}^*,\\ \mathcal{N}(z),\mathcal{N}(z')\le X_k.}} e(\theta(f(z) - f(z'))) \,. \tag{2.176}$$

We then obtain (2.175) on inserting this last expression for $|F_k(\theta)|^2$ into the left hand side of (2.175), interchanging the sum and the integral in the result and using (2.172). From the properties of $\widehat{\phi}$ and (ii) of Definition 13.1 we have

$$\sum_{\substack{z,z'\in\mathcal{G}^*,\\ \mathcal{N}(z),\mathcal{N}(z')\le X_k.}} \widehat{\phi}(f(z) - f(z')) \;\ge\; \sum_{(z,z')\in A_k\times A_k} \widehat{\phi}(f(z) - f(z')) \ge |A_k|^2 \,. \tag{2.177}$$

Also, $|A_k| \;\ge\; c_1 X_k$ by (i) of Definition 13.1. The inequality (2.174) results on combining this with (2.177) and (2.175) and passing to the limit as $k \to +\infty$. $\square$

For the sake of completeness we include a confirmation of the following fact.

Lemma 13.2. *For any real number $c > 0$ there is a continuous function of compact support ϕ on $\mathbf{R}$ such that $\widehat{\phi}$ is a positive real valued function with $\widehat{\phi}(t) \geq 1$ for $|t| \leq c$.*

Proof. Let $h(\theta) = 1 - |\theta|$ for $|\theta| \leq 1$ and $h(\theta) = 0$ when $|\theta| > 1$. Then $h : \theta \mapsto h(\theta)$ is a continuous function on $\mathbf{R}$ supported in $[-1, 1]$ and we have $\widehat{h}(t) = \left(\frac{\sin \pi t}{\pi t}\right)^2$. In particular, it follows from the classical inequality $\frac{\sin t}{t} \geq \frac{2}{\pi}$ for $|t| \leq \frac{\pi}{2}$ that we have $\widehat{h}(t) \geq \frac{4}{\pi^2}$ for $|t| \leq \frac{1}{2}$. Thus, for any $T > 0$, the function ϕ_T defined by $\phi_T(\theta) = \frac{8}{\pi^2 T} h(\frac{2\theta}{T})$ has the property that $\widehat{\phi}_T(t) \geq 0$ for all t in $\mathbf{R}$ and $\widehat{\phi}_T(t) \geq 1$ for $|t| \leq \frac{1}{T}$.

$\square$

13.5 Finite Distribution and Mean Values

When f is real valued, the multiplicative function $z \mapsto e(\theta f(z))$ takes values in $\mathbf{U}$. This allows us to combine Proposition 13.3 with Theorem 11.1, of Halász, and the triangle inequality (2.156). The net result is Theorem 13.3, which is at the heart of Ryavec's method.

Thus for real numbers $c_1, c_2 > 0$, let f be a real (c_1, c_2)-finitely distributed additive function on $\mathcal{G}$, and as before, let us define $F_k(\theta)$, for each $\theta \in \mathbf{R}$ and each integer $k \geq 1$ by

$$F_k(\theta) = \frac{1}{X_k} \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X_k.}} e(\theta f(z)) , \tag{2.178}$$

where X_k are as in Definition 13.1. Further, let $\mathcal{D}$ be the set of θ in $\mathbf{R}$ such that $\lim_{k\to+\infty} F_k(\theta) = 0$. Then $\mathcal{D}$ is a measurable subset of $\mathbf{R}$. Indeed, if for all integers $k, n \geq 1$ we set

$$\mathcal{D}_{n,k} = \left\{ \theta \mid \quad |F_k(\theta)| \leq \frac{1}{n} \right\} \tag{2.179}$$

then since $\theta \mapsto F_k(\theta)$ is a continuous function on $\mathbf{R}$, $\mathcal{D}_{n,k}$ is a closed subset of $\mathbf{R}$ for all n, k and we have

$$\mathcal{D} \; = \bigcap_{n\geq 1} \bigcup_{m\geq 1} \bigcap_{k\geq m} \mathcal{D}_{n,k} \; . \tag{2.180}$$

Lemma 13.3. *The complement of $\mathcal{D}$ in $\mathbf{R}$ is not a null set.*

Proof. Proposition 13.3 tells us that for any integrable function ϕ on $\mathbf{R}$ whose Fourier transform $\widehat{\phi}$ is a positive real valued function with $\widehat{\phi}(t) \geq 1$ for $|t| \leq c_2$ we have

$$\liminf_{k\to+\infty} \int_{\mathbf{R}} \phi(\theta)|F_k(\theta)|^2 \, d\theta \; \geq \; c_1^2 \; . \tag{2.181}$$

Suppose now that the complement of $\mathcal{D}$ is a null set. Then from the definition of the set $\mathcal{D}$ we have

$$\lim_{k\to+\infty} \phi(\theta)|F_k(\theta)|^2 = 0 \;\text{ for almost all } \theta \in \mathbf{R}.$$

Since $|F_k(\theta)| \leq 1$ for all $\theta \in \mathbf{R}$ and all $k \geq 1$, it follows from the Dominated Convergence Theorem that the left hand side of (2.181) is 0, which is absurd since the right hand side of (2.181) is $c_1^2 > 0$. This contradiction proves the lemma.

□

Let $\mathcal{E}$ be the set of all θ in $\mathbf{R}$ with the property that there is a $t \in \mathbf{R}$ for which the series

$$\sum_{\pi \in \mathcal{P}[i]} \frac{1 - \mathrm{Re}\,(e(\theta f(\pi))\mathcal{N}(\pi)^{-it})}{\mathcal{N}(\pi)} \tag{2.182}$$

converges. By Proposition 12.1 applied to the multiplicative function $z \mapsto e(\theta f(z))$, we see that for each θ in $\mathcal{E}$ there is a unique t in $\mathbf{R}$ so that this property holds. We define $t(\theta)$ to be $\frac{t}{2\pi}$, where π is the numerical constant. We then have the following striking assertion.

Theorem 13.3. *We have that $\mathcal{E} = \mathbf{R}$ and that the map $\theta \mapsto t(\theta)$ is an endomorphism of the additive group $\mathbf{R}$.*

Proof. Let us first show that $\mathcal{E}$ is an additive subgroup of $\mathbf{R}$. To see this it is enough to verify that

$$\mathcal{E} - \mathcal{E} \subseteq \mathcal{E} \ . \tag{2.183}$$

Thus suppose θ_1, θ_2 are in $\mathcal{E}$. Then on applying, for each $\pi \in \mathcal{P}[i]$, the inequality (2.156) with $u_1 = e(\theta_1 f(\pi))$, $u_2 = e(-\theta_2 f(\pi))$, $v_1 = \mathcal{N}(\pi)^{it(\theta_1)}$ and $v_2 = \mathcal{N}(\pi)^{-it(\theta_2)}$, we deduce that the series (2.182) converges for $\theta = \theta_1 - \theta_2$ and $t = t(\theta_1) - t(\theta_2)$. This verifies (2.183) and moreover shows that for all $\theta_1, \theta_2 \in \mathcal{E}$ we have the relation

$$t(\theta_1 - \theta_2) = t(\theta_1) - t(\theta_2) \ . \tag{2.184}$$

Since we have $t(0) = 0$ from Lemma 12.1, it now follows that $t : \mathcal{E} \mapsto \mathbf{R}$ is a homomorphism of additive groups. It remains only to verify that $\mathcal{E} = \mathbf{R}$.

Let $\mathcal{D}'$ be the complement of the set $\mathcal{D}$ in $\mathbf{R}$. Then Theorem 11.1 tells us that $\mathcal{D}' \subseteq \mathcal{E}$ and therefore that $\mathcal{D}' - \mathcal{D}' \subseteq \mathcal{E} - \mathcal{E} \subseteq \mathcal{E}$. Since by Lemma 13.3 $\mathcal{D}'$ is a measurable subset of $\mathbf{R}$ that is not a null set, we have that there is an $\epsilon > 0$ so that the open interval $(-\epsilon, \epsilon) \subseteq \mathcal{D}' - \mathcal{D}'$. This follows from the classical lemma given below. Thus $\mathcal{E}$ contains $(-\epsilon, \epsilon)$. Since $\mathcal{E}$ is a subgroup of $\mathbf{R}$, it then follows that $\mathcal{E}$ contains the open interval $(-n\epsilon, n\epsilon)$, for all integers $n \geq 1$. Hence $\mathcal{E} = \mathbf{R}$.

□

The following lemma is due to H. Steinhaus and the proof we give is due to A. Weil (see [4], Chap. VIII, page 42).

Lemma 13.4. *If $X \subseteq \mathbf{R}$ is a measurable subset of $\mathbf{R}$ that is not a null set then $X - X$ contains a neighbourhood of 0.*

Proof. Since X is not a null set, there is a compact interval K of $\mathbf{R}$ such that $Y = K \cap X$ is not a null set. Let χ denote the characteristic function of Y. Then χ is an integrable function on $\mathbf{R}$, since Y is a measurable set of finite measure. Hence $\chi * \chi$ is a continuous function on $\mathbf{R}$. Now $\chi * \chi(0) = \mu(Y) \neq 0$. Therefore, there is a neighbourhood U of 0 such that $\chi * \chi(t) \neq 0$ for all t in U. This means that $U \subseteq Y - Y \subseteq X - X$. □

With Theorem 13.3 in hand, the next step is to show that the endomorphism t satisfies $t(\theta) = t(1)\theta$. This would be an easy consequence of Steinhaus' lemma above, if it can be shown that t is a measurable function. Since this, however, does not appear to be obvious from the definition of t, the proof of the aforementioned characterisation of t requires a careful study of $u(\theta) = t(\theta) - t(1)\theta$, which we will carry out with the aid of the analytic facts given in the following subsection.

13.6 Analytic Lemmas

Here we write $\cos(2\pi u)$ rather than $\mathrm{Re}(e(u))$, for any real number u. The following is a variant of the lemma of W. Schmidt given on page of 399 of Ryavec [40].

Lemma 13.5. *Let c_k and a_k be real numbers with $c_k \geq 0$ and $a_k \in \mathbf{Z}^*$, for each integer $k \geq 1$. Suppose that the series*

$$\sum_{k\geq 1} c_k(1-\cos(2\pi a_k\theta)) \tag{2.185}$$

converges for all $\theta \in [0,1]$. Then the series $\sum_{k\geq 1} c_k$ converges.

Proof. Let us set $Y_n(\theta) = \sum_{1\leq k\leq n} c_k(1-\cos(2\pi a_k\theta))$, for all $\theta \in [0,1]$ and integers $n \geq 1$. Then for all such θ and n we have

$$0 \leq Y_n(\theta) \leq 2\sum_{1\leq k\leq n} c_k = 2\int_0^1 Y_n(\theta)d\theta\ . \tag{2.186}$$

For each integer $K \geq 0$, let $E(K)$ be the set of θ in $[0,1]$ such that $Y_n(\theta) \leq K$ for all $n \geq 1$. That is, $E(K) = [0,1] \cap \cap_{n\geq 1} Y_n^{-1}([0,K])$. Since $\theta \mapsto Y_n(\theta)$ is continuous for each n, $E(K)$ is a measurable subset of $[0,1]$ for each K. Further, we have

$$\int_0^1 Y_n(\theta)d\theta \ \leq\ K\mu(E(K)) + 2(1-\mu(E(K))\int_0^1 Y_n(\theta)d\theta \tag{2.187}$$

for all n and K, on estimating the integral on the left hand side of (2.187) using $Y_n(\theta) \leq K$ for θ in $E(K)$ and using (2.186) for θ in its complement in $[0,1]$.

Since the series (2.185) converges for all θ in $[0,1]$, $\lim_{n\to+\infty} Y_n(\theta)$ exists for all θ in $[0,1]$. It follows from this that $\lim_{K\to+\infty}\mu(E(K)) = 1$. Thus there is a K such that $\mu(E(K)) \geq \frac{3}{4}$. For such a K we obtain from (2.187) after a rearrangement of terms that

$$\sum_{1\le k\le n} c_k \;=\; \int_0^1 Y_n(\theta)d\theta \;\le\; 2K\mu(E(K))\;, \tag{2.188}$$

for all $n \ge 1$, from which we conclude that $\sum_{k\ge1} c_k$ converges. □

We now fashion a pair of propositions from Ryavec's applications of Schmidt's lemma.

Proposition 13.4. *Let c_k be a positive real number for each integer $k \ge 1$. Suppose further that there is a function $v : [0,1] \mapsto \mathbf{R}$ such that the series*

$$\sum_{k\ge1} c_k(1 - \cos(2\pi(k\theta + v(\theta)))) \tag{2.189}$$

converges for all $\theta \in [0,1]$. Then the series $\sum_{k\ge1} c_k$ converges.

Proof. Let $\sigma : \mathbf{N}^* \mapsto \mathbf{N}^*$ be an injective mapping. Then since the series of positive terms (2.189) converges for all $\theta \in [0,1]$ so does the series

$$\sum_{k\ge1} c_{\sigma(k)}(1 - \cos(2\pi(\sigma(k)\theta + v(\theta)))\;. \tag{2.190}$$

Adding (2.189) to (2.190), using the triangle inequality (2.157) and noting that $\cos u = \cos|u|$ for any real u, we deduce that

$$\sum_{k\ge1} \min(c_k, c_{\sigma(k)})(1 - \cos(2\pi|k - \sigma(k)|\theta)) \tag{2.191}$$

converges for all $\theta \in [0,1]$. By means of Lemma 13.5 we then conclude that the series

$$\sum_{\substack{k\geq 1,\\ k\neq\sigma(k).}} \min(c_k, c_{\sigma(k)}) \tag{2.192}$$

converges for any injective map $\sigma : \mathbf{N}^* \mapsto \mathbf{N}^*$. We shall show that this implies that $\sum_{k\geq 1} c_k$ converges. We may, and do, assume that $c_k > 0$ for all $k \geq 1$.

For a real number $y > 0$, let $A(y)$ be the set of integers $k \geq 1$ such that $c_k \geq y$. Suppose $A(y)$ is an infinite set and, for each k in $A(y)$, let $\sigma_y(k)$ be the smallest integer l satisfying $k < l$ and $l \in A(y)$. For integers $k \geq 1$ not in $A(y)$, let $\sigma_y(k) = k$. Then $\sigma_y : \mathbf{N}^* \mapsto \mathbf{N}^*$ is an injection. Also, we have $k \neq \sigma_y(k)$ and $\min(c_k, c_{\sigma(k)}) \geq y$ for all k in the infinite set $A(y)$. This is absurd because the series (2.192) with $\sigma = \sigma_y$ converges. Thus $A(y)$ is a finite set for all $y > 0$.

For any k and l in $\mathbf{N}^*$, let us set $k \preceq l$ if either $c_k > c_l$ or if $c_k = c_l$ and $k \leq l$. Then $\preceq$ is a total order on $\mathbf{N}^*$. We set $\tau(k)$ to be the unique element of $\mathbf{N}^*$ least with respect to $\preceq$ among the l in $\mathbf{N}^*$ satisfying $k \preceq l$ and $k \neq l$, for each $k \in \mathbf{N}^*$. It follows from the finiteness of $A(c_k)$ that $\tau(k)$ exists. Also, $\tau : \mathbf{N}^* \mapsto \mathbf{N}^*$ is an injection. Moreover, we have $k \neq \tau(k)$ and $\min(c_k, c_{\tau(k)}) = c_{\tau(k)}$ for all k in $\mathbf{N}^*$. From the convergence of the series (2.192) with $\sigma = \tau$ we then have that $\sum_{k\geq 1} c_{\tau(k)}$ converges. Since every integer $k \in \mathbf{N}^*$ is in the image of τ except for the unique integer that is the least element of $\mathbf{N}^*$ with respect to $\preceq$, we conclude that $\sum_{k\geq 1} c_k$ converges.

□

Proposition 13.5. *Let I be a subset of $\mathcal{P}[i]$ and $\{\epsilon_i\}$, $\{a_i\}$ be sequences of real numbers indexed by I with $\epsilon_i \geq 0$ and $a_i \in \mathbf{Z}^*$ for each $i \in I$. Also, let $v : [0,1] \mapsto \mathbf{R}$ be any function such that $v(\theta) \in \mathbf{Z}$ for all $\theta \in D$, a dense subset of $[0,1]$. Suppose* *further that for all* $\theta \in [0,1]$ *the series of positive terms*

$$\sum_{i\in I} \epsilon_i(1-\cos(2\pi(a_i\theta+v(\theta))) \tag{2.193}$$

converges. Then $\sum_{i\in I}\epsilon_i$ *converges.*

Proof. For any integer $k\neq 0$, let us set $I_k=\{i\in I|a_i=k\}$. Then since the terms of (2.193) are all positive, its convergence implies that

$$\sum_{k\neq 0}(1-\cos(2\pi(k\theta+v(\theta)))\sum_{i\in I_k}\epsilon_i \tag{2.194}$$

converges for all $\theta\in[0,1]$.

Since D is a dense subset of $[0,1]$, D is not contained in $\frac{1}{k}\mathbf{Z}$ for any integer $k\neq 0$. Hence for each integer $k\neq 0$ there is a $\theta_k\in D$ such that $k\theta_k\notin\mathbf{Z}$. By the assumption on v, it follows that $1-\cos(2\pi(k\theta+v(\theta))\neq 0$ when $\theta=\theta_k$. It follows from convergence of (2.194) for $\theta=\theta_k$ that $c_k=\sum_{i\in I_k}\epsilon_i$ is convergent, for any integer $k\neq 0$. Then on applying Proposition 13.4 separately to $k\geq 1$ and $k\leq -1$ in (2.194), and using $\cos u=\cos(-u)$ for any real u in the latter case, we see that $\sum_{k\neq 0}c_k$ converges. We conclude from this that $\sum_{i\in I}\epsilon_i$ also converges.

□

13.7 End Game

Here we shall complete the proof of Theorem 13.2.

Let $\mathcal{M}$ be the set of real valued functions on $\mathcal{P}[i]$. Then $\mathcal{M}$ has a natural $\mathbf{R}$-vector space structure. Let $\mathcal{V}\subseteq\mathcal{M}$ be the set of $\phi\in\mathcal{M}$ such that the series

$$\sum_{\pi \in \mathcal{P}[i]} \frac{1 - \mathrm{Re}\,(e(\phi(\pi)))}{\mathcal{N}(\pi)} \tag{2.195}$$

converges.

By means of the triangle inequality (2.157), we see that $\mathcal{V}$ is a subgroup of the additive group of $\mathcal{M}$. Let us write $\mathcal{T}$ to denote the set of ϕ in $\mathcal{M}$ such that $\phi(\pi) \in \mathbf{Z}$ for all $\pi \in \mathcal{P}[i]$. Then $\mathcal{T}$ is a subgroup of $\mathcal{V}$. Thus if $\phi, \psi \in \mathcal{M}$ are such that $\phi - \psi \in \mathcal{T}$ then $\phi \in \mathcal{V}$ if and only if $\psi \in \mathcal{V}$.

Let $\mathcal{S}$ denote the set of real valued small functions on $\mathcal{P}[i]$. Then $\mathcal{S}$ is contained in $\mathcal{V}$. Conversely, any $\phi \in \mathcal{V}$ such that $|\phi(\pi)| \le \frac{1}{2}$ for all $\pi \in \mathcal{Z}^c$, the complement in $\mathcal{P}[i]$ of a thin set of primes $\mathcal{Z}$, is contained in $\mathcal{S}$. These remarks are easy consequences of the elementary inequalities

$$4u^2 \;\le\; 1 - \mathrm{Re}\,(e(u)) \;\le\; 10u^2\,, \tag{2.196}$$

valid for any real u with $|u| \le \frac{1}{2}$. Indeed, if ϕ is in $\mathcal{S}$ then by the remark following Definition 13.2 there is a thin set of primes $\mathcal{Z}$ so that $|\phi(\pi)| \le \frac{1}{2}$ for all $\pi \in \mathcal{Z}^c$ and such that the series (2.166) converges. Then from the second inequality in (2.196) and the trivial bound $1 - \mathrm{Re}\,(e(u)) \le 2$ we have

$$\sum_{\pi \in \mathcal{P}[i]} \frac{1 - \mathrm{Re}\,(e(\phi(\pi)))}{\mathcal{N}(\pi)} \;\le\; 10 \sum_{\pi \in \mathcal{Z}^c} \frac{|\phi(u)|^2}{\mathcal{N}(\pi)} + 2 \sum_{\pi \in \mathcal{Z}} \frac{1}{\mathcal{N}(\pi)}\,, \tag{2.197}$$

which implies that $\phi \in \mathcal{V}$. Conversely, if $\phi \in \mathcal{V}$ satisfies $|\phi(\pi)| \le \frac{1}{2}$ for all $\pi \in \mathcal{Z}^c$, then it follows from the first inequality in (2.196) and the convergence of (2.195) that the series (2.166) converges.

Any $\phi \in \mathcal{M}$ can be written in a unique manner as

$$\phi = \phi' + \phi'' \tag{2.198}$$

with $\phi'(\pi)$ in $\mathbf{Z}$ and $\phi''(\pi)$ in the interval $(-\frac{1}{2}, \frac{1}{2}]$, for all $\pi \in \mathcal{P}[i]$. Since $\phi' \in \mathcal{T}$, we have that $\phi \in \mathcal{V}$ if and only if $\phi'' \in \mathcal{V}$ and hence in $\mathcal{S}$. In particular, $\mathcal{V} = \mathcal{T} + \mathcal{S}$.

It is immediate from Definition 13.2 that $\mathcal{S}$ is an $\mathbf{R}$-vector subspace of $\mathcal{M}$. The following lemma tells us that $\mathcal{S}$ is the largest $\mathbf{R}$-vector subspace of $\mathcal{M}$ contained in $\mathcal{V}$.

Lemma 13.6. *For a ϕ in $\mathcal{V}$ to belong to $\mathcal{S}$ it is necessary and sufficient that $\theta\phi \in \mathcal{V}$ for all θ in $\mathbf{R}$.*

Proof. Since S is an $\mathbf{R}$-vector space, the condition is necessary. To verify that it is sufficient, we use the decomposition (2.198). Since $\theta\phi'' \in \mathcal{S}$, and hence in $\mathcal{V}$, we have that $\theta\phi' = \theta\phi - \theta\phi'' \in \mathcal{V}$. Let $\mathcal{Z}$ be the set of $\pi \in \mathcal{P}[i]$ such that $\phi'(\pi) \neq 0$. Then Proposition 13.5 applied with $v(\theta) \equiv 0$ and with $\mathcal{Z}$, $\frac{1}{\mathcal{N}(\pi)}$ and $\phi'(\pi)$ in place of I, ϵ_i and a_i respectively shows that $\sum_{\pi \in \mathcal{Z}} \frac{1}{\mathcal{N}(\pi)}$ converges. Thus $\mathcal{Z}$ is a thin set of primes and hence ϕ' is in $\mathcal{S}$. It follows from (2.198) that ϕ is in $\mathcal{S}$.

□

We now turn to the proof of Theorem 13.2. Let f be a given real valued finitely distributed additive function on $\mathcal{G}$. Then Theorem 13.3 tells us that there is an endomorphism t of the additive group $\mathbf{R}$ such that for each real number θ, the restriction to $\mathcal{P}[i]$ of the additive function ϕ_θ on $\mathcal{G}$ defined for all $z \in \mathcal{G}$ by the relation $\phi_\theta(z) = \theta f(z) - t(\theta) \log \mathcal{N}(z)$ belongs to $\mathcal{V}$. We shall presently show that

$$\phi_\theta = \theta\phi_1 \quad \text{for all } \theta \text{ in } \mathbf{R}. \tag{2.199}$$

On account of Lemma 13.6 we then obtain that ϕ_1 is in $\mathcal{S}$. Theorem 13.2 follows since we have $f(z) = t(1)\log\mathcal{N}(z) + \phi_1(z)$ for all z in $\mathcal{G}$.

For the remainder of this subsection we shall write $\log\mathcal{N}$ to denote the function $z \mapsto \log\mathcal{N}(z)$ on $\mathcal{G}$. It follows from the definition of ϕ_θ that

$$\phi_\theta - \theta\phi_1 = u(\theta)\log\mathcal{N} \tag{2.200}$$

for all θ in $\mathbf{R}$, where $u(\theta) = t(\theta) - \theta t(1)$, as introduced at the end of Subsection 13.5. Thus (2.199) is equivalent to $u(\theta) = 0$ for all $\theta \in \mathbf{R}$. In other words, the proof of Theorem 13.2 reduces to showing that $t(\theta) = \theta t(1)$ for all $\theta \in \mathbf{R}$.

On using the decomposition (2.198) for ϕ_θ and ϕ_1 in (2.200) and rearranging terms we see that

$$\theta\phi_1' + u(\theta)\log\mathcal{N} = \phi_\theta' + \phi_\theta'' - \theta\phi_1''\,. \tag{2.201}$$

Since $\phi_\theta' \in \mathcal{T}$ and $\phi_\theta'' - \theta\phi_1'' \in \mathcal{S}$, we conclude from (2.201) that the left hand side of this relation belongs to $\mathcal{V}$.

We will now use a beautiful device of Ryavec [40] (see also page 13-15, Erdös [13]) to remove the function $\log\mathcal{N}$ from the picture. Let ϕ be an element of $\mathcal{V}$ and let $\sigma : \mathcal{P}[i] \mapsto \mathcal{P}[i]$ be an injective map. Then since the series of positive terms (2.195) converges so does the series

$$\sum_{\pi \in \mathcal{P}[i]} \frac{1 - \mathrm{Re}\,(e(\phi(\sigma(\pi))))}{\mathcal{N}(\sigma(\pi))}\,. \tag{2.202}$$

Let us call an injective map $\sigma : \mathcal{P}[i] \mapsto \mathcal{P}[i]$ a bounded injection if there is a real number $K \geq 1$ such that $\mathcal{N}(\sigma(\pi)) \leq K\mathcal{N}(\pi)$, for all π in $\mathcal{P}[i]$. For such a σ we have $\min(\frac{1}{\mathcal{N}(\sigma(\pi))}, \frac{1}{\mathcal{N}(\pi)}) \geq \frac{1}{K\mathcal{N}(\pi)}$, for all $\pi \in \mathcal{P}[i]$. Thus on adding (2.202) to (2.195) and using the triangle inequality (2.157) we conclude that $\phi \circ \sigma - \phi$ belongs to $\mathcal{V}$. Applying this to the left hand side of (2.201) we deduce that

$$\theta(\phi_1' \circ \sigma - \phi_1') + u(\theta)(\log \mathcal{N} \circ \sigma - \log \mathcal{N}) \text{ belongs to } \mathcal{V} \tag{2.203}$$

for every $\theta \in \mathbf{R}$ and every bounded injection $\sigma : \mathcal{P}[i] \mapsto \mathcal{P}[i]$. Here we have written $\log(\mathcal{N} \circ \sigma)$ for the function $\pi \mapsto \log(\mathcal{N}(\sigma(\pi)))$ on $\mathcal{P}[i]$.

Lemma 13.7. *For any real $\lambda > 0$ there is a bounded injection $\sigma_\lambda : \mathcal{P}[i] \mapsto \mathcal{P}[i]$ such that the function $\pi \mapsto \log(\mathcal{N}(\pi)) - \log(\mathcal{N}(\sigma_\lambda(\pi))) - \lambda$ belongs to $\mathcal{S}$.*

Proof. Let $\mu = e^\lambda$ and for $X > 1$ let us set $l(X) = \frac{X}{\log^2 X}$. Further, suppose that $X_0 > 1$ is a sufficiently large real number and define $X_i = X_{i-1} + l(X_{i-1})$ for any $i \geq 1$. Then $\{X_i\}_{i \geq 0}$ is a strictly increasing sequence of real numbers such that $X_i \to +\infty$ with i.

Let I_0 be the set of $\pi \in \mathcal{P}[i]$ satisfying $2 \leq \mathcal{N}(\pi) < X_0$ and let I_i be the set of $\pi \in \mathcal{P}[i]$ with $X_{i-1} \leq \mathcal{N}(\pi) < X_i$ for any $i \geq 1$. Then the sets I_i form a disjont partition of $\mathcal{P}[i]$. Also, let $J_0 = I_0$ and let J_i be $\pi \in \mathcal{P}[i]$ with $\mu X_{i-1} \leq \mathcal{N}(\pi) < \mu X_i$ for each $i \geq 1$. Since X_0 is sufficiently large, we see using (2.28) that $|I_i| \leq |J_i|$ for all $i \geq 0$. Thus there is an injection $\sigma_i : I_i \mapsto J_i$ for all $i \geq 0$. For any π in $\mathcal{P}[i]$, define $\sigma_\lambda(\pi) = \sigma_i(\pi)$ if $\pi \in I_i$.

The map $\sigma_\lambda : \mathcal{P}[i] \mapsto \mathcal{P}[i]$ is a bounded injection. To see this, we only need to note that if $\pi \in I_i$ then we have

$$\left|\log\left(\frac{\mathcal{N}(\sigma_\lambda(\pi))}{\mu\mathcal{N}(\pi)}\right)\right| \leq \log\left(\frac{X_i}{X_{i-1}}\right) \leq \frac{l(X_{i-1})}{X_{i-1}} \leq 4, \tag{2.204}$$

where we have used the elementary inequality $\log(1+u) \leq u$ valid for real $u > 0$ together with $l(X) \leq 4X$ for $X \geq 2$. Since this last inequality also implies that $X_{i-1} \leq \mathcal{N}(\pi) \leq 5X_{i-1}$, we deduce from the first two inequalities in (2.204) the more precise bound

$$\left|\log\left(\frac{\mathcal{N}(\sigma_\lambda(\pi))}{\mu\mathcal{N}(\pi)}\right)\right| \leq \frac{5l(\mathcal{N}(\pi))}{\mathcal{N}(\pi)}\ , \tag{2.205}$$

for all $\pi \in \mathcal{P}[i]$, from which the conclusion of the proposition follows on remarking that the series $\sum_{\pi\in\mathcal{P}[i]} \frac{l(\mathcal{N}(\pi))}{\mathcal{N}(\pi)^2}$ converges. □

Let us write $\log\mathcal{N} - \log(\mathcal{N}\circ\sigma_\lambda) - \lambda$ for the function supplied by Lemma 13.7. Then since $\mathcal{S}$ is an $\mathbf{R}$-vector space and $\mathcal{V}$ an additive group, we may multiply this function by $u(\theta)$ and add the result to the function in (2.203) to deduce that

$$\theta((\phi_1'\circ\sigma_\lambda) - \phi_1') + u(\theta)\lambda \text{ belongs to } \mathcal{V} \tag{2.206}$$

for all real θ and $\lambda > 0$. Here, of course, $u(\theta)\lambda$ denotes the function $\pi \mapsto u(\theta)\lambda$ for all π in $\mathcal{P}[i]$.

Since t is an endomorphism of the additive group $\mathbf{R}$ we have $t(\theta) = \theta t(1)$ for all $\theta \in \mathbf{Q}$. Let us set $D = \mathbf{Q} \cap [0,1]$, which is a dense subset of $[0,1]$. Moreover, we have $u(\theta) = 0$ for all $\theta \in D$.

Suppose now that there is an $\alpha \in \mathbf{R}$ such that $u(\alpha) \neq 0$. Then let us choose a $\lambda > 0$ such that $u(\alpha)\lambda \notin \mathbf{Z}$. From (2.206) we have that

$$\sum_{\pi \in \mathcal{P}[i]} \frac{1 - \mathrm{Re}\,(e(\theta(\phi_1'(\pi) - \phi_1' \circ \sigma_\lambda(\pi))) - u(\theta)\lambda)}{\mathcal{N}(\pi)} \tag{2.207}$$

converges for all θ in $\mathbf{R}$. If $\mathcal{Z}$ is the set of π such that $-\phi_1'(\pi) + \phi_1' \circ \sigma_\lambda(\pi) = 0$ then since $u(\alpha)\lambda \notin \mathbf{Z}$, it follows from the convergence of (2.207) for $\theta = \alpha$ that $\mathcal{Z}$ is a thin set of primes. On the other hand, Proposition 13.5 applied with $v(\theta) = u(\theta)\lambda$, D as above, and with $\mathcal{Z}^c$, $\frac{1}{\mathcal{N}(\pi)}$ and $-\phi_1'(\pi) + \phi_1' \circ \sigma_\lambda(\pi)$ in place of I, ϵ_i and a_i respectively shows that $\mathcal{Z}^c$ is also a thin set of primes. This means that we have $\mathcal{P}[i]$ is a thin set of primes, which is absurd. Hence $u(\theta) = 0$ for all θ in $\mathbf{R}$, as was to be shown.

14 Strong Finite Distribution

Definition 14.1. We call a complex valued additive function f on $\mathcal{G}$ *strongly finitely distributed* if there is a real number $c_1 > 0$ such that f is (c_1, c_2)-finitely distributed *for every* real number $c_2 > 0$.

The following proposition is immediate from Definition 14.1 and Proposition 13.1.

Proposition 14.1. *Suppose that f and g are complex valued additive functions on $\mathcal{G}$ such that the set of $\pi \in \mathcal{P}[i]$ for which $f(\pi) \neq g(\pi)$ is a thin set of primes. Then f is strongly finitely distributed if and only if so is g.*

Applying this proposition with $g = 0$, which is evidently strongly finitely distributed, we see that any additive function f on $\mathcal{G}$ such that the set of $\pi \in \mathcal{P}[i]$ for which

$f(\pi) \neq 0$ is a thin set of primes is strongly finitely distributed. We have the following remarkable theorem, originally due to Erdös (*loc. cit.*) for additive functions on $\mathbf{N}^*$, that tells us that the converse also holds.

Theorem 14.1. *If f is a strongly finitely distributed complex valued additive function on $\mathcal{G}$ then the set of $\pi \in \mathcal{P}[i]$ for which $f(\pi) \neq 0$ is a thin set of primes.*

Elliott and Ryavec remark on pages 157 - 158 of [12] that the contrapositive version of the above theorem for additive functions on $\mathbf{N}^*$ has an interesting interpretation in the context of Levy's continuity theorem in probability theory. From their point view, it is thus natural to consider additive functions that are not strongly finitely distributed, as we have called it. This is also the case with Erdös (see Theorem IV in [13]), who originally considered these matters.

We will prove this theorem in two steps. First, we will show that a strongly finitely distributed additive function f is necessarily small. This is the conclusion of Theorem 14.2 of the following subsection. We then show in Subsection 14.2 that any small additive function on $\mathcal{G}$ that is strongly finitely distributed must satisfy the conclusion of Theorem 14.1, thereby completing its proof.

Before commencing the proof of Theorem 14.1 let us record the following corollary, which is the form in which we will eventually apply this theorem within the proof of Theorem 9.1 in Section 16.

We recall the definition of upper asymptotic density $\overline{\mathbf{d}}(\mathcal{A}) > 0$ of a subset of $\mathcal{A}$ of $\mathcal{G}$ given in Section 9 (see (2.13)).

Corollary 14.1. *If a complex valued additive function f on $\mathcal{G}$ vanishes on a subset $\mathcal{A}$ of $\mathcal{G}$ with $\overline{\mathbf{d}}(\mathcal{A}) > 0$ then the set of $\pi \in \mathcal{P}[i]$ for which $f(\pi) \neq 0$ is a thin set of* *primes.*

Proof. For any z in $\mathcal{A}$, let z' be the unique conjugate of z in $\mathcal{G}^*$. Then $\mathcal{N}(z) = \mathcal{N}(z')$. Thus if $\mathcal{A}'$ is the set of z' as z varies over $\mathcal{A}$, then $\overline{\mathbf{d}}(\mathcal{A}) = \overline{\mathbf{d}}(\mathcal{A}')$. Also, $f(z) = f(z')$ for all z in $\mathcal{A}$, since $f(u) = 0$ for any unit u of $\mathcal{G}$. Replacing $\mathcal{A}$ with $\mathcal{A}'$, we suppose that $\mathcal{A} \subseteq \mathcal{G}^*$.

For any real number $X \geq 1$, let $\mathcal{A}(X)$ be the set of z in $\mathcal{A}$ with $\mathcal{N}(z) \leq X$. Since $\overline{\mathbf{d}}(\mathcal{A}) > 0$, there is a real number $c > 0$ and an infinite sequence $\{X_k\}_{k\geq 1}$ of real numbers $X_k \to +\infty$ such that $|\mathcal{A}(X_k)| \geq cX_k$ for each $k \geq 1$. Moreover, $\mathrm{dia}(f(\mathcal{A}(X_k))) = 0$ for all $k \geq 1$, since f vanishes on $\mathcal{A}$. Thus f is certainly a strongly finitely distributed complex valued additive function on $\mathcal{G}$ and the corollary follows from Theorem 14.1. □

14.1 Reduction to the Small Case

Here we adapt the intuitively appealing elementary method of Erdös [13], pages 15-17. An alternate argument, relying on the Fourier transform, can be given by modifying that on page 159-160 of Elliott and Ryavec [12]. A third argument is also possible following Elliott [9], pages 15 -16. The centerpiece of our argument is the following proposition, which in a sense refines the conclusion of Proposition 7.1.

Lemma 14.1. *Let $\mathcal{Z}$ be a thin set of primes. Then for each $c > 0$ there is a real number $X(c)$ such that for all $X \geq X(c)$, any $\epsilon \in (0, \frac{c}{c+16})$ and any subset A of $\mathcal{G}^*$ with $\mathcal{N}(z) \leq X$ for all $z \in A$ and $|A| \geq cX$ there are $y \in \mathcal{G}^*$ and $\pi, \pi' \in \mathcal{P}[i]$ satisfying*

(i) π and $\pi' \notin \mathcal{Z}$,

(ii) y is coprime to both π and π' and A contains $y\pi$ and $y\pi'$,

(*iii*) $(1+\epsilon)\mathcal{N}(\pi) < \mathcal{N}(\pi')$.

Proof. With $l(c)$ as in Proposition 7.1, let m, l be integers such that $m \geq l \geq 4l(c)$. We then define

$$K_{l,m} \;=\; \sum_{\substack{\pi\in\mathcal{P}[i],\\ l\leq\mathcal{N}(\pi)\leq m.}} \frac{1}{\mathcal{N}(\pi)}\;. \tag{2.208}$$

For the sake of brevity we write K for $K_{l,m}$. Further, let us write ω_K to denote the totally additive function on $\mathcal{G}$ defined by $\omega_K(\pi) = 1$ when $l \leq \mathcal{N}(\pi) \leq m$ and $\omega_K(\pi) = 0$ for all other $\pi \in \mathcal{P}[i]$.

For any $\epsilon > 0$ and $X \geq 1$, let $\mathcal{E}_1(\epsilon, X)$ denote the set of $z \in \mathcal{G}^*$ with $\mathcal{N}(z) \leq X$ such that $\epsilon K \leq |\omega_K(z) - K|$. From the definition of ω_K and (2.37) we have that

$$E(\omega_K, X) = B(\omega_K, X) = K \tag{2.209}$$

for all $X \geq m$. For such X we obtain from Corollary 6.1 applied with $f = \omega_K$ and $\lambda = \epsilon K$ that

$$|\mathcal{E}_1(\epsilon, X)| \;\ll\; \frac{KX}{(\epsilon K)^2} \;\leq\; \frac{cX}{8}\;, \tag{2.210}$$

when m is large enough for a given l, since $K \to +\infty$ with m for a fixed l, by (2.27). Now let $\mathcal{E}_2(X)$ be the set of $z \in \mathcal{G}^*$ with $\mathcal{N}(z) \leq \frac{cX}{8}$. Then $|\mathcal{E}_2(X)| \leq \frac{cX}{8}$, by (2.10). Thus for $X \geq m$ we have

$$|\mathcal{E}_1(\epsilon, X) \cup \mathcal{E}_2(X)| \;\leq\; \frac{cX}{4}\;. \tag{2.211}$$

Let V be the subset of A supplied by Proposition 7.1 applied with $U = A$. We then set $B = V \setminus \mathcal{E}_1(\epsilon, X) \cup \mathcal{E}_2(X)$. On account of (2.211) we have $|B| \geq \frac{cX}{4}$. Moreover, it follows from (i) of Proposition 7.1 and the definitions of the sets $\mathcal{E}_i$ that every $z \in B$ satisfies the conditions

(α) $\pi | z$ and $\mathcal{N}(\pi) \geq l$ implies $\pi \notin \mathcal{Z}$ and π is coprime to $\frac{z}{\pi}$,

(β) $(1-\epsilon)K \leq \omega_K(z) \leq (1+\epsilon)K$,

(γ) $\frac{cX}{8} \leq \mathcal{N}(z) \leq X$.

For any $y \in \mathcal{G}^*$, let $\mathcal{P}_y$ be the set of $\pi \in \mathcal{P}[i]$ such that $y\pi \in B$ and $l \leq \mathcal{N}(\pi) \leq m$. Let Y be the set of y for which $\mathcal{P}_y$ is not empty and, for each $y \in Y$, let π_y be an element of $\mathcal{P}_y$ of minimal norm. Also, let z_y denote $y\pi_y$. Suppose now that for all y in Y we have

$$\mathcal{N}(\pi_y) \leq \mathcal{N}(\pi) \leq (1+\epsilon)\mathcal{N}(\pi_y) \text{ for all } \pi \text{ in } \mathcal{P}_y. \tag{2.212}$$

We shall presently show that for l, m satisfying additional restrictions, and $X \geq m$ sufficiently large, (2.212) implies for all $\epsilon > 0$ the inequality

$$(1-\epsilon)c \leq 16\epsilon\ . \tag{2.213}$$

The above inequality is plainly false for all $\epsilon \in (0, \frac{c}{c+16})$. Therefore, for such ϵ there is always a $y \in Y$ such that (2.212) does not hold. That is, there is a $y \in Y$ and π' in $\mathcal{P}_y$ with $(1+\epsilon)\mathcal{N}(\pi_y) < \mathcal{N}(\pi')$. This mean that the triple y, $\pi = \pi_y$ and π' satisfies (iii) of the proposition. This triple also satisfies (i) and (ii) of the proposition by (α) above applied to $z_y = y\pi_y$ and $z' = y\pi'$. Thus it only remains to verify the inequality (2.213) assuming (2.212). We begin by observing that

$$(1-\epsilon)K|B| \leq \sum_{z\in B} \omega_K(z) \leq \sum_{y\in Y} |\mathcal{P}_y| \ , \tag{2.214}$$

where the first inequality follows from (β) above and the second from the fact that for any $z \in B$ if $\pi|z$ and $l \leq \mathcal{N}(\pi) \leq m$ then $\pi \in \mathcal{P}_y$ for $y = \frac{z}{\pi}$. Then the prime ideal theorem (2.26) tells us that for a given $\epsilon > 0$ the number of $\pi \in \mathcal{P}[i]$ with $t \leq \mathcal{N}(\pi) \leq (1+\epsilon)t$ is asymptotic to

$$\frac{(1+\epsilon)t}{\log((1+\epsilon)t)} - \frac{t}{\log t} \sim \frac{\epsilon t}{\log t} \ , \tag{2.215}$$

as $t \to +\infty$. On account of (2.212) and since $l \leq \mathcal{N}(\pi_y)$ for all $y \in Y$, we then have

$$|\mathcal{P}_y| \leq \frac{2\epsilon \mathcal{N}(\pi_y)}{\log \mathcal{N}(\pi_y)} \tag{2.216}$$

when l sufficiently large.

For any $z = a + ib$ in $\mathcal{G}$, let us set $|z| = |a| + |b|$, as at the end of Section 3. Then we have $\mathcal{N}(z) \leq |z|^2 \leq 2\mathcal{N}(z)$. Using this together with $\mathcal{N}(y)\mathcal{N}(\pi_y) = \mathcal{N}(z_y)$ and bounds for $\mathcal{N}(z_y)$ from (γ) above, we obtain

$$\frac{cX}{8|y|^2} \ \leq \ \mathcal{N}(\pi_y) \ \leq \frac{2X}{|y|^2} \ , \tag{2.217}$$

for all $y \in Y$. Since $l \leq \mathcal{N}(\pi_y) \leq m$, it follows from (2.217) that we also have

$$\frac{cX}{8m} \ \leq \ |y|^2 \ \leq \frac{2X}{l} \ . \tag{2.218}$$

We then conclude using (2.216) through (2.218) that

$$\sum_{y \in Y} |\mathcal{P}_y| \;\leq\; 2\epsilon X \sum_{\substack{y \in \mathcal{G}^*, \\ \frac{cX}{8m} \leq |y|^2 \leq \frac{2X}{l}}} \frac{2}{|y|^2 \log\left(\frac{cX}{8|y|^2}\right)} \, . \tag{2.219}$$

For any integer $k \geq 0$, the number of $y \in \mathcal{G}^*$ such that $|y| = k$ is at most k. Thus on setting $T = \sqrt{\frac{cX}{8}}$ and $c_2 = \frac{4}{\sqrt{c}}$ we see that the sum on the right hand side of the above inequality does not exceed

$$\sum_{\frac{T}{\sqrt{m}} \leq k \leq \frac{c_2 T}{\sqrt{l}}} \frac{1}{k \log\left(\frac{T}{k}\right)} \;=\; \frac{1}{T} \sum_{\frac{1}{\sqrt{m}} \leq \frac{k}{T} \leq \frac{c_2}{\sqrt{l}}} \frac{T}{k \log\left(\frac{T}{k}\right)} \, . \tag{2.220}$$

The right hand side of the above relation is a Riemann sum and when $T \to +\infty$ it converges to the integral

$$\int_{\frac{1}{\sqrt{m}}}^{\frac{c_2}{\sqrt{l}}} \frac{dt}{t \log\left(\frac{1}{t}\right)} = \log\log\sqrt{m} - \log\log\left(\frac{\sqrt{l}}{c_2}\right) \;\leq\; \log\log\sqrt{m} \, , \tag{2.221}$$

when $\sqrt{l} \geq ec_2$. Thus for all sufficiently large X, the sum on the right hand side of (2.220) does not exceed $\log\log m$. For such X we therefore have the bound

$$\sum_{y \in Y} |\mathcal{P}_y| \;\leq\; 2\epsilon X \log\log m \, . \tag{2.222}$$

Substituting this into (2.214) and noting from (2.27) that for a given l and all large enough m we have $K \geq \frac{1}{2}\log\log m$ and that $|B| \geq \frac{cX}{4}$, we obtain (2.213), completing the proof of the proposition.

□

Corollary 14.2. *Suppose that f is a complex valued additive function on $\mathcal{G}$ given by $f(z) = \kappa \log \mathcal{N}(z) + \phi(z)$ for all $z \in \mathcal{G}$, where $\kappa \in \mathbf{C}^*$ and ϕ is a small additive* *function. Then for each $c > 0$ there is a $\delta > 0$ such that for sufficiently large X and any $A \subseteq \mathcal{G}^*$ with $\mathcal{N}(z) \leq X$ for all $z \in A$ and $|A| \geq cX$ we have* $\mathrm{dia}(f(A)) \geq \delta$.

Proof. Let $\epsilon \in (0, \frac{c}{c+32})$ be fixed. Since ϕ is a small additive function, for any real $\eta > 0$, the set $\mathcal{Z}(\eta)$ of $\pi \in \mathcal{P}[i]$ such that $\eta < |\phi(\pi)|$ is a thin set of primes by the remark following Definition 13.2. Let $y \in \mathcal{G}^*$ and $\pi, \pi' \in \mathcal{P}[i]$ be the triple supplied by the proposition applied with $\mathcal{Z} = \mathcal{Z}(\eta)$ and A as given. Then by means of (i), (ii) and (iii) of the proposition we obtain

$$|f(y\pi) - f(y\pi')| = |f(\pi) - f(\pi')| \geq |\kappa| \log(1 + \epsilon) - 2\eta \ . \tag{2.223}$$

Since $\kappa \neq 0$, we may choose η small enough so that $\delta = |\kappa| \log(1 + \epsilon) - 2\eta > 0$. We then have from (2.223) that $\mathrm{dia}(f(A)) \geq \delta > 0$. □

Theorem 14.2. *Every strongly finitely distributed complex valued additive function on $\mathcal{G}$ is necessarily small.*

Proof. Since such an additive function f on $\mathcal{G}$ is in particular finitely distributed, it follows from Theorem 13.1 that there is a $\kappa \in \mathbf{C}$ and a small additive function ϕ such that $f(z) = \kappa \log \mathcal{N}(z) + \phi(z)$, for all z in $\mathcal{G}$. If $\kappa \neq 0$ then the above corollary shows that the requirements of the Definition 14.1 cannot be met for any $c_1 > 0$. Thus $\kappa = 0$ and $f = \phi$, a small additive function.

□

14.2 The Small Case

In this subsection we shall prove the following theorem, which taken together with Theorem 14.2 yields Theorem 14.1.

Theorem 14.3. *If f is a small complex valued additive function on $\mathcal{G}$ that is strongly finitely distributed then the set of $\pi \in \mathcal{P}[i]$ for which $f(\pi) \neq 0$ is a thin set of primes.*

If an additive function f on $\mathcal{G}$ is strongly finitely distributed then so are the additive functions $\mathrm{Re}(f)$ and $\mathrm{Im}(f)$. Moreover, if these functions satisfy the conclusion of Theorem 14.4 then so does f.

For a small additive function f on $\mathcal{G}$, let $\mathcal{Z}$ be a thin set of primes such that $\sum_{\pi \in \mathcal{Z}^c} \frac{|f(\pi)|^2}{\mathcal{N}(\pi)}$ converges. Define the totally additive function g by $g(\pi) = f(\pi)$ when $\pi \notin \mathcal{Z}$ and $g(\pi) = 0$ otherwise. Then Lemma 13.2 tells us that if f is strongly finitely distributed then so is g. Clearly, if g satisfies the conclusion of Theorem 14.4 then so does f.

The preceding remarks reduce the proof of Theorem 14.3 to that of the following theorem.

Theorem 14.4. *Let f be a real valued totally additive function on $\mathcal{G}$ such that*

(i) $\sum_{\pi \in \mathcal{P}[i]} \frac{f(\pi)^2}{\mathcal{N}(\pi)}$ converges,

(ii) f is strongly finitely distributed.

Then the set of $\pi \in \mathcal{P}[i]$ for which $f(\pi) \neq 0$ is a thin set of primes.

Proof. For any integer $l \geq 1$, let f_l denote the totally additive function on $\mathcal{G}$ defined by $f_l(\pi) = f(\pi)$ if $\mathcal{N}(\pi) \leq l$ and $f_l(\pi) = 0$ for all other $\pi \in \mathcal{P}[i]$. Also, let E_l be the finite set of $\pi \in \mathcal{P}[i]$ such that $f_l(\pi) \neq 0$. Then we shall show that the partial sums $\sum_{\pi \in E_l} \frac{1}{\mathcal{N}(\pi)}$ are bounded independently of l. This assertion evidently implies the conclusion of the theorem.

Thus, let us set $\phi_l = f - f_l$, for each $l \geq 1$. Then ϕ_l is also a small totally additive function. Moreover, if

$$S_l = \sum_{\pi \in \mathcal{P}[i]} \frac{\phi_l(\pi)^2}{\mathcal{N}(\pi)} = \sum_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) > l.}} \frac{f(\pi)^2}{\mathcal{N}(\pi)}, \tag{2.224}$$

then $S_l \to 0$ as l tends to $+\infty$ by (i). On account of (ii) there is a $c_1 > 0$ such that f is (c_1, c_2)-finitely distributed for all $c_2 > 0$. Consequently, it follows from Proposition 13.2 applied with $\phi = -\phi_l$ that there is a $c > 0$ such that for any $\epsilon > 0$ there is an $l(\epsilon)$ so that for all $l \geq l(\epsilon)$, $f_l = f - \phi_l$ is (c, ϵ)-finitely distributed.

For given $\epsilon > 0$ and $l \geq l(\epsilon)$, let $\{X_k\}_{k \geq 1}$ be a sequence of real numbers defining the (c, ϵ)-finite distributivity of f_l as in Definition 13.1 and let

$$F_{k,l}(\theta) = \frac{1}{X_k} \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \leq X_k.}} e(\theta f_l(z)) \tag{2.225}$$

for all θ in $\mathbf{R}$ and $k \geq 1$. For each $\theta \in \mathbf{R}$, $z \mapsto e(\theta f_l(z))$ is a totally multiplicative function on $\mathcal{G}$ that takes the value 1 at all $\pi \in \mathcal{P}[i]$ in the complement of E_l. Using Proposition 10.1 we then deduce that

$$\lim_{k \to +\infty} F_{k,l}(\theta) = \alpha_0 \prod_{\pi \in E_l} \left(1 + \frac{e(\theta f(\pi)) - 1}{\mathcal{N}(\pi)}\right) \tag{2.226}$$

for all θ in $\mathbf{R}$.

Let a be a continuous function on $\mathbf{R}$ supported in the interval $[-1, 1]$ with $|a(\theta)| \leq 1$ for all θ in $\mathbf{R}$ and such that $\widehat{a}(t) \geq 0$ for all t in $\mathbf{R}$. Suppose further that there is a $\delta > 0$ such that $\widehat{a}(t) \geq 1$ for $|t| \leq \delta$. For instance, the "hat function" h used in the proof of Lemma 13.2 satisfies these requirements with $\delta = \frac{1}{2}$.

For a given $T > 0$, let $\phi_T(\theta) = \frac{1}{T} a(\frac{\theta}{T})$ and set $\epsilon = \frac{\delta}{T}$, so that we have $\widehat{\phi_T}(t) \geq 1$ for

$|t| \leq \epsilon$. Also, let us write $l(T)$ for $l(\epsilon)$. Then we have from Proposition 13.3 that

$$\liminf_{k\to+\infty} \int_{\mathbf{R}} \phi_T(\theta)|F_{k,l}(\theta)|^2\, d\theta \;\geq\; c^2 \tag{2.227}$$

for any $T > 0$ and all $l \geq l(T)$. Since $|F_{k,l}(\theta)| \leq 1$ for all $\theta \in \mathbf{R}$ and all $k \geq 1$, it follows from the Dominated Convergence Theorem and (2.226) that

$$\alpha_0^2 \int_{\mathbf{R}} \phi_T(\theta) \prod_{\pi\in E_l} \left|1 + \frac{e(\theta f(\pi)) - 1}{\mathcal{N}(\pi)}\right|^2 d\theta \;\geq\; c^2\,. \tag{2.228}$$

For any $l \geq 1$ and all θ in $\mathbf{R}$, we see by means of the inequality (2.142) that

$$\prod_{\pi\in E_l} \left|1 + \frac{e(\theta f(\pi)) - 1}{\mathcal{N}(\pi)}\right| \ll \exp\left(-\sum_{\pi\in E_l} \frac{1 - \mathrm{Re}(e(\theta f(\pi)))}{\mathcal{N}(\pi)}\right)\,. \tag{2.229}$$

Let us write $G_l(\theta)$ for the right hand side of (2.229). Then we have from (2.228) and (2.229) that

$$\int_{\mathbf{R}} \phi_T(\theta) G_l(\theta)^2\, d\theta \;\gg\; c^2 \tag{2.230}$$

for any $T > 0$ and all $l \geq l(T)$. Since $\frac{1-\mathrm{Re}(e(\theta f(\pi)))}{\mathcal{N}(\pi)}$ is always positive, $G_l(\theta)$ decreases with increasing l, for any θ in $\mathbf{R}$. Consequently, (2.230) is valid for all $T > 0$ and all $l \geq 1$.

Let us make the change of variable $\theta \mapsto T\theta$ in the integral on the left hand side of (2.230). Then since $\phi_T(\theta) = \frac{1}{T}a(\frac{\theta}{T})$ and a is supported in $[-1, 1]$ with $|a(\theta)| \leq 1$ for all θ in $\mathbf{R}$, we see, on passing to the limit, that

$$\liminf_{T\to+\infty} \int_{-1}^{1} G_l(T\theta)^2\, d\theta \;\gg\; c^2\,, \tag{2.231}$$

for all $l \geq 1$.

For each integer $n \geq 1$ let us set

$$W_n = \int_{-1}^{1} \cos^{2n}(2\pi\theta)\, d\theta \ . \tag{2.232}$$

Then it follows from (2.231) and Lemma 14.2 below, applied with E_l, $\frac{1}{\mathcal{N}(\pi)}$ and $f(\pi)$ in place of I, c_i and a_i respectively, that

$$W_n + \exp\left(-\frac{1}{n}\sum_{\pi\in E_l}\frac{1}{\mathcal{N}(\pi)}\right) \gg c^2 \tag{2.233}$$

for all integers $l \geq 1$ and $n \geq 1$. The Dominated Convergence Theorem tells us that $W_n \to 0$ as n tends to $+\infty$. Thus if K is the implied constant in (2.233), there is an integer n such that $\frac{Kc^2}{2} \geq W_n$. For such an n we then conclude from (2.233) that

$$n\log\left(\frac{2}{Kc^2}\right) \geq \sum_{\pi\in E_l}\frac{1}{\mathcal{N}(\pi)} \tag{2.234}$$

for all $l \geq 1$, as was to be shown.

□

Lemma 14.2. *Let I be a finite set and let $\{\epsilon_i\}$ and $\{a_i\}$ be sequences of real numbers indexed by I, with $\epsilon_i \geq 0$ for all $i \in I$. Further, let*

$$G(\theta) = \exp\left(-\sum_{i\in I}\epsilon_i(1-\cos(2\pi a_i\theta))\right) \tag{2.235}$$

for all θ in $\mathbf{R}$. Then we have that

$$\limsup_{T\to+\infty}\int_{-1}^{1} G(T\theta)^2\, d\theta \ \leq \ 2\exp\left(-\frac{1}{n}\sum_{i\in I}\epsilon_i\right) + 4W_n \tag{2.236}$$

for all integers $n \geq 1$*, where* W_n *is as in* (2.232)*.*

Proof. The lemma is essentially the content of page 330 of Tenenbaum [43]. We give the proof for completeness.

For the sake of brevity, let us write R to denote $\sum_{i\in I} \epsilon_i$. Then for any integer $n \geq 1$ and $\theta \in \mathbf{R}$ we have

$$\left|\sum_{i\in I} \epsilon_i \cos(2\pi a_i \theta)\right|^{2n} \leq R^{2n-1} \sum_{i\in I} \epsilon_i \cos^{2n}(2\pi a_i \theta) \tag{2.237}$$

on writing $\epsilon_i = \epsilon_i^{\frac{2n-1}{2n}} \epsilon_i^{\frac{1}{2n}}$ and using Hölder's inequality to exponent $2n$.

For any real a we have

$$\lim_{T\to+\infty} \int_{-1}^{1} \cos^{2n}(2\pi aT\theta)\, d\theta \;=\; \lim_{T\to+\infty} \frac{1}{aT} \int_{-aT}^{aT} \cos^{2n}(2\pi\theta)\, d\theta \;= W_n\ , \tag{2.238}$$

since $\theta \mapsto \cos(2\pi\theta)$ is a periodic with period 1. Thus, on replacing θ with $T\theta$ in (2.237), for any $T > 0$, integrating over $\theta \in [-1, 1]$ and passing to the limit we get

$$\limsup_{T\to+\infty} \int_{-1}^{1} \left|\sum_{i\in I} \epsilon_i \cos(2\pi a_i T\theta)\right|^{2n} d\theta \;\leq\; R^{2n} W_n \tag{2.239}$$

For a given $n \geq 1$ and $T > 0$, let $\mathcal{E}_{T,n}$ be the set of $\theta \in [-1, 1]$ such that $\left|\sum_{i\in I} \epsilon_i \cos(2\pi a_i T\theta)\right| \geq (1 - \frac{1}{2n})R$. Then $\mathcal{E}_{T,n}$ is a measurable subset of $\mathbf{R}$ and (2.239) implies that for all sufficiently large T we have

$$\limsup_{T\to+\infty} \mu(\mathcal{E}_{T,n}) \;\leq\; 4W_n\ , \tag{2.240}$$

since $(1 - \frac{1}{2n})^{2n} \geq \frac{1}{4}$, for any $n \geq 1$.

For all θ in $\mathcal{E}_{T,n}^c$, the complement of $\mathcal{E}_{T,n}$ in $[-1,1]$, we have $G(T\theta) \leq \exp(-\frac{R}{2n})$ and for θ in $\mathcal{E}_{T,n}$ we have the trivial bound $G(T\theta) \leq 1$. Consequently,

$$\int_{-1}^{1} G(T\theta)^2 \, d\theta \ \leq \ \exp\left(-\frac{R}{n}\right) \mu(\mathcal{E}_{T,n}^c) + \mu(\mathcal{E}_{T,n}) \ . \tag{2.241}$$

Since $\mu(\mathcal{E}_{T,n}^c) \leq 2$, we obtain (2.236) on passing to the limit in (2.241) and using (2.240).

□

15 An Application of the Large Sieve

Our final auxiliary results are Theorem 15.1 below and its corollaries. This theorem is an analogue for the Gaussian integers of the classical Satz 4.2, page 45 of [38], obtained there as an application of the Selberg Sieve. We will however prove the theorem below by means of the Large Sieve for number fields, as given by J.-P. Serre on page 163 of [42], specialised to $\mathbf{Q}(i)$.

Theorem 15.1. *Let $l \geq 1$ be an integer and let $a_1, \ldots, a_l$ and $b_1, \ldots, b_l$ be Gaussian integers such that*

$$D = \prod_{1 \leq i \leq l} a_i \prod_{1 \leq i < j \leq l} (a_i b_j - a_j b_i) \neq 0 \tag{2.242}$$

and $(a_i, b_i) = 1$ for each i. Also, let $\omega(\pi)$ be the number of roots in $\mathbf{Z}[i]/\pi\mathbf{Z}[i]$ of the polynomial $P(T) = \prod_{1 \leq i \leq l}(a_i T + b_i)$ and suppose that $\omega(\pi) < \mathcal{N}(\pi)$, for each $\pi \in \mathcal{P}[i]$. Finally, for any real $X \geq 1$ let $\mathcal{B}(X)$ be the set of Gaussian integers x with $\mathcal{N}(x) \leq X$ and such that $a_i x + b_i$ is a Gaussian prime for each i, $1 \leq i \leq l$. Then we have that

$$|\mathcal{B}(X)| \;\leq\; \frac{c(l)X}{(\log X)^l} \prod_{\substack{\pi \in \mathcal{P}[i], \\ \pi | D.}} \left(1 - \frac{1}{\mathcal{N}(\pi)}\right)^{\omega(\pi)-l}, \tag{2.243}$$

where $c(l)$ is a real number that depends only on l.

Proof. For any real number $Q \geq 1$ let $\mathcal{A}(X,Q)$ be the set of Gaussian integers x with $\mathcal{N}(x) \leq X$ and such that none of the $a_i x + b_i$, for $1 \leq i \leq l$, are divisible by a $\pi \in \mathcal{P}[i]$ with $\mathcal{N}(\pi) \leq Q$. Then an $x \in \mathcal{B}(X)$ is contained in $\mathcal{A}(X,Q)$ unless there is an i such that $a_i x + b_i = \pi$ for some $\pi \in \mathcal{P}[i]$ with $\mathcal{N}(\pi) \leq Q$. Since the number of such exceptional $x \in \mathcal{B}(X)$ is no more than $l\Pi(Q) \leq 2lQ$ we conclude that for all $Q \geq 1$ we have

$$|\mathcal{B}(X)| \leq |\mathcal{A}(X,Q)| \,+\, 2lQ. \tag{2.244}$$

Let $\mathcal{A}_\pi$ be the image of $\mathcal{A}(X,Q)$ under reduction modulo the prime ideal $\pi\mathbf{Z}[i]$ for each $\pi \in \mathcal{P}[i]$. Then $\mathcal{A}_\pi$ lies in the complement in $\mathbf{Z}[i]/\pi\mathbf{Z}[i]$ of the set of roots of $P(T)$ modulo $\pi\mathbf{Z}[i]$ and consequently we have

$$|\mathcal{A}_\pi| \leq \left(1 - \frac{\omega(\pi)}{\mathcal{N}(\pi)}\right) |\mathbf{Z}[i]/\pi\mathbf{Z}[i]| \;. \tag{2.245}$$

We now apply the theorem from Serre (*loc. cit*). Thus on taking in this theorem $K = \mathbf{Q}(i)$, $\Lambda = \mathbf{Z}[i]$, so that $d = 2$ and $n = 1$, and setting $|x| = \mathcal{N}(x)^{\frac{1}{2}}$, $x_0 = 0$ and, finally, $N = X^{\frac{1}{2}}$ we obtain

$$|\mathcal{A}(X,Q)| \;\leq\; \frac{c\max(X, Q^2)}{L(Q)} \tag{2.246}$$

where c is a real number and

$$L(Q) = \sum_{\substack{z \in \mathcal{G}^*, \mathcal{N}(z) \le Q, \\ z \text{ square-free.}}} \prod_{\substack{\pi \in \mathcal{P}[i], \\ \pi | z.}} \frac{\omega(\pi)}{\mathcal{N}(\pi) - \omega(\pi)} \,. \tag{2.247}$$

Let a be the multiplicative function on $\mathcal{G}$ defined by $a(\pi) = \frac{\omega(\pi)}{\mathcal{N}(\pi)-\omega(\pi)}$ and $a(\pi^k) = 0$ when $k \ge 2$, for all $\pi \in \mathcal{P}[i]$. Also, let

$$A(t) = \sum_{\substack{z \in \mathcal{G}^*, \\ \mathcal{N}(z) \le e^t.}} a(z) \tag{2.248}$$

for any real number t. Then we have

$$L(Q) = A(\log Q) \quad \text{for all real } Q \ge 1 \tag{2.249}$$

and that $A(t)$ is a non-decreasing function of t, since $a(z) \ge 0$ for all $z \in \mathcal{G}^*$. Moreover,

$$\sum_{z \in \mathcal{G}^*} \frac{a(z)}{\mathcal{N}(z)^s} = \prod_{\pi \in \mathcal{P}[i]} \left(1 + \frac{a(\pi)}{\mathcal{N}(\pi)^s}\right) \,, \tag{2.250}$$

where both sides are normally convergent on any closed half-plane in $\mathrm{Re}(s) > 0$. This is easily seen by noting that $a(\pi) \le \frac{2l}{\mathcal{N}(\pi)}$ when $\mathcal{N}(\pi) \ge 2l$, since $\omega(\pi) \le l$ for all $\pi \in \mathcal{P}[i]$. Thus if we write $F(s)$ to denote the left hand side of (2.250) then

$$F(\sigma) = \int_0^\infty e^{-\sigma t} dA(t) \;\text{ for all real } \sigma > 0. \tag{2.251}$$

We now recall that $G(s)$ denotes $\sum_{z \in \mathcal{G}^*} \frac{1}{\mathcal{N}(z)^s}$. Then by means of the Euler product relation for $G(s)$ and (2.250) we obtain that

$$\frac{F(s)}{G(s+1)^l} = \prod_{\pi \in \mathcal{P}[i]} \left(1 + \frac{a(\pi)}{\mathcal{N}(\pi)^s}\right) \left(1 - \frac{1}{\mathcal{N}(\pi)^{s+1}}\right)^l \tag{2.252}$$

when $\mathrm{Re}(s) > 0$.

If $\pi \in \mathcal{P}[i]$ does not divide D we have $\omega(\pi) = l$ since for such π all the $b_i a_i^{-1}$ are distinct modulo $\pi\mathbf{Z}[i]$. This is in particular the case when $\mathcal{N}(\pi)$ is sufficiently large. Therefore on writing $B_\pi(s)$ for the general term of the product on the right hand side of (2.252) and using (2.142) we see that

$$|B_\pi(s)| \leq \exp\left(\frac{l^2}{(\mathcal{N}(\pi) - l)\mathcal{N}(\pi)^{\sigma+1}} + \frac{3(4l^2+1)}{2\mathcal{N}(\pi)^{2\sigma+2}}\right), \tag{2.253}$$

where $\sigma = \mathrm{Re}(s)$, when $\mathcal{N}(\pi)$ is sufficiently large. It follows that the product on the right hand side of (2.252) converges uniformly on any closed half plane in $\mathrm{Re}(s) > -\frac{1}{2}$. Hence if $H(s)$ denotes the right hand side of (2.252) then $H(s)$ is holomorphic on $\mathrm{Re}(s) > -\frac{1}{2}$ and we have

$$F(s) = H(s)G(s+1)^l\,. \tag{2.254}$$

Since $G(s)$ has a simple pole at $s = 1$ with residue $\frac{\pi}{4}$ the relation above certainly implies that

$$F(\sigma) \sim \left(\frac{\pi}{4}\right)^l \frac{H(0)}{\sigma^l} \quad \text{as } \sigma \to 0^+. \tag{2.255}$$

An application of Karamata's Tauberian Theorem (see Theorem 5, page 222 of [43]) now shows that $A(t) \sim \left(\frac{\pi}{4}\right)^l \frac{H(0)t^l}{l!}$ as $t \to +\infty$, from which and (2.249) it then follows that

$$L(Q) \sim \left(\frac{\pi}{4}\right)^l \frac{H(0)(\log Q)^l}{l!} \quad \text{as } Q \to +\infty. \tag{2.256}$$

A classical inequality of Bernoulli's tells us that $(1 + nu) \leq (1 + u)^n$ for any real number $u \geq -1$ and an integer $n \geq 0$. This is easily checked by induction on n for a given u. Applying this inequality with $n = \omega(\pi)$ and $u = -\frac{1}{\mathcal{N}(\pi)}$ we obtain

$$1 + a(\pi) = \frac{1}{1 - \frac{\omega(\pi)}{\mathcal{N}(\pi)}} \geq \left(1 - \frac{1}{\mathcal{N}(\pi)}\right)^{-\omega(\pi)}, \tag{2.257}$$

for all $\pi \in \mathcal{P}[i]$. It then follows that

$$H(0) = \prod_{\pi \in \mathcal{P}[i]} (1 + a(\pi)) \left(1 - \frac{1}{\mathcal{N}(\pi)}\right)^l \geq \prod_{\substack{\pi \in \mathcal{P}[i], \\ \pi | D.}} \left(1 - \frac{1}{\mathcal{N}(\pi)}\right)^{l-\omega(\pi)}, \tag{2.258}$$

since $\omega(\pi) = l$ when π does not divide D. The conclusion of the theorem now results on combining (2.258) and (2.256) with (2.246) and (2.244) and setting $Q = X^{\frac{1}{2}}$.

□

Corollary 15.1. *For any real number $X \geq 1$ and any $z \in \mathcal{G}$, let $M(X, z)$ denote the number of pairs (π, π') of π, π' in $\mathcal{P}[i]$ such that $\pi' + 1 = z\pi$ with $N(\pi') \leq X$. Then we have that*

$$M(X, z) \ll \frac{X}{\phi(z)(\log X)^2}. \tag{2.259}$$

Proof. Since $X \geq 1$ and $N(\pi') \leq X$, we have $\mathcal{N}(\pi) \leq \frac{4X}{\mathcal{N}(z)}$. We apply the theorem with $l = 2$ and $a_1 = 1, b_1 = 0, a_2 = z, b_2 = -1$ and X in the statement of theorem replaced with $\frac{4X}{\mathcal{N}(z)}$. Then $\omega(\pi) = 1$ for all $\pi \in \mathcal{P}[i]$ that divide z and $D = z$.

Consequently, we have

$$\prod_{\substack{\pi \in \mathcal{P}[i],\\ \pi | D.}} \left(1 - \frac{1}{\mathcal{N}(\pi)}\right)^{l-\omega(\pi)} = \frac{\phi(z)}{\mathcal{N}(z)} \,. \tag{2.260}$$

The bound on $M(X, z)$ now follows from (2.243).

□

Corollary 15.2. *For any real number $X \geq 1$ and any $z \in \mathcal{G}$, let $N(X, z)$ denote the number of pairs (π, π') of π, π' in $\mathcal{P}[i]$ satisfying the conditions $\pi' + 1 = z(\pi + 1)$, $N(\pi') \leq X$ and $X^{\frac{1}{6}} \leq \mathcal{N}(\pi) \leq X^{\frac{1}{5}}$. Then for all sufficiently large X we have we have that*

$$N(X, z) \ll \frac{X}{\mathcal{N}(z)(\log X)^2} \prod_{\substack{\pi \in \mathcal{P}[i],\\ \pi | z(z-1).}} \left(1 - \frac{1}{N(\pi)}\right)^{-1} . \tag{2.261}$$

Proof. Similar to the preceding corollary. Since $\sqrt{\mathcal{N}(\pi + 1)} \geq \sqrt{\mathcal{N}(\pi)} - 1$ we have $\mathcal{N}(\pi + 1) \geq \frac{X^{\frac{1}{6}}}{4}$ when $X \geq 2^{12}$. Since also $\mathcal{N}(\pi' + 1) \leq 4X$ we conclude that $N(X, z) \neq 0$ only if $\mathcal{N}(z) \leq 16X^{\frac{5}{6}}$. For such z the relations $\pi' = z\pi + z - 1$ and $N(\pi') \leq X$ imply that $\mathcal{N}(\pi) \leq \frac{4X}{\mathcal{N}(z)}$, since X is large enough. When $z = 1$ we evidently have $N(X, z) \leq X^{\frac{1}{5}}$ and (2.261) is trivial. Thus supposing $z \neq 1$ we apply the theorem with $a_1 = 1, b_1 = 0, a_2 = z, b_2 = z - 1$ and X in the statement of theorem replaced with $\frac{4X}{\mathcal{N}(z)}$. On noting that then $(z, z - 1) = 1$, $D = z^2(z - 1) \neq 0$ and $\omega(\pi) = 1$ for all $\pi | D$, (2.261) results from (2.243).

□

16 Proof of Theorem 9.1

We follow [9] closely. It may be useful to read the summary of the proof given in Section 9 before studying the detailed presentation given here.

Let $\mathcal{E}$ be the set of z in $\mathcal{G}^*$ such that $\pi' + 1 = z(\pi + 1)$ for some $\pi, \pi' \in \mathcal{P}[i]$, with $\pi + 1$ coprime to z and let $\overline{\mathbf{d}}(\mathcal{E})$ be the upper asymptotic density of $\mathcal{E}$ (see (2.13)).

Proposition 16.1. *We have that* $\overline{\mathbf{d}}(\mathcal{E}) > 0$.

Proof. For any real number $X \geq 1$, let $\mathcal{D}(X)$ be the set of $z \in \mathcal{G}^*$ such that there are $\pi, \pi' \in \mathcal{P}[i]$ satisfying the conditions

(α) $\pi' + 1 = z(\pi + 1)$ and $\pi + 1$ coprime to z,

(β) $\mathcal{N}(\pi') \leq X$, $X^{\frac{1}{6}} \leq \mathcal{N}(\pi) \leq X^{\frac{1}{5}}$.

Then $\mathcal{D}(X) \subseteq \mathcal{E}$ for all $X \geq 1$. To show that $\overline{\mathbf{d}}(\mathcal{E}) > 0$ it suffices to show that there is a real number $c > 0$ such for all X sufficiently large we have

$$\sum_{\substack{z \in \mathcal{D}(X), \\ X^{\frac{3}{5}} < \mathcal{N}(z) \leq X^{\frac{11}{12}}.}} \frac{1}{\mathcal{N}(z)} \geq c \log X. \tag{2.262}$$

Indeed, for any real $Y \geq 1$, let $D(Y)$ be the number of $z \in \mathcal{D}(X)$ with $\mathcal{N}(z) \leq Y$. Then we see from (2.262) that

$$\frac{D(X^{\frac{11}{12}})}{X^{\frac{11}{12}}} - \frac{D(X^{\frac{3}{5}})}{X^{\frac{3}{5}}} + \int_{X^{\frac{3}{5}}}^{X^{\frac{11}{12}}} \frac{D(Y)}{Y^2}\, dY \geq c \log X\ , \tag{2.263}$$

since the sum on the left hand side of (2.262) is the same as the left hand side of (2.263), after an integration by parts. Hence if $\beta(X)$ is $\sup \frac{D(Y)}{Y}$ with Y varying in $(X^{\frac{3}{5}}, X^{\frac{11}{12}}]$, we have from (2.263) that

$$\beta(X)\left(1+\left(\frac{11}{12}-\frac{3}{5}\right)\log X\right)\geq c\log X\ . \tag{2.264}$$

Since $\overline{\mathbf{d}}(\mathcal{E}) \geq \limsup_{X\to+\infty}\beta(X)$, we conclude on passing to the limit in (2.264) that $\overline{\mathbf{d}}(\mathcal{E}) > 0$.

We will prove (2.262) via a typical application of the Cauchy-Schwarz inequality. Thus, let $\mathcal{A}(X,z)$ be the set of pairs (π',π) satisfying the conditions (α) and (β) above for a given $z \in \mathcal{D}(X)$. Then with $A(X,z) = |\mathcal{A}(X,z)|$ we shall verify that

$$\sum_{z\in\mathcal{G}^*} A(X,z) \gg \frac{X}{\log X}\ . \tag{2.265}$$

In effect, it follows from (α) and (β) above that the left hand side of (2.265) is the same as

$$\sum_{\substack{\pi\in\mathcal{P}[i],\\ X^{\frac{1}{6}}\leq\mathcal{N}(\pi)\leq X^{\frac{1}{5}}.}}\ \sum_{\substack{\pi'\in\mathcal{P}[i],\mathcal{N}(\pi')\leq X,\\ \pi+1|\pi'+1,\\ (\frac{\pi'+1}{\pi+1},\pi+1)=1.}} 1\ . \tag{2.266}$$

Using the Möbius inversion formula (2.6) we replace the inner sum in the above expression with

$$\sum_{\substack{\pi'\in\mathcal{P}[i],\mathcal{N}(\pi')\leq X,\\ \pi+1|\pi'+1.}}\ \sum_{\substack{y|(\frac{\pi'+1}{\pi+1},\pi+1),\\ y\in\mathcal{G}^*.}} \mu(y)\ . \tag{2.267}$$

Interchanging summations we then see that (2.266) is the same as

$$\sum_{\substack{\pi\in\mathcal{P}[i],\\ X^{\frac{1}{6}}\leq\mathcal{N}(\pi)\leq X^{\frac{1}{5}}.}}\ \sum_{\substack{y|\pi+1,\\ y\in\mathcal{G}^*.}} \mu(y) \sum_{\substack{\pi'\in\mathcal{P}[i],\mathcal{N}(\pi')\leq X,\\ \pi'\equiv-1 \bmod y(\pi+1).}} 1\ . \tag{2.268}$$

Anticipating an application of the Bombieri-Vinogradov Theorem to treat (2.268) let us note that

$$\sum_{\substack{\pi\in\mathcal{P}[i],\\ X^{\frac{1}{6}}\le\mathcal{N}(\pi)\le X^{\frac{1}{5}}.}}\ \sum_{\substack{y|\pi+1,\\ y\in\mathcal{G}^*.}}\frac{\mu(y)\mathrm{li}(X)}{\phi(y(\pi+1))} = \mathrm{li}(X)\sum_{\substack{\pi\in\mathcal{P}[i],\\ X^{\frac{1}{6}}\le\mathcal{N}(\pi)\le X^{\frac{1}{5}}.}}\frac{1}{\mathcal{N}(\pi+1)}\ . \tag{2.269}$$

In effect, when $y|\pi+1$ we have $\phi(y(\pi+1)) = \mathcal{N}(y)\phi(\pi+1)$. We obtain (2.269) on using this in the left hand side of (2.269) and remarking that

$$\sum_{\substack{y|\pi+1,\\ y\in\mathcal{G}^*.}}\frac{\mu(y)}{\mathcal{N}(y)} = \frac{\phi(\pi+1)}{\mathcal{N}(\pi+1)}\ . \tag{2.270}$$

On subtracting the left hand side of (2.269) from (2.268) and recalling the definition of $E^*(X, y(\pi+1))$ from Section 5 (see 2.34), we conclude using triangle inequality that (2.268) is bounded below by

$$\sum_{\substack{\pi\in\mathcal{P}[i],\\ X^{\frac{1}{6}}\le\mathcal{N}(\pi)\le X^{\frac{1}{5}}.}}\frac{\mathrm{li}(X)}{\mathcal{N}(\pi+1)} - \sum_{\substack{\pi\in\mathcal{P}[i],\\ X^{\frac{1}{6}}\le\mathcal{N}(\pi)\le X^{\frac{1}{5}}.}}\ \sum_{\substack{y|\pi+1,\\ y\in\mathcal{G}^*.}} E^*(X, y(\pi+1))\ . \tag{2.271}$$

Let us dispose of the second term in (2.271) first. We divide the $y|\pi+1$ in this term according as $\mathcal{N}(y) \le (\log X)^3$ and $\mathcal{N}(y) > (\log X)^3$. Using the trivial estimate in (2.35) the latter case we deduce that the second term of (2.271) is majorised by

$$\sum_{\substack{y \in \mathcal{G}^*, \\ \mathcal{N}(y) \leq (\log X)^3.}} \sum_{\substack{\pi \in \mathcal{P}[i], \\ X^{\frac{1}{6}} \leq \mathcal{N}(\pi) \leq X^{\frac{1}{5}}.}} E^*(X, y(\pi+1)) + \sum_{\substack{y,w \in \mathcal{G}^*, \\ \mathcal{N}(y^2 w) \leq 16 X^{\frac{2}{5}}, \\ \mathcal{N}(y) > (\log x)^3.}} \frac{X \log\log X}{\mathcal{N}(y^2 w)}, \quad (2.272)$$

on writing $y(\pi+1)$ as $y^2 w$, possible because $y|\pi+1$, and remarking that since $\mathcal{N}(\pi+1) \leq 4X^{\frac{1}{5}}$, we have $\mathcal{N}(y^2 w) \leq 16X^{\frac{2}{5}}$. When, on the other hand, $y \leq (\log X)^3$ we have $\mathcal{N}(y(\pi+1)) \leq 4X^{\frac{1}{5}}(\log X)^3$. Thus for a fixed y, we may estimate the inner sum in the first term of (2.272) by

$$\sum_{\substack{\pi \in \mathcal{P}[i], \\ X^{\frac{1}{6}} \leq \mathcal{N}(\pi) \leq X^{\frac{1}{5}}.}} E^*(X, y(\pi+1)) \leq \sum_{\substack{v \in \mathcal{G}^*, \\ \mathcal{N}(v) \leq 4X^{\frac{1}{5}} (\log X)^3.}} E^*(X, v) \ll \frac{X}{(\log X)^5}, \quad (2.273)$$

by means of (2.36). Consequently, we obtain

$$\sum_{\substack{y \in \mathcal{G}^*, \\ \mathcal{N}(y) \leq (\log X)^3.}} \sum_{\substack{\pi \in \mathcal{P}[i], \\ X^{\frac{1}{6}} \leq \mathcal{N}(\pi) \leq X^{\frac{1}{5}}.}} E^*(X, y(\pi+1)) \ll \frac{X}{(\log X)^2}. \quad (2.274)$$

Next, we note using $\mathcal{N}(y^2 w) = \mathcal{N}(y)^2 \mathcal{N}(w)$ that

$$\sum_{\substack{y,w \in \mathcal{G}^*, \\ \mathcal{N}(y^2 w) \leq 16 X^{\frac{2}{5}}, \\ \mathcal{N}(y) > (\log x)^3.}} \frac{1}{\mathcal{N}(y^2 w)} \leq \sum_{\substack{w \in \mathcal{G}^*, \\ \mathcal{N}(w) \leq X.}} \frac{1}{\mathcal{N}(w)} \sum_{\substack{y \in \mathcal{G}^*, \\ \mathcal{N}(y) > (\log X)^3.}} \frac{1}{\mathcal{N}(y)^2} \ll \frac{1}{(\log X)^2}, \quad (2.275)$$

taking account of (2.15) and (2.16). It follows from (2.274) and (2.275) that

$$\sum_{\substack{\pi\in\mathcal{P}[i],\\ X^{\frac{1}{6}}\le\mathcal{N}(\pi)\le X^{\frac{1}{5}}.}} \sum_{\substack{y|\pi+1,\\ y\in\mathcal{G}^*.}} E^*(X,y(\pi+1)) \ll \frac{X\log\log X}{(\log X)^2}\,. \tag{2.276}$$

Also, since $\mathrm{li}(X)\sim\frac{X}{\log X}$ we have using (2.27) that

$$\sum_{\substack{\pi\in\mathcal{P}[i],\\ X^{\frac{1}{6}}\le\mathcal{N}(\pi)\le X^{\frac{1}{5}}.}} \frac{\mathrm{li}(X)}{\mathcal{N}(\pi)} \sim \log\left(\frac{6}{5}\right)\frac{X}{\log X}\,. \tag{2.277}$$

Finally, on recalling that (2.271) is a lower bound for (2.268) and hence for the left hand side of (2.265), we conclude from (2.277) and (2.276) that (2.265) indeed holds.

The condition (β) and (2.2) give $\mathcal{N}(\pi+1)\ge\frac{X^{\frac{1}{6}}}{4}$ and $\mathcal{N}(\pi'+1)\le 4X$ when X is sufficiently large. Therefore $A(X,z)\ne 0$ only if $\mathcal{N}(z)\le 16X^{\frac{5}{6}}\le X^{\frac{11}{12}}$, when X is large enough. Also, when $\mathcal{N}(z)\le X^{\frac{3}{5}}$ we have from the condition (α) that $\mathcal{N}(\pi'+1)\le X^{\frac{4}{5}}$. Consequently, we have

$$\sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le X^{\frac{3}{5}}.}} A(X,z)\le\Pi(X^{\frac{4}{5}})\Pi(4X^{\frac{1}{5}})\ll\frac{X}{(\log X)^2}\,. \tag{2.278}$$

On combining the preceding remarks with (2.265) we obtain

$$\sum_{\substack{z\in\mathcal{G}^*,\\ X^{\frac{3}{5}}<\mathcal{N}(z)\le X^{\frac{11}{12}}.}} A(X,z)\gg\frac{X}{\log X}\,. \tag{2.279}$$

Let us denote by S the sum on the left hand side of (2.262). Then on writing $A(X,z)$ in the left hand side of (2.279) as $\mathcal{N}(z)^{-\frac{1}{2}}\mathcal{N}(z)^{\frac{1}{2}}A(X,z)$ and combining an application of the Cauchy-Schwarz inequality with (2.279) we deduce that

$$\frac{X^2}{(\log X)^2} \ll S \sum_{\substack{z\in\mathcal{G}^*,\\ X^{\frac{3}{5}}<\mathcal{N}(z)\le X^{\frac{11}{12}}.}} \mathcal{N}(z)A(X,z)^2, \tag{2.280}$$

since $z \in \mathcal{D}(X)$ is the same as $A(X,z) \neq 0$. Plainly, $A(X,z)$ does not exceed $N(X,z)$ of Corollary 15.2. Thus on using the upper bound supplied by this corollary for $N(X,z)$ in (2.280) and dividing both sides of the resulting relation by $\frac{X^2}{(\log X)^3}$ we obtain

$$\log X \ll \frac{S}{\log X} \sum_{\substack{z\in\mathcal{G}^*,\\ X^{\frac{3}{5}}<\mathcal{N}(z)\le X^{\frac{11}{12}}.}} \frac{1}{\mathcal{N}(z)} \prod_{\substack{\pi\in\mathcal{P}[i],\\ \pi|z(z-1).}} \left(1-\frac{1}{N(\pi)}\right)^{-2}. \tag{2.281}$$

Let us estimate the sum on the right hand side of (2.281). When $\mathcal{N}(z) \geq 4$ we see that $\mathcal{N}(z) \geq \sqrt{\mathcal{N}(z)\mathcal{N}(z-1)}$ and that $\mathcal{N}(z-1) \neq 0$. Thus if for any z in $\mathcal{G}$ we set

$$b(z) = \frac{1}{\mathcal{N}(z)^{\frac{1}{2}}} \prod_{\substack{\pi\in\mathcal{P}[i],\\ \pi|z.}} \left(1-\frac{1}{N(\pi)}\right)^{-2} \tag{2.282}$$

then since z and $z-1$ are coprime when $z, z-1 \neq 0$, we have that

$$\sum_{\substack{z\in\mathcal{G}^*,\\ X^{\frac{3}{5}}<\mathcal{N}(z)\le X^{\frac{11}{12}}.}} \frac{1}{\mathcal{N}(z)} \prod_{\substack{\pi\in\mathcal{P}[i],\\ \pi|z(z-1).}} \left(1-\frac{1}{N(\pi)}\right)^{-2} \leq \sum_{\substack{z\in\mathcal{G}^*,\\ X^{\frac{3}{5}}<\mathcal{N}(z)\le X^{\frac{11}{12}}.}} b(z)b(z-1)\ , \tag{2.283}$$

for all large X. Since $\mathcal{N}(z-1) \leq 4\mathcal{N}(z)$ when $\mathcal{N}(z) \geq 1$, an application of the Cauchy-Schwarz inequality together with positivity of $b(z)$ now shows that

$$\sum_{\substack{z\in\mathcal{G}^*,\\ X^{\frac{3}{5}}<\mathcal{N}(z)\le X^{\frac{11}{12}}.}} b(z)b(z-1) \;\le\; \sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le 4X.}} b(z)^2\,. \tag{2.284}$$

The function $z\mapsto b(z)^2$ is a multiplicative function on $\mathcal{G}$. Moreover, for any $\pi\in\mathcal{P}[i]$ we have

$$\sum_{k\ge 0} b(\pi^k)^2 = 1+\frac{1}{\mathcal{N}(\pi)}\left(1-\frac{1}{\mathcal{N}(\pi)}\right)^{-5}\,, \tag{2.285}$$

since $b(1)=1$ and $b(\pi^k)^2=\frac{1}{\mathcal{N}(\pi)^k}\left(1-\frac{1}{\mathcal{N}(\pi)}\right)^{-4}$ when $k\ge 1$. Therefore, we have

$$\sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le 4X.}} b(z)^2 \;\le\; \prod_{\substack{\pi\in\mathcal{P}[i],\\ \mathcal{N}(\pi)\le 4X}}\left(1+\frac{1}{\mathcal{N}(\pi)}\left(1-\frac{1}{\mathcal{N}(\pi)}\right)^{-5}\right)\,. \tag{2.286}$$

For any $\pi\in\mathcal{P}[i]$ we see using the elementary inequality $1+u\le\exp(u)$, valid for any real u, that

$$1+\frac{1}{\mathcal{N}(\pi)}\left(1-\frac{1}{\mathcal{N}(\pi)}\right)^{-5} \;\le\; \exp\left(\frac{1}{\mathcal{N}(\pi)}+O\left(\frac{1}{\mathcal{N}(\pi)^2}\right)\right)\,. \tag{2.287}$$

On multiplying both side of this inequality over all $z\in\mathcal{G}^*$ with $\mathcal{N}(z)\le 4X$, using (2.27) and combining the result with (2.286) we obtain

$$\sum_{\substack{z\in\mathcal{G}^*,\\ \mathcal{N}(z)\le 4X.}} b(z)^2 \ll \log X\,. \tag{2.288}$$

Finally, on reading the above bound together with (2.286), (2.284), (2.283) and (2.279), we conclude that $\log X\ll S$, which is (2.262) when one takes the implied constant for c and recalls that S is the sum on the left hand side of (2.262).

□

Our second proposition, given below, says, intuitively speaking, that shifted primes behave like generic Gaussian integers (compare proof of Corollary 7.1).

Given a y in $\mathcal{G}^*$, $A \geq 1$ a real number and $\mathcal{Z}$ a thin set of prime, let $\mathcal{S} = \mathcal{S}(y, A, \mathcal{Z})$ be the set of elements of $\mathcal{G}^*$ that can be written as $(1+i)yw$, where w in $\mathcal{G}^*$ satisfies the condition

(γ) $\pi \in \mathcal{P}[i]$ and $\pi | w \implies \pi \nmid (1+i)y$, $\mathcal{N}(\pi) > A$, $\pi \notin \mathcal{Z}$ and $\pi^2 \nmid w$.

Let $\mathcal{T} = \mathcal{T}(y, A, \mathcal{Z})$ be the set of $\pi' \in \mathcal{P}[i]$ such that $\pi' + 1$ is in $\mathcal{S}$.

Proposition 16.2. *For any y in $\mathcal{G}^*$ and a thin set of primes $\mathcal{Z}$ the set $\mathcal{T}$ is infinite when A is sufficiently large.*

Proof. Let $T(X)$ be the number of π' in $\mathcal{T}$ with $\mathcal{N}(\pi') \leq X$, for any real $X \geq 1$ and let us obtain a lower bound for $T(X)$, for large X. To this end, let $\mathcal{Z}' = \mathcal{Z} \cup \{1+i\}$ and for any real number $B \geq 1$ let us set

$$Q = y \prod_{\substack{z \in \mathcal{Z}', \\ \mathcal{N}(z) \leq B.}} z \prod_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) \leq A.}} \pi \,. \tag{2.289}$$

Let $T_1(X)$ be the number of π' in $\mathcal{P}[i]$ with $\mathcal{N}(\pi') \leq X$ and such that $\pi'+1 = (1+i)yu$ where $u \in \mathcal{G}^*$ and is coprime to Q. Also, let $T_2(X)$ be the number of π' in $\mathcal{P}[i]$ with $\mathcal{N}(\pi') \leq X$ such that $\pi'+1$ is divisible by $(1+i)yz$ for some z in $\mathcal{Z}'$ with $\mathcal{N}(z) > B$. Finally, let $T_3(X)$ be the number of π' in $\mathcal{P}[i]$ with $\mathcal{N}(\pi') \leq X$ and such that $\pi' + 1$ is divisible by $(1+i)y\pi^2$ for some $\pi \in \mathcal{P}[i]$ with $\mathcal{N}(\pi) > A$. Then we evidently have

$$T(X) \geq T_1(X) - T_2(X) - T_3(X) \tag{2.290}$$

for all $X \geq 1$. The prime ideal theorem for arithmetical progressions (2.29) easily gives the asymptotic behaviour of $T_1(X)$ as $X \to +\infty$. To see this, let us set $D = (1+i)y$ and set

$$Q^* = D \prod_{\substack{\pi | Q, \\ \pi \nmid D.}} \pi \ . \tag{2.291}$$

Then u in $\mathcal{G}^*$ is coprime to Q if and only it is coprime to Q^* and we have $\frac{Q^*}{D}$ and D are coprime. Now by means of the Möbius inversion formula (2.6) we have

$$T_1(X) = \sum_{\substack{\pi' \in \mathcal{P}[i], \mathcal{N}(\pi') \leq X, \\ D | \pi' + 1.}} \sum_{\substack{v \in \mathcal{G}^*, \\ v | (\frac{\pi'+1}{D}, Q^*).}} \mu(v) \ , \tag{2.292}$$

since $T_1(X)$ counts π' such that $\pi' + 1 = Du$ with $(u, Q) = 1$. An interchange of summations yields

$$T_1(X) = \sum_{\substack{v \in \mathcal{G}^*, \\ v | Q^*.}} \mu(v) \sum_{\substack{\pi' \in \mathcal{P}[i], \mathcal{N}(\pi') \leq X, \\ \pi' \equiv -1 \bmod Dv.}} 1 \ . \tag{2.293}$$

From (2.29) we then obtain

$$T_1(X) \sim \mathrm{li}(X) \sum_{\substack{v \in \mathcal{G}^*, \\ v | Q^*.}} \frac{\mu(v)}{\phi(Dv)} \ , \tag{2.294}$$

as $X \to +\infty$. Since $\frac{Q^*}{D}$ and D are coprime, since to every $v \in \mathcal{G}^*$ satisfying $v | Q^*$ there corresponds a unique pair of (x, z) satisfying the conditions x, z in $\mathcal{G}^*$, $v = xz$

and $x|D$, $z|\frac{Q^*}{D}$. Then we have $\mu(xz) = \mu(x)\mu(z)$ and $\phi(Dv) = \mathcal{N}(x)\phi(D)\phi(z)$. Therefore

$$\sum_{\substack{v\in\mathcal{G}^*,\\ v|Q^*.}} \frac{\mu(v)}{\phi(Dv)} = \frac{1}{\phi(D)} \sum_{\substack{x\in\mathcal{G}^*,\\ x|D.}} \frac{\mu(x)}{\mathcal{N}(x)} \sum_{\substack{z\in\mathcal{G}^*,\\ z|\frac{Q^*}{D}.}} \frac{\mu(z)}{\phi(z)} \,. \tag{2.295}$$

The first sum on the right hand side of the above relation evaluates to $\frac{\phi(D)}{\mathcal{N}(D)}$. On writing the second sum on the right hand side of (2.295) as a product over primes $\pi \in \mathcal{P}[i]$ and recalling the definitions of Q^* and D we then conclude from (2.294) that

$$T_1(X) \sim \frac{\mathrm{li}(X)}{2\mathcal{N}(y)} \prod_{\substack{\pi|Q,\\ \pi\nmid(1+i)y.}} \left(1 - \frac{1}{\mathcal{N}(\pi)-1}\right) . \tag{2.296}$$

Turning now to $T_2(X)$ we have

$$T_2(X) = \sum_{\substack{z\in\mathcal{Z}',\\ \mathcal{N}(z)>B.}} \sum_{\substack{\pi'\in\mathcal{P}[i],\mathcal{N}(\pi')\le X,\\ \pi'\equiv -1 \bmod Dz.}} 1 \tag{2.297}$$

Let α be in $(0, 1)$. Then the Brun-Titchmarsh theorem (2.31) tell us that

$$\sum_{\substack{\pi'\in\mathcal{P}[i],\mathcal{N}(\pi')\le X,\\ \pi'\equiv -1 \bmod Dz.}} 1 \le \frac{c(\alpha)X}{\phi(Dz)\log X} \tag{2.298}$$

for any z in $\mathcal{G}^*$ with $\mathcal{N}(Dz) \le X^\alpha$. Applying this to $z \in \mathcal{Z}'$ and recalling that since such a z is a Gaussian prime we have $\phi(Dz) \ge \phi(z) = \mathcal{N}(z) - 1$, we obtain

$$\sum_{\substack{z\in\mathcal{Z}',\\ B<\mathcal{N}(z)\le\frac{X^\alpha}{\mathcal{N}(D)}.}} \sum_{\substack{\pi'\in\mathcal{P}[i],\mathcal{N}(\pi')\le X,\\ \pi'\equiv -1 \bmod Dz.}} 1 \le \frac{c(\alpha)X}{\log X} \sum_{\substack{z\in\mathcal{Z}',\\ B<\mathcal{N}(z).}} \frac{1}{\mathcal{N}(z)-1} \; . \tag{2.299}$$

When $z \in \mathcal{Z}'$ satisfies $X^\alpha < \mathcal{N}(Dz)$, we switch to the complementary divisor. That is, for any π' in $\mathcal{P}[i]$ with $\mathcal{N}(\pi') \le X$ such that $\pi'+1$ is divisible by Dz, we set $\pi'+1 = Dzu$ and note that $\mathcal{N}(u) \le 4X^{1-\alpha}$. Then on recalling the notation introduced in Corollary 15.1 we have

$$\sum_{\substack{z\in\mathcal{Z}',\\ X^\alpha<\mathcal{N}(Dz).}} \sum_{\substack{\pi'\in\mathcal{P}[i],\mathcal{N}(\pi')\le X,\\ \pi'\equiv -1 \bmod Dz.}} 1 \le \sum_{\substack{u\in\mathcal{G},\\ \mathcal{N}(u)\le 4X^{1-\alpha}.}} M(X,Du) \; . \tag{2.300}$$

On using the bound supplied by (2.259) for $M(X,Du)$ we see that the right hand side of (2.300) is majorised by

$$\sum_{\substack{u\in\mathcal{G},\\ \mathcal{N}(u)\le 4X^{1-\alpha}.}} M(X,Du) \ll \frac{X}{(\log X)^2} \sum_{\substack{u\in\mathcal{G},\\ \mathcal{N}(u)\le 4X^{1-\alpha}.}} \frac{1}{\phi(u)} \ll \frac{(1-\alpha)X}{\log X} \; , \tag{2.301}$$

where the second inequality results on remarking that $u \mapsto \frac{1}{\phi(u)}$ is a positive multiplicative function on $\mathcal{G}$ and we $\sum_{k\ge 0} \frac{1}{\phi(\pi^k)} = 1 + \frac{1}{\mathcal{N}(\pi)}$ for any $\pi \in \mathcal{P}[i]$ so that

$$\sum_{\substack{u\in\mathcal{G},\\ \mathcal{N}(u)\le 4X^{1-\alpha}.}} \frac{1}{\phi(u)} \le \prod_{\substack{\pi\in\mathcal{P}[i],\\ \mathcal{N}(\pi)\le 4X^{1-\alpha}.}} \left(1+\frac{1}{\mathcal{N}(\pi)}\right) \ll (1-\alpha)\log X \; , \tag{2.302}$$

by the elementary inequality $1+t \le \exp(t)$, valid for real all t, and (2.27). From (2.301), (2.300), (2.299) and (2.297) we then conclude that for all α in $(0,1)$ and real $B \geq 1$ we have

$$T_2(X) \ll \left(1 - \alpha + c(\alpha) \sum_{\substack{z \in \mathcal{Z}', \\ B < \mathcal{N}(z).}} \frac{1}{\mathcal{N}(z)} \right) \frac{X}{\log X} , \tag{2.303}$$

where we have used $\mathcal{N}(z) - 1 \geq \frac{\mathcal{N}(z)}{2}$, since $z \in \mathcal{Z}'$ is a Gaussian prime. We now take up the estimation of $T_3(X)$. We have that

$$T_3(X) = \sum_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) > A.}} \sum_{\substack{\pi' \in \mathcal{P}[i], \mathcal{N}(\pi') \leq X, \\ \pi' \equiv -1 \bmod D\pi^2.}} 1 . \tag{2.304}$$

For π with $\mathcal{N}(D\pi^2) \leq X^{\frac{1}{4}}$ we use the Brun-Titchmarsh theorem (2.31) with $\alpha = \frac{1}{4}$. On remarking that $\phi(D\pi^2) \geq \phi(\pi^2) \geq \frac{\mathcal{N}(\pi)^2}{2}$ we then obtain

$$\sum_{\substack{\pi' \in \mathcal{P}[i], \mathcal{N}(\pi') \leq X, \\ \pi' \equiv -1 \bmod D\pi^2.}} 1 \ll \frac{X}{\mathcal{N}(\pi)^2 \log X} . \tag{2.305}$$

Therefore we have

$$\sum_{\substack{\pi \in \mathcal{P}[i], \\ A < \mathcal{N}(\pi), \\ \mathcal{N}(D\pi^2) \leq X^{\frac{1}{4}}.}} \sum_{\substack{\pi' \in \mathcal{P}[i], \mathcal{N}(\pi') \leq X, \\ \pi' \equiv -1 \bmod D\pi^2.}} 1 \ll \frac{X}{\log X} \sum_{\substack{z \in \mathcal{G}^*, \\ A < \mathcal{N}(z).}} \frac{1}{\mathcal{N}(z)^2} \ll \frac{X}{A \log X} \tag{2.306}$$

on taking account of (2.16). When $X^{\frac{1}{4}} < \mathcal{N}(D\pi^2)$ we estimate the left hand side of (2.305) trivially. Indeed, since $\mathcal{N}(\pi' + 1) \leq 4X$ and $D\pi^2 | \pi' + 1$ we have

$$\sum_{\substack{\pi' \in \mathcal{P}[i], \mathcal{N}(\pi') \leq X, \\ \pi' \equiv -1 \bmod D\pi^2.}} 1 \leq \mathcal{L}\left(\frac{4X}{\mathcal{N}(D\pi^2)}\right) \ll \frac{X}{\mathcal{N}(D\pi^2)} \ . \tag{2.307}$$

Consequently, we obtain

$$\sum_{\substack{\pi \in \mathcal{P}[i], \\ X^{\frac{1}{4}} < \mathcal{N}(D\pi^2).}} \sum_{\substack{\pi' \in \mathcal{P}[i], \mathcal{N}(\pi') \leq X, \\ \pi' \equiv -1 \bmod D\pi^2.}} 1 \ll \frac{X}{\mathcal{N}(D)} \sum_{\substack{z \in \mathcal{G}^*, \\ \frac{X^{\frac{1}{8}}}{\sqrt{\mathcal{N}(D)}} < \mathcal{N}(z).}} \frac{1}{\mathcal{N}(z)^2} \ll X^{\frac{7}{8}} \ , \tag{2.308}$$

by (2.16) and since $\mathcal{N}(D) \geq 1$. From (2.307), (2.306) and (2.304) we then conclude that

$$T_3(X) \ll \left(\frac{1}{A} + \frac{\log X}{X^{\frac{1}{8}}}\right) \frac{X}{\log X} \ . \tag{2.309}$$

Let us now set $\theta = \liminf_{X \to +\infty} \frac{T(X)}{\frac{X}{\log X}}$. Then, on combining the estimates (2.309), (2.303) and (2.296) with (2.290) and recalling that $\mathrm{li}(X) \sim \frac{X}{\log X}$ we obtain for all $A, B \geq 1$ and α in $(0,1)$ that

$$\theta \geq \frac{1}{2\mathcal{N}(y)} \prod_{\substack{\pi | Q, \\ \pi \nmid (1+i)y.}} \left(1 - \frac{1}{\mathcal{N}(\pi) - 1}\right) - c_1(1-\alpha) - \sum_{\substack{z \in \mathcal{Z}', \\ B < \mathcal{N}(z).}} \frac{c_2(\alpha)}{\mathcal{N}(z)} - \frac{c_3}{A} \tag{2.310}$$

for some real numbers $c_1, c_2(\alpha), c_3$. Let us write P for the product on the right hand side of (2.310). Then we evidently have that

$$P \geq \prod_{\substack{z \in \mathcal{Z}, \\ z \neq 1+i}} \left(1 - \frac{1}{\mathcal{N}(\pi) - 1}\right) \prod_{\substack{\pi \in \mathcal{P}[i], \\ \mathcal{N}(\pi) \leq A.}} \left(1 - \frac{1}{\mathcal{N}(\pi) - 1}\right) \ , \tag{2.311}$$

where the product over $z \in \mathcal{Z}$ converges because $\mathcal{Z}$ is a thin set. Thus on passing to the limit $B \to +\infty$ first and then setting $\alpha \to 1^-$ on the right hand side of (2.310), we deduce that for any $A \geq 2$ we have

$$\theta \geq \frac{c_4}{2\mathcal{N}(y)\log A} \prod_{\substack{z\in\mathcal{Z},\\ z\neq 1+i}} \left(1 - \frac{1}{\mathcal{N}(\pi)-1}\right) - \frac{c_3}{A}\,, \tag{2.312}$$

for some real number $c_4 > 0$ since we have

$$\prod_{\substack{\pi\in\mathcal{P}[i],\\ \mathcal{N}(\pi)\leq A.}} \left(1 - \frac{1}{\mathcal{N}(\pi)-1}\right) \gg \frac{1}{\log A}\,, \tag{2.313}$$

by the elementary inequality $1 - t \geq (1 - t^2)\exp(-t)$, valid for all $t \in (0, 1)$, and (2.27). It follows from (2.312) that $\theta > 0$ when A is large enough. This certainly means that $\mathcal{T}$ is an infinite set, when A is large enough.

□

Suppose now that f and $\mathcal{X}$ are as in the statement of Theorem 9.1 and let L be $\sup_{x\in\mathcal{X}} \mathcal{N}(x + 1)$. Further, let $\mathcal{E}'$ be the set of $z \in \mathcal{G}^*$ such that $\pi' + 1 = z(\pi + 1)$ with either $\pi'+1$ or $\pi+1$ in $\mathcal{X}$. The number of $z \in \mathcal{E}'$ with $\pi'+1$ in $\mathcal{X}$ is finite, since z is then a divisor of an element of $\mathcal{X}$. Now let $z \in \mathcal{E}'$ be such that $\pi+1$ is in $\mathcal{X}$ and $\mathcal{N}(z) \leq X$. Then $\mathcal{N}(\pi' + 1) \leq LX$. Hence the number of such z does not exceed $L\Pi(4LX)$. These remarks and (2.26) imply that $\overline{\mathbf{d}}(\mathcal{E}') = 0$. Thus if $\mathcal{E}'' = \mathcal{E} \setminus \mathcal{E}'$, then it follows from Proposition 16.1 that $\overline{\mathbf{d}}(\mathcal{E}'') > 0$. Moreover, $f(z) = 0$ for all $z \in \mathcal{E}''$. We then have from Corollary 14.1 that there is a thin set of primes $\mathcal{Z}$ such that $f(\pi) = 0$ when $\pi \notin \mathcal{Z}$. We will now show that this implies that $f(z) = 0$ for all $z \in \mathcal{G}$.

Let y be any element of $\mathcal{G}^*$. Then Proposition 16.2 shows that $\mathcal{T} = \mathcal{T}(y, A, \mathcal{Z})$ is an infinite set when A is large enough. Thus for such A, there is a $\pi' \in \mathcal{T}$ such that such that $\pi' + 1 \notin \mathcal{X}$ and moreover there is a w satisfying the condition (γ) such that

$$\pi' + 1 = (1 + i)yw \ . \tag{2.314}$$

The condition (γ) tells us that w is coprime to $(1 + i)y$, square-free and such that $f(\pi) = 0$ when $\pi | w$. We then have from (2.314) that $f((1 + i)y) = 0$.

We apply the preceding conclusion with $y = (1 + i)^l \pi^k$ for any $\pi \neq 1 + i \in \mathcal{P}[i]$ and any integers $l, k \geq 0$. Then we see that $f((1 + i)^{l+1}) + f(\pi^k) = 0$. Putting $k = 0$ we get $f((1 + i)^{l+1}) = 0$ for all $l \geq 0$ and putting $l = 0$ we then conclude that $f(\pi^k) = 0$, for all $\pi \in \mathcal{P}[i]$ and all $k \geq 1$. This means that $f(z) = 0$ for all $z \in \mathcal{G}^*$. Since $f(u) = 0$ for any unit u of $\mathcal{G}$, it follows that $f(z) = 0$ for all z in $\mathcal{G}$.

17 Proof of Corollary 8.1

We will prove Corollary 8.1 via a generalisation of an observation of D. Wolke [44]. See also F. Dress and B. Volkmann [7]. As usual, for any x in $\mathbf{C}^*$ we call any z in $\mathbf{C}$ satisfying $\exp(z) = x$ a logarithm of x. Further, for any subset X of $\mathbf{C}^*$, we write $\log(X)$ to denote the union of the sets of all logarithms of each element of X.

Let X be a given multiplicative set and let E denote the $\mathbf{Q}$-vector subspace generated by $\log(X)$ in $\mathbf{C}$. Then $2\pi i.\mathbf{Q}$ is a subspace of E. Indeed, let A be any non-empty subset of X. Then if z is in $\log(A)$ so is $z + 2\pi i$. Therefore $2\pi i.\mathbf{Q}$ is contained in the $\mathbf{Q}$-vector subspace of E generated by $\log(A)$.

Proposition 17.1. *A subset A of X is a set of uniqueness for the family of completely additive functions on X if and only if* $\log(A)$ *generates E as a* $\mathbf{Q}$*-vector space.*

Proof. Suppose that $\log(A)$ generates E as a $\mathbf{Q}$-vector space. Then it follows that for each x in X there is an integer $q > 0$ and elements s and s' of the multiplicative set generated by A such that $sx^q = s'$. Thus if f is a completely additive function on X then $f(x) = (f(s') - f(s))/q$. Consequently, if f vanishes on A then it vanishes at all x in X.

Suppose now that every completely additive function on X that vanishes on A, in fact vanishes on all of X. Then let f be a $\mathbf{Q}$-linear form on E that vanishes on the subspace generated by $\log(A)$ in E. In particular, then f vanishes on the subspace $2\pi i.\mathbf{Q}$ of E. Thus for an x in X if z and z' are logarithms of x, we have $f(z) - f(z') = f(z - z') = 0$, since $z - z' \in 2\pi i.\mathbf{Q}$. Therefore, the map $f^* : X \mapsto \mathbf{C}$ defined by $f^*(x) = f(z)$, for any logarithm z of x, is well-defined. Also, since f is a linear form that vanishes on $\log(A)$, we see that f^* is a completely additive function on X that vanishes on A. Hence f^* vanishes on all of X and therefore f on all of E. This means that $\log(A)$ generates E as a $\mathbf{Q}$-vector space.

□

Let us take $\mathcal{G}$ for X and let A be the set of shifted Gaussian primes. Theorem 9.1 tells us, in particular, that A is a set of uniqueness for the family of completely multiplicative functions on $\mathcal{G}$. Let x be any element of $\mathcal{G}$ and let z be a logarithm of x. Then we have from Proposition 17.1 that there are rational numbers $r_1, r_2, \ldots, r_k$ and logarithms of shifted Gaussian primes $z_1, z_2, \ldots, z_k$, for some integer $k \geq 1$, such that

$$z = r_1 z_1 + r_2 z_2 + \ldots + r_k z_k \ . \tag{2.315}$$

We obtain the conclusion of Corollary 8.1 for x on passing to the exponential on the both sides of the above relation. This completes the proof of the corollary.

CHAPTER 3

Sign Changes

1 Introduction

The theme of this chapter is changes in sign of Fourier coefficients of modular forms and q-coefficients of generalised modular forms, when these coefficients are real. We say that a sequence $\{a(n)\}_{n\geq 1}$ of real numbers changes sign infinitely often if there are infinitely many n for which $a(n) > 0$ and infinitely many n for which $a(n) < 0$. The main results of this chapter are Theorems 5.1 and 5.2. Theorem 5.1 states that the sequences $\{a(n^j)\}_{n\geq 1}$, for $j = 2, 3$ and 4, changes sign infinitely often, where $\{a(n)\}_{n\geq 1}$ is the sequence of Fourier coefficients of a Hecke eigenform f on $SL_2(\mathbf{Z})$. For a given $N \in \mathbf{N}^*$, let f be a generalized modular function on $\Gamma_0(N)$ and let $\{c(n)\}_{n\geq 1}$ be the sequence of q-exponents of f. Then Theorem 5.2 tells us that the subsequence $\{c(p)\}$ of q-exponents indexed by the prime numbers changes sign infinitely often under certain conditions. Both of the aforementioned theorems are quantitative. This chapter is based on the paper [35], authored jointly with J. Meher and K. D. Shankhadar.

2 Modular Forms

The modular group $SL_2(\mathbf{Z})$ is the group of 2-by-2 matrices with integer entries and determinant 1. For each $N \geq 1$, let $\Gamma_0(N)$ be the subgroup of $SL_2(\mathbf{Z})$ consisting of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ such that $N|c$. We say that $\Gamma_0(N)$ is a congruence subgroup of level N. Let $\mathcal{H}$ denote the upper half plane, that is, the set of complex numbers z with $\mathrm{Im}(z) > 0$. The group $SL_2(\mathbf{Z})$ acts on the upper half plane $\mathcal{H}$ by

$$\gamma z = \frac{az+b}{cz+d} \ , \quad \text{where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \text{ and } z \in \mathcal{H} \ .$$

For $\gamma \in SL_2(\mathbf{Z})$ and any integer k, we define the *weight-k operator* on the family of functions $f : \mathcal{H} \to \mathbf{C}$ by

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

Since the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ belongs to the congruence subgroup $\Gamma_0(N)$ for each $N \in \mathbf{N}^*$, any meromorphic function $f : \mathcal{H} \to \mathbf{C}$ that satisfies

$$f(\gamma z) = (cz+d)^k f(z) \text{ for any } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \text{ and } z \in \mathcal{H}$$

is $\mathbf{Z}$-periodic. Thus there is a function $g : \mathcal{D}^* \to \mathbf{C}$, where $\mathcal{D}^*$ is the punctured unit disc and $g(e^{2\pi i z}) = f(z)$. If f is a holomorphic function on $\mathcal{H}$ then g is a holomorphic function on the punctured disc. It therefore has Laurent series expansion around the point 0. We say that f is holomorphic at infinity if g extends to the unit disc $\mathcal{D}$

as a holomorphic function. Such a function f has a Fourier expansion of the form

$$f(z) = \sum_{n \geq 0} a(n) e^{2\pi i n z} \quad ,$$

where the $a(n)$ are complex numbers. The numbers $a(n)$ are called the *Fourier coefficients* of f. Hereafter we denote $e^{2\pi i z}$ by q. We say that f vanishes at infinity if $a(0) = 0$.

A *modular form of weight k and level N* is a holomorphic function f on $\mathcal{H}$ such that $f[\gamma]_k = f$ for all $\gamma \in \Gamma_0(N)$ and $f[\gamma]_k$ is holomorphic at infinity for all $\gamma \in SL_2(\mathbf{Z})$. When the later condition holds we say that f is holomorphic at all cusps. If $f[\gamma]_k$ vanishes at infinity for all $\gamma \in SL_2(\mathbf{Z})$ then we say that f is a cusp form.

The family of all modular forms of weight k and level N forms a vector space over $\mathbf{C}$. This vector space is denoted by $M_k(N)$. The set of cusp forms of weight k and level N is a subspace of $M_k(N)$ denoted by $S_k(N)$.

3 New Forms and Hecke Operators

The Petersson inner product on $S_k(N)$ is defined by

$$\langle f, g \rangle = \int_{D_0(N)} f(z)\overline{g(z)} y^{k-2} dx\, dy \ ,$$

where $z = x + iy$ and $D_0(N)$ is a fundamental domain for $\Gamma_0(N)$, that is a closed simply connected region in $\mathcal{H}$ with the following two properties.

(1) For any $z \in \mathcal{H}$ there is a $\gamma \in \Gamma_0(N)$ and a $z_1 \in D_0(N)$ such that $z = \gamma z_1$.

(2) If $z_1 = \gamma z_2$ where $z_1, z_2 \in D_0(N)$ and $\gamma \in \Gamma_0(N)$ then z_1, z_2 are on the boundary

of $D_0(N)$.

Let k and N be fixed integers. Then for any $n \geq 1$, the operator T_n is defined on $M_k(N)$ by

$$T_n f(z) = n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{nz+bd}{d^2}\right) .$$

For each $n \geq 1$, T_n is an endomorphism of $M_k(N)$. It also preserves the space $S_k(N)$. These operators are called the *Hecke operators*. These operators satisfy the relations $T_m T_n = T_n T_m$ for all $m, n \in \mathbf{N}^*$ and $T_{mn} = T_m T_n$ when $(m, n) = 1$. The proposition below is well known and the proof can be found in any standard text on modular forms, for instance, see pages 104-106 of [19].

Proposition 3.1. *Let n be coprime to N. Then the operator T_n acting on the space of cusp forms $S_k(N)$ is normal with respect to the Petersson inner product. More precisely, its adjoint T_n^* is T_n itself.*

From the normality of the T_n with $(n, N) = 1$ and the fact that the T_n commute, we deduce the following (see page 106, Theorem 6.21 of [19]).

Proposition 3.2. *There is an orthonormal basis of the space $S_k(N)$ of cusp forms which consists of eigenfunctions of all the Hecke operators T_n for $(n, N) = 1$.*

The above proposition is a particular case of the following more general result (see Proposition 6.14, page 100 of [19]).

Lemma 3.1. *Let $\mathcal{S}$ be a finite dimensional Hilbert space over $\mathbf{C}$ and let $\mathcal{T}$ be a commuting family of normal operators $T : \mathcal{S} \to \mathcal{S}$. Then there exists an orthonormal basis $\mathcal{F}$ of $\mathcal{S}$ consisting of common eigenfunctions of all the operators in $\mathcal{T}$.*

Let N be any integer. For any integers M and d satisfying $Md|N$, we have $f(dz) \in S_k(N)$ when $f(z) \in S_k(M)$. We denote by $S_k^{\text{old}}(N)$ the subspace of $S_k(N)$ spanned by all forms of the type $f(dz)$ where $d|N$ and $f \in S_k(M)$ for some $M < N$ such that $dM|N$. The subspace $S_k^{\text{old}}(N)$ is called the space of oldforms in $S_k(N)$. The space of newforms $S_k^{\text{new}}(N)$ is defined to be the orthogonal complement of the space $S_k^{\text{old}}(N)$ in $S_k(N)$ with respect to the Petersson inner product. For the details we refer to [1] and [30]. The space $S_k^{\text{new}}(N)$ is invariant under the operators T_m with $\gcd(m, N) = 1$. These operators are normal, and $S_k^{\text{new}}(N)$ has a basis of common eigenfunctions of the operators T_m with $\gcd(m, N) = 1$, on account of Lemma 3.1. Such an eigenfunction is called a newform (for details see Section 1.7 of [27]).

4 Generalized Modular Functions

The notion of generalized modular functions was introduced by M. Knopp and G. Mason [26], where a GMF in the sense below was called a PGMF (P for parabolic).

Definition 4.1. A generalized modular function (GMF) of weight k on $\Gamma_0(N)$ is a function f holomorphic on $\mathcal{H}$, meromorphic at the cusps and

$$f(\gamma z) = \chi(\gamma)(cz + d)^k f(z) \quad \text{for any } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \,, \tag{3.1}$$

for some (not necessarily unitary) character $\chi : \Gamma_0(N) \to \mathbf{C}^*$. We also require that $\chi(\gamma) = 1$ for every parabolic element $\gamma \in \Gamma_0(N)$, i.e. $|\text{trace}(\gamma)| = 2$. We consider here only the generalized modular functions of weight zero.

As with any periodic complex valued meromorphic function on $\mathcal{H}$ with period 1 and meromorphic at infinity, f has a product expansion of the form

$$f(z) = cq^h \prod_{n \geq 1} (1 - q^n)^{c(n)} \ , \tag{3.2}$$

where c and $c(n)(n \geq 1)$ are complex numbers and h is the order of f at infinity (see [5, 24]). The numbers $c(n)$ are called the q-exponents of the generalized modular function f. The infinite product in (3.2) is convergent in a small enough neighbourhood of $q = 0$, see [5, 8]. Here the complex powers are determined by the principal branch of the complex logarithm.

For any given generalized modular function f the divisor of f, denoted by $\mathrm{div}(f)$, is the set of all zeros and poles of f on the upper half plane and at the cusps. Let f be a non-constant GMF of weight zero on $\Gamma_0(N)$ with $\mathrm{div}(f) = \varnothing$. M. Knopp and G. Mason [26] proved that the logarithmic derivative of f, say g, is a cusp form of weight 2 on $\Gamma_0(N)$. Suppose the Fourier expansion of g is given by $g(z) = \sum_{n \geq 1} b(n) q^n$. Then the q-exponents of f and the Fourier coefficients of g are related by the relation

$$b(n) = -\sum_{d|n} dc(d) \ . \tag{3.3}$$

By the Möbius inversion formula, we have

$$c(n) = -\frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) b(d) \ . \tag{3.4}$$

5 Main Results

Let $h(z) = \sum_{n\geq 1} a(n)q^n$ be a Hecke eigenform of weight k on $SL_2(\mathbf{Z})$. Let $\lambda(n)$ be the nth normalized Fourier coefficient of $h(z)$, i.e. $\lambda(n) = \frac{a(n)}{n^{(k-1)/2}}$. Let us set $\delta_j = \frac{2}{11}, \frac{1}{9}, \frac{2}{27}$ for $j = 2, 3, 4$ respectively.

Theorem 5.1. *Suppose that j is 2,3 or 4. Then for any $\epsilon > 0$, there is a real number $C(\epsilon)$ such that the sequence $\{\lambda(n^j)\}_{n\geq 1}$ has at least $C(\epsilon)x^{\delta_j - \epsilon}$ changes in sign in the interval $(x, 2x]$, for all sufficiently large x.*

We now pass to q-exponents of generalized modular functions at primes. We prove that the subsequence of q-exponents indexed by the primes changes sign infinitely often when the logarithmic derivative g of f is a normalized new form.

Theorem 5.2. *Let N be a square-free integer and f be a non-constant generalized modular function on $\Gamma_0(N)$ with $div(f) = \varnothing$ and let $\{c(n)\}_{n\geq 1}$ be the q-exponents of f. Suppose that the logarithmic derivative $g = \frac{1}{2\pi i}\frac{f'}{f}$ is a normalized new form. Then there is a real number $A > 0$ such that the subsequence $\{c(p) \mid p \text{ prime}\}$ has atleast $\gg e^{A\sqrt{\log x}}$ sign changes in the interval $[x, 2x]$ for all sufficiently large x. In particular, the subsequence $\{c(p) \mid p \text{ prime}\}$ changes sign infinitely often.*

The proof of Theorem 5.1 is given in Section 6 and the proof of Theorem 5.2 is in Section 7. The conclusion of Theorem 5.2 was much improved subsequently by N. Kumar [28].

6 Proof of Theorem 5.1

Let $\lambda(n)$ be the nth normalized Fourier coefficient of a Hecke eigenform $h(z)$ of weight k on $SL_2(\mathbf{Z})$ as defined in Section 5. Here we will prove Theorem 5.1 by means of Lemma 6.1 and Lemma 6.2.

Lemma 6.1. *Let* $\beta_j = \frac{1}{2}, \frac{3}{4}, \frac{7}{9}$ *for* $j = 2, 3, 4$ *respectively. Then for each* $\epsilon > 0$ *and* $j \in \{2, 3, 4\}$ *we have*

$$\sum_{n \le x} \lambda(n^j) \ll_{\epsilon, j} x^{\beta_j + \epsilon} \,. \tag{3.5}$$

This lemma, for the case $j = 2$, is proved by O.M. Fomenko [14] and the remaining cases are proved by G.S. Lü (see page 1320 of [31]) using the analytic properties of the symmetric power L-functions.

We also need the following lemma due to H. Lao and A. Sankaranarayanan (see page 2559 of [29]).

Lemma 6.2. *For* $j = 2, 3, 4$ *let* δ_j *be as in Section 5. Then for each* $\epsilon > 0$ *we have*

$$\sum_{n \le x} \lambda^2(n^j) = c_j x + O(x^{1-\delta_j+\epsilon}) \,. \tag{3.6}$$

Here the constants in the O*-symbol may depend on* ϵ*.*

This lemma is also proved using the properties of symmetric power L-functions and their Rankin-Selberg L-functions.

Proof of the Theorem 5.1. Take $\beta_j = \frac{1}{2}, \frac{3}{4}$ or $\frac{7}{9}$ for $j = 2, 3$ or 4 respectively. Let $j \in \{2, 3, 4\}$ be fixed and let $\epsilon > 0$ be any positive real number. Take $h = h(x) = x^{1-\delta_j+2\epsilon}$. Suppose that all the elements in the sequence $\{\lambda(n^j)\}_{n \ge 1}$ have constant sign, say positive, for all $n \in (x, x+h]$. By Deligne's bound we have $\lambda(n^j) \ll_\epsilon x^\epsilon$ and hence

$$\sum_{x < n \le x+h} \lambda^2(n^j) \ll x^\epsilon \sum_{x < n \le x+h} \lambda(n^j) \ll x^{\beta_j + 2\epsilon} \,, \tag{3.7}$$

where the last inequality follows from Lemma 6.1. Using Lemma 6.2 we get

$$\sum_{x<n\leq x+h} \lambda^2(n^j) = c_j h + O_{f,\epsilon}(x^{1-\delta_j+\epsilon}) \gg x^{1-\delta_j+2\epsilon} . \tag{3.8}$$

On combining this estimate with (3.7) we get that

$$x^{1-\delta_j+2\epsilon} \ll \sum_{x<n\leq x+h} \lambda^2(n^j) \ll x^{\beta_j+2\epsilon} . \tag{3.9}$$

Now comparing $1-\delta_j$ and β_j for $j = 2, 3, 4$ we see that the bounds in (3.9) contradict each other when x is sufficiently large. Therefore at least one n in the interval $(x, x+h]$ such that $\lambda(n^j)$ is negative. Hence the sequence $\{\lambda(n^j)\}_{n\geq 1}$, for $j = 2, 3, 4$, changes sign infinitely often and there are at least $\gg x^{\delta_j-2\epsilon}$ sign changes in the interval $(x, 2x]$. □

7 Proof of Theorem 5.2

Let $g(z) = \sum_{n\geq 1} b(n)q^n$ be the Fourier expansion of g. Then we have

$$b(n) = -\sum_{d|n} dc(d) . \tag{3.10}$$

In particular, $b(1) = 1 = -c(1)$ and $b(p) = 1 - pc(p)$ for any prime p.

Let $\lambda(n)$ be the nth normalized Fourier coefficient of g, i.e. $\lambda(n) = \frac{b(n)}{n^{1/2}}$. Then there is a real number A_1 such that

$$\sum_{p\leq x} \lambda(p) \log p \ll x e^{-A_1\sqrt{\log x}} . \tag{3.11}$$

This follows on combining the conclusions of Main Theorem, page 797 of [36] (see Theorem 5.40 [20]) with Theorem B of [18].

Also, we have that there is a positive real number A_2 such that

$$\sum_{p\leq x}\lambda^2(p)\log p = x + O(xe^{-A_2\sqrt{\log x}})\ . \tag{3.12}$$

Indeed, Theorem 4.1 of [41] gives the above for the Fourier coefficients of cusp forms on $SL_2(\mathbf{Z})$. However, a perusal of the proof shows that this conclusion extends to congruence subgroups of square free level on taking account of the zero free region supplied by Theorem 5.44 of [20].

Since $\lambda(p) = \frac{b(p)}{\sqrt{p}} = -\left(\frac{-1}{\sqrt{p}} + \sqrt{p}c(p)\right)$, therefore $\sqrt{p}c(p) = \frac{1}{\sqrt{p}} - \lambda(p)$. Let us set $c'(p) = \sqrt{p}c(p)$ for all primes p. Since $c(p)$ and $c'(p)$ are of same sign, it is enough to prove the theorem for $c'(p)$. From (3.11), we have that

$$\sum_{p\leq x} c'(p)\log p = \sum_{p\leq x}\left(\frac{1}{\sqrt{p}} - \lambda(p)\right)\log p \ll x^{\frac{1}{2}}\log x + xe^{-A_1\sqrt{\log x}}\ . \tag{3.13}$$

On the other hand,

$$\sum_{p\leq x} c'^2(p)\log p = \sum_{p\leq x}\lambda^2(p)\log p - 2\sum_{p\leq x}\frac{\lambda(p)\log p}{\sqrt{p}} + \sum_{p\leq x}\frac{\log p}{p}\ . \tag{3.14}$$

On estimating the first and second terms by means of (3.12) and (3.11) respectively, we obtain

$$\sum_{p\le x} c'^2(p)\log p = x + O(xe^{-A_3\sqrt{\log x}})\ , \tag{3.15}$$

for some real number $A_3 > 0$.

Let $h : \mathbf{R} \to \mathbf{R}$ be a function such that $0 < h(u) < u$ for all $u > 0$. Suppose $c'(p)$ has constant sign, say positive, in the interval $(x, x+h]$. Then Deligne's bound gives $|c'(p)| \le 3$ and consequently

$$\sum_{x<p\le x+h} c'^2(p)\log p \le 3 \sum_{x<p\le x+h} c'(p)\log p \ll xe^{-A_1\sqrt{\log x}}\ , \tag{3.16}$$

where we have used the equation (3.13) for the last inequality. On the other hand, we have from (3.15) that

$$\sum_{x<p\le x+h} c'^2(p)\log p = h + O(xe^{-A_3\sqrt{\log x}})\ . \tag{3.17}$$

It now follows from (3.17) and (3.16) that

$$h + O(xe^{-A_3\sqrt{\log x}}) = \sum_{x<p\le x+h} c'^2(p)\log p \ll xe^{-A_1\sqrt{\log x}}\ . \tag{3.18}$$

When $h(x) = \frac{x}{e^{A\sqrt{\log x}}}$, with $A < \min\{A_1, A_3\}$ these bounds contradict each other, and the theorem follows.

Bibliography

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

[2] N.L. Bassily, J.M. De Koninck and I. Kátai, On a theorem of Daboussi related to the set of Gaussian integers, *Math. Pannon.* **14** (2003), no. 2, 267-272.

[3] G. Bhowmik and O. Ramaré, A Turán-Kubilius inequality for integer matrices, *J. Number Theory* **73** (1998), no. 1, 59-71.

[4] N. Bourbaki, *Integration-II Chapters 7-9*, Elements of Mathematics, Springer, Berlin (2004).

[5] J.H. Brunier, W. Kohnen and K. Ono, The arithmetic of the values of modular functions and the divisors of modular forms, *Compos. Math.* **140** (2004), 552-566.

[6] J. Dieudonné, *Foundations of Modern Analysis*, Pure and Applied Mathematics, Vol. **X** Academic Press, New York-London (1960).

[7] F. Dress and B. Volkmann, Ensembles d'unicité pour les fonctions arithmétiques additives ou multiplicatives, *C. R. Acad. Sci. Paris Sr. A-B* **287** (1978), no. 2, A43-A46.

[8] W. Eholzer and N.-P. Skoruppa, Product expansions of conformal characters, *Phys. Lett. B* **388** (1996), 82-89.

[9] P.D.T.A. Elliott, A conjecture of Kátai, *Acta. Arith.* **26** (1974), 11-20.

[10] P.D.T.A. Elliott, The Turán-Kubilius inequality, *Proc. Amer. Math. Soc.* **65** (1977), no. 1, 8-10.

[11] P.D.T.A. Elliott, *Probabilistic Number Theory-II*, Springer-Verlag (1980).

[12] P.D.T.A. Elliott and C. Ryavec, The distribution of the values of additive arithmetical functions, *Acta. Math.* **126** (1971), 143-164.

[13] P. Erdös, On the distribution function of additive functions, *Ann. Math.* **47** (1946), 1-20.

[14] O.M. Fomenko, On the behaviour of the automorphic L-functions at the centre of the critical strip, *J. Math. Sci. (N. Y.)* **118** (2003), 4910-4917.

[15] D. Goldfeld, J. Hoffstein and D. Lieman, Appendix: An effective zero free region, *Ann. Math.* **140** (1994), 177-181.

[16] G. Halász, Über die mittelwerte multiplikativer zahlentheoretischer funktionen, *Acta Math. Acad. Sci. Hung.* **19**, 365-403.

[17] J. Hinz and M. Lodemann, On Siegel zeros of Hecke-Landau zeta-functions, *Monatsh. Math.* **118** (1994), 231-248.

[18] J. Hoffstein and D. Ramakrishnan, Siegel zeros and cusp forms, *Internat. Math. Res. Notices.* **6** (1995), 279-308.

[19] H. Iwaniec, *Topics in Classical Automorphic Forms,* AMS (1997).

[20] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ., Vol. 53, Amer. Math. Soc., Providence, RI (2004).

[21] D. Johnson, Mean values of Hecke L-functions, *J. Reine Angew. Math.* **305** (1979), 195-205.

[22] I. Kátai, On sets characterizing number theoretical functions, *Acta Arith.* **13** (1968), 315-320.

[23] I. Kátai, On sets characterizing number theoretical functions-II, *Acta Arith.* **16** (1968), 1-4.

[24] W. Kohnen, On certain generalized modular forms, *Funct. Approx. Comment. Math.* **43** (2010), 23-29.

[25] W. Kohnen and J. Meher, Some remarks on the q-exponents of generalized modular functions, *Ramanujan J.* **25** (2011), 115-119.

[26] M. Knopp and G. Mason, Generalized modular forms, *J. Number Theory* **99** (2003), 1-18.

[27] G. Köhler, *Eta Products and Theta Series Identities*, Springer, Berlin (2011).

[28] N. Kumar, On sign changes of q-exponents of generalized modular functions, *J. Number Theory* **133** (2013), no.11, 3589-3597.

[29] H. Lao and A. Sankaranarayanan, The average behaviour of Fourier coefficients of cusp forms over sparse sequences, *Proc. Amer. Math. Soc.* **8** (2009), 2557-2565.

[30] W.-C.W. Li, Newforms and functional equations, *Math. Ann.* **212** (1975), 285-315.

[31] G.S. Lü, On an open problem of Sankaranarayanan, *Sci. China Math.* **53** (2010), 1319-1324.

[32] J. Mehta, *Characterization of Certain Arithmetical Functions*, Ph.D. Thesis, HBNI, Feb. 2015.

[33] J. Mehta and G.K. Viswanadham, Quasi-uniqueness of the set of "Gaussian prime plus one's", *Int. J. Number Theory* **10** (2014), no. 7, 1783-1790.

[34] J. Mehta and G.K. Viswanadham, Set of uniqueness of shifted Gaussian primes, *Funct. Approx. Comm. Math.*, To appear.

[35] J. Meher, K.D. Shankhadar and G.K. Viswanadham, A short note on sign changes, *Proc. Indian Acad. Sci. Math. Sci.* **123** (2013), 315-320.

[36] C.J. Moreno, Prime number theorems for the coefficients of modular forms, *Bull. of AMS.* **78** (1972), 796-798.

[37] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Third edition, Springer-Verleg, Berlin (2004).

[38] K. Prachar, *Primzahlverteilung*, Springer, Berlin (1957).

[39] M. Ram Murty, Oscillations of the Fourier coefficients of modular forms, *Math. Ann.* **262** (1983), 431-446.

[40] C. Ryavec, A characterization of finitely distributed additive functions, *J. Number Theory* **2** (1970), 393-403.

[41] A. Sankaranarayanan, On Hecke L-functions associated with cusp forms II: on the sign changes of $S_f(T)$, *Ann. Acad. Scient. Fenn. Math.* **31** (2006), 213-238.

[42] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, Aspects Math. E15, Friedrich Vieweg & Sohn, Braunschweig (1990).

[43] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Studies in Advanced Mathematics **46**, Cambridge University Press (1995).

[44] D. Wolke, Bemerkungen über eindeutigkeitsmengen additiver funcktionen, *Elem. Math.* **33** (1978), 14-16.