Normal order of certain arithmetic functions and new analogues of the Erdős-Kac theorem

by

Arpita Kar

A thesis submitted to the
Department of Mathematics and Statistics
in conformity with the requirements for
the degree of Doctor of Philosophy

Queen's University
Kingston, Ontario, Canada
August 2020

Copyright © Arpita Kar, 2020

Abstract

In 1917, Hardy and Ramanujan planted the seeds of Probabilistic Number Theory through [27] when they defined 'normal order' of an arithmetic function. This was nurtured further by Erdős and Kac and many other great minds who infused further improvements to the probabilistic theory of additive functions. A systematic generalisation of this study to non-additive functions was initiated by Ram Murty and Kumar Murty in 1984 in [38]. In this thesis, we study the theorem of Hardy and Ramanujan more deeply from a different perspective where we view the normal order results as estimates on sizes of certain exceptional sets. Using these results, we study the normal order of various non-additive functions like $\Omega(\phi(p+a))$ and $\Omega(\tau(p+a))$, thus generalising the results of Murty and Murty ([38], [39]) to shifts of prime arguments. We also study the distribution of these functions. Here $\Omega(n)$ counts the number of prime factors of a natural number n, with multiplicity, $\phi(n)$ denotes the Euler totient function and $\tau(n)$ denotes the Ramanujan tau function. Here and throughout the thesis, we denote p as a prime. Finally, we study the moments of Dirichlet characters and establish normal order results in that direction as well.

Co-Authorship

The results in Chapter 3, 4 are obtained jointly with my supervisor Prof. Ram Murty. Results in Chapter 2 are about to appear in [30].

Acknowledgments

First and foremost, I would like to sincerely thank Prof. Ram Murty, who has encouraged me, inspired me and motivated me over the last five years. I have learned a lot from him, both in Mathematics and Philosophy. I will cherish our mathematical discussions in his office and the 'chai party' discussions in 361 Barrie Street forever. Without him, this journey would not be possible.

Also, I would like to thank Prof. Greg Martin, Prof. Francesco Cellarosi, Prof. Selim Akl, Prof. Daniel Offin and Prof. Wenyu Jiang for serving in my examining committee, helping me go through the process even in these uncertain times of COVID -19 pandemic, as well as their valuable comments on the previous version of this thesis.

Next, I thank Prof. Sanoli Gun, Prof. Purusottam Rath, Prof. Anirban Mukhopadhyay and Prof. Balakrishnan from my CMI days for their encouragement. They initiated me to number theory through their amazing courses and I am grateful to them for the same. I always enjoyed going back to India in the summer and having insightful discussions with them on various interesting problems.

I thank Prof. Alan Abelson, Dr. Ping Li and Mike for all their support while I was teaching at Queen's. They made it so much easier for me to teach alongside conducting research. I also thank Jennifer, Anne, Rianna, Johanna, Claire and Jeananne for making any administrative process so smooth. I will always cherish my occasional chats with Rianna while dropping by the office on my way to Prof.

Murty's office.

Thanks to my peers at Jeffery, for making the learning environment so much better. Pei Lun was a great officemate for the first two years. I deeply enjoyed Tariq and Kaly dropping by my office for math discussions. Esme's occasional visits to Kingston and mine to Toronto would make my study breaks way more fun.

I want to thank Siddhi, Harshas (HT, HL) for being such great housemates. I also thank Somya for being such a great friend. I also thank my friends Sougata and Ranadeep. Thanks for putting up with me from the other side of the world, my countless rants over the phone and helping me to keep going. My life has been cheerful in Kingston, thanks to Vasu and Basu. I made friends for life. Hanging out with them at the end of a busy week made life so much better.

I also thank Rahul for supporting me so much. Thanks for supporting me in all my endeavours, motivating me to follow my heart. He gave me the courage I needed to jump into the unknown and pursue my dream. His presence and encouragement made the journey so much more enjoyable. Thanks for believing in me.

Last but not the least, I want to thank Ma, Baba, and my little sister Srijita for all they have done for me. They believed in me and I am what I am today, because of them. They taught me to face the world and enabled me to pursue my career. My younger sister became my didi ('elder sister') and motivated me from the other side of the world. She was always there as a bridge between me and my parents when I felt down and did not want to upset Ma and Baba. I would not be the same person without them. Salute to them.

Statement of Originality

I hereby certify that the work described in this thesis is the original work of the author. Collaboration with other authors is acknowledged and detailed in the section Co-Authorship. Results due to other authors are fully acknowledged and presented as such, in conformity with standard referencing practices in Mathematics.

List of Abbreviations and Symbols

- p : prime
- $\omega(n)$: Number of distinct prime factors of n, counted without multiplicity.
- $\Omega(n)$: Number of prime factors of n, counted with multiplicity.
- $\phi(n)$: Euler totient function.
- $p|n$: p divides n.
- $p^{\alpha}||n$: $p^{\alpha}|n$ but $p^{\alpha+1} \nmid n$.
- $\tau(n)$: Ramanujan tau function.
- $\sigma(n)$: Sum of divisors of n.
- $d(n)$: Number of divisors of n.
- $\pi(x)$: Number of primes $p \leq x$.
- π : Transcendental number
- $\pi(x, q, a)$: Number of primes $p \leq x$ of the form $am + q$.
- $\chi(n)$: Dirichlet character.

Other abbreviations and definitions will be explained in detail when introduced.

Contents

Abstract **i**

Co-Authorship **ii**

Acknowledgments **iii**

Statement of Originality **v**

List of Abbreviations and Symbols **vi**

Contents **vii**

Chapter 1: Introduction **1**
1.0.1 Organisation of the thesis 16

Chapter 2: The Hardy-Ramanujan Theorem revisited **18**
2.1 Introduction 18
2.2 Preliminaries : Selberg's Sieve and some elementary inequalities . . . 21
2.3 Revisiting the 1917 theorem of Hardy and Ramanujan 26
2.4 Proofs of Theorems 2.1.2 and 2.1.3 33
2.4.1 Strategy of proof of Theorems 2.1.2 and 2.1.3 33
2.4.2 Proofs of related lemmas and Theorem 2.1.2 and 2.1.3 35

Chapter 3: On the normal number of prime factors of the Euler phi function at shifts of prime arguments **43**
3.1 Preliminaries: Brun's sieve and error in the estimate of number of primes in arithmetic progression 46
3.2 Review of results of Erdős and Pomerance 53
3.3 Erdős' theorem for $\Omega(p-1)$ 56
3.4 Mean and Variance for $\Omega(\phi(p+a))$ 62
3.5 Erdős-Kac type result for $\Omega(\phi(p+a))$ 79

Chapter 4: On the normal number of prime factors of the Ramanujan tau function at shifts of prime arguments **87**
4.1 Introduction 87
4.2 Background 89
4.2.1 Chebotarev density theorem, Galois representations 90
4.3 Application of Selberg's sieve to estimate size of exceptional set for $\Omega(\tau(q))$ 95
4.4 Mean and Variance for $\Omega(\tau(p+a))$ 102
4.5 Erdős-Kac type result for $\Omega(\tau(p+a))$ 121
4.6 Further generalisation 125

Chapter 5: Moments of Sums of Characters **127**
5.1 Result of Heilbronn Revisited 134
5.2 Sums over product of characters - a generalisation of Heilbronn's arguments 137
5.3 Viewing through the lens of probability theory 141

Chapter 6: Concluding Remarks and Scope of Future Research **146**
6.1 Joint Distribution of non-additive functions 147
6.2 Probabilistic Relations to the Riemann Hypothesis 149

Bibliography **160**

Chapter 1

Introduction

The central limit theorem ([4]) is one of the remarkable theorems of 20th century mathematics and there are even good reasons to say it is the most remarkable discovery of our time. With its humble origins emanating from a simple combinatorial problem involving coin tosses studied by de-Moivre and Laplace in the 18th and 19th centuries, it has evolved over decades into a profound principle of probability theory. It gave birth to statistical methods and now influences disciplines outside of mathematics such as biology, medical science, economics and artificial intelligence. This thesis will not expound these connections and ramifications outside the mathematical field but rather our goal is to elucidate its impact on number theory, particularly probabilistic number theory.

Concisely, probabilistic number theory can be thought of as "*the study of asymptotic behaviour of arithmetically defined sequences of probability measures*". To explain what that means, we travel back to 1917 when G.H Hardy and S. Ramanujan ([27]) proved that $\omega(n)$, the number of distinct prime factors of an integer n, has normal

order $\log\log n$. Specifically, this means that if $\nu_N(n;P)$ denotes the number of positive integers in the interval $[1,N]$ that possess a certain property P, then for each $\epsilon > 0$,

$$\lim_{N\to\infty} \nu_N(n; |\omega(n) - \log\log n| > \epsilon \log\log n) = 0. \tag{1.0.1}$$

They also showed that the result stays true when $\omega(n)$ is replaced by $\Omega(n)$, the number of prime factors of n counted with multiplicity. Their argument was elementary and largely combinatorial in nature. In this paper of 1917, Hardy and Ramanujan wished to draw attention to the relative infrequency of those integers n for which $\omega(n)$ is appreciably large or rather small, and such integers exist. At that time, the theory of probability lacked a sound foundation and Hardy, who had worked hard to introduce clarity and rigor into the teaching of mathematics in England, no doubt viewed the ideas of probability theory with suspicion. Hardy and Ramanujan thus express their results in terms of asymptotic density, a notion familiar from analytic number theory and the study of primes.

It was not until 1933 that Kolmogorov's monograph [34] appeared, in which he proposed the current accepted model for the foundation of the theory of probability. In the world of probability theory, it took almost a century for the de-Moivre Laplace theorem to evolve into the modern Central Limit Theorem. Beginning with the work of Chebycheff (1887), and then his two pupils Markov (1898) and Lyapunov (1901), Lindeberg (1922), and finally Lévy (1935) and Feller (1935), the central limit theorem morphed into its following modern form.

Theorem 1.0.1. (The central limit theorem) *Suppose for each n,*

$$X_{n1}, X_{n2}, ..., X_{nr_n}$$

are independent random variables on some probability space Y_n *with measure* P_n*. Put*

$$S_n = X_{n1} + X_{n2} + \cdots + X_{nr_n}.$$

Assume the expectation $E(X_{nk}) = 0$ *and set*

$$\sigma_n^2 = \sum_{k=1}^{r_n} \sigma_{nk}^2$$

where $\sigma_{nk}^2 = E(X_{nk}^2)$*. Then*

$$P\left(\omega : \alpha \leq \frac{S_n(\omega)}{\sigma_n} \leq \beta\right) \to \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta e^{-t^2/2} dt,$$

and

$$\max_{k \leq r_n} \frac{\sigma_{nk}^2}{\sigma_n^2} \to 0$$

as $n \to \infty$ *if and only if*

$$\lim_{n\to\infty} \sum_{k=1}^{r_n} \frac{1}{\sigma_n^2} \int_{|X_{nk}| > \epsilon\sigma_n} X_{nk}^2 dP_n = 0 \tag{1.0.2}$$

for every $\epsilon > 0$*.*

The sufficiency was shown by Lindeberg (1922) and the necessity by Feller (1935). The condition (1.0.2) is often referred to as the Lindeberg condition. According to the historical article [51], Alan Turing also discovered this independently in 1934 while still an undergraduate at the age of 22.

It is worth mentioning here that $\omega(n)$ and $\Omega(n)$ are examples of *additive functions*. In other words, $\omega(mn) = \omega(m) + \omega(n)$ whenever m and n are coprime.

Thus, one can write

$$\omega(n) = \sum_{p|n} \omega(p),$$

and it is suggestive to view $\omega(n)$ as a sum of "independent random variables" when looked at this way. However, in 1917, when Hardy and Ramanujan proved their normal order result, this viewpoint was long in coming and had a roundabout emergence taking several decades.

It was in 1934 when Paul Turán [49] gave a simpler and more transparent treatment of Hardy and Ramanujan's theorem using what can be viewed as Tchebycheff's inequality from probability theory. Here and throughout, p will always denote a prime number. Using essentially the two basic facts from analytic number theory, the first is a (weak version of) theorem of Mertens :

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + O(1). \tag{1.0.3}$$

and the next one, a theorem of Euler which gives the following upper bound.

$$\sum_{p \leq x} \frac{1}{p^2} < \sum_{p} \frac{1}{p^2} < \sum_{n} \frac{1}{n^2} = \frac{\pi^2}{6} = O(1) \tag{1.0.4}$$

(see the first two chapters of [37]), Paul Turán approached the Hardy-Ramanujan theorem and his two page paper gave rise to a spectacular cascade of events which ultimately led to the development of probabilistic number theory. It paved the way

for probabilist Mark Kac to relate this "density theorem" to the world of probability theory. Turán calculated the *mean* of $\omega(n)$ as n ranges over integers up to x.

$$\begin{aligned}\sum_{n\leq x}\omega(n) &= \sum_{n\leq x}\sum_{p|n}1 = \sum_{p\leq x}\left\lfloor\frac{x}{p}\right\rfloor\\ &= x\sum_{p\leq x}\frac{1}{p}+O(\pi(x))\\ &= x\,(\log\log x)+O(x).\end{aligned}$$

He then estimated the *variance*

$$\sum_{n\leq x}(\omega(n)-\log\log x)^2 = O(x\log\log x).$$

Now, to prove Hardy and Ramnaujan's normal order result, one needs to show that the number of $n\leq x$ such that

$$|(\omega(n)-\ \log\log x)|>\epsilon\log\log x$$

is $o(x)$. It is at this step that Tchebycheff's inequality from probability theory plays a pivotal role. Recall this inequality from probability theory.

Tchebycheff's inequality : Let X be a random variable with mean μ and variance σ^2, then

$$P\left\{|X-\mu|\geq c\right\}\leq\frac{\sigma^2}{c^2}.$$

In the context of $\omega(n)$, for $\epsilon>0$, the number of $n\leq x$ such that $|(\omega(n)-$

$\log\log x)| > \epsilon \log\log x$ holds is at most

$$O(\frac{x \log\log x}{\epsilon^2 (\log\log x)^2}) = o(x).$$

Paul Turán had not seen Kolmogorov's book in 1934; he even did not know Tchebycheff's inequality ([17], pg. 18). In a letter to Elliott (pg. 18 of [17]) written in 1976, Turán recalls "When writing Hardy first in 1934 on my proof of Hardy-Ramanujan's theorem I did not know what Tchebycheff's inequality was and a fortiori of the central limit theorem. Erdős, to my best knowledge, was at that time not aware too. It was Mark Kac who wrote to me a few years later that he discovered when reading my proof in JLMS that this is basically probability and so was his interest turned to this subject." Apparently, Kac asked if Turán could prove similar estimates for the higher moments:

$$\sum_{n \leq x} (\omega(n) - \log\log n)^k.$$

Kac even hinted in his letter that if one could derive similar estimates, then there is a normal distribution law for $\omega(n)$. Turán continues that though he realised he could estimate the higher moments, he "found absolutely no interest to do it actually." His reasons, he confesses, "could not see a single possibility of similar application of higher moments or even of such a value distribution theorem." As we know today, as it transpired later on, that there is indeed an intimate connection of this result to the normal distribution. Around the same time in 1936, Erdős proved that those integers m in the interval $1 \leq m \leq n$ for which $\omega(m) > \log\log n$, are $\frac{1}{2}n + o(n)$ in number. Brun's Sieve was an essential ingredient in the proof of this

theorem. Thus lacking the appropriate knowledge from the theory of probability, he settled for establishing that the density of integers $n \leq x$ for which

$$\frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} \leq \alpha$$

tends to

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-\frac{t^2}{2}} dt$$

in the particular case $\alpha = 0$. Three years later, Mark Kac was giving a lecture in Princeton, in which he stated as a conjecture the general case for any α, that is $\frac{\omega(n) - \log\log n}{\sqrt{\log\log n}}$ is "normally distributed" in the probabilistic sense. Quoting Kac, "Fortunately for me and possibly for Mathematics, Erdős was in the audience, and he immediately perked up. Before the lecture was over he had completed the proof." Erdős and Kac published their celebrated theorem in 1940 [20]. Their method was a combination of the central limit theorem of probability, applied by viewing the divisibility of an integer by distinct primes as essentially "independent" events, an idea due to Kac; and the sieve method of Brun together with other number theoretic methods, which were contributed by Erdős. A most simple version of their result is as follows :

Theorem 1.0.2 (Erdős -Kac, 1940)**.** *For any positive integer $n > 1$, let $\omega(n)$ denote the number of prime divisors of n, counted without multiplicity. Then for any real numbers $\alpha < \beta$, we have*

$$\lim_{N\to\infty} \left(\frac{1}{N} \# \left\{ n \leq N : \alpha \leq \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} \leq \beta \right\} \right) = \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\beta} e^{-t^2/2} dt.$$

To spell out the connection between the statement of this theorem and the Central Limit Theorem, one sequence of probability measures involved here is the sequence $(\mu_N)_{N\geq 1}$ defined as the uniform probability measures supported on the finite set $\Omega_N = \{1, \cdots N\}$. This sequence is defined arithmetically, because the study of integers is part of arithmetic. The asymptotic behaviour is revealed by the statement. Namely, consider the sequence of random variables

$$X_N(n) = \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}}$$

defined on Ω_N for $N \geq 3$ (simply so $\log\log N \geq 1$), and the sequence of their probability distributions, which are (Borel) probability measures on $\mathbb{R}$ defined by

$$\mu_N(X_N \in A) = \frac{1}{N}\#\left\{1 \leq n \leq N;\ \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} \in A\right\}$$

for any measurable set $A \subset \mathbb{R}$. These form another arithmetically-defined sequence of probability measures, since primes are arithmetic objects. Theorem (1.0.2) is, by basic Central Limit Theorem, equivalent to the fact that the sequence $\mu_N(X_N \in A)$ converges in law to the standard normal random variable as $N \to \infty$.

The Erdős -Kac theorem is probably the simplest case where a natural deterministic arithmetic quantity (the number of prime factors of an integer), individually hard to grasp, nevertheless exhibits a probabilistic distribution. This is the prototype of some results we prove in this thesis.

In general, additive arithmetic functions such as $\omega(n)$, are real valued and satisfy $f(ab) = f(a) + f(b)$ whenever $\gcd(a, b) = 1$. They are completely additive if we omit the condition that $\gcd(a, b) = 1$. It is to be noted here, that additivity in the

context of number theory is different from additivity in the context of probability theory. Throughout the thesis, we would always refer to additivity of arithmetic functions, in the number theoretic sense, as discussed here.

A sequence of distribution functions $\{\mu_n\}_{n=1}^{\infty}$ is said to converge weakly to a function μ if we have

$$\lim_{n\to\infty} \mu_n(z) = \mu(z), \ (z \in \mathcal{C}(\mu))$$

where $\mathcal{C}(\mu)$ denotes the set of continuity points of μ. For a more detailed discussion on limiting distribution of arithmetic functions, see p. 426 of [46]. The well known theorem of Erdős and Wintner, [23], 1939, asserts that for an additive function, there is a distribution function $F(z)$ towards which the frequencies $\nu_N(n; f(n) \leq z)$, $N = 1, 2, \cdots$ converge weakly if and only if the three series

$$\sum_{|f(p)|>1} \frac{1}{p}, \quad \sum_{|f(p)|\leq 1} \frac{f(p)^2}{p}, \quad \sum_{|f(p)|\leq 1} \frac{f(p)}{p},$$

taken over prime numbers, converge. More explicitly, Erdős and Wintner prove the following theorem.

Theorem 1.0.3 (Erdős, Wintner, 1939)**.** *Let f be a real-valued additive function. Then $\nu_N(n; f(n) \leq z)$ converges weakly to $F(z)$ for a suitable distribution function $F(z)$, if and only if the series*

$$\sum_p \frac{||f(p)^2||}{p}, \ \sum_p \frac{||f(p)||}{p}, \tag{1.0.5}$$

taken over the sequence of primes, converge, where $||u||$ is defined by

$$||u|| = \begin{cases} 1 & \text{if } u \geq 1 \\ u & \text{if } -1 \leq u \leq 1 \\ -1 & \text{if } u \leq -1 \end{cases}$$

The following result by Levin, Timofeev and Elliott contains as special cases the Erdős-Kac theorem and the results of the Kubilius theory for additive functions.

Theorem 1.0.4 (Levin, Timofeev, Elliott)**.** *Let f be a real-valued additive function and let $\alpha(x)$ and $\beta(x)$ be real valued functions satisfying $\beta(x) \to \infty$ as $x \to \infty$ and it is slowly increasing in the sense that*

$$sup_{1 \leq t \leq 2} \| \frac{\beta(x^t)}{\beta(x)} - 1 \| \to 0 \text{ as } x \to \infty.$$

In order that $\nu_N(n; f(n) \leq z)$ converges weakly to some distribution function $F(z)$, it is necessary and sufficient that there exists a constant λ such that if X_p (p prime) are independent random variables defined by

$$X_p = \begin{cases} f(p) - \lambda \log p & \text{with probability } \dfrac{1}{p} \\ 0 & \text{with probability } 1 - \dfrac{1}{p} \end{cases}$$

then

$$P\left(\sum_{p \leq x} X_p \leq \ z\beta(x) + \alpha(x) - \lambda \log x \right)$$

converges to the distribution function $F(z)$.

This result [29] represents the most important result about the behaviour of additive functions on the sequence of positive integers and describes their behaviour fully for large classes of additive functions. As a natural generalisation, one might try to develop a similar theory for the behaviour of additive and multiplicative functions on certain arithmetically interesting subsequences of the sequence of positive integers. Particular cases that have been studied in literature are polynomial sequences like $\{n^2+1\}$ or sequences of "*shifted primes*" $\{p+a\}$ for any fixed non-zero integer a. To study the distribution of additive functions f on the sequence $\{p+a\}$, one has the following analogue of the Erdős Wintner theorem [29], which completely characterises those additive functions for which the distribution function

$$\frac{1}{\pi(x)}\#\{p \leq x : f(p+1) \leq z\}$$

as $x \to \infty$ converges to the limit distribution function $F(z)$.

Theorem 1.0.5 (Hildebrand, 1989)**.** *Let f be a real-valued additive function. Then*

$$\nu_x(p; f(p+1) \leq z)$$

as $x \to \infty$, converges weakly to $F(z)$ for a suitable distribution function $F(z)$, if and only if the two series (1.0.5) converge. If this condition is satisfied then the characteristic function of the limit distribution $F(z)$ is given by

$$\Phi(t) = \prod_p \left(1 - \frac{1}{p-1} + \sum_{p \leq x} \frac{e^{itf}(p^m)}{p^m}\right) \tag{1.0.6}$$

In the same paper, there is also a further generalization, an analogue of Theorem 1.0.4 which is as follows:

Theorem 1.0.6 (Hildebrand, 1989)**.** *Let f be a real-valued additive function and let $\alpha(x)$ and $\beta(x)$ be real valued functions satisfying $\beta(x) \to \infty$ as $x \to \infty$ and it is slowly increasing in the sense that*

$$sup_{1\leq t\leq 2}\|\frac{\beta(x^t)}{\beta(x)} - 1\| \to 0 \text{ as } x \to \infty.$$

In order that $\nu_x(p; f(p+1) \leq z)$ converges weakly to some distribution function $F(z)$, it is necessary and sufficient that there exists a constant λ such that if Y_p (p prime) are independent random variables defined by

$$Y_p = \begin{cases} f(p) - \lambda \log p & \text{with probability } \dfrac{1}{p-1} \\ 0 & \text{with probability } 1 - \dfrac{1}{p-1} \end{cases} \tag{1.0.7}$$

then

$$P\left(\sum_{p\leq x} Y_p \leq\ z\beta(x) + \alpha(x) - \lambda \log x\right)$$

converges to the distribution function $F(z)$.

Theorem 1.0.6 is a result of great generality and includes analogues of a number of classical limit theorems for additive functions. As an example we consider the case when $F(z)$ is the normal distribution function

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-t^2/2} dt.$$

By the central limit theorem, 1.0.7 holds with $F(z) = \Phi(z)$ and a suitable function

$\alpha(x)$ if and only if, for every $\epsilon > 0$,

$$\lim_{x\to\infty} \sum_{\substack{p\le x \\ |h(p)|>\epsilon\beta(x)}} \frac{1}{p-1} = 0, \ \lim_{x\to\infty} \frac{1}{\beta(x)^2} \sum_{\substack{p\le x \\ |h(p)|\le\epsilon\beta(x)}} \frac{h(p)^2}{p-1} = 1 \tag{1.0.8}$$

where $h = f - \lambda \log$.

Thus, the distribution of additive functions on sequences of positive integers or interesting subsequences of integers is well-explored. These investigations which began with Hardy and Ramanujan, later developed in the beautiful probabilistic theory of numbers, starting with the work of Turán and culminating in the celebrated Erdős-Kac theorem. Afterwards, the mantle was taken up by many other mathematicians like Kubilius, LeVeque, Rényi, Elliott, Hildebrand to name a few, who infused finer improvements into the probabilistic theory of additive functions.

For functions which are not additive, such generalised results were not known until 1984. M. R. Murty and V. K. Murty were the first to investigate such functions and in [38], they defined a certain class of multiplicative functions $\mathcal{F}$ and for each $f \in \mathcal{F}$, proved that

$$\sum_{\substack{p\le x \\ f(p)\neq 0}} (\omega(f(p)) - \log\log p)^2 \ll \pi(x)\log\log x$$

and

$$\sum_{\substack{n\le x \\ f(n)\neq 0}} (\omega(f(n)) - \frac{1}{2}(\log\log n)^2)^2 \ll x(\log\log x)^3 \log_4 x.$$

Here, $\log_4 x$ denotes $\log\log\log\log x$. This result is also true when $\omega(n)$ is replaced by $\Omega(n)$. Following Turán's approach, this shows that the normal order of $\omega(f(n))$

is $\frac{(\log\log n)^2}{2}$. As it turns out, this class of multiplicative functions is quite general and not only does it contain simple arithmetic functions like $\sigma(n)$ and $\phi(n)$, where $\sigma(n)$ denotes the sum of divisors of n and $\phi(n)$ is the Euler totient function, but also, using the theory of ℓ -adic representations and assuming a quasi- generalised Riemann Hypothesis, one can show that (integer) Fourier coefficients of Hecke eigenforms also belong to $\mathcal{F}$. By a quasi-generalized Riemann hypothesis, we mean that there exists $\delta > 0$ such that the Dedekind zeta function $\zeta_K(s)$ for any number field has no zeroes for $\mathrm{Re}(s) > 1 - \delta$. These results can be thought of as "modular analogues" of the Hardy-Ramanujan theorem. In a later paper in 1984, M. R. Murty and V. K. Murty [39] also address the distribution of $\omega(f(n))$ and $\Omega(f(n))$ for $f \in \mathcal{F}$ and show that when normalised, they follow the normal distribution. Here we explain briefly how the quasi-Riemann hypothesis enters these questions while proving the existence of Fourier coefficients of eigenforms in $\mathcal{F}$. Consider the Ramanujan τ function defined by

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

As a consequence of his solution to the Weil conjectures, Deligne discovered the existence of an ℓ-adic representation

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to Gl_2(\mathbb{Z}_\ell)$$

such that $tr(\rho_\ell(\sigma_p)) = \tau(p)$ where σ_p denotes the Frobenius automorphism at p. Thus, questions about prime divisors of $\tau(p)$ translate to questions about the trace of the Frobenius automorphism, thus opening the entry of the Chebotarev density

theorem which is intimately connected to the theory of Artin L-series.

There are two main approaches to establishing a normal distribution result. One can compute all higher moments and use the probabilistic method that says that convergence in moments imply convergence in distribution. Another way to go about this is to compute the first and second moments of sums of "random variables" and then use the existing artillery of probabilistic results for additive functions and apply them to approximate the distribution of non-additive function. We take the second approach in this thesis, following Murty and Murty ([38] and [39]).

There is another direction of these investigations into character sums. The reduced residue class group to a prime modulus is cyclic. An estimate for the least positive representative of a generator for the group that is anywhere near the estimate guaranteed by the Riemann hypothesis for Dirichlet L-series seems very far away. In fact an old conjecture of I. M. Vinogradov that $n_2(p)$, the least positive integer that is not a square $(\mathrm{mod} p)$ is $O(p^\epsilon)$ for each fixed $\epsilon > 0$ and all odd primes p seems hardly nearer. In 1919, Pólya and Vinogradov independently established the inequality

$$|\sum_{n\leq y} \chi(n)| \leq cq^{1/2}\log q$$

for some constant c, valid uniformly for all real y and all non-principal Dirichlet characters $\chi(\mathrm{mod}\ q)$. In [28], Heilbronn proved that

$$\sum_{p\leq x}\sum_{q\leq x}\left(\frac{p}{q}\right) = O(x^{7/4}(\log x)^{-5/4}).$$

A critical application of the Pólya-Vinogradov inequality is the central idea in Heilbronn's theorem. We will generalise this result in this thesis.

1.0.1 Organisation of the thesis

We address all these aspects of probabilistic number theory in this thesis. We go back to 1917 to revisit Hardy and Ramanujan's result. In chapter 2, we re-examine this theorem and view the normal order result as an estimate on the size of an exceptional set. We show that injecting some sieve methods and some elementary inequalities into Hardy and Ramanujan's original arguments yields a more explicit bound for this set.

In Chapter 3, we investigate the normal number of prime factors of Euler ϕ function at shifts of prime arguments, that is, the normal order of $\omega(\phi(p+a))$ or $\Omega(\phi(p+a))$, for any natural number a. The same method also works for $\Omega(\sigma(p+a))$ where as before, $\sigma(n)$ denotes the sum of divisor function. $\phi(n)$ and $\sigma(n)$ belong to $\mathcal{F}$, the group of multiplicative functions, defined by Murty and Murty in [38]. They had studied $\omega(f(n))$ for $f \in \mathcal{F}$. However to study the behaviour on shift of primes, we have to employ a different "divide and conquer" method. We also study the distribution of $\omega(\phi(p+a))$ or $\Omega(\phi(p+a))$ in this chapter.

In Chapter 4, we consider the more general case and study normal order and distribution of the number of prime factors of Fourier coefficients of Hecke eigenforms at shifts of prime arguments. Using the theory of ℓ-adic representations and assuming a quasi-generalised Riemann hypothesis, we establish results in this direction as well.

We also study the moments of sums of Dirichlet characters, in the spirit of Heilbronn, in Chapter 6 and establish some normal order results. We achieve this by viewing sums of characters as sums of random variables.

Fianlly, in the last chapter, we record certain cognate ideas that arose during the course of our study, which we have relegated to future research.

Chapter 2

The Hardy-Ramanujan Theorem revisited

2.1 Introduction

The roots of probabilistic number theory are sown deep in this classical result of Hardy and Ramanujan [27] who proved more than a century ago, in 1917 that a natural number n "usually" has $\log\log n$ prime factors. The aim of this chapter is to investigate the word "usually" in the above statement and make it as precise as possible.

Let $\omega(n)$ denote the number of distinct prime factors of a natural number n. For a prime p, $\omega(p) = 1$. On the other hand, Ramanujan proved in [42] that $\omega(n)$ can take values as large as $\frac{\log n}{\log\log n}$ asymptotically. Thus the function $\omega(n)$ behaves very erratically. But it is elementary to show that asymptotically, the average value of $\omega(n)$ as n ranges over integers $\leq x$ is $\log\log x$. Now it is natural to ask how often $\omega(n)$ strays from its average value. To study this, Hardy and Ramanujan

coined the phrase "normal order" in [27].

We say an arithmetical function $f(n)$ has normal order $g(n)$ (continuous, monotone function) if for any $A > 0$,

$$|\{n \leq x, |f(n) - g(n)| > Ag(n)\}| = o(x) \text{ as } x \to \infty.$$

With this definition in hand, Hardy and Ramanujan proved the following remarkable result.

Theorem 2.1.1 (Hardy, Ramanujan, 1917)**.** *For any $\epsilon > 0$,*

$$\#\left\{n \leq x, |\omega(n) - \log\log n| > (\log\log n)^{1/2+\epsilon}\right\} = o(x) \text{ as } x \to \infty,$$

that is, $\omega(n)$ has normal order $\log\log n$.

They also prove in the same paper that this result is true when $\omega(n)$ is replaced by $\Omega(n)$, where $\Omega(n)$ counts the number of prime factors of n with multiplicity.

In 1934, Paul Turán gave a simple, probabilistic proof of the Hardy-Ramanujan theorem [49] where he computed the variance of $\omega(n)$ as n ranges over integers $\leq x$. Then using an idea reminiscent of Tchebycheff's inequality, he showed that the set of exceptional integers $n \leq x$ which satisfy for any $A > 0$, the inequality $|\omega(n) - \log\log n| > A\log\log n$, has size $O\left(\frac{x}{\log\log x}\right)$. He also showed that the same result holds true for $\Omega(n)$.

In this chapter, we will prove a stronger bound for the size of the exceptional set of integers in the above context, for both $\omega(n)$ and $\Omega(n)$. More precisely, we prove the following theorems.

Theorem 2.1.2. *Given any $A > 0$, let $B = (A+1)(\log(A+1)) - A$. Then*

$$\#\{n \leq x,\ |\omega(n) - \log\log n| > A\log\log n\} \ll \frac{x}{(\log x)^B}.$$

A cognate series of exercises related to this theorem appears in [26]. We give a detailed exposition for the sake of the reader and for other applications. We also prove an analogue of Theorem 2.1.2 for $\Omega(n)$.

Theorem 2.1.3. *For $A > 0$,*

$$\#\{n \leq x : \Omega(n) > (1+A)(\log\log x)\} \ll \frac{x\log\log x}{(\log x)^{(1+A)\log 2+1}}.$$

For $0 < A < 1$,

$$\#\{n \leq x : \Omega(n) < (1-A)\log\log x\}$$

$$\ll \frac{x\log\log x}{(\log x)^{(1-A)(\log(1-A)-1)+1}} + x^{3/4}(\log\log x)(\log x)^2.$$

Though Theorems 2.1.2 and 2.1.3 do not give any new information regarding the normal order of $\omega(n)$ and $\Omega(n)$, the explicit power of logarithms in the denominator of the estimates of the exceptional sets in these results plays a key role in the proofs of the theorems in later chapters. We will refer back to them according to necessity. Before proving these results in Section 2.4, we discuss some preliminaries in Section 2.2 for the sake of completeness. In Section 2.2, in subsection 2.4.1, we sketch an idea for the proofs of the main theorems of this chapter. It is worth remarking here that Theorem 2.1.2 improves upon Turán's estimate for the size of

the exceptional set. We obtain a much stronger bound here. For a proof of Theorem 2.1.3, we use Selberg's sieve to give a simpler exposition of the proof of this stronger theorem.

2.2 Preliminaries : Selberg's Sieve and some elementary inequalities

At first we give a lightning exposition of a beautiful sieve method, the discovery of which is attributed to Atle Selberg, who in the 1940s, developed this sieve, to study the zeroes of the Riemann zeta function. It is rumoured that Selberg wanted to understand Brun's sieve, but, Brun's 1915 paper was extremely difficult to read. Hence Selberg developed his own sieve method. A very elegant and enjoyable exposition to both Brun's Sieve and Selberg's sieve can be found in Chapters 6 and 7 of [13].

Suppose we are given a sequence of integers $\mathcal{A} = \{a_n\}_{n=1}^{\infty}$ and a set of primes $\mathcal{P}$. Let z be any positive real number. We would like to count the number $S(\mathcal{A}, \mathcal{P}, z)$ of $n \leq x$ such that $(a_n, P(z)) = 1$ where

$$P(z) = \prod_{\substack{p<z \\ p\in\mathcal{P}}} p,$$

that is, number of a_n's such that they are not divisible by any of primes in the set $\mathcal{P}$ which are less than z.

For each prime $p \in \mathcal{P}$, let $\mathcal{A}_p$ be a subset of $\mathcal{A}$ given by

$$\mathcal{A}_p = \{n \leq x;\ p|a_n\}.$$

We denote by d, squarefree numbers composed of primes of $\mathcal{P}$. Let $\mathcal{A}_1 = \mathcal{A}$ and for squarefree integers d composed of primes of $\mathcal{P}$, let $\mathcal{A}_d = \cap_{p|d}\mathcal{A}_p$. Then clearly,

$$S(\mathcal{A}, \mathcal{P}, z) = |\mathcal{A} \setminus \cup_{p|P(z)}\mathcal{A}_p|.$$

Write for convenience,

$$|\mathcal{A}_d| = \frac{X}{f(d)} + R_d$$

for $X = |\mathcal{A}|$ and for some multiplicative function $f(n)$ satisfying $f(p) > 1$ for any prime $p \in \mathcal{P}$.

Theorem 2.2.1 (Selberg's Sieve, 1947)**.** *In the above setting, write*

$$f(n) = \sum_{d|n} f_1(d)$$

for some multiplicative function $f_1(n)$ which is uniquely determined by f using the Möbius inversion formula; that is,

$$f_1(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}).$$

Setting $V(z) = \sum_{\substack{d \leq z \\ d|P(z)}} \frac{\mu^2(d)}{f_1(d)}$,

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{X}{V(z)} + O\left(\sum_{\substack{d_1, d_2 \leq z \\ d_1, d_2 | P(z)}} |R_{[d_1, d_2]}| \right)$$

where $[a, b]$ *denotes the least common multiple of* a *and* b.

For a proof of this theorem, see p. 120 of [13]. Let n be a natural number. Then it is elementary to show that the number of solutions of the equation $[a, b] = n$ is $d(n^2)$ where $d(n)$ is the number of divisors of n. For a proof of this fact, see p. 444 of [37]. Thus, using this we see that the error term in Selberg's sieve (Theorem 2.2.1) is

$$O\left(\sum_{t < z^2} d(t^2) |R_t| \right).$$

It is this error term that we will use in our application of Selberg's sieve in the next section.

To estimate the error stated above, we would need a small application of the Tauberian theorem. Here we state the version of the Tauberian theorem that we use in this paper, but we do not prove it here. For a proof see p. 67 of [37].

Theorem 2.2.2. *Let*

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

with $a_n = O(n^{\epsilon})$. *Suppose that* $h(s) = \zeta(s)^k g(s)$, *where* k *is a natural number and* $g(s)$

is a Dirichlet series absolutely convergent in $Re(s) > 1 - \delta$ *for* $0 < \delta < 1$. *Then,*

$$\sum_{n \leq x} a_n \sim g(1)x(\log x)^{k-1}/(k-1)!$$

as $x \to \infty$.

Finally, we state an elementary lemma which we will use in our proof in the next section. The proof of the first two parts of the lemma appears in [21]. But we include it here for the sake of completeness.

Lemma 2.2.3. *For* $\theta > 1$,

$$\sum_{k > \theta y} \frac{y^k}{k!} \leq \theta^{-\theta y} e^{\theta y};$$

for $0 < \theta < 1$,

$$\sum_{k < \theta y} \frac{y^k}{k!} \leq \theta^{-\theta y} e^{\theta y};$$

for $\theta > 1$ *and fixed* $c > 0$,

$$\sum_{\theta y + \theta c > k > \theta y} \frac{y^k}{k!} \leq \frac{\theta c e^{\theta y(-\log\theta + 1)}}{(\theta y)^{1/2}},$$

and for $\theta > 1$ *and* $\lambda > 1$,

$$\sum_{\theta y < k < \lambda y} \frac{y^k}{k!} \leq \frac{(\lambda - \theta) y e^{\theta y(-\log\theta + 1)}}{(\theta y)^{1/2}},$$

provided $y > 1$.

Proof.

$$\sum_{k > \theta y} \frac{y^k}{k!} = \theta^{-k} \sum_{k > \theta y} \frac{(\theta y)^k}{k!} \leq \theta^{-\theta y} e^{\theta y}$$

for $\theta > 1$. This proves the first part of the statement. For the second part, we note that

$$e^k \geq \frac{k^k}{k!}.$$

For $y > 1$, $y^k/k!$ is an increasing function of k when $k < \theta y$ and $\theta < 1$. Hence,

$$\sum_{k<\theta y} \frac{y^k}{k\,!} \leq (\theta)^{-\theta y} e^{\theta y}$$

For the third and fourth parts, we use the following lower bound in Stirling's formula for $n!$ (see [44]),

$$n! > \sqrt{2\pi} n^{n+1/2} e^{-n}.$$

Using this bound, we observe $\frac{y^k}{k!} \leq e^{k\log y - (k+1/2)\log k + k - \log\sqrt{2\pi}}$. Since

$$f(k) = e^{k\log y - (k+1/2)\log k + k - \log\sqrt{2\pi}}$$

is decreasing, we get that

$$\begin{aligned}\sum_{\theta y + \theta c > k > \theta y} \frac{y^k}{k\,!} &< \theta c(e^{\theta y(\log y - \log(\theta y)+1) - 1/2\log(\theta y)}) \\ &= \theta c \frac{e^{\theta y(-\log\theta + 1)}}{(\theta y)^{1/2}}\end{aligned}$$

and similarly,

$$\begin{aligned}\sum_{\theta y < k < \lambda y} \frac{y^k}{k\,!} &< (\lambda - \theta) y(e^{\theta y(\log y - \log(\theta y)+1) - 1/2\log(\theta y)}) \\ &= (\lambda - \theta) y \frac{e^{\theta y(-\log\theta + 1)}}{(\theta y)^{1/2}}\end{aligned}$$

and thus the estimate in the lemma follows. □

2.3 Revisiting the 1917 theorem of Hardy and Ramanujan

In this section, we revisit Theorem 2.1.1 and walk through the original proof given by Hardy and Ramanujan. As Erdős mentions in [19], this proof is "elementary but fairly complicated" and uses an estimate on the number of integers $\leq x$ having exactly k prime factors. Landau had obtained such a result for a fixed k and Hardy and Ramanujan extended it for all k. They prove by the principle of mathematical induction the following lemma.

Lemma 2.3.1. *There are absolute constants K and C such that*

$$f_{k+1}(x) < \frac{Kx}{\log x}\frac{(\log\log x + C)^k}{k!} \tag{2.3.1}$$

for $k = 0, 1, 2, \cdots$, *and* $x \geq 2$ *where* $f_k(x)$ *denotes the number of integers* $n \leq x$ *with* $\omega(n) = k$.

As mentioned above, Landau (see [26]) proved in 1900 that, for each fixed k,

$$f_k(x) \sim \frac{x}{\log x}\frac{(\log\log x)^{(k-1)}}{(k-1)!}$$

as $x \to \infty$. This result has been generalised by many authors like Selberg, Norton, Tenenbaum and it remains true, whether $\omega(n)$ is replaced by the number of prime factors belonging to certain subsets (to be described in the theorem below)

of primes or k is allowed to tend to ∞ with x suitably slowly. The most general version is that of Halasz who proved the following in 1972.

Theorem 2.3.2 (Halasz, 1972)**.** *Let E be an arbitrary set of primes and p_o be the minimum of $\{p : p \in E\}$ and define*

$$E(x) = \sum_{\substack{p \leq x \\ p \in E}} \frac{1}{p},$$

$$\Omega(n, E) = \sum_{\substack{p^{\alpha} | n \\ p \in E}} \alpha.$$

Then, uniformly for $0 \leq k \leq (p_0 - \epsilon)E(x)$, we have both

$$|\{n : n \leq x, \Omega(n, E) = k\}| \ll_{\epsilon, p_o} \frac{xe^{-E(x)}E(x)^k}{k!}$$

and

$$\sum_{\substack{n \leq x \\ \Omega(n,E)=k}} \frac{1}{n} \ll_{\epsilon, p_0} \frac{(\log x)e^{-E(x)}E(x)^k}{k!}.$$

To stay on track, let us sketch the original proof of Lemma 2.3.1, given by Hardy and Ramanujan.

Proof of Lemma 2.3.1 As stated above, Hardy and Ramanujan use induction on k to prove this lemma. The inequality follows trivially for $k = 0$ for any constant C from Chebyshev's estimate in the prime number theorem. This is the base case of induction. One knows from elementary number theory (see p. 37 of [37]) that

$$\sum_{p \leq x} \frac{1}{p} < \log\log x + C_1 \tag{2.3.2}$$

and

$$\sum_{p\leq x}\frac{\log p}{p} < C_2 \log x \tag{2.3.3}$$

where C_1 and C_2 are constants. We will prove by induction that (2.3.1) is true if $C > C_1 + C_2 + C_3$ where

$$C_3 = \sum_{s=2}^{\infty}(s+1)(2^{-s}+3^{-s}+5^{-s}+\cdots) \tag{2.3.4}$$

Consider numbers $\leq x$, which for some prime $P \leq x$ belong to the table

$$2^a q_1^{a_1} q_2^{a_2}\cdots q_k^{a_k},$$

$$3^a q_1^{a_1} q_2^{a_2}\cdots q_k^{a_k},$$

$$\cdots\cdots\cdots\cdots,$$

$$P^a q_1^{a_1} q_2^{a_2}\cdots q_k^{a_k},$$

where $q_1 < q_2 \cdots < q_k$, are primes and $q_k \geq 2$ in first row, $q_k \geq 3$ in second row and so on. Clearly, $P \leq x^{1/2}$ if $a = 1$, and $P \leq x^{1/3}$ if $a = 2, \cdots$. Then the total number of integers in the table of integers above is bounded above by

$$\sum_{p^{a+1}\leq x} f_k\left(\frac{x}{p^a}\right).$$

If $u_1, u_2, \cdots$ are primes, with $u_1 < u_2 < \cdots < u_{k+1}$ and $m = u_1^{a_1} u_2^{a_2}\cdots u_{k+1}^{a_{k+1}} \leq x$, then m occurs at least k many times in one of the tables which correspond to

different values of a. This implies that

$$kf_{k+1}(x) \leq \sum_{p^2 \leq x} f_k(\frac{x}{p}) + \sum_{p^3 \leq x} f_k(\frac{x}{p^2}) + \cdots . \tag{2.3.5}$$

Let us assume the induction hypothesis that the statement in the lemma is true for k. Thus we got from (2.3.5) that

$$f_{k+1}(x) < \frac{Kx(\log\log x + D)^{k-1}}{k!} \left[\sum_{p^2 \leq x} \frac{1}{p \log(x/p)} + \sum_{p^3 \leq x} \frac{1}{p^2 \log(x/p^2)} + \cdots \right]$$

Now since $(1-x)^{-1} = 1 + x + x^2 + \cdots$,

$$\begin{aligned} \frac{1}{\log(x/p)} &= \frac{1}{\log x - \log p} \\ &= \frac{1}{\log x} \left(1 - \frac{\log p}{\log x}\right)^{-1} \\ &= \frac{1}{\log x} \left(1 + \frac{\log p}{\log x} \left(1 + \frac{\log p}{\log x} + \cdots\right)\right) \\ &\leq \frac{1}{\log x} + \frac{2\log p}{(\log x)^2} \end{aligned}$$

since $\log p \leq \frac{1}{2}\log x$. This implies that

$$\begin{aligned} \sum_{p^2 \leq x} \frac{1}{p \log(x/p)} &< \left(\frac{1}{\log x} \left(\sum_{p^2 \leq x} \frac{1}{p} \right) + \frac{2}{(\log x)^2} \left(\sum_{p^2 \leq x} \frac{\log p}{p} \right) \right) \\ &< \frac{\log\log x + C_1}{\log x} + \frac{C_2}{\log x} \\ &= \frac{\log\log x + C_1 + C_2}{\log x}. \end{aligned}$$

Also, if $p^{s+1} \leq x$, then $\frac{x}{p^s} \geq x^{1/(s+1)}$,

$$\log(\frac{x}{p^s}) \geq \frac{\log x}{s+1}$$

and so

$$\sum_{p^{s+1} \leq x} \frac{1}{p^s \log(x/p^s)} \leq \frac{s+1}{\log x} \left(2^{-s} + 3^{-s} + 5^{-s} + \cdots\right), s \geq 2.$$

Then,

$$\begin{aligned}\sum_s \sum_{p^{s+1} \leq x} \frac{1}{p^s \log(x/p^s)} &< \frac{\log\log x + C_1 + C_2 + C_3}{\log x} \\ &< \frac{\log\log x + C}{\log x}.\end{aligned}$$

Then, by induction, the lemma follows.

□

To prove the main theorem, it is enough to prove that

$$S_1 = \sum_{k < \log\log x - (\log\log x)^{1/2+\epsilon}} f_{k+1}(x) = o(x)$$

and

$$S_2 = \sum_{k > \log\log x + (\log\log x)^{1/2+\epsilon}} f_{k+1}(x) = o(x)$$

The estimations of both these sums are similar so we just consider S_2 here. Using

the upper bound of $f_{k+1}(x)$ from the lemma, we see that

$$S_2 < K\frac{x}{\log x}\sum_{k>\log\log x+(\log\log x)^{1/2+\epsilon}}\frac{(\log\log x+C)^k}{k!}.$$

Let $\log\log x + C = \xi$. Then, the condition $k > \log\log x + (\log\log x)^{1/2+\epsilon}$ with any $\epsilon > 0$, is equivalent to the condition that $k > \xi + \psi\sqrt{\xi}$ where ψ is some function of ξ which tends steadily to ∞ with ξ, that is, we need to show that

$$S = \sum_{k>\xi+\psi\sqrt{\xi}}\frac{\xi^k}{k!} = o(e^\xi).$$

Let $0 < \delta < 1$ be such that

$$\sum_{k=1}^{\infty}\frac{\delta^k}{(k+1)(k+2)} < \frac{1}{4}$$

and

$$S = S' + S''$$

where

$$S' = \sum_{\xi+\psi\sqrt{\xi}<k<(1+\delta)\xi}\frac{\xi^k}{k!}$$

and

$$S'' = \sum_{k>(1+\delta)\xi}\frac{\xi^k}{k!}.$$

Then,

$$\begin{aligned} S'' &< \frac{\xi^{k_1}}{k_1!}\left[1+\frac{\xi}{k_1+1}+\frac{\xi^2}{(k_1+1)(k_1+2)}+\cdots\right] \\ &< \frac{\xi^{k_1}}{k_1!}\left(\sum_{m=0}^{\infty}\frac{1}{(1+\delta)^m}\right) \\ &= \frac{1+\delta}{\delta}\frac{\xi^{k_1}}{k_1!} \end{aligned}$$

where k_1 is the smallest integer greater than $(1+\delta)\xi$. Then

$$\begin{aligned} S'' &< \frac{K}{\delta\sqrt{k_1}}\exp(k_1(\log\xi-\log k_1+1)) \\ &< \frac{K}{\delta\sqrt{\xi}}e^{\Delta\xi} \end{aligned}$$

where K is the absolute constant and $\Delta = (1+\delta)\log(1+\delta)-\delta$. Since $\Delta > 0$, clearly

$$S'' = o(e^{\xi})$$

as we wanted. To estimate S', writing $k = \xi+\mu$ with $\psi\sqrt{\xi} < \mu \leq \delta\xi$, we get

$$\begin{aligned} \frac{\xi^k}{k!} &= \frac{\xi^{\xi+\mu}}{(\xi+\mu)!} \\ &< \frac{K}{\sqrt{\xi}}\exp\left((\xi+\mu)\log\xi-(\xi+\mu)\log(\xi+\mu)+(\xi+\mu)\right) \\ &= \frac{K}{\sqrt{\xi}}\exp\left((\xi+\mu)\left(\sum_{r=0}^{\infty}(-1)^r\frac{\mu^r}{r\xi^r}\right)\right) \\ &< \frac{K}{\sqrt{\xi}}e^{\xi-(\mu^2/4\xi)} \end{aligned}$$

Thus,

$$\begin{aligned} S' &\ll \frac{e^{\xi}}{\sqrt{\xi}} \left(\sum_{\mu=\psi\sqrt{\xi}}^{\delta\xi} e^{-(\mu^2/4\xi)} \right) \\ &\ll \frac{e^{\xi}}{\sqrt{\xi}} \int_{\psi\sqrt{\xi}}^{\delta\xi} e^{-t^2/4\xi} dt \\ &= o(e^{\xi}) \end{aligned}$$

as $\psi \to \infty$. This proves the theorem.

2.4 Proofs of Theorems 2.1.2 and 2.1.3

In this section we prove the theorems stated in Section 2.1. We first give a summary of the method we use to prove the same.

2.4.1 Strategy of proof of Theorems 2.1.2 and 2.1.3

We will follow the same strategy to prove both Theorem 2.1.2 and Theorem 2.1.3. As discussed in Section 2.3, in [27], Hardy and Ramanujan estimated an upper bound for

$$f_k(x) = \#\{n \leq x : \omega(n) = k\},$$

for any $k = 1, 2, 3, \cdots$. Using Selberg's sieve, we will estimate in Lemma 2.4.3, $\tilde{f}_k(x)$, which is the number of elements in the set,

$$\{n \leq x : \Omega(n) = k\},$$

for $k = 1, 2, 3, \cdots$. Another uniform (in k) upper bound for $\tilde{f}_k(x)$ is proved in [26]. We mention it in Theorem 2.4.4 and use it together with our estimate of $\tilde{f}_k(x)$ to prove Theorem 2.1.3.

Next, since $\Omega(n) \leq \frac{\log n}{\log 2}$ for any integer n, to prove Theorem 2.1.2 we would want to estimate for a given $A > 0$, the sum

$$\begin{aligned} S_1 = \sum_{\substack{n \leq x \\ \frac{\log x}{\log 2} > \omega(n) > (A+1)\log\log x}} 1 &= \sum_{\frac{\log x}{\log 2} > k > (A+1)\log\log x} \sum_{\substack{n \leq x \\ \omega(n)=k}} 1 \\ &= \sum_{\frac{\log x}{\log 2} > k > (A+1)\log\log x} f_k(x) \end{aligned}$$

and for $0 < A < 1$, the sum

$$S_2 = \sum_{\substack{n \leq x \\ \omega(n) < (1-A)\log\log x}} 1 = \sum_{k < (1-A)\log\log x} \sum_{\substack{n \leq x \\ \omega(n)=k}} 1 = \sum_{k < (1-A)\log\log x} f_k(x).$$

Then,

$$|\{n \leq x,\ |\omega(n) - \log\log n| > A\log\log n\}| = S_1 + S_2.$$

Similarly, to prove Theorem 2.1.3, we would want to estimate for $0 < A < 1$,

$$T_2 = \sum_{k < (1-A)\log\log x} \tilde{f}_k(x)$$

and for any given $A > 0$,

$$T_1 = \sum_{k > (A+1)\log\log x} \tilde{f}_k(x).$$

We stated an elementary lemma (Lemma 2.2.3) in Section 2.2, which enables us to establish upper bounds for these sums, thus proving Theorem 2.1.2 and Theorem 2.1.3.

2.4.2 Proofs of related lemmas and Theorem 2.1.2 and 2.1.3

To begin this section, we state the following lemma which is crucial in our proof of Theorem 2.1.2. We sketched its proof in Section 2.3.

Lemma 2.4.1. *As in Section 2.3, let* $f_k(x) = \#\{n \leq x;\ \omega(n) = k\}$. *Then, there are absolute constants C and D such that*

$$f_{k+1}(x) < \frac{Cx}{\log x}\frac{(\log\log x + D)^k}{k!}$$

for $k = 0, 1, 2, \cdots$.

To prove an analogue of this result for $\Omega(n)$, we need to estimate $\sum_{t\leq z} d(t^2)$.

Lemma 2.4.2. *Let* $d(n)$ *denote the number of divisors of n. Then,*

$$\sum_{t\leq z} d(t^2) \sim g(1)\frac{z(\log z)^2}{2}$$

where $g(s)$ *is a Dirichlet series converging absolutely in* $Re(s) > 1/2$.

Proof. The proof follows from an application of the Tauberian theorem (Theorem 2.2.2) mentioned in Section 2.2. Let

$$h(s) = \sum_{n=1}^{\infty} \frac{d(n^2)}{n^s}.$$

By Euler product factorisation, we get that $h(s)$ is

$$\begin{aligned}
&\prod_p \left(1+\frac{d(p^2)}{p^s}+\frac{d(p^4)}{p^{2s}}+\cdots\right)\\
=&\prod_p \left(1+\frac{3}{p^s}+\frac{5}{p^{2s}}+\cdots\right)\\
=&\zeta(s)^3\prod_p \left(1-\frac{1}{p^s}\right)^3\left(1+\frac{3}{p^s}+\frac{5}{p^{2s}}+\cdots\right)\\
=&\zeta(s)^3\prod_p \left(1-\frac{1}{p^{2s}}+\cdots\right)\\
=&\zeta(s)^3 g(s).
\end{aligned}$$

Here $g(s)$ denotes the Dirichlet series which has Euler factorisation given by

$$\prod_p \left(1-\frac{1}{p^{2s}}+\cdots\right)$$

as above. Hence it converges absolutely in $\mathrm{Re}(s) > 1/2$. Hence by the Theorem 2.2.2, the lemma follows. □

Now we are equipped to prove the following analogue of Lemma 2.4.1.

Lemma 2.4.3. *Let $\tilde{f}_k(x) = \#\{n \le x;\ \Omega(n) = k\}$. Then there are absolute constants C' and D' such that*

$$\tilde{f}_{k+1}(x) < C'\frac{kx}{\log x}\frac{(\log\log x + D')^k}{k!} + O\left(\frac{x^{1/2+1/2k}(\log x)^2}{4k^2}\right)$$

for all positive integers k.

Proof. For any positive real number z, we say a positive integer m is z-smooth if

$p|m \implies p \leq z$ and m is z-crunchy if $p|m \implies p > z$.

Any integer $n \leq x$ can be expressed as $n = a \cdot b$ where a is z-smooth and b is z-crunchy and z is a parameter to be chosen later. Now let n be such that $\Omega(n) = k$. Write $n = a \cdot b$ as above. If $\Omega(a) = k$, then $b = 1$ and number of such integers $n \leq x$ is at most z^k. Otherwise if $\Omega(a) \leq (k-1)$, then fixing such an a, let

$$S_a(x) = \#\left\{n \leq x : \ n \equiv 0 \ (\mathrm{mod}\ a),\ \frac{n}{a} \text{ has no prime factor less than z}\right\}.$$

Then,

$$\tilde{f_k}(x) = \sum_{\substack{a \leq z^{k-1} \\ \Omega(a) \leq k-1}} S_a(x) + O(z^k).$$

Now in order to use Theorem 2.2.1 to estimate $S_a(x)$, we set up our sieve problem.

Let $\mathcal{A} = \{n \leq x;\ n \equiv 0 (\mathrm{mod}\ a)\}$. Let $\mathcal{P}$ be the set of primes less than z. For each prime $q \in \mathcal{P}$,

$$\mathcal{A}_q = \{n \leq x;\ n \equiv 0 \ (\mathrm{mod}\ a),\ n \equiv 0 \ (\mathrm{mod}\ q),\ (a,q) = 1\}.$$

Then, clearly, $S_a(x) = S(\mathcal{A}, \mathcal{P}, z)$. Clearly, $|\mathcal{A}| = [x/a] = x/a + O(1)$ and $|\mathcal{A}_q| = \frac{x/a}{q} + O(1)$. It is easy to show that with notation as in Theorem 2.2.1, $f_1(d) = \phi(d)$ and $V(z) \geq \log z + O(1)$. Hence, we get

$$S_a(x) \leq \frac{x}{a \log z} + O\left(\sum_{t \leq z^2} d(t^2)\right).$$

The error above is $O(z^2(\log z)^2)$ by Lemma 2.4.2. Thus, we get,

$$\begin{aligned}\tilde{f}_k(x) &\leq \sum_{\substack{a\leq z^{k-1}\\ \Omega(a)\leq k-1}} \frac{x}{a\log z} + O\left(\sum_{\substack{a\leq z^{k-1}\\ \Omega(a)\leq k-1}} z^2(\log z)^2\right) + O(z^k).\\ &= \frac{x}{\log z}\sum_{\substack{a\leq z^{k-1}\\ \Omega(a)\leq k-1}} \frac{1}{a} + O(z^{1+k}(\log z)^2) + O(z^k)\\ &\leq \frac{x}{\log z}\frac{\left(1+\sum_{p\leq z^{k-1}}\frac{1}{p}\right)^{k-1}}{(k-1)\,!} + O(z^{1+k}(\log z)^2).\end{aligned}$$

Choosing $z = x^{\frac{1}{2k}}$ for $k \geq 1$ and using the elementary fact that

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + O(1),$$

we get

$$\tilde{f}_k(x) \leq \frac{2C'kx}{\log x}\frac{(\log\log x^{(k/2k-1/2k)} + D')^{k-1}}{(k-1)\,!} + O\left(\frac{x^{1/2k+k/2k}(\log x)^2}{4k^2}\right)$$

for some absolute constants C' and D' which upon simplification gives the theorem. □

We also state the following upper bound for $\tilde{f}_k(x)$ obtained by Hall and Tenenbaum in p. 12 of [26].

Theorem 2.4.4 (Hall, Tenenbaum)**.** *Let* $\tilde{f}_k(x) = \#\{n \leq x;\ \Omega(n) = k\}$ *. Then*

$$\tilde{f}_k(x) \ll \frac{x}{\log x}\frac{k}{2^k}$$

uniformly for $k \geq 1$, $x \geq 2$.

Proof of Theorem 2.1.2 As explained in Section 2.4.1, we want to estimate

$$S_1 = \sum_{\frac{\log x}{\log 2} > k > (A+1)\log\log x} f_k(x)$$

and

$$S_2 = \sum_{k < (1-A)\log\log x} f_k(x).$$

First, we estimate S_1. Since

$$S_1 \leq \sum_{k > (A+1)\log\log x} f_k(x),$$

by using Lemma 2.4.1, we get

$$\begin{aligned} S_1 &\leq \frac{Cx}{\log x} \sum_{k > (A+1)\log\log x} \frac{(\log\log x + D)^{k-1}}{(k-1)\,!} \\ &= U_1 + U_2 \end{aligned}$$

where

$$U_1 = \frac{Cx}{\log x} \sum_{k > (A+1)(\log\log x + D)} \frac{(\log\log x + D)^{k-1}}{(k-1)\,!}$$

and

$$U_2 = \frac{Cx}{\log x} \sum_{(A+1)(\log\log x + D) > k > (A+1)\log\log x} \frac{(\log\log x + D)^{k-1}}{(k-1)\,!}.$$

Then using the first part of Lemma 2.2.3, we get that

$$\begin{aligned} U_1 &\leq \frac{Cx}{\log x}(A+1)^{-(A+1)(\log\log x+D)}e^{(A+1)(\log\log x+D)} \\ &= \frac{Cx}{\log x}e^{(A+1)(1-\log(A+1))\log\log x}e^{(A+1)D(1-\log(A+1))} \\ &\leq \frac{C_1 x}{\log x}(\log x)^{(A+1)(1-\log(A+1))}. \end{aligned}$$

Using second part of Lemma 2.2.3, we get

$$U_2 \leq (A+1)De^{-(A+1)(\log(A+1)-1)(\log\log x+D)}.$$

Thus, we get

$$S_1 \leq \frac{\hat{C}x}{(\log x)^{(A+1)(\log(A+1)-1)+1}}.$$

Now to estimate S_2, using Lemma 2.4.1 and the second part of Lemma 2.2.3, we get that for $0 < A < 1$,

$$\begin{aligned} S_2 &\leq \frac{Cx}{\log x}\sum_{k<(1-A)\log\log x}\frac{(\log\log x+D)^{k-1}}{(k-1)\,!} \\ &\leq \frac{Cx}{\log x}\sum_{k<(1-A)(\log\log x+D)}\frac{(\log\log x+D)^{k-1}}{(k-1)\,!} \\ &\leq \frac{\hat{C}x}{(\log x)^{(1-A)(\log(1-A)-1)+1}}. \end{aligned}$$

Thus combining the two estimates for S_1 and S_2, we get that

$$|\{n \leq x,\ |\omega(n)-\log\log n| > A\log\log n\}| = O\left(\frac{x}{(\log x)^{(A+1)(\log(A+1)-1)+1}}\right).$$

This proves the theorem. □

Clearly, this proof is much more organised and easier to follow than Hardy and Ramanujan's original proof. We can work in the same framework now to obtain similar upper bound for exceptional sets associated to $\Omega(n)$.

Proof of Theorem 2.1.3 As before, we first want to estimate for $A > 0$,

$$T_1 = \sum_{k>(A+1)\log\log x} \tilde{f}_k(x)$$

For this we use Hall and Tenenbaum's estimate from Theorem 2.4.4 in the following manner.

Let $f(t) = \dfrac{t}{2^t}$ for any $t > 1$. Then clearly $f(t)$ is a decreasing function since

$$\begin{aligned} &\frac{k}{2^k} > \frac{k+1}{2^{k+1}} \\ \iff &\frac{k}{k+1} > \frac{1}{2} \\ \iff &2k > k+1 \iff k > 1. \end{aligned}$$

Then, $f(k) < \int_{k-1}^{k} f(t)dt$. For any $N > 0$, summing over all $k > N$, we get

$$\sum_{k>N} f(k) < \int_{N-1}^{\infty} f(t)dt.$$

Using $f(t) = te^{-(\log 2)t}$, and substituting $s = (\log 2)t$, we see that the integral is

$$\frac{1}{(\log 2)^2} \int_{(\log 2)N-1}^{\infty} se^{-s}ds$$

which evaluates to

$$\frac{N-1}{(\log 2)}\frac{1}{e^{(N-1)\log 2}}+\frac{1}{(\log 2)^2}e^{-(N-1)\log 2}.$$

To estimate T_1, substituting $N=(1+A)\log\log x$, we get an upper bound of

$$\tilde{C}\frac{x\log\log x}{(\log x)^{(1+A)\log 2+1}}$$

which proves the first part of the theorem. To estimate T_2, we use Lemma 2.4.3 and the second part of Lemma 2.2.3 and get that for $O<A<1$,

$$\begin{aligned}
T_2 &\leq \frac{C'x}{\log x}\sum_k k\frac{(\log\log x+D')^{k-1}}{(k-1)\,!}+O\left((\log x)^2\sum_k\frac{x^{1/2+1/2k}}{4k^2}\right)\\
&\leq \frac{\tilde{C}x\log\log x}{\log x}\sum_k\frac{(\log\log x+D')^{k-1}}{(k-1)\,!}+O\left(x^{3/4}(\log x)^2(\log\log x)\right)\\
&\leq \frac{\hat{C}x\log\log x}{(\log x)^{(1-A)(\log(1-A)-1)+1}}+O\left(x^{3/4}(\log x)^2(\log\log x)\right).
\end{aligned}$$

Here in the above calculation, $\sum_k$ is the sum over all k with $k<(1-A)\log\log x$. Thus, this proves the other part of the theorem. □

Chapter 3

On the normal number of prime factors of the Euler phi function at shifts of prime arguments

In 1935, Paul Erdős [18] used Hardy and Ramanujan's method of proof from their 1917 paper, along with Brun's sieve to show that for a prime p, the normal number of prime factors of $p-1$ is $\log\log p$. In particular, he showed, given any $\epsilon > 0$,

$$\#\{p \leq x : \ |\Omega(p-1) - \log\log p| > \epsilon \log\log p\} = O\left(\frac{x}{(\log x)^{1+\delta}}\right),$$

for some δ sufficiently small. In this chapter, we first prove the following stronger variant of Erdős's result, with a more explicit error term.

Theorem 3.0.1. *Given any $A > 4$, set $c(A) = (A+1)(\log 2) - 2$. Then,*

$$\#\{p \leq x : \Omega(p-1) > A\log\log x\} = O\left(\frac{\pi(x)}{(\log x)^{c(A)}}\right).$$

In 1995, Timofeev [47] proved an explicit result of the similar form using Selberg's sieve and the Bombieri - Vinogradov theorem. His result is very general in nature, where he considers primes p in a given set. In this chapter, we revisit Erdős's method of proof (involving Brun's Sieve) and use some elementary inequalities to simplify his arguments and hence get an explicit error term in the process for the classical case, which is sufficient for our purposes.

In 1984, R. Murty and K. Murty [38] proved a general normal order result applicable to a wide class of functions including Fourier coefficients of Hecke eigenforms. This general result applies to the study of the number of prime factors of $\phi(p) = p-1$ and $\phi(n)$. They use Turán's probabilistic method of proof to prove this general theorem. All these methods break down if we want to study $\phi(p+1)$ or in general, $\phi(p+a)$. In Section 4, we adapt Turán's normal order method, equipped with the above stronger version of Erdős's result to prove that the normal order of $\omega(\phi(p+a))$ and $\Omega(\phi(p+a))$ for any non-zero integer a, is $\frac{1}{2}(\log\log p)^2$. More precisely, we show

Theorem 3.0.2. *For any $a \neq 0$, $a \in \mathbb{Z}$,*

$$\sum_{p\leq x}\left(\Omega(\phi(p+a)) - \frac{(\log\log x)^2}{2}\right)^2 = \pi(x)\frac{(\log\log x)^3}{3} + o(\pi(x)(\log\log x)^3);$$

which implies, $\Omega(\phi(p+a))$ has normal order $\dfrac{(\log\log p)^2}{2}$.

In Section 5, we also obtain a distribution function for $\omega(\phi(p+a))$ and $\Omega(\phi(p+a))$, that is, we show that

$$\frac{\omega(\phi(p+a)) - \frac{1}{2}(\log\log p)^2}{((\log\log p)^{3/2}/\sqrt{3})}$$

is normally distributed. More precisely, we prove:

Theorem 3.0.3. *For any non-zero integer a,*

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\left|\left\{p\le x;\frac{\Omega(\phi(p+a))-\frac{1}{2}(\log\log x)^2}{(\log\log x)^{3/2}}\le\frac{\alpha}{\sqrt{3}}\right\}\right|=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\alpha}e^{-t^2/2}dt.$$

i.e., $\Omega(\phi(p+a))$, under suitable normalisation, is "normally distributed".

This is the analog of the general theorem of R. Murty and K. Murty [39] which they proved for $\omega(\phi(n))$ (that was also proved independently by Erdős and Pomerance [22]). In [2], Bassily, Kátai and Wijsmuller prove normal distribution for iterates of the ϕ function at natural numbers and also shifts of primes. Their remarkable results are more general than Theorem 3.0.2 and Theorem 3.0.3. However, we give a simpler proof in this particular case.

Some intuition will guide the reader through this chapter. By the theorem of Hardy and Ramanujan, a random integer n has "usually" $\log\log n$ prime factors. If p is prime and a is a non-zero integer, we expect $p+a$ to be "random" in the sense that we expect it to have "usually" $\log\log p$ prime factors.

If now we take a multiplicative function f and consider

$$f(p+a)=\prod_{q^\alpha||p+a}f(q^\alpha)$$

we expect that the number of prime factors on the right side to be "usually" $\log\log p$. If the $f(q^\alpha)$ are "independent", we would then expect each factor to have $\log\log p$ prime factors so that $f(p+a)$ has around $(\log\log p)^2$ prime factors. This is the correct order of magnitude apart from the constant $\frac{1}{2}$ that emerges from a careful analysis. One way to heuristically see the constant $\frac{1}{2}$ is to note that for a typical integer

n (and hence presumably for a typically shifted prime), its $\log\log n$ prime factors are roughly uniformly distributed, on the log-log scale, in the interval $[0, \log\log n]$. In other words the j-th smallest prime factor p_j of n tends to satisfy $\log\log p_j \sim j$. Then $\log\log(f(p_j^{\alpha})) \sim j$ as well, and so the expected number of prime factors of $f(n)$ is the sum of j as j runs from 1 to $\log\log n$, which is $\frac{(\log\log n)^2}{2}$.

This heuristic reasoning can be made rigorous by the "divide and conquer" method; we approximate our complicated function by suitable additive functions and inject results from sieve theory and probabilistic number theory.

3.1 Preliminaries: Brun's sieve and error in the estimate of number of primes in arithmetic progression

At first, we give a brief review to Brun's sieve which we use in Section 3.3 to revisit Theorem 3.0.1. For an introduction, see [13] or [25].

Suppose we are given a sequence of integers $\mathcal{A} = \{a_n\}_{n=1}^{\infty}$. For any square-free $d > 0$, we denote by $\mathcal{A}_d = \{a : a \in \mathcal{A}, d|a)\}$. Clearly for $d = 1$, $|\mathcal{A}| = |\mathcal{A}_d|$. Let X be a convenient close approximation to $|\mathcal{A}|$. Let $r_1 = |\mathcal{A}| - X$. For a prime p, choose $w_o(p)$ such that $(\frac{w_o(p)}{p})X$ estimates $|\mathcal{A}_p|$. Set for all primes p, $r_p := |\mathcal{A}_p| - (\frac{w_o(p)}{p})X$. Define $w_0(1) = 1$, and for a square-free integer $d > 0$, $w_0(d) = \prod_{p|d} w_o(p)$ and $r_d := |\mathcal{A}_d| - \frac{w_o(d)}{d}X$. Suppose $\mathcal{P}$ is a set of primes. Let $P(z) = \prod_{\substack{p<z \\ p\in\mathcal{P}}} p$. The sieve problem is to estimate

$$S(\mathcal{A}, \mathcal{P}, z) := |\{a \in \mathcal{A} : (a, P(z)) = 1\}|.$$

For a suitable description of divisibility properties of $\mathcal{A}$ relative to $\mathcal{P}$, it is natural to consider the arithmetic function

$$w(p) = \begin{cases} w_0(p), \text{ if } p \in \mathcal{P}; \\ 0, \text{ otherwise.} \end{cases} \tag{3.1.1}$$

Then $w(1) = 1$, $w(d) = \prod_{p|d} w(p)$ for a square-free integer d. Clearly, w is a multiplicative function and we set $R_d = |\mathcal{A}_d| - \left(\frac{w(d)}{d}\right) X$. We make the following assumptions.

1. Suppose there is a constant A_0 such that $w(p) \leq A_0$ for all primes p. Call this condition (Ω_0).

2. Also, further assume for some suitable constant $A_1 \geq 1$, $0 \leq \frac{w(p)}{p} \leq 1 - \frac{1}{A_1}$. Call this condition (Ω_1).

Define $W(z) = \prod_{p<z} \left(1 - \frac{w(p)}{p}\right)$. Also for d square-free

$$g(d) := \frac{w(d)}{d \prod_{p|d} \left(1 - \frac{w(p)}{p}\right)}$$

is well defined and the product in the denominator is bounded away from 0. We now impose further conditions :

1. Let A_1' be such that $g(p) \leq A_1' \frac{w(p)}{p}$. Call this condition (Ω_1').

2. For a suitable $\kappa > 0$, $A_2 \geq 1$,

$$\sum_{w \leq p < z} \frac{w(p) \log p}{p} \leq \kappa \log \frac{z}{w} + A_2$$

if $2 \leq w \leq z$. Call this condition $(\Omega_2(\kappa))$.

3. By (R), we denote the condition that

$$|R_d| \leq w(d)$$

whenever d is square-free and $p|d \implies p \in \mathcal{P}$.

We have the following general upper bound result to estimate $S(\mathcal{A}, \mathcal{P}, z)$ when we impose the above conditions. For a proof, see Theorem 2.2, pg. 68 of [25].

Theorem 3.1.1 (Brun's Sieve)**.** *Assume (Ω_1), $(\Omega_2(\kappa))$, (R) hold. Then for any $A > 0$,*

$$S(\mathcal{A}, \mathcal{P}, z) \leq B_5 X \prod_{p<z} \left(1 - \frac{w(p)}{p}\right),\ z < X^{1/A}$$

and

$$S(\mathcal{A}, \mathcal{P}, z) \leq B_5 X \prod_{p<X} \left(1 - \frac{w(p)}{p}\right),\ z \geq X^{1/A}.$$

Here B_5 is a constant depending on A, A_1, A_2, κ. Also $(\Omega_2(\kappa))$ can be replaced by (Ω_0).

As an application of Theorem 3.1.1, we prove the following theorem.

Theorem 3.1.2. *Given any $a > 0$ and $a < x$, we have the estimate :*

$$\left| \left\{ q \leq x : q \text{ prime}, a|(q-1),\ \frac{q-1}{a} \text{ prime} \right\} \right| \ll \frac{x}{a} \frac{(\log\log a)^2}{(\log \frac{x}{a})^2}.$$

Proof. Let

$$S_a(x) = \left| \left\{ q \leq x : q \text{ prime}, a|(q-1),\ \frac{q-1}{a} \text{ prime} \right\} \right|.$$

Writing $q-1=a\cdot t$, $q\leq x$, we get

$$S_a(x)=\Big|\Big\{t\leq\frac{x}{a},\ t \text{ prime}, at+1 \text{ prime}\Big\}\Big|.$$

Let $\mathcal{A}=\{t\leq x/a\}$. Set $\mathcal{P}=\{p\leq z : p\nmid a\}$, where z is a parameter to be chosen later. For any prime p, set

$$\begin{aligned}\mathcal{A}_p&=\{t\leq x/a;\ p|t, \text{ or } p|(at+1)\}\\&=\{t\leq x/a;\ t\equiv 0\ (\text{mod } p),\ at+1\equiv 0\ (\text{ mod } p)\}.\end{aligned}$$

Now if $p|a$, then there is no t such that $at+1\equiv 0\ (\text{mod } p)$, so we see $w(p)=1$ in this case. If $p\nmid a$, $t\in\mathcal{A}_p$ must belong to one of the two residue classes mod p, that is, for $p<z$

$$w(p)=\begin{cases}2,\ p\nmid a;\\ 1,\ \text{otherwise.}\end{cases}\tag{3.1.2}$$

Also, $|\mathcal{A}|=\left[\frac{x}{a}\right]$. Below a^{-1} is the residue class $<p$ which is inverse to a (mod p).

With $\{x\}$ denoting the fractional part of x, we have:

$$|\mathcal{A}_p| = \begin{cases} \left[\frac{x/a}{p}\right], \ p|a, \\ \left[\frac{x/a}{p}\right] + \left[\frac{\frac{x}{a}+a^{-1}}{p}\right], \ p \nmid a \end{cases}$$
$$= \begin{cases} \frac{x}{ap} + \left\{\frac{x}{ap}\right\}, p|a \\ \frac{x}{ap} + \frac{x/a+a^{-1}}{p} + \left\{\frac{x}{ap}\right\} + \left\{\frac{x/a+a^{-1}}{p}\right\}, p \nmid a \end{cases}$$
$$= \begin{cases} \frac{x}{ap} + R_p, p|a \\ \frac{2x}{ap} + R_p, p \nmid a. \end{cases}$$

where $|R_p| \leq 1$ when $p|a$ and $|R_p| \leq 2$ when $p \nmid a$. Clearly, for d square-free, $|R_d| \leq 2^{\omega(d)} = w(d)$. Thus, (R) holds.

As $w(p)$ is either 1 or 2, we have,

$$0 \leq \frac{w(p)}{p} \leq 1 - \frac{1}{A_1}$$

for some constant A_1. Clearly, (Ω_0) holds. Thus applying Theorem 3.1.1 with $A = 2$, $z \geq x^{1/2}$,

$$S_a(x) \leq B_5 \frac{x}{a} \prod_{p<x/a} \left(1 - \frac{w(p)}{p}\right)$$
$$= B_5 \frac{x}{a} \prod_{\substack{p<x/a \\ p \nmid a}} \left(1 - \frac{2}{p}\right) \prod_{p|a} \left(1 - \frac{1}{p}\right)$$
$$\leq B_5 \frac{x}{a} \frac{\prod_{p<x/a} \left(1 - \frac{2}{p}\right)}{\prod_{\substack{p<x/a \\ p|a}} \left(1 - \frac{2}{p}\right)}.$$

In the last inequality, we used the fact that

$$\prod_{p|a}\left(1-\frac{1}{p}\right)=\frac{\phi(a)}{a}\leq 1.$$

Using Mertens' theorem, we have

$$\prod_{p<z}\left(1-\frac{1}{p}\right)^2=\frac{e^{-2\gamma}}{(\log z)^2}\left(1+O\left(\frac{1}{\log z}\right)\right)$$

where γ is Euler's constant. However,

$$\begin{aligned}\prod_{p<z}\left(1-\frac{1}{p}\right)^2&=\prod_{p<z}\left(1+\frac{1}{p^2}-\frac{2}{p}\right)\\&=\prod_{p<z}\left(1-\frac{2}{p}\right)\left(1+\frac{1}{p^2(1-2/p)}\right)\\&=\prod_{p<z}\left(1-\frac{2}{p}\right)\prod_{p<z}\left(1+\frac{1}{p(p-2)}\right).\end{aligned}$$

Thus,

$$\begin{aligned}\prod_{p<z}\left(1-\frac{2}{p}\right)&\leq\prod_{p<z}\left(1-\frac{1}{p}\right)^2\\&\leq\frac{e^{-2\gamma}}{(\log z)^2}.\end{aligned}$$

Therefore in the estimate for $S_a(x)$, we obtain

$$\prod_{p<x/a}\left(1-\frac{2}{p}\right)\leq\frac{c_1}{(\log\frac{x}{a})^2}.$$

Next, we note that

$$\begin{aligned}\prod_{p|a}\left(1-\frac{2}{p}\right) &= \prod_{p|a}\left(1-\frac{1}{p}\right)^2\prod_{p|a}\left(1+\frac{1}{p(p-2)}\right)\\ &\asymp c\prod_{p|a}\left(1-\frac{1}{p}\right)^2\\ &\asymp c(\phi(a)/a)^2.\end{aligned}$$

Since for some constant c, $\frac{a}{\phi(a)} < c\log\log a$, we get

$$S_a(x) \ll \frac{x}{a}\frac{1}{(\log x/a)^2}(\log\log a)^2.$$

□

Next we recall a few standard theorems here from analytic number theory which we use in the next few sections. We denote by $\pi(x;q,h)$, as usual the number of primes $p \leq x$ such that $p \equiv h(\text{mod } q)$, that is p lies in the arithmetic progression h modulo q.

Theorem 3.1.3 (Brun-Titchmarsh, 1930)**.** *For any $\epsilon > 0$, for $q \leq x^{1-\epsilon}$, $(q,h) = 1$,*

$$\pi(x;q,h) \ll \frac{x}{\phi(q)\log(x/q)}.$$

Theorem 3.1.4 (Bombieri-Vinogradov, 1965)**.** *Let $A > 0$ be fixed, $E(x;q,h) = \pi(x;q,h) - \frac{\pi(x)}{\phi(q)}$*

$$\sum_{q\leq y}\max_{\substack{1\leq h\leq q\\(h,q)=1}}|E(x;q,h)| \ll \frac{x}{(\log x)^A}$$

for $y \leq \dfrac{x^{1/2}}{(\log x)^B}$ *with* $B = B(A) > 0$.

We would also use following theorem in the proofs of the main theorems in this chapter. We mentioned in Chapter 2 but for the sake of completeness, we state it here as well.

Lemma 3.1.5. *For* $\theta > 1$,

$$\sum_{k>\theta y} \frac{y^k}{k!} \leq \theta^{-\theta y} e^{\theta y};$$

for $0 < \theta < 1$,

$$\sum_{k<\theta y} \frac{y^k}{k!} \leq \theta^{-\theta y} e^{\theta y};$$

for $\theta > 1$ *and fixed* $c > 0$,

$$\sum_{\theta y+\theta c>k>\theta y} \frac{y^k}{k!} \leq \frac{\theta c e^{\theta y(-\log\theta+1)}}{(\theta y)^{1/2}},$$

and for $\theta > 1$ *and* $\lambda > 1$,

$$\sum_{\theta y<k<\lambda y} \frac{y^k}{k!} \leq \frac{(\lambda-\theta) y e^{\theta y(-\log\theta+1)}}{(\theta y)^{1/2}},$$

provided $y > 1$.

3.2 Review of results of Erdős and Pomerance

Erdős and Pomerance ([22]) and Ram Murty and Kumar Murty ([38], [39]) independently discuss the normal order and distribution of $\omega(\phi(p))$ and $\omega(\phi(n))$ for

any prime p and any natural number n. We will discuss these results and the intuition behind their truth in this section. It is important to note here that both these groups of authors use Turán's normal order method to achieve these results. Earlier in 1935, Erdős had proved that the normal order of $\omega(\phi(p))$ is $\log\log p$ using Brun's Sieve and Hardy and Ramanujan's 1917 theorem on normal number of prime factors of a natural number n. We will revisit this result in the upcoming section. The result on the normal order of $\omega(\phi(p))$ and $\omega(\phi(n))$ is as follows.

Theorem 3.2.1. *For any prime p and natural number n,*

$$\sum_{p\leq x}(\omega(\phi(p))-\log\log p)^2 \ll \pi(x)\log\log x$$

and

$$\sum_{n\leq x}(\omega(\phi(n))-\frac{1}{2}(\log\log n)^2)^2 \ll x(\log\log x)^3\log\log\log\log x.$$

In other words, $\omega(\phi(p))$ has normal order $\log\log p$ and $\omega(\phi(n))$ has normal order $\frac{1}{2}(\log\log n)^2$. This result is also true when $\omega(n)$ is replaced by $\Omega(n)$.

The Erdős-Kac type distribution result for $\omega(\phi(p))$ and $\omega(\phi(n))$ is the following.

Theorem 3.2.2. *For prime p and any natural number n,*

$$\lim_{x\to\infty}\frac{1}{x}\left|\left\{n\leq x;\frac{\omega(\phi(n))-\frac{1}{2}(\log\log x)^2}{(\log\log x)^{3/2}}\leq\frac{\alpha}{\sqrt{3}}\right\}\right| = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\alpha}e^{-t^2/2}dt.$$

Also,

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\left|\left\{p\leq x;\frac{\omega(\phi(p))-\log\log p}{(\log\log p)^{1/2}}\leq\alpha\right\}\right| = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\alpha}e^{-t^2/2}dt.$$

Let $\Omega_z(n)$ denote the number of prime factors (counted with multiplicity) of n, which are less than or equal to z, i.e., if $n = \prod_{i \le k} {p_i}^{\alpha_i}$, then $\Omega_z(n) = \sum_{\substack{p^\alpha || n \\ p \le z}} \alpha$. The above results on the normal order and distribution of $\omega(\phi(p))$ and $\omega(\phi(n))$ rely mainly on the first and second moment of $\Omega_z(\phi(p))$ for a prime p. The following lemmas estimates these moments.

Lemma 3.2.3. *If $3 \le z \le x$, then,*

$$\sum_{\substack{q \le x \\ q \text{ prime}}} \Omega_z(\phi(q)) = \pi(x) \log\log z + O(\pi(x))$$

where the implied constant is absolute.

Lemma 3.2.4. *If $3 \le z \le x$, then,*

$$\sum_{\substack{q \le x \\ q \text{ prime}}} \Omega_z(\phi(q))^2 = \pi(x)(\log\log z)^2 + O(\pi(x) \log\log z)$$

where the implied constant is absolute.

For a proof of the results , we refer the readers to Section 2 of [22] or Section 3 of [38], where a more general theorem is discussed.

Heuristically, for prime p, $\phi(p)$ behaves randomly and usually has $\log\log|\phi(p)|$ prime factors. Since $|\phi(p)| = p - 1 < p$, $\omega(\phi(p))$ can be expected to behave like $\log\log p$. By the Hardy-Ramanujan theorem, n "usually" has $\log\log n$ prime factors. Also heuristically, $\omega(\phi(n)) \sim \sum_{p|n} \omega(\phi(p))$. Since each of the summands above is approximately $\log\log p$, we get $\omega(\phi(n))$ should have normal order $\frac{(\log\log n)^2}{2}$. These heuristics can be made rigorous by using the Bombieri- Vinogradov theorem

and the Brun Titchmarsh theorem. We will see a similar methodology in action in the estimation of the normal order of $\omega(\phi(p+a))$ where p is prime and a any non-zero integer.

3.3 Erdős' theorem for $\Omega(p-1)$

In this section, we will sketch a proof of Theorem 3.0.1. We note here that even though we essentially follow Erdős' method of proof, we use certain elementary inequalities to give a simpler exposition.

In the previous chapter, we proved the following stronger version of the Hardy-Ramanujan theorem which estimates the normal number of prime factors of any natural number n.

Theorem 3.3.1. *Given any $A > 0$, let $B = (A+1)(\log(A+1)) - A$. Then*

$$|\{n \leq x,\ |\omega(n) - \log\log n| > A\log\log n\}| = O\left(\frac{x}{(\log x)^B}\right).$$

For $0 < A < 1$,

$$|\{n \leq x : \Omega(n) < (1-A)\log\log x\}|$$

$$\ll \frac{x\log\log x}{(\log x)^{(1-A)(\log(1-A)-1)+1}} + O\left(x^{3/4}(\log\log x)(\log x)^2\right).$$

For $A > 0$,

$$|\{n \leq x : \Omega(n) > (1+A)(\log\log x)\}| \ll \frac{x\log\log x}{(\log x)^{(1+A)\log 2+1}}.$$

This theorem will play a key role in the proof of Erdős' theorem. Let us define $g_k(x)$, for $k = 0, 1, 2, \cdots$, to be the number of primes $p \leq x$ such that

$$\Omega(p-1) = k. \tag{3.3.1}$$

As a first step towards the proof of Theorem 3.0.1, we will use Theorem 3.3.1 along with Brun's sieve to prove the following technical lemma.

Lemma 3.3.2. *Given any $A > 0$, set $B = (A+1)\log 2 + 1$. Then, except for $O\left(\frac{x \log\log x}{(\log x)^B}\right)$ many integers $n \leq x$, any natural number $n(\leq x)$ can be expressed as $n = r_1^{\alpha_1} \cdots r_k^{\alpha_k}$ where r_i denote prime for all $1 \leq i \leq k$, $r_i < r_j$ for $i < j$, $k < (A+1)\log\log x$, $\alpha_k = 1$ and $r_k > x^{\frac{1}{M \log\log x}}$ for some constant M.*

Proof. Clearly, by Theorem 3.3.1, given any $A > 0$, except for $O\left(\frac{x \log\log x}{(\log x)^B}\right)$ many integers $n \leq x$, any natural number n can be expressed as $n = r_1^{\alpha_1} \cdots r_k^{\alpha_k}$, $r_i < r_j$ for $i < j$ and $k < (A+1)\log\log x$ and the r_i's are prime.

1. Given any $A > 0$, for $M > A$, let us note that

$$\left| \left\{ n \leq x : n = r_1^{\alpha_1} \cdots r_k^{\alpha_k}, k < (A+1)\log\log x,\ r_k < x^{1/M \log\log x} \right\} \right|$$

   is $O(x^\theta)$, for some $\theta < 1$. This is quite straightforward to see. Since r_k is the largest prime factor and $r_k < x^{1/M\log\log x}$, each $r_i < x^{1/M\log\log x}$ for $1 \leq i \leq k$ and $k < (A+1)\log\log x$. This gives an upper bound of $(x^{1/M\log\log x})^{(A+1)\log\log x} = x^{(A+1)/M}$. Choosing any $M > A+1$ proves the assertion.

2. Next we observe that

$$\left| \left\{ n \leq x : n = r_1^{\alpha_1} \cdots r_k^{\alpha_k},\ r_k > x^{1/M \log\log x},\ \alpha_k \geq 2 \right\} \right|$$

is $O\left(\frac{x}{(\log x)^{\theta})}\right)$ for any $\theta > 1$. Indeed each integer n in the above set is divisible by a square bigger than $x^{1/M \log\log x}$. So, the number of such integers is less than

$$\begin{aligned}
\sum_{l > x^{1/M \log\log x}} \frac{x}{l^2} &= x \sum_{l > x^{1/M \log\log x}} \frac{1}{l^2} \\
&= O\left(\frac{x}{x^{1/M \log\log x}}\right) \\
&= O\left(\frac{x}{e^{\log x / M \log\log x}}\right) \\
&\ll O\left(\frac{x}{(\log x)^{\theta}}\right) \text{ for any } \theta > 1.
\end{aligned}$$

□

Lemma 3.3.3. *For $k = 0, 1, 2, \cdots$, given any $A > 0$, set $B = (A+1)\log 2$. Then,*

$$g_k(x) \leq \frac{C' x (\log\log x)^4}{(\log x)^2} \frac{(\log\log x + D)^{k-1}}{(k-1)!} + O\left(\frac{(x \log\log x)}{(\log x)^B}\right)$$

for some constants C' and D, where g_k is defined in (3.3.1).

Proof. Using Lemma 3.3.2, we can say that given any prime $p \leq x$ and $A > 0$, setting $B = (A+1)\log 2 + 1$, we have that except for $O\left(\frac{x \log\log x}{(\log x)^B}\right)$ many $n \leq x$, $n = p - 1$ can be expressed as

$$p - 1 = q_1 \cdots q_k \tag{3.3.2}$$

where $q_1 \leq q_2 \leq \cdots \leq q_k$, $q_k > x^{1/M \log\log x}$, $k < (A+1)\log\log x$ for some $M > A+1$. Then we write $a := q_1 \cdots q_{k-1}$, $p-1 = a \cdot q_k$ where $a < x^{1-\frac{1}{M\log\log x}}$ and $\Omega(a) = k-1$. Fixing such an a, let

$$S_a(x) = \left| \left\{ p \leq x : p-1 \equiv 0 \pmod{a}, \frac{p-1}{a} \text{ is prime} \right\} \right|.$$

Then,

$$\begin{aligned} g_k(x) &= \sum_{\substack{p \leq x \\ \Omega(p-1)=k}} 1 \\ &= \sum_{\substack{a < x^{1-\frac{1}{M\log\log x}} \\ \Omega(a)=k-1}} S_a(x) + O\left(\frac{x\log\log x}{(\log x)^B}\right). \end{aligned}$$

Note, the error term in the last equality comes from the fact that we have to take into account the set of integers which do not have factorisation as in (3.3.2).

By Theorem 3.1.2, we know

$$S_a(x) \leq C' \frac{x}{a} \frac{(\log\log x)^2}{(\log \frac{x}{a})^2}.$$

Using this upper bound to estimate $g_k(x)$, we have

$$g_k(x) \leq \sum_{\substack{a < x^{1-\frac{1}{M\log\log x}} \\ \Omega(a)=k-1}} C' \frac{x}{a} \frac{(\log\log x)^2}{(\log \frac{x}{a})^2}.$$

In the above sum, since $a < x^{1-\frac{1}{M\log\log x}}$, $\frac{x}{a} \geq x^{1/M\log\log x}$. This implies

$$\left(\log\frac{x}{a}\right)^2 \geq \left(\frac{\log x}{M\log\log x}\right)^2.$$

Thus,

$$\begin{aligned} g_k(x) &\leq Cx(\log\log x)^2\frac{(M\log\log x)^2}{(\log x)^2}\sum_{\substack{a<x\\ \Omega(a)=k-1}}\frac{1}{a} + O\left(\frac{x\log\log x}{(\log x)^B}\right) \\ &\leq C'x\frac{(\log\log x)^4}{(\log x)^2}\frac{1}{(k-1)!}\left(\sum_{p\leq x}\frac{1}{p}\right)^{k-1} + O\left(\frac{x\log\log x}{(\log x)^B}\right). \end{aligned}$$

Since $\sum_{p\leq x}\frac{1}{p} = \log\log x + O(1)$,

$$g_k(x) \leq \frac{C'x(\log\log x)^4}{(\log x)^2}\frac{(\log\log x + D)^{k-1}}{(k-1)!} + O\left(\frac{x\log\log x}{(\log x)^B}\right)$$

for some constants C' and D. This proves the lemma. □

Proof of Theorem 3.0.1 Given any $A > 0$, we want an estimate for

$$\begin{aligned} \sum_{\substack{p\leq x\\ \Omega(p-1)>A\log\log x}} 1 &= \sum_{k>A\log\log x}\left(\sum_{\substack{p\leq x\\ \Omega(p-1)=k}} 1\right) \\ &= \sum_{k>A\log\log x} f_k(x). \end{aligned}$$

Using Lemma 3.3.3 and the fact that $\forall n$, $\Omega(n) \leq \frac{\log n}{\log 2}$, and letting $B = (A+1)\log 2 + 1$, this is

$$< \frac{C'x}{(\log x)^2} \sum_{\frac{\log x}{\log 2} > k > A \log\log x} \frac{(\log\log x + D)^{k+3}}{(k-1)!} + O\left(\sum_{\frac{\log x}{\log 2} > k > A\log\log x} \frac{x \log\log x}{(\log x)^B} \right)$$
$$\leq \frac{C'x(\log\log x + D)^4}{(\log x)^2} \sum_{k > A\log\log x} \frac{(\log\log x + D)^{k-1}}{(k-1)!} + O\left(\frac{x\log\log x}{(\log x)^{B-1}} \right).$$

Now let us write

$$\sum_{k > A\log\log x} \frac{(\log\log x + D)^{k-1}}{(k-1)!} = U_1 + U_2$$

where

$$U_1 = \sum_{k > A(\log\log x + D)} \frac{(\log\log x + D)^{k-1}}{(k-1)!}$$

and

$$U_2 = \sum_{A(\log\log x + D) > k > A\log\log x} \frac{(\log\log x + D)^{k-1}}{(k-1)!}$$

Using the first part of Lemma 3.1.5,

$$\begin{aligned} U_1 &\leq A^{-A(\log\log x + D)} e^{A(\log\log x + D)} \\ &= e^{A\log\log x(1-\log A)} e^{AD(1-\log A)} \\ &\leq (\log x)^{A(1-\log A)}. \end{aligned}$$

Using the third part of Lemma 3.1.5,

$$\begin{aligned} U_2 &\leq ADe^{A(\log\log x+D)(-\log A+1)} \\ &= AD((\log x)^A e^{AD})^{-\log A+1} \\ &= AD(\log x)^{A(1-\log A)} e^{AD(-\log A+1)} \\ &= \frac{AD}{e^{AD(\log A-1)}}(\log x)^{A(1-\log A)}. \end{aligned}$$

Combining the estimates for U_1 and U_2, we thus obtain

$$\begin{aligned} \sum_{\substack{p\leq x \\ \Omega(p-1)>A\log\log x}} 1 &\leq \frac{C'x(\log\log x+D)^4}{(\log x)^2(\log x)^{A(\log A-1)}} + O\left(\frac{x\log\log x}{(\log x)^{B-1}}\right) \\ &= \frac{C'x(\log\log x+D)^4}{(\log x)^{A(\log A-1)+2}} + O\left(\frac{x\log\log x}{(\log x)^{B-1}}\right). \end{aligned}$$

For $A > 4$, $A(\log A - 1) + 2 > (B-1)$, that is, the second term in the above expression dominates. Thus, $c(A) = (A+1)\log 2 - 2$, we get that for $A > 4$,

$$\#\{p \leq x : \Omega(p-1) > A\log\log x\} \ll \frac{\pi(x)}{(\log x)^{c(A)}}.$$

3.4 Mean and Variance for $\Omega(\phi(p+a))$

In this section, we will compute the first and second moments of $\Omega(\phi(p+a))$ and hence compute the normal number of prime factors of the Euler totient function at shifts of primes.

For a prime p and any non-zero integer a, let

$$p + a = \prod_{i \leq k} q_i^{\alpha_i}$$

be the unique prime power decomposition for $(p + a)$. Since ϕ is a multiplicative function, we have that

$$\phi(p+a) = \phi(\prod_{i \leq k} q_i^{\alpha_i}) = \prod_{i=1}^{k} \phi(q_i^{\alpha_i}) = \phi_0(p+a)\phi_1(p+a)$$

where

$$\phi_0(p+a) = \left(\prod_{q^\alpha \leq y} \phi(q^\alpha) \right), \ \phi_1(p+a) = \left(\prod_{q^\alpha > y} \phi(q^\alpha) \right)$$

and y is a parameter to be chosen later. Since $\Omega(n)$ is a completely additive function,

$$\Omega(\phi(p+a)) = \Omega(\prod_{i=1}^{k} \phi(q_i^{\alpha_i})) = \sum_{q^\alpha || p+a} \Omega(\phi(q^\alpha)).$$

We can write

$$\Omega(\phi(p+a)) = \sum_{q^\alpha \leq y} \Omega(\phi(q^\alpha)) + \sum_{q^\alpha > y} \Omega(\phi(q^\alpha)), \tag{3.4.1}$$

where the sum is over prime powers $q^\alpha || (p + a)$. As before, let $\Omega_z(n)$ denote the number of prime factors (counted with multiplicity) of n, which are less than or equal to z, i.e., if $n = \prod_{i \leq k} {p_i}^{\alpha_i}$, then $\Omega_z(n) = \sum_{\substack{p^\alpha || n \\ p \leq z}} \alpha$. Since

$$\phi(n) = O(n), \tag{3.4.2}$$

choosing $z = x^\theta$ for some $\theta > 0$, we observe that

$$\Omega(\phi(p+a)) = \Omega_z(\phi(p+a)) + O(1)$$

because the number of prime power divisors r^β of $\phi(p+a)$ with $r^\beta > x^\theta$ is absolutely bounded by virtue of (3.4.2).

Note that (3.4.1) still holds when Ω is replaced by Ω_z.

The next lemma gives an estimate for the first moment (mean) of prime power divisors of prime shifts of $\phi(n)$, that is, $\phi(p+a)$ for any fixed $a > 0$.

Theorem 3.4.1. *For any non-zero integer a,*

$$\sum_{p\le x} \Omega(\phi(p+a)) = \frac{1}{2}\pi(x)(\log\log x)^2 + O(\frac{x}{\log x})$$

Proof. By our observation earlier, and with our choice of $z = x^\theta$, $(\theta > 0)$,

$$\begin{aligned}\sum_{p\le x} \Omega(\phi(p+a)) &= \sum_{p\le x} \{\Omega_z(\phi(p+a)) + O(1)\} \\ &= \sum_{p\le x} \Omega_z(\phi(p+a)) + O(\frac{x}{\log x}).\end{aligned}$$

Thus it suffices to investigate $\sum_{p\le x} \Omega_z(\phi(p+a))$.

$$\sum_{p\le x} \Omega_z(\phi(p+a)) = \sum_{p\le x} \sum_{\substack{q^\alpha || p+a \\ q^\alpha \le y}} \Omega_z(\phi(q^\alpha)) + \sum_{p\le x} \sum_{\substack{q^\alpha || p+a \\ q^\alpha > y}} \Omega_z(\phi(q^\alpha)).$$

Let us write the above two sums as Σ_1, Σ_2. Interchanging sums in Σ_1, we get

$$\begin{aligned}\Sigma_1 &= \sum_{q^\alpha \leq y} \Omega_z(\phi(q^\alpha)) \left(\sum_{\substack{p \leq x \\ q^\alpha | p+a}} 1 \right) \\ &= \sum_{q^\alpha \leq y} \Omega_z(\phi(q^\alpha)) \pi(x; q^\alpha, -a).\end{aligned}$$

The above sum is

$$\sum_{q^\alpha \leq y} \Omega_z(\phi(q^\alpha)) \frac{\pi(x)}{\phi(q^\alpha)} + \sum_{q^\alpha \leq y} \Omega_z(\phi(q^\alpha)) E(x; q^\alpha, -a).$$

Choosing $y = \dfrac{x^{1/2}}{(\log x)^{12}}$ and applying the Bombieri-Vinogradov theorem (Theorem (3.1.4)), we get

$$\sum_{q^\alpha \leq y} |E(x; q^\alpha, -a)| = O\left(\frac{x}{(\log x)^2} \right).$$

So the required sum Σ_1 is

$$\pi(x) \sum_{q^\alpha \leq y} \frac{\Omega_z(\phi(q^\alpha))}{\phi(q^\alpha)} + O\left(\frac{x}{\log x} \right).$$

Note, if $\alpha \geq 2$, $\dfrac{\Omega_z(\phi(q^\alpha))}{\phi(q^\alpha)} \ll \dfrac{\log(q^\alpha)}{q^\alpha}$ (since, $\Omega(n) \ll \log n$ for all $n \in \mathbb{N}$ and $\phi(n) \gg n$ when n is restricted to prime powers). Now for $\alpha \geq 2$, $\dfrac{\alpha}{q^\alpha} \leq \dfrac{2}{q^2}$, and $\sum_{\alpha \geq 2} \frac{\alpha}{q^\alpha} \ll \frac{1}{q^2}$. Thus, the contribution to the first sum from q^α with $\alpha \geq 2$, is bounded absolutely. Therefore,

$$\Sigma_1 = \pi(x) \sum_{q \leq y} \frac{\Omega_z(\phi(q))}{\phi(q)} + O\left(\frac{x}{\log x} \right).$$

Let $A(y)$ denote the sum $\sum_{q\leq y}\Omega_z(\phi(q))$. Since $\phi(q)=q-1$, by Lemma 3.2.3 and by the partial summation formula, we get,

$$\begin{aligned}\Sigma_1 &= \pi(x)\int_2^y \frac{A(t)}{t^2}dt + O\left(\frac{x}{\log x}\right)\\ &= \pi(x)\int_2^y \frac{\pi(t)\log\log t}{t^2}dt + O\left(\frac{x}{\log x}\right).\end{aligned}$$

Thus,

$$\Sigma_1 = \pi(x)\frac{(\log\log y)^2}{2} + O\left(\frac{x}{\log x}\right).$$

Now,

$$\Sigma_2 = \sum_{p\leq x}\sum_{\substack{q^\alpha||p+a\\ q^\alpha>y}}\Omega_z(\phi(q^\alpha)).$$

Since $y=\frac{x^{1/2}}{(\log x)^{12}}$, there are only finitely many q^α in the inner sum in Σ_2. But $\Omega_z(\phi(q^\alpha))$ can take a large value. So, to investigate this phenomenon, we divide the inner sum into two parts,

$$\Sigma_2 = T_1 + T_2$$

where

$$T_1 = \sum_{p\leq x}\sum_{\substack{q^\alpha|p+a\\ q^\alpha>y\\ \Omega_z(\phi(q^\alpha))<100\log\log x}}\Omega_z(\phi(q^\alpha))$$

and

$$T_2 = \sum_{p\leq x}\sum_{\substack{q^\alpha|p+a\\ q^\alpha>y\\ \Omega_z(\phi(q^\alpha))>100\log\log x}}\Omega_z(\phi(q^\alpha)).$$

Here, the choice of 100 above is arbitrary. Any value A such that $((A+1)\log 2 -$

$2) > 0$ works. Clearly,

$$\begin{aligned} T_1 &= O\left(\log\log x \sum_{p\le x} \sum_{\substack{q^\alpha \mid p+a \\ q^\alpha > y}} 1\right) \\ &= O\left(\pi(x)\log\log x\right) \end{aligned}$$

because there are only finitely many such q^α. Thus,

$$\Sigma_2 = T_2 + O\left(\pi(x)\log\log x\right).$$

Now, we can write

$$T_2 = {\sum_{p\le x}}' \sum_{\substack{q^\alpha \mid p+a \\ q^\alpha > y \\ \Omega_z(\phi(q^\alpha)) > 100\log\log x}} \Omega_z(\phi(q^\alpha)) + O\left(\pi(x)\log\log x\right).$$

Here, $\sum_p'$ denotes the sum over $p \le x$ such that $p+a$ is not prime, because if $p+a$ is a prime, then

$$\sum_{p\le x} \Omega_z(\phi(p+a) \ll \sum_{\substack{l\le x \\ l \text{ prime}}} \Omega_z(\phi(l)) = O(\pi(x)\log\log x).$$

Therefore, we have

$$T_2 = \sum_{p\le x}{}' \sum_{\substack{q^\alpha || p+a \\ q^\alpha > y \\ \Omega(\phi(q^\alpha))>100\log\log x}} \Omega_z(\phi(q^\alpha)) + O(\pi(x)\log\log x)$$

$$\ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\phi(q^\alpha))>100\log\log x}} \Omega_z(\phi(q^\alpha)) \sum_{\substack{p\le x \\ q^\alpha | p+a}} 1 + O(\pi(x)\log\log x).$$

This is because if $q^\alpha > x/4$, and $q^\alpha | p+a$, then $1 < \dfrac{p+a}{q^\alpha} < 4$ has only finitely many choices, and since ϕ is multiplicative function and Ω is completely additive, T_2 gets changed by a constant. Thus,

$$T_2 \ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\phi(q^\alpha))>100\log\log x}} \Omega_z(\phi(q^\alpha))\pi(x;q^\alpha,-a) + O(\pi(x)\log\log x).$$

By the Brun-Titchmarsh theorem (Theorem 3.1.3), this has an upper bound of

$$\ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\phi(q^\alpha))>100\log\log x}} \frac{\Omega_z(\phi(q^\alpha))x}{q^\alpha\log(x/q^\alpha)}$$

$$= x \sum_{\substack{y<q<x/4 \\ \Omega(\phi(q))>100\log\log x}} \frac{\Omega_z(\phi(q))}{q\log(x/q)} + O(\pi(x)),$$

where the last equality follows because the sum over q^α is convergent when $\alpha \ge 2$. To estimate the sum, we divide the sum into dyadic subintervals. Without loss of generality, choose $y = 2^\alpha$, $x/4 = 2^{\beta+1}$ for some $\alpha, \beta > 0$ and $\alpha \le \beta + 1$. Then, the

sum is bounded by

$$x\sum_{j=\alpha}^{\beta}\frac{1}{(\beta+2)-(j+1)}\sum_{\substack{2^j\le q<2^{j+1}\\ \Omega(\phi(q))>100\log\log x}}\frac{\Omega_z(\phi(q))}{q}$$
$$\ll x\sum_{j=\alpha}^{\beta}\frac{1}{(\beta+2)-(j+1)}\sum_{\substack{2^j\le q<2^{j+1}\\ \Omega(\phi(q))>100\log\log x}}\frac{\log q}{q}.$$

Now, by the partial summation formula,

$$\sum_{\substack{q\ge m\\ \Omega(\phi(q))>100\log\log m}}\frac{\log q}{q}\ll\int_m^{\infty}\frac{\log t}{t^2}\tilde{S}_{100}(t)dt$$

where

$$\tilde{S}_A(t)=\sum_{\substack{p\le t\\ \Omega(\phi(p))>A\log\log x}}1$$

which by Theorem 3.0.1 is $O\left(\frac{\pi(x)}{(\log x)^{c(100)}}\right)$ where $c(100)=(100+1)\log 2-2$. Thus the statement of the theorem follows.

□

Next, our aim is to prove the following theorem.

Theorem 3.4.2. *For any $a\neq 0$, $a\in\mathbb{Z}$,*

$$\sum_{p\le x}\left(\Omega(\phi(p+a))-\frac{(\log\log x)^2}{2}\right)^2=\pi(x)\frac{(\log\log x)^3}{3}+o(\pi(x)(\log\log x)^3);$$

which implies, $\Omega(\phi(p+a))$ has normal order $\frac{(\log\log p)^2}{2}$.

The proof of this theorem relies on the following lemma.

Lemma 3.4.3. *For any $a \neq 0$, $a \in \mathbb{Z}$,*

$$\sum_{p\leq x} \Omega^2(\phi(p+a)) = \pi(x)\left(\frac{(\log\log x)^2}{2}\right)^2 + \pi(x)\frac{(\log\log x)^3}{3} + O(\frac{x}{\log x}).$$

Proof. Clearly, since $\Omega(n)$ is a completely additive function and $\phi(n)$ is multiplicative,

$$\begin{aligned}\Omega^2(\phi(p+a)) &= \left[\sum_{q^\alpha||p+a} \Omega(\phi(q^\alpha))\right]^2 \\ &= \sum_{q^\alpha||p+a} \Omega(\phi(q^\alpha))^2 + \sum_{\substack{q_i^{\alpha_i}||p+a \\ q_j^{\alpha_j}||p+a \\ q_i\neq q_j}} \Omega(\phi(q_i^{\alpha_i}))\Omega(\phi(q_j^{\alpha_j})).\end{aligned}$$

Again, choosing $z = x^\theta$, for some $\theta > 0$, and noting that the number of prime divisors r^β of $\phi(q^\alpha)$ with $r^\beta > x^\theta$ is absolutely bounded ,

$$\sum_{p\leq x} \Omega^2(\phi(p+a)) = S_1 + S_1' + S_2 + S_2' + O\left(\frac{x}{\log x}\right)$$

where

$$S_1 = \sum_{p\leq x} \sum_{\substack{q^\alpha||p+a \\ q^\alpha\leq y}} \Omega_z(\phi(q^\alpha))^2,\ S_1' = \sum_{p\leq x} \sum_{\substack{q^\alpha||p+a \\ q^\alpha> y}} \Omega_z(\phi(q^\alpha))^2$$

$$S_2 = \sum_{p\leq x} \sum_{\substack{q_i^{\alpha_i}||p+a \\ q_j^{\alpha_j}||p+a \\ q_i^{\alpha_i}\neq q_j^{\alpha_j}\leq y}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j})),\ S_2' = \sum_{p\leq x} \sum_{\substack{q_i^{\alpha_i}||p+a \\ q_j^{\alpha_j}||p+a \\ q_i^{\alpha_i}\neq q_j^{\alpha_j}> y}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j})).$$

Consider the sum S_1. As before, by the Brun-Titchmarsh theorem (Theorem 3.1.3)

and the Bombieri-Vinogradov theorem (Theorem 3.1.4), choosing $y = \frac{x^{1/2}}{(\log x)^{14}}$, we get

$$\begin{aligned} S_1 &= \sum_{q^\alpha \le y} \Omega_z(\phi(q^\alpha))^2 \pi(x; q^\alpha, -a) \\ &= \pi(x) \sum_{q^\alpha \le y} \frac{\Omega_z(\phi(q^\alpha))^2}{\phi(q^\alpha)} + \sum_{q^\alpha \le y} \Omega_z(\phi(q^\alpha))^2 |E(x; q^\alpha, -a)| \\ &= \pi(x) \sum_{q^\alpha \le y} \frac{\Omega_z(\phi(q^\alpha))^2}{\phi(q^\alpha)} + O\left(\frac{x}{\log x}\right). \end{aligned}$$

Since the contribution from q^α with $\alpha \ge 2$ is $O(x/\log x)$,

$$S_1 = \pi(x) \sum_{q \le y} \frac{\Omega_z(\phi(q))^2}{\phi(q)} + O\left(\frac{x}{\log x}\right).$$

Again denoting $B(y) = \sum_{q \le y} \Omega_z^2(\phi(q))$, since $\phi(q) = q - 1$, by Lemma 3.2.4 and the partial summation formula, we get

$$\sum_{q \le y} \frac{\Omega_z(\phi(q))^2}{\phi(q)} = \frac{1}{3}(\log\log y)^3 + O((\log\log y)^2).$$

Thus,

$$S_1 = \pi(x) \left(\frac{1}{3}(\log\log x)^3 + O((\log\log x)^2)\right) + O\left(\frac{x}{\log x}\right).$$

Now let us consider S_2. It follows that

$$S_2 = \pi(x) \sum_{\substack{q_i^{\alpha_i}, q_j^{\alpha_j} \le y \\ q_i \ne q_j}} \frac{\Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j}))}{\phi(q_i^{\alpha_i} q_j^{\alpha_j})} + \sum_{q_i^{\alpha_i} q_j^{\alpha_j} \le y^2} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j}))E(x; q_i^{\alpha_i} q_j^{\alpha_j}, -a).$$

Choosing $y = \frac{x^{1/4}}{(\log x)^7}$ and using the Bombieri-Vinogradov theorem, we get

$$\sum_{q_i^{\alpha_i} q_j^{\alpha_j} \leq y^2} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j}))|E(x; q_i^{\alpha_i} q_j^{\alpha_j}, -a)| = O\left(\frac{x}{(\log x)^2}\right).$$

Also if either α_i or $\alpha_j \geq 2$, $\dfrac{\Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j}))}{\phi(q_i^{\alpha_i} q_j^{\alpha_j})} \leq \frac{\log \phi(p)}{(q_i q_j)^2}$ and thus in this case, there is at most a contribution of $O\left(\dfrac{x}{\log x}\right)$ to S_2. Thus we can write

$$S_2 = \pi(x) \sum_{\substack{q_i, q_j \leq y \\ q_i \neq q_j}} \frac{\Omega_z(\phi(q_i))\Omega_z(\phi(q_j))}{\phi(q_i q_j)} + O\left(\frac{x}{\log x}\right).$$

Now we observe that, since $\Omega(n)$ is a completely additive function,

$$\sum_{\substack{q_i, q_j \leq y \\ q_i \neq q_j}} \frac{\Omega_z(\phi(q_i))\Omega_z(\phi(q_j))}{\phi(q_i q_j)} = \left(\sum_{q \leq y} \frac{\Omega_z(\phi(q))}{\phi(q)}\right)^2 - \sum_{q \leq y} \frac{\Omega_z(\phi(q))^2}{\phi(q)^2}.$$

But we know from the proof of Theorem 3.4.1,

$$\left(\sum_{q \leq y} \frac{\Omega_z(\phi(q))}{\phi(q)}\right) = \frac{1}{2}(\log\log y)^2 + O\left(\frac{x}{\log x}\right)$$

and $\sum_{q \leq y} \dfrac{\Omega_z(\phi(q))^2}{\phi(q)^2}$ is convergent, hence absolutely bounded. Thus,

$$S_2 = \pi(x)\left(\frac{1}{2}(\log\log x)^2\right)^2 + O(\pi(x)).$$

Thus we get,

$$\sum_{p\le x}\Omega^2(\phi(p+a)) = S_1 + S_2 + S_1' + S_2' + O\left(\pi(x)\right)$$
$$= S_1' + S_2' + \pi(x)\left(\frac{(\log\log x)^2}{2}\right)^2 + \pi(x)\frac{(\log\log x)^3}{3} + O\left(\pi(x)\right)$$

Now we can write S_1' as

$$S_1' = S_{1,1}' + S_{1,2}'$$

where

$$S_{1,1}' = \sum_{p\le x} \sum_{\substack{q^\alpha \mid p+a \\ q^\alpha > y \\ \Omega(\phi(q^\alpha)) < 100\log\log x}} \Omega_z^2(\phi(q^\alpha))$$

and

$$S_{1,2}' = \sum_{p\le x} \sum_{\substack{q^\alpha \mid p+a \\ q^\alpha > y \\ \Omega(\phi(q^\alpha)) > 100\log\log x}} \Omega_z^2(\phi(q^\alpha)).$$

Clearly,

$$S_{1,1}' = O\left((\log\log x)^2 \sum_{p\le x}\sum_{\substack{q^\alpha \mid p+a \\ q^\alpha > y}} 1\right)$$
$$= O\left(\pi(x)(\log\log x)^2\right)$$

because there are only finitely many such q^α. Thus,

$$S_1' = S_{1,2}' + O\left(\pi(x)(\log\log x)^2\right).$$

Now, we can write

$$S'_{1,2} = \sum_{p\le x}{}' \sum_{\substack{q^\alpha | p+a \\ q^\alpha > y \\ \Omega(\phi(q^\alpha))>100\log\log x}} \Omega_z^2(\phi(q^\alpha)) + O\left(\pi(x)\log\log x\right).$$

Here, $\sum'_p$ denotes the sum over $p \le x$ such that $p+a$ is not prime, because if $p+a$ is a prime, then

$$\sum_{p\le x} \Omega^2(\phi(p+a) \ll \sum_{\substack{l\le x \\ l \text{ prime}}} \Omega^2(\phi(l)) = O(\pi(x)(\log\log x)^2).$$

So,

$$\begin{aligned} S'_{1,2} &= \sum_{p\le x}{}' \sum_{\substack{q^\alpha | p+a \\ q^\alpha > y \\ \Omega(\phi(q^\alpha))>100\log\log x}} \Omega_z^2(\phi(q^\alpha)) + O(\pi(x)(\log\log x)^2) \\ &\ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\phi(q^\alpha))>100\log\log x}} \Omega_z^2(\phi(q^\alpha)) \sum_{\substack{p\le x \\ q^\alpha | p+a}} 1 + O(\pi(x)(\log\log x)^2). \end{aligned}$$

This is because if $q^\alpha > x/4$, and $q^\alpha | p+a$, then $1 < \dfrac{p+a}{q^\alpha} < 4$ has only finitely many choices, and since ϕ is multiplicative function and Ω is completely additive, $S'_{1,2}$ gets changed by a constant. Thus,

$$S'_{1,2} \ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\phi(q^\alpha))>100\log\log x}} \Omega_z^2(\phi(q^\alpha))\pi(x;q^\alpha,-a) + O(\pi(x)(\log\log x)^2).$$

By the Brun-Titchmarsh theorem, this has an upper bound of

$$\sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\phi(q^\alpha))>100\log\log x}} \frac{\Omega_z^2(\phi(q^\alpha))x}{q^\alpha \log(x/q^\alpha)}$$
$$= x \sum_{\substack{y<q<x/4 \\ \Omega(\phi(q))>100\log\log x}} \frac{\Omega_z^2(\phi(q))}{q\log(x/q)} + O(\pi(x)),$$

where the last equality follows because the sum over q^α is convergent when $\alpha \geq 2$. Now again divide the sum into dyadic subintervals. Without loss of generality, choose $y = 2^\alpha$, $x/4 = 2^{\beta+1}$ for some α, $\beta > 0$ and $\alpha \leq \beta + 1$. Then, the sum is bounded by

$$x \sum_{j=\alpha}^{\beta} \frac{1}{(\beta+2)-(j+1)} \sum_{\substack{2^j\leq q<2^{j+1} \\ \Omega(\phi(q))>100\log\log x}} \frac{\Omega_z^2(\phi(q))}{q}$$
$$\ll x \sum_{j=\alpha}^{\beta} \frac{1}{(\beta+2)-(j+1)} \sum_{\substack{2^j\leq q<2^{j+1} \\ \Omega(\phi(q))>100\log\log x}} \frac{(\log q)^2}{q}.$$

Now, by the partial summation formula,

$$\sum_{\substack{q\geq m \\ \Omega(\phi(q))>100\log\log m}} \frac{(\log q)^2}{q} \ll \int_m^\infty \frac{(\log t)^2}{t^2} \tilde{S}_{100}(t)dt$$

where

$$\tilde{S}_A(t) = \sum_{\substack{p\leq t \\ \Omega(\phi(p))>A\log\log x}} 1$$

which by Theorem 3.0.1 is $O\left(\frac{\pi(x)}{(\log x)^{c(100)}}\right)$ where $c(100) = (100+1)\log 2 - 2$. Now

we can write

$$S_2^{'} = \sum_{p \le x} \sum_{\substack{q_i^{\alpha_i} || p+a \\ q_j^{\alpha_j} || p+a \\ q_i^{\alpha_i} \neq q_j^{\alpha_j} > y}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j})) = S'_{2,1} + S'_{2,2}$$

where

$$S'_{2,1} = \sum_{p \le x} \sum_{\substack{q_i^{\alpha_i} || p+a \\ q_j^{\alpha_j} || p+a \\ q_i^{\alpha_i} \neq q_j^{\alpha_j} > y \\ \Omega(\phi(q_i^{\alpha_i})), \Omega(\phi(q_j^{\alpha_j})) < 100 \log\log x}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j}))$$

and

$$S'_{2,2} = \sum_{p \le x} \sum_{\substack{q_i^{\alpha_i} || p+a \\ q_j^{\alpha_j} || p+a \\ q_i^{\alpha_i} \neq q_j^{\alpha_j} > y \\ \Omega(\phi(q_i^{\alpha_i})), \Omega(\phi(q_j^{\alpha_j})) > 100 \log\log x}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j})).$$

Now, as before,

$$\begin{aligned} S'_{2,1} &= O\left((\log\log x)^2 \sum_{p \le x} \sum_{\substack{q_i^{\alpha_i} || p+a \\ q_j^{\alpha_j} || p+a \\ q_i^{\alpha_i} \neq q_j^{\alpha_j} > y}} 1 \right) \\ &= O\left(\pi(x) (\log\log x)^2 \right) \end{aligned}$$

because there are only finitely many such q^{α}. Thus,

$$S_2' = S_{2,2}' + O\left(\pi(x)(\log\log x)^2\right).$$

Now, we can write

$$S_{2,2}' = \sum_{p\le x}{}' \sum_{\substack{q_i^{\alpha_i}||p+a \\ q_j^{\alpha_j}||p+a \\ q_i^{\alpha_i}\neq q_j^{\alpha_j}>y \\ \Omega(\phi(q_i^{\alpha_i})),\Omega(\phi(q_j^{\alpha_j}))>100\log\log x}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j})) + O\left(\pi(x)(\log\log x)^2\right).$$

Here, $\sum_p'$ denotes sum over $p \le x$ such that $p+a$ is not prime, because if $p+a$ is a prime, then

$$\sum_{p\le x}\Omega^2(\phi(p+a) \ll \sum_{\substack{l\le x \\ l \text{ prime}}}\Omega^2(\phi(l)) = O(\pi(x)(\log\log x)^2).$$

Thus we get

$$S_{2,2}' = \sum_{p\le x}{}' \sum_{\substack{q_i^{\alpha_i},q_j^{\alpha_j}|p+a \\ q_i^{\alpha_i},q_j^{\alpha_j}>y \\ \Omega(\phi(q_i^{\alpha_i})),\Omega(\phi(q_j^{\alpha_j}))>100\log\log x}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j})) + O(\pi(x)(\log\log x)^2)$$

$$\ll \sum_{\substack{y<q_i^{\alpha_i}q_j^{\alpha_j}<x/4 \\ \Omega(\phi(q_i^{\alpha_i})),\Omega(\phi(q_j^{\alpha_j}))>100\log\log x}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\phi(q_j^{\alpha_j})) \sum_{\substack{p\le x \\ q_i^{\alpha_i},q_j^{\alpha_j}|p+a}} 1 + O(\pi(x)(\log\log x)^2).$$

This is because if $q_i^{\alpha_i}q_j^{\alpha_j} > x/4$, and $q_i^{\alpha_i}q_j^{\alpha_j}|p+a$, then $1 < \dfrac{p+a}{q_i^{\alpha_i}q_j^{\alpha_j}} < 4$ has only

finitely many choices, and since ϕ is a multiplicative function and Ω is completely additive, $S'_{2,2}$ gets changed by a constant. Thus,

$$S'_{2,2} \ll \sum_{\substack{y<q_i^{\alpha_i}q_j^{\alpha_j}<x/4 \\ ,\Omega(\phi(q_i^{\alpha_i})),\Omega(\phi(q_j^{\alpha_j}))>100\log\log x}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega(\phi(q_j^{\alpha_j}))\pi(x;q_i^{\alpha_i}q_j^{\alpha_j},-a)+O(\pi(x)(\log\log x)^2).$$

By the Brun-Titchmarsh theorem, this has an upper bound of

$$\sum_{\substack{y<q_i^{\alpha_i}q_j^{\alpha_j}<x/4 \\ \Omega(\phi(q_i^{\alpha_i})),\Omega(\phi(q_j^{\alpha_j}))>100\log\log x}} \frac{\Omega_z(\phi(q_i^{\alpha_i}))\Omega(\phi(q_j^{\alpha_j}))x}{q_i^{\alpha_i}q_j^{\alpha_j}\log(x/q_i^{\alpha_i}q_j^{\alpha_j})}$$

$$=x\left(\sum_{\substack{y<q_iq_j<x/4 \\ \Omega(\phi(q_i)),\Omega(\phi(q_j))>100\log\log x}} \frac{\Omega_z(\phi(q_i))\Omega(\phi(q_j))}{q_iq_j\log(x/q_iq_j)}+O(\pi(x))\right),$$

where the last equality follows because the sum over $q_i^{\alpha_i}q_j^{\alpha_j}$ where $\alpha_i,\alpha_j \geq 2$ is convergent. Now as before, divide the sum into dyadic subintervals. Without loss of generality, choose $y = 2^{\alpha}$, $x/4 = 2^{\beta+1}$ for some α, $\beta > 0$ and $\alpha \leq \beta+1$. Then, the sum is bounded by

$$O\left(\frac{\pi(x)}{\log x}\right).$$

Thus, the assertion in the lemma follows.

□

Proof of Theorem 3.4.2 : To see this, we unfold the square on the left hand side to get

$$\sum_{p\leq x}\left\{\Omega^2(\phi(p+a))+\frac{1}{4}\left(\log\log x\right)^4-2.\frac{1}{2}\left(\log\log x\right)^2\Omega(\phi(p+a))\right\}.$$

Now applying Lemma 3.4.1 and Lemma 3.4.3, the assertion of the theorem follows.

3.5 Erdős-Kac type result for $\Omega(\phi(p+a))$

A strongly additive function $g:\mathbb{N}\to\mathbb{R}$ is an additive function such that $g(p^a)=g(p)$ for all primes p and all integers $a\geq 1$. In 1940, Paul Erdős and Mark Kac proved the following celebrated result.

Theorem 3.5.1 (Erdős, Kac, 1940)**.** *Let $f:\mathbb{N}\to\mathbb{R}$ be a real valued strongly additive function such that $|f(p)|\leq 1$ and set*

$$A(x)=\sum_{p\leq x}\frac{f(p)}{p},$$

and

$$B(x)=\left(\sum_{p\leq x}\frac{f^2(p)}{p}\right)^{1/2}$$

where $B(x)\to\infty$ as $x\to\infty$. Then, given any real number z,

$$\lim_{x\to\infty}\frac{1}{x}\#\left\{n\leq x; f(n)\leq A(x)+zB(x)\right\}=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z}e^{-t^2/2}dt.$$

Setting $f(n) = \omega(n)$, Erdős-Kac theorem says

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{n \leq x; \omega(n) \leq \log\log x + z\sqrt{\log\log x}\right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-t^2/2} dt.$$

In [38], R. Murty and K. Murty initiated the study of $\omega(\phi(n))$ and $\omega(\phi(p))$ and later in [39] (see also [22]). They showed that $\omega(\phi(n))$ and $\omega(\phi(p))$ (respectively, $\Omega(\phi(n))$ and $\Omega(\phi(p))$) obey a normal distribution law, very analogous to $\omega(n)$.

Here, in this section, we aim to prove that a similar result holds for $\Omega(\phi(p+a))$ for any non-zero integer a. The proof follows the similar line of thought as in [39] and [22]. Since $\Omega(\phi(p+a))$ is not strongly additive, we approximate $\Omega(\phi(p+a))$ by a strongly additive function and apply the general existing theory. Finally, we show that the error introduced is small enough to deduce our results.

The following theorem is a "shifted prime analogue" of the celebrated Kubilius-Shapiro theorem for strongly additive functions in probabilistic number theory. For complete proofs of these results, we refer the reader to Chapter 12 of [17].

As before, for a strongly additive function $g(n)$, for positive real x,

$$A(x) = \sum_{p\leq x} \frac{g(p)}{p},$$

and

$$B(x) = \left(\sum_{p\leq x} \frac{g^2(p)}{p}\right)^{1/2} \geq 0.$$

Theorem 3.5.2 (Barban, Vinogradov, Levin, 1965)**.** *Let $g(n)$ be a strongly additive*

function. Then,

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\#\{p\le x;\ g(p+1)\le A(x)+zB(x)\}$$

converges weakly to a limiting distribution as $x\to\infty$, if and only if there is a distribution function $K(u)$ such that as $x\to\infty$,

$$\frac{1}{B^2(x)}\sum_{\substack{p\le x\\ g(p)\le uB(x)}}\frac{g^2(p)}{p}\to K(u).$$

When this condition is satisfied, the characteristic function $\phi(t)$ of the limit law will be given by Kolmogorov's formula

$$\log\phi(t)=\int_{-\infty}^{\infty}(e^{itu}-1-itu)u^{-2}dK(u)$$

and the limit law will have mean 0 *and variance* 1*. In the special case, in order that*

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\#\{p\le x;g(p+1)\le A(x)+zB(x)\}=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z}e^{-t^2/2}dt,$$

it is sufficient that for each fixed $\epsilon>0$, as $x\to\infty$

$$\frac{1}{B^2(x)}\sum_{\substack{p\le x\\ |g(p)|>\epsilon B(x)}}\frac{g^2(p)}{p}\to 0.$$

The statement is valid when $p+1$ is replaced by $p+a$, for some fixed non-zero integer a.

Consider the function $h(n)=\sum_{q|n}\Omega(\phi(q))$, where the sum is over distinct prime divisors q of n. This is strongly additive and hence we can apply Theorem

4.5.1 to it. In [22], the authors showed that

$$A(x) = \sum_{p \leq x} \frac{h(p)}{p} = \frac{1}{2}(\log\log x)^2 + O(\log\log x)$$

and

$$B(x) = \left(\sum_{p \leq x} \frac{h^2(p)}{p} \right)^{1/2} = \frac{1}{\sqrt{3}}(\log\log x)^{3/2} + O(\log\log x).$$

They also check that for each fixed $\epsilon > 0$,

$$\sum_{\substack{p \leq x \\ \Omega(\phi(p)) \geq \epsilon B(x)}} \frac{\Omega^2(\phi(p))}{p} = o(B^2(x)).$$

Hence, a direct application of Theorem 4.5.1 shows that for any non-zero integer a,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \# \left\{ p \leq x; \frac{h(p+a) - \frac{1}{2}(\log\log x)^2}{(\log\log x)^{3/2}} \leq \frac{\alpha}{\sqrt{3}} \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2} dt.$$

Now we want to prove that $\Omega(\phi(p+a))$ is normally distributed. This can be established if we can show that

$$\Omega(\phi(p+a)) - h(p+a) = o((\log\log x)^{3/2})$$

for all but $o(x)$ many primes $p \leq x$.

Lemma 3.5.3. *For any non-zero integer a,*

$$D(x) := \sum_{p \leq x} \left(\Omega(\phi(p+a)) - h(p+a)\right)^2 = O(\pi(x)).$$

Proof. First note that

$$\begin{aligned}\Omega(\phi(p+a)) - h(p+a) &= \sum_{q^\alpha || p+a} \Omega(\phi(q^\alpha)) - \sum_{q | p+a} \Omega(\phi(q)) \\ &= \sum_{\substack{q^\alpha || p+a \\ \alpha \geq 2}} (\Omega(\phi(q^\alpha)) - \Omega(\phi(q))).\end{aligned}$$

Since the number of divisors r^β of $\phi(p+a)$ which are $\geq x^\theta$, for some $\theta > 0$, is absolutely bounded, choosing $z = x^\theta$,

$$\Omega(\phi(p+a)) - h(p+a) = O(\Omega_z(\phi(p+a)) - h_z(p+a))$$

where $h_z(n) = \sum_{\substack{q|n \\ q<z}} \Omega(\phi(q))$. Thus,

$$D(x) \ll \sum_{p \leq x} \left(\sum_{\substack{q^\alpha || p+a \\ \alpha \geq 2, q^\alpha \leq x}} (\Omega_z(\phi(q^\alpha)) - \Omega_z(\phi(q))) \right)^2.$$

We know that $\Omega(n) \leq \frac{\log n}{\log 2}$ for all $n \in \mathbb{N}$. Using this, we get

$$D(x) \ll \sum_{p \leq x} \left(\sum_{\substack{q^\alpha || p+a \\ \alpha \geq 2, q^\alpha \leq x}} (\log q^\alpha)^2 \right)^2.$$

Expanding the square and interchanging sums,

$$
\begin{aligned}
D(x) &= \sum_{p\le x}\left(\sum_{\substack{q_1^{\alpha_1},q_2^{\alpha_2}\mid\mid p+a\\ \alpha_1,\alpha_2\ge 2, q_i^{\alpha_i}\le x}} (\log q_1^{\alpha_1})^2(\log q_2^{\alpha_2})^2\right)\\
&= \sum_{\substack{q_1^{\alpha_1},q_2^{\alpha_2}\le x\\ \alpha_1,\alpha_2\ge 2}} (\log q_1^{\alpha_1})^2(\log q_2^{\alpha_2})^2\left(\sum_{\substack{p\le x\\ p+a\equiv 0(q_i^{\alpha_i}),i=1,2}} 1\right)\\
&= \sum_{\substack{q^{\alpha}\le x\\ \alpha\ge 2}} (\log q^{\alpha})^2\left(\sum_{\substack{p\le x\\ p+a\equiv 0(q^{\alpha})}} 1\right) + \sum_{\substack{q_1^{\alpha_1},q_2^{\alpha_2}\le x\\ \alpha_1\ne\alpha_2\ge 2}} (\log q_1^{\alpha_1})^2(\log q_2^{\alpha_2})^2\left(\sum_{\substack{p\le x\\ p+a\equiv 0(q_1^{\alpha_1}q_2^{\alpha_2})}} 1\right).
\end{aligned}
$$

By the Brun-Titchmarsh theorem (Theorem 3.1.3),

$$
D(x) \ll \pi(x)\left(\sum_{\substack{q^{\alpha}\le x\\ \alpha\ge 2}} \frac{(\log q^{\alpha})^2}{\phi(q^{\alpha})} + \sum_{\substack{q_1^{\alpha_1},q_2^{\alpha_2}\le x\\ \alpha_1\ne\alpha_2\ge 2}} \frac{(\log q_1^{\alpha_1})^2(\log q_2^{\alpha_2})^2}{\phi(q_1^{\alpha_1}q_2^{\alpha_2})}\right).
$$

Since $\alpha \ge 2$ and $\phi(n) = O(n)$, the above expression in braces is bounded which gives

$$
D(x) \ll \pi(x)
$$

which is what we wanted to prove. □

Using this key lemma, we prove the following analogue of the Erdős-Kac theorem.

Theorem 3.5.4. *For any non-zero integer a,*

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\#\left\{p\leq x;\frac{\Omega(\phi(p+a))-\frac{1}{2}(\log\log x)^2}{(\log\log x)^{3/2}}\leq\frac{\alpha}{\sqrt{3}}\right\}=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\alpha}e^{-t^2/2}dt.$$

i.e., $\Omega(\phi(p+a))$, under suitable normalisation, is "normally distributed".

Proof. According to our discussion earlier, it is sufficient to show that

$$\Omega(\phi(p+a))-h(p+a)=o((\log\log x)^{3/2})$$

for all but $o(x)$ many primes $p\leq x$. Indeed, if $p\leq x$ does not satisfy the above equality, then a summand coming from p in $D(x)$ in Lemma 4.5.2 satisfies

$$|\Omega(\phi(p+a))-h(p+a)|\geq(\log\log x)^{3/2}.$$

Lemma 4.5.2 implies that the number of such $p\leq x$ is $O\left(\frac{\pi(x)}{(\log\log x)^3}\right)=o(x)$. □

Remarks To conclude, we remark that the results obtained in Sections 3.4 and 3.5 for $\Omega(\phi(p+a))$ hold for $\omega(\phi(p+a))$ too. We worked with $\Omega(n)$ because its complete additivity works to our advantage in the proofs.

These results also hold for the sum of divisor function $\sigma(n)$. An analogue of Theorem 3.0.1 holds for $\Omega(\sigma(p))$, that is, $\Omega(p+1)$ and thus using similar methods as in Section 4, we can show that $\Omega(\sigma(p+a))$ has normal order $\frac{1}{2}(\log\log p)^2$. In fact, for the number of divisor function $d(n)$, since

$$2^{\omega(n)}\leq d(n)\leq 2^{\Omega(n)},$$

(see p. 274 of [27]), it easily follows that

$$\sum_{p\leq x}\omega(\phi(p+a))\leq\frac{1}{\log 2}\sum_{p\leq x}\log d(\phi(p+a))\leq\sum_{p\leq x}\Omega(\phi(p+a)),$$

and

$$\sum_{p\leq x}\omega^2(\phi(p+a))\leq\frac{1}{(\log 2)^2}\sum_{p\leq x}(\log(d(\phi(p+a))))^2\leq\sum_{p\leq x}\Omega^2(\phi(p+a)).$$

Hence, we can show that $\log(d(\phi(p+a)))$ has normal order $\frac{1}{\log 2}\frac{(\log\log p)^2}{2}$.

These methods can also be adapted to investigate normal number of prime factors of prime shifts of (integer) Fourier coefficients of Hecke eigenforms. But this requires more sophisticated results from algebraic number theory. We treat this case in the next chapter.

Chapter 4

On the normal number of prime factors of the Ramanujan tau function at shifts of prime arguments

4.1 Introduction

There is a further direction for the probabilistic investigations we discussed in the previous chapters into the domain of Fourier coefficients of modular forms, which was noticed first by Ram Murty and Kumar Murty in 1984 [38]. The τ-function defined by

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

has been subject to numerous investigations since Ramanujan discovered its remarkable properties in 1916 [43]. He observed, but did not prove the following properties of the τ function:

1. $\tau(n)$ is multiplicative in n, i.e.,

$$\tau(mn) = \tau(m)\tau(n), \text{ if } \gcd(m,n) = 1. \tag{4.1.1}$$

2. $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$ for p prime and $r > 0$.

3. For all primes p,

$$|\tau(p)| \leq 2p^{11/2}. \tag{4.1.2}$$

Mordell in 1917 proved the first two properties and the third was proved by Deligne in 1974.

The study of divisors of $\tau(n)$ goes back to Ramanujan who conjectured in [43] that $\tau(n) \equiv 0 \pmod{691}$ for almost all n. This was proved by Watson [50] in 1935. Serre proved a stronger statement in [45] : given an integer $d \in \mathbb{Z}_{>0}$, $\tau(n) \equiv 0 \pmod{d}$ for almost all n. Further divisibility properties of $\tau(n)$ have been investigated in [38]. Assuming a quasi-generalised Riemann Hypothesis, Murty and Murty show that

$$\sum_{\substack{p \leq x \\ \tau(p) \neq 0}} (\omega(\tau(p)) - \log\log p)^2 \ll \pi(x)\log\log x$$

and

$$\sum_{n \leq x} (\omega(\tau(n)) - \frac{1}{2}(\log\log n)^2)^2 \ll x(\log\log x)^3 \log_4 x.$$

Here, $\log_4 x$ denotes $\log\log\log\log x$. This result is also true when ω is replaced by Ω. Also, by a quasi-generalized Riemann hypothesis, we mean that there exists a $\delta \in (0, \frac{1}{2})$ such that the Dedekind zeta function $\zeta_K(s)$ for any number field has no

zeroes for $\mathrm{Re}(s) > 1 - \delta$. These results can be thought of as "modular analogues" of the Hardy-Ramanujan theorem. More generally, they also prove a general result for Hecke eigenforms without complex multiplication. We aim to prove a similar normal order result for the number of prime divisors of these Fourier coefficients at shifts of prime arguments.

In [39], the authors obtained a distribution function for $\Omega(\tau(p)), \Omega(\tau(n)), \omega(\tau(p))$ and $\omega(\tau(n))$. In this chapter, assuming the generalised Riemann Hypothesis, we also obtain the same for $\Omega(\tau(p+a))$. This can be thought of as another "modular analogue" of the Erdős Kac theorem.

Notation As before, let S be a subset of $\mathbb{N}$. Let $f : S \to \mathbb{N}$. Denote by $S(N) = \Big|\{s \in S : s \leq N\}\Big|$. We say $f(n)$ has *normal order* $g(n)$ (where $g(n)$ is a continuous monotone function) if given any $\epsilon > 0$,

$$|\{n \leq x, n \in S : \ |f(n) - g(n)| > \epsilon g(n)\}| = o(S(x)),$$

as $x \to \infty$. We introduce other notation as and when they are needed in the chapters.

4.2 Background

By the modified proof of the prime number theorem due to de la Vallée-Poussin in 1899, there exists a constant $c > 0$ such that

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O\left(xe^{-c\sqrt{\log x}}\right).$$

This follows from detailed analysis of the non-trivial zeroes of the Riemann zeta function $\zeta(s)$. In particular, Hadamard and de la Vallée-Poussin proved that if $\rho = \beta + i\gamma$ is a non-trivial zero of the zeta function (that is, ρ is in the critical strip $0 < Re(s) < 1$), then $\beta < 1$. The much celebrated Riemann hypothesis is the statement that $Re(\rho) = \frac{1}{2}$ for all nontrivial zeroes ρ. Assumption of the Riemann Hypothesis improves de la Vallée-Poussin's estimate to

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O\left(\sqrt{x}\log x\right).$$

This fugitive Riemann hypothesis has been both a source of inspiration and frustration for many generations of mathematicians. The assumption of its truth has far reaching consequences; it simplifies many problems and also acts like a telescope to see very far and predict what we can expect. In this chapter, we will assume the Generalised Riemann Hypothesis which is the statement that the non-trivial zeroes of other normalized L-functions have real part equal to $\frac{1}{2}$.

4.2.1 Chebotarev density theorem, Galois representations

Let K be an algebraic number field which is Galois over $\mathbf{Q}$ with group G. For each prime p, we consider a prime $\mathcal{P}$ above p and define the decomposition group

$$D_{\mathcal{P}} = \{\sigma \in G : \mathcal{P}^{\sigma} = \mathcal{P}\} \tag{4.2.1}$$

and the inertia group

$$I_{\mathcal{P}} = \{\sigma \in G : \sigma(x) \equiv x (\text{mod } \mathcal{P})\ \forall x \in \mathcal{O}_K\} \tag{4.2.2}$$

where $\mathcal{O}_K$ denotes the ring of integers of K.

For all but finitely many prime ideals $\mathcal{P}$, $I_{\mathcal{P}} = 1$ and $D_{\mathcal{P}}$ is cyclic. For such prime ideals $\mathcal{P}$, $D_{\mathcal{P}}$ has a canonical generator $\sigma_{\mathcal{P}}$, called the Frobenius automorphism, which has the property that

$$\sigma_{\mathcal{P}}(x) \equiv x^{N\mathcal{P}} \pmod{\mathcal{P}}$$

for each prime ideal $\mathcal{P}$ lying above p. The $\sigma_{\mathcal{P}}$ lie in a conjugacy class as $\mathcal{P}|p$, and this conjugacy class is denoted σ_p. It is called the Artin symbol of p. (If $K/\mathbf{Q}$ is a quadratic extension, the Artin symbol is a generalisation of the familiar Legendre and Kronecker symbols.)

We can form the (incomplete) Artin $L-$function: for each irreducible representation

$$\rho : G \to GL(V)$$

with V a finite dimensional $\mathbf{C}-$vector space, we set

$$L^*(s,\rho) = \prod_p \Big(\det \ \big(1 - \rho(\sigma_p p^{-s})\big)^{-1} \Big)$$

where the product is over p for which the Artin symbol is defined. Artin proved that each $L^*(s,\rho)$ extends to an analytic function for $Re(s) \geq 1$ and does not vanish there, provided $\rho \neq 1$. (If $\rho = 1$, of course $L^*(s,\rho)$ is equal to the Riemann zeta function apart from a finite number of factors.) The Chebotarev density theorem states the following :

Theorem 4.2.1 (Chebotarev Density Theorem)**.** *Let $K/\mathbf{Q}$ be Galois with group G. As*

p varies over the primes for which the Artin symbol is defined, the σ_p's are uniformly distributed in the space of conjugacy classes of G. More precisely, let C be a conjugacy class of G and defined $\pi_C(x, K/\mathbf{Q})$ to be the number of primes p for which σ_p is defined and $\sigma_p = C$. Then

$$\pi_C(x, K/\mathbf{Q}) \sim \frac{|C|}{|G|}\pi(x)$$

as $x \to \infty$, and $\pi(x)$ denote the number of primes upto x.

This theorem is a vast generalisation of both the classical prime number theorem and the prime number theorem for arithmetic progressions.

Let $H(z)$ be a normalized cuspidal newform of even weight $k(\geq 2)$ for $\Gamma_0(N)$ and let χ be its nebentypus. Let $q = e^{2\pi iz}$ with $\mathrm{Im}(z) > 0$. Then $H(z)$ has the following Fourier expansion at $i\infty$,

$$H = \sum_{n\geq 1} a_H(n)q^n. \tag{4.2.3}$$

We know that there is a totally real number field K with ring of integers $\mathcal{O}_K$ such that the Fourier coefficients $a_H(n)$ lie in $\mathcal{O}_K$. For the purposes of our discussion in this chapter, let us assume that these coefficients are rational integers. This forces χ to be real and χ is non-trivial if and only if H has complex multiplication (An eigen form H is said to have *complex multiplication* if there exists an imaginary quadratic field k such that $a_H(p) = 0$ for all primes p unramified and inert in k). Then the function $n \to a_H(n)$ is multiplicative. Then for integers m, n such that $\gcd(m, n) = 1$,

$$a_H(mn) = a_H(m)a_H(n). \tag{4.2.4}$$

Let G denote the absolute Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and d be any positive integer.

Then by Deligne ([14]), there exists a representation

$$\rho_d : G \to GL_2(\prod_{l|d} \mathbf{Z}_l)$$

(here the product is over primes l dividing d) with the following essential property: if p is a prime and $p \nmid dN$ and σ_p is the Frobenius element at p in G, then ρ_d is unramified at p and the trace of ρ_d, that is,

$$tr(\rho_d) = a_p = a_H(p),$$

and the determinant of ρ_d, that is,

$$det(\rho_d(\sigma_p)) = p^{k-1}\chi(p).$$

Hence, questions of divisibility of Fourier coefficients can be investigated through this representation, and by the Chebotarev density theorem. Denote by $\tilde{\rho}_d$ the reduction modulo p map

$$G_{\mathbf{Q}} \to GL_2(\prod_{l|d} \mathbf{Z}_l) \to GL_2(\mathbf{Z}/d\mathbf{Z}).$$

Let the kernel of $\tilde{\rho}_d$ be denoted H_d and K_d denote the subfield of $\overline{\mathbf{Q}}$ fixed by H_d and

$$G_d = G/H_d = \mathrm{Gal}(K_d/\mathbf{Q}).$$

Let C_d be the subset of $\tilde{\rho}_d(G)$ consisting of elements of trace 0 and let $\delta(d) = |C_d|/|G_d|$. The condition $a_q \equiv 0 \pmod{d}$ (for q a prime not dividing dN) means

that for any Frobenius element σ_q of q, $\tilde{\rho}_d(\sigma_q) \in C_d$. Then by Chebotarev Density theorem (Theorem (4.2.1)) applied to $K_d/\mathbf{Q}$,

$$|\{q \leq x : a_H(q) \equiv 0 \pmod{d}\}| \sim \frac{|C_d|}{|G_d|}\pi(x) = \delta(d)\pi(x). \tag{4.2.5}$$

Let us write

$$\pi_H(x,d) = |\{q \leq x : 0 \neq a_H(q) \equiv 0 \pmod{d}\}|$$

and

$$Z_H(x) = |\{q \leq x : a_H(q) = 0\}|.$$

Then the following two lemmas estimates the size of $\pi_H(x,d)$ and $Z_H(x)$. For proofs of these lemmas, see p. 72 of [38].

Lemma 4.2.2. *If H has complex multiplication, $Z_H(x) \sim \frac{1}{2}\pi(x)$. If H does not have complex multiplication,*

$$Z_H(x) \ll \begin{cases} \dfrac{x}{(\log x)^{3/2-\epsilon}} & \text{(for all } \epsilon > 0\text{) unconditionally} \\ x^{3/4} & \text{on the assumption of GRH.} \end{cases}$$

Lemma 4.2.3. *Suppose that H does not have complex multiplication. Then*

$$\pi_H(x,d) \sim \delta(d)\pi(x).$$

If the Generalised Riemann Hypothesis is assumed for all Artin L-series, then for $x \geq 2$,

$$\pi_H(x,d) = \delta(d)\pi(x) + O\left(d^3 x^{1/2}\log(dNx)\right) + O\left(x^{3/4}\right).$$

The above lemma follows from results of Lagarias and Odlyzko [32]. We will also need the following result which describes the density $\delta(l)$ for primes l.

Lemma 4.2.4. *If H is of level 1 or of weight 2, then*

$$\delta(l) = \frac{1}{l} + O\left(\frac{1}{l^2}\right)$$

for all sufficiently large primes l and

$$\delta(ll') = \delta(l)\delta(l')$$

for all sufficiently large primes l, l'. In any case

$$\delta(l) \ll \frac{1}{l}.$$

As Murty and Murty point out in pg. 73 of [38], this lemma is true for weight ≥ 2 without any restriction on level. This follows from work of Carayol ([9] and [10]).

4.3 Application of Selberg's sieve to estimate size of exceptional set for $\Omega(\tau(q))$

We will now see how the use of Galois representations, in combination with the sieve methods can be exploited in an effective manner to give very precise results for the number of prime factors of the Ramanujan tau function. Even though, for the sake of simplicity and clarity of exposition, we state and prove results for

the Ramanujan tau function, all of the results go through for any (integer) Fourier coefficients of non-CM Hecke eigenforms, that is for $a_H(n)$ for H as in (4.2.3)

For any integer $k = 0, 1, \ldots$ let

$$m_k(x) = \{q \leq x : \tau(q) \neq 0,\ \Omega(\tau(q)) = k\}$$

Following the strategy of [18], we first prove the following theorem.

Theorem 4.3.1. *For any integer $k = 0, 1, \ldots$, assuming generalised Riemann Hypothesis for all Artin L-functions, we have*

$$m_k(x) \ll \frac{k\pi(x)}{\log x} \frac{(\log\log x + D)^{k-1}}{(k-1)!} + O\left(\frac{x^{5/6}(\log x)^3}{k^3}\right)$$

for absolute constant D. The implied constant in the O-estimate is absolute.

Proof. Given any prime $q \leq x$, if $\tau(q) \neq 0$, it can be expressed as

$$\tau(q) = a \cdot b$$

where a is z-smooth (all prime factors of a are $\leq z$) and b is z-crunchy (all prime factors of b are $> z$) and $z \in \mathbb{R}$ is a parameter to be chosen later. Let $k \in \mathbb{N}$ be such that

$$\Omega(\tau(q)) = k.$$

If $\Omega(a) = k$, then $b = 1$ and number of such primes $q \leq x$ is at most $O(\pi(z)^k)$. Otherwise if $\Omega(a) \leq (k-1)$, then fixing such an a, let

$$T_a(x) = \left| \left\{ q \leq x :\ \tau(q) \equiv 0 (\text{mod } a),\ \frac{\tau(q)}{a} \text{ has no prime factor less than z} \right\} \right|.$$

Then,

$$m_k(x) = \sum_{\substack{a \leq z^{k-1} \\ \Omega(a) \leq k-1}} T_a(x) + O(\pi(z)^k).$$

Now in order to use Theorem 2.2.1 to estimate $T_a(x)$, we set up our sieve problem.

Let

$$\mathcal{A} = \{q \leq x;\ 0 \neq \tau(q) \equiv 0 (\text{mod } a)\}.$$

Let $\mathcal{P}$ be the set of primes less than z and co-prime to a. For each prime $p \in \mathcal{P}$,

$$\mathcal{A}_p = \{q \leq x;\ 0 \neq \tau(q) \equiv 0 (\text{mod } a),\ \tau(q) \equiv 0 (\text{mod } p)\}$$

and for any square-free integer $d > 0$,

$$\mathcal{A}_d = \bigcap_{\substack{p|d \\ p \in \mathcal{P}}} \mathcal{A}_p.$$

Then, clearly, $T_a(x) = S(\mathcal{A}, \mathcal{P}, z)$. By Lemma 4.2.3,

$$|\mathcal{A}| = \delta(a)\pi(x) + O\left(a^3 x^{1/2} \log(aNx)\right) + O(x^{3/4})$$

and

$$|\mathcal{A}_p| = \delta(p)\delta(a)\pi(x) + O\left((ap)^3 x^{1/2} \log(apNx)\right) + O(x^{3/4}).$$

It is easy to show that with notation as in Theorem 2.2.1,

$$f_1(d) = \phi(d)\ ,\ V(z) \geq \log z + O(1)$$

and

$$R_t = O\left((at)^3 x^{1/2}\log(atNx)\right) + O(x^{3/4}).$$

Hence, we get

$$\begin{aligned} T_a(x) &\leq \frac{\delta(a)\pi(x)}{\log z} + O\left(\sum_{t\leq z^2} d(t^2)|R_t|\right) \\ &\ll \frac{\pi(x)}{a\log z} + O\left(\sum_{t\leq z^2} d(t^2)|R_t|\right) \end{aligned}$$

This follows from the estimate of $\delta(p)$, for a prime p, from Lemma 4.2.4. The error term above is

$$\begin{aligned} E_z(a) &:= O\left(\sum_{t\leq z^2} d(t^2)(at)^3 x^{1/2}\log(atNx)\right) + O\left(\sum_{t\leq z^2} d(t^2)x^{3/4}\right) \\ &= O\left(x^{1/2}a^3(\log a)\sum_{t\leq z^2} d(t^2)t^3\right) + O\left(x^{3/4}\sum_{t\leq z^2} d(t^2)\right) \\ &= O\left(x^{1/2}a^3(\log a)z^6z^2(\log z)^2\right) + O\left(x^{3/4}(z^2)(\log z)^2\right) \\ &= O\left(x^{1/2}a^3(\log a)z^8(\log z)^2\right) + O\left(x^{3/4}(z^2)(\log z)^2\right) \end{aligned}$$

Here we use the Lemma 2.4.2 to estimate $\sum_{t\leq z^2} d(t^2)$. Thus we get that

$$\begin{aligned}
m_k(x) &\ll \sum_{\substack{a\leq z^{k-1}\\ \Omega(a)\leq k-1}} \frac{\pi(x)}{a\log z} + O\left(\sum_{\substack{a\leq z^{k-1}\\ \Omega(a)\leq k-1}} E_z(a)\right) + O(\pi(z)^k).\\
&= \frac{\pi(x)}{\log z}\left(\sum_{\substack{a\leq z^{k-1}\\ \Omega(a)\leq k-1}} \frac{1}{a}\right) + O\left(x^{\frac{1}{2}} z^8 (\log z)^2 \sum_{a\leq z^{k-1}} a^3\log a\right) + O\left(x^{\frac{3}{4}}(z^2)(\log z)^2 \sum_{a\leq z^{k-1}} 1\right)\\
&\ll \frac{\pi(x)}{\log z}\frac{\left(1+\sum_{p\leq z^{k-1}}\frac{1}{p}\right)^{k-1}}{(k-1)\,!} + O\left(x^{\frac{1}{2}} z^8 (\log z)^3 (z^{k-1})^3 z^{k-1}\right) + O\left(x^{\frac{3}{4}}(z^2)(\log z)^2 z^{k-1}\right)\\
&\ll \frac{\pi(x)}{\log z}\frac{(\log\log z^{k-1}+C)^{k-1}}{(k-1)\,!} + O\left(x^{\frac{1}{2}} z^{4k+4}(\log z)^3\right) + O\left(x^{\frac{3}{4}} z^{k+1}(\log z)^2\right)
\end{aligned}$$

Note, in estimating the error above, we have only used the crude upper bound of a, which is z^{k-1} and used the elementary fact that

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + O(1).$$

Choosing $z = x^{1/12k}$, we get an upper bound of

$$\frac{k\pi(x)}{\log x}\frac{(\log\log x + D)^{k-1}}{(k-1)!} + O\left(\frac{x^{5/6}(\log x)^3}{k^3}\right).$$

□

In [38], Murty and Murty showed assuming quasi-GRH, that the normal order of $\Omega(\tau(q))$ is $\log\log q$. In other words, $\Omega(\tau(q))$ "usually" behaves like $\log\log q$. In particular, they have the following theorem.

Theorem 4.3.2 (Murty, Murty, 1984)**.** *Assuming the quasi-Generalized Riemann Hypothesis for Artin L-series(related to τ function),*

$$\sum_{\substack{p\leq x\\ \tau(p)\neq 0}} (\omega(\tau(p)) - \log\log p)^2 \ll \pi(x)\log\log x$$

and

$$\sum_{\substack{n\leq x\\ \tau(n)\neq 0}} (\omega(\tau(n)) - \frac{1}{2}(\log\log n)^2)^2 \ll x(\log\log x)^3 \log\log\log\log x.$$

In other words, $\omega(\tau(p))$ has normal order $\log\log p$ and $\omega(\tau(n))$ has normal order $\frac{1}{2}(\log\log n)^2$. This result is also true when $\omega(n)$ is replaced by $\Omega(n)$.

In the following theorem, we estimate the size of the exceptional set where $\Omega(\tau(q))$ deviates from its usual behaviour.

Theorem 4.3.3. *Given any $A > 6$, let $B = A(\log A - 1)$. Then, assuming the generalised Riemann Hypothesis for all Artin L-functions, we have*

$$M_{A,\tau}(x) = |\{q \leq x : |\Omega(\tau(q))| > A\log\log x\}| = \frac{\pi(x)}{(\log x)^B}. \tag{4.3.1}$$

Proof. Given any $A > 0$, we want to estimate

$$\begin{aligned} M_{A,\tau}(x) &= \sum_{\substack{q\leq x\\ |\Omega(\tau(q))|>A\log\log x}} 1 = \sum_{k>A\log\log x} \sum_{\substack{q\leq x\\ \tau(q)\neq 0\\ |\Omega(\tau(q))|=k}} 1 \\ &= \sum_{k>A\log\log x} m_k(x) \end{aligned}$$

However, since for any $n \in \mathbf{N}$, $\Omega(n) \leq \dfrac{\log n}{\log 2}$, it implies that

$$\begin{aligned}\Omega(\tau(q)) &\leq \frac{(\log|\tau(q)|)}{\log 2}\\ &\leq \frac{\log(2q^{\frac{11}{2}})}{\log 2}\\ &\leq \frac{11}{2}\frac{\log(2q)}{\log 2}\\ &\leq 11\frac{\log q}{\log 2} \text{ [since } q \geq 2]\end{aligned}$$

Thus, to estimate $M_{A,\tau}(x)$, instead of considering the whole sum, we can consider k in the interval $A\log\log x < k < 11\dfrac{\log x}{\log 2}$,

$$M_{A,\tau}(x) = \frac{\pi(x)}{\log x}\tilde{\sum}\frac{(\log\log x + D)^{k-1}}{(k-1)\,!} + O\left(x^{\frac{5}{6}}(\log x)^3\tilde{\sum}\frac{1}{k^3}\right) \tag{4.3.2}$$

Here $\tilde{\sum}$ denotes the sum over k in $A\log\log x < k < 11\frac{\log x}{\log 2}$. This is

$$\begin{aligned}&\ll \pi(x)\tilde{\sum}\frac{(\log\log x + D)^{k-1}}{(k-1)\,!} + O\left(\frac{x^{\frac{5}{6}}(\log x)^3}{(A\log\log x)^3}\tilde{\sum}1\right)\\ &\ll \pi(x)\sum_{k>A\log\log x}\frac{(\log\log x + D)^{k-1}}{(k-1)\,!} + O\left(\frac{x^{\frac{5}{6}}(\log x)^3}{(\log\log x)^3}(\log x)\right)\end{aligned}$$

As in Theorem 3.0.1, writing

$$\sum_{k>A\log\log x}\frac{(\log\log x + D)^{k-1}}{(k-1)!} = U_1 + U_2$$

where

$$U_1 = \sum_{k>A(\log\log x+D)} \frac{(\log\log x + D)^{k-1}}{(k-1)!}$$

and

$$U_2 = \sum_{A(\log\log x+D)>k>A\log\log x} \frac{(\log\log x + D)^{k-1}}{(k-1)!},$$

and estimating U_1 and U_2 as

$$U_1 \leq (\log x)^{A(1-\log A)} \tag{4.3.3}$$

and

$$U_2 \leq \frac{AD}{e^{AD(\log A-1)}}(\log x)^{A(1-\log A)}, \tag{4.3.4}$$

we get that

$$M_{\tau,A}(x) \ll \frac{\pi(x)}{(\log x)^{A(\log A-1)}} + O\left(\frac{x^{\frac{5}{6}}(\log x)^4}{(\log\log x)^3}\right).$$

Clearly, for $A > 6$, $A(\log A - 1) > 5$ and the first term above dominates. Thus, the theorem follows. □

4.4 Mean and Variance for $\Omega(\tau(p+a))$

In this section, we will compute the first and second moments of $\Omega(\tau(p+a))$ and hence compute the normal number of prime factors of the Ramanujan tau function at shifts of primes. Of course in all of these results we assume that the generalised Riemann Hypothesis holds true for all Artin L-functions. As in the case for the Euler phi function, we proceed by employing the "divide and conquer" method.

For a prime p and any non-zero integer a, let

$$p + a = \prod_{i \leq k} q_i^{\alpha_i}$$

be the unique prime power decomposition for $(p + a)$. Since τ is a multiplicative function, we have that

$$\tau(p+a) = \tau(\prod_{i \leq k} q_i^{\alpha_i}) = \prod_{i=1}^{k} \tau(q_i^{\alpha_i}) = \tau_0(p+a)\tau_1(p+a)$$

where

$$\tau_0(p+a) = \left(\prod_{q^\alpha \leq y} \tau(q^\alpha) \right), \ \tau_1(p+a) = \left(\prod_{q^\alpha > y} \tau(q^\alpha) \right)$$

and y is a parameter to be chosen later. Since $\Omega(n)$ is a completely additive function,

$$\Omega(\tau(p+a)) = \Omega(\prod_{i=1}^{k} \tau(q_i^{\alpha_i})) = \sum_{q^\alpha || p+a} \Omega(\tau(q^\alpha)).$$

We can write

$$\Omega(\tau(p+a)) = \sum_{q^\alpha \leq y} \Omega(\tau(q^\alpha)) + \sum_{q^\alpha > y} \Omega(\tau(q^\alpha)), \tag{4.4.1}$$

where the sum is over prime powers $q^\alpha || (p + a)$.

As before, let $\Omega_z(n)$ denote the number of prime factors (counted with multiplicity) of n, which are less than or equal to z, that is, if $n = \prod_{i \leq k} {p_i}^{\alpha_i}$, then $\Omega_z(n) = \sum_{\substack{p^\alpha || n \\ p \leq z}} \alpha$. Since for any prime p, $\tau(p)$ is bounded by (4.1.2), and $\tau(n)$ is

multiplicative by (4.1.1), choosing $z = x^\theta$ for some $\theta > 0$, we observe that

$$\Omega(\tau(p+a)) = \Omega_z(\tau(p+a)) + O(1)$$

because the number of prime power divisors r^β of $\tau(p+a)$ with $r^\beta > x^\theta$ is absolutely bounded by virtue of (4.1.2). Note that (4.4.1) still holds when Ω is replaced by Ω_z.

Since we are assuming the generalised Riemann hypothesis in all our results in this section, we assume $\tau(n) \neq 0$ for all integers n. Lehmer conjectured this in 1947. Even though it is unresolved until now, by Lemma 4.2.2, we know that the generalised Riemann Hypothesis implies that the exceptional set where $\tau(n) \neq 0$ is $O(x^{3/4})$ which is much smaller compared to the error term in our results. Hence we will assume this non-vanishing property of the τ function to simplify our discussion.

In the following theorem, we estimate the first moment (mean) of prime power divisors of prime shifts of $\tau(n)$, that is, $\tau(p+a)$ for any fixed $a > 0$.

Theorem 4.4.1. *For any non-zero integer a, assuming the generalised Riemann hypothesis for all Artin L-functions,*

$$\sum_{\substack{p \leq x \\ \tau(p+a)\neq 0}} \Omega(\tau(p+a)) = \frac{1}{2}\pi(x)(\log\log x)^2 + O\left(\frac{x}{\log x}\right).$$

Proof. By our observation earlier, and with our choice of $z = x^\theta$, $(\theta > 0)$,

$$\begin{aligned}\sum_{p\le x}\Omega(\tau(p+a)) &= \sum_{p\le x}(\Omega_z(\tau(p+a))+O(1))\\ &= \sum_{p\le x}\Omega_z(\tau(p+a))+O\left(\frac{x}{\log x}\right).\end{aligned}$$

Thus it suffices to investigate $\sum_{p\le x}\Omega_z(\tau(p+a))$.

$$\sum_{p\le x}\Omega_z(\tau(p+a)) = \sum_{p\le x}\sum_{\substack{q^\alpha||p+a\\ q^\alpha\le y}}\Omega_z(\tau(q^\alpha))+\sum_{p\le x}\sum_{\substack{q^\alpha||p+a\\ q^\alpha> y}}\Omega_z(\tau(q^\alpha)).$$

Let us write the above two sums as Σ_1, Σ_2. Interchanging sums in Σ_1, we get

$$\begin{aligned}\Sigma_1 &= \sum_{q^\alpha\le y}\Omega_z(\tau(q^\alpha))\left(\sum_{\substack{p\le x\\ q^\alpha|p+a}}1\right)\\ &= \sum_{q^\alpha\le y}\Omega_z(\tau(q^\alpha))\pi(x;q^\alpha,-a).\end{aligned}$$

The above sum is

$$\sum_{q^\alpha\le y}\Omega_z(\tau(q^\alpha))\frac{\pi(x)}{\phi(q^\alpha)}+\sum_{q^\alpha\le y}\Omega_z(\tau(q^\alpha))E(x;q^\alpha,-a).$$

As in the previous chapter, in the case of the Euler ϕ-function, choosing $y = \dfrac{x^{1/2}}{(\log x)^{12}}$ and applying the Bombieri-Vinogradov theorem (Theorem (3.1.4)), we get

$$\sum_{q^\alpha\le y}|E(x;q^\alpha,-a)| = O\left(\frac{x}{(\log x)^2}\right).$$

So the required sum Σ_1 is

$$\pi(x) \sum_{q^\alpha \leq y} \frac{\Omega_z(\tau(q^\alpha))}{\phi(q^\alpha)} + O\left(\frac{x}{\log x}\right).$$

Note, if $\alpha \geq 2$,$\frac{\Omega_z(\tau(q^\alpha))}{\phi(q^\alpha)} \ll \frac{\log(q^\alpha)}{q^\alpha}$ (since, $\Omega(n) \ll \log n$ for all $n \in \mathbb{N}$, $\tau(n)$ is multiplicative and by (4.1.2), $|\tau(q)|$ is bounded above by $2q^{11/2}$). Now for $\alpha \geq 2$, $\frac{\alpha}{q^\alpha} \leq \frac{2}{q^2}$, and so, $\frac{\log(q^\alpha)}{q^\alpha} \leq \frac{\log q^2}{q^2}$. Thus, the contribution to the first sum from q^α with $\alpha \geq 2$, is bounded absolutely. Therefore,

$$\Sigma_1 = \pi(x) \sum_{q \leq y} \frac{\Omega_z(\tau(q))}{\phi(q)} + O\left(\frac{x}{\log x}\right).$$

Let $B(y)$ denote the sum $\sum_{q \leq y} \Omega_z(\tau(q))$. To prove the normal order result, Theorem 4.3.2, Murty and Murty showed that assuming quasi-GRH,

$$\sum_{\substack{q \leq x \\ \tau(q) \neq 0}} \Omega_z(\tau(q)) = \pi(x) \log\log z + O(\pi(x)) \tag{4.4.2}$$

Using (4.4.2) and by the partial summation formula, we get,

$$\begin{aligned}\Sigma_1 &= \pi(x) \int_2^y \frac{B(t)}{t^2} dt + O\left(\frac{x}{\log x}\right) \\ &= \pi(x) \int_2^y \frac{\pi(t) \log\log t}{t^2} dt + O\left(\frac{x}{\log x}\right).\end{aligned}$$

Thus,

$$\Sigma_1 = \pi(x) \frac{(\log\log y)^2}{2} + O\left(\frac{x}{\log x}\right).$$

Now,

$$\Sigma_2 = \sum_{p \le x} \sum_{\substack{q^\alpha || p+a \\ q^\alpha > y}} \Omega_z(\tau(q^\alpha)).$$

Since $y = \frac{x^{1/2}}{(\log x)^{12}}$, there are only finitely many q^α in the inner sum in Σ_2. But $\Omega_z(\tau(q^\alpha))$ can take a large value. So, to investigate this phenomenon, we divide the inner sum into two parts,

$$\Sigma_2 = T_1 + T_2$$

where

$$T_1 = \sum_{p \le x} \sum_{\substack{q^\alpha | p+a \\ q^\alpha > y \\ \Omega(\tau(q^\alpha)) < 100 \log\log x}} \Omega_z(\tau(q^\alpha))$$

and

$$T_2 = \sum_{p \le x} \sum_{\substack{q^\alpha | p+a \\ q^\alpha > y \\ \Omega(\tau(q^\alpha)) > 100 \log\log x}} \Omega_z(\tau(q^\alpha)).$$

Clearly,

$$\begin{aligned} T_1 &= O\left(\log\log x \sum_{p \le x} \sum_{\substack{q^\alpha | p+a \\ q^\alpha > y}} 1 \right) \\ &= O\left(\pi(x) \log\log x\right) \end{aligned}$$

because there are only finitely many such q^α. Thus,

$$\Sigma_2 = T_2 + O\left(\pi(x) \log\log x\right).$$

Now, we can write

$$T_2 = \sum_{p\le x}{}' \sum_{\substack{q^\alpha | p+a \\ q^\alpha > y \\ \Omega(\tau(q^\alpha))>100\log\log x}} \Omega_z(\tau(q^\alpha)) + O\left(\pi(x)\log\log x\right).$$

Here, $\sum_p'$ denotes the sum over $p \le x$ such that $p+a$ is not prime, because if $p+a$ is a prime, then by (4.4.2),

$$\sum_{p\le x} \Omega(\tau(p+a) \ll \sum_{\substack{l\le x \\ l \text{ prime}}} \Omega(\tau(l)) = O(\pi(x)\log\log x).$$

Therefore, we have

$$\begin{aligned} T_2 &= \sum_{p\le x}{}' \sum_{\substack{q^\alpha || p+a \\ q^\alpha > y \\ \Omega(\tau(q^\alpha))>100\log\log x}} \Omega_z(\tau(q^\alpha)) + O(\pi(x)\log\log x) \\ &\ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\tau(q^\alpha))>100\log\log x}} \Omega_z(\tau(q^\alpha)) \sum_{\substack{p\le x \\ q^\alpha | p+a}} 1 + O(\pi(x)\log\log x). \end{aligned}$$

This is because if $q^\alpha > x/4$, and $q^\alpha | p+a$, then $1 < \dfrac{p+a}{q^\alpha} < 4$ has only finitely many choices, and since τ is multiplicative function and Ω is completely additive, T_2 gets changed by a constant. Thus,

$$T_2 \ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\tau(q^\alpha))>100\log\log x}} \Omega_z(\tau(q^\alpha))\pi(x;q^\alpha,-a) + O(\pi(x)\log\log x).$$

By the Brun-Titchmarsh theorem (Theorem 3.1.3), this has an upper bound of

$$\begin{aligned}
&\ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\tau(q^\alpha))>100\log\log x}} \frac{\Omega_z(\tau(q^\alpha))x}{q^\alpha \log(x/q^\alpha)} \\
&= x \sum_{\substack{y<q<x/4 \\ \Omega(\tau(q))>100\log\log x}} \frac{\Omega_z(\tau(q))}{q\log(x/q)} + O(\pi(x)),
\end{aligned}$$

where the last equality follows because the sum over q^α is convergent when $\alpha \geq 2$. To estimate the sum, we divide the sum into dyadic subintervals. Without loss of generality, choose $y = 2^\alpha$, $x/4 = 2^{\beta+1}$ for some α, $\beta > 0$ and $\alpha \leq \beta + 1$. Then, the sum is bounded by

$$\begin{aligned}
&x \sum_{j=\alpha}^{\beta} \frac{1}{(\beta+2)-(j+1)} \sum_{\substack{2^j\leq q<2^{j+1} \\ \Omega(\tau(q))>100\log\log x}} \frac{\Omega_z(\tau(q))}{q} \\
\ll &x \sum_{j=\alpha}^{\beta} \frac{1}{(\beta+2)-(j+1)} \sum_{\substack{2^j\leq q<2^{j+1} \\ \Omega(\tau(q))>100\log\log x}} \frac{\log q}{q}.
\end{aligned}$$

Now, by the partial summation formula,

$$\sum_{\substack{q\geq m \\ \Omega(\tau(q))>100\log\log m}} \frac{\log q}{q} \ll \int_m^\infty \frac{\log t}{t^2} M_{100,\tau}(t)dt$$

where

$$M_{A,\tau}(t) = \sum_{\substack{p\leq t \\ \Omega(\tau(p))>A\log\log x}} 1$$

which by Theorem 4.3.3 is $O\left(\frac{\pi(x)}{(\log x)^B}\right)$ where $B = 100(\log 100 - 1)$. Thus the statement of the theorem follows.

□

Next, our aim is to prove the following theorem.

Theorem 4.4.2. *For any $a \neq 0$, $a \in \mathbb{Z}$, assuming the generalised Riemann hypothesis for all Artin L-functions,*

$$\sum_{\substack{p \leq x \\ \tau(p+a)\neq 0}} \left(\Omega(\tau(p+a)) - \frac{1}{2}(\log\log x)^2\right)^2 = \pi(x)\frac{(\log\log x)^3}{3} + o(\pi(x)(\log\log x)^3);$$

which implies, $\Omega(\tau(p+a))$ has normal order $\frac{(\log\log p)^2}{2}$.

The proof of this theorem relies on the following lemma.

Lemma 4.4.3. *For any $a \neq 0$, $a \in \mathbb{Z}$, assuming the generalised Riemann hypothesis for all Artin L-functions,*

$$\sum_{\substack{p \leq x \\ \tau(p+a)\neq 0}} \Omega^2(\tau(p+a)) = \pi(x)\left(\frac{(\log\log x)^2}{2}\right)^2 + \pi(x)\frac{(\log\log x)^3}{3} + O(\frac{x}{\log x}).$$

Proof. Again, throughout the proof, we assume that we are summing over primes p, such that $\tau(p+a) \neq 0$, because by Theorem 4.2.2, the number of such primes is

$O(\pi(x))$. Clearly, since $\Omega(n)$ is a completely additive function and $\tau(n)$ is multiplicative,

$$\begin{aligned}\Omega^2(\tau(p+a)) &= \left[\sum_{q^\alpha||p+a} \Omega(\tau(q^\alpha))\right]^2 \\ &= \sum_{q^\alpha||p+a} \Omega(\tau(q^\alpha))^2 + \sum_{\substack{q_i^{\alpha_i}||p+a \\ q_j^{\alpha_j}||p+a \\ q_i \neq q_j}} \Omega(\tau(q_i^{\alpha_i}))\Omega(\tau(q_j^{\alpha_j})).\end{aligned}$$

Again, choosing $z = x^\theta$, for some $\theta > 0$, and noting that the number of prime divisors r^β of $\phi(q^\alpha)$ with $r^\beta > x^\theta$ is absolutely bounded ,

$$\sum_{p\leq x} \Omega^2(\tau(p+a)) = S_1 + S_1' + S_2 + S_2' + O\left(\frac{x}{\log x}\right)$$

where

$$S_1 = \sum_{p\leq x} \sum_{\substack{q^\alpha||p+a \\ q^\alpha \leq y}} \Omega_z(\tau(q^\alpha))^2,\ S_1' = \sum_{p\leq x} \sum_{\substack{q^\alpha||p+a \\ q^\alpha > y}} \Omega_z(\tau(q^\alpha))^2$$

$$S_2 = \sum_{p\leq x} \sum_{\substack{q_i^{\alpha_i}||p+a \\ q_j^{\alpha_j}||p+a \\ q_i^{\alpha_i} \neq q_j^{\alpha_j} \leq y}} \Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j})),\ S_2' = \sum_{p\leq x} \sum_{\substack{q_i^{\alpha_i}||p+a \\ q_j^{\alpha_j}||p+a \\ q_i^{\alpha_i} \neq q_j^{\alpha_j} > y}} \Omega_z(\phi(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j})).$$

Consider the sum S_1. As before, by the Brun-Titchmarsh theorem (Theorem 3.1.3) and the Bombieri-Vinogradov theorem (Theorem 3.1.4), choosing $y = \frac{x^{1/2}}{(\log x)^{14}}$, we

get

$$\begin{aligned} S_1 &= \sum_{q^\alpha \le y} \Omega_z(\tau(q^\alpha))^2 \pi(x; q^\alpha, -a) \\ &= \pi(x) \sum_{q^\alpha \le y} \frac{\Omega_z(\tau(q^\alpha))^2}{\phi(q^\alpha)} + \sum_{q^\alpha \le y} \Omega_z(\tau(q^\alpha))^2 E(x; q^\alpha, -a) \\ &= \pi(x) \sum_{q^\alpha \le y} \frac{\Omega_z(\tau(q^\alpha))^2}{\phi(q^\alpha)} + O\left(\frac{x}{\log x}\right). \end{aligned}$$

Since the contribution from q^α with $\alpha \ge 2$ is $O(x/\log x)$,

$$S_1 = \pi(x) \sum_{q \le y} \frac{\Omega_z(\tau(q))^2}{\phi(q)} + O\left(\frac{x}{\log x}\right).$$

Denote by $D(y) = \sum_{q \le y} \Omega_z^2(\tau(q))$. Then in order to prove Theorem (4.3.2), Murty and Murty showed that assuming the generalised Riemann Hypothesis,

$$\sum_{\substack{q \le x \\ \tau(q) \ne 0}} \Omega_z^2(\tau(q)) = \pi(x)(\log\log z)^2 + O(\pi(x)\log\log x). \tag{4.4.3}$$

Using (4.4.3) and the partial summation formula, as before, we get

$$\sum_{q \le y} \frac{\Omega_z(\tau(q))^2}{\phi(q)} = \frac{1}{3}(\log\log y)^3 + O(\log\log y)^2).$$

Thus,

$$S_1 = \pi(x)\left(\frac{1}{3}(\log\log x)^3 + O((\log\log x)^2)\right) + O\left(\frac{x}{\log x}\right).$$

Now let us consider S_2.

It follows that

$$S_2 = \pi(x) \sum_{\substack{q_i^{\alpha_i}, q_j^{\alpha_j} \le y \\ q_i \neq q_j}} \frac{\Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j}))}{\phi(q_i^{\alpha_i} q_j^{\alpha_j})} + \sum_{q_i^{\alpha_i} q_j^{\alpha_j} \le y^2} \Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j}))E(x; q_i^{\alpha_i} q_j^{\alpha_j}, -a).$$

Choosing $y = \frac{x^{1/4}}{(\log x)^7}$ and using the Bombieri-Vinogradov theorem, we get

$$\sum_{q_i^{\alpha_i} q_j^{\alpha_j} \le y^2} \Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j}))E(x; q_i^{\alpha_i} q_j^{\alpha_j}, -a) = O\left(\frac{x}{(\log x)^2}\right).$$

Also if either α_i or $\alpha_j \ge 2$, $\dfrac{\Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j}))}{\phi(q_i^{\alpha_i} q_j^{\alpha_j})} \le \dfrac{\alpha_i \alpha_j \log(q_i q_j)}{(q_i q_j)^2}$ and thus in this case, there is at most a contribution of $O\left(\dfrac{x}{\log x}\right)$ to S_2. Thus we can write

$$S_2 = \pi(x) \sum_{\substack{q_i, q_j \le y \\ q_i \neq q_j}} \frac{\Omega_z(\tau(q_i))\Omega_z(\tau(q_j))}{\phi(q_i q_j)} + O\left(\frac{x}{\log x}\right).$$

Now we observe that, since $\Omega(n)$ is a completely additive function,

$$\sum_{\substack{q_i, q_j \le y \\ q_i \neq q_j}} \frac{\Omega_z(\tau(q_i))\Omega_z(\tau(q_j))}{\phi(q_i q_j)} = \left(\sum_{q \le y} \frac{\Omega_z(\tau(q))}{\tau(q)}\right)^2 - \sum_{q \le y} \frac{\Omega_z(\tau(q))^2}{\tau(q)^2}.$$

But we know from the proof of Theorem 4.4.1, $\left(\sum_{q \le y} \dfrac{\Omega_z(\tau(q))}{\phi(q)}\right) = \frac{1}{2}(\log\log y)^2 +$

$O\left(\frac{x}{\log x}\right)$ and $\sum_{q\leq y}\frac{\Omega_z(\tau(q))^2}{\phi(q)^2}$ is convergent, hence absolutely bounded. Thus,

$$S_2 = \pi(x)\left(\frac{1}{2}(\log\log x)^2\right)^2 + O(\pi(x)).$$

Thus we get,

$$\begin{aligned}\sum_{p\leq x}\Omega^2(\tau(p+a)) &= S_1 + S_2 + S_1' + S_2' + O\left(\frac{x}{\log x}\right)\\ &= S_1' + S_2' + \pi(x)\left(\frac{(\log\log x)^2}{2}\right)^2 + \pi(x)\frac{(\log\log x)^3}{3} + O\left(\frac{x}{\log x}\right)\end{aligned}$$

Now we can write S_1' as

$$S_1' = S_{1,1}' + S_{1,2}'$$

where

$$S_{1,1}' = \sum_{p\leq x}\sum_{\substack{q^\alpha | p+a\\ q^\alpha > y\\ \Omega(\tau(q^\alpha))<100\log\log x}}\Omega_z^2(\tau(q^\alpha))$$

and

$$S_{1,2}' = \sum_{p\leq x}\sum_{\substack{q^\alpha | p+a\\ q^\alpha > y\\ \Omega(\tau(q^\alpha))>100\log\log x}}\Omega_z^2(\tau(q^\alpha)).$$

Clearly,

$$\begin{aligned}S_{1,1}' &= O\left((\log\log x)^2\sum_{p\leq x}\sum_{\substack{q^\alpha | p+a\\ q^\alpha > y}}1\right)\\ &= O\left(\pi(x)(\log\log x)^2\right)\end{aligned}$$

because there are only finitely many such q^α. Thus,

$$S_1' = S_{1,2}' + O\left(\pi(x)(\log\log x)^2\right).$$

Now, we can write

$$S_{1,2}' = \sum_{p\le x}{}' \sum_{\substack{q^\alpha | p+a \\ q^\alpha > y \\ \Omega(\tau(q^\alpha))>100\log\log x}} \Omega_z^2(\tau(q^\alpha)) + O\left(\pi(x)\log\log x\right).$$

Here, $\sum_p'$ denotes the sum over $p \le x$ such that $p+a$ is not prime, because if $p+a$ is a prime, then

$$\sum_{p\le x} \Omega^2(\tau(p+a) \ll \sum_{\substack{l\le x \\ l \text{ prime}}} \Omega^2(\tau(l)) = O(\pi(x)(\log\log x)^2).$$

Also, since $\tau(n) = O(n^6)$, the number of prime power divisors r^β of $\tau(q^\alpha)$ with $\alpha \ge 2$ is $O(1)$. So,

$$\begin{aligned} S_{1,2}' &= \sum_{p\le x}{}' \sum_{\substack{q^\alpha || p+a \\ q^\alpha > y \\ \Omega(\tau(q^\alpha))>100\log\log x}} \Omega_z^2(\tau(q^\alpha)) + O(\pi(x)(\log\log x)^2) \\ &\ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\tau(q^\alpha))>100\log\log x}} \Omega_z^2(\tau(q^\alpha)) \sum_{\substack{p\le x \\ q^\alpha | p+a}} 1 + O(\pi(x)(\log\log x)^2). \end{aligned}$$

This is because if $q^\alpha > x/4$, and $q^\alpha | p+a$, then $1 < \dfrac{p+a}{q^\alpha} < 4$ has only finitely many choices, and since τ is multiplicative function and Ω is completely additive,

$S'_{1,2}$ gets changed by a constant. Thus,

$$S'_{1,2} \ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\tau(q^\alpha))>100\log\log x}} \Omega_z^2(\tau(q^\alpha))\pi(x;q^\alpha,-a) + O(\pi(x)(\log\log x)^2).$$

By the Brun-Titchmarsh theorem (Theorem 3.1.3), this has an upper bound of

$$\begin{aligned} &\ll \sum_{\substack{y<q^\alpha<x/4 \\ \Omega(\tau(q^\alpha))>100\log\log x}} \frac{\Omega_z^2(\tau(q^\alpha))x}{q^\alpha\log(x/q^\alpha)} \\ &= x \sum_{\substack{y<q<x/4 \\ \Omega(\tau(q))>100\log\log x}} \frac{\Omega_z^2(\tau(q))}{q\log(x/q)} + O(\pi(x)), \end{aligned}$$

where the last equality follows because the sum over q^α is convergent when $\alpha \geq 2$. Now again divide the sum into dyadic subintervals. Without loss of generality, choose $y = 2^\alpha$, $x/4 = 2^{\beta+1}$ for some α, $\beta > 0$ and $\alpha \leq \beta + 1$. Then, the sum is bounded by

$$\begin{aligned} &x\sum_{j=\alpha}^{\beta} \frac{1}{(\beta+2)-(j+1)} \sum_{\substack{2^j\leq q<2^{j+1} \\ \Omega(\tau(q))>100\log\log x}} \frac{\Omega_z^2(\tau(q))}{q} \\ \ll &x\sum_{j=\alpha}^{\beta} \frac{1}{(\beta+2)-(j+1)} \sum_{\substack{2^j\leq q<2^{j+1} \\ \Omega(\tau(q))>100\log\log x}} \frac{(\log q)^2}{q}. \end{aligned}$$

Now, by the partial summation formula,

$$\sum_{\substack{q\geq m \\ \Omega(\tau(q))>100\log\log m}} \frac{(\log q)^2}{q} \ll \int_m^\infty \frac{(\log t)^2}{t^2} M_{100,\tau}(t)dt$$

where

$$M_{A,\tau}(t) = \sum_{\substack{p \le t \\ \Omega(\tau(p)) > A \log\log x}} 1$$

which by Theorem 4.3.3 is $O\left(\frac{\pi(x)}{(\log x)^B}\right)$ where $B = 100(\log 100 - 1)$. Now we can write

$$S_2' = \sum_{p \le x} \sum_{\substack{q_i^{\alpha_i} || p+a \\ q_j^{\alpha_j} || p+a \\ q_i^{\alpha_i} \neq q_j^{\alpha_j} > y}} \Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j})) = S_{2,1}' + S_{2,2}'$$

where

$$S_{2,1}' = \sum_{p \le x} \sum_{\substack{q_i^{\alpha_i} || p+a \\ q_j^{\alpha_j} || p+a \\ q_i^{\alpha_i} \neq q_j^{\alpha_j} > y \\ \Omega(\tau(q_i^{\alpha_i})), \Omega(\tau(q_j^{\alpha_j})) < 100 \log\log x}} \Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j}))$$

and

$$S_{2,2}' = \sum_{p \le x} \sum_{\substack{q_i^{\alpha_i} || p+a \\ q_j^{\alpha_j} || p+a \\ q_i^{\alpha_i} \neq q_j^{\alpha_j} > y \\ \Omega(\tau(q_i^{\alpha_i})), \Omega(\tau(q_j^{\alpha_j})) > 100 \log\log x}} \Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j})).$$

Now, as before,

$$\begin{aligned} S'_{2,1} &= O\left((\log\log x)^2 \sum_{p\le x} \sum_{\substack{q_i^{\alpha_i}||p+a \\ q_j^{\alpha_j}||p+a \\ q_i^{\alpha_i}\neq q_j^{\alpha_j}>y}} 1 \right) \\ &= O\left(\pi(x)(\log\log x)^2\right) \end{aligned}$$

because there are only finitely many such q^α. Thus,

$$S'_2 = S'_{2,2} + O\left(\pi(x)(\log\log x)^2\right).$$

Now, we can write

$$S'_{2,2} = \sum_{p\le x}{}' \sum_{\substack{q_i^{\alpha_i}||p+a \\ q_j^{\alpha_j}||p+a \\ q_i^{\alpha_i}\neq q_j^{\alpha_j}>y \\ \Omega(\tau(q_i^{\alpha_i})),\Omega(\tau(q_j^{\alpha_j}))>100\log\log x}} \Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j})) + O\left(\pi(x)(\log\log x)^2\right).$$

Here, $\sum'_p$ denotes sum over $p \le x$ such that $p+a$ is not prime, because if $p+a$ is a prime, then

$$\sum_{p\le x} \Omega^2(\tau(p+a)) \ll \sum_{\substack{l\le x \\ l \text{ prime}}} \Omega^2(\tau(l)) = O(\pi(x)(\log\log x)^2).$$

Thus we get

$$S'_{2,2} = \sum_{p\le x}{}' \sum_{\substack{q_i^{\alpha_i}, q_j^{\alpha_j} | p+a \\ q_i^{\alpha_i} q_j^{\alpha_j} > y \\ \Omega(\tau(q_i^{\alpha_i})), \Omega(\tau(q_j^{\alpha_j})) > 100 \log\log x}} \Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j})) + O(\pi(x)(\log\log x)^2)$$

$$\ll \sum_{\substack{y < q_i^{\alpha_i} q_j^{\alpha_j} < x/4 \\ \Omega(\tau(q_i^{\alpha_i})), \Omega(\tau(q_j^{\alpha_j})) > 100 \log\log x}} \Omega_z(\tau(q_i^{\alpha_i}))\Omega_z(\tau(q_j^{\alpha_j})) \sum_{\substack{p\le x \\ q_i^{\alpha_i}, q_j^{\alpha_j} | p+a}} 1 + O(\pi(x)(\log\log x)^2).$$

This is because if $q_i^{\alpha_i} q_j^{\alpha_j} > x/4$, and $q_i^{\alpha_i} q_j^{\alpha_j} | p+a$, then $1 < \dfrac{p+a}{q_i^{\alpha_i} q_j^{\alpha_j}} < 4$ has only finitely many choices, and since τ is a multiplicative function and Ω is completely additive, $S'_{2,2}$ gets changed by a constant. Thus, $S'_{2,2}$ is bounded above by

$$\sum_{\substack{y < q_i^{\alpha_i} q_j^{\alpha_j} < x/4 \\ \Omega(\tau(q_i^{\alpha_i})), \Omega(\tau(q_j^{\alpha_j})) > 100 \log\log x}} \Omega_z(\tau(q_i^{\alpha_i}))\Omega(\tau(q_j^{\alpha_j}))\pi(x; q_i^{\alpha_i} q_j^{\alpha_j}, -a) + O(\pi(x)(\log\log x)^2).$$

By the Brun-Titchmarsh theorem, this has an upper bound of

$$\ll \sum_{\substack{y < q_i^{\alpha_i} q_j^{\alpha_j} < x/4 \\ \Omega(\tau(q_i^{\alpha_i})), \Omega(\tau(q_j^{\alpha_j})) > 100 \log\log x}} \frac{\Omega_z(\tau(q_i^{\alpha_i}))\Omega(\tau(q_j^{\alpha_j}))x}{q_i^{\alpha_i} q_j^{\alpha_j} \log(x/q_i^{\alpha_i} q_j^{\alpha_j})}$$

$$= x \left(\sum_{\substack{y < q_i q_j < x/4 \\ \Omega(\tau(q_i)), \Omega(\tau(q_j)) > 100 \log\log x}} \frac{\Omega_z(\tau(q_i))\Omega(\tau(q_j))}{q_i q_j \log(x/q_i q_j)} + O(\pi(x)) \right),$$

where the last equality follows because the sum over $q_i^{\alpha_i} q_j^{\alpha_j}$ where $\alpha_i, \alpha_j \ge 2$ is

convergent. Now as before, divide the sum into dyadic subintervals. Without loss of generality, choose $y = 2^{\alpha}$, $x/4 = 2^{\beta+1}$ for some α, $\beta > 0$ and $\alpha \leq \beta + 1$. Then, the sum is bounded by

$$O\left(\frac{\pi(x)}{\log x}\right).$$

Thus, the assertion in the lemma follows.

□

Proof of Theorem 4.4.2 : To see this, we unfold the square on the left hand side to get

$$\sum_{\substack{p\leq x \\ \tau(p+a)\neq 0}} \left\{\Omega^2(\tau(p+a)) + \frac{1}{4}\,(\log\log x)^4 - 2.\frac{1}{2}(\log\log x)^2\Omega(\tau(p+a))\right\}.$$

Now applying Lemma 4.4.1 and Lemma 4.4.3, the assertion of the theorem follows.

As we mentioned earlier, $\tau(n)$ is just a prototype. In general, let $H(z)$ be a normalized cuspidal newform of even weight $w \geq 2$ for $\Gamma_0(N)$ without complex multiplication, Then its Fourier coefficients $a_H(n)$ are multiplicative by (4.2.4). Also, by estimates of Hecke,

$$|a_H(n)| \leq n^{\frac{1}{2}(w+1)}. \tag{4.4.4}$$

In all the proofs above, we can use (4.2.4) and (4.4.4) in place of (4.1.1) and (4.1.2), to show the following.

Theorem 4.4.4. *Let H satisfy*

1. *H is a normalized cuspidal new form with a Fourier expansion*

$$H = \sum_{n\geq 1} a_H(n)e^{2\pi inz},\ 0 \neq a_H(n) \in \mathbf{Z},$$

2. *H does not have complex multiplication.*

Suppose also the generalised Riemann hypothesis is true for all Artin L-functions. Then, for any $a \neq 0$, $a \in \mathbb{Z}$

$$\sum_{\substack{p\leq x \\ a_H(p+a)\neq 0}} \left(\Omega(a_H(p+a)) - \frac{1}{2}(\log\log x)^2\right)^2 = \pi(x)\frac{(\log\log x)^3}{3} + o(\pi(x)(\log\log x)^3);$$

which implies, $\Omega(a_H(p+a))$ *has normal order* $\dfrac{(\log\log p)^2}{2}$.

4.5 Erdős-Kac type result for $\Omega(\tau(p+a))$

In this section, in the spirit of Murty and Murty, we find the distribution function associated to $\Omega(\tau(p+a))$. As in the previous chapter, we use Barban, Levin and Vinogradov's 1965 result to achieve this. For clarity of exposition, we mention the theorem here once more. For a strongly additive function $g(n)$, for positive real x,

$$A(x) = \sum_{p\leq x} \frac{g(p)}{p},$$

and

$$B(x) = \left(\sum_{p\leq x} \frac{g^2(p)}{p}\right)^{1/2} \geq 0.$$

Theorem 4.5.1 (Barban, Vinogradov, Levin, 1965)**.** *Let $g(n)$ be a strongly additive function. Then,*

$$\lim_{x\to\infty}\frac{1}{\pi(x)}|\{p\le x; g(p+1)\le A(x)+zB(x)\}|$$

converges weakly to a limiting distribution as $x\to\infty$, if and only if there is a distribution function $K(u)$ such that as $x\to\infty$,

$$\frac{1}{B^2(x)}\sum_{\substack{p\le x\\ g(p)\le uB(x)}}\frac{g^2(p)}{p}\to K(u).$$

When this condition is satisfied, the characteristic function $\alpha(t)$ of the limit law will be given by Kolmogorov's formula

$$\log\alpha(t)=\int_{-\infty}^{\infty}(e^{itu}-1-itu)u^{-2}dK(u)$$

and the limit law will have mean 0 and variance 1. In the special case, in order that

$$\lim_{x\to\infty}\frac{1}{\pi(x)}|\{p\le x; g(p+1)\le A(x)+zB(x)\}|=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z}e^{-t^2/2}dt,$$

it is sufficient that for each fixed $\epsilon>0$, as $x\to\infty$

$$\frac{1}{B^2(x)}\sum_{\substack{p\le x\\ |g(p)|>\epsilon B(x)}}\frac{g^2(p)}{p}\to 0.$$

The statement is valid when $p+1$ is replaced by $p+a$, for some fixed non-zero integer a.

Consider the function $h(n)=\sum_{q|n}\Omega(\tau(q))$, where the sum is over distinct

prime divisors q of n. This is strongly additive and hence we can apply Theorem 4.5.1 to it. In [39], Murty and Murty showed that

$$A(x) = \sum_{p \leq x} \frac{h(p)}{p} = \frac{1}{2}(\log\log x)^2 + O(\log\log x)$$

and

$$B(x) = \left(\sum_{p \leq x} \frac{h^2(p)}{p} \right)^{1/2} = \frac{1}{\sqrt{3}}(\log\log x)^{3/2} + O(\log\log x).$$

They also check that for each fixed $\epsilon > 0$,

$$\sum_{\substack{p \leq x \\ \Omega(\tau(p)) \geq \epsilon B(x)}} \frac{\Omega^2(\tau(p))}{p} = o(B^2(x)).$$

Hence, a direct application of Theorem 4.5.1 shows that for any non-zero integer a,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \left| \left\{ p \leq x; \frac{h(p+a) - \frac{1}{2}(\log\log x)^2}{(\log\log x)^{3/2}} \leq \frac{\alpha}{\sqrt{3}} \right\} \right| = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2} dt.$$

Now we want to prove that $\Omega(\tau(p+a))$ is normally distributed. This can be established if we can show that

$$\Omega(\tau(p+a)) - h(p+a) = o((\log\log x)^{3/2})$$

for all but $o(x)$ many primes $p \leq x$. We state the following lemma without proof, as the proof is exactly same as that for the Euler phi function in Lemma 3.5.3.

Lemma 4.5.2. *For any non-zero integer a,*

$$D(x) := \sum_{p \leq x} (\Omega(\tau(p+a)) - h(p+a))^2 = O(\pi(x)).$$

Using this key lemma, we can thus show that $\Omega(\tau(p+a))$ follows the normal distribution.

Theorem 4.5.3. *For any non-zero integer a, assuming the generalised Riemann hypothesis for all Artin L-functions, we have*

$$\lim_{x \to \infty} \frac{1}{\pi(x)} | \left\{ p \leq x; \frac{\Omega(\tau(p+a)) - \frac{1}{2}(\log\log x)^2}{(\log\log x)^{3/2}} \leq \frac{\alpha}{\sqrt{3}} \right\} | = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2} dt.$$

In other words, $\Omega(\tau(p+a))$, under suitable normalisation, is "normally distributed".

Proof. According to our discussion earlier, it is sufficient to show that

$$\Omega(\tau(p+a)) - h(p+a) = o((\log\log x)^{3/2})$$

for all but $o(x)$ many primes $p \leq x$. Indeed, if $p \leq x$ does not satisfy the above equality, then a summand coming from p in $D(x)$ in Lemma 4.5.2 satisfies

$$|\Omega(\tau(p+a)) - h(p+a)| \geq (\log\log x)^{3/2}.$$

Lemma 4.5.2 and Theorem 4.4.2 implies that the number of such $p \leq x$ is $O\left(\frac{\pi(x)}{(\log\log x)^3}\right)$ $= o(x)$. □

Of course, as before $\tau(n)$ is a prototype. The result holds true for any integer fourier coefficients $a_H(n)$ of normalized cuspidal newform of even weight $w \geq 2$

for $\Gamma_0(N)$ without complex multiplication.

4.6 Further generalisation

The results in this chapter and the previous can be generalised further. The Euler totient function, integer Fourier coefficients of Hecke eigen forms, all fall under the umbrella of a larger class of functions. As in [38], we can define a class of functions $\mathcal{F}$ and then the results in this chapter generalise to functions $f(n)$ in $\mathcal{F}$.

Let f be a non-zero multiplicative function such that for $n \in \mathbb{N}$, $f(n) \in \mathbb{Z}$, $f(n) \neq 0$. We say $f \in \mathcal{F}$ if:

- (H0) For some $\beta > 0$, $|f(n)| \leq n^{\beta}$ for all n.
- (H1) Denote $\pi_f(x;d) := |\{p \leq x : f(p) \equiv 0 (\text{mod } d)\}|$. Suppose there exists a function $\delta(d)$ such that for any $\theta > 0$, $\sum_{d \leq x^{\theta}} |\pi_f(x;d) - \delta(d)\pi(x)| \ll \frac{x}{(\log x)^{1+\gamma}}$ for some $\gamma > 0$, and some $\theta > 0$.
- (H2) For prime powers p^{α}, q^{β}, $(p \neq q)$,

$$\delta(p^{\alpha}) = p^{-\alpha}\left(1 + O(p^{-1})\right)$$

and

$$\delta(p^{\alpha}q^{\beta}) = p^{-\alpha}q^{-\beta}\left(1 + O\left(\frac{1}{p} + \frac{1}{q}\right)\right)$$

where the implied constants are absolute.

- (H1)' Denote $\pi_f^*(x,d) := \sum_{\substack{p\leq x \\ f(p)\equiv 0(d)}} \log p$. Then

$$\pi_f^*(x,d) - \delta(d)x = O(x^{1/2+\theta}d^{\gamma}) \text{ for some } \theta < 1/2,\ \gamma > 0.$$

Any multiplicative function f is said to belong to $\mathcal{F}$ if it satisfies (H0), (H1), (H2), (H1)'.

As shown in [38], using the theory of ℓ -adic representations, it can be shown that the Ramanujan τ function and more generally, Fourier coefficients of normalised Hecke eigenforms, whenever they are non-zero, satisfy the properties (H0), (H1) and (H2), under a quasi-GRH.

Chapter 5

Moments of Sums of Characters

Analytic number theory, in the modern sense, is said to begin with the work of Dirichlet. Modifying Euler's well-known analytic proof that there are infinitely many primes, Dirichlet's idea was to generalise Euler's formula

$$\prod_p \left(1 - p^{-s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}, \tag{5.0.1}$$

valid for $\mathrm{Re}(s) > 1$. He introduced characters, now bearing his name, to prove that any arithmetic progression $a + nq$, $n = 0, 1, 2, \ldots$, where a and q are relatively prime, contains infinitely many prime numbers. Ever since, these characters and their associated $L-$functions have been studied extensively.

By definition, a Dirichlet character modulo d is a group homomorphism

$$\chi : (\mathbb{Z}/d\mathbb{Z})^* \to \mathbb{C}^*.$$

One extends χ to all of $\mathbb{Z}$ by setting $\chi(n) = 0$ for any integer n not coprime to

d. This is a periodic function, whose values are the $\phi(d)$-th roots of unity. The trivial (or principal) character modulo d, denoted χ_0, is defined by $\chi_0(n) = 1$ for all n coprime to d. A character is called principal if it assumes the value 1 for arguments coprime to its modulus and otherwise is 0. A character is called real if it assumes real values only. A character which is not real is called complex.

In the theory of applications of Dirichlet characters, other important concepts are the conductor of a character and primitive characters. Let $\chi(n)$ be an arbitrary non-principal character modulo k. If, for values of n such that $\gcd(n,k) = 1$, the number k is the smallest period of χ, then k is the conductor of the character χ and χ is called a primitive character (mod k). Otherwise, there exists an unique $k_1 > 1$, $k_1 < k$, $k_1|k$ and a primitive character $\chi_1(\text{mod } k_1)$ such that

$$\chi(n) = \begin{cases} \chi_1(n) & \text{if } (n,k) = 1 \\ 0 & \text{if } (n,k) \neq 1. \end{cases}$$

Then $\chi(\text{mod } k)$ is called an imprimitive character of $\chi_1(\text{mod } k_1)$ and we say χ_1 induces χ.

For an odd prime p, the symbol $\left(\frac{a}{p}\right)$ is simply the usual Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a(\text{mod } p) \text{ for some } x \in (\mathbb{Z}/d\mathbb{Z})^*, p \nmid a \\ -1 & \text{if } x^2 \not\equiv a(\text{mod } p) \text{ for all } x \in (\mathbb{Z}/d\mathbb{Z})^*, p \nmid a \\ 0 & \text{if } a \equiv 0(\text{mod } p). \end{cases}$$

The Legendre symbol $\left(\frac{a}{p}\right)$ as a function of a, is a Dirichlet character (mod p). Its

special values are

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{5.0.2}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{5.0.3}$$

If p and q are distinct primes, then the quadratic reciprocity law states that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}. \tag{5.0.4}$$

For an odd prime integer P, which has prime factorisation, say, $P = \prod_{p_r} p_r^{a_r}$, the Jacobi symbol is defined as

$$\left(\frac{a}{P}\right) = \prod_{p_r}\left(\frac{a}{p_r}\right)^{a_r}$$

where $\left(\frac{a}{1}\right) = 1$. The Jacobi symbol $\left(\frac{a}{P}\right)$ is a Dirichlet character (mod P). Both (5.0.2) and (5.0.3) are valid with p replaced by P. The reciprocity law (5.0.4) holds if p, q are replaced by any two relatively prime odd integers P, Q.

A Gaussian sum $\tau(\chi)$ related to the character χ modulo n is the exponential sum

$$\tau_k(\chi) = \sum_{a(\mathrm{mod}\ n)} \chi(a) e\left(\frac{ak}{n}\right) \tag{5.0.5}$$

for $k \in \mathbb{Z}$, $e(z) = e^{2\pi i z}$. If $\gcd(k, n) = 1$, then

$$\tau_k(\chi) = \chi(k)\tau(\chi),$$

where

$$\tau(\chi) = \tau_1(\chi) = \sum_{a(\mathrm{mod}\ n)} \chi(a) e\left(\frac{a}{n}\right).$$

Actually, in 1801, Gauss introduced the quadratic character sum

$$\sum_{a=1}^{n-1} e\left(\frac{ka^2}{n}\right)$$

which coincides with the sum $\tau_k(\chi)$ if χ is a real character, n odd square-free integer and $\gcd(n,k) = 1$. (see [37]) Here the character is defined by the Jacobi symbol $\left(\frac{a}{n}\right)$ and it is easy to show that

$$\tau(\chi) = \begin{cases} \pm\sqrt{n} & \text{if } n \equiv 1 \pmod 4 \\ \pm i\sqrt{n} & \text{if } n \equiv 3 \pmod 4 \end{cases}$$

The sign is not so easy to decide. Even Gauss needed several years before in 1805, he was able to prove that the sign is always positive.

Dirichlet ([15], [16]) proved his famous theorem on primes in arithmetic progressions in 1837 by studying the series

$$L(s,\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s}$$

where χ is a character modulo n. The series known as the Dirichlet L-function is absolutely convergent in the half plane $\sigma > 1$, where it has the Euler product

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

The Euler product formula shows that the L-function has no zeroes if $\mathrm{Re}(s) > 1$. Therefore, there are no zeroes in the plane $\mathrm{Re}(s) < 0$ either, except the trivial zeroes. It is known that there are no zeroes on the line $\mathrm{Re}(s) = 1$ and the generalised Riemann hypothesis (GRH) asserts that there are no zeroes with real part $\mathrm{Re}(s) > \frac{1}{2}$. Therefore all non trivial zeroes should lie on the line $\mathrm{Re}(s) = \frac{1}{2}$. However, like for the Riemann zeta function, only a certain zero free region is known.

A central question in analytic number theory is to understand the behaviour of the character sums

$$\sum_{n<Y} \chi(n)$$

where χ is a non-principal real character modulo q. Since characters are periodic functions, it is easy to show that this sum is always $\leq |q|$ in absolute value, that is

$$|\sum_{n=M+1}^{N} \chi(n)| \leq |q|$$

for any positive integers M and N. However a sharper bound is desirable. Around 1918, Pólya and Vinogradov, independently, improved the upper bound to $O\left(\sqrt{|q|}\log q\right)$.

Theorem 5.0.1 (Pólya, Vinogradov, 1918)**.** *For any non-principal character modulo q,*

$$|\sum_{n=M+1}^{N} \chi(n)| \ll O\left(\sqrt{|q|}\log q\right).$$

This is popularly known as the Pólya-Vinogradov inequality. The proof of this follows easily using Gauss sums. We refer the reader to p. 345 of [37] to see a complete proof.

Paley [41] has shown, in 1932, that there exist character sums of size $\sqrt{|q|\log\log|q|}$.

For short character sums, Burgess [8] has shown some better estimates, but albeit plenty of work has been done, the classical upper bound of Pólya and Vinogradov is still the best known in general. We know that this powerful inequality plays a key role in the proofs of multiple big theorems including the celebrated Bombieri-Vinogradov theorem, which we saw helped us establish the main results in Chapter 3 and 4.

Another direction in which one can study these characters is by considering the sums of all Dirichlet characters modulo n. In particular, consider the classical quadratic sum of the form

$$\sum_{x<p<2x} \left(\frac{n}{p}\right)$$

where the sum is over primes p and n is a fixed number. One expects on the Generalised Riemann Hypothesis

$$\sum_{x<p<2x} \left(\frac{n}{p}\right) \ll O(x^{1/2} \log nx)$$

when we fix n and average over primes p. This is where we bring in the perspective of probability theory. We want to view the Legendre symbol $\left(\frac{n}{\cdot}\right)$ and later Dirichlet characters as "random variables" so that the above sum can be viewed as sum over random variables. In [40], Murty and Prabhu use this poetic insight to prove some averaged central limit theorems (under suitable growth conditions) for sums of quadratic characters by the method of moments approach. The following theorem of Heilbronn [28] will be at the heart of this chapter.

Theorem 5.0.2 (Heilbronn, 1958)**.** *Let p and q denote odd primes. Let $\left(\frac{p}{q}\right)$ denote the*

Legendre symbol. Then for $x \geq 2$,

$$\sum_{p \leq x} \sum_{q \leq x} \left(\frac{p}{q}\right) = O(x^{7/4}(\log x)^{-5/4}).$$

We will use this key theorem at the centre and instead prove results on size of exceptional sets. Since GRH predicts the sums of these characters to be $O\left(x^{1/2+\epsilon}\right)$, we will see how to estimate the size of the set where the sums are bigger than the expected value.

Theorem 5.0.2 can be generalised to Hecke characters of a general number field.

Theorem 5.0.3 (Heilbronn, 1958)**.** *Let K be an algebraic number field of degree k and discriminant D. Let $\chi_1, \chi_2, \cdots, \chi_N$ be N distinct abelian characters in K with moduli whose norms do not exceed m. Let g be a natural integer, $x > 1$, Then*

$$\sum_{n=1}^{N} \sum_{N(\mathfrak{p}) \leq x} \chi_n(\mathfrak{p}) = O\left(N^{1-\frac{1}{4g}} x^{1+\epsilon} + Nx(x^{-g}|D|^{\frac{1}{2}}m)^{\frac{1}{g(k+2)}+\epsilon}\right)$$

where $\mathfrak{p}$ is restricted to prime ideals in K and the constants implied by the symbol O depends on k, g and ϵ only.

An immediate corollary to this is a similar statement for Dirichlet characters.

Corollary 5.0.4. *Let $\chi_1, \chi_2, \cdots, \chi_N$ be N distinct Dirichlet characters with moduli not exceeding m. Let g be a natural integer, $x > 1$. Then, for any g,*

$$\sum_{n=1}^{N} \sum_{p \leq x} \chi_n(p) = O\left(N^{1-\frac{1}{4g}} x + Nx^{\frac{1}{2}}(m \log m)^{\frac{1}{2g}}\right)$$

where p is restricted to primes and the constant implied by the O symbol depends on g only.

Just like the Legendre symbols, GRH also predicts

$$\sum_{x<N(\mathfrak{p})<2x} \chi_n(\mathfrak{p}) \ll O(x^{1/2}\log nx) \tag{5.0.6}$$

We will use Heilbronn's idea from Theorem 5.0.3 and prove an upper bound on the size of the exceptional set of primes where the sum in 5.0.6 is different from its expected bound.

5.1 Result of Heilbronn Revisited

We reproduce the original proof of Theorem 5.0.2 here for the sake of clarity, and with a view to a generalization needed for our discussion. A critical application of the Polya-Vinogradov inequality (Theorem 5.0.1) is the central idea in Heilbronn's theorem. Another result which plays a major role is the most ubiquitous of inequalities in mathematics, the Cauchy-Schwarz inequality. First discovered by Cauchy in the year 1821, it states that if $a_1, \cdots, a_n$ and $b_1, \cdots, b_n$ are arbitrary real numbers, then

$$\Big|\sum_{j=1}^{n} a_j b_j\Big| \leq \left(\sum_{j=1}^{n} |a_j|^2\right)^{1/2} \left(\sum_{j=1}^{n} |b_j|^2\right)^{1/2} \tag{5.1.1}$$

with equality arising if and only if there is a $\lambda \in \mathbb{R}$ such that $a_j = \lambda b_j$ for $j = 1, 2, \cdots, n$.

Let us begin walking over the main idea of the proof of Heilbronn's theorem (Theorem 5.0.2). We consider the square of the double sum, that is,

$$\left[\sum_{p\leq x}\sum_{q\leq y}\left(\frac{p}{q}\right)\right]^2.$$

Applying the Cauchy Schwarz inequality, this is

$$\begin{aligned}&\leq \pi(y) \sum_{q\leq y} \left(\sum_{p\leq x} \left(\frac{p}{q}\right)\right)^2 \\ &= \pi(y) \sum_{q\leq y} \sum_{p_1\leq x} \sum_{p_2\leq x} \left(\frac{p_1p_2}{q}\right)\end{aligned}$$

Squaring again and applying the Cauchy-Schwarz inequality, we get

$$\begin{aligned}\left[\sum_{p\leq x}\sum_{q\leq y}\left(\frac{p}{q}\right)\right]^4 &\leq \pi^2(y) \sum_{\substack{p_1\leq x\\ p_2\leq x}} 1^2 \sum_{\substack{p_1\leq x\\ p_2\leq x}} \left(\sum_{q\leq y} \left(\frac{p_1p_2}{q}\right)\right)^2 \\ &\leq \pi^2(y)\pi^2(x) 2 \sum_{n\leq x^2} \sum_{\substack{q_1\leq y\\ q_2\leq y}} \left(\frac{n}{q_1}\right)\left(\frac{n}{q_2}\right) \\ &= 2\pi^2(y)\pi^2(x) \sum_{\substack{q_1\leq y\\ q_2\leq y\\ q_1=q_2}} \sum_{n\leq x^2} \left(\frac{n}{q_1q_2}\right) + 2\pi^2(y)\pi^2(x) \sum_{\substack{q_1\leq y\\ q_2\leq y\\ q_1\neq q_2}} \sum_{n\leq x^2} \left(\frac{n}{q_1q_2}\right)\end{aligned}$$

Using the Polya-Vinogradov inequality on the second term, we see that that the upper bound is

$$2\pi^3(y)\pi^2(x)x^2 + O(\pi^4(y)\pi^2(x)y\log y).$$

Setting $y = x$, and taking fourth roots on both sides of the inequality, we get Heilbronn's bound.

An essential ingredient in the proof of Theorem 5.0.3 is the following straightforward generalization of the Pólya Vinogradov inequality to algebraic number fields.

Lemma 5.1.1. *Let K be an algebraic number field of discriminant D, degree k. Let $\chi(\mathfrak{a})$ be an abelian non-principal character defined in K to a modulus $\mathfrak{m}$. Let $m = N(\mathfrak{m})$. Then*

for $x > 1, \epsilon > 0$,

$$\sum_{N(\mathfrak{a}) \leq x} \chi(\mathfrak{a}) = O\left(x^k |D| m\right)^{\frac{1}{k+2}+\epsilon}$$

where the implied constants depend on k and ϵ only.

For a proof, see [28]. Another important component of the proof of Theorem 5.0.3 is Holder's inequality.

Lemma 5.1.2 (Holder's inequality)**.** *Let $\frac{1}{p} + \frac{1}{q} = 1$ for $p, q > 1$. Then for $a_i, b_i \in \mathbf{R}$, for all $1 \leq i \leq n$,*

$$\sum_{k=1}^{n} |a_k b_k| \leq \left(\sum_{k=1}^{n} |a_k|^p\right)^{1/p} \left(\sum_{k=1}^{n} |b_k|^q\right)^{1/q}$$

with equality if and only if $|b_k| = c|a_k|^{p-1}$.

To keep the chapter self-contained and since Heilbronn's arguments form the framework in this chapter, we show the proof of Theorem 5.0.3.

Proof of Theorem 5.0.3 Applying Holder's inequality for $\frac{1}{q} = \frac{1}{2g}$, $a_k = 1$ and $b_k = \chi_k(\mathfrak{p})$ for $1 \leq k \leq N$, we get,

$$\begin{aligned} |\sum_{n=1}^{N} 1 \sum_{N(\mathfrak{p}) \leq x} \chi_n(\mathfrak{p})| &\leq \left(\sum_{n=1}^{N} |1|\right)^{1-\frac{1}{2g}} \left(\sum_{n=1}^{N} |\sum_{\mathfrak{p}} \chi_n(\mathfrak{p})|^{2g}\right)^{\frac{1}{2g}} \\ &= N^{1-\frac{1}{2g}} \left(\sum_{n=1}^{N} \left(\sum_{\mathfrak{a}} c(\mathfrak{a}) \chi_n(\mathfrak{a}) \sum_{\mathfrak{b}} c(\mathfrak{b}) \chi_n(\mathfrak{b})\right)\right)^{\frac{1}{2g}} \end{aligned}$$

where $0 \leq c(\mathfrak{a}) \leq g!$ denotes the number of ways $\mathfrak{a}$ can be written as a product of prime ideals. Again, by the Cauchy-Schwarz inequality with respect to the sum

over $\mathfrak{a}$ and $\mathfrak{b}$,

$$\begin{aligned}|\sum_{n=1}^{N}\sum_{N(\mathfrak{p})\leq x}\chi_n(\mathfrak{p})| &\leq N^{1-\frac{1}{2g}}\left(\sum_{\mathfrak{a}}c^2(\mathfrak{a})\sum_{\mathfrak{b}}c^2(\mathfrak{b})\right)^{\frac{1}{4g}}\left(\sum_{\mathfrak{a}}\sum_{\mathfrak{b}}|\sum_{n=1}^{N}\chi_n(\mathfrak{a})\bar{\chi}_n(\mathfrak{b})|^2\right)^{\frac{1}{4g}}\\ &\leq N^{1-\frac{1}{2g}}O\left(x^{\frac{1}{2}+\epsilon}\right)\left(\sum_{n_1=1}^{N}\sum_{n_2=1}^{N}\sum_{\mathfrak{a}}\sum_{\mathfrak{b}}\chi_{n_1}(\mathfrak{a})\bar{\chi}_{n_1}(\mathfrak{b})\chi_{n_2}(\mathfrak{a})\bar{\chi}_{n_2}(\mathfrak{b})\right)^{\frac{1}{4g}}\\ &= N^{1-\frac{1}{2g}}O\left(x^{\frac{1}{2}+\epsilon}\right)\left(\sum_{n_1=1}^{N}\sum_{n_2=1}^{N}|\sum_{\mathfrak{a}}\chi_{n_1}(\mathfrak{a})\bar{\chi}_{n_2}(\mathfrak{a})|^2\right)^{\frac{1}{4g}}\end{aligned}$$

Here the sums with respect to $\mathfrak{a}$ are $O(x^{g+\frac{1}{2}\epsilon})$. Using this result if $n_1 = n_2$, we obtain

$$|\sum_{n=1}^{N}\sum_{N(\mathfrak{p})\leq x}\chi_n(\mathfrak{p})| \leq N^{1-\frac{1}{4g}}O(x^{1+\epsilon}) + N^{1-\frac{1}{2g}}O\left(x^{\frac{1}{2}+\epsilon}\right)\left(\sum_{n_1=1}^{N}\sum_{n_2=1}^{N}|\sum_{\mathfrak{a}}\chi_{n_1}(\mathfrak{a})\bar{\chi}_{n_2}(\mathfrak{a})|^2\right)^{\frac{1}{4g}}$$

Here the sum over $\mathfrak{a}$ is $O\left(x^{gk}|D|m^2\right)^{\frac{1}{k+2}+\epsilon}$ by Lemma 5.1.1. □

5.2 Sums over product of characters - a generalisation of Heilbronn's arguments

In this section, we now adapt Heilbronn's approximation technique to estimate the following sums

$$\sum_{p\leq x}\sum_{q_1\leq y}\sum_{q_2\leq y}\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)$$

and

$$\sum_{n_1\leq N}\sum_{n_2\leq N}\sum_{N(\mathfrak{p})\leq x}\chi_{n_1}(\mathfrak{p})\chi_{n_2}(\mathfrak{p})$$

where in the first sum $\left(\frac{p}{q}\right)$ denotes the Legendre symbol and in the second sum $\chi_n(\mathfrak{p})$ denotes an abelian character of an algebraic number field K. We prove the following theorems.

Theorem 5.2.1. *Let $\left(\frac{p}{q}\right)$ denote the Legendre symbol. For any $x > 0$,*

$$\Big| \sum_{p\leq x} \sum_{q_1\leq x} \sum_{q_2\leq x} \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right) \Big| \leq x^2(\log x)^{-5/4}.$$

Proof. We start by considering

$$\sum_{p\leq x} \sum_{q_1\leq y} \sum_{q_2\leq y} \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right).$$

Taking 4th powers and first applying the Cauchy-Schwarz inequality, we see that

$$\begin{aligned}\left(\sum_{p\leq x} \sum_{q_1\leq y} \sum_{q_2\leq y} \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\right)^4 &\leq \left(\sum_{p\leq x} 1^2\right)^2 \left(\sum_{p\leq x}\left(\sum_{q_1\leq y}\sum_{q_2\leq y}\left(\frac{p}{q_1q_2}\right)\right)^2\right)^2 \\ &= \pi^2(x)\left(\sum_{p\leq x}\left(\sum_{q_1,q_2,q_3,q_4\leq y}\left(\frac{p}{q_1q_2q_3q_4}\right)\right)\right)^2 \\ &\leq \pi^2(x)\left(\sum_{n\leq x}\left(\sum_{q_1,q_2,q_3,q_4\leq y}\left(\frac{n}{q_1q_2q_3q_4}\right)\right)\right)^2\end{aligned}$$

In the last equality we expand the outer sum to run over all integers $n \leq x$ instead of just primes $p \leq x$. Unwrapping the outer square we get

$$\left(\sum_{p\leq x} \sum_{q_1\leq y} \sum_{q_2\leq y} \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\right)^4 \leq \pi^2(x) \sum_{n_1\leq x}\sum_{n_2\leq x}\sum_{q_1,q_2,q_3,q_4\leq y}\left(\frac{n_1n_2}{q_1q_2q_3q_4}\right)$$

Writing $n_1 n_2 = m$, we get the upper bound to be

$$= 2\pi^2(x) \sum_{m \leq x^2} \sum_{\substack{q_i \leq y \\ 1 \leq i \leq 4 \\ \prod_i q_i = \text{square}}} \left(\frac{n}{q_1 q_2 q_3 q_4} \right) + 2\pi^2(x) \sum_{m \leq x^2} \sum_{\substack{q_i \leq y \\ 1 \leq i \leq 4 \\ \prod_i q_i \neq \text{square}}} \left(\frac{n}{q_1 q_2 q_3 q_4} \right).$$

Again applying the Polya-Vinogradov inequality (Theorem 5.0.1) on the second term, we get an upper bound of

$$2\pi^2(x) x^2 (\pi(y))^2 + 2\pi^2(x) y^2 \log(y^4) \pi^4(y).$$

Setting $x = y$ and taking 4-th roots, we get

$$\Big| \sum_{p \leq x} \sum_{q_1 \leq x} \sum_{q_2 \leq x} \left(\frac{p}{q_1} \right) \left(\frac{p}{q_2} \right) \Big| \leq x^2 (\log x)^{-5/4}. \tag{5.2.1}$$

□

Next, we generalise Theorem 5.0.3 to obtain the following result.

Theorem 5.2.2. *Let K be an algebraic number field of degree k and discriminant D. Let $\chi_1, \chi_2, \cdots, \chi_N$ be N distinct abelian characters in K with moduli whose norms do not exceed m. Let g be a natural integer, $x > 1$. Then, for any $\delta > 0$,*

$$\sum_{n_1 \leq N} \sum_{n_2 \leq N} \sum_{N(\mathfrak{p}) \leq x} \chi_{n_1}(\mathfrak{p}) \chi_{n_2}(\mathfrak{p}) \leq O\left(N^{2 - \frac{1-\delta}{2g}} x^{1 + \frac{\epsilon}{4g}} + N^{2 - \frac{1}{g}} x^{\frac{1}{2} + \epsilon} \left(x^k |D| m \right)^{\frac{1}{2g}\left(\frac{1}{k+2} + \epsilon\right)} \right)$$

where the implied constants only depend on k, g and ϵ.

Proof. We start by considering

$$\sum_{n_1\leq N}\sum_{n_2\leq N}\sum_{N(\mathfrak{p})\leq x}\chi_{n_1}(\mathfrak{p})\chi_{n_2}(\mathfrak{p}).$$

By Holder's inequality with $q=2g$,

$$\begin{aligned}|\sum_{n_1\leq N}\sum_{n_2\leq N}\sum_{N(\mathfrak{p})\leq x}\chi_{n_1}(\mathfrak{p})\chi_{n_2}(\mathfrak{p})| &\leq \left(\sum_{n_1\leq N}\sum_{n_2\leq N}1\right)^{1-\frac{1}{2g}}\left(\sum_{n_1\leq N}\sum_{n_2\leq N}|\sum_{\mathfrak{p}}\chi_{n_1n_2}(\mathfrak{p})|^{2g}\right)^{\frac{1}{2g}}\\ &= (N^2)^{1-\frac{1}{2g}}\left(\sum_{n_1,n_2\leq N}\left(\sum_{\mathfrak{a}}c(\mathfrak{a})\chi_{n_1n_2}(\mathfrak{a})\sum_{\mathfrak{b}}c(\mathfrak{b})\bar{\chi}_{n_1n_2}(\mathfrak{b})\right)\right)^{\frac{1}{2g}}\end{aligned}$$

where as before, $0\leq c(\mathfrak{a}),c(\mathfrak{b})\leq g!$ denotes the number of ways $\mathfrak{a}$ can be written as a product of prime ideals. Applying Cauchy-Schwarz with respect to the summation over $\mathfrak{a}$, $\mathfrak{b}$, we get

$$\begin{aligned}&|\sum_{n_1\leq N}\sum_{n_2\leq N}\sum_{N(\mathfrak{p})\leq x}\chi_{n_1}(\mathfrak{p})\chi_{n_2}(\mathfrak{p})|\\ &\leq (N^2)^{1-\frac{1}{2g}}\left(\sum_{\mathfrak{a}}c^2(\mathfrak{a})\sum_{\mathfrak{b}}c^2(\mathfrak{b})\right)^{\frac{1}{4g}}\left(\sum_{\mathfrak{a}}\sum_{\mathfrak{b}}|\sum_{n_1=1}^{N}\sum_{n_2=1}^{N}\chi_{n_1n_2}(\mathfrak{a})\bar{\chi}_{n_1n_2}(\mathfrak{b})|^2\right)^{\frac{1}{4g}}\\ &\leq \left(N^2\right)^{1-\frac{1}{2g}}O\left(x^{\frac{1}{2}+\epsilon}\right)\left(\sum_{n_1=1}^{N}\sum_{n_2=1}^{N}\sum_{n_3=1}^{N}\sum_{n_4=1}^{N}\sum_{N(\mathfrak{a})\leq x^g}\sum_{N(\mathfrak{b})\leq x^g}\chi_{n_1n_2}(\mathfrak{a})\bar{\chi}_{n_1n_2}(\mathfrak{b})\chi_{n_3n_4}(\mathfrak{a})\bar{\chi}_{n_3n_4}(\mathfrak{b})\right)^{\frac{1}{4g}}\\ &= \left(N^2\right)^{1-\frac{1}{2g}}O\left(x^{\frac{1}{2}+\epsilon}\right)\left(\sum_{n_1,n_2,n_3,n_4\leq N}|\sum_{\mathfrak{a}}\chi_{n_1n_2}(\mathfrak{a})\bar{\chi}_{n_3n_4}(\mathfrak{a})|^2\right)^{\frac{1}{4g}}\end{aligned}$$

Now we have two cases: if $n_1n_2=n_3n_4$, sum over $\mathfrak{a}$ is $O\left(x^{g+\frac{1}{2}\epsilon}\right)$. For $n_1,n_2\leq N$, if $n_1n_2=n_3n_4$,, then the number of choices of n_3 and n_4 is limited since the integer n_1n_2 can only have at most N^δ factorization for any $\delta>0$. Thus in this case, we

get an upper bound of

$$\begin{aligned}&\left(N^2\right)^{1-\frac{1}{2g}} O\left(x^{\frac{1}{2}+\epsilon}\right)\left(N^{2+\delta}x^{2g+\epsilon}\right)^{\frac{1}{4g}}\\&= N^{2-\frac{1}{2g}+\frac{\delta}{4g}} O\left(x^{1+\frac{\epsilon}{4g}}\right).\end{aligned}$$

When $n_1n_2 \neq n_3n_4$, by Lemma 5.1.1, the upper bound is

$$\begin{aligned}&(N^2)^{1-\frac{1}{2g}} O\left(x^{\frac{1}{2}+\epsilon}\right) N\left(x^k|D|m\right)^{\left(\frac{1}{k+2}+\epsilon\right)\frac{1}{2g}}\\&= N^{2-\frac{1}{g}} x^{\frac{1}{2}+\frac{k}{k+2}+(k+1)\epsilon}|D|^{\frac{1}{k+2}}.\end{aligned}$$

Putting the two bounds together, the theorem follows. □

5.3 Viewing through the lens of probability theory

In this section, we will introduce the flavor of probability theory into the context of sums of characters. We start by heuristically treating the Legendre symbols as random variables,

$$\delta_q(r) = \left(\frac{r}{q}\right),$$

where the variables are indexed by primes $q \leq y$. So we have $\pi(y)$ many random variables. Then we study the sum of these random variables

$$g(r) = \sum_{q\leq y} \delta_q(r) = \sum_{q\leq y} \left(\frac{r}{q}\right)$$

and derive the following results. These can be viewed as reflecting that estimates violating GRH occur (if ever) very rarely.

Theorem 5.3.1. *Let p and q denote primes. Then*

$$\Big|\Big\{x \leq p \leq 2x : \Big|\sum_{q\leq x}\left(\frac{p}{q}\right)\Big| > x^{\frac{1}{2}}\log px\Big\}\Big| \leq \frac{\pi(x)}{(\log x)^{9/4}}$$

as $x \to \infty$.

Proof. With

$$g(p) = \sum_{q\leq x}\left(\frac{p}{q}\right),$$

the mean of $g(p)$ as p runs over primes upto x is

$$\frac{1}{\pi(x)}\sum_{p\leq x}(g(p)) = \frac{1}{\pi(x)}\sum_{p\leq x}\left(\sum_{q\leq x}\left(\frac{p}{q}\right)\right).$$

When $x = y$, using Theorem 5.0.2, this is bounded above by

$$\frac{x^{7/4}(\log x)^{-5/4}}{\pi(x)}.$$

Now let's consider the second moment of $g(p)$. It is

$$\frac{1}{\pi(x)}\sum_{p\leq x}g(p)^2 = \frac{1}{\pi(x)}\sum_{p\leq x}\sum_{q_1\leq x}\sum_{q_2\leq x}\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right).$$

By Theorem 5.2.1, this is bounded above by

$$\frac{x^2(\log x)^{-5/4}}{\pi(x)}.$$

Similarly, for $p \leq 2x$, $(\pi(x))^{-1} \sum_{p \leq 2x} g(p)^2$ is bounded above by

$$\frac{(2x)^2 (\log 2x)^{-5/4}}{\pi(2x)}.$$

Now let us consider the set of primes $x \leq p \leq 2x$ for which $|g(p)|$ exceeds $(x^{1/2} \log px)$. Since the second moment of $g(p)$ in this range of p is bounded by

$$\frac{1}{\pi(x)} \sum_{x \leq p \leq 2x} g(p)^2 \ll \frac{\left(x^2 (\log x)^{-5/4}\right)}{\pi(x)},$$

using a Chebychev-type argument as in Turán's proof of the Hardy-Ramanujan theorem, we see that,

$$\begin{aligned} |\{x \leq p \leq 2x : |g(p)| > x^{1/2} \log px\}| &\ll \frac{x^2 (\log x)^{-5/4}}{(x^{1/2} \log px)^2} \\ &= \frac{\pi(x)}{(\log x)^{1/4} (\log px)^2} \end{aligned}$$

as $x \to \infty$. Since $\log px \geq \log x$ for $x \leq p \leq 2x$, that proves the theorem. □

Similarly we have the following generalisation for abelian characters in a algebraic number field K. Consider the random variables

$$X_i(\mathfrak{p}) = \chi_i(\mathfrak{p})$$

for $1 \leq i \leq x$ defined on the prime ideals $\mathfrak{p}$ of K. The sum of these random variables is

$$h(\mathfrak{p}) = \sum_{i \leq x} X_i(\mathfrak{p}) = \sum_{i \leq x} \chi_i(\mathfrak{p}).$$

We study this sum and derive the following result.

Theorem 5.3.2. *Let K be an algebraic number field of degree k and discriminant D. Let $\chi_1, \chi_2, \cdots, \chi_N$ be N distinct abelian characters in K with moduli whose norms do not exceed m. Let g be a natural integer, $x > 1$, for any $\delta, \epsilon > 0$,*

$$\begin{aligned}&\left|\left\{\mathfrak{p} \in K : N(\mathfrak{p}) \leq x, \left|\sum_{q} \chi_q(\mathfrak{p})\right| > x^{\frac{1}{2}} \log mx\right\}\right| \\ &= O\left(\frac{x^{1-\frac{1}{2g}+\frac{\epsilon}{4g}+\frac{\delta}{2g}}}{\log x(\log mx)^2} + \frac{x^{-\frac{1}{2}-\frac{1}{g}+\frac{k}{2g(k+2)}+\frac{k\epsilon}{2g}}(|D|m)^{\frac{1}{2g(k+2)}+\frac{\epsilon}{2g}}}{\log x(\log mx)^2}\right)\end{aligned}$$

as $x \to \infty$ and the implied constants depend on k, g, ϵ and δ only.

Proof. With

$$h(\mathfrak{p}) = \sum_{i \leq x} \chi_i(\mathfrak{p}),$$

the mean of $h(\mathfrak{p})$ as $\mathfrak{p}$ runs over prime ideals in K with $N(\mathfrak{p}) \leq x$ is

$$\frac{1}{\pi(x)} \sum_{\mathfrak{p}} h(\mathfrak{p}) = \frac{1}{\pi(x)} \sum_{N(\mathfrak{p}) \leq x} \sum_{i \leq x} \chi_i(\mathfrak{p}).$$

By Theorem 5.0.3, when $N = x$, this is bounded by

$$\frac{1}{\pi(x)} \left(x^{2-\frac{1}{4g}+\epsilon} + x^2(x^{-g}|D|^{\frac{1}{2}}m)^{\frac{1}{g(k+2)}+\epsilon}\right).$$

Here $\pi(x)$ denotes the number of prime ideals $\mathfrak{p}$ in K with $N(\mathfrak{p}) \leq x$. Now let us estimate the second moment of $h(\mathfrak{p})$. By Theorem 5.2.2, when $N = x$, this is

bounded by

$$\frac{1}{\pi(x)}\left(x^{3+\frac{\epsilon}{4g}+\frac{\delta}{2g}-\frac{1}{2g}}+x^{\frac{5}{2}-\frac{1}{g}+\frac{k}{2g(k+2)}+\frac{k\epsilon}{2g}}(|D|m)^{\frac{1}{2g(k+2)}+\frac{\epsilon}{2g}}\right).$$

To consider the set of prime ideals $\mathfrak{p}$, with $N(\mathfrak{p}) \leq x$ for which $h(\mathfrak{p})$ exceeds $x^{\frac{1}{2}}\log mx$, using a Chebychev type argument as in Turán's proof of the Hardy-Ramanujan Theorem, we get

$$\begin{aligned}
&\left|\left\{\mathfrak{p}\in K : N(\mathfrak{p})\leq x, \left|\sum_q \chi_q(\mathfrak{p})\right| > x^{\frac{1}{2}}\log mx\right\}\right| \\
&\leq \frac{1}{x(\log mx)^2}\left(\frac{x^{2+\frac{\epsilon}{4g}+\frac{\delta}{2g}-\frac{1}{2g}}}{\log x}+\frac{x^{\frac{1}{2}-\frac{1}{g}+\frac{k}{2g(k+2)}+\frac{k\epsilon}{2g}}(|D|m)^{\frac{1}{2g(k+2)}+\frac{\epsilon}{2g}}}{\log x}\right) \\
&= \left(\frac{x^{1-\frac{1}{2g}+\frac{\epsilon}{4g}+\frac{\delta}{2g}}}{\log x(\log mx)^2}+\frac{x^{-\frac{1}{2}-\frac{1}{g}+\frac{k}{2g(k+2)}+\frac{k\epsilon}{2g}}(|D|m)^{\frac{1}{2g(k+2)}+\frac{\epsilon}{2g}}}{\log x(\log mx)^2}\right) \\
&= o(\pi(x))
\end{aligned}$$

as $x\to\infty$ for any $\delta,\epsilon>0$. That proves the theorem.

□

Remarks The results in the last section, Theorem 5.3.1 and Theorem 5.3.2 show that except for only a small set of primes p (or $\mathfrak{p}$ in case of algebraic number fields), $o(\pi(x))$, the predictions on the sum of abelian characters made by the generalised Riemann hypothesis hold true. One can also use Heilbronn's simple method to calculate the higher moments of the sums of these characters and use the method of moments to prove the Central Limit Theorem for the sums of characters. But we do not do this analysis here in this thesis. We relay it to future work.

Chapter 6

Concluding Remarks and Scope of Future Research

In this thesis so far, we have made progress in understanding the distribution of certain non-additive functions, specifically the Euler totient function and certain integer Fourier coefficients of Hecke eigenforms. We concentrated only on the shifts of prime arguments, $p + a$ for any integer $a > 0$ and primes p. Needless to say, the same methods easily generalise when the arguments are in an arithmetic progression, that is, to study $\Omega(f(an + b))$ for any $f \in \mathcal{H}$ (as in Chapter 4), any non-zero integers a, b.

However, there are many other paths that one could take here onwards, which we have not explored yet. We record some of these ideas in this chapter.

6.1 Joint Distribution of non-additive functions

The joint distribution of two additive functions was first studied by Levéque in 1949 in his thesis when he proved the following theorem.

Theorem 6.1.1 (Levéque, 1949). *Let $f(m)$ be a strongly additve function, with $f(p) \leq 1$ for all primes p. Suppose further that $\sum_p \frac{f^2(p)}{p} = \infty$. Let z_1, z_2 be real numbers. Then,*

$$\lim_{n\to\infty} \frac{1}{n}\left|\left\{m \leq n : \frac{f(m) - A_n}{B_n} \leq z_1, \frac{f(m+1) - A_n}{B_n} \leq z_2\right\}\right| = \left(\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z_1} e^{-\frac{t^2}{2}}dt\right)\left(\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z_2} e^{-\frac{t^2}{2}}dt\right)$$

where

$$A_n = \sum_{p\leq n} \frac{f(p)}{p} \text{ and } B_n = \left(\sum_{p\leq n} \frac{f^2(p)}{p}\right)^{\frac{1}{2}}.$$

This idea was further explored by Kubilius in his book [31] where he proved the following more general result.

For any strongly additive function $f_i(n)$, $1 \leq i \leq s$, let

$$A_i(x) = \sum_{p\leq x} \frac{f_i(p)}{p}$$

and

$$B_i(x) = \left(\sum_{p\leq x} \frac{f_i^2(p)}{p}\right)^{\frac{1}{2}} \geq 0.$$

Theorem 6.1.2 (Kubilius, 1950). *Let $a_1, a_2, \cdots, a_s$ be distinct fixed non-negative integers and let $f_1(m), f_2(m), \cdots, f_s(m)$ be strongly additive functions. Then as $x \to \infty$, the*

distribution function

$$\lim_{x\to\infty}\frac{1}{x}\Big|\Big\{m\leq x: \frac{f_1(m+a_1)-A_1(x)}{B_1(x)}\leq z_1,\cdots,\frac{f_s(m+a_s)-A_s(x)}{B_s(x)}\leq z_s\Big\}\Big|$$

tends to

$$\frac{1}{(2\pi)^{s/2}}\prod_{i=1}^{s}\left(\int_{-\infty}^{z_i}e^{-\frac{t^2}{2}}dt\right)$$

if for each $1\leq j\leq s$,

$$\sum_{\substack{p\leq x\\ |f_j(p)|>\epsilon B_j(x)}}\frac{1}{p}\to 0$$

and

$$\overline{\lim_{x\to\infty}}\frac{1}{B_j^2(x)}\sum_{\substack{p\leq x\\ |f_j(p)|<\epsilon B_j(x)}}\frac{f_j(p)}{p}\to 1.$$

Though in the above theorem, only the case of shifts of integer arguments is proved, one can show that the same result holds true over shifts of prime arguments as well (similar to the proof of Barban-Levin-Vinogradov Theorem (Theorem 4.5.1).

One avenue of research would be to see if these results can be adapted to show joint distribution for non-additive functions. In particular, one could try to use the approach as in Chapter 3, 4 Theorems 3.5.4 and 4.5.3 It would be a two step process. First, we would need to find strongly additive functions which would satisfy Theorem 6.1.2, following which we would show that this strongly additive function estimates the non-additive function under consideration. This general approach could be adapted to investigate many sets of non-additive functions, for example

1. $\Omega(\phi(n))$ and $\Omega(\phi(n+1))$

2. $\Omega(\tau(n))$ and $\Omega(\tau(n+1))$

3. $\Omega(\phi(p+a))$ and $\Omega(\phi(p+a+1))$

4. $\Omega(\tau(p+a))$ and $\Omega(\tau(p+a+1))$.

We have not investigated this completely but understanding these combinations could be a reasonable start. This is one of the problems we would tackle in future research.

6.2 Probabilistic Relations to the Riemann Hypothesis

On a different note, we have some partial results where we explore the connection of the notorious Riemann Hypothesis to Laguerre polynomials. We record this connection here.

Indeed, in a paper of Biane, Pitman and Yor [3], we find the following exposition. Let

$$\theta(t) = \sum_{n=-\infty}^{\infty} e^{-n^2\pi t}$$

be the classical Jacobi theta function. It is well known that it satisfies the modular transformation

$$\sqrt{t}\theta(t) = \theta(1/t), \qquad t > 0. \tag{6.2.1}$$

By means of this transformation, Let us define

$$\xi(s) := \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Then, by 6.2.1,

$$\frac{4\xi(s)}{s(s-1)} = \int_0^\infty (\theta(t)-1)t^{s/2}\frac{dt}{t}, \tag{6.2.2}$$

which is valid for $\Re(s) > 1$, can be extended analytically to the entire complex plane. Thus, we deduce the celebrated functional equation of the Riemann zeta function

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

Now, if we define

$$G(y) := \theta(y^2) = \sum_{n=-\infty}^{\infty} e^{-n^2\pi y^2},$$

then (6.2.1) becomes

$$G(1/y) = yG(y). \tag{6.2.3}$$

Set

$$\begin{aligned} H(y) &= \frac{d}{dy}\left(y^2\frac{d}{dy}G(y)\right) \\ &= 2yG'(y) + y^2G''(y). \end{aligned}$$

By definition of $G(y)$, this becomes

$$H(y) = 4y^2\left(\sum_{n=1}^{\infty}(2\pi^2n^4y^2 - 3\pi n^2)e^{-\pi n^2y^2}\right)$$

and $H(y)$ satisfies the same functional equation as G, namely

$$yH(y) = H(y^{-1}), \qquad y > 0.$$

Then Riemann's formula (6.2.2) for $\xi(s)$ becomes

$$2\xi(s) = \int_0^\infty H(y) y^s \frac{dy}{y}.$$

Since

$$2\pi^2 n^4 y^2 > 3\pi n^2$$

for $y \geq 1$, we see $H(y) > 0$ in this region. But then, by the functional equation, we have $H(y) > 0$ for $y > 0$ also. A routine computation shows that

$$2\xi(0) = 2\xi(1) = 1$$

and so

$$\int_0^\infty \frac{H(y)}{y} dy = \int_0^\infty H(y) dy = 1.$$

Thus, the function $H(y)$ can be viewed as the density function of a probability distribution on $(0, \infty)$ with mean 1. If Y is a random variable with this distribution, the functional equation for H translates as

$$E(f(1/Y)) = E(Yf(Y)).$$

Also, one can view $2\xi(s)$ as $E(Y^s)$.

In 1997, Xian-Jin Li [33] derived a remarkable criterion for the truth of the Riemann hypothesis. To state Li's criterion, we define for each natural number n,

$$\lambda_n = \sum_\rho \left(1 - \left(1 - \frac{1}{\rho}\right)^n\right),$$

where the sum is over the non-trivial zeros of the Riemann zeta function. Then, Li's criterion is that the Riemann hypothesis is true if and only if

$$\lambda_n \geq 0,$$

for all natural numbers n. It is not difficult to see that

$$\lambda_n = \frac{1}{(n-1)!}\frac{d^n}{ds^n}\left(s^{n-1}\log\xi(s)\right)\Big|_{s=1}.$$

Using Leibniz's rule,

$$\lambda_n = n\sum_{j=0}^{n-1}\binom{n-1}{j}\frac{k_{n-j}}{(n-j)!}, \tag{6.2.4}$$

where

$$k_n = \frac{d^n}{ds^n}\left(\log\xi(s)\right)\Big|_{s=1}.$$

If all the k_n's were positive, then by (6.2.4), the Riemann hypothesis follows. However, this is not always the case. For example,

$$k_3 = -0.000222316,\ k_4 = -0.0000441763$$

according to the table on pg. 441 of [3]. In fact, one can interpret the k_n's as cumulants of the random variable $\log(1/Y)$ with Y as before. Recall that given a random variable X, the moment generating function is $E(e^{tX})$ and the cumulant generating function is $\log E(e^{tX})$.

The cumulants k_n are also related to the Stieltjes constants γ_n which are defined

as the coefficients of the Laurent expansion of $\zeta(s)$ about $s = 1$,

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

where $\gamma_0 = \gamma$ is Euler's constant and one views the γ_n's as generalizations of this. In fact, it is not difficult to show that γ_n are given by the limits

$$\gamma_n = \lim_{m \to \infty} \left(\sum_{k=1}^{m} \frac{\log^n k}{k} - \frac{\log^{n+1} m}{n+1} \right).$$

We are more interested in the generalized Stieltjes constants η_n given by the Laurent expansion of $\frac{\zeta'}{\zeta}(s)$ about $s = 1$. Thus,

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s-1} + \sum_{n=0}^{\infty} \eta_n (s-1)^n.$$

By basic algebra, it is easy to express the η_n's as polynomials in the constants γ_n with rational coefficients. For example,

$$\eta_0 = -\gamma_0, \; \eta_1 = -\gamma_1 + \frac{1}{2}\gamma_0^2.$$

The significance of these constants lies in an important arithmetic formula for the λ_n's derived by Bombieri and Lagarias [5].

Theorem 6.2.1 (Bombieri, Lagarias, 1999)**.** *Let λ_n denote Li's coefficients for each natural number n. Then*

$$\lambda_n = 1 - \frac{n}{2}(\gamma + \log 4\pi) + S_1(n) + S_2(n) \tag{6.2.5}$$

where

$$S_1(n) = \sum_{j=2}^{n} \binom{n}{j} (-1)^j \left(1 - \frac{1}{2^j}\right) \zeta(j)$$

and

$$S_2(n) = \sum_{j=1}^{n} \binom{n}{j} \eta_{j-1} = -n\gamma_0 + \sum_{j=2}^{n} \binom{n}{j} \eta_{j-1}. \tag{6.2.6}$$

In fact, if for any $\epsilon > 0$, there is a constant $c(\epsilon) > 0$ such that for all $n \geq 1$,

$$\lambda_n \geq -c(\epsilon) e^{\epsilon n}$$

then the Riemann hypothesis follows.

Thus, a one-sided tempered growth of coefficients is enough for the Riemann Hypothesis. Also, Coffey [12] has shown that for $n \geq 2$,

$$\frac{1}{2}(n(\log n + \gamma - 1) + 1) \leq S_1(n) \leq (n(\log n + \gamma + 1) - 1).$$

In particular, $S_1(n)$ is non-negative for all $n \geq 2$ so that apart from $S_2(n)$, the contributions of the other terms to λ_n in (6.2.5) is $O(n \log n)$. Thus the truth of Riemann hypothesis hinges on $S_2(n)$ and the growth of the generalized Stieltjes constants. Omar and Bouanani [6] extend Li's criterion to the function field setting.

Clearly, we should therefore focus our attention on η_j's. As noted in [5], one can show that

$$\eta_j = \frac{(-1)^j}{j!} \lim_{x \to \infty} \left(\sum_{m \leq x} \frac{\Lambda(m) \log^j m}{m} - \frac{(\log x)^{j+1}}{j+1} \right)$$

where

$$\Lambda(m) = \begin{cases} \log p, \ m = p^{\alpha}, \alpha \geq 1, \\ 0, \ \text{otherwise.} \end{cases}$$

This expression is unwieldly. We offer an alternate expression via Laguerre polynomials.

For $\psi(x) = \sum_{n \leq x} \Lambda(n)$, we know

$$\begin{aligned} -\frac{\zeta'}{\zeta}(s) &= s \int_1^{\infty} \frac{\psi(x)}{x^{s+1}} dx \\ &= \frac{s}{s-1} + s \int_1^{\infty} \frac{\psi(x) - x}{x^{s+1}} dx \\ &= \frac{1}{s-1} + 1 + s \int_1^{\infty} \frac{\psi(x) - x}{x^{s+1}} dx. \end{aligned}$$

Here, we can write the integral as

$$\begin{aligned} &(s-1+1) \int_1^{\infty} \frac{(\psi(x) - x)}{x^2} e^{-(s-1)\log x} dx \\ =&(s-1+1) \sum_{j=0}^{\infty} \frac{(-1)^j (s-1)^j}{j!} \int_1^{\infty} \frac{\Delta(x) \log^j x}{x^2} dx \end{aligned}$$

where $\Delta(x) = \psi(x) - x$. If we let

$$\delta_j = \int_1^{\infty} \frac{\Delta(x) \log^j x}{x^2} dx, \tag{6.2.7}$$

then

$$\eta_j = \frac{(-1)^j \delta_j}{j!} + \frac{(-1)^{j-1} \delta_{j-1}}{(j-1)!}. \tag{6.2.8}$$

It is possible to derive estimates for η_j, δ_j and γ_j but all of these estimates have exponential growth. So we need to explore cancellations.

In this context, we have the Laguerre polynomials:

$$L_n(x) = \sum_{j=0}^{n} \binom{n}{j} \frac{(-x)^j}{j}.$$

The generalised Laguerre polynomials which can be defined by the following generating function (see [1], [11], [36]):

$$\sum_{n=0}^{\infty} L_n^{(\alpha)}(x) t^n = \frac{1}{(1-t)^{\alpha+1}} \exp\left(-\frac{tx}{1-t}\right), \ (|t| < 1)$$

can also be defined by the closed formula for $n \geq 0$,

$$L_n^{(\alpha)}(x) = \sum_{k=0}^{n} (-1)^k \binom{n+\alpha}{n-k} \frac{x^k}{k!} \tag{6.2.9}$$

where $\binom{r}{k}$ denote the binomial coefficients given by

$$\binom{r}{0} = 1 \text{ and } \binom{r}{k} = \frac{r(r-1)(r-2)\cdots(r-k+1)}{k(k-1)\cdots 1}$$

for positive integer k and any complex number r.

Theorem 6.2.2. *Let $\Delta(x) = \sum_{n \leq x} \Lambda(n) - x$ and $S_2(n)$ be as in 6.2.6. Further suppose that $L_n^{(\alpha)}(x)$ denote the Laguerre polynomials. Then*

$$S_2(n) = -n\gamma_0 + \int_1^{\infty} \frac{\Delta(x)}{x^2} L_{n-1}^{(2)}(\log x) dx - n \int_1^{\infty} \frac{\Delta(x)}{x^2} dx \tag{6.2.10}$$

where γ_0 denotes the Euler's constant.

Proof. In order to understand $S_2(n)$, we can try to get the expression of η_{j-1} in (6.2.6) in terms of integrals of generalised Laguerre polynomials. Using (6.2.6) and

(6.2.8), we get

$$\begin{aligned} S_2(n) &= -n\gamma_0 + \sum_{j=2}^{n} \binom{n}{j} \left(\frac{(-1)^{j-1}\delta_{j-1}}{(j-1)!} + \frac{(-1)^{j-2}\delta_{j-2}}{(j-2)!} \right) \\ &= -n\gamma_0 + T_1(n) + T_2(n) \end{aligned}$$

where using (6.2.7)

$$\begin{aligned} T_1(n) &= \sum_{j=2}^{n} \binom{n}{j} \frac{(-1)^{j-1}\delta_{j-1}}{(j-1)!} \\ &= \int_1^{\infty} \frac{\Delta(x)}{x^2} \left(\sum_{j=2}^{n} \binom{n}{j} \frac{(-\log x)^{j-1}}{(j-1)!} \right) dx \end{aligned}$$

and

$$\begin{aligned} T_2(n) &= \sum_{j=2}^{n} \binom{n}{j} \frac{(-1)^{j-2}\delta_{j-2}}{(j-2)!} \\ &= \int_1^{\infty} \frac{\Delta(x)}{x^2} \left(\sum_{j=2}^{n} \binom{n}{j} \frac{(-\log x)^{j-2}}{(j-2)!} \right) dx. \end{aligned}$$

Writing $j' = j - 1$ and using $\binom{n}{k} = \binom{n}{n-k}$ for $0 \leq k \leq n$, we can rewrite the sum in expression for $T_1(n)$ as

$$\begin{aligned} &\sum_{j'=1}^{n-1} \binom{n}{j'+1} (-1)^{j'} \frac{(\log x)^{j'}}{(j')!} \\ &= \sum_{j'=1}^{n-1} \binom{(n-1)+1}{(n-1)-j'} (-1)^{j'} \frac{(\log x)^{j'}}{(j')!} \\ &= -n + L_{n-1}^{(1)}(\log x). \end{aligned}$$

A similar calculation for the sum in the expression for $T_2(n)$ gives

$$\begin{aligned}
&\sum_{j=2}^{n} \binom{n}{j} \frac{(-\log x)^{j-2}}{(j-2)!} \\
=&\sum_{j'=0}^{n-2} \binom{(n-2)+2}{(n-2)-j'} \frac{(-\log x)^{j'}}{(j')!} \\
=&L_{n-2}^{(2)}(\log x).
\end{aligned}$$

Thus, we get the following expression for $S_2(n)$ in terms of the generalised Laguerre polynomials

$$S_2(n) = -n\gamma_0 - n\int_1^\infty \frac{\Delta(x)}{x^2}dx + \int_1^\infty \frac{\Delta(x)}{x^2}\left[L_{n-1}^{(1)}(\log x) + L_{n-2}^{(2)}(\log x)\right]dx \tag{6.2.11}$$

The integral in the last term of (6.2.11) can be simplified as follows:

$$\begin{aligned}
&L_{n-1}^{(1)}(\log x) + L_{n-2}^{(2)}(\log x) \\
=&\sum_{k=0}^{n-1} \binom{n}{n-1-k} (-1)^k \frac{(\log x)^k}{k!} + \sum_{k=0}^{n-2} \binom{n}{n-2-k} (-1)^k \frac{(\log x)^k}{k!} \\
=&\frac{(\log x)^{n-1}}{(n-1)!} + \sum_{k=0}^{n-2} \left(\binom{n}{n-1-k} + \binom{n}{n-2-k} \right) (-1)^k \frac{(\log x)^k}{k!} \\
=&\frac{(\log x)^{n-1}}{(n-1)!} + \sum_{k=0}^{n-2} \binom{n+1}{n-1-k} \frac{(-\log x)^k}{k!} \\
=&\frac{(\log x)^{n-1}}{(n-1)!} - \binom{n-1+2}{n-1-(n-1)} \frac{(\log x)^{n-1}}{(n-1)!} + \sum_{k=0}^{n-1} \binom{n-1+2}{n-1-k} \frac{(-\log x)^k}{k!} \\
=&\sum_{k=0}^{n-1} \binom{n-1+2}{n-1-k} \frac{(-\log x)^k}{k!} \\
=&L_{n-1}^{(2)}(\log x).
\end{aligned}$$

Thus the theorem follows. □

The last term in 6.2.10 is actually $O(n)$ by a simple application of the unconditional error term in the prime number theorem. So, to prove the Riemann hypothesis, we need to focus on the integral in the second term in view of the results of Bombieri and Lagarias.

Thus, this particular connection shows that understanding Laguerre polynomials and their integrals could give some insight into Li's coefficients which in turn would connect to the Riemann Hypothesis. We plan to pursue this and derive some definitive results in this context in our future research.

Bibliography

[1] G. B. Arfken, H. J. Weber, F. E. Harris, Mathematical Methods for Physicists: A Comprehensive Guide, Academic Press, Oxford, (2011).

[2] N. L. Bassily, I. Kátai, M. Wijsmuller, Number of prime divisors of $\phi_k(n)$, where ϕ_k is the k-fold iterate of ϕ. J. Number Theory 65 (1997), no. 2, 226–239.

[3] P. Biane, J. Pitman, M. Yor, Probability laws related to the Jacobi theta and Riemann zeta functions and Brownian excursions, Bulletin of the American Mathematical Society, 38 (2001), 435-465.

[4] P. Billingsley, Probability and measure, Anniversary edition, Wiley Series in Probability and Statistics, John Wiley and Sons, Inc., Hoboken, NJ, (2012).

[5] E.Bombieri, J. Lagarias, Complements to Li's criterion for the Riemann hypothesis, J. Number Theory 77 (1999), no. 2, 274-287.

[6] S. Bouanani, S. Omar, Li's criterion and the Riemann hypothesis for function fields II, Finite Fields Appl. 45 (2017), 53-58.

[7] V. Brun, Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare, Archiv for Mathematik og Naturvidenskab. B34 (8), (1915).

[8] D. A. Burgess, The distribution of quadratic residues and non-residues, Mathematika 4, 1957, 106–112.

[9] H. Carayol, Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert, Ann. scient. Éc. Norm. Sup., 4^e série 19 (1986), 409–468.

[10] H. Carayol, Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires, Duke Math. J. 59 (1989), 785–801.

[11] L. Carlitz, Some generating functions for Laguerre polynomials, Duke Math. J., 35 (1968), 825-827.

[12] M. W. Coffey, Toward verification of the Riemann hypothesis: application of the Li criterion, Math. Phys. Anal. Geom. 8 (2005), 211-255.

[13] A. C. Cojocaru, M. R. Murty, An introduction to sieve methods and their applications, London Mathematical Society Student Texts, 66 (2005), Cambridge University Press.

[14] P. Deligne, Formes modulaires et représentations l-adiques, (French) (Modular forms and l-adic representations) Séminaire Bourbaki, Vol. 1968/69, Exposés 347–363, Exp. No. 355, 139–172, Lecture Notes in Math., 175, Springer, Berlin, 1971.

[15] G. L. Dirichlet, G. Lejeune Dirichlet's Werke I, Berlin Georg Reimer, 1889.

[16] G. L. Dirichlet, Vorlesungen über Zahlentheorie, Braunschweig Vieweg, 1879.

[17] P. D. T. A. Elliott, Probabilistic Number Theory II, Central Limit Theorems, Springer-Verlag, 1980.

[18] P. Erdős, On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ function, The Quarterly Journal of Mathematics, Volume no.-6, Issue 1, 1 January 1935, Pages 205–213.

[19] P. Erdős, Ramanujan and I, Number theory, Madras 1987, 1–20, Lecture Notes in Math., 1395, Springer, Berlin, 1989.

[20] P. Erdős and M. Kac, The Gaussian law of errors in the theory of additive number theoretic functions, Amer. J. Math. 62 (1940), 738–742.

[21] P. Erdős, R. Murty, On the order of a mod p, CRM Proceedings and Lecture Notes, Volume 19, (1999), 87-97.

[22] P. Erdős, C. Pomerance, On the normal number of prime factors of $\phi(n)$. Number theory (Winnipeg, Man., 1983). Rocky Mountain J. Math. 15 (1985), no. 2, 343–352.

[23] P. Erdős, A. Wintner, Additive arithmetical functions and statistical independence, Amer. J. Math. 61 (1939), 713–721.

[24] F.Gerth III, S.W.Graham, Application of a character sum estimate to a 2-class number density, Journal of Number Theory, Vol 19 -2, (1984), 239-247.

[25] H. Halberstam, H. -E. Richert, Sieve Methods, Academic Press, 1974.

[26] R. R. Hall, G. Tenenbaum, Divisors, Cambridge Tracts in Mathematics, Vol. 90. Cambridge University Press, Cambridge, New York, New Rochelle, Melbourne, and Sydney, 1988.

[27] G. H. Hardy, S. Ramanujan, The normal number of prime factors of a number n, Quarterly Journal of Mathematics, 48 (1917), 76-92.

[28] H. Heilbronn, On the averages of some arithmetical functions of two variables, Mathematika, A journal of Pure and Applied Mathematics, Vol 5, Part 1, June 1958.

[29] A. Hildebrand, Additive and multiplicative functions on shifted primes, Proc. London Math. Soc. (3) 59 (1989), no. 2, 209–232.

[30] A. Kar, The Hardy Ramanujan theorem revisited, (submitted).

[31] J. Kubilius, Probabilistic methods in the theory of numbers, Translations of Mathematical Monographs, Vol. 11, American Mathematical Society, Providence, R.I. (1964).

[32] J. C. Lagarias and A. M. Odlyzko, Effective versions of the Chebotarev density theorem. In Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, (1977) 409–464.

[33] X-J Li, The positivity of a sequence of numbers and the Riemann hypothesis, Journal of Number Theory, 65 (1997), 325-333.

[34] A. N. Kolmogorov, Grundbegriffe der Wahrscheinlichkeitsfelder und-räume, Springer-Verlag, Heidelberg, 1933; Foundations of the Theory of Probability, Chelsea, New York, 1956.

[35] W. J. LeVeque, On the size of certain number-theoretic functions. Trans. Amer. Math. Soc. 66 (1949), 440–463.

[36] W. Magnus, F. Oberhettinger, R. P. Soni, Formulas and Theorems for the Special Functions of Mathematical Physics, Springer-Verlag, New York, (1966).

[37] M. R. Murty, Problems in analytic number theory, Second edition, Graduate Texts in Mathematics, 206. Readings in Mathematics. Springer, New York, 2008.

[38] M. R. Murty, V. K. Murty, Prime divisors of Fourier coefficients of modular forms, Duke Mathematical Journal, 51, (1984), 57-76.

[39] M. R. Murty, V. K Murty, An analogue of the Erdős-Kac theorem for Fourier coefficients of modular forms, Indian J. Pure Appl. Math. 15 (1984), no. 10, 1090–1101.

[40] M. R. Murty, N. Prabhu, Central limit theorems for sums of quadratic characters, Hecke eigenforms, and elliptic curves. Proc. Amer. Math. Soc. 148 (2020), no. 3, 965–977.

[41] R. E. A. C. Paley, A theorem on characters, J. London Math. Soc. 7, 1932, 28–32.

[42] S. Ramanujan, On the number of divisors of a number, Journal of the Indian Mathematical Society, 7 (1915), 131-133.

[43] S. Ramanujan, On certain arithmetical functions [Trans. Cambridge Philos. Soc. 22 (1916), no. 9, 159–184]. Collected papers of Srinivasa Ramanujan, 136–162, AMS Chelsea Publ., Providence, RI, 2000.

[44] H. Robbins, A remark on Stirling's formula. Amer. Math. Monthly 62, (1955). 26–29.

[45] J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, L'Ens. Math. 22 (1976), 227-260.

[46] G. Tenenbaum, Introduction to analytic and probabilistic number theory (Third edition). Translated from the 2008 French edition by Patrick D. F. Ion. Graduate Studies in Mathematics, 163. American Mathematical Society, Providence, RI, 2015.

[47] N. M. Timofeev, Hardy-Ramanujan and Halasz inequalities for shifted prime numbers. (Russian. Russian summary) Mat. Zametki 57 (1995), no. 5, 747–764, 799; translation in Math. Notes 57 (1995), no. 5-6, 522–535.

[48] E. C. Titchmarsh, Theory of functions, Second Edition, Oxford University Press, 1939.

[49] P. Turán, On a theorem of Hardy and Ramanujan, J. London Math. Soc.,9 (1934), 274–276.

[50] G. Watson, Uber Ramanujansche Kongruenzeigenschaften der Zerfillungsanzahlen, Math. Z. 39 (1935), 712-731.

[51] S. L. Zabell, Alan Turing and the Central Limit Theorem, *American Mathematical Monthly,* **102** (1995), 483-494.