# MS (Master of Science) Thesis

Part 1: The Vinogradov Theorem

Part 2: Prime Numbers and Arithmetic Progressions

Anurag Sahay
11141/11917141
BS-MS Dual Degree,
Mathematics and Scientific Computing

under the supervision of

Dr. Somnath Jha
Dept. of Mathematics and Statistics

7th April, 2016

**Abstract**

In this thesis, we consider two separate, but inter-related problems about prime numbers across two semesters. In the first part of the thesis, done over the 2015-16/Ist Semester, we consider the Odd Goldbach Conjecture, in particular the partial result knonw as the Vinagradov theorem. In the second part of the thesis, done over the 2015-16/IInd Semester, we consider the prime number theorem in arithmetic progressions.

# Notation

We shall describe here the notation that we will need from analytic number theory.

We shall use the Landau notation

$$f(x) = \mathcal{O}(g(x))$$

equivalently with $f \ll g$ and $g \gg f$to mean that there exists some positive constant $C$ such that $|f(x)| \leq Cg(x)$ for sufficiently large $x$. Such an estimate is called a "big-oh estimate".

We use

$$f(x) = o(g(x))$$

to mean that $f(x)/g(x) \to 0$ as $x \to \infty$. Such an estimate is called a "little-oh estimate", and being $o(g(x))$ is strictly stronger than being $\mathcal{O}(g(x))$. However, little-oh estimates are qualitative statements, and not very good for calculation. Hence, in practice, one always use more precise big-oh estimates for calculation (ie, with a smaller $g(x)$) and only return to the little-oh estimate in the last step to give a neater but strictly weaker estimate in the end, if at all. (See for example, the Prime Number Theorem).

We will often write

$$f(x) = g(x) + \mathcal{O}(h(x)) \text{ or } f(x) = g(x) + o(h(x))$$

to mean that there exists a function $p(x)$ which is respectively $= \mathcal{O}(h(x))$ or $= o(h(x))$ such that $f(x) = g(x) + p(x)$.

Finally we use

$$f(x) \sim g(x)$$

interchangeably with

$$f(x) = g(x) + o(g(x))$$

to denote the asymptotic equality $f(x)/g(x) \to 1$ as $x \to \infty$.

We use $(a, b)$ to denote the greatest common divisor of $a$ and $b$ and $\varphi(n)$ for Euler's totient function,

$$\varphi(n) = \#\{x \in \mathbb{Z} : 1 \leq x \leq n, (x, n) = 1\}$$

For any $A \subset \mathbb{Z}$, we use $1_A(n)$ for its indicator function,

$$1_A(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{otherwise} \end{cases}$$

We use $p_n$ for the $n$th prime number. Furthermore, for us, $n$ will always be an integer, $p$ will always be prime, and $\mathcal{P}$ shall denote the set of prime numbers.

We will use the convention $e(x) = e^{2\pi i x}$.

For summations and products, we shall use the standard practice of specifying the variable over which the operation is taking place under the $\sum$ or $\prod$ as well as specifying the other conditions the variable needs to satisfy. Furthermore, sums over $p$ are over primes and sums over $n$ are over positive integers. This may lead to sums of the form

$$\sum_{n \leq x}, \sum_{p \leq x}, \sum_{p|m}, \sum_{n|m}, \sum_{\chi \bmod q}$$

and so on, which are respectively sums over positive integers up to $x$, primes up to $x$, all prime divisors of $m$, all divisors of $m$, and all Dirichlet character modulo $q$.

Unless otherwise specified, all Dirichlet characters are modulo $q$.

A $\star$ will be used to denote any theorem which has not been proved in this report.

# Contents

# Part I

# MTH598A: The Vinogradov Theorem

**Abstract**

The Goldbach conjecture is one of the oldest problems in Number Theory, specifically in additive number theory. This project is a reading project on the Vinogradov theorem, proved by I. M. Vinogradov in 1937, which is the one of the best partial results towards settling the odd Goldbach conjecture. We briefly survey some basic tools in the field of analytic number theory, and then present an exposition of a proof of the theorem under the assumption of the Generalized Riemann Hypothesis. We are following [1] and [2] in our approach.

This report was submitted as part of the course MTH598A (MS Thesis) in the 2015-16/1st Semester towards the completion of the degree requirements for the BS-MS dual degree programme.

# Chapter 1

# Introduction

The Goldbach conjecture, first introduced by Christian Goldbach in a sequence of letters to Leonhard Euler, has two versions, the even/strong/binary conjecture and the odd/weak/ternary conjecture. These are as follows:

**Conjecture 1.1** (Binary Goldbach Conjecture)**.** Every even integer $n > 2$ can be written as a sum of two primes. That is, there exist $p_1, p_2 \in \mathcal{P}$ such that

$$n = p_1 + p_2$$

**Conjecture 1.2** (Ternary Goldbach Conjecture)**.** Every odd integer $n > 5$ can be written as a sum of three primes. That is, there exist $p_1, p_2, p_3 \in \mathcal{P}$ such that

$$n = p_1 + p_2 + p_3$$

The binary conjecture is clearly stronger than the ternary conjecture since if $n$ is an odd number greater than 5, then $n - 3$ is an even number greater than 2, and is hence expressible as the sum of two primes $p_1 + p_2$. Thus,

$$n = 3 + p_1 + p_2$$

is a representation of $n$ as the sum of three primes.

The closest theorem that we have to the binary conjecture is known as Chen's theorem, which is the following:

**Theorem 1.1** (Chen's Theorem, $\star$)**.** *Any even integer $n > 2$ can be written as*

$$n = p + P$$

*where $p \in \mathcal{P}$ is prime, and $P = p_1$ or $P = p_1 p_2$ where $p_1, p_2 \in \mathcal{P}$ (in other words $P$ is a product of at most two primes).*

The barrier between establishing Chen's theorem and the even conjecture is a relatively well-known issue in Sieve Theory known as the Parity problem (see [3] for details). This is also the barrier that makes the odd conjecture considerably easier than the even conjecture.

In the 1920s, Hardy and Littlewood proved an asymptotic version of the odd Goldbach conjecture under the assumption of the Generalized Riemann Hypothesis (GRH) using the novel Hardy-Littlewood Circle Method. Extending their ideas, in 1937, Vinogradov proved his celebrated theorem by establishing this asymptotic result unconditionally, without relying on the unproved GRH. In essence, the theorem states that the odd Goldbach conjecture is true for sufficiently large numbers. In other words,

**Theorem 1.2** (Vinogradov's theorem)**.** *There exist an integer $N$ such that for all odd $n > N$, $n$ is a sum of three primes. That is, there exist $p_1, p_2, p_3 \in \mathcal{P}$ such that*

$$n = p_1 + p_2 + p_3$$

Since Vinogradov's work, there has been many subsequent improvements towards the odd Goldbach conjecture. In 1956, K. Borozdin proved that N can be chosen to be $3^{3^{15}}$. Finally in 2013, Harald Helfgott [4] settled the conjecture in its entirety.

In this report, we shall establish Vinogradov's theorem under the assumption of GRH.

We shall devote the rest of this chapter to introducing key concepts from analytic number theory that we shall use in our proof.

## 1.1 The Prime Number Theorem for Arithmetic Progressions

A central question in analytic number theory is that of the distribution of prime numbers among the positive integers. The "macrostructure" of this distribution is normally studied by examining the *prime-counting function* $\pi(x)$ given by

$$\pi(x) = \sum_{p \leq x} 1$$

where the summation is over primes less than or equal to $x$, and trying to determine its asymptotic behaviour as $x \to \infty$. One of the early achievements of analytic methods in number theory was the *Prime Number Theorem* (PNT) proved independently by Hadamard and de la Valle-Poussin, which gives an asymptotic formula for $\pi(x)$ which says

$$\pi(x) \sim \frac{x}{\log x}$$

Another question of much importance in number theory is the distribution of prime numbers within arithmetic progressions. Information about this distribution can be used to prove a plethora of interesting facts about the prime numbers. Another early result (perhaps the seminal result in analytic number theory) proven by Dirichlet states that if

$$\pi(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} 1$$

is the number of primes less than $x$ in a given congruence class modulo $q$ and further suppose that $(a, q) = 1$ (that is, $a$ is *coprime* to $q$), then $\pi(x; q, a) \to \infty$ as $x \to \infty$.

If $(a, q) \neq 1$, there are obviously only finitely many primes in the congruence class containing $a$, since $p \equiv a \pmod{q}$ implies that any prime which divides both $a$ and $q$ must divide $p$. Thus, if $(a, q) > 1$ then the only primes which can be in the congruence class are the ones divisible by $(a, q)$. If $(a, q)$ is composite, then there are zero such primes, and if $(a, q)$ is prime there is one such prime, and hence the number of primes in this congruence class is

finite. Trivially, thus, any arithmetic progression has infinitely many primes if and only if the first term and common difference are coprime. This is known as "Dirichlet's theorem on primes in arithmetic progressions".

However, we can do much more than simply show infinitude for $(a, q) = 1$, and we are interested in obtaining a numerical estimate similar to PNT for primes in a particular progresson. There is no natural reason to expect that the primes would be more concentrated in one particular congruence class than the others. Thus, we would expect that all such congruence classes should roughly have the "same" number of primes. Since there are $\varphi(q)$ many such congruence classes we would expect that for some fixed $a$ and sufficiently large $x$, $\pi(x; q, a)$ should roughly be $\pi(x)/\varphi(q)$. This turns out to be true, in what is a quantitative version of Dirichlet's theorem which states that

$$\pi(x; q, a) \sim \frac{\pi(x)}{\varphi(q)} \sim \frac{1}{\varphi(q)} \frac{x}{\log x}$$

This quantitative version of Dirichlet's theorem is known as the "Prime Number Theorem for arithmetic progressions".

While this is a deep theorem, the asymptotically equality is not sufficient and we need more information about the error in this theorem. We can write the above estimate as

$$\pi(x; q, a) = \frac{1}{\varphi(q)} \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

Where $o()$ is the little-oh asymptotic notation. The goal of many results is to replace the error term with a more precise big-oh estimate. In particular, the Generalized Riemann Hypothesis provides an improved estimate (this is, in fact, one of the major reasons why GRH is such an important conjecture).

We shall now elaborate on an alternative way to state these theorems that is much more natural to use and prove.

## 1.2 Chebyshev's $\vartheta$ and $\psi$ Functions

It turns out that the prime-counting function $\pi(x; q, a)$ is very difficult to use in proofs. Instead, it has been typical since Chebyshev to replace them

by the theta and psi functions, $\vartheta(x;q,a)$ and $\psi(x;q,a)$.

An alternative way to write $\pi$ is the following:

$$\pi(x;q;a) = \sum_{\substack{n\leq x \\ n\equiv a \bmod q}} 1_{\mathcal{P}}(n)$$

Where $1_A(n)$ is the indicator function of a set of integers $A$. Thus, $\pi$ can be interpreted as a weighted sum over all elements in a congruence class with the prime elements weighted with 1 and the composite elements weighted with 0.

However, it turns out that this method of weighting is not ideal for proving results. Instead, a better weight is the von Mangoldt function, which we shall define presently. We thus consider instead the sum

$$\sum_{\substack{n\leq x \\ n\equiv a \bmod q}} \Lambda(n)$$

where $\Lambda(n)$ is the more appropriate weight, the von Mangoldt function.

In this and the subsequent section we will provide a recipe for turning results about one of the above weighted sums to the other, and try to establish why the second sum is better suited for manipulation.

One way to motivate this is the following. Clearly, by PNT

$$\frac{\pi(x)\log x}{x} = 1 + o(1)$$

Taking natural logarithms both sides

$$\log \pi(x) - \log x + \log\log x = \log(1 + o(1)) = o(1)$$

where the last equality is easily established.[1] Now, if $x = p_n$, the $n$th prime number, then clearly $\pi(x) = n$. Thus we have

[1] As the logarithm is continuous at 1, if $f(x) = o(1)$, then $\lim_{x\to\infty} f(x) = 0$. Thus $\lim_{x\to\infty} \log(1+f(x)) = \log\left(1 + \lim_{x\to\infty} f(x)\right) = \log(1) = 0$. Hence, clearly, $\log(1+o(1)) = o(1)$.

$$\log n - \log p_n + \log\log p_n = o(1)$$

Noting that $\log\log x = o(\log x)$, we thus get

$$\log n = \log p_n + o(\log p_n)$$

Or, in other words,

$$\log n \sim \log p_n$$

This suggests that if instead of giving all primes the same weight 1, we weight them by their logarithm, the higher primes would contribute more, multiplying a rough factor of a logarithm. We can formalize this heursitic by a partial summation[2] argument.

Thus, we define a new function, called the Chebyshev $\vartheta$-function in the literature as follows

$$\vartheta(x) = \sum_{p \leq x} \log p$$

which weights each prime by their logarithm instead of 1.

As mentioned above, using partial summation, we can establish the following two identities

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt$$

$$\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t} dt$$

Using these, we can convert any estimate on the first function into one of the second, and vice-versa.

In particular, it is easily shown that

$$\lim_{x\to\infty} \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = \lim_{x\to\infty} \frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt = 0$$

[2]See Appendix

which shows that PNT is equivalent to $\vartheta(x) \sim x$. In any case, the first identity can be used to change any estimate for $\vartheta$ to one for $\pi$.

Analogous to the prime-counting function for progressions, $\pi(x; q, a)$, we can define a $\vartheta(x; q, a)$ for progressions as follows

$$\vartheta(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \log p$$

The above identities can then be proved in exactly the same way by replacing $\pi(x)$ with $\pi(x; q, a)$ and $\vartheta(x)$ with $\vartheta(x; q, a)$.

In some sense, it is natural to work with logarithms of primes when working with weighted sums. Primes are essentially multiplicative objects, and the logarithm allows one to pass from the multiplicative to the additive, and thus form a natural candidate for dealing with sums over primes. However, it turns out even weighting all primes by their logarithms and all composites by 0 does not give the most convenient form. The most convenient form is given instead by Chebyshev's $\psi$-function,

$$\psi(x) = \sum_{p^k \leq x} \log p$$

where the sum is over all primes $p$ and all positive integers $k$ such that $p^k \leq x$. In other words, we weight all prime powers by the logarithm of the prime of which they are a power, and all other numbers by 0. The hope then, is that since the prime powers contribute a smaller amount than the primes, the contribution from them can be controlled.

Clearly,

$$\psi(x) = \sum_{k=1}^{\infty} \sum_{p^k \leq x} \log p = \sum_{k=1}^{\infty} \sum_{p \leq \sqrt[k]{x}} \log p = \sum_{k=1}^{\infty} \vartheta(x^{1/k})$$

Here note that since for a fixed positive $x$, $\lim_{k \to \infty} x^{1/k} = 1$ thus for sufficiently large $k$, $x^{1/k} < 2$, and thus $\vartheta(x^{1/k}) = 0$. Thus, all but finitely many terms vanish, and in particular, the terms are non-vanishing if and only if $x^{\frac{1}{k}} \geq 2$. Taking logarithm to the base 2 on both sides, we see this is the same as requiring $k \leq \log_2 x$.

Thus,

$$\psi(x) = \sum_{k \leq \log_2 x} \vartheta(x^{\frac{1}{k}})$$

Now, trivially, $\vartheta(x) = \sum_{p \leq x} \log p \leq \sum_{p \leq x} \log x \leq x \log x$. Also, we know that $\vartheta(x)$ is increasing and thus, $\vartheta(x^{1/2}) \geq \vartheta(x^{1/k})$ for $k \geq 2$. With this we can see that

$$\begin{aligned}
\psi(x) - \vartheta(x) &= \sum_{2 \leq k \leq \log_2 x} \vartheta(x^{1/k}) \\
&\leq \sum_{2 \leq k \leq \log_2 x} \vartheta(x^{1/2}) \\
&\leq \vartheta(x^{1/2}) \log_2 x \\
&\leq x^{1/2} (\log_2 x)(\log x^{\frac{1}{2}}) \\
&= O\left(x^{1/2} (\log x)^2\right)
\end{aligned}$$

Thus, any estimate for $\psi$ can be converted into an estimate for $\vartheta$, provided the estimate has an error larger than $O(\sqrt{x})$ by at least two logarithmic factors. In particular, since logarithms always grow slower than powers, for any $\epsilon > 0$, an error of the form $O(x^{1/2+\epsilon})$ can be tolerated. This is much tighter than most bounds we have, and thus in any theorem we shall prove here, $\psi$ may be interchanged with $\vartheta$ and vice-versa. This also means that the PNT is equivalent to $\psi(x) \sim x$. Using the bound $\vartheta(x) = O(x)$, which is substantially weaker than PNT and was proven by Chebyshev using elementary methods, we can sharpen the estimate to $\psi(x) - \vartheta(x) = O(\sqrt{x})$.[3]

Identically to $\pi$ and $\vartheta$, we define $\psi(x; q, a)$

$$\psi(x; q, a) = \sum_{\substack{p^k \leq x \\ p^k \equiv a \bmod q}} \log p$$

[3] Clearly

$$\psi(x) - \vartheta(x) = \vartheta(x^{1/2}) + \sum_{k=3}^{\lfloor \log_2 x \rfloor} \vartheta(x^{1/k}) \leq \vartheta(x^{1/2}) + \vartheta(x^{1/3}) \log_2 x = O(x^{1/2})$$

Furthermore, as above

$$\psi(x;q,a) = \sum_{k \leq \log_2 x} \vartheta(x^{1/k};q,a)$$

and thus,

$$\begin{aligned} \psi(x;q,a) - \vartheta(x;q,a) &= \sum_{2 \leq k \leq \log_2 x} \vartheta(x^{\frac{1}{k}};q,a) \\ &\leq \sum_{2 \leq k \leq \log_2 x} \vartheta(x^{1/k}) \\ &= \psi(x) - \vartheta(x) \end{aligned}$$

Hence, all comments as above apply to the Chebyshev functions of a particular progression as well.

## 1.3 The von Mangoldt Function

We are now in a position to define the von Mangoldt function. This function is the weight by which the $\psi$-function had been defined, above. In other words,

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some } p \in \mathcal{P} \text{ and } k \in \mathbb{Z}^+ \\ 0 & \text{otherwise} \end{cases}$$

Thus we have

$$\psi(x;q,a) = \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \Lambda(n)$$

The reason $\Lambda(n)$ is used is because it arises naturally in the Dirichlet series of the logarithmic derivative of the Riemann Zeta function. The Riemann Zeta function is defined as

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

which is absolutely convergent for $\Re(s) > 1$. In this same region, it can be shown that

$$-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

The following identity is equivalent to the above Dirichlet series equality, and can be interpreted as an analytic statement of the fundamental theorem of arithmetic.

**Theorem 1.3.** *For any $n \in \mathbb{N}$,*

$$\log n = \sum_{d|n} \Lambda(d)$$

*Proof.* By the fundamental theorem,

$$n = \prod_{p^a||n} p^a$$

Hence, taking logarithms both sides

$$\begin{aligned} \log n &= \sum_{p^a||n} a \log p \\ &= \sum_{p^a||n} \sum_{k \leq a} \log p \\ &= \sum_{p^k|n} \log p \\ &= \sum_{d|n} \Lambda(d) \end{aligned}$$

where the last equality follows from the definition.

□

This theorem gives another example of how $\Lambda(n)$ can arise naturally in situations involving divisibility.

# Chapter 2

# Dirichlet Characters and Ramanujan Sums

Virtually any discussion regarding multiplicative structure in arithmetic progressions must depend in some way on the concept of Dirichlet characters. In this chapter, we will introduce Dirichlet characters and associated mathematical furniture and prove some theorems about them we will be using in our exposition.

## 2.1 Definition

A Dirichlet character $\chi$ is an extension of a character of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ into one on the entirety of $\mathbb{Z}$.

Suppose $(G, \cdot)$ is a finite abelian group. Then a function $e : G \to \mathbb{T}$ is called a character if, for all $a, b \in G$

$$e(a \cdot b) = e(a)e(b)$$

or, in other words, $e$ is a group homomorphism from $G$ to $\mathbb{T}$. The character given by $e(a) = 1$ for all $a \in G$ is called the "trivial character".

Now, fix an integer $q$. For any character of $(\mathbb{Z}/q\mathbb{Z})^\times$, we can create a corresponding *Dirichlet character modulo* $q$, $\chi : \mathbb{Z} \to \mathbb{C}$ as follows:

$$\chi(n) = \begin{cases} e(n) & \text{if } n \in (\mathbb{Z}/q\mathbb{Z})^\times \\ 0 & \text{otherwise} \end{cases}$$

In other words, $\chi$ is supported on the integers coprime to $q$ and is essentially the same as $e$ at these points. The unique Dirichlet character associated with the trivial character is called the *principal character* and is denoted as $\chi_0$. All other characters are known as *non-principal characters*.

The reader should verify that $\chi$ is completely multiplicative (ie, $\chi(mn) = \chi(m)\chi(n)$ for all integers $m$ and $n$) and periodic with period $q$. It can be shown that, in fact, any completely multiplicative function on $\mathbb{N}$ which is periodic with minimal period $q$ which does not vanish everywhere is actually a Dirichlet character modulo $q$.

We can then show the following orthogonality equation, that we will use throughout implicitly.

**Theorem 2.1** (Orthogonality of Dirichlet Characters, $\star$)**.** *For any fixed integer $q$, if $\chi$ and $\chi_1$ are two Dirichlet characters modulo $q$, then*

$$\sum_{a \bmod q} \chi(a)\overline{\chi_1(a)} = \begin{cases} \varphi(q) & \text{if } \chi = \chi_1 \\ 0 & \text{if } \chi \neq \chi_1 \end{cases}$$

*where the summation is over any complete residue class of integers modulo $q$. Furthermore, if $\chi$ is some Dirichlet characters modulo $q$ and $a$ and $b$ are integers coprime to $q$, then*

$$\sum_{\chi \bmod q} \chi(a)\overline{\chi(b)} = \begin{cases} \varphi(q) & \text{if } a \equiv b \pmod q \\ 0 & \text{otherwise} \end{cases}$$

We omit the proofs of the above theorem. The interested reader can find a proof in any book on analytic number theory, such as say [**?**] or [**?**].

## 2.2 The Twisted $\psi$ Function

We are now in a position the twisted $\psi$-function, which is essentially Chebyshev's $\psi$-function, "twisted" by a factor of $\chi(n)$ for some Dirichlet character

$\chi$ modulo $q$. That is, we define the summatory function $\psi(x;\chi)$ for a Dirichlet character $\chi$ as follows:

$$\psi(x;\chi) = \sum_{n \leq x} \chi(n)\Lambda(n)$$

Now, clearly, like $\psi(x)$ and unlike $\psi(x;q,a)$, this function is a sum over all integers up to a given quantity and is not restricted at all in terms of which congruence class the integer lies in. This is thus much easier to handle in principle. This now shows the application of the orthogonality of Dirichlet characters - they can be used to "pick out" elements in a particular congruence class and convert a sum over them into one over all integers. In particular, a basic sum interchange combined with orthogonality can be used to easily establish the following identities

$$\psi(x;q,a) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(a)}\psi(x;\chi)$$

$$\psi(x;\chi) = \sum_{a=1}^{q} \chi(a)\psi(x;q,a)$$

Thus information about $\psi$ for all Dirichlet characters modulo $q$ can be converted into information about congrunce classes modulo $q$, and vice-versa.

## 2.3 The Generalized Riemann Hypothesis and Error Terms

We are now in a position to pin-point exactly how the Generalized Riemann Hypothesis enters into the proof. GRH is a statement about the nature of the non-trivial zeroes of the L-functions associated with the Dirichlet characters. In particular, for a Dirichlet character $\chi$, we define $L(s,\chi)$ for $\Re(s) > 1$ as follows:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

This function can then be analytically continued onto the entire complex plane, with potentially at most one pole (this occurs when $\chi$ is the principal character). The GRH states that any zero of $L(s,\chi)$ with $\Re(s) \geq 0$ must in fact satisfy $0 < \Re(s) < 1$.

It can be shown that there is an intimate connection between the the twisted $\psi$ function, and the zeroes of the L-function. In particular, one can show the following theorem.

**Theorem 2.2.** *(Corrollary of GRH, $\star$) Under the Generalized Riemann Hypothesis, if $\chi$ is a non-principal character, then*

$$\sum_{n \leq x} \chi(n)\Lambda(n) \ll x^{1/2} \log^2 x$$

Relatedly the GRH for principal characters (or in fact, the regular Riemann Hypothesis for the $\zeta$ function given by $\zeta(s) = L(s,1)$) gives the following result.

**Theorem 2.3.** *(Corrollary of RH, $\star$) Under the Riemann Hypothesis, if $\chi$ is a principal character, then*

$$\begin{aligned} \sum_{n \leq x} \chi(n)\Lambda(n) &= \sum_{n \leq x} \Lambda(n) + \mathcal{O}(\log^2 qx) \\ &= x + \mathcal{O}(x^{1/2} \log^2 qx) \end{aligned}$$

Combining the two, and using the orthogonality of Dirichlet characters, it easily follows that for $x \geq q$,

$$\psi(x; q, a) = \frac{x}{\varphi(q)} + \mathcal{O}(x^{1/2} \log^2 x)$$

This shall be the input of GRH/RH in our proof.

## 2.4 Gauss Sums

The Dirichlet characters can be interpreted as an orthogonal basis of the function space on $(\mathbb{Z}/q\mathbb{Z})^\times$), with respect to a particular inner product.

However, another possible orthogonal basis can be created from $e(a/q) = e^{\frac{2\pi ia}{q}}$. These are in some sense "additive" characters, where Dirichlet characters are "multiplicative". It is strikingly clear that the additive characters are much easier to handle in certain settings than multiplicative characters, and thus we wish for some medium by which we can easily translate between the two. This is done primarily by the Gauss sum

$$\tau(\chi) = \sum_{a=1}^{q} \chi(a)e(a/q)$$

This can be thought of as the above inner product applied on additive and multiplicative characters, respectively.

We will need the following lemmata regarding Gauss sums.

**Lemma 2.1** ($\star$)**.** *Let $\chi$ be a Dirichlet character modulo $q$. Then,*

$$|\tau(\chi)|^2 \leq \sqrt{q}$$

**Lemma 2.2.** *Let $\chi_0$ be the principal Dirichlet character modulo $q$. Then,*

$$\tau(\chi_0) = \mu(q)$$

*where $\mu(q)$ is the Moebius function.*

*Proof.* We have the identity that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

which can easily be shown by noting the multiplicativity of both sides and then evaluating on prime powers.

Thus,

$$\begin{aligned}\tau(\chi_0) &= \sum_{n\in\mathbb{Z}/q\mathbb{Z}} \chi_0(n) e\left(\frac{n}{q}\right) \\ &= \sum_{\substack{n\in\mathbb{Z}/q\mathbb{Z} \\ (n,q)=1}} e\left(\frac{n}{q}\right) \\ &= \sum_{n\in\mathbb{Z}/q\mathbb{Z}} \sum_{d|(n,q)} \mu(d) e\left(\frac{n}{q}\right)\end{aligned}$$

Letting $n = dm$, we get

$$\tau(\chi_0) = \sum_{d|q} \mu(d) \sum_{m=1}^{q/d} e\left(\frac{md}{q}\right)$$

Now, note that the inner sum is a sum over all the roots of unity modulo $q/d$, and is hence zero unless $d = q$. Hence we get that

$$\tau(\chi_0) = \mu(d)$$

□

## 2.5 Ramanujan Sums

The Ramanujan sums, $c_q(n)$ are defined as follows

$$c_q(n) = \sum_{\substack{a\in\mathbb{Z}/q\mathbb{Z} \\ (a,q)=1}} e\left(\frac{an}{q}\right)$$

Let $*$ be the Dirichlet convolution defined by

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a) g(b)$$

It is an important exercise to show that the set of all $\mathbb{C}$-valued functions over $\mathbb{N}$ forms a ring with with this operation and pointwise addition. In particular, the unity is

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Thus, clearly, the earlier identity about the Moebius function devolves to

$$1 * \mu = \delta$$

Convolving $c_q(n)$ under the $q$ variable with 1 we get that

$$=$$

$$\begin{aligned} 1(q) * c_q(n) &= \sum_{d|q} c_{\frac{q}{d}}(n) \\ &= \sum_{d|q} \sum_{\substack{a \in \mathbb{Z}/q\mathbb{Z} \\ (a,q/d)=1}} e\left(\frac{adn}{q}\right) \end{aligned}$$

Replacing $a$ by $ad$

$$\begin{aligned} 1(q) * c_q(n) &= \sum_{d|q} \sum_{\substack{a \in \mathbb{Z}/q\mathbb{Z} \\ (a,q)=d}} e\left(\frac{an}{q}\right) \\ &= \sum_{a \in \mathbb{Z}/q\mathbb{Z}} e\left(\frac{an}{q}\right) \\ &= \begin{cases} q & \text{if } q|n \\ 0 & \text{otherwise} \end{cases} \\ &= q1_{q|n}(q) \end{aligned}$$

Convolving both sides by $\mu$, and using $1 * \mu = \delta$,

$$c_q(n) = \sum_{d|q} d 1_{d|n} \mu\left(\frac{q}{d}\right)$$

Thus we get

$$c_q(n) = \sum_{d|(q,n)} d\mu\left(\frac{q}{d}\right)$$

It is now easy to see that $c_q(n)$ is multiplicative in $q$. Further, we can evaluate it at prime powers as follows (assuming $p^\alpha || n$, that is, it is the highest power of $p$ to divide $n$)

$$c_{p^\beta}(n) = \sum_{i=0}^{\alpha} p^i \mu(p^{\beta-i}) = \begin{cases} p^\beta - p^{\beta-1} & \text{if } \beta \leq \alpha \\ -p^\alpha & \text{if } \beta = \alpha + 1 \\ 0 \text{ otherwise} & \end{cases}$$

We now move on to the actual statement of Vinogradov's theorem.

# Chapter 3

# Vinogradov's Theorem

With the background we have established, we can now state Vinogradov's actual theorem. The essential idea is to consider a function $R(N)$ as follows

$$R(N) = \sum_{p_1+p_2+p_3=N} 1$$

where the sum runs over all triplets of primes that sum to $N$.

If we can show that R(N) is bounded away from 0 for large enough $N$, then we have established Vinogradov's theorem. However, as with the prime-counting function, the function $R(N)$ is intractable. Instead, we replace it with the function $r(N)$ given by

$$r(N) = \sum_{n_1+n_2+n_3=N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)$$

In fact, the theorem we shall prove is the following

**Theorem 3.1** (Vinogradov's Theorem)**.** *Let $A > 0$ be any large enough real number. Then,*

$$r(N) = \frac{N^2}{2}\mathfrak{G}(N) + \mathcal{O}_A\left(\frac{N^2}{\log^A N}\right)$$

*where*

$$\mathfrak{G}(N) = \prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right)$$

Now note that if $N$ is even, then one of $n_1, n_2, n_3$ must be even (and in fact, a power of 2, as the sum is supported on prime powers). Thus,

$$\begin{aligned} r(N) &= \sum_{2^k+n_2+n_3=N} \Lambda(2^k)\Lambda(n_2)\Lambda(n_3) \\ &\leq \log^3 N \sum_{2^k+n_2+n_3=N} 1 \\ &\leq \log^3 N \sum_{2^k\leq N} \sum_{n_2+n_3=N-2^k} 1 \\ &\leq N \log^3 N \sum_{2^k\leq N} 1 \\ &= \mathcal{O}(N \log^4 N) \end{aligned}$$

Which is a much strong bound than we obtain from Vinogradov's theorem (note that $\mathfrak{G}(N) = 0$ if $2|N$, hence Vinogradov's theorem reduces to the error term bound). Thus, Vinogradov's theorem is only a useful result for $N$ odd.

We will now show how the statement of Vinogradov's theorem given above leads to the asymptotic form of the odd Goldbach conjecture.

## 3.1 Establishing the Asymptotic Goldbach

Essentially, we will show that the sum

$$r'(N) = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3$$

diverges to infinity as $N \to \infty$, thus establishing that the sum is non-zero for large enough $N$. In particular, this means that the condition $p_1+p_2+p_3 = N$ shall be satisfied for some triplet of primes for large enough $N$.

To see this, first note that for $N$ odd,

$$\prod_{p\neq 2}\left(1-\frac{1}{(p-1)^2}\right)\leq \mathfrak{G}(N)\leq \prod_{p}\left(1+\frac{1}{(p-1)^3}\right)$$

Thus, in particular, $r(N)\gg N^2$.

Further note that

$$r(N)-r'(N)=\sum_{n_1+n_2+n_3=N}^{*}\Lambda(n_1)\Lambda(n_2)\Lambda(n_3)$$

where the $*$ denotes that at least one of $n_1, n_2, n_3$ is not prime. It is easy to see due to symmetry that

$$\begin{aligned}
r(N)-r'(N) &\leq 3\sum_{\substack{p^k+n_2+n_3=N\\ k\geq 2}}\Lambda(p^k)\Lambda(n_2)\Lambda(n_3)\\
&\leq 3\log^2 N\sum_{\substack{p^k+n_2+n_3=N\\ k\geq 2}}\Lambda(p^k)\\
&\leq 3\log^2 N\sum_{\substack{p^k\leq N\\ k\geq 2}}\log p\sum_{n_2+n_3=N-p^k}1\\
&\leq 3N\log^2 N\sum_{\substack{p^k\leq N\\ k\geq 2}}\log p\\
&= 3N\log^2 N\sum_{k\geq 2}\vartheta(N^{1/k})\\
&\leq 3N\log^2 N\sum_{2\leq k\leq \log_2 N}\vartheta(N^{1/k})\\
&= \mathcal{O}(N^{3/2}\log^4 N)
\end{aligned}$$

where we have used the bound on $\vartheta$ that we derived in the first chapter.

Thus,

$$r'(N)=r(N)+\mathcal{O}(N^{3/2}\log^4 N\gg N^2$$

establishing what we wish.

## 3.2 Setting up the Proof: The Hardy-Littlewood Circle Method

We shall now set up the proof via the Hardy-Littlewood Circle Method. To do this, we shall define an auxillary function as follows

$$f(\alpha) = \sum_{n \leq N} \Lambda(n) e(n\alpha)$$

Here there is a dependence on the parameter $N$ that we have suppressed in the notation. Note that $\alpha \in \mathbb{R}/\mathbb{Z}$ is uniquely determined upto difference by integers. We have the following theorem,

**Theorem 3.2.** *With $f$ as given above, we have that*

$$r(N) = \int_0^1 f(\alpha)^3 e(-N\alpha) d\alpha = \int_{\mathbb{R}/\mathbb{Z}} f(\alpha)^3 e(-N\alpha) d\alpha$$

*Proof.* Let

$$r(k, N) = \sum_{\substack{n_1+n_2+n_3=k \\ n_1,n_2,n_3 \leq N}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)$$

It is easy to see that

$$r(k, N) = \begin{cases} r(k) & k \leq N \\ 0 & k \to \infty \end{cases}$$

Now,

$$\begin{aligned} f(\alpha)^3 &= f(\alpha) \times f(\alpha) \times f(\alpha) \\ &= \sum_{n_1,n_2,n_3 \leq N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) e\left((n_1+n_2+n_3)\alpha\right) \\ &= \sum_k e(k\alpha) \left( \sum_{\substack{n_1+n_2+n_3=k \\ n_1,n_2,n_3 \leq N}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) \right) \\ &= \sum_k r(k,N) e(k\alpha) \end{aligned}$$

Now note that the final sum is a finite Fourier series. Hence we can use the inversion formula to get that

$$r(N) = r(N,N) = \int_0^1 f(\alpha)^3 e(-N\alpha) d\alpha$$

Thus,

$$r(N) = \int_{\mathbb{R}/\mathbb{Z}} f(\alpha)^3 e(-N\alpha) d\alpha$$

□

The crux of the circle method is to realize that the major contribution to the integral comes from points that are "close" to rational numbers in a certain sense. More explicitly, let $P$ and $Q$ be two integers (to be fixed later). Let $\mathcal{F}_P$ be the sequence of Farey fractions of denominator $\leq P$. For $a/q \in \mathcal{F}_P$ (such that $a$ and $q$ are co-prime), define

$$\mathfrak{M}(a/q) = \mathfrak{M}(a,q) = \left\{ \alpha \in \mathbb{R}/\mathbb{Z} : \left| \alpha - \frac{a}{q} \right| \leq \frac{1}{qQ} \right\}$$

We now define

$$\mathfrak{M} = \cup_{a/q \in \mathcal{F}_p} \mathfrak{M}(a,q)$$

and

$$\mathfrak{m} = (\mathbb{R}/\mathbb{Z})\backslash\mathfrak{M}$$

as respectively the "Major Arcs" and the "Minor Arcs". The major arcs will give the main term, along with some error, while the minor arcs will contribute wholly to the error term.

# Chapter 4

# Major Arcs and Minor Arcs

In this chapter, we will finish the proof of Vinogradov's theorem by doing the necessary calculations for the major arcs and the minor arcs.

We proceed by proving a sequence of lemmata.

**Lemma 4.1.** *Let $a/q \in \mathfrak{P}$. Then, assuming GRH,*

$$\sum_{n\leq x} \Lambda(n)e(na/q) = \frac{\mu(q)}{\varphi(q)}x + \mathcal{O}(\sqrt{qx}\log^2 x)$$

*Proof.* We have

$$\sum_{n\leq x} \Lambda(n)e(na/q) = \sum_{\substack{n\leq x \\ (n,q)=1}} \Lambda(n)e(na/q) + \mathcal{O}(\log^2 x)$$

Now, with $(an, q) = 1$, and using the orthogonality of Dirichlet characters, we have that

$$e(an/q) = \frac{1}{\varphi(q)} \sum_{b\in\mathbb{Z}/q\mathbb{Z}} \sum_{\chi \pmod q} \chi(b)\overline{\chi(an)}e(b/q) = \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi(an)}\tau(\chi)$$

Thus we get that

$$\sum_{n\leq x}\Lambda(n)e(na/q)=\frac{1}{\varphi(q)}\sum_{\chi \pmod q}\overline{\chi(a)}\tau(\chi)\psi(x,\overline{\chi})+\mathcal{O}(\log^2 x)$$

Now, applying the bound on *psi* from GRH for non-trivial $\chi$, and the bound on $\tau$ obtained in the second chapter, we get that the non-trivial characters contribute $\ll \sqrt{qx}\log^2 x$.

By the bound from RH from the second chapter, we get that the trivial character contributes

$$\frac{1}{\varphi(q)}\tau(\chi_0)(x+\mathcal{O}(\sqrt{x}\log^x)=\frac{\mu(q)}{\varphi(q)}(x+\mathcal{O}(\sqrt{x}\log^2 x)$$

which completes the proof of the lemma.

□

**Lemma 4.2.** *Let $a/q\in\mathfrak{P}$, $\alpha=a/q+\beta$. Then, assuming GRH,*

$$f(\alpha)=\frac{\mu(q)}{\varphi(q)}\int_0^N e(\beta x)dx+\mathcal{O}\left((1+|\beta|N)\sqrt{qN}\log^2 N\right)$$

*Proof.* Note that,

$$f(\alpha)=\int_0^N e(x\beta)d\left(\sum_{n\leq x}\Lambda(n)e(an/q)\right)$$

This can be shown easily by integrating by parts. Now, by using the previous lemma with $E(x,a/q)$ as the error term,

$$f(\alpha)=\int_0^N e(x\beta)d\left(\frac{\mu(q)}{\varphi(q)}x+E(x,a/q)\right)$$

The first term here gives the main term of the lemma. Applying integration by parts on the second term, we get

$$E(N,a/q)e(N\beta)-\int_0^N 2\pi i\beta e(x\beta)E(x,a/q)dx$$

Using $E(x, a/q) = \mathcal{O}(\sqrt{(}qx)\log^2 x)$ and computing the integral, we get the error term from the lemma.

This establishes the lemma.

□

**Lemma 4.3.** *Let $a/q \in \mathfrak{P}$. $\alpha \in \mathfrak{M}(a,q)$, $q \leq Q$ and $Q = N^{2/3}$. Then, assuming GRH,*

$$f(\alpha) \ll \frac{N}{\varphi(q)} + N^{\frac{5}{6}+\epsilon}$$

*Proof.* We apply the previous lemma, by noting that $\beta = \frac{1}{qQ}$, and taking the maximum possible value for the integral to get

$$f(\alpha) \ll \frac{N}{\varphi(q)} + \left(1 + \frac{N}{qQ}\right)\sqrt{qN}\log^2 N \ll \frac{N}{\varphi(q)} + \left(\sqrt{(}QN) + \frac{N^{3/2}}{Q}\right)\log^2 N$$

It is now easy to see that $Q = N^{2/3}$ is optimal, giving the desired lemma.

□

We now set $P = \log^{10} N$

## 4.1 Minor Arc Contribution

We can now calculate the minor arc contribution as follows.

**Theorem 4.1.** *For some $A > 0$,*

$$\int_{\mathfrak{m}} |f(\alpha)|^3 d\alpha \ll \frac{N^2}{\log^A N}$$

*Proof.* We have that $q > \log^{10} N$, and hence $\varphi(q) \geq \log^9 N$. Thus, by the previous lemma, on the minor arcs we have that

$$f(\alpha) \ll \frac{N}{\log^9 N}$$

Hence,

$$\int_{\mathfrak{m}} |f(\alpha)|^3 d\alpha \ll \frac{N}{\log^9 N} \int_0^1 |f(\alpha)|^2 d\alpha$$

Now,

$$\int_0^1 |f(\alpha)|^2 d\alpha = \int_0^1 \sum_{n_1,n_2 \leq N} \Lambda(n_1)\Lambda(n_2) e\left((n_1 - n_2)\alpha\right) d\alpha = \sum_{n \leq N} \Lambda(n)^2 \ll N \log^2 N$$

This establishes our theorem

□

## 4.2 Major Arc Contribution

We now calculate the major arc contribution as follows.

**Theorem 4.2.** *For all large enough $A > 0$,*

$$\int_{\mathfrak{M}} f(\alpha)^3 e(-N\alpha) d\alpha = \frac{N^2}{2} \sum_{q=1}^{\infty} \frac{\mu(q)^3}{\varphi(q)^3} c_q(N) + \mathcal{O}\left(\frac{N^2}{\log^A N}\right)$$

*Proof.* We have that

$$\int_{\mathfrak{M}} f(\alpha)^3 e(-N\alpha) d\alpha = \sum_{q \leq P} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \int_{-1/(qQ)}^{1/(qQ)} f(a/q + \beta)^3 e(-N(a/q + \beta)) d\beta$$

Applying lemma 4.2,

$$f(a/q+\beta)^3 = \frac{\mu(q)^3}{\varphi(q)^3} \left(\int_0^N e(\beta x) dx\right)^3 + \mathcal{O}\left(\frac{1}{\varphi(q)^2} \min\left(N^2, \frac{1}{|\beta|^2}\right) (1 + |\beta|N|) \sqrt{qN} \log^2(qN) + (1 + |\beta|$$

We can see with a little calulation that the error term is within the bound prescribed by the theorem.

Therefore, the main term of the major arc contribution is

$$\sum_{q\leq P}\frac{\mu(q)^3}{\phi(q)^3}\left(\sum_{\substack{1\leq a\leq q\\(a,q)=1}}e(-Na/q)\right)\left(\int_{-1/(qQ)}^{1/(qQ)}\left(\int_0^N e(\beta x)dx\right)^3 e(-N\beta)d\beta\right)$$

Now, making the substitution $x = Ny$ and $N\beta = \xi$ in the integrals, we can evaluate the integral to be

$$N^2\int_{-N/(qQ)}^{N/(qQ)}\left(\int_0^1 e(y\xi)dy\right)^3 e(-\xi)d\xi = N^2\left(\int_{-\infty}^{\infty}\left(\int_0^1 e(y\xi)dy\right)^3 e(-\xi)d\xi + \mathcal{O}\left(\frac{(qQ)^2}{N^2}\right)\right)$$

This gives

$$\frac{N^2}{2} + \mathcal{O}((qQ)^2)$$

Discarding the error term as it is acceptable, we get the main term

$$\frac{N^2}{2}\sum_{q\leq P}\frac{\mu(q)^3}{\phi(q)^3}\left(\sum_{\substack{1\leq a\leq q\\(a,q)=1}}e(-Na/q)\right)$$

The inner sum is the Ramanujan sum $c_q(N) \leq \varphi(q)$, thus extending the outer sum to infinity will induce an error of at most $N^2\sum_{q>P}\mu(q)^2/\varphi(q)^2 \ll N^2(\log N)^{-10}$ which is acceptable. This establishes our theorem.

□

Now note that the sum is multiplicative, and hence we can write down its Euler product. Using the fact that $\mu(p^k) = 0$ for $k > 2$, and the values of $c_{p^\beta}(n)$ that we calculated in chapter 2, we get that the sum is in fact equal to $\mathfrak{G}(N)$.

This establishes Vinogradov's theorem under the Generalized Riemann Hypothesis.

# Part II

# MTH599A: Prime Numbers and Arithmetic Progressions

**Abstract**

One of the most important aspects of the distribution of prime numbers among the integers is the distribution of the prime numbers within the various congruence classes modulo some given integer $q$ - in other words, the distribution of prime numbers in an infinite arithmetic progression. The most basic question about this distribution is the following: for given numbers $a$ and $q$, what is the number of primes in the congruence class containing $a$ modulo $q$? This question was answered by Dirichlet's theorem, the first result in analytic number theory, and a discussion by the author regarding this theorem can be found at [6].

A lot more is known about the distribution of prime numbers in arithmetic progressions in modern times; in fact, these statistics (in the form of strong results such as the Siegel-Walfisz theorem and the Bombieri-A.I. Vinogradov theorem) are essential tools in many modern results in analytic (especially additive) number theory, including the I.M. Vinogradov theorem regarding the ternary Goldbach conjecture and Yitang Zhang's recent theorem regarding gaps between primes.

In particular, the classical (relatively) qualitative result in this context is a generalization of Dirichlet's theorem and the Prime Number Theorem, into what is called the Prime Number Theorem for Arithmetic Progressions. In this project report, we consider a proof the PNT for APs, and discuss various generalizations and their applications. For most of the proof, we assume undergraduate proficiency in complex analysis, as well as Chapters 0, 1, 2 and 3 and parts of Chapter 4 from [5]. We will follow Chapters 5, 6 and 7 of [5] for our proof.

Similar project work has been done by the author in past discussion on the Bombieri-A.I. Vinogradov theorem [7], Dirichlet's theorem [6], and the I.M. Vinogradov theorem [8].

# Notation

We shall describe here the notation that we will need from analytic number theory.

We shall use the Landau notation

$$f(x) = \mathcal{O}(g(x))$$

equivalently with $f \ll g$ and $g \gg f$to mean that there exists some positive constant $C$ such that $|f(x)| \leq Cg(x)$ for sufficiently large $x$. Such an estimate is called a "big-oh estimate". We may index our notation with a variable to denote that the implicit constant depends on the variable in question, and is only constant when that variable is held constant.

We use

$$f(x) = o(g(x))$$

to mean that $f(x)/g(x) \to 0$ as $x \to \infty$. Such an estimate is called a "little-oh estimate", and being $o(g(x))$ is strictly stronger than being $\mathcal{O}(g(x))$. However, little-oh estimates are qualitative statements, and not very good for calculation. Hence, in practice, one always use more precise big-oh estimates for calculation (ie, with a smaller $g(x)$) and only return to the little-oh estimate in the last step to give a neater but strictly weaker estimate in the end, if at all. (See for example, the Prime Number Theorem). We may index here as well, as above.

We will often write

$$f(x) = g(x) + \mathcal{O}(h(x)) \text{ or } f(x) = g(x) + o(h(x))$$

to mean that there exists a function $p(x)$ which is respectively $= \mathcal{O}(h(x))$ or $= o(h(x))$ such that $f(x) = g(x) + p(x)$.

Finally we use

$$f(x) \sim g(x)$$

interchangeably with

$$f(x) = g(x) + o(g(x))$$

to denote the asymptotic equality $f(x)/g(x) \to 1$ as $x \to \infty$.

We use $(a, b)$ to denote the greatest common divisor of $a$ and $b$ and $\varphi(n)$ for Euler's totient function,

$$\varphi(n) = \#\{x \in \mathbb{Z} : 1 \leq x \leq n, (x, n) = 1\}$$

For any $A \subset \mathbb{Z}$, we use $1_A(n)$ for its indicator function,

$$1_A(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{otherwise} \end{cases}$$

We use $p_n$ for the $n$th prime number. Furthermore, for us, $n$ will always be an integer, $p$ will always be prime, and $\mathcal{P}$ shall denote the set of prime numbers.

For summations and products, we shall use the standard practice of specifying the variable over which the operation is taking place under the $\sum$ or $\prod$ as well as specifying the other conditions the variable needs to satisfy. Furthermore, sums over $p$ are over primes and sums over $n$ are over positive integers. This may lead to sums of the form

$$\sum_{n \leq x}, \sum_{p \leq x}, \sum_{p|m}, \sum_{n|m}, \sum_{\chi \bmod q}$$

and so on, which are respectively sums over positive integers up to $x$, primes up to $x$, all prime divisors of $m$, all divisors of $m$, and all Dirichlet character modulo $q$.

Unless otherwise specified, all Dirichlet characters are modulo $q$.

A $\star$ will be used to denote any theorem which has not been proved in this report.

# Contents

# Chapter 5

# Introduction

## 5.1 The Prime Number Theorem for Arithmetic Progressions

One of the, if not **the** central question in analytic number theory is that of the distribution of prime numbers among the positive integers. The "macrostructure" of this distribution is normally studied by examining the *prime-counting function* $\pi(x)$ given by

$$\pi(x) = \sum_{p \leq x} 1$$

where the summation is over primes less than or equal to $x$, and trying to determine its asymptotic behaviour as $x \to \infty$. One of the early achievements of analytic methods in number theory was the *Prime Number Theorem* (PNT) proved independently by Hadamard and de la Valle-Poussin, which gives an asymptotic formula for $\pi(x)$ which says

$$\pi(x) \sim \frac{x}{\log x}$$

Another question of much importance in number theory is the distribution of prime numbers within arithmetic progressions. Information about this distribution can be used to prove a plethora of interesting facts about the

prime numbers. Another early result (perhaps the seminal result in analytic number theory) proven by Dirichlet states that if

$$\pi(x;q,a) = \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} 1$$

is the number of primes less than $x$ in a given congruence class modulo $q$ and further suppose that $(a,q) = 1$ (that is, $a$ is *coprime* to $q$), then $\pi(x;q,a) \to \infty$ as $x \to \infty$.

If $(a,q) \neq 1$, there are obviously only finitely many primes in the congruence class containing $a$, since $p \equiv a \pmod{q}$ implies that any prime which divides both $a$ and $q$ must divide $p$. Thus, if $(a,q) > 1$ then the only primes which can be in the congruence class are the ones divisible by $(a,q)$. If $(a,q)$ is composite, then there are zero such primes, and if $(a,q)$ is prime there is one such prime, and hence the number of primes in this congruence class is finite. Trivially, thus, any arithmetic progression has infinitely many primes if and only if the first term and common difference are coprime. This is known as "Dirichlet's theorem on primes in arithmetic progressions".

Looking at the previous two results, a natural question to ask is a more precise estimate of exactly how many prime numbers there are in a particular arithmetic progression; that is, an estimate for $\pi(x;q,a)$ similar to the PNT's estimate for $\pi(x)$. *A priori*, there is no reason to assume that the primes will be more inclined to being concentrated in one co-prime congruence class modulo $q$ than the others. In fact, there is at least one great conjecture (now settled, see [4]) which suggests otherwise - the ternary Goldbach conjecture asserts that any odd prime greater than 5 can be expressed as the sum of three prime numbers. Suppose that the primes are more in the congruence class congruent to 1 than congruent to 2 modulo 3. This means that the sum of three primes is more likely to be 0 modulo 3 than it is to be 1 or 2, suggesting that the Goldbach conjecture is false. While this is not a rigorous argument, it gives an indication as to why the PNT for APs could potentially be useful in proving the ternary Goldbach conjecture (and in fact, a partial statement towards the Goldbach conjecture, which is the I.M. Vinogrdov theorem crucially depends on a strong form of the PNT for APs - that is, a form with an explicit error term rather than just a qualitative asymptotic equivalence).

Thus, we would expect that all co-prime congruence classes should roughly

have the "same" number of primes. Since there are $\varphi(q)$ many such congruence classes we would expect that for some fixed $a$ and sufficiently large $x$, $\pi(x;q,a)$ should roughly be $\pi(x)/\varphi(q)$. This turns out to be true, and is known as the PNT for APs. Precisely, this states that

$$\pi(x;q,a) \sim \frac{\pi(x)}{\varphi(q)} \sim \frac{1}{\varphi(q)} \frac{x}{\log x}$$

This quantitative version of Dirichlet's theorem is known as the "Prime Number Theorem for arithmetic progressions".

While this is a deep theorem, the asymptotically equality is not sufficient and we need more information about the error in this theorem. We can write the above estimate as

$$\pi(x;q,a) = \frac{1}{\varphi(q)} \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

Where $o()$ is the little-oh asymptotic notation. The goal of many results is to replace the error term with a more precise big-oh estimate. In particular, the Generalized Riemann Hypothesis provides an improved estimate (this is, in fact, one of the major reasons why GRH is such an important conjecture).

We shall now elaborate on an alternative way to state these theorems that is much more natural to use and prove.

## 5.2 Chebyshev's $\vartheta$ and $\psi$ Functions

It turns out that the prime-counting function $\pi(x;q,a)$ is very difficult to use in proofs. Instead, it has been typical since Chebyshev to replace them by the theta and psi functions, $\vartheta(x;q,a)$ and $\psi(x;q,a)$.

An alternative way to write $\pi$ is the following:

$$\pi(x;q;a) = \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} 1_{\mathcal{P}}(n)$$

Where $1_A(n)$ is the indicator function of a set of integers $A$. Thus, $\pi$ can be interpreted as a weighted sum over all elements in a congruence class with

the prime elements weighted with 1 and the composite elements weighted with 0.

However, it turns out that this method of weighting is not ideal for proving results. Instead, a better weight is the von Mangoldt function, which we shall define presently. We thus consider instead the sum

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \Lambda(n)$$

where $\Lambda(n)$ is the more appropriate weight, the von Mangoldt function.

In this and the subsequent section we will provide a recipe for turning results about one of the above weighted sums to the other, and try to establish why the second sum is better suited for manipulation.

One way to motivate this is the following. Clearly, by PNT

$$\frac{\pi(x) \log x}{x} = 1 + o(1)$$

Taking natural logarithms both sides

$$\log \pi(x) - \log x + \log \log x = \log(1 + o(1)) = o(1)$$

where the last equality is easily established.[1] Now, if $x = p_n$, the $n$th prime number, then clearly $\pi(x) = n$. Thus we have

$$\log n - \log p_n + \log \log p_n = o(1)$$

Noting that $\log \log x = o(\log x)$, we thus get

$$\log n = \log p_n + o(\log p_n)$$

Or, in other words,

$$\log n \sim \log p_n$$

[1] As the logarithm is continuous at 1, if $f(x) = o(1)$, then $\lim_{x \to \infty} f(x) = 0$. Thus $\lim_{x \to \infty} \log(1+f(x)) = \log\left(1 + \lim_{x \to \infty} f(x)\right) = \log(1) = 0$. Hence, clearly, $\log(1+o(1)) = o(1)$.

This suggests that if instead of giving all primes the same weight 1, we weight them by their logarithm, the higher primes would contribute more, multiplying a rough factor of a logarithm. We can formalize this heuristic by a partial summation[2] argument.

Thus, we define a new function, called the Chebyshev $\vartheta$-function in the literature as follows

$$\vartheta(x) = \sum_{p \leq x} \log p$$

which weights each prime by their logarithm instead of 1.

As mentioned above, using partial summation, we can establish the following two identities

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt$$

$$\vartheta(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt$$

Using these, we can convert any estimate on the first function into one of the second, and vice-versa.

In particular, it is easily shown that

$$\lim_{x \to \infty} \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = \lim_{x \to \infty} \frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt = 0$$

which shows that PNT is equivalent to $\vartheta(x) \sim x$. In any case, the first identity can be used to change any estimate for $\vartheta$ to one for $\pi$.

Analogous to the prime-counting function for progressions, $\pi(x; q, a)$, we can define a $\vartheta(x; q, a)$ for progressions as follows

$$\vartheta(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \log p$$

[2]See Appendix

The above identities can then be proved in exactly the same way by replacing $\pi(x)$ with $\pi(x;q,a)$ and $\vartheta(x)$ with $\vartheta(x;q,a)$.

In some sense, it is natural to work with logarithms of primes when working with weighted sums. Primes are essentially multiplicative objects, and the logarithm allows one to pass from the multiplicative to the additive, and thus form a natural candidate for dealing with sums over primes. However, it turns out even weighting all primes by their logarithms and all composites by 0 does not give the most convenient form. The most convenient form is given instead by Chebyshev's $\psi$-function,

$$\psi(x) = \sum_{p^k \leq x} \log p$$

where the sum is over all primes $p$ and all positive integers $k$ such that $p^k \leq x$. In other words, we weight all prime powers by the logarithm of the prime of which they are a power, and all other numbers by 0. The hope then, is that since the prime powers contribute a smaller amount than the primes, the contribution from them can be controlled.

Clearly,

$$\psi(x) = \sum_{k=1}^{\infty} \sum_{p^k \leq x} \log p = \sum_{k=1}^{\infty} \sum_{p \leq \sqrt[k]{x}} \log p = \sum_{k=1}^{\infty} \vartheta(x^{1/k})$$

Here note that since for a fixed positive $x$, $\lim_{k\to\infty} x^{1/k} = 1$ thus for sufficiently large $k$, $x^{1/k} < 2$, and thus $\vartheta(x^{1/k}) = 0$. Thus, all but finitely many terms vanish, and in particular, the terms are non-vanishing if and only if $x^{\frac{1}{k}} \geq 2$. Taking logarithm to the base 2 on both sides, we see this is the same as requiring $k \leq \log_2 x$.

Thus,

$$\psi(x) = \sum_{k \leq \log_2 x} \vartheta(x^{\frac{1}{k}})$$

Now, trivially, $\vartheta(x) = \sum_{p\leq x} \log p \leq \sum_{p\leq x} \log x \leq x \log x$. Also, we know that $\vartheta(x)$ is increasing and thus, $\vartheta(x^{1/2}) \geq \vartheta(x^{1/k})$ for $k \geq 2$. With this we can see that

$$\begin{aligned}
\psi(x) - \vartheta(x) &= \sum_{2 \le k \le \log_2 x} \vartheta(x^{1/k}) \\
&\le \sum_{2 \le k \le \log_2 x} \vartheta(x^{1/2}) \\
&\le \vartheta(x^{1/2}) \log_2 x \\
&\le x^{1/2} (\log_2 x)(\log x^{\frac{1}{2}}) \\
&= O\left(x^{1/2} (\log x)^2\right)
\end{aligned}$$

Thus, any estimate for $\psi$ can be converted into an estimate for $\vartheta$, provided the estimate has an error larger than $\mathcal{O}(\sqrt{x})$ by at least two logarithmic factors. In particular, since logarithms always grow slower than powers, for any $\epsilon > 0$, an error of the form $\mathcal{O}(x^{1/2+\epsilon})$ can be tolerated. This is much tighter than most bounds we have, and thus in any theorem we shall prove here, $\psi$ may be interchanged with $\vartheta$ and vice-versa. This also means that the PNT is equivalent to $\psi(x) \sim x$. Using the bound $\vartheta(x) = \mathcal{O}(x)$, which is substantially weaker than PNT and was proven by Chebyshev using elementary methods, we can sharpen the estimate to $\psi(x) - \vartheta(x) = \mathcal{O}(\sqrt{x})$.[3]

Identically to $\pi$ and $\vartheta$, we define $\psi(x; q, a)$

$$\psi(x; q, a) = \sum_{\substack{p^k \le x \\ p^k \equiv a \bmod q}} \log p$$

Furthermore, as above

$$\psi(x; q, a) = \sum_{k \le \log_2 x} \vartheta(x^{1/k}; q, a)$$

and thus,

[3] Clearly

$$\psi(x) - \vartheta(x) = \vartheta(x^{1/2}) + \sum_{k=3}^{\lfloor \log_2 x \rfloor} \vartheta(x^{1/k}) \le \vartheta(x^{1/2}) + \vartheta(x^{1/3}) \log_2 x = \mathcal{O}(x^{1/2})$$

$$\begin{aligned}\psi(x;q,a) - \vartheta(x;q,a) &= \sum_{2\leq k\leq \log_2 x} \vartheta(x^{\frac{1}{k}};q,a) \\ &\leq \sum_{2\leq k\leq \log_2 x} \vartheta(x^{1/k}) \\ &= \psi(x) - \vartheta(x)\end{aligned}$$

Hence, all comments as above apply to the Chebyshev functions of a particular progression as well.

## 5.3 The von Mangoldt Function

We are now in a position to define the von Mangoldt function. This function is the weight by which the $\psi$-function had been defined, above. In other words,

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some } p \in \mathcal{P} \text{ and } k \in \mathbb{Z}^+ \\ 0 & \text{otherwise} \end{cases}$$

Thus we have

$$\psi(x;q,a) = \sum_{\substack{n\leq x \\ n\equiv a \bmod q}} \Lambda(n)$$

The reason $\Lambda(n)$ is used is because it arises naturally in the Dirichlet series of the logarithmic derivative of the Riemann Zeta function. The Riemann Zeta function is defined as

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

which is absolutely convergent for $\Re(s) > 1$. In this same region, it can be shown that

$$-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

The following identity is equivalent to the above Dirichlet series equality, and can be interpreted as an analytic statement of the fundamental theorem of arithmetic.

**Theorem 5.1.** *For any $n \in \mathbb{N}$,*

$$\log n = \sum_{d|n} \Lambda(d)$$

*Proof.* By the fundamental theorem,

$$n = \prod_{p^a||n} p^a$$

Hence, taking logarithms both sides

$$\begin{aligned} \log n &= \sum_{p^a||n} a \log p \\ &= \sum_{p^a||n} \sum_{k \le a} \log p \\ &= \sum_{p^k|n} \log p \\ &= \sum_{d|n} \Lambda(d) \end{aligned}$$

where the last equality follows from the definition.

□

This theorem gives another example of how $\Lambda(n)$ can arise naturally in situations involving divisibility.

We will arrange the rest of the report in the following manner. We will first prove Dirichlet's theorem and the regular PNT, developing the means to

doing so while we do that in Chapter 2 and Chapter 3 respectively. Then, in Chapter 4, we will combine the two proofs to prove the PNT for APs, and finally in Chapter 5 we will talk about generalizations and applications.

# Chapter 6

# Dirichlet's Theorem

The discussion in this Chapter has been adapted from [6].

The proof by Dirichlet of the infinitude of primes in arithmetic progressions is a generalization of a proof by Euler for Euclid's theorem (that is, that there are infinitely many primes). Before presenting either of the proofs, we will develop the mathematical machinery of Dirichlet characters, which will allow us to perform this generalization.

Virtually any discussion regarding multiplicative structure in arithmetic progressions must depend in some way on the concept of Dirichlet characters.

## 6.1 Definition of a Dirichlet Character

A Dirichlet character $\chi$ is an extension of a character of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ into one on the entirety of $\mathbb{Z}$.

Suppose $(G, \cdot)$ is a finite abelian group. Then a function $e : G \to \mathbb{T}$ is called a character if, for all $a, b \in G$

$$e(a \cdot b) = e(a)e(b)$$

or, in other words, $e$ is a group homomorphism from $G$ to $\mathbb{T}$. The character given by $e(a) = 1$ for all $a \in G$ is called the "trivial character".

Now, fix an integer $q$. For any character of $(\mathbb{Z}/q\mathbb{Z})^\times$, we can create a corresponding *Dirichlet character modulo* $q$, $\chi : \mathbb{Z} \to \mathbb{C}$ as follows:

$$\chi(n) = \begin{cases} e(n) & \text{if } n \in (\mathbb{Z}/q\mathbb{Z})^\times \\ 0 & \text{otherwise} \end{cases}$$

In other words, $\chi$ is supported on the integers coprime to $q$ and is essentially the same as $e$ at these points. The unique Dirichlet character associated with the trivial character is called the *principal character* and is denoted as $\chi_0$. All other characters are known as *non-principal characters*.

The reader should verify that $\chi$ is completely multiplicative (ie, $\chi(mn) = \chi(m)\chi(n)$ for all integers $m$ and $n$) and periodic with period $q$. It can be shown that, in fact, any completely multiplicative function on $\mathbb{N}$ which is periodic with minimal period $q$ which does not vanish everywhere is actually a Dirichlet character modulo some $q$.

We can then show the following orthogonality equation, that we will use throughout implicitly.

**Theorem 6.1** (Orthogonality of Dirichlet Characters, $\star$)**.** *For any fixed integer $q$, if $\chi$ and $\chi_1$ are two Dirichlet characters modulo $q$, then*

$$\sum_{a \bmod q} \chi(a)\overline{\chi_1(a)} = \begin{cases} \varphi(q) & \text{if } \chi = \chi_1 \\ 0 & \text{if } \chi \neq \chi_1 \end{cases}$$

*where the summation is over any complete residue class of integers modulo $q$. Furthermore, if $\chi$ is some Dirichlet characters modulo $q$ and $a$ and $b$ are integers coprime to $q$, then*

$$\sum_{\chi \bmod q} \chi(a)\overline{\chi(b)} = \begin{cases} \varphi(q) & \text{if } a \equiv b \pmod q \\ 0 & \text{otherwise} \end{cases}$$

We omit the proofs of the above theorem. The interested reader can find a proof in any book on analytic number theory or in the report [6].

## 6.2 Euler's Proof for Euclid's Theorem

We now move to a proof of Euclid's theorem due to Euler that encapsulate many ideas that shall be used in our proof of Dirichlet's theorem. Euclid's theorem, which states that there are infinitely many prime numbers has a elementary proof known since classical times. However, Euler provided an "analytical" proof of the theorem. He considered the limit

$$\lim_{s\to 1^+} \sum_p \frac{1}{p^s}$$

where the sum is over all primes $p$, and showed that this limit is $\infty$. If there were only finitely many primes, then this would not be possible, hence proving the infinitude of primes.

We will now prove that the limit above is actually $\infty$.

### 6.2.1 The Riemann Zeta Function

For any real number $s > 1$, we define the Riemann zeta function,

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

We can see this function converges by noting that

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{n^s} \leq 1 + \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{x^s} = 1 + \int_1^{\infty} \frac{dx}{x^s}$$

Thus,

$$\zeta(s) \leq 1 + \frac{1}{s-1}$$

is convergent for all $s > 1$.

The zeta function encodes in it a lot of information about the distribution of primes among the integers. In particular, it can be extended to a holomorphic function on the entire complex plane except for $s = 1$, where it

has a simple pole. The distribution of zeroes of this extensison is intimately connected to the distribution of primes and the Riemann Hypothesis, one of the biggest unsolved problems in mathematics is a statement about these zeroes.

### 6.2.2 Euler Product

Notwithstanding the holomorphic extension, the zeta function we have defined itself encodes a lot about the primes. In particular, the zeta function admits a product formula which is essentially an analytic statement of the fundamental theorem of arithmetic. This product formula, known as the Euler product of $\zeta(s)$ is given in the following theorem.

**Theorem 6.2.** *For every $s > 1$,*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - 1/p^s}$$

*where the product is over all primes $p$.*

*Proof.* Suppose $M$ and $N$ are positive integers such that $M > N$. Every $n \leq N$ can be uniquely written as a product of primes. These primes shall obviously be $\leq N$, and cannot occur more than $M$ times in the product. Hence, it follows that every term in the left of the following inequality shall also be in the right of the inequality. That is,

$$\sum_{n=1}^{N} \frac{1}{n^s} \leq \prod_{p \leq N} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{Ms}}\right)$$

Taking first $M \to \infty$ and then $N \to \infty$ in the left, we get

$$\sum_{n=1}^{N} \frac{1}{n^s} \leq \prod_{p} \left(\frac{1}{1 - p^{-s}}\right)$$

Finally, taking $N \to \infty$,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leq \prod_{p} \left( \frac{1}{1-p^{-s}} \right)$$

For the reverse inequality, note that if we consider all products of primes such that each prime is $\leq N$ and does not occur more than $M$ times, we shall get finitely many distinct integers. Thus,

$$\prod_{p \leq N} \left( 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{Ms}} \right) \leq \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Again, taking $M \to \infty$ and then $N \to \infty$, we obtain

$$\prod_{p} \left( \frac{1}{1-p^{-s}} \right) \leq \sum_{n=1}^{\infty} \frac{1}{n^s}$$

The equality follows from these two inequalites. □

### 6.2.3 Proof of Euclid's Theorem

We are now in a position to prove Euclid's theorem.

**Theorem 6.3.** *We have,*

$$\lim_{s \to 1^+} \sum_{p} \frac{1}{p^s} = \infty$$

*where the sum is taken over all primes $p$.*

*Proof.* Taking the natural logarithm of both sides of the Euler product, and using the continuity of logarithms,

$$-\sum_{p} \log \left( 1 - \frac{1}{p^s} \right) = \log \zeta(s)$$

Since $\log(1+x) = x + \mathcal{O}(x^2)$, we get,

$$-\sum_p \left[-\frac{1}{p^s} + O\left(\frac{1}{p^{2s}}\right)\right] = \log \zeta(s)$$

Thus, since $\sum_p 1/p^{2s} \leq \sum_n 1/n^{2s}$, which is convergent, and hence bounded,

$$\sum_p \frac{1}{p^s} + \mathcal{O}(1) = \log \zeta(s)$$

Now, $\zeta(s) \geq \sum_{n=1}^{M} 1/n^s$ for every $M$. Hence,

$$\liminf_{s \to 1^+} \zeta(s) \geq \sum_{n=1}^{M} \frac{1}{n}$$

for every $M$. Clearly, since the harmonic series diverges, the right side is unbounded. Thus, $\lim_{s \to 1^+} \zeta(s) = \infty$.

Combining this with the earlier estimate on $\sum_p 1/p^s$, we get that

$$\lim_{s \to 1^+} \sum_p \frac{1}{p^s} = \infty$$

□

## 6.3 Proof Sketch

In this section, we will connect the previous two sections to give a sketch of our proof of Dirichlet's theorem. Please refer to [6] for information about characters of finite abelian groups.

Now, we shall adapt our theorems for groups characters to Dirichlet characters.

**Theorem 6.4.** *For any non-trivial Dirichlet character modulo $q$, we have*

$$\sum_{n=1}^{q} \chi(n) = 0$$

*Proof.* Since $\chi(n) = 0$ if $(n, q) > 1$, we have

$$\sum_{n=1}^{q} \chi(n) = \sum_{\substack{1 \leq n \leq q \\ (a,q)=1}} \chi(n) = \sum_{\substack{1 \leq n \leq q \\ (a,q)=1}} e([n]) = \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} e(a)$$

Where the last equality follows from the fact that $n$ varies over the given domain, $[n]$ goes traverses all the elements of $(\mathbb{Z}/q\mathbb{Z})^\times$. Thus invoking the fact about group characters that $\sum_{a \in G} e(a) = 0$, we get

$$\sum_{n=1}^{q} \chi(n) = 0$$

□

We now state and prove the final property of Dirichlet characters that we shall need.

**Theorem 6.5.** *For any non-principal Dirichlet character $\chi$, and any integer $k$, we have*

$$\left| \sum_{n \leq k} \chi(n) \right| \leq q$$

*Proof.* Clearly, by previous theorems and the periodicity of $\chi$, if we write $k = aq + b$, with $b < q$

$$\sum_{n \leq k} \chi(n) = \sum_{n \leq aq} \chi(n) + \sum_{aq < n \leq aq+b} \chi(n) = \sum_{n \leq b} \chi(n)$$

Thus, by the triangle inequality,

$$\left| \sum_{n \leq k} \chi(n) \right| \leq \sum_{n \leq b} |\chi(n)| \leq b \leq q$$

□

### 6.3.1 Adapting Euler's Proof of Euclid's Theorem

We can now see how Euler's proof for Eulcid's theorem may be adapted here. Fix integers $q$ and $a$ such that $(a, q) = 1$. We consider the following limit

$$\lim_{s \to 1^+} \sum_{p \equiv a \pmod{q}} \frac{1}{p^s}$$

where the sum is now only over all primes in the same congruence class as $a$ modulo $q$. Our attempt shall be to show that this limit is $\infty$, which would, analogous to Euclid's theorem, show that there are infinitely many primes in that congruence class.

As stated before, sums over elements in a particular congruence class are normally intractable. However, using a trick, we can reduce these sums to over all prime $p$.

Now, since $(a, q) = 1$, we have that

$$\frac{1}{\phi(q)} \sum_{\chi} \chi(p)\overline{\chi(a)} = \begin{cases} 1 & \text{if } p \equiv a \pmod{q} \\ 0 & \text{otherwise} \end{cases}$$

Hence, we can rewrite the sum as

$$\sum_{p \equiv a \pmod{q}} \frac{1}{p^s} = \sum_{p} \frac{1}{\phi(q)} \sum_{\chi} \frac{\chi(p)\overline{\chi(a)}}{p^s}$$

Since everything converges uniformly and absolutely for $s > s_0 > 1$, we can rewrite this as

$$\sum_{p \equiv a \pmod{q}} \frac{1}{p^s} = \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \sum_{p} \frac{\chi(p)}{p^s}$$

Hence, it suffices to study the behaviour of $\sum_p \chi(p)/p^s$ as $s \to 1^+$.

Now, the sum can be rewritten as

$$\sum_{p \equiv a \pmod q} \frac{1}{p^s} = \frac{1}{\phi(q)} \sum_p \frac{\chi_0(p)}{p^s} + \frac{1}{\phi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^s}$$

where the second sum is over non-prinicipal characters.

Clearly,

$$\sum_p \frac{\chi_0(p)}{p^s} = \sum_{p \nmid q} \frac{1}{p^s}$$

Since there are only finitely many primes dividing $q$, this last sum goes to infinity as $s \to 1^+$, as in the proof of Euclid's theorem. Thus, if we show that as $s \to 1^+$, the non-principal part is bounded (that is, $\sum_p \chi(p)/p^s = \mathcal{O}_q(1)$),the theorem is proved.

Hence, we see that by careful use of Dirichlet characters, we have reduced our problem to a sum over all primes $p$.

### 6.3.2 Sketch of the Proof

We shall now sketch a proof of the fact that for non-principal characters, $\sum_p \chi(p)/p^s = \mathcal{O}(1)$ as $s \to 1^+$. This shall be similar to the proof of Euclid's theorem, using the zeta function.

In place of $\zeta(s)$, we will consider a generalization associated with each character $\chi$ called the Dirichlet L-function, $L(s, \chi)$, given by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

wherever the series converges.

Similar to $\zeta(s)$, there exists an Euler product formula for $L(s, \chi)$ viz.

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)/p^s}$$

Taking logarithms on both sides, we get

$$\log L(s,\chi) = -\sum_p \log\left(1 - \frac{\chi(p)}{p^s}\right)$$

Using $\log(1+x) = x + \mathcal{O}(x^2)$,

$$\log L(s,\chi) = -\sum_p \left[-\frac{\chi(p)}{p^s} + O\left(\frac{1}{p^{2s}}\right)\right]$$

Thus, we get

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + \mathcal{O}(1)$$

Hence, if $L(1,\chi)$ is finite and non-zero, and $L(s,\chi)$ is continuous, then the left of this equation will be bounded as $s \to 1^+$, and hence $\sum_p \chi(p)/p^s$ is bounded.

In the above argument, there are several holes we need to fill to make the argument rigorous. Firstly, we need to prove the product formula for $L(s,\chi)$; secondly, since the numbers involved may, in general, be complex numbers, we need to clearly define the branch of the logarithm we are using and its properties; thirdly, we need to show that $L(s,\chi)$ is continuous at $s = 1$; and finally, we need to show that $L(1,\chi) \neq 0$.

## 6.4 Filling the Holes: Reducing to $L(1,\chi) \neq 0$

### 6.4.1 The First Logarithm

We define our first logarithm, $\log_1$ as

$$\log_1\left(\frac{1}{1-z}\right) = \sum_{k=1}^{\infty} \frac{z^k}{k}$$

for $|z| < 1$. Clearly in the chosen domain, this function converges absolutely.

**Theorem 6.6.** *If $|z| < 1$, then*

$$e^{\log_1\left(\frac{1}{1-z}\right)} = \frac{1}{1-z}$$

*Proof.* Let $z = re^{i\theta}$. Note that it is sufficient to show that $(1-re^{i\theta})e^{\sum_{k=1}^{\infty}(re^{i\theta})^k)/k}$ is constant (since putting $r = 0$ gives 1, as it should).

Thus, differentiating this we get

$$\left[-e^{i\theta} + (1 - re^{i\theta})e^{i\theta}\left(\sum_{k=1}^{\infty}(re^{i\theta})^{k-1}\right)\right] e^{\sum_{k=1}^{\infty}(re^{i\theta})^k)/k}$$

A quick calculation using the sum of an infinite geometric series shows that the term in the square brackets is zero, hence we are done. □

### 6.4.2 Euler Product

We now prove the Euler product for $L(s, \chi)$.

**Theorem 6.7.** *For any character $\chi$ and $s > 1$,*

$$L(s,\chi) = \sum_n \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)/p^s}$$

*Proof.* Clearly, the product converges since $\sum_p \chi(p)/p^s$ converges. Let us represent the sum over positive integeres by $\Sigma$ and the product as $\Pi$. Further, define

$$\Sigma_N = \sum_{n \le N} \frac{\chi(n)}{n^s}$$

$$\Pi_N = \prod_{p \le N}\left(\frac{1}{1 - \chi(p)/p^s}\right)$$

$$\Pi_{N,M} = \prod_{p \le N}\left(1 + \frac{\chi(p)}{p^s} + \cdots + \frac{\chi(p^M)}{p^{Ms}}\right)$$

Now, fix $\epsilon > 0$. Clearly, since the product is finite, $\lim_{M\to\infty} \Pi_{N,M} = \Pi_N$. Furthermore, since the sum and product converge, $\lim_{N\to\infty} \Pi_N = \Pi$ and $\lim_{N\to\infty} \Sigma_N = \Sigma$. Hence, we can choose $N$ and $M$ large enough that

$$|\Pi_{N,M} - \Pi_N| < \epsilon$$

$$|\Pi_N - \Pi| < \epsilon$$

$$|\Sigma_N - \Sigma| < \epsilon$$

Furthermore, by the fundamental theorem of arithmetic, and the multiplicativity of the Dirichlet characters, for large enough $M$, $\Pi_{M,N} - \Sigma_N$ is the tail end of a convergent series, and can thus be made $< \epsilon$.

Hence,

$$|\Sigma - \Pi| \leq |\Sigma_N - \Sigma| + |\Pi_{M,N} - \Sigma_N| + |\Pi_{N,M} - \Pi_N| + |\Pi_N - \Pi| < 4\epsilon$$

for any $\epsilon > 0$. Thus, clearly $\Sigma = \Pi$. □

### 6.4.3 Behaviour of $L(s, \chi)$

In this section, we examine the behaviour of $L(s, \chi)$.

**Theorem 6.8.** *If $\chi_0$ is the principal character modulo $q$, then*

$$L(s, \chi_0) = \zeta(s) \prod_{p|q} \left(1 - \frac{1}{p^s}\right)$$

*where the product is over all primes $p$ dividing $q$.*

*Proof.* This trivially follows from the Euler products of the two sides.

□

Thus, in some sense, the behaviour of the L-function associated with the principal Dirichlet character is the same as the zeta function. For non-principal characters, the situation is very different.

**Theorem 6.9.** *If $\chi$ is a non-principal character, then $L(s,\chi)$ exists for $s > 0$. Moreover, it is continuously differentiable for $0 < s < \infty$, and there exists constants $c, c' > 0$ such that as $s \to \infty$*

$$L(s,\chi) = 1 + \mathcal{O}(e^{-cs})$$

$$L'(s,\chi) = \mathcal{O}(e^{-c's})$$

*Proof.* Suppose $s > 0$. Using summation by parts[1]

$$\sum_{n \leq N} \frac{\chi(n)}{n^s} = \frac{1}{N^s} \sum_{n \leq N} \chi(n) + \int_0^N \left( \sum_{n \leq x} \chi(n) \right) \left( \frac{-s}{x^{s+1}} \right) dx$$

Note that since $\left| \sum_{n \leq N} \chi(n) \right| \leq q$, the first term goes to zero as $N \to \infty$. Furthermore, the integral is bounded above by the integral $\int \frac{qs}{x^{s+1}} dx$, which clearly converges for $s + 1 > 1$ (that is $s > 0$) when $N \to \infty$. Hence, the partial sums of the series converges, and hence $L(s,\chi)$ exists for $s > 0$. Furthermore, the series converges uniformly for $s > \sigma > 0$. We can apply a similar argument to show that the term-wise derivative also converges uniformly for $s > \sigma > 0$, proving that $L(s,\chi)$ is continuously differentiable.

□

With this, we can now define our second logarithm.

### 6.4.4 The Second Logarithm

We define our second logarithm, $\log_2$ as

$$\log_2 L(s,\chi) = -\int_s^\infty \frac{L'(t,\chi)}{L(t,\chi)} dt$$

[1] See appendices

**Theorem 6.10.** *If $s > 1$,*

$$e^{\log_2 L(s,\chi)} = L(s,\chi)$$

*Proof.* Differentiating $e^{-\log_2 L(s,\chi)} L(s,\chi)$ with respect to $s$, we get

$$-\frac{L'(s,\chi)}{L(s,\chi)} e^{-\log_2 L(s,\chi)} L(s,\chi) + e^{-\log_2 L(s,\chi)} L'(s,\chi) = 0$$

Hence $e^{-\log_2 L(s,\chi)} L(s,\chi)$ is constant. Taking $s \to \infty$, this is easily seen to be 1. □

We can now connect our two logarithms to show that we can meaningfully "take logarithms on both sides" of the Euler product for $L(s,\chi)$.

**Theorem 6.11.** *If $s > 1$,*

$$\log_2 L(s,\chi) = \sum_p \log_1 \left( \frac{1}{1 - \chi(p)/p^s} \right)$$

*Proof.* We see that

$$e^{\sum_p \log_1 \left( \frac{1}{1-\chi(p)/p^s} \right)} = \prod_p e^{\log_1 \left( \frac{1}{1-\chi(p)/p^s} \right)} = \prod_p \left( \frac{1}{1 - \chi(p)/p^s} \right)$$

The right most quantity is, by the Euler product, $L(s,\chi)$.

Also,

$$e^{\log_2 L(s,\chi)} = L(s,\chi)$$

Hence, since their exponential is the same, they must differ by some integer multiple of $2\pi$. That is,

$$\log_2 L(s,\chi) - \sum_p \log_1 \left( \frac{1}{1 - \chi(p)/p^s} \right) = 2\pi M(s)$$

Now, clearly, the left side of the equality is a continuous function of $s$. Hence, $M(s)$ is an integer valued continuous function, and thus constant. Taking $s \to \infty$, this is clearly 0.

□

Putting all of this together, the proof sketch given earlier can be formalized by filling the holes in the argument with these patches.

Therefore, to prove this theorem, we need to establish that $L(1, \chi) \neq 0$.

## 6.5 The Non-vanishing of the L-function

We shall now prove that $L(1, \chi) \neq 0$ for all non-principal Dirichlet characters. We shall distinguish between two types of characters. If a character $\chi$ is always real, (that is $\chi(n) = 0, +1, -1$ or, to put it another way $\chi(n) = \overline{\chi(n)}$), we call it a real character. An equivalent characterization of a real character is that it is a character $\chi$ such that $\chi^2 = \chi_0$. A character which is not a real character is called a complex character. We shall treat these two separately.

### 6.5.1 Complex Characters

Suppose $\chi_1$ is a complex Dirichlet character such that $L(1, \chi_1) = 0$. We will now derive a contradiction.

For $s > 1$, define $f$ as follows

$$f(s) = \prod_{\chi} L(s, \chi)$$

where the product is taken over all Dirichlet characters modulo $q$.

**Theorem 6.12.** *If $s > 1$, $f(s)$ is real-valued, and furthermore*

$$f(s) \geq 1$$

*Proof.* We know that

$$L(s,\chi) = \exp\left(\sum_p \log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right)$$

Hence,

$$\prod_\chi L(s,\chi) = \exp\left(\sum_\chi \sum_p \log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right)$$

Now, using the definition of $\log_1$ and the multiplicativity of $\chi$,

$$\prod_\chi L(s,\chi) = \exp\left(\sum_\chi \sum_p \sum_{k=1}^{\infty} \frac{1}{k}\frac{\chi(p^k)}{p^{ks}}\right)$$

Now, we can rearrange the summation to get

$$\prod_\chi L(s,\chi) = \exp\left(\sum_p \sum_{k=1}^{\infty} \frac{1}{kp^{ks}} \sum_\chi \chi(p^k)\right)$$

However, from a previous theorem we know that $\sum_\chi \chi(n)$ is either 0 or $\phi(q)$, and thus is a real non-negative quantity. Hence, the term in the exponential shall be a sum over non-negative quantities and, thus non-negative. This implies that its exponential shall be real and greater than 1.

□

Now we know that $L(1,\chi_1) = 0$, that is $L(s,\chi_1)$ has a zero of order at least 1. Hence, to compensate for that, some other L-function in the product must be diverging to infinity. We know that $L(s,\chi_0)$ has a pole of order 1 at $s = 1$, since $\zeta(s)$ has a pole of order 1. However, if $L(1,\chi_1) = 0$, then $L(1,\overline{\chi_1}) = \overline{L(1,\chi_1)} = 0$, and hence, $L(1,\overline{\chi_1})$ also has a zero of order at least 1 at $s = 1$. However, these are all distinct terms in the product, and no other term in the product can diverge to infinity (since we have show that for non-principal characters, their L-functions are well-defined and bounded at $s = 1$). Hence, the product $f(s)$ has a zero of at least order 1 at $s = 1$, contradicting the above theorem.

The above contradiction shall yield that no complex character can satisfy $L(1,\chi_1) = 0$. Note that the above proof does not work for real characters

as for them $\chi = \overline{\chi}$, and thus we can only show that one L-function in the product vanishes, which is not sufficient to make the entire product vanish.

We formalize the above argument in the following theorems.

**Theorem 6.13.** *If $L(1, \chi_1) = 0$ then $L(1, \overline{\chi_1}) = 0$.*

*Proof.* It is easy to see from their definitions that $L(1, \overline{\chi_1}) = \overline{L(1, \chi_1)}$, from which the claim follows.

□

**Theorem 6.14.** *If $\chi$ is a non-principal character, such that $L(1, \chi) = 0$, then*

$$L(s, \chi) = \mathcal{O}(s - 1)$$

*as $s \to 1$.*

*Proof.* Applying the mean-value theorem on $L(s, \chi)$ in $1 \leq s \leq 2$, we get that for some $t \in (1, s)$

$$L(s, \chi) - L(1, \chi) = L'(t, \chi)\,(s - 1)$$

Now note that $|L'(s, \chi)|$ is continuous and thus has a maximum (say $C$) on $[1, 2]$. Furthermore, $L(1, \chi) = 0$.

Hence for $1 \leq s \leq 2$,

$$|L(s, \chi)| \leq C|s - 1|$$

proving the claim.

□

**Theorem 6.15.** *For the principal Dirichlet character $\chi_0$, we have*

$$L(s, \chi_0) = O\left(\frac{1}{s - 1}\right)$$

*as $s \to 1$.*

*Proof.* We know that

$$L(s, \chi_0) = \zeta(s) \prod_{p|q} \left(1 - \frac{1}{p^s}\right)$$

Also, clearly as $s \to 1$, the terms in the product are $O(1)$.

However, we have shown earlier that for $s > 1$

$$\zeta(s) < 1 + \frac{1}{s-1}$$

Putting this together, clearly $L(s, \chi_0) = \mathcal{O}(1/(s-1))$.

□

**Theorem 6.16.** *For any complex character $\chi_1$, $L(1, \chi_1) \neq 0$.*

*Proof.* We know that for $\chi$ ($\neq \chi_0, \chi_1, \overline{\chi_1}$), $L(s, \chi)$ exists and is bounded. That is $L(s, \chi) = \mathcal{O}(1)$ as $s \to 1$. Now,

$$f(s) = \prod_{\chi} L(s, \chi) = L(s, \chi_0) L(s, \chi_1) L(s, \overline{\chi_1}) \prod_{\chi \neq \chi_0, \chi_1, \overline{\chi_1}} L(s, \chi)$$

Therefore, by our theorems

$$f(s) = O\left(\frac{1}{s-1}\right) \times \mathcal{O}(s-1) \times \mathcal{O}(s-1) \times \mathcal{O}(1) = \mathcal{O}(s-1)$$

Therefore, at $s = 1$, $f(s) = 0 < 1$, contradicting our previous theorem.

□

### 6.5.2 Real Characters

We now move on to the final, and the deepest part of this theorem, the proof that for real characters $\chi$, $L(1, \chi) \neq 0$.

Define $S(x)$ as follows

$$S(x) = \sum_{mn \leq x} \frac{\chi(n)}{(mn)^{1/2}}$$

We will obtain two different asymptotic formulae for $S(x)$ which shall establish our theorem.

Before that, we shall prove the facts we need to establish the formulae.

**Theorem 6.17.** *Suppose that $\chi$ is a real Dirichlet character and $n$ is any positive integer. Then,*

$$\sum_{d|n} \chi(d) \geq \begin{cases} 0 & \text{for all } n \\ 1 & \text{if } n = t^2, t \in \mathbb{Z} \end{cases}$$

*Proof.* Note that since $\chi$ is multiplicative absolutely,

$$\sum_{d|n} \chi(d) = \prod_{p^a || n} \left( \sum_{k=0}^{a} \chi(p^a) \right)$$

Where $p^a || n$ denotes that $p$ is a prime dividing $n$ such that $a$ is the largest exponent for which $p^a$ divides $n$.

Hence, clearly, it is sufficient to establish this fact for prime powers, to establish it in general.

Now for $n = p^a$, clearly,

$$\sum_{d|n} \chi(d) = \chi(1) + \chi(p) + \chi(p^2) + \cdots + \chi(p^a) = \chi(1) + \chi(p) + \chi(p)^2 + \cdots + \chi(p)^a$$

Clearly, since $\chi(p)$ is $0, 1, -1$,

$$\sum_{d|n} \chi(d) = \begin{cases} a+1 & \text{if } \chi(p) = 1 \\ 0 & \text{if } \chi(p) = -1 \text{ and } a \text{ is odd} \\ 1 & \text{if } \chi(p) = -1 \text{ and } a \text{ is even} \\ 1 & \text{if } \chi(p) = 0 \end{cases}$$

Thus, we see that this sum satisfies the inequality for prime powers, and thus for all positive integers.

□

With this, we can establish a lower bound on the growth rate of $S(x)$.

**Theorem 6.18.** *We have,*

$$S(x) \gg \log x$$

*In particular* $S(x) \to \infty$ *as* $x \to \infty$.

*Proof.* The defining formula of $S(x)$ can clearly be rewritten the following way,

$$S(x) = \sum_{n \leq x} \sum_{d|n} \frac{\chi(d)}{n^{1/2}}$$

where we have replaced $mn$ by $n$ and $n$ by $d$.

Hence, clearly

$$S(x) = \sum_{n \leq x} \frac{1}{n^{1/2}} \sum_{d|n} \chi(d)$$

Now, using the bound earlier established, we know the inner sum is greater than 0 always, and greater than 1 for square $n$. Hence,

$$S(x) \geq \sum_{\substack{n \leq x \\ n = t^2, t \in \mathbb{Z}}} \frac{1}{n^{1/2}}$$

Or, in other words,

$$S(x) \geq \sum_{t^2 \leq x} \frac{1}{t} = \sum_{t \leq x^{1/2}} \frac{1}{t} \gg \log x$$

□

We shall now use Dirichlet's hyperbola method[2] to prove an asymptotic formula for $S(x)$.

**Theorem 6.19.**

$$S(x) = 2x^{1/2}L(1,\chi) + \mathcal{O}(1)$$

*Proof.* Note that the defining formula for $S(x)$ can be written as follows

$$S(x) = \sum_{n\leq x}\sum_{d|n}\frac{\chi(d)}{d^{1/2}}\frac{1}{\left(\frac{n}{d}\right)^{1/2}}$$

Thus, taking $g(n) = \chi(n)/\sqrt{n}$, $h(n) = 1/\sqrt{n}$ and $y = \sqrt{x}$, in Dirichlet's hyperbola method,

$$S(x) = \sum_{d\leq\sqrt{x}}\frac{\chi(d)}{d^{1/2}}H\left(\frac{x}{d}\right) + \sum_{d\leq\sqrt{x}}\frac{1}{d^{1/2}}G\left(\frac{x}{d}\right) - G(\sqrt{x})H(\sqrt{x})$$

Where by partial summation[3],

$$G(x) = \sum_{n\leq x}\frac{\chi(n)}{n^{1/2}} = O\left(\frac{1}{x^{1/2}}\right)$$

and

$$H(x) = \sum_{n\leq x}\frac{1}{n^{1/2}} = 2\sqrt{x} + O\left(\frac{1}{x^{1/2}}\right) = \mathcal{O}(x^{1/2})$$

Therefore, $G(\sqrt{x})H(\sqrt{x}) = \mathcal{O}(1)$. Furthermore,

$$\sum_{d\leq\sqrt{x}}\frac{1}{d^{1/2}}G\left(\frac{x}{d}\right) = \sum_{d\leq\sqrt{x}}\frac{1}{d^{1/2}}\times O\left(\frac{1}{(x/d)^{1/2}}\right) = O\left(\sum_{d\leq\sqrt{x}}\frac{1}{d^{1/2}}\frac{d^{1/2}}{x^{1/2}}\right) = \mathcal{O}(1)$$

Hence the main term comes from the first part of the sum. That is,

[2]See appendix
[3]See appendix

$$\sum_{d\leq\sqrt{x}}\frac{\chi(d)}{d^{1/2}}H\left(\frac{x}{d}\right)=\sum_{d\leq\sqrt{x}}\frac{\chi(d)}{d^{1/2}}\left(2\frac{x^{1/2}}{d^{1/2}}+O\left(\frac{d^{1/2}}{x^{1/2}}\right)\right)$$

Now, note that the error term, when multiplied out evaluates to $O(\sum_{d\leq\sqrt{x}}\chi(d))=\mathcal{O}(1)$, by the previous bound on character sums.

Further, the main term evaluates to

$$2x^{1/2}\sum_{d\leq\sqrt{x}}\frac{\chi(d)}{d}$$

Now,

$$\sum_{d\leq\sqrt{x}}\frac{\chi(d)}{d}=\sum_{d=1}^{\infty}\frac{\chi(d)}{d}-\sum_{d>\sqrt{x}}\frac{\chi(d)}{d}=L(1,\chi)+O\left(\frac{1}{x^{1/2}}\right)$$

where the error term is obtained by partial summation. Thus,

$$2x^{1/2}\sum_{d\leq\sqrt{x}}\frac{\chi(d)}{d}=2x^{1/2}L(1,\chi)+\mathcal{O}(1)$$

Putting all the estimates together, we get

$$S(x)=2\sqrt{x}L(1,\chi)+\mathcal{O}(1)$$

□

This, estimate, together with the previously obtained lower bound are sufficient to establish the theorem. To see this, note that by the lower bound, $S(x)$ is unbounded as $x$ goes to infinity. Suppose $L(1,\chi)=0$. The estimate we have obtained then reduces to $S(x)=\mathcal{O}(1)$, contradicting the unboundedness of $S(x)$.

Putting all of this together, we have obtained Dirichlet's theorem.

# Chapter 7

# The Prime Number Theorem

The Prime Number Theorem, conjectured in some form by Gauss is one of the central results in analytic number theory. In this section, we will provide a proof of the theorem (which will later be generalized) - in most of this chapter we are adapting [5].

To prove the theorem, we will be making use of Tauberian theory. Tauberian theory is a general idea in analysis whereby when we know the expression of a function as a series or as an integral that converges, as well as appropriate control over the growth rates of the terms, as well as other regularity properties, then we may know more about the function or its terms. A classical, simple and real-analytic example of this is Abel's theorem regarding power series, which is the following:

**Theorem 7.1** (Abel's theorem, $\star$)**.** *Let $f(x) = \sum_{n\geq 1} a_n x^n$, with $a_n \in \mathbb{R}$ that converges on the real interval $(-1, 1)$, such that*

1. $$\lim_{x\to 1^-} f(x) = \alpha$$

2. $$\lim_{n\to\infty} na_n = 0$$

*then we have that $\sum_n a_n$ converges, and takes the value $\alpha$.*

Looking closely at the theorem, we have a function $f$ presented as a series, whose terms have desirable growth properties. Then, under this regularity we know that the limit of the function is actually equal to the sum of a series

associated with $f$. A theorem of the above nature is called a Tauberian theorem.

From the general Tauberian theory, there is a large body of research which is applicable to number theory through the PNT. We will state a Tauberian theorem that, after some work, will give us the PNT. Due to paucity of space, we will not present a proof of the theorem here, however a proof may be found in Chapter 6 of [5].

## 7.1 Tauberian Theorem

Let $f : \mathbb{N} \to \mathbb{C}$ be an arithmetical function. We define,

$$L_f(s) = \sum_{n \geq 1} \frac{f(n)}{n^s}$$

and

$$A_f(x) = \sum_{n \leq x} f(n)$$

**Theorem 7.2** (Tauberian Theorem for Dirichlet Series, $\star$)**.** *Let $f$, $L_f$ and $A_f$ as above be such that:*

1. *$f(n) \geq 0$ for all $n \in \mathbb{N}$*
2. *There exists a $\sigma \in \mathbb{R}$, such that $A_f(x) = \mathcal{O}(x^\sigma)$*
3. *$L_f$ converges for all complex $s$ such that $\Re(s) > \sigma$*
4. *If $S_f = \{s \in \mathbb{C} : \Re(s) \geq \sigma, s \neq \sigma\}$, then there exists an open set containing $S_f$ on which $L_f$ continues analytically so that*

$$\lim_{s \to \sigma} (s - \sigma) L_f(s) = \alpha$$

*then*

$$A_f(x) \sim \frac{\alpha}{\sigma} x^\sigma$$

We now make some generally useful remarks about this theorem. The first thing is to note that by a simple application of partial summation, 3 follows from 2, and 1 will typically be trivially true. Hence, it suffices to show 2 and 4, and hence deduce the asymptotic. Furthermore, 3 implies that $L_f$ is analytic wherever it converges, while 4 implies that $L_f$ has either a pole or a removable singularity at $s = \sigma$, with residue $\alpha$ (when it is a pole).

## 7.2 Satisfying the Conditions of the Tauberian Theorem

We will now choose an $f$ such that the Tauberian Theorem will imply PNT. The choice of $f$ is probably extremely natural, given all our preceding discussion. Define $f(n) = \Lambda(n)$, and take $\sigma = 1$. It is easy to see that $f$ is non-negative. Furthermore, it is clear by the definitions that $L_f = -\frac{\zeta'}{\zeta}$ and $A_f = \psi$. Now, 2 follows from the Chebyshev inequality that $\psi(x) = \mathcal{O}(x)$. Hence, it remains to continue it analytically to an open set containing $S_f$, and compute the desired residue.

Note that in any region where $\zeta$ is analytic and non-zero, $\frac{\zeta'}{\zeta}$ is well-defined, and hence analytic. Thus, to show that $L_f$ satisfies the hypotheses of the theorem, it suffices to show that on some open set containing $S_f$, $\zeta$ extends analytically such that $\zeta$ takes no zeroes on this set. This directly underlines the connection between zeroes of the Riemann zeta function and the distribution of prime numbers, and is suggestive of how questions of this type occur naturally in this context.

To do this, we apply partial summation as follows,

$$\sum_{n \leq x} \frac{1}{n^s} = \frac{\lfloor x \rfloor}{x^s} + s \int_1^x \frac{\lfloor t \rfloor}{t^{s+1}} dt$$

Now applying the formula $\lfloor x \rfloor = x - \{x\}$, we get that

$$\sum_{n \leq x} \frac{1}{n^s} = \frac{1}{x^{s-1}} - \frac{\{x\}}{x^s} + s \int_1^x \frac{dt}{t^s} - s \int_1^x \frac{t}{t^{s+1}} dt$$

Evaluating the first integral, and simplifying,

$$\sum_{n\leq x}\frac{1}{n^s}=\frac{1}{1-s}\times\frac{1}{x^{s-1}}+\frac{s}{s-1}-\frac{\{x\}}{x^s}-s\int_1^x\frac{\{t\}}{t^{s+1}}dt$$

Everything we've done till this point is unconditionally true. At this point, we assume that $\Re(s)>1$ and take the limit $x\to\infty$. Note that the integral is convergent in this region as well, and hence

$$\zeta(s)=\frac{s}{s-1}-s\int_1^\infty\frac{\{t\}}{t^{s+1}}$$

This identity holds for $\Re(s)>1$. At this point, note that the first term is analytic everywhere but $s=1$ where it has a simple pole of residue 1. Further, note that for $\Re(s)>0$, $\Re(s+1)>1$, and hence the integral converges absolutely. Thus, it follows that the second term is an analytic function for all $\Re(s)>0$. Thus, on the set $\{s\in\mathbb{C}:\Re(s)>0,s\neq 0\}$ the right hand side is analytic. However, since this is an analytic function that agrees with $\zeta$ on an open set, it follows that it is the unique analytic continuation of $\zeta$ to this set. Thus, we now need to show that on some open subset of this set, which still contains $S_f$, $\zeta$ is non-zero. To pursue this, we claim that *on* $S_f$ $\zeta$ is non-zero. Since $\zeta$ is a continuous function, it follows that there is an open set containing $S_f$ on which $\zeta$ is non-zero.

Further, note that as shown above,

$$\zeta(s)=\frac{1}{s-1}+g(s)$$

for some analytic function $g$ (as demonstrated by the integral representation. Using this, it is clear that

$$\zeta'(s)=-\frac{1}{(s-1)^2}+g'(s)$$

Thus,

$$-\frac{\zeta'}{\zeta}(s)=\frac{\frac{1}{(s-1)^2}-g'(s)}{\frac{1}{s-1}+g(s)}$$

And thus,

$$-\frac{\zeta'}{\zeta}(s) = \frac{\frac{1}{(s-1)} - (s-1)g'(s)}{1 + (s-1)g(s)}$$

It is now clear to see that $L_f$ has a pole at $s = \sigma = 1$, with residue $\alpha = 1$.

Hence, to prove that the hypotheses of the theorem hold, we need to show that $\zeta(s) \neq 0$ for $s \in S_f$. Now note that for $\Re(s) > 1$, $\zeta$ is given by a product representation by Euler, and hence cannot be 0. Thus, we now only need to consider $\zeta(1 + it)$, $t \neq 0$. If we can show that all of these are non-zero (and hence that there is no zero of the zeta function on the $\Re(s) = 1$ line), then we have shown the hypotheses of the Tauberian theorem, and hence, it's conclusion would follow, that is

$$\psi(x) = A_f(x) \sim \frac{\alpha}{\sigma} x^\sigma = x$$

proving the PNT. We now move on to the next section.

## 7.3 $\zeta(1 + it) \neq 0$ if $t \neq 0$

This part of the proof is truly ingenious, and was part of the original Hadamard and de la Valée Poussin proofs of the PNT. We have the following fact,

$$3 + 4\cos\theta + \cos 2\theta = 2(1 + \cos\theta)^2 \geq 0$$

Now let

$$F_t(s) = \zeta(s)^3 \zeta(s + it)^4 \zeta(s + 2it)$$

Now note that the final factor is analytic around $s = 1$, as $\zeta$ is analytic on the set $S_f$. Further, not that the first factor has a pole of order 3.

Now suppose that for some $t$, $\zeta(1+it) = 0$. It follows that the second factor has a zero of order at least 4 at $s = 1$, and hence $F_t(s)$ over all has a zero at $s = 1$. However, this contradicts the following lemma

**Lemma 7.1.** *If $\sigma > 1$, then,*

$$|F(\sigma)| \geq 1$$

as taking $\sigma \to 1$ can never reach let $F$ reach 0. We will now prove the lemma. We will instead show that its logarithm is greater than 0.

So,

$$\log|F(\sigma)| = \log|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+i2t)| = 3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma+it)| + \log|\zeta(\sigma+i2t)|$$

Now,

$$\log|\zeta(s)| = \log\left|\prod_p \frac{1}{1-1/p^s}\right|$$

Now, if $s = \sigma + it$, $p^{-s} = p^{-\sigma}e^{i\varphi_p}$ for some $\varphi_p$. Now, noting the branch cut of the logarithm that we had defined in Chapter 2, we have that

$$\log\left(\frac{1}{1-re^{i\theta}}\right) = \sum_{n\geq 1}\frac{r^n e^{in\theta}}{n}$$

Hence,

$$\log\left|\frac{1}{1-re^{i\theta}}\right| = \Re\left(\sum_{n\geq 1}\frac{r^n e^{in\theta}}{n}\right) = \sum_{n\geq 1}\Re\left(\frac{r^n e^{in\theta}}{n}\right) = \sum_{n\geq 1}\frac{r^n\cos n\theta}{n}$$

Thus,

$$\log|\zeta(s)| = \log\left|\prod_p \frac{1}{1-1/p^s}\right| = \sum_p\sum_{n\geq 1}\frac{p^{-n\sigma}\cos n\varphi_p}{n}$$

Finally this gives that

$$\log|F(\sigma)| = \sum_{p}\sum_{n\geq 1}\frac{p^{-n\sigma}(3+4\cos n\varphi_p+\cos 2n\varphi_p)}{n} \geq 0$$

as individually each element is non-zero. Hence we have proved the theorem.

# Chapter 8

# The Prime Number Theorem for Arithmetic Progressions

Now that we have proved both Dirichlet's theorem and PNT, we can combine the two proofs in order to create a proof for the Prime Number Theorem for Arithmetic Progressions. Like the previous chapter, in most of this chapter we are adapting [5]. We will use the same Tauberian theorem that we did for PNT, with a different $f$.

## 8.1 Satisfying the Conditions of the Tauberian Theorem: Second Time

We will now choose an $f$ such that the Tauberian Theorem will imply the PNT for APs. The choice of $f$ is very, very natural, when looked at from the context of the generalization from Euler's proof to Dirichlet's proof - instead of $f(n) = \Lambda(n)$, $f(n) = 1_{\equiv a \mod q}(n)\Lambda(n)$, and take $\sigma = 1$. It is easy to see that $f$ is non-negative. Furthermore, it is clear by the definitions that $A_f(x) = \psi(x; q, a)$. Now, 2 follows from the Chebyshev inequality that $\psi(x; q, a) \leq \psi(x) = \mathcal{O}(x)$.

Thus, let $F(s) = L_f(s)$, then by the orthogonality of Dirichlet characters, for $s \in \mathbb{C}, \Re(s) > 1$,

$$F(s) = -\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi}(a) \frac{L'(s,\chi)}{L(s,\chi)}$$

Hence, it remains to continue $F$ analytically to an open set containing $S_f$, and compute the desired residue.

Now, note that for any region in which $L(s,\chi)$ is analytic and non-zero simultaneously for all $\chi$, $\frac{L'(s,\chi)}{L(s,\chi)}$ is well-defined, and hence analytic. Thus, to show that $F$ satisfies the hypotheses of the theorem, it suffices to show that on open set containing $S_f$, each of the $L(s,\chi)$ functions extends analytically, and none of them are zero on this set. This demonstrates why the Generalized Riemann Hypothesis is such an important conjecture.

To do this, we apply partial summation as follows,

$$\sum_{n \leq x} \frac{\chi}{n^s} = \frac{\sum_{n \leq x} \chi(n)}{x^s} + s \int_1^x \frac{\sum_{n \leq t} \chi(n)}{t^{s+1}} dt$$

Now, assuming that $\chi$ is non-principal, one can note that taking $x \to \infty$ on both sides will result in convergence, as the integral is absolutely convergent (due to the character sums being bounded). Thus, we get

$$L(s,\chi) = s \int_1^\infty \frac{\sum_{n \leq t} \chi(n)}{t^{s+1}} dt$$

It is easy to see that this integral is conditionally convergent for $\Re(s) > 0$, and hence is analytic there. Further, for $s \neq 1$, $\Re(s) > 0$ by Theorem 2.8, $L(s,\chi_0)$ will be analytic (due to the analyticity of $\zeta$ in this region).

We will now compute the residue of F at $s = 1$. Note that the only element of the sum which has a non-removable singularity (more precisely, a pole at $s = 1$ is the term coming from the principal character. Furthermore, from Theorem 2.8, we know that

$$L(s,\chi_0) = \zeta(s) \prod_{p|q} \left(1 - \frac{1}{p^s}\right)$$

Taking logarithmic derivatives,

$$\frac{L'(s,\chi_0)}{L(s,\chi)} = \frac{\zeta'(s)}{\zeta(s)} + \sum_{p|q} \frac{\frac{\log p}{p^s}}{1-1/p^s}$$

It is easy to see that the terms under the summation symbol are entire, and hence will not contribute to the residue at $s = 1$. Hence, by this calculation $F(s)$ has a pole with residue $1/\varphi(q)$ at $s = 1$.

Thus, assuming the hypotheses of the theorem hold, we have that

$$\psi(x;q,a) = A_f(x) = \frac{\alpha}{\sigma}x^\sigma = \frac{x}{\varphi(q)}$$

which is the PNT for APs. As in the case for PNT, we know that $L(s,\chi)$ has a product for $\Re(s) > 1$, and hence is non-zero there. So we only need to consider the terms of the form $L(1+it,\chi)$.

## 8.2 $L(1+it,\chi)$

Here we have the following generalization of the ingenious argument used for $\zeta$. The lemma is as follows:

**Lemma 8.1.** *Suppose either that $t \neq 0$ or that $t = 0$, but $\chi^2 \neq \chi_0$ (or, in other words, $\chi$ is not a real character), then we have that*

$$L(1+it,\chi) \neq 0$$

Now note that the only case left out now is $L(1,\chi)$ for $\chi^2 = \chi_0$. However, we have already shown that the non-vanishing of L in this case when we were trying to prove Dirichlet's theorem.

Thus, if the lemma is proved, we are done.

Starting again from the same point,

$$3 + 4\cos\theta + \cos 2\theta = 2(1+\cos\theta)^2 \geq 0$$

Now let

$$F_t(s) = L(s, \chi_0)^3 L(s + it, \chi)^4 L(s + 2it, \chi^2)$$

The first factor has a pole of order 3, and the final factor is analytic (provided either that $t \neq 0$ or that $\chi^2 \neq \chi_0$, as provided for in the theorem's hypothesis). Thus, suppose that $L(1 + it, \chi) = 0$ for some $t$. Then, the middle factor has a zero of order at least 4, and hence $F_t$ has a zero at $s = 1$.

However, this contradicts the following lemma

**Lemma 8.2.** *If $\sigma > 1$, then,*

$$|F(\sigma)| \geq 1$$

as taking $\sigma \to 1$ can never reach let $F$ reach 0. We will now prove the lemma. We will instead show that its logarithm is greater than 0.

So,

$$\log |F(\sigma)| = \log |L(\sigma, \chi_0)^3 L(\sigma + it, \chi)^4 L(\sigma + 2it, \chi^2)| = 3 \log |L(\sigma, \chi_0)| + 4 \log |L(\sigma + it, \chi)| + \log |L(\sigma +$$

Now,

$$\log |L(s, \chi)| = \log \left| \prod_p \frac{1}{1 - \chi(p)/p^s} \right|$$

Now, if $s = \sigma + it$, $\chi(p)p^{-s} = p^{-\sigma}\chi(p)p^{-it} = p^{-\sigma}e^{i\varphi_p}$ for some $\varphi_p$ (since $|\chi(p)| = 1$. Now, as before, we have that

$$\log \left| \frac{1}{1 - re^{i\theta}} \right| = \Re \left( \sum_{n \geq 1} \frac{r^n e^{in\theta}}{n} \right) = \sum_{n \geq 1} \Re \left( \frac{r^n e^{in\theta}}{n} \right) = \sum_{n \geq 1} \frac{r^n \cos n\theta}{n}$$

Thus,

$$\log |L(s, \chi)| = \log \left| \prod_p \frac{1}{1 - \chi(p)/p^s} \right| = \sum_p \sum_{n \geq 1} \frac{p^{-n\sigma} \cos n\varphi_p}{n}$$

Finally this gives that

$$\log|F(\sigma)| = \sum_{p}\sum_{n\geq 1}\frac{p^{-n\sigma}(3+4\cos n\varphi_p+\cos 2n\varphi_p)}{n} \geq 0$$

as individually each element is non-zero.

Thus, putting it all together, the PNT for APs is proved.

# Chapter 9

# Generalizations and Applications

The strongest form of the PNT for APs that is known at present is the following theorem:

**Theorem 9.1** (Siegel-Walfisz theorem, $\star$)**.** *For any $N > 0$, there exists a constant $C_N > 0$, such that*

$$\psi(x; q, a) = \frac{x}{\varphi(q)} + \mathcal{O}(x \exp(-C_N(\log x)^{1/2}))$$

*for any $(a, q) = 1$ & $q \leq (\log x)^n$.*

## 9.1 The Generalized Riemann Hypothesis and Error Terms

We are now in a position to pin-point exactly how the Generalized Riemann Hypothesis enters into the landscape we have set up. GRH is a statement about the nature of the non-trivial zeroes of the L-functions associated with the Dirichlet characters. In particular, for a Dirichlet character $\chi$, we define $L(s, \chi)$ for $\Re(s) > 1$ as follows:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

This function can then be analytically continued onto the entire complex plane, with potentially at most one pole (this occurs when $\chi$ is the principal character). The GRH states that any zero of $L(s,\chi)$ with $\Re(s) \geq 0$ must in fact satisfy $\Re(s) = 1/2$.

In particular, using the machinery set up with some new ideas, one can show the following theorem.

**Theorem 9.2.** *(Corrollary of GRH, $\star$) Under the Generalized Riemann Hypothesis, if $\chi$ is a non-principal character, then*

$$\sum_{n \leq x} \chi(n)\Lambda(n) \ll x^{1/2} \log^2 x$$

Further the GRH for principal characters (or in fact, the regular Riemann Hypothesis for the $\zeta$ function given by $\zeta(s) = L(s,1)$) gives the following result.

**Theorem 9.3.** *(Corrollary of RH, $\star$) Under the Riemann Hypothesis, if $\chi$ is a principal character, then*

$$\begin{aligned} \sum_{n \leq x} \chi(n)\Lambda(n) &= \sum_{n \leq x} \Lambda(n) + \mathcal{O}(\log^2 qx) \\ &= x + \mathcal{O}(x^{1/2} \log^2 qx) \end{aligned}$$

Combining the two, and using the orthogonality of Dirichlet characters, it easily follows that for $x \geq q$,

$$\psi(x;q,a) = \frac{x}{\varphi(q)} + \mathcal{O}(x^{1/2} \log^2 x)$$

This theorem is well out of reach of present methods. The closest we have gotten is an "averaged" form of the GRH error term, which is known as the Bombieri-Vinogradov theorem. In any application of GRH, where instead

the GRH of one $L$, the general purpose behaviour of the $L$ across $\chi$ is used, then sometimes we can replace GRH in the proof with the Bombieri-Vinogradov theorem. See [7] for more details.

This brings the report to an end.

# Appendix A

# Elementary Techniques in Analytic Number Theory

## A.1 Partial Summation

We now give an account for partial summation. In general, summation by parts is an identity similar to integration by parts, which relates the sum of the product of two functions with the sum of one function, and the difference of the other. However, for our purposes we shall need the following, much weaker version called partial summation.

**Theorem A.1** (Partial Summation)**.** *Suppose $a_1, a_2, a_3 \cdots$ is a sequence of complex numbers, $A(x) = \sum_{n \leq x} a_n$ and $f(x)$ is some differentiable function on $(1, \infty)$. Then*

$$\sum_{n \leq x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt$$

*Proof.* Suppose $x$ is a natural number. Therefore,

$$\begin{aligned} \sum_{n \leq x} a_n f(n) &= \sum_{n \leq x} \{A(n) - A(n-1)\} f(n) \\ &= A(x)f(x) - \sum_{n \leq x-1} A(n)\{f(n+1) - f(n)\} \end{aligned}$$

Now, using the fact that $f$ is differentiable,

$$\sum_{n\leq x} a_n f(n) = A(x)f(x) - \sum_{n\leq x-1} A(n)\int_n^{n+1} f'(t)dt$$

Now, $A(x)$ is a step function changing values at positive integers. Hence $A(n)$ can be taken inside and replaced by $A(t)$.

$$\sum_{n\leq x} a_n f(n) = A(x)f(x) - \sum_{n\leq x-1} \int_n^{n+1} A(t)f'(t)dt$$

and thus

$$\sum_{n\leq x} a_n f(n) = A(x)f(x) - \int_1^{\infty} A(t)f'(t)dt$$

proving our theorem for integers. For non-integers, note that the theorem holds for $\lfloor x \rfloor$, the greatest integer less than $x$, and that

$$A(x)\{f(x) - f(\lfloor x \rfloor)\} - \int_{\lfloor x \rfloor}^{x} A(t)f'(t)dt = 0$$

which establishes the theorem.

□

This identity is a powerful tool for obtaining elementary estimates for many sums that arise in number theory, and is used in this report often without any specific appeal. We now use it to prove some common knowledge facts.

**Theorem A.2.** *For $x > 0$,*

$$\sum_{n\leq x} \frac{1}{x} = \log x + \mathcal{O}(1)$$

*Proof.* Putting $a_n = 1$ and $f(t) = 1/t$ in the partial summation identity, we see that $A(x) = \sum_{n\leq x} 1 = \lfloor x \rfloor$ and thus,

$$\sum_{n\leq x}\frac{1}{x}=\frac{\lfloor x\rfloor}{x}+\int_1^x\frac{\lfloor t\rfloor}{t^2}dt$$

Now, using $\lfloor x\rfloor = x-\{x\} = x+\mathcal{O}(1)$,

$$\sum_{n\leq x}\frac{1}{x}=\frac{x+O(1)}{x}+\int_1^x\frac{t+O(1)}{t^2}dt$$

Thus, the first term is clearly $O(1)$. Furthermore, the error term in the integral evaluates to

$$\int_1^x\frac{dt}{t^2}=1-\frac{1}{x}$$

which contributes $O(1)$. Hence, the main term is

$$\int_1^x\frac{dt}{t}=\log x+\mathcal{O}(1)$$

Hence our claim follows.

□

**Theorem A.3.** *For $x>0$,*

$$\sum_{n\leq x}\frac{1}{\sqrt{x}}=2\sqrt{x}+O\left(\frac{1}{\sqrt{x}}\right)$$

*Proof.* Taking $a_n=1$, $f(x)=1/\sqrt{x}$, we see that $A(x)=\lfloor x\rfloor$. Thus,

$$\sum_{n\leq x}\frac{1}{\sqrt{x}}=\frac{\lfloor x\rfloor}{\sqrt{x}}+\frac{1}{2}\int_1^x\frac{\lfloor t\rfloor}{t^{3/2}}dt$$

Again, using the estimate $\lfloor x\rfloor = x+\mathcal{O}(1)$, we get a contribution of $\sqrt{x}+\mathcal{O}(1/x^{1/2})$ from the first term. From the integral again, we get a contribution of $\sqrt{x}+\mathcal{O}(1/x^{1/2})$. Thus, we obtain the estimate

$$\sum_{n\leq x}\frac{1}{\sqrt{x}} = 2\sqrt{x} + O\left(\frac{1}{\sqrt{x}}\right)$$

□

Now, using analogous techniques to the previous two theorems, in particular taking $a_n = \chi(n)$ and noting that then $|A(x)| \leq q$, we can prove the following

**Theorem A.4.** *For $x > 0$*

$$\sum_{n>x}\frac{\chi(n)}{n} = O\left(\frac{1}{x^{1/2}}\right)$$

*and*

$$\sum_{n\leq x}\frac{\chi(n)}{\sqrt{n}} = O\left(\frac{1}{x^{1/2}}\right)$$

The proof of this claim is left as an exercise to the reader.

We now turn to the identities relating $\pi(x)$ and $\vartheta(x)$.

**Theorem A.5.** *For any real number $x > 0$, we have*

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t(\log t)^2}dt$$

$$\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}dt$$

*Furthermore, these relations hold with $\pi(x)$ replaced by $\pi(x;q,a)$ and $\vartheta(x)$ replaced by $\vartheta(x;q,a)$.*

*Proof.* Putting $a_n = 1_{\mathcal{P}}(n)\log n$ and $f(t) = 1/\log t$, we get $A(x) = \vartheta(x)$ and $f'(t) = -1/t(\log t)^2$ in the partial summation identity. Furthermore, the left hand side become $\pi(x)$, giving us the first identity.

Similarly, putting $a_n = 1_{\mathcal{P}}(n)$ and $f(t) = \log t$, we get $A(x) = \pi(x)$ and $f'(t) = 1/t$. Furthermore the left hand side becomes $\vartheta(x)$, giving us the second identity.

In either identity if we replace $1_{\mathcal{P}}(n)$ with $1_{\mathcal{P}(a,q)}(n)$ where

$$\mathcal{P}(a,q) = \{p \in \mathcal{P} : p \equiv a \pmod{q}\}$$

then we obtain the relations between $\pi(x;q,a)$ and $\vartheta(x;q,a)$, analogously.

□

## A.2 Dirichlet's Hyperbola Method

For us, the Dirichlet's Hybperbola method is an easily proven identity. We now prove the identity and expound on its importance.

**Theorem A.6** (Dirichlet's Hyperbola Method)**.** *Suppose $g(n)$ and $h(n)$ are functions on the natural numbers such that*

$$f(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

$$F(x) = \sum_{n \leq x} f(n)$$

$$G(x) = \sum_{n \leq x} g(n)$$

$$H(x) = \sum_{n \leq x} h(n)$$

*then for any real number $y > 0$ we have the following identity*

$$F(x) = \sum_{d \leq y} g(d)H\left(\frac{x}{d}\right) + \sum_{d \leq \frac{x}{y}} g(d)H\left(\frac{x}{d}\right) - G(y)H\left(\frac{x}{y}\right)$$

*Proof.* We have

$$\sum_{n \leq x} f(n) = \sum_{n \leq x} \sum_{de=n} g(d)h(e) = \sum_{de \leq x} g(d)h(e)$$

Pick a $y > 0$. Hence,

$$\sum_{n \leq x} = \sum_{\substack{de \leq x \\ d \leq y}} g(d)h(e) + \sum_{\substack{de \leq x \\ d > y}} g(d)h(e)$$

On, in other words,

$$\sum_{n \leq x} = \sum_{d \leq y} \sum_{e \leq x/d} g(d)h(e) + \sum_{e \leq x/y} \sum_{y < d \leq x/e} g(d)h(e)$$

Hence, recalling the definition of $G$ and $H$,

$$\sum_{n \leq x} = \sum_{d \leq y} g(d) H\left(\frac{x}{d}\right) + \sum_{e \leq x/y} h(e) \left\{ G\left(\frac{x}{e}\right) - G(y) \right\}$$

and thus,

$$F(x) = \sum_{d \leq y} g(d) H\left(\frac{x}{d}\right) + \sum_{e \leq \frac{x}{y}} g(d) H\left(\frac{x}{d}\right) - G(y) H\left(\frac{x}{y}\right)$$

as desired.

□

This identity is an important one, as it gives the summatory function of the Dirichlet convolution of two number-theoretic functions in terms of the summatory functions of those number-theoretic functions. Both summatory functions and Dirichlet convolutions are commonly occurring in number theory. Furthermore, the freedom to choose the parameter $y$ allows one to choose the optimal $y$ to obtain the asymptotic behaviour we wish to prove. We typically choose $y$ so that two of the terms become negligible, while the third contains the main term. The name of the method comes from counting lattice points on hyperbolas and is used when trying to obtain the average order of the number of divisors function.

## A.3 Farey Fractions

The Farey fractions are sequences of rational numbers which are recurring in number theory. For a fixed positive integer $Q$, the sequence of Farey fractions, $\mathcal{F}_Q$ is the set of all rational numbers in $[0, 1]$ whose denominator in reduced form is $\leq Q$, ordered with respect to the natural ordering on the reals.

Thus, for example, $\mathcal{F}_1$ is

$$\frac{0}{1}, \frac{1}{1}$$

$\mathcal{F}_2$ is

$$\frac{0}{1}, \frac{1}{2}, \frac{1}{1}$$

$\mathcal{F}_3$ is

$$\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$$

and so on.

# Bibliography


[1] I. Petrow, *Vinogradov's Three Primes Theorem* (2008), http://imbsrv1.epfl.ch/~petrow/V3.pdf

[2] K. Soundararajan, *Additive Combinatorics: Winter 2007* (2007), http://math.stanford.edu/~ksound/Notes.pdf

[3] T. Tao, *Open question: The parity problem in sieve theory* (2007), https://terrytao.wordpress.com/2007/06/05/open-question-the-parity-problem-in-sieve-theory/

[4] H. Helfgott, *The ternary Goldbach conjecture is true* (2013), http://arxiv.org/abs/1312.7748

[5] Jan-Hendrik Evertse, Course: *Analytic Number Theory* (Fall, 2014) http://www.math.leidenuniv.nl/~evertse/ant.shtml

[6] A. Sahay, *MTH391A Project Report: Dirichlet's Theorem* (2013), http://home.iitk.ac.in/~asahay/Projects/mth391.pdf

[7] A. Sahay, *The Bombieri-Vinogradov Theorem* (2013), http://home.iitk.ac.in/~asahay/Projects/imsc2013.pdf

[8] A. Sahay, *MTH598A Report: The Vinogradov Theorem* (2015), http://home.iitk.ac.in/~asahay/Projects/mth598.pdf