MTH598A Report
The Vinogradov Theorem

Anurag Sahay
11141/11917141
under the supervision of

Dr. Somnath Jha
Dept. of Mathematics and Statistics

4th November, 2015

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 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.

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 nth 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

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 $3^{3^{1}5}$. 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 ϑ and ψ 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 π 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, π 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 nth 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 ϑ-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 ϑ to one for π.

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 ψ-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,

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

Now, trivially, $\vartheta(x) = \sum_{p \le x} \log p \le \sum_{p \le x} \log x \le x \log x$. Also, we know that $\vartheta(x)$ is increasing and thus, $\vartheta(x^{1/2}) \ge \vartheta(x^{1/k})$ for $k \ge 2$. 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 ψ can be converted into an estimate for ϑ, 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, ψ may be interchanged with ϑ 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 π and ϑ, we define $\psi(x; q, a)$

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

[3]Clearly

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

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 ψ-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

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

where the last equality follows from the definition.

□

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

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 χ 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, χ 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 χ_0. All other characters are known as *non-principal characters.*

The reader should verify that χ 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 χ and χ_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 χ 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 ψ Function

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

χ modulo q. That is, we define the summatory function $\psi(x;\chi)$ for a Dirichlet character χ 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 ψ 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 χ, 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 χ 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 ψ 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 χ 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 ζ function given by $\zeta(s) = L(s, 1)$) gives the following result.

Theorem 2.3. *(Corrollary of RH, $\star$) Under the Riemann Hypothesis, if χ 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 $e(a/q) = e^{\frac{2\pi i a}{q}}$. 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 χ be a Dirichlet character modulo q. Then,*

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

Lemma 2.2. *Let χ_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

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

Convolving both sides by μ, 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

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

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 $\mathfrak{S}(N) = 0$ 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 ϑ 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,

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

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 $\le P$. For $a/q \in \mathcal{F}_P$ (such that a and q are co-prime), define

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

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

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

Thus we get that

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

Now, applying the bound on *psi* from GRH for non-trivial χ, and the bound on τ 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,

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

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

$\square$

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,

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

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

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

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

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

The inner sum is the Ramanujan sum $c_q(N) \le \varphi(q)$, 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.

$\square$

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.

Appendix A

Appendix

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, $A(x) = \sum_{n \le x} a_n$ and $f(x)$ is some differentiable function on $(1, \infty)$. Then*

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

Proof. Suppose x is a natural number. Therefore,

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

Now, using the fact that f is differentiable,

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

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

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

and thus

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

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.

$\square$

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 $x > 0$,*

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

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

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

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

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

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

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

Hence our claim follows.

□

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

Theorem A.3. *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.

$\square$

A.2 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`