university of groningen

faculty of science and engineering

mathematics and applied mathematics

Investigation of the Circle Method: its origin and some applications

Bachelor's Project Mathematics

July 2020

Student: E.D.G. Drummond

First supervisor: Prof.dr. J. Top

Second assessor: Stevan Gajovic

Abstract

The circle method was developed by Hardy & Littlewood in their attempts to apply analytic function theory to Waring's problem, which asks for the smallest integer s such that all sufficiently large integers can be written as a sum of s k^{th} powers. The method can be applied to problems of an additive nature, and in particular the method was used to prove Goldbach's weak conjecture for sufficiently large integers. This was first done by Hardy & Littlewood, but they assumed the generalised Riemann hypothesis; Vinogradov managed to use the method without this assumption to prove the same result. This thesis, after introducing the main ideas behind the method and how it works, explores how it can be applied to prove Vinogradov's theorem, that the weak Goldbach conjecture is true for all sufficiently large integers. Following this, there is a short look at how the method can be applied to proving that all positive integers can be written as a sum of three triangular numbers.

Notation

There are various number theory related notations used in this thesis. This short section clarifies what is meant by each of them.

$$(a, b) = \gcd(a, b) = \text{the greatest common divisor of } a \text{ and } b$$

$$\begin{aligned} &\text{Take any } x \in \mathbb{R}, \text{ then} \\ \lfloor x \rfloor &= \text{ the largest integer } y \text{ such that } y \leq x \\ \lceil x \rceil &= \text{ the smallest integer } y \text{ such that } y \geq x \\ \{x\} = x - \lfloor x \rfloor &= \text{ the non-integral part of } x. \end{aligned}$$

Oh-notation: This notation was developed to talk about what happens asymptotically, i.e. as some term tends to infinity. Firstly there is **big Oh** notation: $A(x) = O(B(x))$ (read as $A(x)$ is of order (or big-Oh) $B(x)$) means explicitly that

$$\exists c > 0 \text{ and some } x_0 \text{ such that } |A(x)| \leq c \cdot B(x) \quad \forall x \geq x_0.$$

this is also written as $A(x) \ll B(x)$, or $B(x) \gg A(x)$. Moreover, if the constant c depends on specific variables, for example N, the dependency is noted in a subscript, e.g.

$$A(x) \ll O(g(x))_N.$$

Next there is **small Oh** notation. We write

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

to mean that

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} \to 0.$$

This is akin to saying that $f(x)$ is of smaller order than $g(x)$, and for example if we have

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

then the value of $f(x)$ only depends on the first term asymptotically because the second term is negligible.

For additional clarity, we note that throughout we have that

$$\log = \log_e = \ln.$$

Furthermore, in any case where we use an integer p, we are referring to a prime number p.

One function that will be seen is **Euler's totient function**, $\phi(n)$, which gives for an input n the number of positive integers less than n that are also coprime with n.

Contents

Introduction

The circle method was first conceived in a paper by Hardy & Ramanujan, when attempting to apply analytic function theory to Waring's problem, between 1918-20 [Nat13], and Hardy & Littlewood would go on to develop the method further [Vau97]. Since then, the method has been applied with respectable success to number theoretic problems of an additive nature. This thesis will investigate what the circle method is, and look in more detail at how it has been applied to two problems: Waring's problem and the Goldbach conjectures.

Waring's problem itself can be stated as follows: for every positive integer k, show that a bound $B = g(k)$ exists such that every positive integer can be written as a sum of at most B k^{th} powers (i.e. $n = a_1^k + a_2^k + \cdots + a_B^k$ for all $n \in \mathbb{Z}_{>0}$ where $a_i \in \mathbb{Z}_{\geq 0}$ for all i). For example, Lagrange's four square theorem states that every natural number can be written as the sum of four integer squares. The problem then evolved over time to ask something slightly different; what is the smallest such $s = G(k)$ such that all *sufficiently large* integers can be written as a sum of s k^{th} powers.

Most of what has been shown about Waring's problem involves the circle method; however there is still much to do. Only two cases of k in Waring's modern problem ($G(k)$) have complete solutions. This thesis will outline some of the contributions the method has had in solving Waring's problem.

Goldbach's conjectures state that all odd numbers larger than 5, and all even numbers larger than 2, can be written as a sum of at most three and two primes respectively. The circle method has had a lot of success with the former conjecture, but the latter appears harder to work with. We will see in this thesis how the method has been applied to the first conjecture in detail, and to the second in less detail.

The circle method can be stated briefly as a series of steps:

- Construct a generating function that in some sense represents our problem, we will for example use the generating function to find an expression for $G(k)$.
- From this generating function, and some complex analysis, find an integral representation of our desired function (e.g. $G(k)$).
- Separate this integral into the integral over the major ($\mathfrak{M}$) and minor ($\mathfrak{m}$) arcs; this involves partitioning to be integrated over, where the partition is decided based on the specific problem,

$$G(k) = \int_0^1 \text{integrand}\, dx = \int_{\mathfrak{M}} \text{integrand}\, dx + \int_{\mathfrak{m}} \text{integrand}\, dx$$
$$= \text{main term } + \text{ error term.}$$

- Evaluate the value of the integral over major arcs (this will likely only be possible asymptotically).
- Bound the minor arc such that its contribution is negligible compared to the major arc.
- If done successfully, the value of the sum of the integral over the major and minor arcs will tell us something about our problem, e.g. that $G(k)$ is positive for some k and therefore that in this case Waring's problem is true.

In this investigation we will see some evidence supporting the claim that finding a small enough bound for the minor arc is “the hardest part of the problem”. Yet even though one might struggle trying to create this bound and question whether it is possible, numerical investigations often support the belief that the minor arc contribution is negligible compared to the major arcs' [MMTB06].

Chapter 1

Preliminaries

1.1 Classical Vs Modern Waring's Problem

> "Every integer is a cube or the sum of two, three, ... nine cubes; every integer is also the square of a square, or the sum of up to nineteen such; and so forth."
>
> (Waring — [War91], p. 336)

The nature of Waring's problem has changed over time [VW02]. As can be inferred from the above quote, when Waring first discussed the problem, the desire was to show that for every $k \geq 3$ there exists a number s such that *all* natural numbers can be written as a sum of at most s k^{th} powers. The interesting aspect of this question is the smallest such s that this is true for, but of course prior to answering that it must be shown that such an s even exists.

It is handy to define the function **g(k)** $:= s$ for the smallest such s, for example Waring claimed that $g(3) = 9$ and $g(4) = 19$. By 1900, it had only been shown that $g(k)$ had a finite value for finitely many cases [VW02]. Finally, in 1909, Hilbert proved that such a number s exists for all $k \geq 3$ [Hil09] via a combinatorial argument built upon various algebraic identities; this was a significant step in the problem, but it provided a very poor upper bound for $g(k)$. The next step was to work on bringing the upper bound for $g(k)$ down.

Upper bounds for $g(k)$ were brought down for various cases by the mathematical community, but it turns out that the value of $g(k)$ is essentially decided by a few cases for (relatively) small integers. In particular, take the integer

$$n = 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 < 3^k.$$

This integer is strictly less than 3^k, and therefore can only be written as a sum of k^{th} powers of 1 and 2. It is this lower bound for $g(k)$ that largely determines it. As a result, mathematicians also began to ask the question of what happens if we ignore smaller integers, and we only care about splittings into s integers that occur infinitely often?

Thus the modern form of Waring's problem asks what $s =:$ **G(k)** is the smallest integer such that all *sufficiently large* integers are a sum of at most s k^{th} powers of? So far, only two cases of this have been solved, $G(2) = 4$ and $G(4) = 16$. Although no other cases have yet been fully solved, there has been progress. For example Samir Siksek recently proved that $G(k) \leq 7$ [Sik16]. He did this without the circle method, but much of what has been shown for Waring's problem in general has relied in large part upon the circle method.

1.2 Generating Functions

An essential first step to applying the circle method to any problem is creating a generating function; this is a function that in some sense represents the problem. Some examples should serve to make this meaning clear. A common first example is an identity of Euler's [MMTB06].

Proposition 1.2.1. (Euler) We have as an identity of formal power series

$$\frac{1}{(1-x)(1-x^2)(1-x^3)\cdots} = \sum_{n=0}^{\infty} P(n)x^n,$$

where $P(n)$ is the partition function; i.e. the number of ways are there to write n as a sum of positive integers. (we set $P(0) = 1$, and for example $P(4) = 5$ since $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$).

For clarity, an "identity of formal power series" means that we are not considering convergence properties or issues, but only that the coefficients of the corresponding powers of x on each side are the same.

Proof. Let's start with the left hand side and see how we can rewrite it,

$$\begin{aligned}
\frac{1}{(1-x)(1-x^2)(1-x^3)\cdots} &= \frac{1}{1-x}\frac{1}{1-x^2}\frac{1}{1-x^3}\cdots \\
&= \left(\sum_{a=0}^{\infty} x^a\right)\left(\sum_{b=0}^{\infty} x^{2b}\right)\left(\sum_{c=0}^{\infty} x^{3c}\right)\cdots \\
&= 1 + \sum_{n=1}^{\infty} c_n x^n.
\end{aligned}$$

We now want to show that $c_n = P(n)$ for all $n \geq 1$. Let's try to calculate c_n from the product of sums on the second line then. The first thing we notice is that all coefficients in the second line are 1, and this makes the evaluation simpler. If we want to calculate c_n then we get a contribution of 1 from all combinations $n = a + 2b + 3c + \cdots$, where $a, b, c, ... \in \mathbb{Z}_{\geq 0}$. Now notice that this is actually just another way to state the definition of $P(n)$. This is because a represents the number of 1's in the sum, b represents the number of 2's in the sum, and so on. □

The function on the left is what we would call the generating function because we can use it to find a representation of $P(n)$. At the moment it of course is representing $P(n)$ for all n simultaneously, but with some further manipulations (to be seen in future sections), we can extract $P(n)$ for some specific n.

We can generalise this type of relationship. Let A be a set of positive integers, and order the elements increasingly so that (a_i) enumerates them; e.g. $(1, 3, 5, ...)$ is the odd numbers, $(1, 4, 9, ...)$ is the square numbers, etc.

Proposition 1.2.2. For any set $A = (a_i)$ as defined above, we have that

$$\frac{1}{(1-x^{a_1})(1-x^{a_2})(1-x^{a_3})\cdots} = 1 + \sum_{n=1}^{\infty} K(n)x^n,$$

where $K(n)$ is the number of ways to write n as a sum of elements from A (repeats allowed).

The proof proceeds exactly as the previous one did. Now what if we wanted to find a function that represents partitions where elements cannot be used more than once (i.e. write n as a sum of unequal parts)? We would have to find a different type of generating function.

Proposition 1.2.3. For any set $A = (a_i)$ as defined above, we have that

$$(1 + x^{a_1})(1 + x^{a_2})(1 + x^{a_3}) \cdots = 1 + \sum_{n=1}^{\infty} Q(n)x^n,$$

where $Q(n)$ is the number of ways to write n as a sum of unequal elements from A.

For example, we have that

$$(1 + x)(1 + x^2)(1 + x^3) \cdots = 1 + \sum_{n=1}^{\infty} q(n)x^n,$$

where $q(n)$ is the number of ways to write n as a sum of unequal positive integers.

Depending on the problem, we obviously need a different generating function. From the examples so far, we may already have the sense that we can only create generating functions of an additive or combinatorial nature.

Chapter 2

The Hardy-Littlewood Circle Method

2.1 Initial Conditions

In this section we will elaborate on the details of the circle method as it was first employed by Hardy & Littlewood, and then move on to a few important alterations that somewhat simplified it. In order to do this, let's first clearly define the function we want to evaluate.

Definition 2.1.1. $r_{A,s}(N) :=$ the number of ways of writing N as a sum of s elements from the set A.

Definition 2.1.2. Let A be any set of non negative integers, then $f(z) := \sum_{a \in A} z^a$ is the **generating function** of A.

Remark. The reader may be wondering about the radius of convergence of the generating function; we can assume a radius of convergence of 1 if the set A is infinite, or ∞ if the set is finite. However we are not actually concerned with these convergence issues, and we will not expand on them. This is because, as we will shortly see, the alterations to the original method remove these worries.

Remark. By taking $A = K = \{k^{th}$ powers of non-negative integers$\}$, we can formulate Waring's problem as 'what is the smallest s such that $r_{K,s}$ is at least 1 for all sufficiently large integers?'. Moreover, by taking $A = P$ the prime numbers and $s \in \{2, 3\}$ we can formulate the Goldbach conjectures.

The function $r_{A,s}$ is what we want to investigate, but so far we only have a descriptive definition of it; ideally we want to be able to make it. Let's see how our generating function achieves this.

Proposition 2.1.3.

$$f(z)^s = \sum_{n=0}^{\infty} r_{A,s}(n) z^n.$$

Proof.

$$\begin{aligned} f(z)^s &= \left(\sum_{a\in A} z^a\right)^s \\ &= \sum_{a_1\in A}\cdots\sum_{a_s\in A} z^{a_1+\cdots+a_s} \\ &= \sum_{n=0}^{\infty} r_{A,s}(n) z^n. \end{aligned}$$

The reasoning behind the last inequality proceeds analogously to the explanation in the proof of Proposition 1.2.1, although it should be relatively easy to see from the preceding line. □

Notice that our function of interest is now a coefficient in a power series that we constructed from our generating function. As such, it is possible to apply Cauchy's integral formula to extract the coefficient of interest (where γ is the unit circle oriented counter-clockwise),

$$r_{A,s}(n) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)^s}{z^{n+1}} dz.$$

Thus we have produced an integral representation of our function of interest, and if we can sufficiently evaluate this integral our problem will be solved. This integral is evaluated over a circle centred at the origin (and hence where the name 'circle method' originates from). As mentioned before, the interval of integration will be separated into two disjoint parts, the major arcs $\mathfrak{M}$, and the minor arcs $\mathfrak{m} := \gamma\backslash\mathfrak{M}$.

At this point some work must be carried out to determine where the integrand takes on large values, and where it takes on smaller values. With this information at hand, it is possible to decide how to pick the major arcs and thus partition the interval. After this, the contribution from the major arcs would be investigated, and the contribution from the minor arcs would hopefully be provably negligible due to cancellation from oscillations around the circle.

However, this is a good place to go into the alterations to the method that simplify it and remove the convergence issues.

2.2 Vinogradov's Alteration to the Method

Vinogradov noticed that if we wanted to study $r_{A,s}(n)$ we could restrict the generating function to the finite sum

$$p(z) = \sum_{\substack{a\in A\\ a\leq n}} z^a.$$

This would sidestep any question of convergence as well as remove unnecessary terms. We can however go further still, and change the polynomial into a sum of complex exponentials using the function $e(\alpha) := e^{2\pi i\alpha}$ (this function is commonly seen in number theory and has this compact form as a result). Moreover, we will decide to fix the set A for pedagogical reasons; it is easier to work under a specific example rather than a general one. Let $A = K$, which was the set of k^{th} powers on non-negative numbers (so for example if $k = 3$, then $K = \{0, 1, 8, 27, 64, ...\}$). Next we will actually restrict K (and subsequently call it K_N) by only including all its elements $a \in K$ such that $a \leq N := \lfloor n^{1/k}\rfloor$. Now, take the function

$$\begin{aligned} F(\alpha) &= \sum_{r\in K_N} e(r^k\alpha) \\ &= \sum_{t=0}^{N} e(t^k\alpha). \end{aligned}$$

Thus we see that

$$\begin{aligned} F(\alpha)^s &= \left(\sum_{t=0}^{N} e(t^k\alpha)\right)^s \\ &= \sum_{t_1=0}^{N} \cdots \sum_{t_s=0}^{N} e((t_1^k + \cdots + t_s^k)\alpha) \\ &= \sum_{t=0}^{sN} r_{K_N,s}(t)e(t\alpha). \end{aligned}$$

This time Cauchy's integral formula gives us a simple orthogonality relation,

$$\int_0^1 e(m\alpha)e(-n\alpha)d\alpha = \begin{cases} 1 & \text{if } m = n \\ 0 & \text{if } m \neq n. \end{cases} \tag{2.1}$$

This gives us a different formula for our desired function for a fixed n,

$$r_{K,s}(n) = r_{K_N,s}(n) = \int_0^1 F(\alpha)^s e(-n\alpha)d\alpha.$$

The first equality is hopefully clear; since K_N contains all k^{th} powers that do not exceed n, then this set restriction does not affect the value of this function. This relation allows us to make the changes Vinogradov added to remove convergence issues, whilst not losing any functionality of the method.

We will continue with the formalism from Vinogradov for the rest of this paper for due to its simplicity.

2.3 An Upper Bound for $G(k)$

Most of what is known about Waring's problem has been achieved through the use of the circle method [VW02]. Here we would like to note a few of these results.

The first explicit upper bound was achieved by Hardy and Littlewood, and it tells us that

$$G(k) \leq (k-2)2^{k-1} + 5.$$

This result was soon improved to give

$$G(k) \leq (k-2)2^{k-2} + k + 5 + \lfloor \zeta_k \rfloor,$$

where

$$\zeta_k = \frac{(k-2)\log 2 - \log k + \log(k-2)}{\log k - \log(k-1)}.$$

There is a table stating this bound over the years in [VW02] which we present here. It is interesting to see how the bound is reduced over time, and the fact that when a new method is introduced it takes time for the method to be used more effectively.

Author	Bound
Vinogradov	$32(k \log k)^2$
Vinogradov	$k^2 \log 4 + (2 - \log 16)k, \ (k \geq 3)$
Vinogradov	$6k \log k + 3k \log 6 + 4k, \ (k \geq 14)$
Vinogradov	$k(3 \log k + 11)$
Tong	$k(3 \log k + 9)$
Jing-Run Chen	$k(3 \log k + 5.2)$
Vinogradov	$2k(\log k + 2 \log \log k + O(\log \log \log k))$
Vaughan	$2k(\log k + \log \log k + O(1))$
Wooley	$k(\log k + \log \log k + O(1))$

2.4 Beyond Waring's Problem

For completion further generalisations of Waring's problem will be briefly presented. The first is the **Waring-Goldbach Problem**, which is essentially the same as Waring's problem, but the difference being that we can only take k^{th} powers of prime numbers; i.e. what is the smallest s such that the equation below has a solution for all sufficiently large positive integers n?

$$n = p_1^k + \cdots + p_s^k,$$

where the p_i are prime numbers.

Next is Waring's problem for mixed powers. As the name suggests, this time around we are not restricted to taking a single power but can study any combination of powers. For example, in a recent paper Friedlander & Wooley shows that (under the assumption of two unproved conjectures) "all large natural numbers n with $8 \nmid n$, $n \not\equiv 2 \bmod 3$ and $n \not\equiv 14 \bmod 16$ are the sum of 2 squares and 3 biquadrates" [FW13]. In general it is possible to take any combination of powers. Of particular interest is this specific remark from this paper, "it is generally conjectured that, whenever $k_1^{-1} + \cdots + k_s^{-1} > 1$, all large natural numbers n satisfying appropriate congruence conditions should be representable in the form

$$x_1^{k_1} + x_2^{k_2} + \cdots + x_s^{k_s} = n".$$

Interestingly both known values of $G(k)$ ($G(2) = 4$ and $G(4) = 16$) require their sum of reciprocals to be larger than 1, being in fact 2 and 4 respectively. Looking at the congruence conditions, we see that since every square is congruent to 0 mod 8, 1 mod 8 or 4 mod 8, we cannot make 7 mod 8 from a sum of three squares. As such, $G(2) \geq 4$.

Lastly, Waring's problem has been generalised to algebraic number fields; the circle method was subsequently generalised to these fields too.

2.5 Conclusion for Waring's Problem

As mentioned earlier, finding a value for $G(k)$, the smallest number such that every sufficiently large integer can be represented as a sum of at most s k^{th} powers has only been found for two values of k. This problem is not easy, but "the bulk of what is known about $G(k)$ has been obtained through the medium of the Hardy-Littlewood method" [VW02]. We have exemplified what the generating function for all forms of Waring's problem would be, and found an integral representation for them - but actually evaluating the integral and bounding the minor arcs is difficult.

Chapter 3

The Goldbach Conjectures

The Goldbach conjectures have their origin in correspondence between Goldbach and Euler in 1742. They can be stated as follows:

Conjecture 1. Weak Goldbach Conjecture All odd integers larger than 7 can be expressed as the sum of at most three prime numbers. (Also known as the Ternary Goldbach Conjecture)

Conjecture 2. Strong Goldbach Conjecture All even integers larger than 2 can be expressed as the sum of two prime numbers. (Also known as the Binary Goldbach Conjecture)

This section will explore in detail how the circle method has been applied to the weak Goldbach conjecture. This will provide an extensive example of how the method can be applied, and provide context for some of the complexities that arise from its use. For some more context, Hardy & Littlewood used the circle method to show that all but finitely many many odd integers are the sum of three primes - but they had to assume the generalised Riemann hypothesis (GRH) in order to do so [KT04].

In 1937 I.M. Vinogradov proved an asymptotic formula showing that the weak conjecture is true for all sufficiently large integers [Vin37] without relying on the GRH (the Siegel Walfisz theorem can be used instead); it is this formula and its proof that we will be exposing. Following this, a brief look at the method's use in the strong conjecture will demonstrate that the circle method is not always successful.

For clarity, everything that follows, up until the last section (section 3.9), is under the context of the weak Goldbach conjecture.

3.1 Generating Function

As with every application of the circle method, we must start by representing the problem in a generating function. For Goldbach, we will define the weighted generating function

$$F_N(\alpha) := \sum_{p \leq N} \log p \cdot e(p\alpha).$$

The weight is the value $\log p$, and it is included as it makes some of the required derivations simpler whilst not altering the method in essence; the weights can be removed later through partial summation. As we have seen before, we now have

$$R_3(N) = \int_0^1 F_N(\alpha)^3 e(-N\alpha)d\alpha,$$

where

$$R_3(N) := \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3.$$

How can we relate this new, weighted expression to $r_{P,3}(N)$ (recall that P denotes the set of prime numbers)? Note that P needs to be specified in $r_{P,s}(N)$, but not in $R_3(N)$ because it is implicit in its definition. We can relate these two functions rather trivially by

$$\begin{aligned} R_3(N) &\leq (\log N)^3 \sum_{p_1+p_2+p_3=N} 1 \\ &= (\log N)^3 r_{P,3}(N). \end{aligned}$$

This inequality may be crude, but for our purposes it is sufficient. Our hope is to show that $R_3(N)$ is positive for all large enough inputs N - because if $R_3(N)$ is positive, then $r_{P,3}(N)$ must also be positive. We will then be able to conclude that there is indeed a way to represent any large enough natural number as a sum of three primes. This is because $r_{P,3}(N)$ must take integral values, so if it is positive then it is at least 1 and if this means that there is at least one way to express N as desired.

3.2 Evaluating $F_N(x)$

In this section we will exemplify a tool that can be used to help bound our integral on the arcs, namely finding the "average value" of $|F_N(x)|^2$. First note that

$$\begin{aligned} |F_N(x)| &= \left| \sum_{p \leq N} \log p \cdot e(px) \right| \\ &\leq \sum_{p \leq N} \log p \\ &\leq \pi(N) \log N, \end{aligned}$$

where $\pi(N)$ is the prime counting function, giving the number of primes that are at most N. At this point we can use the prime number theorem, which states that

$$\pi(N) = \frac{N}{\log N} + o(\frac{N}{\log N}).$$

Rearranging this, we find that

$$\pi(N) \log N = N + o(N) \tag{3.1}$$

This allows us to conclude that

$$|F_N(x)| \leq N + o(N).$$

From here, do we expect the average value of $|F_N(x)|^2$ to be on the order of N^2, or do we expect it to be lower? We hope, and find, that the average value is lower - it is this fact that we can use to help bound the minor arcs.

Lemma 3.2.1. The average value of $|F_N(x)|^2$ on the interval $[0, 1]$ is $N \log N + o(N \log N)$, i.e.

$$\int_0^1 |F_N(x)|^2 dx \leq N \log N + o(N \log N).$$

Proof. The absolute value can be expressed as $|F_N(x)|^2 = F_N(x)\overline{F_N(x)}$, but in our case we have that $\overline{F_N(x)} = F_N(-x)$; so we have that $|F_N(x)|^2 = F_N(x)F_N(-x)$.

$$\begin{aligned}
\int_0^1 |F_N(x)|^2 dx &= \int_0^1 F_N(x)F_N(-x)dx \\
&= \int_0^1 \sum_{p\leq N} \log p \cdot e(px) \sum_{q\leq N} \log q \cdot e(-qx)dx \\
&= \sum_{p\leq N}\sum_{q\leq N} \log p \log q \int_0^1 e((p-q)x)dx \\
&= \sum_{p\leq N} \log^2 p \\
&\leq \log N \sum_{p\leq N} \log p \\
&\leq \log N(N + o(N)) \\
&= N\log N + o(N\log N),
\end{aligned} \tag{3.2}$$

where in the fourth equality we have used the orthogonality relationship presented in Equation 2.1, and in the second inequality we have used the prime number theorem as given by Equation 3.1 (since $\sum_{p\leq N}$ logp$\leq \log N \sum_{p\leq N} 1 = \log N\pi(N)$). □

One of the things we did here that turns out to be powerful in a non-negligible number of situations, is evaluate a function multiplied by its complex conjugate. This is far easier to work with than the absolute value function. Next a remark is given on something that [MMTB06] highlights too, as it is an interesting and important idea in what we are doing.

Remark. (Square root cancellation) The average value of the square of the absolute of our function, $N\log N$, is far lower than the theoretical maximum value of N^2. We have, on average, almost square root cancellation. In general, if we add together a 'random' set of numbers on the unit circle their average value will often be at most $\sqrt{N}$.
This would appear linked to random walk theory. In fact in $d-$dimensional space, the expected value of the distance from the origin after N steps is $\sqrt{\frac{2N}{d}\frac{\Gamma(\frac{d+1}{2})}{\Gamma(\frac{d}{2})}}$. If we were to consider summing random numbers from the unit circle as a random walk in two dimensions we would find an expected distance of $\sqrt{N}\cdot 0.8862....$ But this would be ignoring the fact that although we are in two dimensions, the numbers from the circle are not restricted to two directions as in the random walk. Perhaps, in a sense, the infinite number of directions they represent is analogous to taking d to be infinite. Given that $\sqrt{\frac{2N}{d}\frac{\Gamma(\frac{d+1}{2})}{\Gamma(\frac{d}{2})}}$ converges to $\sqrt{N}$ (as $d\to\infty$), perhaps there is the possibility that we can bound the average value of $|F_N(x)|^2$ by $\sqrt{N}$.

3.3 Arc Selection

How do we decide how to separate the unit interval into the separate arcs? Since we are trying to bound the integral over the minor arcs and show its contribution is negligible compared to the major arcs', we probably desire the major arcs to contain the regions of the unit interval where our function F_N is largest. It turns out that $F_N(x)$ is large when $x = \frac{a}{q}$ under a few conditions on a and q. We will be assuming these conditions on a, q for the remainder of this chapter.

Fix some $B > 0$, and let $Q := \log^B N$; now fix some $q \leq Q$ and an $a \leq q$ such that $(a, q) = 1$. Let's now see how we can express our function; we will first separate the sum into a double sum over the congruence classes $\bmod q$, and then simplify.

$$\begin{aligned} F_N\left(\frac{a}{q}\right) &= \sum_{p\leq N} \log p \cdot e\left(p\frac{a}{q}\right) \\ &= \sum_{r=1}^{q} \sum_{\substack{p\equiv r \bmod q \\ p\leq N}} \log p \cdot e\left(\frac{ap}{q}\right) \\ &= \sum_{r=1}^{q} \sum_{\substack{p\equiv r \bmod q \\ p\leq N}} \log p \cdot e\left(\frac{ar}{q}\right) \\ &= \sum_{r=1}^{q} e\left(\frac{ar}{q}\right) \sum_{\substack{p\equiv r \bmod q \\ p\leq N}} \log p \end{aligned} \tag{3.3}$$

The next thing we need to do is evaluate the sum over $p \equiv r \bmod q$, and in order to do this we make use of the Siegel-Walfisz theorem (see below). We can also see before that though that we can ignore the case where $(r, q) > 1$. This is because if $(r, q) = d > 1$, we have that $r = r'd$, $q = q'd$ and $p = r + kq = d(r' + kq')$. However since p is prime, we must have that $r' + kq' = 1$. And since $r, q \geq 1$, and therefore that $r', q' \geq 1$, we conclude that $k = 0$. Thus $p = r$ is the only case in this scenario. And if we only have a single case, but are looking at what happens asymptotically, this single case represents a diminishing fraction of the cases as we increase N; this case thus can be seen as negligible.

Theorem 3.3.1. **(Siegel-Walfisz)** Take the non-negative integers a, q such that $(a, q) = 1$ and $q \geq 1$. Then, for any $C > 0$ we have that

$$\sum_{\substack{p\equiv a \bmod q \\ p\leq N}} \log p = \frac{N}{\phi(q)} + O\left(\frac{N}{\log^C N}\right)_C$$

for all $N \geq 2$.

Remark. Hardy & Littlewood in fact also proved Vinogradov's theorem, but they did it in 1923. However, their proof used an unproven assumption: the generalised Riemann hypothesis [HL+23]. As such, what they had done was technically invalid (until GRH is proved of course). By incorporating the Siegel-Walfisz theorem, Vinogradov avoided the need to assume the GRH, and hence in a sense improved the effectiveness of the method.

Now if we take any $C > 0$, this theorem will let us simplify Equation 3.3 by simplifying the innermost sum.

$$\sum_{\substack{p\equiv r \bmod q \\ p\leq N}} \log p = \frac{N}{\phi(q)} + O\left(\frac{N}{\log^C N}\right).$$

Recall that q is at most $\log^B N$, so we have at least that

$$\sum_{\substack{p\equiv r \bmod q \\ p\leq N}} \log p \geq \frac{N}{\log^B N} + O\left(\frac{N}{\log^C N}\right).$$

This gives us some sense of the order of the two terms; at the moment it appears that if we want our error term to be negligible compared to the main term, we only need $C > B$. We can now substitute this result into what we derived earlier to find that

$$\begin{aligned} F_N\left(\frac{a}{q}\right) &= \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right)\left(\frac{N}{\phi(q)} + O\left(\frac{N}{\log^C N}\right)\right) \\ &= \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right)\frac{N}{\phi(q)} + O\left(\frac{qN}{\log^C N}\right) \\ &= \frac{N}{\phi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right) + O\left(\frac{N}{\log^{C-B} N}\right). \end{aligned} \tag{3.4}$$

Provided that the sum of exponentials over r is not too small, our function is of order $N/\phi(q)$; and if we take $C > 2B$, then the main term is far larger than the error term, and the main term itself is large. We are now in a good position to define the arcs.

3.3.1 Major Arcs $\mathfrak{M}$

We have shown a condition to ensure that the value of $F_N(x)$ is large, so let's use it. Take $B > 0$ and $Q = \log^B N$, (where we note that $Q = O(N)$). Taking $q \in \{1, 2, ..., Q\}$ and $a \in \{1, 2, ..., q\}$ such that $(a, q) = 1$ define the set

$$\mathfrak{M}_{a,q} = \left\{ x \in [0, 1] : \left| x - \frac{a}{q} \right| < \frac{Q}{N} \right\}.$$

We also need to include 'the end' of the unit interval

$$\mathcal{E} := \left[0, \frac{Q}{N}\right).$$

Although the end just defined is not shown to be large by the previous subsection, it is not so hard to do so using Equation 3.1,

$$\begin{aligned} F_N(0) &= \sum_{p \leq N} \log p \cdot e(2\pi i \cdot 0 \cdot x) \\ &= \sum_{p \leq N} \log p \\ &\leq N + o(N). \end{aligned}$$

Finally, define the major arc $\mathfrak{M}$ as

$$\mathfrak{M} := \bigcup_{q=1}^{Q} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}_{a,q}$$

We should also include the end $\mathcal{E}$, but it extends the length of derivation without contributing much in the way of understanding the method. As such, we will simply ignore it; formally we should have that $\mathfrak{M} := \mathcal{E} \cup \bigcup_{q=1}^{Q} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}_{a,q}$.

There are two important things to notice about the definition of the major arc. The first is, as noted before, that we can apply the Siegel-Walfisz theorem to evaluate $F_N(\frac{a}{q})$. The second is that each interval around $\frac{a}{q}$ is of length $2\frac{Q}{N} = \frac{2\log^B N}{N}$. The importance of this is that as N tends to infinity, the length of the interval tends to 0. Thus as N becomes large, the value of F_N around a point $\frac{a}{q}$ becomes better understood because the value will be closer to $F_N(\frac{a}{q})$.

3.3.2 Minor arcs $\mathfrak{m}$

The minor arc is the complement of the major arc, so

$$\mathfrak{m} := [0,1]\backslash\mathfrak{M}.$$

As noted before, as N tends to infinity the intervals around each a/q tend to zero. As a result, as N tends to infinity, the minor arcs will tend to containing almost all of the interval $[0,1]$. If these arcs have been constructed sufficiently well, the integral over the minor arcs should be negligible compared to that from the major arcs due to cancellation in $F_N(x)$.

3.4 The Singular Series

Finally, we would like to evaluate the integral over the arcs, starting with the major arcs. We currently have that

$$\int_0^1 F_N(x)^3 e(-Nx)dx = \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3\leq N}} \log p_1 \log p_2 \log p_3.$$

In order to calculate the value of this integral only over the major arcs, it is first necessary to show that $F_N(x) \approx F_N(\frac{a}{q})$ for $x \in \mathfrak{M}_{a,q}$. This can be done by finding the Taylor series, but it may be simpler to instead find a non-constant function that agrees with $F_N(x)$ at $x = \frac{a}{q}$. To begin with, we will do this via approximating $F_N(x)e(-Nx)$ around a/q simply by setting it to $F_N\left(\frac{a}{q}\right) e\left(-N\frac{a}{q}\right)$. This serves as a gentle introduction, and in later sections we will cover the more accurate calculation.

$$\begin{aligned}
\int_{\mathfrak{M}} F_N(x)^3 e(-Nx)dx &\approx \int_{\mathfrak{M}} F_N\left(\frac{a}{q}\right)^3 e\left(-N\frac{a}{q}\right) dx \\
&= \sum_{q=1}^{Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} F_N\left(\frac{a}{q}\right)^3 e\left(-N\frac{a}{q}\right) dx \\
&= \frac{2Q}{N} \sum_{q=1}^{Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} F_N\left(\frac{a}{q}\right)^3 e\left(-N\frac{a}{q}\right)
\end{aligned}$$

In Equation 3.4 we found a value for $F_N(\frac{a}{q})$ that we can make use of here. We will ignore the lower order terms for heuristic purposes.

$$\begin{aligned}
F_N\left(\frac{a}{q}\right)^3 e\left(-N\frac{a}{q}\right)\frac{2Q}{N} &\approx \frac{2Q}{N}\sum_{q=1}^{Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\frac{N}{\phi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right)\right)^3 e\left(-N\frac{a}{q}\right) \\
&= \left[2Q\sum_{q=1}^{Q} \frac{1}{\phi(q)^3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right)\right)^3 e\left(-N\frac{a}{q}\right)\right] N^2
\end{aligned}$$

We will be done if we can show that the factor that multiplies N^2 is positive and large enough such that it cannot be cancelled by the contribution from the integral over the minor arcs. A more lengthy and detailed analysis of the integral over the major arcs, where we do not simply replace $F_N(x)e(-Nx)$ with $F_N\left(\frac{a}{q}\right) e\left(-N\frac{a}{q}\right)$ will find a contribution of

$$\mathfrak{S}(N)\frac{N^2}{2} + o(N^2),$$

where

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \frac{\mu(q)}{\phi(q)^3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{aN}{q}\right),$$

and μ is the **Möbius Function** defined as

$$\mu(q) := \begin{cases} 1 & q = 1 \\ (-1)^k & q = p_1 \cdots p_k, \text{ where each prime } p_i \text{ is distinct} \\ 0 & q \text{ has a prime squared as a factor.} \end{cases}$$

Let's now take a look at how to solve this integral more accurately, and prove the weak Goldbach conjecture for sufficiently large integers.

3.5 The Singular Series of Vinogradov's Thoerem

Theorem 3.5.1. **(Vinogradov's Theorem)** There exists an arithmetic function $\mathfrak{S}(N)$ and positive constants c_1 and c_2 such that

$$c_1 < \mathfrak{S}(N) < c_2$$

for all sufficiently large, odd integers N, and

$$r_{P,3}(N) = \mathfrak{S}(N) \frac{N^2}{2\log^3 N}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right)$$

The arithmetic function $\mathfrak{S}(N)$ is called the Singular Series (we will give a more formal definition of this in Equation 3.7, for now we are just noting its name). Every application of the circle method will result in such a series. From here, we would like to specifically show how we find the contribution of

$$\mathfrak{S}(N)\frac{N^2}{2} + o(N^2)$$

from the integral over the major arcs; namely, to prove the following theorem.

Theorem 3.5.2. For positive integers B, C and ϵ such that $C > 2B$, the integral over the major arcs is

$$\begin{aligned} \int_{\mathfrak{M}} F_N(\alpha)^3 e(-N\alpha) d\alpha &= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{\log^{(1-\epsilon)B} N}\right) + O\left(\frac{N^2}{\log^{C-5B} N}\right) \\ &= \mathfrak{S}(N)\frac{N^2}{2} + o(N^2), \end{aligned}$$

where the implied constants depend only on B, C and ϵ.

This will be done in accordance with how it is presented in [Nat13]. We derived in Equation 3.4 that

$$F_N\left(\frac{a}{q}\right) = \frac{N}{\phi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e\left(\frac{ar}{q}\right) + O\left(\frac{N}{\log^{C-B} N}\right).$$

Let us now define the **Ramanujan sum**

$$c_q(N) := \sum_{\substack{k=1 \\ (k,q)=1}}^{q} e\left(\frac{kN}{q}\right).$$

Lemma 3.5.3. We have the following properties of Ramanujan sums.

1.
$$c_q(N) = \sum_{d|(q,N)} \mu\left(\frac{q}{d}\right) d. \tag{3.5}$$

2.
$$(q, N) = 1 \implies c_q(N) = \mu(q).$$

3. $c_q(N)$ is multiplicative, i.e.
$$(m, n) = 1 \implies c_m(N)c_n(N) = c_{mn}(N).$$

Proof. 1. First note that

$$f_d(n) = \sum_{v=1}^{d} e\left(\frac{vn}{d}\right) = \begin{cases} d & \text{if } d|n \\ 0 & \text{if } d \nmid n. \end{cases}$$

The first case follows simply, because under this condition n/d is just an integer and therefore $e(vn/d) = 1$ for all integers v. The result in the second condition follows from the fact if $d \not| n$, then $(d, n) = k$. From this we now have the sum $\sum_{v=1}^{d'k} e(vn'/d')$; these are the d'^{th} roots of units, and we have k copies of each root. We know that the sum of each set is zero (because they sum to the coefficient of $x^{d'-1}$ in $x^{d'} - 1$). Another fact we will use is a property of the Möbius function, namely that

$$\sum_{d|m} \mu(d) = \begin{cases} 1 & \text{if } m = 1 \\ 0 & \text{if } m > 1. \end{cases}$$

We will use these results in the following derivation.

$$\begin{aligned} c_q(n) &= \sum_{\substack{k=1 \\ (k,q)=1}}^{q} e\left(\frac{kn}{q}\right) \\ &= \sum_{k=1}^{q} e\left(\frac{kn}{q}\right) \sum_{d|(k,q)} \mu(d) \\ &= \sum_{d|q} \mu(d) \sum_{\substack{k=1 \\ d|k}}^{q} e\left(\frac{kn}{q}\right) \\ &= \sum_{d|q} \mu(d) \sum_{m=1}^{q/d} e\left(\frac{mn}{q/d}\right) \\ &= \sum_{d|q} \mu(d) f_{q/d}(n) \\ &= \sum_{d|q} \mu(q/d) f_d(n) \\ &= \sum_{\substack{d|q \\ d|n}} \mu(q/d) d \\ &= \sum_{d|(n,q)} \mu(q/d) d \end{aligned}$$

2. This follows immediately from property 1.

3. Since every congruence class relatively prime to mn can be written uniquely in the form $an + a'm$ with $1 \leq m$, $1 \leq a' \leq n$, and $(a,m) = (a',n) = 1$, then if we have that $(m,n) = 1$ we get that

$$\begin{aligned} c_m(N)c_n(N) &= \sum_{\substack{a=1 \\ (a,m)=1}}^{m} e\left(\frac{aN}{m}\right) \sum_{\substack{a'=1 \\ (a',n)=1}}^{n} e\left(\frac{a'N}{n}\right) \\ &= \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \sum_{\substack{a'=1 \\ (a',n)=1}}^{n} e\left(\frac{(an+a'm)N}{mn}\right) \\ &= \sum_{\substack{a''=1 \\ (a'',mn)=1}}^{mn} e\left(\frac{a''N}{mn}\right) \\ &= c_{mn}(N). \end{aligned}$$

□

Putting this together, we have that

$$\begin{aligned} F_N\left(\frac{a}{q}\right) &= \frac{N}{\phi(q)} c_q(a) + O\left(\frac{N}{\log^{C-B} N}\right) \\ &= \frac{\mu(q)}{\phi(q)} N + O\left(\frac{N}{\log^{C-B} N}\right), \end{aligned} \tag{3.6}$$

since we are working under the assumption that $(a,q) = 1$.

Lemma 3.5.4. Continuing under the assumptions tat $C > 2B > 0$, we have that if $\alpha \in \mathfrak{M}_{a,q}$ and $\beta = \alpha - a/q$, then

$$F_N(\alpha) = \frac{\mu(q)}{\phi(q)} u(\beta) + O\left(\frac{Q^2 N}{\log^C N}\right)$$

and

$$F_N(\alpha)^3 = \frac{\mu(q)}{\phi(q)^3} u(\beta)^3 + O\left(\frac{Q^2 N^3}{\log^C N}\right),$$

where $u(\beta) := \sum_{m=1}^{N} e(m\beta)$.

Proof. Given $\alpha \in \mathfrak{M}_{a,q}$, we first note that $\alpha = a/q + \beta$, and that $|\beta| \leq Q/N$. Define

$$\lambda(m) := \begin{cases} \log p & \text{if } m = p \text{ is prime} \\ 0 & \text{otherwise.} \end{cases}$$

Now we have

$$\begin{aligned} F_N(\alpha) - \frac{\mu(q)}{\phi(q)}u(\beta) &= \sum_{p\le N} \log p \cdot e(p\alpha) - \frac{\mu(q)}{\phi(q)} \sum_{m=1}^{N} e(m\beta) \\ &= \sum_{m=1}^{N} \lambda(m)e(m\alpha) - \frac{\mu(q)}{\phi(q)} \sum_{m=1}^{N} e(m\beta) \\ &= \sum_{m=1}^{N} \lambda(m)e\left(\frac{ma}{q} + m\beta\right) - \sum_{m=1}^{N} \frac{\mu(q)}{\phi(q)} e(m\beta) \\ &= \sum_{m=1}^{N} \left(\lambda(m)e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\phi(q)}\right) e(m\beta) \end{aligned}$$

Let's now take some $1 \le x \le N$ and define $A(x)$,

$$\begin{aligned} A(x) &:= \sum_{1\le m\le x} \left(\lambda(m)e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\phi(q)}\right) \\ &= \sum_{1\le m\le x} \lambda(m)e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\phi(q)}x + O\left(\frac{1}{\phi(q)}\right) \\ &= F_x\left(\frac{a}{q}\right) - \frac{\mu(q)}{\phi(q)}x + O(1) \\ &= O\left(\frac{Qx}{\log^C x}\right), \end{aligned}$$

where the final equality follows from Equation 3.6. Next we will use partial summation (see Theorem A.0.1 for more details) and the just derived result to see that

$$\begin{aligned} F_N(\alpha) - \frac{\mu(q)}{\phi(q)}u(\beta) &= A(N)e(N\beta) - 2\pi i\beta \int_1^N A(x)e(x\beta)dx \\ &\ll |A(N)| + |\beta|N \cdot \max\{A(x) : 1 \le x \le N\} \\ &\ll \frac{Q^2N}{\log^C N}, \end{aligned}$$

where the last line follows in part from the fact that $|\beta| \le Q/N$. All it takes to conclude now is a rearranging of this last equation; we find that

$$F_N(\alpha) = \frac{\mu(q)}{\phi(q)}u(\beta) + O\left(\frac{Q^2N}{\log^C N}\right)$$

as desired. The second statement in the lemma follows from this result. □

We still need several results before we can prove Theorem 3.5.2. Let's first define the measurement $\|\alpha\| := \min\{|n-\alpha| : n \in \mathbb{Z}\} = \inf\{\{\alpha\}, 1 - \{\alpha\}\}$.

Lemma 3.5.5. For all real numbers α and all integers $N_1 < N_2$, we have that

$$\sum_{n=N_1+1}^{N_2} e(\alpha n) \ll \min\{N_2 - N_1, \|\alpha\|^{-1}\}.$$

Proof. Reminding ourselves that $|e(\alpha n)| = 1$ for all integers n, we have that

$$\left|\sum_{n=N_1+1}^{N_2} e(\alpha n)\right| \le \sum_{n=N_1+1}^{N_2} 1 = N_2 - N_1.$$

Next, if $\alpha \notin \mathbb{Z}$, then $\|\alpha\| > 0$ and $e(\alpha) \neq 1$. Using that the sum is also a geometric progression, we can derive that

$$\begin{aligned}
\left|\sum_{n=N_1+1}^{N_2} e(\alpha n)\right| &= \left|e(\alpha(N_1+1)) \sum_{n=0}^{N_2-N_1-1} e(\alpha)^n\right| \\
&= |e(\alpha(N_1+1))| \left|\sum_{n=0}^{N_2-N_1-1} e(\alpha)^n\right| \\
&= \left|\sum_{n=0}^{N_2-N_1-1} e(\alpha)^n\right| \\
&= \left|\frac{e(\alpha(N_2-N_1))-1}{e(\alpha)-1}\right| \\
&\leq \frac{2}{|e(\alpha)-1|} \\
&= \frac{2}{|e(\alpha/2)-e(-\alpha/2)|} \\
&= \frac{2}{|2i\sin\pi\alpha|} \\
&= \frac{1}{|\sin\pi\alpha|} \\
&= \frac{1}{\sin(\pi\|\alpha\|)} \\
&\leq \frac{1}{2\|\alpha\|},
\end{aligned}$$

□

where the second last line follows from looking at the four separate cases, and the last inequality follows from the fact that if $0 < \beta < 1/2$, we have that $2\beta < \sin(\pi\beta) < \pi\beta$. One result we will need to use is the case of Waring's problem for $k = 1$, which is solved exactly.

Theorem 3.5.6. **(Waring's problem for $k = 1$)** Recall that $r_{1,s}(N)$ is the number of ways to write N as a sum of s *first* powers, i.e. the number of $s-$tuples $(a_1, a_2, ..., a_s)$ where $a_i \in \mathbb{Z}_{\geq 0}$ $\forall i$. Then define $t_{1,s}(N)$ to be the same thing, but with the added condition that the powers must be of positive integers (i.e. not including zero; $a_i \geq 1$ $\forall i$). This new function states the number of ways to split N into *exactly* s positive parts, whereas $r_{1,s}(N)$ split it into *at most* s positive parts. Then,

$$t_{1,s}(N) = \binom{N-1}{s-1} = \frac{N^{s-1}}{(s-1)!} + O(N^{s-2})$$

for all positive integers N.

Proof. Take $N \geq s$. Note that

$$N = a_1 + \cdots + a_s \iff N - s = (a_1 - 1) + \cdots + (a_s - 1),$$

i.e. N is a sum of s positive parts if and only if $N - s$ is a sum of s non-negative parts. Hence,

$$t_{1,s}(N) = r_{1,s}(N - s).$$

We can now do the proof combinatorially. Take a string of binary digits of length $N - 1$, i.e. so that we have a word of length $N - 1$ where each letter is either 0 or 1. We ensure that the word has exactly $N - s$ zeros, and exactly $s - 1$ ones. This is in fact a representation, as each zero can be though of as contributing a value of one to the value of N, and each one can be though of as a partition between a_i and a_{i+1}. For example, 00100, 01000 and 10000 are three ways to separate 4

into two non-negative parts, corresponding to $2+2$, $1+3$, $0+4$ respectively.
We can now assess how many permutations of this exist to determine the number of ways to separate $N-s$ into s non-negative parts, which as we just established will be akin to separating N into s positive parts. From combinatorics, we take the fact that we have a word of length $N-1$ made from 2 letters where one letter occurs $N-s$ times to conclude that the number of permutations is

$$\frac{(N-1)!}{(N-s)!(s-1)!} = \binom{N-1}{s-1}.$$

□

Lemma 3.5.7. Recalling the definition

$$u(x) = \sum_{m=1}^{N} e(mx),$$

we have that

$$J(N) := \int_{-1/2}^{1/2} u(x)^3 e(-Nx)dx = \frac{N^2}{2} + O(N).$$

Proof. We have that

$$\begin{aligned} J(N) &= \int_{-1/2}^{1/2} u(x)^3 e(-Nx)dx \\ &= \int_{-1/2}^{1/2} \sum_{m_1=1}^{N} \sum_{m_2=1}^{N} \sum_{m_3=1}^{N} e((m_1+m_2+m_3-N)x)dx. \end{aligned}$$

We recognise the integrand as an expression for writing N as a sum of three positive integers, and thus by the previously established orthogonality relationship the integral along a unit (in this case from $-1/2$ to $1/2$ rather than from zero to one) will give a value of 1 for each instance of (m_1, m_2, m_3) such that $m_1+m_2+m_3 = N$ and $1 \le m_i \le N$. So by Theorem 3.5.6

$$J(N) = t_{1,3}(N) = \binom{N-1}{3-1} = \binom{N-1}{2} = \frac{N^2}{2} + O(N).$$

□

We need one more result before we can derive the contribution from our function over the major arcs in the case of Goldbach's weak conjecture. This result lets us illustrate the singular series more clearly. First, recall the Ramanujan sums

$$c_q(N) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{aN}{q}\right).$$

We can give a formal definition of the **Singular Series**,

$$\mathfrak{S}(N) := \sum_{q=1}^{\infty} \frac{\mu(q)c_q(N)}{\phi(q)^3}. \tag{3.7}$$

Theorem 3.5.8. (Singular Series Convergence) The singular series $\mathfrak{S}(N)$ converges absolutely and uniformly, and has the Euler product

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

Also, there exist positive constants c_1, c_2 such that

$$c_1 < \mathfrak{S}(N) < c_2$$

for all positive integers N. Moreover, for any $\epsilon > 0$,

$$\mathfrak{S}(N,Q) := \sum_{q\leq Q}\frac{\mu(q)c_q(N)}{\phi(q)^3} = \mathfrak{S}(N) + O(Q^{-(1-\epsilon)}),$$

where the implied constant depends only on ϵ.

Proof. Notice that

$$\begin{aligned} |c_q(N)| &= \left|\sum_{\substack{a=1\\(a,q)=1}}^{q} e\left(\frac{aN}{q}\right)\right| \\ &\leq \sum_{\substack{a=1\\(a,q)=1}}^{q} 1 \\ &= \phi(q), \end{aligned}$$

implying that $c_q(N) \ll \phi(q)$. By a theorem,

$$\phi(q) > q^{1-\epsilon}$$

for any $\epsilon > 0$ provided q is a sufficiently large integer; the interested reader should refer to Theorem A.16 in [Nat13]. Thus we have that

$$\frac{\mu(q)c_q(N)}{\phi(q)^3} \ll \frac{1}{\phi(q)^2} \ll \frac{1}{q^{2-\epsilon}}.$$

Hence, the singular series converges absolutely and uniformly in N by the Weierstrass criterion for uniform convergence. Furthermore,

$$\mathfrak{S}(N) - \mathfrak{S}(N,Q) = \sum_{q>Q}\frac{\mu(q)c_q(N)}{\phi(q)^3} \ll \sum_{q>Q}\frac{1}{\phi(q)^2} \ll \sum_{q>Q}\frac{1}{q^{2-\epsilon}} \ll \frac{1}{Q^{1-\epsilon}},$$

where the last manipulation follows from the fact that harmonic series converge when their inverse power is more than 1. From Equation 3.5 it can be derived that $c_q(N)$ is a multiplicative function of q, and (where p is prime)

$$c_p(N) = \begin{cases} p-1 & \text{if } p \text{ divides } N \\ -1 & \text{if } p \text{ does not divide } N \end{cases}$$

Now since the arithmetic function

$$\frac{\mu(q)c_q(N)}{\phi(q)^3}$$

is multiplicative in q and $\mu(p^j) = 0$ for all $j \geq 2$, it follows (from Theorem A.28 in [Nat13]) that the singular series has the Euler product

$$\begin{aligned}\mathfrak{S}(N) &= \prod_p \left(1 + \sum_{j=1}^{\infty} \frac{\mu(p^j)c_{p^j}(N)}{\phi(p^j)^3}\right) \\ &= \prod_p \left(1 - \frac{c_p(N)}{\phi(p)^3}\right) \\ &= \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \\ &= \prod_p \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \left(1 - \frac{1}{p^2-3p+3}\right),\end{aligned}$$

and so there exist positive constants c_1, c_2 such that

$$c_1 < \mathfrak{S}(N) < c_2$$

for all positive integers N. □

We can briefly investigate the values of c_1 and c_2. Notice that in the product representation of $\mathfrak{S}(N)$, each term in the finite product on the right is less than 1. So if each term in this product reduces the overall size of the whole product, by removing this finite product we have an upper bound of $\mathfrak{S}(N)$. Similarly, since each term in the first product is large than 1, each term increases the overall size f the function. If we truncate this product to make it a finite product, we thus get a lower bound on the size of $\mathfrak{S}(N)$. For example, we then know that

$$\prod_{p|N} \left(1 + \frac{1}{(p-1)^3}\right)\left(1 - \frac{1}{p^2-3p+3}\right) \leq c_1 \quad \& \quad c_2 \leq \prod_p \left(1 + \frac{1}{(p-1)^3}\right).$$

Though of course, we could remove fewer terms to get a more accurate bound for these constants.

We are now in a position to prove Theorem 3.5.2, a detailed case of evaluating the integral over the major arcs.

Proof. First note that the length of a single major arc $\mathfrak{M}_{a,q}$ is Q/N if $q = 1$ and $2Q/N$ if $q \geq 2$. Using Lemma 3.5.4 we have that

$$\begin{aligned}&\int_{\mathfrak{M}} \left(F_N(\alpha)^3 - \frac{\mu(q)}{\phi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3\right) e(-N\alpha)d\alpha \\ &= \sum_{q\leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}_{a,q}} \left(F_N(\alpha)^3 - \frac{\mu(q)}{\phi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3\right) e(-N\alpha)d\alpha \\ &\ll \sum_{q\leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}_{a,q}} \frac{Q^2N^3}{\log^C N} d\alpha \\ &\ll \sum_{q\leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \frac{Q^3N^2}{\log^C N} \\ &\leq \frac{Q^5N^2}{\log^C N} \\ &\leq \frac{N^2}{\log^{C-5B} N}.\end{aligned}$$

If we have that $\alpha = a/q + \beta \in \mathfrak{M}_{a,q}$, then as before $|\beta| \le Q/N$ and

$$\begin{aligned}
&\sum_{q\le Q}\sum_{\substack{a=0\\(a,q)=1}}^{q}\frac{\mu(q)}{\phi(q)^3}\int_{\mathfrak{M}_{a,q}} u\left(\alpha-\frac{a}{q}\right)^3 e(-N\alpha)d\alpha\\
&=\sum_{q\le Q}\sum_{\substack{a=0\\(a,q)=1}}^{q}\frac{\mu(q)}{\phi(q)^3}\int_{a/q-Q/N}^{a/q+Q/N} u\left(\alpha-\frac{a}{q}\right)^3 e(-N\alpha)d\alpha\\
&=\sum_{q\le Q}\frac{\mu(q)}{\phi(q)^3}\sum_{\substack{a=0\\(a,q)=1}}^{q} e(-Na/q)\int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta\\
&=\sum_{q\le Q}\frac{\mu(q)c_q(-N)}{\phi(q)^3}\int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta\\
&=\mathfrak{S}(N,Q)\int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta.
\end{aligned}$$

Next we want to use Lemma 3.5.5; if we have that $|\beta| \le 1/2$, then

$$u(\beta) \ll |\beta|^{-1}$$

and

$$\begin{aligned}
\int_{Q/N}^{1/2} u(\beta)^3 e(-N\beta)d\beta &\ll \int_{Q/N}^{1/2} |u(\beta)|^3 d\beta\\
&\ll \int_{Q/N}^{1/2} \beta^{-3} d\beta\\
&< \frac{N^2}{Q^2}.
\end{aligned}$$

The last line follows from direct integration and bounding. In a similar manner,

$$\int_{-1/2}^{-Q/N} u(\beta)^3 e(-N\beta)d\beta \ll \frac{N^2}{Q^2}.$$

Making use of Lemma 3.5.7 in combination with the two results just derived, we find that

$$\begin{aligned}
\int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta &= \int_{-1/2}^{1/2} u(\beta)^3 e(-N\beta)d\beta + O\left(\frac{N^2}{Q^2}\right)\\
&= \frac{N^2}{2} + O(N) + O\left(\frac{N^2}{Q^2}\right)\\
&= \frac{N^2}{2} + O\left(\frac{N^2}{Q^2}\right).
\end{aligned}$$

From Theorem 3.5.8, we know that

$$\mathfrak{S}(N,Q) = \mathfrak{S}(N) + O\left(\frac{1}{Q^{1-\epsilon}}\right).$$

To finish the proof, we put all this together,

$$\begin{aligned}
\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha &= \mathfrak{S}(N,Q)\int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta + O\left(\frac{N^2}{\log^{C-5B} N}\right)\\
&= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{Q^{1-\epsilon}}\right) + O\left(\frac{N^2}{\log^{C-5B} N}\right)\\
&= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{\log^{(1-\epsilon)B} N}\right) + O\left(\frac{N^2}{\log^{C-5B} N}\right)
\end{aligned}$$

□

So even just to get an asymptotic formula for the integral over the major arcs took a lot of work; yet there is still a lot more to do in order to give the proof of the weak conjecture for sufficiently large integers. We must get an asymptotic formula for the integral over the minor arcs, and we need to achieve this such that the contribution is negligible compared to the one just found.

3.6 Minor arcs' Contribution

In order to derive the asymptotic estimate over the minor arcs, we need to first derive several results. It has been mentioned a few times that bounding the integral over the minor arcs is the hardest part, and the several lemmas that follow, which are required for the bound, are testament to that.

3.6.1 An Exponential Sum Over Primes

Theorem 3.6.1. **(Vinogradov)** If

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2},$$

where a and q are integers such that $1 \leq q \leq N$ and $(a, q) = 1$, then

$$F_N(\alpha) \ll \left(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2}q^{1/2}\right) \log^4 N.$$

This is the main result we want to achieve in this subsection. We do not want to deviate too much from the circle method however, and the results required to prove this theorem (and the theorem itself) are specific results needed to apply the circle method successfully in this case. Since these results are not generally applicable with regards to the circle method, we will mostly just state the results.

The proof of this theorem follows from several lemmas.

Lemma 3.6.2. **(Vaughan's identity)** For $u \geq 1$, let

$$M_u(k) := \sum_{\substack{d|k \\ d \leq u}} \mu(d).$$

Let $\Phi(k, l)$ be an arithmetic function of two variables. Then

$$\sum_{u<l\leq N} \Phi(1, l) + \sum_{u<k\leq N} \sum_{u<l\leq \frac{N}{k}} M_u(k)\Phi(k, l) = \sum_{d\leq u} \sum_{u<l\leq \frac{N}{d}} \sum_{m\leq \frac{N}{ld}} \mu(d)\Phi(dm, l).$$

The next lemma we will prove. First, we remind the reader of the **von Mangoldt Function**,

$$\Lambda(l) = \begin{cases} \log p & \text{if } l = p^k \text{ for some prime } p \text{ and some integer } k \geq 1 \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 3.6.3. For every real number α, we have that

$$F_N(\alpha) = S_1 - S_2 - S_3 + O(N^{1/2}),$$

where

$$S_1 := \sum_{d \le N^{2/5}} \sum_{l \le \frac{N}{d}} \sum_{m \le \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm),$$

$$S_2 := \sum_{d \le N^{2/5}} \sum_{l \le N^{2/5}} \sum_{m \le \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm),$$

$$S_3 := \sum_{k > N^{2/5}} \sum_{N^{2/5} < l \le \frac{N}{k}} M_{N^{2/5}}(k)\Lambda(l)e(\alpha kl).$$

(Note that in the definition of S_3, k only makes sense if $k \le N^{3/5}$, since if larger than this then l can take no value.)

Proof. We want to apply Lemma 3.6.2 with

$$u = N^{2/5},$$

and

$$\Phi(k, l) = \Lambda(l)e(\alpha kl).$$

The first term of the left hand side of the equality in Lemma 3.6.2 will then be

$$\begin{aligned}
\sum_{u < l \le N} \Phi(1, l) &= \sum_{N^{2/5} < l \le N} \Lambda(l)e(\alpha l) \\
&= \sum_{l=1}^{N} \Lambda(l)e(\alpha l) - \sum_{l \le N^{2/5}} \Lambda(l)e(\alpha l) \\
&= \sum_{p^k \le N} (\log p)e(\alpha p^k) + O(N^{2/5}\log N) \\
&= \sum_{p \le N} (\log p)e(\alpha p) + \sum_{\substack{p^k \le N \\ k \ge 2}} (\log p)e(\alpha p^k) + O(N^{2/5}\log N) \\
&= F_N(\alpha) + O\left(\sum_{\substack{p^k \le N \\ k \ge 2}} \log p \right) + O(N^{2/5}\log N) \\
&= F_N(\alpha) + O\left(\sum_{p^2 \le N} \left[\frac{\log N}{\log p} \right] \log p \right) + O(N^{2/5}\log N) \\
&= F_N(\alpha) + O\left(\pi(N^{1/2}) \log N \right) + O(N^{2/5}\log N) \\
&= F_N(\alpha) + O(N^{1/2}),
\end{aligned}$$

where the second last equality follows from a theorem of Chebyshev (which states that there exist positive constants c_1, c_2 such that

$$c_1 x \le \vartheta(x) \le \psi(x) \le \pi(x)\log x \le c_2 x, \tag{3.8}$$

where $\vartheta(x) := \sum_{p \le x} \log p$ and $\psi(x) := \sum_{p^k \le x} \log p$ are types of prime counting functions). The next term in the identity in Lemma 3.6.2 is

$$\sum_{N^{2/5} < k \le N} \sum_{N^{2/5} < l \le \frac{N}{k}} M_{N^{2/5}}(k)\Lambda(l)e(\alpha kl) = \sum_{N^{2/5} < k \le N^{3/5}} \sum_{N^{2/5} < l \le \frac{N}{k}} M_{N^{2/5}}(k)\Lambda(l)e(\alpha kl) = S_3.$$

The final term is given by

$$\begin{aligned}
&\sum_{d\leq N^{2/5}} \sum_{N^{2/5}<l\leq \frac{N}{k}} \sum_{m\leq \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm) \\
&= \sum_{d\leq N^{2/5}} \sum_{l\leq \frac{N}{k}} \sum_{m\leq \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm) - \sum_{d\leq N^{2/5}} \sum_{l\leq N^{2/5}} \sum_{m\leq \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm) \\
&= S_1 - S_2.
\end{aligned}$$

Putting all of this together, we have that

$$\left(F_N(\alpha) + O(N^{1/2})\right) + (S_3) = S_1 - S_2$$

according to the identity. The result follows trivially. □

There are three more lemmas that are needed to prove Theorem 3.6.1; we state them here as one, and prove it's second statement.

Lemma 3.6.4. If

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2},$$

where $1 \leq q \leq N$ and $(a, q) = 1$, then

1. $|S_1| \ll \left(\frac{N}{q} + N^{2/5} + q\right)\log^2 N.$
2. $|S_2| \ll \left(\frac{N}{q} + N^{4/5} + q\right)\log^2 N.$
3. $|S_3| \ll \left(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2}q^{1/2}\right)\log^4 N.$

In order to prove the second result, we need an additional result. Under the conditions of Lemma 3.6.4, we have that for any real number $U \geq 1$, and positive integer N, we have that

$$\sum_{a\leq k\leq U} \min\left\{\frac{N}{k}, \frac{1}{\|\alpha k\|}\right\} \ll \left(\frac{N}{q} + U + q\right)\log 2qU. \tag{3.9}$$

Proof. If we have $d \leq N^{2/5}$ and $l \leq N^{2/5}$, then $dl \leq N^{4/5}$ follows naturally. Using the substitution $k = dl$, we see that

$$\begin{aligned}
S_2 &= \sum_{d\leq N^{2/5}} \sum_{l\leq N^{2/5}} \sum_{m\leq \frac{N}{dl}} \mu(d)\Lambda(l)e(\alpha dlm) \\
&= \sum_{k\leq N^{4/5}} \left(\sum_{m\leq \frac{N}{k}} e(\alpha km)\right)\left(\sum_{\substack{k=dl\\ d,l\leq N^{2/5}}} \mu(d)\Lambda(l)\right).
\end{aligned}$$

Now since μ only takes values of $\{0, 1, -1\}$, it follows that

$$\sum_{\substack{k=dl\\ d,l\leq N^{2/5}}} \mu(d)\Lambda(l) \ll \sum_{\substack{k=dl\\ d,l\leq N^{2/5}}} \Lambda(l) \leq \sum_{l|k} \Lambda(l) = \log k \ll \log N.$$

Using this, along with Equation 3.9 we can see that

$$\begin{aligned} S_2 &\ll \log N \sum_{k \leq N^{4/5}} \sum_{m \leq N/k} e(\alpha k m) \\ &\ll \sum_{k \leq N^{4/5}} \min\left\{\frac{N}{k}, \|\alpha k\|^{-1}\right\} \log N \\ &\ll \left(\frac{N}{q} + N^{4/5} + q\right) \log^2 N. \end{aligned}$$

□

Stringing all these results together in the right way will give a proof of Theorem 3.6.1.

3.6.2 Asymptotic Formula from the Minor Arcs

We will be ready to prove the asymptotic formula after we state one result from Dirichlet on Diophantine approximation.

Theorem 3.6.5. **(Dirichlet)** Let α and Q be real numbers such that $Q \geq 1$. There exist integers a, q such that

$$1 \leq q \leq Q, \qquad (a, q) = 1,$$

and

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

There are various proofs of this theorem, the interested reader can look at theorem 4.1 in [Nat13]. We are now ready.

Theorem 3.6.6. **(Asymptotic Formula)** For any $B > 0$, we have that

$$\int_{\mathfrak{m}} F_N(\alpha)^3 e(-\alpha N) d\alpha \ll \frac{N^2}{\log^{(B/2)-5} N},$$

where the implied constant depends only on B.

Proof. Let $\alpha \in \mathfrak{m} = [0,1] \backslash \mathfrak{M}$. By Theorem 3.6.5 we know that for any such real number α there exists some fraction $a/q \in [0,1]$ where $1 \leq q \leq N/Q$ and $(a, q) = 1$ such that

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{Q}{qN} \leq \min\left\{\frac{Q}{N}, \frac{1}{q^2}\right\}.$$

Now if $q \leq Q$, then $\alpha \in \mathfrak{M}_{a,q} \subset \mathfrak{M}$; but we specifically assumed that $\alpha \notin \mathfrak{M}$. Thus we see that

$$Q < q \leq \frac{N}{Q}.$$

From the main theorem of the last subsection, Theorem 3.6.1 (and reminding ourselves of the condition that we are taking $B > 0$ and $Q = \log^B N$), we can do some manipulations to find that

$$\begin{aligned}F(\alpha) &\ll \left(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2}q^{1/2}\right)\log^4 N \\ &\ll \left(\frac{N}{\log^{B/2} N} + N^{4/5} + N^{1/2}\left(\frac{N}{\log^B N}\right)^{1/2}\right)\log^4 N \\ &\ll \frac{N}{\log^{(B/2)-4} N}.\end{aligned}$$

From the derivation in Lemma 3.2.1, we have that

$$\int_0^1 |F(\alpha)|^2 d\alpha \ll N \log N.$$

Using this, we get that

$$\begin{aligned}\int_{\mathfrak{m}} |F(\alpha)|^3 d\alpha &\ll \sup\{|F(\alpha)| : \alpha \in \mathfrak{m}\} \int_0^1 |F(\alpha)|^2 d\alpha \\ &\ll \frac{N}{\log^{(B/2)-4} N} \int_0^1 |F(\alpha)|^2 d\alpha \\ &\ll \frac{N^2}{\log^{(B/2)-5} N}.\end{aligned}$$

□

3.7 Proof of the Asymptotic Formula

We have everything we need to prove Theorem 3.5.1, that Goldbach's weak conjecture is true for all sufficiently large integers. Let's piece it together.

Theorem 3.7.1. (Vinogradov) Let $\mathfrak{S}(N)$ be the singular series for the weak Goldbach conjecture. Then for all sufficiently large, odd integers N and for all $A > 0$, we have that

$$R_3(N) = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{\log^A N}\right),$$

where the implied constant depends only on A.

Proof. Using what we have shown in the previous sections, specifically Theorem 3.5.2 and Theorem 3.6.6, we have that for any positive numbers B, C, ϵ such that $C > 2B$ and $\epsilon < 1$,

$$\begin{aligned}R_3(N) &= \int_0^1 F_N(\alpha)^3 e(-N\alpha) d\alpha \\ &= \int_{\mathfrak{M}} F_N(\alpha)^3 e(-N\alpha) d\alpha + \int_{\mathfrak{m}} F_N(\alpha)^3 e(-N\alpha) d\alpha \\ &= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{\log^{(1-\epsilon)B} N}\right) + O\left(\frac{N^2}{\log^{C-5B} N}\right) + O\left(\frac{N^2}{\log^{(B/2)-5} N}\right),\end{aligned}$$

where the implied constants depend only on B, C, ϵ. Now take any $A > 0$, and let $B = 2A + 10$, $C = A + 5B$ and $\epsilon = 1/2$. This will give us

$$\min\{(1-\epsilon)B, C - 5B, (B/2) - 5\} = \min\{A + 5, A, A\} = A,$$

and hence

$$R_3(N) = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{\log^A N}\right).$$

□

With this preliminary reorganising of what we already know, we are sufficiently ready to state the proof of Theorem 3.5.1. We restate the theorem here for the reader's benefit.

Theorem 3.7.2. (Vinogradov's Theorem) There exists an arithmetic function $\mathfrak{S}(N)$ and positive constants c_1 and c_2 such that

$$c_1 < \mathfrak{S}(N) < c_2$$

for all sufficiently large, odd integers N, and

$$r_{P,3}(N) = \mathfrak{S}(N)\frac{N^2}{2\log^3 N}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right)$$

Proof. We want to bound $R_3(N)$ above and below; let's start with an upper bound.

$$\begin{aligned} R_3(N) &= \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3 \\ &\leq \log^3 N \sum_{p_1+p_2+p_3=N} 1 \\ &= r_{P,3}(N)\log^3 N. \end{aligned}$$

Let's define $r_\delta(N)$ as the number of representations $N = p_1 + p_2 + p_3$ such that $p_i \leq N^{1-\delta}$ for some i, with the additional condition that $0 < \delta < 1/2$. This leads us to

$$\begin{aligned} r_\delta(N) &\leq 3 \sum_{\substack{p_1+p_2+p_3=N \\ p_1 \leq N^{1-\delta}}} \\ &\ll \sum_{p_1 \leq N^{1-\delta}} \left(\sum_{p_2+p_3=N-p_1} 1 \right) \\ &\leq \sum_{p_1 \leq N^{1-\delta}} \left(\sum_{p_2 < N} 1 \right) \\ &\leq \pi(N^{1-\delta})\pi(N) \\ &\ll \frac{N^{2-\delta}}{\log^2 N}. \end{aligned}$$

Next for the lower bound,

$$\begin{aligned} R_3(N) &\geq \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3 > N^{1-\delta}}} \log p_1 \log p_2 \log p_3 \\ &\geq (1-\delta)^3 \log^3 N \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3 > N^{1-\delta}}} 1 \\ &\geq (1-\delta)^3 \log^3 N (r_{P,3}(N) - r_\delta(N)) \\ &\gg (1-\delta)^3 \log^3 N \left(r_{P,3}(N) - \frac{N^{2-\delta}}{\log^2 N} \right) \end{aligned}$$

where the last line follows from the prior result. This last derivation also allows us to see that

$$(1-\delta)^{-3}R_3(N) + N^{2-\delta}\log N \gg (\log^3 N) r_{P,3}(N). \tag{3.10}$$

Now if we take $0 < \delta < 1/2$, we get that

$$0 < (1-\delta)^{-3} - 1 = \frac{1-(1-\delta)^3}{(1-\delta)^3} \leq 8\left(1-(1-\delta)^3\right) < 24\delta.$$

From Theorem 3.7.1 and Theorem 3.5.8, we have that $R_3(N) \ll N^2$. Using this, as well as the upper bound for the first inequality, and Equation 3.10 for the second, we get

$$\begin{aligned} 0 \leq (\log^3 N) r_{P,3}(N) - R_3(N) &\ll \left((1-\delta)^{-3} - 1\right) R_3(N) + (\log N) N^{2-\delta} \\ &\ll \delta R_3(N) + (\log N) N^{2-\delta} \\ &\ll \delta N^2 + (\log N) N^{2-\delta} \\ &= N^2\left(\delta + \frac{\log N}{N^\delta}\right). \end{aligned}$$

this is all dependent on $0 < \delta < 1/2$, and let's maintain this while choosing

$$\delta = \frac{2\log\log N}{\log N}.$$

Then we get that

$$\delta + \frac{\log N}{N^\delta} = \frac{2\log\log N}{\log N} + \frac{\log N}{\log^2 N} \ll \frac{\log\log N}{\log N},$$

and by inserting this result into the previous one, we find that

$$0 \leq (\log^3 N) r_{P,3}(N) - R_3(N) \ll \frac{N^2 \log\log N}{\log N}.$$

By rearranging this result, and then applying Theorem 3.7.1, we ge that

$$\begin{aligned} (\log^3 N) r_{P,3}(N) &= R_3(N) + O\left(\frac{N^2\log\log N}{\log N}\right) \\ &= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{\log^A N}\right) + O\left(\frac{N^2\log\log N}{\log N}\right) \\ &= \mathfrak{S}(N)\frac{N^2}{2}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right). \end{aligned}$$

Once we remove the $\log^3 N$, we will be done,

$$r_{P,3}(N) = \mathfrak{S}(N)\frac{N^2}{2\log^3 N}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right).$$

□

3.8 Summary for Weak Goldbach

We have gone through Vinogradov's impressive proof of the asymptotic formula for the weak Goldbach conjecture, and this provides an impression of how difficult it can be to apply the circle method; the method can tell us a lot when applied successfully, but that doesn't mean it can tell us everything. It would feel natural to conclude from this exposition that Vinogradov had proved the weak Goldbach conjecture, but, alas, this was not sufficient. We know that $R_3(N) > 0$ for large enough N, but we would like to have a specific bound B such that $R_3(N) > 0$ for all $N \geq B$.

Unfortunately, when a bound was eventually identified from the inner workings of the proof, it turned out to be far too large to check all the remaining cases computationally. Allegedly Vinogradov's student K.G Borozdkin found a bound of $e^{e^{16.038}} \approx 3^{3^{15}} = 3^{14,348,907}$ in his unpublished PhD thesis (apparently this bound was also presented at a conference in the 1950's, but finding an actual reference for either of these resources has been unsuccessful). If we assume this bound to have been found, it represents a number with at least $4,008,660$ digits; perhaps now it is clear why it is too large. For further success with this approach, the bound would have to be improved significantly.

In 1989 J.-R. Chen and T. Wang improved the bound to $3.33 \cdot 10^{43,000}$ [CW89], and in 2002 M.-Ch. Liu and T. Wang improved it significantly further to $2 \cdot 10^{1346}$ [LW02]. For context of scale, there have been 10^{30} picoseconds since the assumed beginnings of the universe, and there are predicted to be around 10^{80} protons (the Eddington number) in our observable universe. There was still some way to go to refine the bound to something manageable.

Finally, in a preprint by the Peruvian mathematician Harald Helfgott, the bound was brought down to 10^{27} [Hel13]. Given that the conjecture had already been checked for all integers less than $8.875 \cdot 10^{30}$, this could be the final step of the proof. Having first been conjectured in 1742, the question may finally have a valid verification (that is of course if and when the proof is accepted in a peer-reviewed mathematics journal, although in the years since Helfgott's preprint no major errors have yet been found).

We note that Helfgott managed to reduce the bound by using "the close relation between the circle method and the large sieve". Taking some ideas from an optimised large sieve for primes, and applying those ideas to the circle method, yielded enough of a gain. So even if the circle method doesn't result in a complete proof in the beginning, it can be optimised to improve the bound until it is sufficient. Helfgott is in the process of writing a book for the purpose of providing a peer-reviewed form of the proof to anybody interested. The book explains the analytical techniques used along the way, a large part of this is of course the circle method - the book is currently projected to be five hundred pages [Hel].

3.9 The Strong Goldbach Conjecture

Having finalised a proof of Goldbach's weak conjecture, what can we say about the strong one; how far has the circle method taken us to proving its validity? There appears to be very little literature on the application of the circle method on the strong Goldbach conjecture, which indicates that there has not been much success. What can be demonstrated is that if we approach it in the same way as has been done for the weak conjecture, the minor arc is not sufficiently well bounded.

$$\begin{aligned}\left|\int_{\mathfrak{m}} F_N(x)^2 e(-Nx)dx\right| &\leq \int_0^1 |F_N(x)|^2 dx \\ &\leq N\log N + o(N\log N),\end{aligned}$$

by Lemma 3.2.1. However, it turns out that this is the same order as we expect to see from the integral over the major arcs. There may yet be hope for the future, as it may be possible to bound the integral over the minor arcs more significantly. Notice that we do not need to bound

$$\int_0^1 |F_N(x)|^2 dx,$$

but instead we have to bound the oscillating function

$$\left|\int_{\mathfrak{m}} F_N(x)^2 e(-Nx)dx\right|.$$

As such, the oscillations likely result in significant cancellation, and this hypothesis can be given extra weight through numerical calculations. As a final remark, note what happens when we input an even integer into the singular series, using a representation of the singular series that was found during the proof of Theorem 3.5.8,

$$\begin{aligned}\mathfrak{S}(2N) &= \prod_{p}\left(1-\frac{c_p(2N)}{\phi(p)^3}\right)\\ &= \left(1-\frac{c_2(2N)}{\phi(2)^3}\right)\prod_{\substack{p\\ p\neq 2}}\left(1-\frac{c_p(2N)}{\phi(p)^3}\right)\\ &= \left(1-\frac{1}{1^3}\right)\prod_{\substack{p\\ p\neq 2}}\left(1-\frac{c_p(2N)}{\phi(p)^3}\right)\\ &= 0\cdot\prod_{\substack{p\\ p\neq 2}}\left(1-\frac{c_p(2N)}{\phi(p)^3}\right)\\ &= 0.\end{aligned}$$

The third equality follows from a fact about Ramanujan sums, namely that

$$c_p(k) = \begin{cases} p-1 & \text{if } p|k \\ -1 & \text{otherwise.}\end{cases}$$

Thus $\mathfrak{S}(N) = 0$ for all even N, and the contribution to the integral from the major arc is zero (according to the asymptotic formula we put a lot of work into finding). In some sense, the Singular Series 'knows' that the Goldbach conjecture is hard.

Chapter 4

Integers as sums of three Triangular Numbers

4.1 A theorem of Gauss

The purpose of this chapter is to see how what has been so far can be applied to another problem, and to see what kind of difficulties arise and how quickly. As a bachelor thesis primarily devoted to learning what the circle method is, it makes sense to include a short section at the end seeing what can be done with the method to reinforce learning.

Following an in depth look at the circle method via its involvement in Vinogradov's theorem, we would like to see how we could apply the method to a theorem of Gauss; that every positive integer is a sum of three triangular numbers (including $t_0 = 0$).

Theorem 4.1.1. Defining the **Triangular Numbers**

$$T := \left\{ \frac{k(k+1)}{2} : k \in \mathbb{Z}_{\geq 0} \right\},$$

we have that

$$r_{T,3}(n) \geq 1$$

for all $n \in \mathbb{Z}_{\geq 0}$.

Proof. The first part of this proof would be to show that all positive integers m of the form

$$m \equiv 3 \bmod 8$$

can be written as a sum of three square numbers. As this proof is only secondary to the topic of this thesis, we will assume this part of the proof; the interested reader can for instance look at [Ank57], or at a proof of Legendre's three square theorem.

Take any positive integer n, then by above we have that

$$8n + 3 = (2x+1)^2 + (2y+1)^2 + (2z+1)^2$$

where $x, y, z \in \mathbb{Z}_{\geq 0}$. Due to the congruence conditions, we must have that each square is odd, hence the form of each square. Manipulating this, we find that

$$\begin{aligned}8n + 3 &= 4x^2 + 4x + 4y^2 + 4y + 4z^2 + 4z + 3 \\ 8n &= 4x^2 + 4x + 4y^2 + 4y + 4z^2 + 4z \\ n &= \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2}.\end{aligned}$$

So n can be represented as a sum of three triangular numbers. □

4.2 Setup

We can take either the unweighted generating function

$$f_N(x) := \sum_{t \in T_N} e(tx),$$

where T_N is the set of triangular numbers that are at most N, or the weighted version

$$F_N(x) := \sum_{t \in T_N} \log t \cdot e(tx).$$

If we look at the cubes of these two, we find

$$\begin{aligned}f_N(x)^3 &= \sum_{n=0}^{3N} r_{T_N,3}(n) e(nx), \\ F_N(x)^3 &= \sum_{n=0}^{3N} R_3(n) e(nx),\end{aligned}$$

where

$$R_3(n) := \sum_{\substack{t_1+t_2+t_3=n \\ t_1,t_2,t_3 \in T_N}} \log t_1 \log t_2 \log t_3.$$

Finally, application of our orthogonality relationship gives

$$\begin{aligned}r_{T_N,3}(n) &= \int_0^1 f_N(x)^3 e(-nx) dx \\ R_3(n) &= \int_0^1 F_N(x)^3 e(-nx) dx.\end{aligned}$$

Note that we once again have that

$$R_3(n) \leq (\log N)^3 r_{T_N,3}(n),$$

and therefore that

$$R_3(n) \implies r_{T_N,3}(n) \geq 1.$$

4.3 Large $F_N(x)$?

In order to select the arcs we need to have some idea of where $F_N(x)$ (or $f_N(x)$) is large. How are we to determine this? The manipulations used in our exploration of Vinogradov's theorem involved manipulating the generating function such that it was a multiple of the sum of the log of primes up to some point; because then we could apply the Siegel-Walfisz theorem. However we are working with the set of triangular numbers, not primes; so perhaps this isn't a viable strategy here.

Let's blindly try the same approach and see where it leads us.

$$\begin{aligned} F_N\left(\frac{a}{q}\right) &= \sum_{t \in T} \log t \cdot e\left(t\frac{a}{q}\right) \\ &= \sum_{r=1}^{q} \sum_{\substack{t \equiv r \bmod q \\ t \leq N}} \log t \cdot e\left(\frac{ar}{q}\right) \\ &= \sum_{r=1}^{q} e\left(\frac{ar}{q}\right) \sum_{\substack{t \equiv r \bmod q \\ t \leq N}} \log t. \end{aligned}$$

This is familiar, but the Siegel Walfisz theorem tells us about the distribution of primes in congruence classes, not of triangular numbers. Perhaps there are other things we can try however. First note that if the largest triangular number is at most N, and it is of the form $t = z(z+1)/2$, we have that

$$\begin{aligned} \frac{z(z+1)}{2} &\leq N \\ z^2 + z &\leq 2N \\ z^2 + z - 2N &\leq 0 \\ \implies z = \frac{-1 + \sqrt{1+8N}}{2} &\approx \sqrt{2N}, \end{aligned}$$

since z must be positive, and when N is large the last approximation is very close to the true value. Now we can try to rearrange what we had.

$$\begin{aligned} F_N\left(\frac{a}{q}\right) &= \sum_{t \in T} \log t \cdot e\left(t\frac{a}{q}\right) \\ &\approx \sum_{1 \leq z \leq \sqrt{2N}} \log\left(\frac{z(z+1)}{2}\right) \cdot e\left(t_z\frac{a}{q}\right) \\ &= \sum_{1 \leq z \leq \sqrt{2N}} (\log(z) + \log(z+1) - \log(2))\, e\left(t_z\frac{a}{q}\right) \\ &= \sum_{1 \leq z \leq \sqrt{2N}} \log(z) e\left(t_z\frac{a}{q}\right) + \sum_{1 \leq z \leq \sqrt{2N}} \log(z+1) e\left(t_z\frac{a}{q}\right) - \log(2) \sum_{1 \leq z \leq \sqrt{2N}} e\left(t_z\frac{a}{q}\right) \end{aligned}$$

The hope here was to create a sum of the form $\sum_{1 \leq z \leq \sqrt{2N}} \log z = \log(\lfloor \sqrt{2N} \rfloor !)$, and then to use Stirling's approximation. However due to each $\log z$ being multiplied by a member of the unit circle, this is clearly not possible.

It would appear that for this application, it would be wiser to use the unweighted generating function. Moreover, taking an approach similar to that taken for Goldbach's problem doesn't seem a natural choice; the problem we are tackling now takes, in some sense, all nonnegative integers as its primary set, but Goldbach's problem takes prime numbers. As such, it would likely be more fruitful to approach the problem in the way Waring's problem was approached as it is a more similar problem.

We can get a feel for how Waring's problem is approached by reviewing the methods used in [Vau97] to show that $G(k) \leq 2^k + 1$. The proof of this around the same length as the proof of Vinogradov's theorem, so there are many results found along the way. Here are two of the first results used in this proof.

Theorem 4.3.1. **(Weyl)** Let

$$T(\phi) = \sum_{x=1}^{Q} e(\phi(x)),$$

where ϕ is an arbitrary arithmetical function. Then

$$|T(\phi)|^{2^j} \leq (2Q)^{2^j - j - 1} \sum_{|h_1|<Q} \cdots \sum_{|h_j|<Q} T_j,$$

where

$$T_j = \sum_{x \in I_j} e(\Delta_j(\phi(x); h_1, ..., h_j))$$

and Δ_j is the j^{th} iterate of the forwards difference operator, and the intervals $I_j = I_j(h_1, ..., h_j)$ (possibly empty) satisfy

$$I_1(h_1) \subset [1, Q], \qquad I_j(h_1, ..., h_j) \subset I_{j-1}(h_1, ..., h_{j-1}).$$

Theorem 4.3.2. **(Weyl's inequality)** Suppose that $(a, q) = 1$,

$$|\alpha - a/q| \leq \frac{1}{q^2}, \qquad \phi(x) = \alpha x^k + \alpha_q x^{k-1} + \cdots + \alpha_{k-1} x + \alpha_k$$

and

$$T(\phi) = \sum_{x=1}^{Q} e(\phi(x)).$$

Then

$$T(\phi) \ll Q^{q+\epsilon}(q^{-1} + Q^{-1} q Q^{-k})^{1/K},$$

where $K = 2^{k-1}$.

Since these theorems take in arbitrary arithmetical functions, there is hope we could apply them in our scenario. Firstly, we can write our generating function in a different form,

$$\begin{aligned} f_N(x) &= \sum_{t \in T_N} e(tx) \\ &\approx \sum_{k=1}^{\sqrt{2N}} e\left(\frac{k^2+k}{2} x\right) \\ &= \sum_{k=1}^{\sqrt{2N}} e\left(\frac{k^2}{2} x\right) e\left(\frac{k}{2} x\right). \end{aligned}$$

This looks a little close to the desired form in the theorems above, but there is still more to do. Perhaps a future thesis could attempt to see how the method could be applied to this problem with more success.

4.4 Summary

Clearly problems applying the method arise very quickly. Creating an integral representation is easy to do for any problem of an additive nature, but the following step of determining where the integrand is large is certainly difficult. Visual software graphing the integrand could be useful in developing a picture of the integrand, but even that could only do so much to determine specific input values to sequester enough of the large parts of the function to leave only a minor quantity for the minor arcs.

The message however is clear: application of the circle method is probably never going to be straightforward. There will be a lot of difficulty doing any more than just representing the problem through a generating function; and the more progress is made, the harder the tasks are that need to be done next.

It would be of great interest to see how users of the method discovered where to set the major arcs; was there some general approach they used, more trial and error, or some level of understanding that indicated to them what to try.

Conclusion

It has been just over one hundred years since the inception of the circle method; we have explored what the method is, how it was first discovered, and seen a detailed application of it to Vinogradov's theorem. The method applies analytic function theory to show that relationships of an additive nature hold (or do not hold) asymptotically. The method has seen successive improvements in effectiveness and generalisation as it has been moulded to attack different problems.

It's effectiveness is best seen by the fact that it has contributed the most to solving Waring's problem, and has also seen considerable success in attacking all Waring-type problems, as well as to the weak Goldbach conjecture. The exposition of it being used to prove Vinogradov's theorem does also highlight the fact that is is not a simple method to use. In order to prove Vinogradov's theorem it was necessary to prove several other results beforehand. An exposition is one thing, but applying the method in a novel way without knowing what results could be of use and will be needed is far more difficult.

The final chapter looking at how the method can be applied to representing positive integers as triangular numbers demonstrates that even far before the 'hardest part' of the method (bounding the minor arcs), problems arise quickly; how does one even determine how to partition the unit interval?

Continuing the dialogue of this report, one might be inclined to look in more detail at how the circle method was applied to Waring's problem, or a variant of Waring's problem, and highlight the differences in approach that the two problems required from the method. Following this, it would be useful to see if any of those insights suggest what might be the best strategy to employ to apply the method successfully to representing positive integers as sums of three triangular numbers.

Appendix A

Partial Summation

Theorem A.0.1. **Partial Summation** Take two arithmetic functions, $f(n)$ and $u(n)$. Define the sum function

$$U(t) = \sum_{n \leq t} u(n).$$

Let a, b be nonnegative integers with $a < b$. Then we have that

$$\sum_{n=a+1}^{b} u(n)f(n) = U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)).$$

Let x, y be real numbers such that $0 \leq y < x$. If $f(t)$ is a function with a continuous derivative on the interval $[y, x]$, then

$$\sum_{y < n \leq x} u(n)f(n) = U(x)f(x) - U(y)f(y) - \int_y^x U(t)f'(t)dt.$$

In particular, we have that

$$\sum_{n \leq x} u(n)f(n) = U(x)f(x) - \int_1^x U(t)f'(t)dt.$$

Proof. The first part follows simply from evaluating the sum,

$$\begin{aligned}\sum_{n=a+1}^{b} u(n)f(n) &= \sum_{n=a+1}^{b} (U(n) - U(n-1))f(n) \\ &= \sum_{n=a+1}^{b} U(n)f(n) - \sum_{n=a}^{b-1} U(n)f(n+1) \\ &= U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)).\end{aligned}$$

Now if we take a continuously differentiable $f(t)$ on $[y, x]$, we have that

$$f(n+1) - f(n) = \int_n^{n+1} f'(t)dt,$$

and

$$U(n)(f(n+1)-f(n)) = \int_n^{n+1} U(t)f'(t)dt.$$

Letting $a = \lfloor y \rfloor$, and $b = \lfloor x \rfloor$, we get that

$$\begin{aligned}
\sum_{y<n\leq x} u(n)f(n) &= \sum_{n=a+1}^{b} u(n)f(n) \\
&= U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1)-f(n)) \\
&= U(x)f(b) - U(y)f(a+1) - \sum_{n=a+1}^{b-1} \int_n^{n+1} U(t)f'(t)dt \\
&= U(x)f(x) - U(y)f(y) - U(x)(f(x)-f(b)) - U(y)(f(a+1)-f(y)) - \int_{a+1}^{b} U(t)f'(t)dt \\
&= U(x)f(x) - U(y)f(y) - \int_y^x U(t)f'(t)dt.
\end{aligned}$$

The last result follows from the fact that if $f(t)$ is continually differentiable on $[1, x]$, then

$$\begin{aligned}
\sum_{n\leq x} u(n)f(n) &= u(1)f(1) + \sum_{1<n\leq x} u(n)f(n) \\
&= u(1)f(1) + U(x)f(x) - U(1)f(1) - \int_1^x U(t)f'(t)dt \\
&= U(x)f(x) - \int_1^x U(t)f'(t)dt.
\end{aligned}$$

□

Bibliography

[Ank57] NC Ankeny. Sums of three squares. *Proceedings of the American Mathematical Society*, 8(2):316–319, 1957.

[Bor56] K. G. Borozdkin. On a problem of Vinogradov's constant, trudy mat. *Soc, SSSR*, 1(3), 1956.

[CW89] Jing Run Chen and Tian Ze Wang. On the Goldbach problem. *Acta Math. Sinica*, 32(5):702–718, 1989.

[FW13] John B. Friedlander and Trevor D. Wooley. On Waring's problem: two squares and three biquadrates. *Mathematika*, 60(1):153–165, Jun 2013.

[Hel] Harald Helfgott. The ternary Goldbach problem. https://webusers.imj-prg.fr/~harald.helfgott/anglais/book.html/.

[Hel13] Harald A Helfgott. The ternary Goldbach conjecture is true. *arXiv preprint arXiv:1312.7748*, 2013.

[Hil09] David Hilbert. Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahln ter Potenzen (Waringsches problem). *Mathematische Annalen*, 67(3):281–300, 1909.

[HL+23] Godfrey H Hardy, John E Littlewood, et al. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. *Acta Mathematica*, 44:1–70, 1923.

[KT04] A. V. Kumchev and D. I. Tolev. An invitation to additive prime number theory, 2004.

[LW02] Ming-Chit Liu and Tian-Ze Wang. On the Vinogradov bound in the three primes Goldbach conjecture. *AcAri*, 105(2):133–175, 2002.

[MMTB06] Steven J Miller, Steven J Miller, and Ramin Takloo-Bighash. *An invitation to modern number theory*. Princeton University Press, 2006.

[Nat13] Melvyn B. Nathanson. *Additive Number Theory The Classical Bases*, volume 164. Springer Science & Business Media, 2013.

[Sik16] Samir Siksek. Every integer greater than 454 is the sum of at most seven positive cubes. *Algebra & Number Theory*, 10(10):2093–2119, Dec 2016.

[Vau97] Robert Charles Vaughan. *The Hardy-Littlewood method*, volume 125. Cambridge University Press, 1997.

[Vin37] Ivan Matveevich Vinogradov. Representation of an odd number as the sum of three primes. In *Dokl. Akad. Nauk SSSR*, volume 15, pages 129–132, 1937.

[VW02] R.C. Vaughan and T. D. Wooley. Waring's problem: a survey. *Surveys in Number Theory*, pages 285–324, 2002.

[War91] Edward Waring. *Meditationes Algebraicae: An English Translation of the Work of Edward Waring; Ed. and Transl. from the Latin by Dennis Weeks*. American Mathematical Society, 1991.