

UNIVERSITY OF TARTU
FACULTY OF SCIENCE AND TECHNOLOGY
INSTITUTE OF MATHEMATICS AND STATISTICS

Martti Karl Elvisto
**On Waring's problem and the
Hardy-Littlewood Circle method**

Mathematics
Bachelor's Thesis (9 ECTS)

Supervisors: PhD Loïs Jérôme Faisant
Prof. Valdis Laan

TARTU 2026

ON WARING'S PROBLEM AND THE HARDY-LITTLEWOOD CIRCLE METHOD

Bachelor thesis

Martti Karl Elvisto

Abstract

In this thesis, Waring's problem is expressed via generating functions and a certain integral. A partial proof via the Hardy-Littlewood circle method is then given.

CERCS research specialisation: P120 Number theory, field theory, algebraic geometry, algebra, group theory.

Key Words: Waring's problem, analytic number theory, complex analysis

WARINGI PROBLEEMIST JA HARDY-LITTLEWOODI RINGI MEETODIST

Bakalaureusetöö

Martti Karl Elvisto

Lühikokkuvõte

Käesolevas bakalaureusetöös on Waringi probleem väljendatud genereerivate funktsioonide ja integraali läbi. Seejärel on rakendatud Hardy-Littlewoodi ringi meetodit, et Waringi probleem positiivse vastusega lahendada.

CERCS teaduseriala: P120 Arvuteooria, korpuseteooria, algebraline geomeetria, algebra, rühmateooria.

Märksõnad: Waringi hüpotees, analüütiline arvuteooria, kompleksanalüüs

Contents

Introduction	3
1 Theoretical Background	4
2 The circle method	7
2.1 Waring's problem	7
2.2 Hardy-Littlewood circle method	7
2.3 Decomposition of $[0, 1]$	10
2.4 Minor arcs	11
2.5 Major arcs	13
2.6 Completion of the proof	21
Conclusions	22
References	23

Introduction

This thesis presents parts from the proof of Waring's theorem, showcasing the Hardy-Littlewood circle method and other techniques used in analytic number theory. The statement of Waring's theorem is: for all positive integers k there exists a positive integer s such that any positive integer N can be expressed as the sum of at most s positive k -th powers. The Hardy-Littlewood circle method has its genesis in [1], when Godfrey Harold Hardy and Srinivasa Ramanujan used it in 1918 to find an asymptotic formula for the number of integer partitions $p(n)$. Since then it has found many other uses in additive number theory, and we will present one such case.

The work consists of two chapters.

In the first chapter we present some theorems and notation used in the main part of the thesis. The most important of those, which we will use without proof, are Weyl's inequality and Hua's lemma.

In the second chapter we describe the circle method, and then apply it to provide a partial proof of Waring's theorem. We then give a brief overview of the rest of the proof.

The thesis is mainly based on [2].

1 Theoretical Background

We will make use of a function $e : \mathbb{R} \rightarrow \mathbb{C}$ defined as $e(x) = e^{2\pi ix}$.

Whenever we write $(a, b) = d$ for integers a, b, d we mean that the positive greatest common divisor of a and b is d .

For a complex number $z = a + bi$ written in algebraic form, we define the absolute value of z as $|z| = \sqrt{a^2 + b^2}$.

Whenever we have functions f, g , with $f : \mathbb{R} \rightarrow \mathbb{C}$, $g : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ we will write

$$f(x) = O(g(x)) \text{ or } f = O(g) \text{ or } f(x) \ll g(x) \text{ or } f \ll g$$

to mean that there exist real constants $c, X > 0$ such that for all $x > X$, $|f(x)| \leq cg(x)$.

In this thesis, we will make use of two theorems from analytic number theory without proof. The theorems now follow.

Theorem 1 (Weyl's inequality). *[2, Theorem 4.3] Let $f(x) = \alpha x^k + \dots$ be a polynomial with real coefficients. Let $S(f) = \sum_{n=1}^P e(f(n))$. Let $\varepsilon > 0$ be a real number, and a, q be integers such that $\frac{a}{q}$ is an approximation to α satisfying*

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

Then we have

$$S(f) \ll P^{1+\varepsilon} \left(P^{-1} + q^{-1} + P^{-k} q \right)^{1/2^{k-1}}$$

for any real number $\varepsilon > 0$. Here the constant c depends on k and ε , but importantly not on α or on P . Usually we will write K instead of 2^{k-1} .

At first glance we might ask, how is this useful at all? The sum $S(f)$ has P terms, each with an absolute value of 1, so clearly we always at least have $|S(f)| \leq P$, but in Theorem 1 the exponent of P is $1 + \varepsilon$. A simple way to see that this actually

does provide an improvement in at least some cases, is to consider $q = P^{k/2}$. With the value of P varying, always having this exact equality is impossible, but there is nothing stopping us from changing the value of q based on P in general, and we will end up doing this later when using the inequality. That being said, provided that $k \geq 2$ we would then have

$$\begin{aligned}
& P^{1+\varepsilon} \left(P^{-1} + P^{-1} + q^{-1} + P^{-k}q \right)^{1/K} \\
&= P^{1+\varepsilon} \left(P^{-1} + 2P^{-k/2} \right)^{1/K} \\
&\leq P^{1+\varepsilon} \left(3P^{-1} \right)^{1/K} \\
&= 3^{1/K} P^{1-1/K+\varepsilon} \\
&\ll P^{1-1/K+\varepsilon}.
\end{aligned}$$

In the last line, we can make the exponent less than 1 by choosing an ε which is smaller than $\frac{1}{K}$. This is then an improvement over the triangle inequality.

Theorem 2 (Hua's lemma). *[2, Theorem 4.6] Let $k \geq 2$ be an integer and α be any real number. Then let*

$$T(\alpha) = \sum_{n=1}^P e(\alpha n^k).$$

Then

$$\int_0^1 |T(\alpha)|^{2^k} d\alpha \ll P^{2^k-k+\varepsilon}.$$

We will later need the following equality, usually called an orthogonality relation, which holds for any integers m and n :

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

Proof. We will assume knowledge of integrating the exponential function with complex arguments over a range of real numbers, and of Euler's identity. If $m = n$, we

then have

$$\begin{aligned} \int_0^1 e(m\alpha)e(-n\alpha) d\alpha &= \int_0^1 e^{2\pi im\alpha} e^{2\pi i(-n)\alpha} d\alpha = \int_0^1 e^{2\pi i(m-n)\alpha} d\alpha \\ &= \int_0^1 e^0 d\alpha = \int_0^1 1 d\alpha = 1. \end{aligned}$$

If $m \neq n$, we have

$$\begin{aligned} \int_0^1 e(m\alpha)e(-n\alpha) d\alpha &= \int_0^1 e^{2\pi im\alpha} e^{2\pi i(-n)\alpha} d\alpha = \int_0^1 e^{2\pi i(m-n)\alpha} d\alpha \\ &= \left(\frac{e^{2\pi i(m-n)\alpha}}{2\pi i(m-n)} \right) \Big|_{\alpha=0}^{\alpha=1} = \left(\frac{e^{2\pi i(m-n)}}{2\pi i(m-n)} \right) - \left(\frac{e^0}{2\pi i(m-n)} \right) \\ &= \frac{1}{2\pi i(m-n)} - \frac{1}{2\pi i(m-n)} = 0. \end{aligned}$$

□

We will also need the following theorem

Theorem 3 (Dirichlet's approximation theorem). *[2, Theorem 4.1] Let α and Q be real numbers, $Q \geq 1$. Then there exist integers a, q such that $1 \leq q \leq Q$ and $(a, q) = 1$ for which we have*

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

2 The circle method

Unless stated otherwise, everything in this chapter is based on [2].

2.1 Waring's problem

In 1770, Edward Waring in his book *Meditationes Algebrae*, states ([3, pp. 204–205]):

Omnis integer numerus est quadratus, vel e duobus, tribus vel quatuor quadratis compositus.

Has proprietates invenit, sed non demonstravit Fermat.

Omnis integer numerus vel est cubus, vel e duobus, tribus, 4, 5, 6, 7, 8, vel novem cubis compositus, est etiam quadrato-quadratus, vel e duobus, tribus, &c. usque ad novemdecim compositus & sic deinceps.

What this means in modern language, is:

Theorem 4 (Waring's theorem). *For every positive integer k , there exists some bound s , such that every positive integer N can be represented as a sum of at most s positive k -th powers.*

The quote from Waring's book also contains the statement, that for $k = 2, 3, 4$, these bounds are 4, 9 and 19 respectively. It is exceedingly likely, that Waring did not have a proof of his statement.

For $k = 2$, this result is also known as Lagrange's 4 square theorem.

2.2 Hardy-Littlewood circle method

Whenever we talk of powers of numbers, we actually mean positive powers.

Now, to actually get started with applying the circle method to Waring's problem, we have to rephrase the problem in terms of generating functions. We will denote, for given positive integers N, k and s the number of solutions in positive integers to the equation

$$N = x_1^k + x_2^k + \cdots + x_s^k$$

as $r_{k,s}(N)$. We count solutions with the values of a_n reordered separately. As an example, the value of $r_{2,2}(5)$ would be the amount of solutions in positive integers x, y to the equation $5 = x^2 + y^2$. Considering any value of x uniquely determines y , $3^2 > 5$ and there exists a valid y for both $x = 1$ and $x = 2$, we have $r_{2,2}(5) = 2$.

The generating function for any subset of the integers A , is $f(x) = \sum_{a \in A} x^a$, where we regard $f(x)$ as a formal power series. We see, that

$$f(x)^s = \sum_{N=0}^{\infty} r_{A,s}(N) x^N,$$

where $r_{A,s}(N)$ is defined as the number of ways to express N as the sum of s elements of A . However, if we just want to determine a single value $r_{k,s}(N)$ by multiplying together power series, we don't actually need all the elements from the set of all positive k -th powers. Clearly the terms with exponent bigger than N will never contribute anything to the value of $r_{k,s}(N)$, and we can just ignore them.

So, if we write

$$f_N(x) = \sum_{\substack{a \in A \\ a \leq N}} x^a,$$

where we now use A to denote the set of positive k -th powers, we can say that for $0 \leq m \leq N$, $r_{A,s}(m) = c_m$ in

$$f_N(x)^s = \sum_{m=0}^{sN} c_m x^m.$$

Now, the generating function we will actually use moving forward, is

$$F(\alpha) = f_N(e(\alpha)) = \sum_{\substack{a \in A \\ a \leq N}} e^{2\pi i a \alpha} = \sum_{\substack{a \in A \\ a \leq N}} e(a\alpha).$$

Using this function, we again see, that

$$F(\alpha)^s = \sum_{m=0}^{sN} c_m e(m\alpha).$$

Using the relation (1) together with the generating function we just formed, we can recover the value of $r_{k,s}(N)$ using the simple looking integral

$$r_{k,s}(N) = \int_0^1 F(\alpha)^s e(-N\alpha) d\alpha. \quad (2)$$

Now we will proceed to the main result of our thesis, proving Waring's problem.

Note that, Waring's problem is equivalent to the statement, that for every k there exists an s such that for all N bigger than some n , $r_{k,s}(N) \geq 1$. This is because for any integer $k \geq 2$, 1^k is a k -th power, and any integer smaller than n , could just be written as a sum of 1^k taken $n - 1$ times. We will prove this statement, by showing that the following asymptotic equality holds:

Theorem 5 ([2, Theorem 5.7]). *There exists a real number $\delta > 0$ dependent on $k \geq 2$ and $s \geq 2^k + 1$ such that in the process of N going to infinity,*

$$r_{k,s}(N) = \mathfrak{S}(N) \frac{\Gamma(1 + \frac{1}{k})^s}{\Gamma(\frac{s}{k})} N^{\frac{s}{k}-1} + O(N^{\frac{s}{k}-1-\delta}).$$

Here

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^q \left(\frac{S(q,a)}{q} \right)^s e\left(-N \frac{a}{q}\right)$$

and

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt$$

is the gamma function.

In all that follows, k and s are assumed to satisfy $k \geq 2$, $s \geq 2^k + 1$.

2.3 Decomposition of $[0, 1]$

In general it is not possible to evaluate the integral in (2) exactly. Instead we want to approximate it. To do that we will split the interval $[0, 1]$ into 2 parts, called the major and minor arcs, and approximate it separately over both parts. In all that follows, N , k and s will be used in the context of $r_{k,s}(N)$. We will prove Waring's theorem for $s \geq 2^k + 1$.

Let $N \geq 2^k$, and denote $P = \lfloor N^{1/k} \rfloor$. We can arbitrarily choose $0 < \nu < \frac{1}{5}$, and then for all $q, a \in \mathbb{Z}$ satisfying

$$1 \leq q \leq P^\nu, \quad 0 \leq a \leq q, \quad (a, q) = 1,$$

let

$$\mathfrak{M}(q, a) = \left[\frac{a}{q} - P^{\nu-k}, \frac{a}{q} + P^{\nu-k} \right] \cap [0, 1].$$

The set $\mathfrak{M}(q, a)$ for any a, q satisfying the conditions we just described, is called a major arc. The union of all possible major arcs, that is

$$\mathfrak{M} = \bigcup_{1 \leq q \leq P^\nu} \bigcup_{\substack{a=0 \\ (a,q)=1}}^q \mathfrak{M}(q, a)$$

is called the set of major arcs.

As we can see, the set of major arcs consists of the parts of the closed interval $[0, 1]$ that are in a sense close to rational numbers with large denominators.

The minor arcs are just the complement of $\mathfrak{M}$

$$\mathfrak{m} = [0, 1] \setminus \mathfrak{M},$$

with each contiguous interval the totality of which makes up $\mathfrak{m}$ being called a minor arc.

2.4 Minor arcs

We will now estimate the integral 2 over the minor arcs, with the following result:

Theorem 6 ([2, Theorem 5.2]). *There exists a real number $\delta_1 > 0$ such that*

$$\int_{\mathfrak{m}} F(\alpha)^s e(-N\alpha) d\alpha = O(P^{s-k-\delta_1}),$$

and the constant in the Landau notation depends on both k and s .

This is a desirable result, because the exponent of P is low enough, that the entirety of the integral actually falls under the error term of 2. This means, that the entirety of the main term actually comes from evaluating the integral over the major arcs!

The idea of the proof is something like this: the simplest way to try bounding an integral, is to apply the triangle inequality. If we do that, we get an expression which we can almost apply Hua's lemma (Theorem 2) to. We can rewrite (remember that $s \geq 2^k + 1$):

$$|F(\alpha)|^s = |F(\alpha)|^{s-2^k} |F(\alpha)|^{2^k}.$$

This actually gets us a $-k$ in the exponent, so now we just need to find any improvement at all in $|F(\alpha)|^{s-2^k}$. We can do this with Weyl's inequality, and we have our result.

Proof. By Dirichlet's theorem (Theorem 3), for any real number α there exists an

approximation $\frac{a}{q}$ with a, q integers such that

$$1 \leq q \leq P^{k-\nu}, \quad (a, q) = 1,$$

and

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{qP^{k-\nu}} \leq \min \left(\frac{1}{P^{k-\nu}}, \frac{1}{q^2} \right). \quad (3)$$

The right inequality holds, because $\frac{1}{qP^{k-\nu}}$ is smaller than both $\frac{1}{P^{k-\nu}}$ and $\frac{1}{q^2}$. If $\alpha \in \mathfrak{m}$, we must have $P^\nu < q$, as otherwise α would be in $\mathfrak{M}(q, a)$ and thus $\mathfrak{M}$ by definition. Thus for $\alpha \in \mathfrak{m}$, we have $P^\nu < q \leq P^{k-\nu}$. Remember that $0 < \nu < \frac{1}{5}$. Then from Weyl's inequality (Theorem 1) with $f(x) = \alpha x^k$ and $S(f) = F(\alpha)$ we get

$$\begin{aligned} F(\alpha) &\ll P^{1+\varepsilon} \left(P^{-1} + q^{-1} + P^{-k}q \right)^{1/K} \\ &\leq P^{1+\varepsilon} \left(P^{-1} + P^{-\nu} + P^{-k}P^{k-\nu} \right)^{1/K} \\ &\leq P^{1+\varepsilon} (3P^{-\nu})^{1/K} \\ &= 3^{1/K} P^{1-\nu/K+\varepsilon} \\ &\ll P^{1-\nu/K+\varepsilon}. \end{aligned}$$

We got the second line by substituting both q with the value that maximizes each respective term. If we choose epsilon small enough in the final expression, the exponent will be less than 1, which was exactly what we needed! Now we can show

the final result:

$$\begin{aligned}
& \left| \int_{\mathfrak{m}} F(\alpha)^s e(-N\alpha) d\alpha \right| \\
& \leq \int_{\mathfrak{m}} |F(\alpha)^s e(-N\alpha)| d\alpha \\
& = \int_{\mathfrak{m}} |F(\alpha)^s| d\alpha \\
& = \int_{\mathfrak{m}} |F(\alpha)|^{s-2^k} |F(\alpha)|^{2^k} d\alpha \\
& \leq \int_{\mathfrak{m}} \max_{\beta \in \mathfrak{m}} (|F(\beta)|^{s-2^k}) |F(\alpha)|^{2^k} d\alpha \\
& = \max_{\beta \in \mathfrak{m}} (|F(\beta)|^{s-2^k}) \int_{\mathfrak{m}} |F(\alpha)|^{2^k} d\alpha \\
& \leq \max_{\beta \in \mathfrak{m}} (|F(\beta)|^{s-2^k}) \int_0^1 |F(\alpha)|^{2^k} d\alpha \\
& \ll \left(P^{1-\nu/K+\varepsilon} \right)^{s-2^k} P^{2^k-k+\varepsilon'} \\
& = P^{s-(s-2^k)\nu/K+\varepsilon(s-2^k)-k+\varepsilon'} \\
& = P^{s-k-\delta}.
\end{aligned}$$

□

2.5 Major arcs

The aim of this subchapter is to show part of the proof of the following theorem:

Theorem 7 ([2, Theorem 5.3]).

$$\int_{\mathfrak{M}} F(\alpha)^s e(-N\alpha) d\alpha = \mathfrak{S}(N, P^\nu) J^*(N) + O(P^{s-k-\delta}),$$

where

$$\mathfrak{S}(N, P^\nu) = \sum_{q=1}^{\lfloor P^\nu \rfloor} \sum_{\substack{a=1 \\ (a,q)=1}}^q \left(\frac{S(q, a)}{q} \right)^s e \left(-N \frac{a}{q} \right)$$

and

$$J^*(N) = \int_{-P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e(-N\beta) d\beta.$$

Both $\mathfrak{S}(N, P^\nu)$ and $J^*(N)$ are functions which can be approximated well enough to show the truth of (5).

First, we want to approximate the value of $F(\alpha)$ in a single major arc $\mathfrak{M}(q, a)$. We will do this with the help of the following two functions:

$$v(\beta) = \sum_{m=1}^N k^{-1} m^{-1+1/k} e(\beta m)$$

and

$$S(q, a) = \sum_{r=1}^q e\left(\frac{a}{q} r^k\right).$$

By Weyl's inequality with $f(x) = \frac{a}{q} x^k$ we see, that

$$\begin{aligned} S(q, a) &\ll q^{1+\varepsilon} \left(q^{-1} + q^{-1} + q^{-k} q \right)^{1/K} \\ &\leq q^{1+\varepsilon} (3q^{-1})^{1/K} \\ &= 3^{-1/K} q^{1-1/K+\varepsilon} \\ &\ll q^{1-1/K+\varepsilon}. \end{aligned}$$

Thus also

$$\frac{S(q, a)}{q} \ll q^{-1/K+\varepsilon}. \tag{4}$$

Note, that here the constant hidden by $\ll$ does not actually depend on k . Let us show why that is. For all $k > 1 - \log_2(\varepsilon)$, the exponent is greater than 1. Since $S(q, a)$ is a sum of q terms, each with absolute value 1, it is clearly always less than q itself. From this we get

$$\frac{S(q, a)}{q} \leq 1,$$

or in other words, for all $k > 1 - \log_2(\varepsilon)$, the constant hidden in (4) can be chosen

to be 1. This means, that among all the constants we get from each $k \leq 1 - \log_2(\varepsilon)$, we can choose a maximal one, and it will be valid for any k .

Let us now prove two lemmas that will be useful afterwards.

Lemma 1 has been slightly changed compared to the original in [2].

Lemma 1 ([2, Lemma 4.7]). *For any real number β with $|\beta| \leq \frac{1}{2}$, and any integer N , we have*

$$\sum_{n=1}^N e(\beta n) \ll \min(N, |\beta|^{-1}),$$

where in the case $\beta = 0$ we say that $|\beta|^{-1}$ is bigger than any real number.

Proof. To prove the lemma, we show separately that both $\sum_{n=1}^N e(\beta n) \ll N$ and $\sum_{n=1}^N e(\beta n) \ll |\beta|^{-1}$ hold.

Since $|e(\beta n)| = 1$, we have

$$\left| \sum_{n=1}^N e(\beta n) \right| \leq \sum_{n=1}^N 1 = N \ll N.$$

If $\beta = 0$, we consider $|\beta|^{-1}$ to be bigger than any real number, and thus bigger than the absolute value of any finite sum. If $\beta \neq 0$, we have a geometric progression, the

sum of which can be calculated easily:

$$\begin{aligned}
\left| \sum_{n=1}^N e(\beta n) \right| &= \left| \sum_{n=1}^N e(\beta)^n \right| \\
&= \left| e(\beta) \frac{e(\beta)^{N+1} - 1}{e(\beta) - 1} \right| \\
&\leq \frac{2}{|e(\beta) - 1|} \\
&= \frac{2}{\left| e\left(\frac{\beta}{2}\right) - e\left(\frac{\beta}{2}\right) \right|} \\
&= \frac{2}{|2i \sin(\pi\beta)|} \\
&= \frac{1}{\sin(\pi|\beta|)} \\
&\leq \frac{1}{2|\beta|}.
\end{aligned}$$

The last inequality is equivalent to $2|\beta| \leq \sin(\pi|\beta|)$, let us show why that holds. The function $\sin(\pi x)$ is concave on the range $[0, \frac{1}{2}]$, and we also have $\sin(\pi \cdot 0) = 0$ and $\sin(\pi \cdot \frac{1}{2}) = 1$. Thus by the definition of concavity, $\sin(\pi x)$ lies above the line connecting $(0, 0)$ to $(\frac{1}{2}, 1)$ which is $y = 2x$. $\square$

Lemma 2 has been simplified compared to the original in [2].

Lemma 2 (Partial summation). [2, Lemma A.4] *Let $u : \mathbb{N} \rightarrow \mathbb{C}$ and $f : \mathbb{N} \rightarrow \mathbb{R}$ be any functions, and let $U(x) = \sum_{n=1}^{\lfloor x \rfloor} u(n)$, that is $U : \mathbb{R}_{\geq 0} \rightarrow \mathbb{C}$. We consider $U(x)$ to be zero for $x \in [0, 1)$. Let a, b be integers satisfying $0 \leq a < b$. Then*

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

If f is instead a function from $\mathbb{R}_{\geq 0}$ to $\mathbb{R}$ with a continuous derivative in $[a, b]$, we also have

$$\sum_{n=a+1}^b u(n)f(n) = U(b)f(b) - U(a)f(a) - \int_a^b U(t)f'(t) dt.$$

Notice, that both equations have a similarity to the formula for integration by parts.

Proof. We have

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

This is the first part done. For the second part, first recall the fundamental theorem of algebra, from which we get

$$f(n+1) - f(n) = \int_n^{n+1} f'(x) \, dx,$$

as long as $[n, n+1] \subseteq [a, b]$. This requirement also holds for the next result. If n is additionally an integer, $U(x) = U(n)$ for $x \in [n, n+1]$. This means that

$$U(n)(f(n+1) - f(n)) = \int_n^{n+1} U(x)f'(x) \, dx.$$

Using the first part and the demonstrated equalities, we can show the truth of the

second part:

$$\begin{aligned}
\sum_{n=a+1}^b u(n)f(n) &= U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)) \\
&= U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} \int_n^{n+1} U(x)f'(x) dx \\
&= U(b)f(b) - U(a)f(a+1) - \int_{a+1}^b U(x)f'(x) dx \\
&= U(b)f(b) - U(a)f(a) - U(a)(f(a+1) - f(a)) - \int_{a+1}^b U(x)f'(x) dx \\
&= U(b)f(b) - U(a)f(a) - \int_a^{a+1} U(x)f'(x) dx - \int_{a+1}^b U(x)f'(x) dx \\
&= U(b)f(b) - U(a)f(a) - \int_a^b U(x)f'(x) dx.
\end{aligned}$$

□

We can now proceed with

Lemma 3 ([2, Lemma 5.1]). *For a real number β satisfying $|\beta| \leq \frac{1}{2}$, we have*

$$v(\beta) \ll \min(P, |\beta|^{-1/k}).$$

Proof. We will once again show separately, that $v(\beta) \ll P$ and $v(\beta) \ll |\beta|^{-1/k}$ both hold.

Note, that the function $f(x) = k^{-1}x^{-1+1/k}$ is positive, continuous and decreasing for $x > 0$. We will also continue to use f to denote the function just described.

Thus we have

$$\begin{aligned}
|v(\beta)| &\leq \sum_{m=1}^N |k^{-1}m^{-1+1/k}e(\beta m)| \\
&= \sum_{m=1}^N k^{-1}m^{-1+1/k} \\
&\leq \int_1^N k^{-1}x^{-1+1/k} dx + f(1) \\
&< N^{1/k} \quad \text{(by evaluation of the integral)} \\
&\ll P.
\end{aligned} \tag{5}$$

For the second part, if $|\beta| \leq \frac{1}{N}$, we can multiply both sides by $\frac{N}{|\beta|}$ and take both sides to the $\frac{1}{k}$ -th power. Then together with the definition of P we get $P \leq N^{1/k} \leq |\beta|^{-1/k}$. Since we already know $|v(\beta)| \ll P$, we now only have the case $\frac{1}{N} < |\beta| \leq \frac{1}{2}$ left.

Let $M = \lfloor |\beta|^{-1} \rfloor$. Then we have

$$M \leq \beta^{-1} \leq M + 1 \leq N,$$

where $M + 1 \leq N$ because from $\frac{1}{N} < |\beta|$ we get $|\beta|^{-1} < N$, N is an integer and $M + 1$ is the smallest integer greater than $|\beta|^{-1}$. We can thus split $v(\beta)$ into two sums:

$$v(\beta) = \sum_{m=1}^M k^{-1}m^{-1+1/k}e(\beta m) + \sum_{m=M+1}^N k^{-1}m^{-1+1/k}e(\beta m).$$

Let $U(x) = \sum_{m=1}^{\lfloor x \rfloor} e(\beta m)$ for all real numbers $x \geq 1$. Then for the second sum we

have:

$$\begin{aligned}
& \sum_{m=M+1}^N k^{-1} m^{-1+1/k} e(\beta m) \\
&= \sum_{m=M+1}^N f(m) e(\beta m) \\
&= f(N)U(N) - f(M)U(M) - \int_M^N U(x) f'(x) dx \quad (\text{by lemma 2}) \\
&\leq |f(N)||U(N)| + |f(M)||U(M)| + \int_M^N |U(x)||f'(x)| dx \\
&\quad (\text{by the triangle inequality and properties of } |\cdot|) \\
&\ll |f(N)||\beta|^{-1} + |f(M)||\beta|^{-1} + \int_M^N |\beta|^{-1} |f'(x)| dx \quad (\text{by lemma 1}) \\
&= |\beta|^{-1} \left(f(N) + f(M) - \int_M^N f'(x) dx \right) \\
&\quad (f(x) \text{ and } -f'(x) \text{ are positive for all positive } x) \\
&= |\beta|^{-1} (f(N) + f(M) - f(N) + f(M)) \\
&= 2|\beta|^{-1} f(M) = 2|\beta|^{-1} k^{-1} M^{-1+1/k} \ll M^{-1+1/k} |\beta|^{-1} \\
&\leq (|\beta|^{-1})^{-1+1/k} |\beta|^{-1} = |\beta|^{-1/k}.
\end{aligned}$$

So that we don't lose sight of what's important, we just showed that

$$\sum_{m=M+1}^N k^{-1} m^{-1+1/k} e(\beta m) \ll |\beta|^{-1+1/k}.$$

About the first sum:

$$\left| \sum_{m=1}^M k^{-1} m^{-1+1/k} e(\beta m) \right| \leq M^{1/k} \leq (|\beta|^{-1})^{1/k} = |\beta|^{-1/k} \ll |\beta|^{-1/k},$$

where the first inequality is due to (5).

Putting the two sums together:

$$v(\beta) = \sum_{m=1}^M k^{-1} m^{-1+1/k} e(\beta m) + \sum_{m=M+1}^N k^{-1} m^{-1+1/k} e(\beta m) \ll |\beta|^{-1/k},$$

which is the second half of lemma 3 done. $\square$

The result we just proved, is then used to prove the following lemma:

Lemma 4 ([2, Lemma 5.2]). *Let a, q be integers such that $1 \leq q \leq P^\nu$, $0 \leq a \leq q$ and $(a, q) = 1$. Then, if $\alpha \in \mathfrak{M}(q, a)$, we have*

$$F(\alpha) = \frac{S(q, a)}{q} v \left(\alpha - \frac{a}{q} \right) + O(P^{2\nu}),$$

which can in turn be used to prove Theorem 7

2.6 Completion of the proof

As is shown in [2], $J^*(N)$ is asymptotically equal to $\frac{\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k})}$ and $\mathfrak{S}(N, P^\nu)$ is asymptotically equal to $\mathfrak{S}(N)$, which is positive and bounded above and below by positive constants. All of these statements together form the proof of 5.

Conclusions

In this thesis, we demonstrated the Hardy-Littlewood circle method and showed roughly how it can be used to prove Waring's theorem.

In the first chapter, we presented theorems that we later needed for the proof of Waring's theorem in the main part of the work.

In the second chapter, we described how generating functions are used to form an expression to which we can apply the circle method. We then partially proved Waring's theorem using the circle method.

References

- [1] G. H. Hardy and S. Ramanujan. “Asymptotic Formulae in Combinatory Analysis”. In: *Proceedings of the London Mathematical Society* s2-17.1 (1918), pp. 75–115. DOI: [10.1112/plms/s2-17.1.75](https://doi.org/10.1112/plms/s2-17.1.75).
- [2] Melvyn B. Nathanson. *Additive Number Theory: The Classical Bases*. Springer-Verlag New York, Inc, 1996. DOI: [10.1007/978-1-4757-3845-2](https://doi.org/10.1007/978-1-4757-3845-2).
- [3] Edward Waring. *Meditationes Algebraicae*. Cambridge University Press, 1770.

Non-exclusive licence to reproduce thesis and make thesis public

I, Martti Karl Elvisto,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright, On Waring's problem and the Hardy-Littlewood Circle method, supervised by Loïs Jérôme Faisant and Valdis Laan.
2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.
3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.
4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Martti Karl Elvisto

18/08/2026