A Tale of Two Arcs: The Circle Method and Waring's Problem

Author: Jing Guo
Faculty of Mathematics, University of Regensburg

Advisor: Prof. Dr. Guido Kings
Faculty of Mathematics, University of Regensburg

Abstract

In this thesis, we explore the application of the circle method to Waring's problem, which asks how many k-th powers are required to represent all sufficiently large natural numbers. We begin by outlining the historical context of Waring's conjecture, highlighting the foundational results of Lagrange, Hilbert, Hardy, Littlewood, and Vinogradov. We then present key technical tools central to the circle method, namely Weyl's inequality and Hua's inequality, which provide powerful estimates for exponential sums of the form

$$T(\alpha) \coloneqq \sum_{1 \leq x \leq P} e(\alpha x^k).$$

Using these bounds, we develop the major- and minor-arc decomposition of the unit interval in the integral representation of the number of solutions to

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

We show that the main contribution to this integral comes from a small set of "major arcs", yielding an asymptotic formula for the number of representations when $s \geq 2^k + 1$. Central to this formula is the singular series $\mathfrak{S}(N)$, whose non-vanishing under the same condition ensures that sufficiently large integers can indeed be expressed as sums of s k-th powers.

Finally, we discuss refinements concerning absolute convergence of the singular series. Through this thesis, we highlight how the classical circle method continues to be a cornerstone in analytic number theory, underpinning deep results and ongoing developments in the field.

Zusammenfassung

In dieser Arbeit untersuchen wir die Anwendung der Kreismethode auf das Waringsche Problem, welches fragt, wie viele k-te Potenzen erforderlich sind, um alle hinreichend großen natürlichen Zahlen darzustellen. Wir beginnen mit einer Darstellung des historischen Kontexts der Waringschen Vermutung und heben die grundlegenden Ergebnisse von Lagrange, Hilbert, Hardy, Littlewood und Vinogradov hervor. Anschließend präsentieren wir zentrale technische Werkzeuge der Kreismethode, nämlich die Weylsche Ungleichung und die Huasche Ungleichung, welche mächtige Abschätzungen für Exponentialsummen der Form

$$T(\alpha) \coloneqq \sum_{1 \leq x \leq P} e(\alpha x^k)$$

liefern. Mit Hilfe dieser Schranken entwickeln wir die Zerlegung des Einheitsintervalls in Haupt- und Nebenbögen in der Integraldarstellung der Anzahl der Lösungen von

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

Wir zeigen, dass der Hauptbeitrag zu diesem Integral von einer kleinen Menge von „Hauptbögen“ herrührt, was eine asymptotische Formel für die Anzahl der Darstellungen ergibt, wenn $s \geq 2^k + 1$. Zentral für diese Formel ist die singuläre Reihe $\mathfrak{S}(N)$, deren Nichtverschwinden unter derselben Bedingung sicherstellt, dass hinreichend große natürliche Zahlen tatsächlich als Summen von s k-ten Potenzen ausgedrückt werden können.

Schließlich diskutieren wir Verfeinerungen bezüglich der absoluten Konvergenz der singulären Reihe. Durch diese Arbeit zeigen wir auf, wie die klassische Kreismethode weiterhin ein Grundpfeiler der analytischen Zahlentheorie ist und tiefgreifende Ergebnisse sowie laufende Entwicklungen in diesem Gebiet untermauert.

Acknowledgements

First, I would like to thank my supervisor Prof. Dr. Guido Kings for granting me the opportunity to investigate the circle method and Waring's problem – topics seldom explored within the Faculty of Mathematics at the University of Regensburg. Second, I would like to thank Lukas Prader for our (bi-)weekly discussions that greatly helped me to understand the circle method, as well as his help and comments on improving my seminar-giving skills. I also thank Prof. Antal Balog for introducing me to the beautiful world of analytic and additive number theory.

I am indebted to Prof. Tim Browning, Prof. Gergely Harcos, and Prof. Ritabrata Munshi for their insightful suggestions and comments on the circle method and analytic number theory.

During the past three years in Regensburg, I have been fortunate to make good friends among my fellow students. As is customary in mathematics, in alphabetical order, I would like to thank Kaicheng Dong, Hua Jing, Qike Li, Wenbo Liao, Zhicheng Lyu, Rui Ni, Yiming Wang, and Jixin Yan for mathematical and career discussions. Furthermore, my gratitude goes to Bowen Ding, Zhenghang Du, Chenying Lin, Weichen Xue, Jun Xu, Ruoyu Xu, and Jiangyue Yao; thank you not only for many happy board-game afternoons and evenings, but also for the valuable mathematical and professional discussions and insights many of you have shared – especially Zhenghang Du, Chenying Lin, and Jiangyue Yao. I thank Chenxin Zhong for discussions about cryptography and large language models over multiple dinners. A special note of gratitude goes to Shiyu James Yan, for the countless meals we cooked and shared, the wide-ranging conversations, and his constant help and encouragement.

My deepest appreciation belongs to my fiancée, Xiaoyu Qin. She has supported my academic endeavour now for nearly half a decade, continuously supporting me through slow progress and encouraging and being the light of my life through the ups-and-downs in my graduate school life. I am thankful for her everyday, and I am as excited as I have been about our future together.

Finally, I thank my parents for their unconditional love and support in all my pursuits.

Contents

1 Introduction **3**

1.1 Objectives and Scope of This Thesis 4

2 Weyl and Hua inequalities **6**

3 The asymptotic formula **14**

4 The singular series **22**

5 The singular series continued **31**

6 Conclusion **36**

6.1 Broader Implications 37

6.2 Future Directions 37

Chapter 1

Introduction

Waring's problem is a classic question in analytic and additive number theory that dates back to 1770, when Edward Waring in his "*Meditationes algebraicae*" made the following conjecture:

Conjecture 1.1 (Waring, 1770)**.** All natural numbers are the sum of at most 4 squares, 9 cubes, or 19 fourth powers.

This conjecture generalized the earlier result of Lagrange's four-square theorem proved in the same year, stating that *every integer is a sum of four squares.* Waring's conjecture remained unproven until Hilbert [Hil09] provided an affirmative answer in 1909. Hilbert's theorem established that for each k, there exists some finite number s such that every integer is the sum of at most s k-th powers. Though one should note that some credits should go to Hurwitz, who showed that if Waring's conjecture is true for any exponent k, then it is true for $2k$. However, Hilbert's proof was existential and did not give explicit values or effective bounds. This set the stage for further breakthroughs to quantify Waring's problem, which came with the development of the circle method in the early 20th century.

The *circle method*, pioneered by Ramanujan, Hardy, and Littlewood [HR18; HL20], introduced powerful analytic techniques to tackle additive problems like Waring's conjecture. In a series of papers in the 1920s (the *Partitio Numerorum* series), Hardy and Littlewood developed an *asymptotic formula* for the function $R(N)$, the number of representations of a sufficiently large integer N as a sum of s k-th powers. They demonstrated that if the number of summands s is large enough (in fact, $s \geq s_0(k)$ for some threshold $s_0(k)$), then one can derive an asymptotic expression for the representation function $R(N)$ of Waring's problem. A central feature of their formula was the *singular series* $\mathfrak{S}(N)$, an infinite product capturing local arithmetic densities. They proved that for sufficiently many variables s, the singular series converges to a positive constant, thereby guaranteeing that the asymptotic formula does not degenerate and that all sufficiently large N are representable in the desired form. Hardy and Littlewood also defined the function $G(k)$ to be the smallest number of k-th powers required to represent all sufficiently large integers. They established explicit but rather large bounds on $G(k)$; for instance, they showed $G(k) \leq (k-2)2^{k-1} + 5$, which was later improved upon by other mathematicians.

Building on Hardy and Littlewood's foundation, subsequent mathematicians refined the circle method and dramatically improved the bounds in Waring's problem. An important simplification was made by Vinogradov, who in the 1930s reformulated the method using finite exponential sums instead of integral contour integrals, streamlining the analysis. Notably, Vinogradov showed that one can reduce the number of k-th power terms substantially; for large k, he proved results like $G(k) \leq k(3\log k + 11)$ [Vin47], a striking improvement over the original bound of Hardy–Littlewood. Around the same time, Hua Luogeng (also known as Hua Loo-Keng) introduced what is now known as *Hua's inequality* [HUA38] in 1938 to strengthen the control over exponential sums on the minor arcs. Using these new analytic tools, Hua was able to show that an asymptotic formula holds provided $s \geq 2^k + 1$ [HUA38].

More recently, work by Vaughan, Wooley, and others has further refined the circle method, leading to increasingly tight bounds for $G(k)$. Wooley's development of *efficient congruencing* in the 1990s and 2000s brought the general bound for large k down to essentially $G(k) \ll k(\log k + \log\log k)$. Additionally, Bourgain–Demeter–Guth's *decoupling method* [BDG16] has introduced new perspectives on bounding exponential sums, contributing to further improvements in the application of the circle method to additive number theory.

1.1 Objectives and Scope of This Thesis

In this thesis, we apply the circle method to Waring's problem, with the twin goals of *exposition* and *refinement*, following Davenport's classical treatment [Dav05]. On one hand, we present a self-contained development of the classical circle method approach to Waring's problem, retracing how an asymptotic formula for the representation function $R_s^{(k)}(N)$ can be obtained when s is sufficiently large. This includes a careful treatment of the *major arc* contribution (which produces the main term of the formula) and the *minor arc* estimates (which bound the error term). In doing so, we introduce and prove two fundamental inequalities: *Weyl's inequality* and *Hua's inequality*, which provide upper bounds for exponential sums of the form

$\sum_{1\leq x\leq P} e(\alpha x^k)$, where $e(x) = \exp(2\pi i x)$, and are crucial for controlling the minor arc integrals. Using these inequalities, we derive the classical *asymptotic formula* for the number of representations of a large integer N as a sum of s k-th powers, under the condition that $s \geq 2^k + 1$.

We also examine some refinements of the method, particularly concerning the *singular series* $\mathfrak{S}(N)$. We investigate the convergence and positivity of $\mathfrak{S}(N)$ in detail, since the singular series being non-zero is essential to deduce that every sufficiently large N has at least one such representation.

The questions we address in this thesis can be summarized as follows:

1. *How does the circle method yield an asymptotic formula for Waring's problem?* We analyse the contributions of the major and minor arcs and derive an explicit asymptotic formula for $R(N)$.

2. *What conditions on s ensure that the asymptotic formula holds and that sufficiently large integers are representable?* We seek to determine the minimal s required for success and confirm that $s = 2^k + 1$ suffices.

3. *Why is the singular series $\mathfrak{S}(N)$ central to the formula, and how can we rigorously justify its properties?* We examine its role as a product of local densities and prove that it remains bounded away from zero.

By answering these questions, the thesis provides a comprehensive understanding of how the circle method works in the context of Waring's problem. Moreover, this research highlights the enduring relevance of the circle method as a foundational tool in analytic number theory, demonstrating how deep analytic techniques yield concrete number-theoretic results.

Chapter 2

Weyl and Hua inequalities

Before introducing Weyl's and Hua's inequalities, two of the most important tools in the study of Waring's problem, as well as in the estimates of the exponential sums, we would like to motivate why do we need these two inequalities:

In the context of Waring's problem, we are interested in the following representation function:

$$R(N) \coloneqq \#\{(x_1, \dots, x_s) \in \mathbb{N}^s : 1 \leq x_i \leq P, x_1^s + \cdots + x_s^k = N\}.$$

The igniting spark in the circle method is the following *character orthogonality*:

$$\int_0^1 e(n\alpha)\,\mathrm{d}\alpha = \begin{cases} 1 & \text{if } n = 0, \\ 0 & \text{if } n \in \mathbb{Z} \setminus \{0\}. \end{cases} \tag{2.1}$$

This allows to write

$$R(N) = \int_0^1 T(\alpha)^s e(-N\alpha)\,\mathrm{d}\alpha, \tag{2.2}$$

where

$$e(x) = \exp(2\pi i x), \quad T(\alpha) = \sum_{1 \leq x \leq P} e(\alpha x^k), \quad \text{and} \quad P = \left\lceil N^{1/k} \right\rceil.$$

As mentioned in the Introduction, the circle method splits the unit circle into major arcs and minor arcs. In general, it is usually easier to work with the major arcs, and the difficulty really lies in controlling the minor arcs. Therefore, we will need these two inequalities to show that $T(\alpha)$ is so small that its contribution cannot upset the main term coming from the major arcs.

We will prove (2.2) as follows:

Proposition 2.1. *The representation function*

$$R(N) \coloneqq \#\{(x_1, \dots, x_s) \in \mathbb{N}^s : 1 \le x_i \le P, x_1^s + \cdots + x_s^k = N\}$$

admits the Fourier-additive integral formula

$$R(N) = \int_0^1 T(\alpha)^s e(-N\alpha)\,\mathrm{d}\alpha.$$

Proof. We first construct the following indicator identity: For each s-tuple $(x_1, \dots, x_s) \in \mathbb{N}^s$, put

$$1_{x_1^s+\cdots+x_s^k=N} \coloneqq \int_0^1 e\left(\alpha(x_1^k + \cdots + x_s^k - N)\right)\mathrm{d}\alpha,$$

by the character orthogonality (2.1) with $n = x_1^k + \cdots + x_s^k - N$.

We then notice

$$R(N) = \sum_{1\le x_1,\dots,x_s\le P} 1_{x_1^s+\cdots+x_s^k=N} = \int_0^1 \sum_{1\le x_1,\dots,x_s\le P} e\left(\alpha(x_1^k + \cdots + x_s^k - N)\right)\mathrm{d}\alpha.$$

Inside the integral, we notice that we can further factor the inner sum:

$$\sum_{1\le x_1,\dots,x_s\le P} e\left(\alpha(x_1^k + \cdots + x_s^k)\right) = \left(\sum_{1\le x\le P} e(\alpha x^k)\right)^s = T(\alpha)^s.$$

Collecting everything we obtain

$$R(N) = \int_0^1 T(\alpha)^s e(-N\alpha)\,\mathrm{d}\alpha,$$

which is the desired identity. □

Now we are ready to prove Weyl's inequality – it was first given by Weyl in 1916 and was given the following explicit form by Hardy and Littlewood in 1920.

Lemma 2.2 (Weyl's inequality)**.** *Let $k \ge 2$ and $f(x) = \alpha x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k$ be a degree k real polynomial with leading coefficient α. Assume that α has a rational approximation a/q, satisfying*

$$\gcd(a, q) = 1, \quad q > 0, \quad \left|\alpha - \frac{a}{q}\right| \le \frac{1}{q^2}.$$

Then, for all $\varepsilon > 0$,

$$\left|\sum_{x\le P} e(f(x))\right| \ll_{k,\varepsilon} P^{1+\varepsilon}(\frac{1}{P} + \frac{1}{q} + \frac{q}{P^k})^{1/2^{k-1}}.$$

Note that the trivial bound for the exponential sum is $O(P)$, and Weyl's inequality gives an improvement on this whenever $q \in [P^\delta, P^{k-\delta}]$, for some fixed $\delta > 0$. We cannot obtain any useful information if q is very small, since the sum is of order P, at least if $f(x) = \alpha x^k$.

Proof. Without loss of generality, we may assume that $q \le P^k$, since otherwise the right hand side of the claimed inequality would be larger than $O(P)$, implying that the inequality holds trivially in this case. The key idea of the proof is *squaring and differencing*, which relates the sum to one that involves an average of similar sums with polynomials of degree one less. In the following, we allow all implied constants to depend on the degree k of f.

Let P_1, P_2 be two integers, such that $0 \le P_2 - P_1 \le P$. We are interested in the exponential sum

$$T_k(f) \coloneqq \sum_{P_1 < x \le P_2} e(f(x)),$$

where k is the degree of f.

First, we go through the *squaring* process:

$$\begin{aligned}
|T_k(f)|^2 &= T_k(f) \cdot \overline{T_k(f)} \\
&= [e(f(P_1+1)) + \cdots + e(f(P_2))] \cdot [e(-f(P_1+1)) + \cdots + e(-f(P_2))] \\
&= \sum_{P_1 < x_1 \le P_2} \sum_{P_1 < x_2 \le P_2} e(f(x_2) - f(x_1)) \\
&= P_2 - P_1 + 2 \cdot \Re \sum_{\substack{P_1 < x_1, x_2 \le P_2 \\ x_2 > x_1}} e(f(x_2) - f(x_1))),
\end{aligned}$$

where $\Re x$ refers to the real part of x.

Then, we go through the *differencing* process: Let $x_2 = x_1 + y$. We define the *differencing operator*:

$$\Delta_y f(x_1) \coloneqq f(x_1 + y) - f(x_1).$$

We then have $1 \le y \le P_2 - P_1 \le P$ and $\Delta_y f(x_1) = f(x_2) - f(x_1)$.

So we get

$$|T_k(f)|^2 = P_2 - P_1 + 2 \cdot \Re \sum_{1 \le y \le P} \sum_{x \in I(y)} e(\Delta_y f(x)),$$

where $I(y)$ is the interval cut out by the inequalities $P_1 < x \le P_2$ and $P_1 < x+y \le P_2$.

Then we have

$$\begin{aligned}|T_k(f)|^2 &\leq P + 2\cdot\Re\sum_{1\leq y\leq P}|T_{k-1}(\Delta_y f)|\\ &\ll P + \sum_{1\leq y\leq P}|T_{k-1}(\Delta_y f)|\,,\end{aligned}$$

where the interval for $T_{k-1}(\Delta_y f)$ is contained in the interval $(P_1, P_2]$.

If we repeat the above argument again, we get

$$\begin{aligned}|T_{k-1}(\Delta_y f)|^2 &= \sum_{P_1\leq x_1\leq P_2}\sum_{P_1\leq x_2\leq P_2} e((\Delta_y f)(x_2)-(\Delta_y f)(x_1))\\ &= P_2 - P_1 + 2\cdot\Re\sum_{y,z\leq P} e((\Delta_y f)(x+z)-(\Delta_y f)(x))\\ &= P_2 - P_1 + 2\cdot\Re\sum_{y,z\leq P} e(\Delta_{y,z} f(x))\\ &\ll P + \sum_{1\leq z\leq P}|T_{k-2}(\Delta_{y,z} f)|\,,\end{aligned}$$

where the interval of summation in $T_{k-2}(\Delta_{y,z} f)$ is again contained in the interval $(P_1, P_2]$. By applying the Cauchy–Schwarz inequality, we obtain

$$\begin{aligned}|T_k(f)|^4 &\ll (P + \sum_{1\leq y\leq P}|T_{k-1}(\Delta_y f)|)^2\\ &= P^2 + (\sum_{1\leq y\leq P}|T_{k-1}(\Delta_y f)|)^2 + P\sum_{1\leq y\leq P}|T_{k-1}(\Delta_y f)|\\ &\ll P^2 + P\sum_{1\leq y\leq P}|T_{k-1}(\Delta_y f)|^2 && \text{(Cauchy–Schwarz inequality)}\\ &= P^2 + P\sum_{1\leq y\leq P}(P + \sum_{1\leq z\leq P}|T_{k-2}(\Delta_{y,z} f)|) && \text{(Substitution)}\\ &= P^2 + P^3 + P\sum_{1\leq y\leq P}\sum_{1\leq z\leq P}|T_{k-2}(\Delta_{y,z} f)|\\ &\ll P^3 + P\sum_{1\leq y\leq P}\sum_{1\leq z\leq P}|T_{k-2}(\Delta_{y,z} f)|\,.\end{aligned}$$

By iterating this way, via induction on j, applying the Cauchy–Schwarz inequality with squaring and differencing, we obtain the following estimate

$$|T_k(f)|^{2^j} \ll P^{2^j-1} + P^{2^j-j-1}\sum_{y_1,\ldots,y_j\leq P}\left|T_{k-j}(\Delta_{y_1,\ldots,y_j} f)\right|\,, \tag{2.3}$$

for any $0 \le j < k$. Again, the range of summation for x in $T_{k-j}(\Delta_{y_1,\ldots,y_j} f)$ is an interval contained in $(P_1, P_2]$.

Now, we may take $P_1 = 0$ and $P_2 = P$ in the original sum $T_k(f)$, and observe that

$$\Delta_{y_1,\ldots,y_{k-1}} f(x) = k!\alpha y_1 \cdots y_{k-1} x + \Psi,$$

where Ψ is a collection of terms independent of x. Thus, we have

$$\left|T_1(\Delta_{y_1,\ldots,y_{k-1}} f)\right| = \left| \sum_{x \in I(y_1,\ldots,y_{k-1})} e(k!\alpha y_1 \cdots y_{k-1} x) \right|,$$

where $I(y_1, \ldots, y_{k-1})$ is an interval of length at most P.

Notice that we are in fact dealing with a geometric series. We recall the following estimate

$$\left| \sum_{a<x\le b} e(\beta x) \right| \le \min\left(b - a, \frac{2}{|1 - e(\beta)|}\right),$$

for any $a < b$ and $\beta \in \mathbb{R}$. We also notice the following estimate

$$\frac{2}{|1 - e(\beta)|} = \frac{1}{\sin(\pi\beta)} \ll \frac{1}{\|\beta\|},$$

where $\|\beta\|$ is the distance of β to the nearest integer.

Now after taking $j = k - 1$ in (2.3) and applying the two estimates above, we have

$$\begin{aligned}
|T_k(f)|^{2^{k-1}} &\ll P^{2^{k-1}-1} + P^{2^{k-1}-k} \sum_{1 \le y_1,\ldots,y_{k-1} \le P} \left|T_1(\Delta_{y_1,\ldots,y_{k-1}} f)\right| \\
&= P^{2^{k-1}-1} + P^{2^{k-1}-k} \sum_{1 \le y_1,\ldots,y_{k-1} \le P} \left| \sum_{x \in I(y_1,\ldots,y_{k-1})} e(k!\alpha y_1 \cdots y_{k-1} x) \right| \\
&\le P^{2^{k-1}-1} + P^{2^{k-1}-k} \sum_{1 \le y_1,\ldots,y_{k-1} \le P} \min\left(P, \frac{2}{|1 - e(k!\alpha y_1 \cdots y_{k-1})|}\right) \\
&\ll P^{2^{k-1}-1} + P^{2^{k-1}-k} \sum_{1 \le y_1,\ldots,y_{k-1} \le P} \min\left(P, \frac{1}{\|k!\alpha y_1 \cdots y_{k-1}\|}\right).
\end{aligned}$$

Let $d(m) = \sum_{s|m} 1$ denote the divisor function. For any $\varepsilon > 0$ and positive integer m, we have the following classical bound

$$d(m) = O_\varepsilon(m^\varepsilon).$$

Therefore, the number of possible integers $y_1, \dots, y_{k-1}$ satisfy $m = k! y_1 \cdots y_{k-1}$ is at most

$$d(m)^{k-1} = O_\varepsilon(m^\varepsilon),$$

where the implied constant depends on k and ε. Hence, by redefining the choice of ε, we obtain

$$|T_k(f)|^{2^{k-1}} \ll_\varepsilon P^{2^{k-1}-1} + P^{2^{k-1}-k+\varepsilon/2} \sum_{1 \le m \le k! P^{k-1}} \min\left(P, \frac{1}{\|\alpha m\|}\right).$$

At last, we still need to estimate the last sum, with the assumption of the rational approximation a/q: Put $\alpha = a/q + \theta$, where $\gcd(a,q) = 1$, $q > 0$, and $|\theta| \le q^{-2}$, as in the assumption of Lemma 2.2. We divide the sum into residue classes modulo q, thus we obtain

$$\sum_{1 \le m \le k! P^{k-1}} \min(P, \frac{1}{\|\alpha m\|}) = \sum_{b \pmod q} \sum_{\substack{m \le k! P^{k-1} \\ m \equiv b \pmod q}} \min(P, \frac{1}{\|(a/q + \theta) m\|}).$$

If we write $m = b + qm'$, we obtain

$$\sum_{1 \le m \le k! P^{k-1}} \min(P, \frac{1}{\|\alpha m\|}) = \sum_{b \pmod q} \sum_{m' \le q^{-1} k! P^{k-1}} \min(P, \frac{1}{\|ab/q + \theta q m' + O(q^{-1})\|}),$$

since $b\,|\theta| \le 1/q$.

If we take $r = \lfloor \theta q^2 m' \rfloor$, then we have $\theta q m' - r/q = O(q^{-1})$. If we replace b by $\bar{a}(b - r)$, where $\bar{a}$ is the multiplicative inverse of a modulo q, then we get

$$\sum_{b \pmod q} \min(P, \frac{1}{\|ab/q + \theta q m' + O(q^{-1})\|}) = \sum_{b \pmod q} \min(P, \frac{1}{\|b/q + O(q^{-1})\|}).$$

Now we consider the two cases of b: When $b \ll 1$, we take P as the minimum; when $b \gg 1$, the denominator $\|b/q + O(q^{-1})\| \gg b/q$. Therefore, we have

$$\sum_{b \pmod q} \min(P, \frac{1}{\|ab/q + \theta q m' + O(q^{-1})\|}) \ll P + \sum_{1 \le b \le q} \frac{q}{b} \ll P + q \log(q).$$

Since $q \le P^k$, we have $\log(q) = O_\varepsilon(P^{\varepsilon/2})$. Introducing the sum over m' and noticing that the number of admissible m' is $O(1 + q^{-1} P^{k-1})$, we have shown that

$$\sum_{m \le k! P^{k-1}} \min(P, \frac{1}{\|\alpha m\|}) \ll_\varepsilon (1 + \frac{P^{k-1}}{q})(P + q P^{\varepsilon/2}) \ll_\varepsilon P^{k+\varepsilon/2}(\frac{1}{q} + \frac{1}{P} + \frac{q}{P^k}).$$

Hence,

$$|T_k(f)|^{2^{k-1}} \ll_\varepsilon P^{2^{k-1}-1} + P^{2^{k-1}+\varepsilon}(\frac{1}{q} + \frac{1}{P} + \frac{q}{P^k}).$$

We are now complete with the proof. □

After having shown the proof of Weyl's inequality, we now turn to the second important ingredient in the analysis of the exponential sums. The following is a famous result of Hua:

Lemma 2.3 (Hua's inequality)**.** *If*

$$T(\alpha) := \sum_{x=1}^{P} e(\alpha x^k),$$

then for any fixed $\varepsilon > 0$*, we have*

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

Proof. Let

$$I_v := \int_0^1 |T(\alpha)|^{2^v} \,\mathrm{d}\alpha.$$

We wish to show that

$$I_v \ll P^{2^v-v+\varepsilon} \quad \text{for } v = 1, \dots, k,$$

where the case $v = k$ is the result claimed in the lemma.

We will proceed by induction on v: For $v = 1$, we can see that

$$I_1 = \int_0^1 T(\alpha) \cdot T(-\alpha) \,\mathrm{d}\alpha = P$$

by the character orthogonality (2.1).

Now, we suppose our claim holds for $1 \leq v \leq k-1$. As in the proof of Weyl's inequality, the differencing trick (2.3) gives

$$|T(\alpha)|^{2^v} \ll P^{2^v-1} + P^{2^v-v-1}\Re\left(\sum_{1\leq y_1,\dots,y_v\leq P} S_{k-v}(\alpha)\right),$$

where

$$S_{k-v}(\alpha) = \sum_{x\in I(y_1,\dots,y_v)} e(\alpha\Delta_{y_1,\dots,y_v}(x^k)).$$

If we multiply both sides of the inequality by $|T(\alpha)|^{2^v}$ and integrate from 0 to 1, we get

$$\int_0^1 |T(\alpha)|^{2^{v+1}} \,\mathrm{d}\alpha = I_{v+1} \ll \int_0^1 |T(\alpha)|^{2^v} \cdot \left(P^{2^v-1} + P^{2^v-v-1} \Re \left(\sum_{1 \le y_1, \ldots, y_v \le P} S_{k-v}(\alpha) \right) \right)$$
$$= P^{2^v-1} I_v + P^{2^v-v-1} \sum_{1 \le y_1, \ldots, y_v \le P} \Re \int_0^1 S_{k-v}(\alpha) \, |T(\alpha)|^{2^v} \,\mathrm{d}\alpha.$$

Now we consider the last integral from previous estimate:

$$\int_0^1 S_{k-v}(\alpha) \, |T(\alpha)|^{2^v} \,\mathrm{d}\alpha = \int_0^1 \sum_{x \in I(y_1, \ldots, y_v)} e(\alpha \Delta_{y_1, \ldots, y_v}(x^k)) \sum_{\substack{u_1, \ldots, u_{2^{v-1}} \\ v_1, \ldots, v_{2^{v-1}}}} e(\alpha u_1^k + \cdots) e(-\alpha v_1^k - \cdots) \,\mathrm{d}\alpha,$$

where u_i and v_i go from 1 to P.

We notice that this integral actually counts the number of solutions to the following equation:

$$N \coloneqq \#\{\Delta_{y_1, \ldots, y_v}(x^k) + u_1^k + \cdots - v_1^k - \cdots = 0 : 1 \le x, y_i, u_i, v_i \le P\}.$$

By substitution, we get

$$I_{v+1} \ll P^{2^v-1} I_v + P^{2^v-v-1} N. \tag{2.4}$$

What remains is that we need to give an estimate for counting N: We observe that $\Delta_{y_1, \ldots, y_v}(x^k)$ is positive and divisible by each of $y_1, \ldots, y_v$. By the bound for the divisor function, if we fix every u_i and every v_i, we have at most P^{ε} choices for each $1 \le y_1, \ldots, y_v \le P$. Given all y_i, u_i, and v_i, we note that x is uniquely determined. Thus, we have

$$N \ll P^{2^v + v\varepsilon}.$$

Substituting in (2.4) and using the induction hypothesis, we have

$$I_{v+1} \ll P^{2^v-1} P^{2^v-v+\varepsilon} + P^{2^v-v-1} P^{2^v+v\varepsilon} \ll P^{2^{v+1}-(v+1)+v\varepsilon}.$$

Therefore we are complete with the proof. □

Chapter 3

The asymptotic formula

We now return to the starting point of our studies on Waring's problem:

$$R(N) = \int_0^1 T(\alpha)^s e(-N\alpha)\,\mathrm{d}\alpha, \tag{3.1}$$

where

$$e(x) = \exp(2\pi i x), \quad T(\alpha) = \sum_{1\le x\le P} e(\alpha x^k), \quad \text{and} \quad P = \left\lceil N^{1/k} \right\rceil.$$

As mentioned in the Introduction, the general plan of attack in the application of the circle method to Waring's problem and relevant problems is to divide the values of α into two sets: The *major arcs*, which contribute to the main term in the asymptotic formula, and the *minor arcs*, which go into the error term. In general, it is usually easier to work with the major arcs, and the crux of the problem lies in the minor arcs.

First, we are going to define the major arcs: Around every rational a/q, for some parameter $\delta > 0$, we put an interval

$$\mathfrak{M}_{a,q} \coloneqq \{\alpha \in [0,1] : \left|\alpha - \frac{a}{q}\right| \le P^{-k+\delta}\},$$

and we let

$$\mathfrak{M} \coloneqq \bigcup_{1\le q\le P^\delta} \bigcup_{\substack{a \pmod q \\ \gcd(a,q)=1}} \mathfrak{M}_{a,q}.$$

We will show that these intervals do not overlap: Suppose there exists a common point $\alpha \in \mathfrak{M}_{a,q} \cap \mathfrak{M}_{a',q'}$ for fractions $a/q \ne a'/q'$. Then we would have the following upper bound:

$$\left|\frac{a}{q}-\frac{a'}{q'}\right| \leq \left|\alpha-\frac{a}{q}\right|+\left|\alpha-\frac{a'}{q'}\right| \leq 2P^{-k+\delta}$$

and its corresponding lower bound:

$$\left|\frac{a}{q}-\frac{a'}{q'}\right| = \left|\frac{aq'-a'q}{qq'}\right| \geq \left|\frac{1}{qq'}\right| \geq \left|\frac{1}{P^{2\delta}}\right| = P^{-2\delta}.$$

If we combine the two bounds, we obtain

$$1 \leq 2P^{3\delta-k},$$

where cannot be achieved if $\delta < 1/3$. The set $\mathfrak{M} \subset [0,1]$ is called the set of major arcs for Waring's problem, and we define $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$ to be the set of minor arcs.

We then can estimate the contribution from the minor arcs to $R(N)$ as follows:

Lemma 3.1. *If $s \geq 2^k+1$, then we have*

$$\int_{\mathfrak{m}} |T(\alpha)|^s \,\mathrm{d}\alpha \ll P^{s-k-\delta'},$$

where δ' is a positive number dependent on δ.

Proof. By Dirichlet's approximation theorem, every $\alpha \in [0,1]$ has a rational approximation a/q satisfying

$$1 \leq q \leq P^{k-\delta}, \quad |\alpha - a/q| \leq q^{-1}P^{-k+\delta}. \tag{3.2}$$

We notice that if $q \leq P^{\delta}$, then by definition, we have $\alpha \in \mathfrak{M}_{a,q}$. It implies that if $\alpha \in \mathfrak{m}$, then

$$q > P^{\delta}. \tag{3.3}$$

By the consequences of application of Dirichlet's approximation theorem (3.2), we have

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

Then, we can apply Weyl's inequality (Lemma 2.2): Since (3.3) implying $q^{-1} < P^{-\delta}$ and $P^k/q \geq P^{\delta}$, we have

$$|T(\alpha)| \ll P^{1+\delta}\left(\frac{1}{P}+\frac{1}{q}+\frac{q}{P^k}\right)^{\frac{1}{2^{k-1}}} \ll P^{1+\varepsilon-\delta/2^{k-1}},$$

Combining with Hua's inequality (Lemma 2.3), we have

$$\begin{aligned}\int_{\mathfrak{m}} |T(\alpha)|^s \,\mathrm{d}\alpha &= \int_{\mathfrak{m}} |T(\alpha)|^{s-2^k} \cdot |T(\alpha)|^{2^k} \,\mathrm{d}\alpha \\ &\ll P^{(s-2^k)(1+\varepsilon-\delta/2^{k-1})} \int_0^1 |T(\alpha)|^{2^k} \,\mathrm{d}\alpha \\ &\ll P^{(s-2^k)(1+\varepsilon-\delta/2^{k-1})+2^k-k+\varepsilon}.\end{aligned}$$

Now we recall the assumption $s \geq 2^k+1$ and calculate the terms in the exponent explicitly:

$$\begin{aligned}(s-2^k)(1+\varepsilon-\frac{\delta}{2^{k-1}})+2^k-k+\varepsilon &= s-k+(s-2^k+1)\varepsilon+(2-\frac{s}{2^{k-1}})\delta \\ &\leq s-k+(s-2^k+1)\varepsilon-\frac{\delta}{2^{k-1}} \\ &\leq s-k+\frac{\delta}{2^k}.\end{aligned}$$

In the last step, we set $\varepsilon := \delta/(s-2^k+1)2^k$. Setting $\delta' := \delta/2^k$ in the following inequality, we obtain

$$\int_{\mathfrak{m}} |T(\alpha)|^s \,\mathrm{d}\alpha \ll P^{s-k-\delta'},$$

which completes the proof. □

Note 3.2. As mentioned above, in general, the treatment of the minor arcs is the challenging part of the circle method. Therefore, once one has found a solution to deal with minor arcs, one usually would make the minor arcs as large as the method permits. Then, one would hope that the rest can be attacked with the machinery of the major arcs.

It remains to study the contribution from the major arcs: To achieve this goal, we need to define the following:

$$S_{a,q} = \sum_{1\leq x\leq q} e\left(\frac{ax^k}{q}\right) \quad \text{and} \quad I(\beta) = \int_0^P e(\beta t^k)\,\mathrm{d}t.$$

Our first job is to approximate $T(\alpha)$ with these two integrals:

Lemma 3.3. *Let $\alpha \in \mathfrak{M}_{a,q}$ and $\beta = \alpha - a/q$. We have*

$$T(\alpha) = q^{-1}S_{a,q}I(\beta) + O(P^{2\delta}). \tag{3.4}$$

Proof. We write $1 \le x \le P$ as $x = qy + z$, where $1 \le z \le q$. We then have

$$T(\alpha) = \sum_{z=1}^{q} \sum_{y} e(\alpha(qy+z)^k) = \sum_{z=1}^{q} e\left(\frac{az^k}{q}\right) \cdot \sum_{y} e(\beta(qy+z)^k).$$

Next, we want to write the y-sum as an integral, where we would pick up some errors. We recall that for any differentiable function f, the mean-value theorem tells us that

$$|f(x) - f(y)| \le \frac{1}{2} \max |f'(x)| \quad \text{for } |x - y| \le \frac{1}{2}.$$

Then we would have

$$\left| \int_A^B f(x)\,\mathrm{d}x - \sum_{A<x<B} f(x) \right| \ll (B - A) \max |f'(x)| + \max |f(x)|.$$

In our case, $f(y) = e(\beta(qy+z)^k)$ with $|f(y)| \le 1$. Now we need to compute the derivate of $f(y)$:

$$f'(y) = 2\pi i k q \beta (qy+z)^{k-1} f(y) \ll q\,|\beta|\,P^{k-1}.$$

Notice that we also have $B - A \ll P/q$, so we have

$$\begin{aligned}\sum_{y} e(\beta(qy+z)^k) &= \int_A^B e(\beta(qy+z)^k)\,\mathrm{d}y + O(|\beta|\,P^k + 1) \\ &= q^{-1} \int_0^P e(\beta t^k)\,\mathrm{d}t + O(|\beta|\,P^k + 1).\end{aligned}$$

After plugging the y-sum into the right-hand side of first equation of the proof, we get

$$T(\alpha) = q^{-1} S_{a,q} I(\beta) + O(q(|\beta|\,P^k + 1)),$$

since we are only dealing with the major arcs, which means that we have $q \le P^{\delta}$ and $|\beta| \le P^{-k+\delta}$. Applying these two bounds in the error term completes the proof. □

Now we are ready to calculate the contribution from the major arcs:

Lemma 3.4. *Recall that $\mathfrak{M}$ denotes the totality of the major arcs $\mathfrak{M}_{a,q}$. We have*

$$\int_{\mathfrak{M}} T(\alpha)^s e(-N\alpha)\,\mathrm{d}\alpha = P^{s-k} \mathfrak{S}(P^{\delta}, N) J(P^{\delta}) + O(P^{s-k-\delta'}),$$

for some $\delta' > 0$, where

$$\mathfrak{S}(P^\delta, N) = \sum_{q \le P^\delta} \sum_{\substack{1 \le a \le q \\ \gcd(a,q)=1}} (q^{-1} S_{a,q})^s \cdot e\left(-N\frac{a}{q}\right),$$

$$J(P^\delta) = \int_{|\gamma| < P^\delta} \left(\int_0^1 e(\gamma t^k)\,\mathrm{d}t\right)^s e(-\gamma)\,\mathrm{d}\gamma.$$

Proof. First we notice the following simple observation:

$$\left|q^{-1} S_{a,q} I(\beta)\right| \le P,$$

then by binomial expansion of (3.4), we have

$$T(\alpha)^s = (q^{-1}S_{a,q})^s I(\beta)^s + O(P^{s-1+2\delta}).$$

Therefore, multiplying by $e(-Na)$ and integrating over $\mathfrak{M}_{a,q}$, that is, over $|\beta| < P^{-k+\delta}$, each arc yields

$$\begin{aligned}\int_{\mathfrak{M}_{a,q}} T(\alpha)^s e(-N\alpha)\,\mathrm{d}\alpha &= \int_{\mathfrak{M}_{a,q}} \left((q^{-1}S_{a,q})^s I(\beta)^s + O(P^{s-1+2\delta})\right) \cdot e\left(-N(\frac{a}{q}+\beta)\right) \\ &= (q^{-1}S_{a,q})^s e(-N\frac{a}{q}) \int_{|\beta|<P^{-k+\delta}} I(\beta)^s e(-N\beta)\,\mathrm{d}\beta + O(P^{s-k-1+3\delta})\end{aligned}$$

Now we collect all admissible a and q, we obtain

$$\int_{\mathfrak{M}} T(\alpha)^s e(-N\alpha)\,\mathrm{d}\alpha = \mathfrak{S}(P^\delta, N) \int_{|\beta|<P^{-k+\delta}} I(\beta)^s e(-N\beta)\,\mathrm{d}\beta + O(P^{s-k-1+5\delta}),$$

where we trivially bound the number of tuples (a,q) by $P^{2\delta}$. Similarly, it can also be used to bound $\mathfrak{S}(P^\delta, N) \ll P^{2\delta}$.

Now, we only need to determine the β-integral: Recall $P = \lceil N^{1/k} \rceil$, hence $N - P^k \ll P^{k-1}$. Again, by the mean-value theorem, we have

$$\left|e(-\beta N) - e(-\beta P^k)\right| \ll |\beta|\, P^{k-1} \ll P^{(-k+\delta)+(k-1)} \ll P^{-1+\delta}.$$

It implies that we could replace N with P^k and put the error in the error term:

$$\int_{\mathfrak{M}} T(\alpha)^s e(-N\alpha)\,\mathrm{d}\alpha = \mathfrak{S}(P^\delta, N) \int_{|\beta|<P^{-k+\delta}} I(\beta)^s e(-P^k\beta)\,\mathrm{d}\beta + O(P^{s-k-1+5\delta}).$$

If we look more closely at the β-integral, we obtain

$$\int_{|\beta|<P^{-k+\delta}} I(\beta)^s e(-P^k\beta)\,\mathrm{d}\beta = \int_{|\beta|<P^{-k+\delta}} \left(\int_0^P e(\beta t^k)\,\mathrm{d}t\right)^s e(-\beta P^k)\,\mathrm{d}\beta.$$

If we put $t = P\zeta$ and $\beta = P^k\gamma$ in the above equation, we get

$$\int_{|\beta|<P^{-k+\delta}} I(\beta)^s e(-P^k\beta)\,\mathrm{d}\beta = P^{s-k}J(P^\delta).$$

This completes the proof. □

Definition 3.5 (Singular series)**.** The *singular series* for the problem of representing N as a sum of s positive integral k-th power is

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

If $s \geq 2^k + 1$, the series is absolutely convergent, and uniformly with respect to N. By Weyl's inequality (Lemma 2.2), we have

$$\left|(q^{-1}S_{a,q})^s e\left(-N\frac{a}{q}\right)\right| \ll q^{-\frac{s}{2^{k-1}}+\varepsilon} \ll q^{-2-2^{-k+1}+\varepsilon}. \tag{3.5}$$

Later, we will prove that it is also true under the less restrictive condition that $s \geq 2k + 1$.

Theorem 3.6. *If $s \geq 2^k + 1$, the number $R(N)$ of representing N as a sum of s positive integral k-th powers satisfies*

$$R(N) = C_{k,s}N^{s/k-1}\mathfrak{S}(N) + O(N^{s/k-1-\delta'}), \tag{3.6}$$

for some fixed $\delta' > 0$, where

$$C_{k,s} = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)}.$$

Proof. By definition of $R(N)$ of (2.2), Lemma 3.1 (minor arc contribution), and Lemma 3.4 (major arc contribution), combining all our results so far, we obtain

$$\begin{aligned} R(N) &= \int_{\mathfrak{M}} T(\alpha)^s e(-Na)\,\mathrm{d}\alpha + \int_{\mathfrak{m}} T(\alpha)^s e(-Na)\,\mathrm{d}\alpha \\ &= \left(P^{s-k}\cdot\mathfrak{S}(P^\delta, N)J(P^\delta) + O(P^{s-k-\delta'})\right) + P^{s-k-\delta'} \\ &= P^{s-k}\cdot\mathfrak{S}(P^\delta, N)J(P^\delta) + O(P^{s-k-\delta'}) \end{aligned} \tag{3.7}$$

Once again, we can see that the most significant contribution comes from the major arc, as mentioned above.

We will first investigate the contribution from $J(P^\delta)$, whose definition we recall in the following:

$$J(P^\delta) = \int_{|\gamma|<P^\delta} \left(\int_0^1 e(\gamma t^k) \, \mathrm{d}t \right)^s e(-\gamma) \, \mathrm{d}\gamma$$

We first observe that the inner integral can be expressed in the following three ways, by changes of variables:

$$\int_0^1 e(\gamma t^k) \, \mathrm{d}t = k^{-1} \int_0^1 \zeta^{-1+\frac{1}{k}} e(\gamma\zeta) \, \mathrm{d}\zeta = k^{-1}\gamma^{-\frac{1}{k}} \int_0^1 \zeta^{-1+\frac{1}{k}} e(\zeta) \, \mathrm{d}\zeta, \tag{3.8}$$

where the first equality is obtained by setting $\zeta := t^k$ and the second by $\zeta := \gamma t^k$.

Since the integral in the last expression is bounded for all γ, by Dirichlet's test for infinite integrals with absolute convergence at 0, we obtain the estimate

$$\left| \int_0^1 e(\gamma t^k) \, \mathrm{d}t \right| \ll |\gamma|^{-\frac{1}{k}} .$$

It allows us to extend the γ-integral in $J(P^\delta)$ to infinity:

$$J(P^\delta) = J + O(P^{-(\frac{s}{k}-1)\delta}),$$

where (we choose the second expression in (3.8))

$$J = \int_{-\infty}^{\infty} \left(k^{-1} \int_0^1 t^{-1+\frac{1}{k}} e(\gamma t) \, \mathrm{d}t \right)^s e(-\gamma) \, \mathrm{d}\gamma.$$

We can see that J only depends on k and s, though in fact, $J = C_{k,s}$, which we will prove later. We will call J the *singular integral* for Waring's problem.

By the absolute convergence of the series $\mathfrak{S}(N)$ and the fact that $J(P^\delta) = J + O(P^{-(s/k-1)\delta})$, in (3.7), we can replace $\mathfrak{S}(P^\delta, N)$ by $\mathfrak{S}(N)$, $J(P)$ by J, and P by $N^{1/k}$, with permissible errors. As a result, we get (3.6) as in the theorem statement, except for the proof of $J = C_{k,s}$. However, we are not too concerned with the exact value of J, but only the fact that $J > 0$.

To actually evaluate J, we recall the following identity:

$$\int_{-\lambda}^{\lambda} e(\mu\gamma) \, \mathrm{d}\gamma = \frac{\sin(2\pi\gamma\mu)}{\pi\mu}.$$

We then can replace the infinite γ-integral in J with a suitable limit and interchanging integrals:

$$\begin{aligned} k^s J &= \lim_{\lambda\to\infty} \int_0^1 \cdots \int_0^1 (\zeta_1 \cdots \zeta_s)^{-1+\frac{1}{k}} \frac{\sin(2\pi\lambda(\zeta_1 + \cdots + \zeta_s - 1))}{\pi(\zeta_1 + \cdots + \zeta_s - 1)} \,\mathrm{d}\zeta_1 \cdots \mathrm{d}\zeta_s \\ &= \lim_{\lambda\to\infty} \int_0^s \varphi(u) \frac{\sin(2\pi\lambda(u-1))}{\pi(u-1)} \,\mathrm{d}u, \end{aligned}$$

where

$$\varphi(u) = \int_0^1 \cdots \int_0^1 (\zeta_1 \cdots \zeta_{s-1} \cdot (u - \zeta_1 - \cdots - \zeta_{s-1}))^{-1+\frac{1}{k}} \,\mathrm{d}\zeta_1 \cdots \mathrm{d}\zeta_{s-1},$$

and is taken over $\zeta_1, \ldots, \zeta_{s-1}$ for which $u - 1 < \zeta_1 + \cdots + \zeta_{s-1} < u$. We made the change of variable from ζ_s to u, where $\zeta_1 + \cdots + \zeta_s = u$.

Note that $\varphi(1)$ can be evaluated directly, for instance, by Dirichlet. We can also see that it is an extension of Euler's integral for the beta-function (i.e., $B(p,q) = \Gamma(p)\Gamma(q)/\Gamma(p+q)$). We then have

$$\varphi(1) = \frac{\Gamma(1/k)^s}{\Gamma(s/k)},$$

thus

$$J = k^{-s}\frac{\Gamma(1/k)^s}{\Gamma(s/k)} = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)}.$$

A sufficient condition for applying Fourier's integral theorem is that $\varphi(u)$ should be of bounded variation. To verify this, we put $\zeta_j = ut_j$, then we have

$$\varphi(u) = u^{s/k-1} \int_0^{1/u} \cdots \int_0^{1/u} (t_1 \cdots t_{s-1} \cdot (1 - t_1 - \cdots - t_{s-1}))^{-1+1/k} \,\mathrm{d}t_1 \cdots \mathrm{d}t_{s-1},$$

where the integral is over $t_1, \ldots, t_{s-1}$ for which $1 - 1/u < t_1 + \cdots + t_{s-1} < 1$. Since the integrand is now independent of u and the range of integration contracts as u increases, thus this completes the proof. □

Chapter 4

The singular series

In this chapter, we will study the singular series

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

We will find that the value of $\mathfrak{S}(N)$ is related to the number of solutions of the congruences

$$x_1^k + \cdots + x_s^k \equiv N \pmod{q},$$

for all possible integers q. If any such congruence is insoluble, then $\mathfrak{S}(N) = 0$.

We let

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q), \quad \text{where} \quad A(q) = \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{q} (q^{-1}S_{a,q})^s e\left(-N\frac{a}{q}\right).$$

Lemma 4.1. *If* $\gcd(q_1, q_2) = 1$*, then*

$$A(q_1q_2) = A(q_1)A(q_2).$$

Proof. We will start by writing

$$f(a,q) = S_{a,q}^s e\left(-N\frac{a}{q}\right).$$

If we have

$$\gcd(a_1, q_1) = \gcd(a_2, q_2) = 1, \quad \frac{a}{q} \equiv \frac{a_1}{q_1} + \frac{a_2}{q_2} \pmod{1}, \quad \text{and} \quad q = q_1q_2, \qquad (4.1)$$

then

$$f(a,q) = f(a_1,q_1)f(a_2,q_2).$$

To see this, we first compute

$$\begin{aligned}\frac{a}{q}q^k\left(\frac{z_1}{q_1}+\frac{z_2}{q_2}\right)^k &\equiv \frac{a}{q}q^k\left(\frac{z_1q_2+z_2q_1}{q_1q_2}\right)^k\\ &\equiv \frac{a}{q}(z_1q_2+z_2q_1)^k\\ &\equiv \left(\frac{a_1}{q_1}+\frac{a_2}{q_2}\right)(z_1q_2+z_2q_1)^k\\ &\equiv \frac{a_1}{q_1}(z_1q_2+z_2q_1)^k+\frac{a_2}{q_2}(z_1q_2+z_2q_1)^k\\ &\equiv \frac{a_1}{q_1}(q_2z_1)^k+\frac{a_2}{q_2}(q_1z_2)^k \pmod 1.\end{aligned}$$

With this, we then can write

$$\begin{aligned}S_{a,q} &= \sum_{z=1}^{q} e\left(\frac{a}{q}z^k\right)\\ &= \sum_{z_1=1}^{q_1}\sum_{z_2=1}^{q_2} e\left(\frac{a}{q}q^k\left(\frac{z_1}{q_1}+\frac{z_2}{q_2}\right)^k\right)\\ &= \sum_{z_1=1}^{q_1} e\left(\frac{a_1}{q_1}(q_2z_1)^k\right)\cdot\sum_{z_2=1}^{q_2} e\left(\frac{a_2}{q_2}(q_1z_2)^k\right)\\ &= S_{a_1,q_1}\cdot S_{a_2,q_2}.\end{aligned}$$

The last equality follows from changes of variables. We then notice that the multiplicativity of f follows from the following identity:

$$e\left(-N\frac{a}{q}\right) = e\left(-N\frac{a_1}{q_1}\right)e\left(-N\frac{a_2}{q_2}\right).$$

The statement of this lemma follows by observing

$$\sum_{\substack{a=1\\ \gcd(a,q)=1}}^{q} f(a,q) = \left(\sum_{\substack{a_1=1\\ \gcd(a_1,q_1)=1}}^{q_1} f(a_1,q_1)\right)\left(\sum_{\substack{a_2=1\\ \gcd(a_2,q_2)=1}}^{q_2} f(a_2,q_2)\right),$$

which we obtain from the three assumptions (4.1) in the beginning of this proof, which sets a one-to-one correspondence between reduced residue classes $a \pmod q$ and pairs of reduced residue classes $a_1 \pmod{q_1}$ and $a_2 \pmod{q_2}$. □

Lemma 4.2. *If $s \geq 2^k + 1$, then we have*

$$\mathfrak{S}(N) = \prod_p \chi(p),$$

where

$$\chi(p) = 1 + \sum_{v=1}^{\infty} A(p^v).$$

Furthermore, we have

$$\chi(p) = 1 + O(p^{-1-\delta}),$$

for some fixed $\delta > 0$.

Proof. From previous lemma, we know that if

$$q = p_1^{v_1} p_2^{v_2} p_3^{v_3} \cdots ,$$

then

$$A(q) = A(p_1^{v_1}) A(p_2^{v_2}) A(p_3^{v_3}) \cdots .$$

Thus we have

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q) = \prod_p \left(\sum_{v=0}^{\infty} A(p^v) \right) = \prod_p \chi(p),$$

by the absolute convergence of $\mathfrak{S}(N)$.

Recall the following estimate:

$$|A(q)| \ll q^{1-s/2^{k-1}+\varepsilon} \ll q^{-1-\delta},$$

which implies that

$$|\chi(p) - 1| \ll \sum_{v=1}^{\infty} p^{-v(1+\varepsilon)} \ll p^{-1-\delta},$$

by a standard geometric series argument. □

Corollary 4.3. *If $s \geq 2^k + 1$, then there exists $p_0 = p_0(k)$, such that*

$$\frac{1}{2} \leq \prod_{p > p_0} \chi(p) \leq \frac{3}{2}$$

We will see this also holds if $s \geq 2k + 1$.

This result will be greatly improved by relating the numbers $\chi(p)$ to the number of solutions to some congruence, thus we define

$$M(q) \coloneqq \#\{0 < x_i \leq q : x_1^k + \cdots + x_s^k \equiv N \pmod{q}\}.$$

Lemma 4.4. *We have*

$$1 + \sum_{v=1}^{n} A(p^v) = \frac{M(p^n)}{p^{n(s-1)}},$$

and consequently

$$\chi(p) = \lim_{n \to \infty} \frac{M(p^n)}{p^{n(s-1)}}.$$

Proof. We notice that by the definition of $M(q)$, we can express it in terms of exponential sums as an arithmetic analogue of that used to express $r(N)$ as an integral in (2.2):

$$M(q) = \frac{1}{q} \sum_{t=1}^{q} \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} e\left(\frac{t}{q}(x_1^k + \cdots + x_s^q - N)\right),$$

since the sum over t gives q if the congruence is satisfied, and 0 otherwise.

We then collect together those values of t that have the same highest common factor with q. If this highest common factor is denoted by q/q_1, then the values of t in question are uq/q_1, where $1 \leq u \leq q_1$ and $\gcd(u, q_1) = 1$. Therefore, by the above reasoning, we obtain

$$M(q) = \frac{1}{q} \sum_{q_1 | q} \sum_{\substack{u=1 \\ \gcd(u,q_1)=1}}^{q_1} \sum_{x_1=1}^{q} \cdots \sum_{x_s=1}^{q} e\left(\frac{u}{q}(x_1^k + \cdots + x_s^q - N)\right).$$

We notice

$$\sum_{x=1}^{q} e\left(\frac{u}{q_1} x^k\right) = \frac{q}{q_1} \sum_{x=1}^{q_1} e\left(\frac{u}{q_1} x^k\right) = \frac{q}{q_1} S_{u,q_1}.$$

Then we would obtain the following

$$M(q) = \frac{1}{q}\sum_{q_1|q}\sum_{\substack{u=1\\ \gcd(u,q_1)=1}}^{q_1}\left(\frac{q}{q_1}\right)^s S_{u,q_1}^s e\left(-\frac{uN}{q_1}\right) = q^{s-1}\sum_{q_1|q} A(q_1).$$

We are complete by setting $q = p^n$. □

It remains to thoroughly investigate the congruence at hand:

Definition 4.5. For each prime p, let p^τ be the highest power of p dividing k, and put $k = p^\tau k_0$. Define γ by

$$\gamma = \begin{cases} \tau + 1 & \text{if } p > 2, \\ \tau + 2 & \text{if } p = 2. \end{cases}$$

Of course, γ depends on both p and k.

We will then need the following result to lift certain congruences, which is a specific version of Hensel's lemma:

Lemma 4.6. *If the congruence $y^k \equiv m \pmod{p^\gamma}$ is soluble where $m \not\equiv 0 \pmod{p}$, then the congruence $x^k \equiv \pmod{p^v}$ is soluble for every $v > \gamma$.*

Proof. We first begin by considering the case $p > 2$: The relatively prime residue classes $\pmod{p^v}$ form a cyclic group of order $\varphi(p^v) = p^{v-1}(p-1)$. A generator g of this group is called a *primitive root to the modulus p^v*. If $v > \gamma$, then g is necessarily also a primitive root to the modulus p^γ.

We then write

$$m \equiv g^\mu, \quad y \equiv g^\eta, \quad , x \equiv g^\xi \pmod{p^v}.$$

Then, we find that the hypothesis $y^k \equiv m \pmod{p^\gamma}$ is equivalent to

$$k\eta \equiv \mu \pmod{p^{\gamma-1}(p-1)}.$$

Since $k = p^\tau k_0$ and $\tau = \gamma - 1$, it follows that μ is divisible by $p^{\gamma-1}$ and $\gcd(k_0, p-1)$.

Now, we can find ξ to satisfy

$$k\xi \equiv \mu \pmod{p^{v-1}(p-1)},$$

since μ is divisible by the highest common factor of k and $p^{v-1}(p-1)$. The last congruence is equivalent to $x^k \equiv m \pmod{p^v}$.

Now, we consider the case when $p = 2$: Notice that if k is odd, that is, $\tau = 0$, then there would be no problem, as every odd m is a n-th power modulo 2^v.

Then we suppose $\tau \geq 1$. Since $k = 2^\tau k_0$ is even, we have $x^k \equiv 1 \pmod 4$ for all x. Further, 5 is a generating element or a primitive root for the cyclic group of residue classes modulo 2^v with $\equiv 1 \pmod 4$ of order 2^{v-2}. As before, we proceed as

$$m \equiv 5^\mu, \quad y \equiv 5^\eta, \quad , x \equiv 5^\xi \pmod{2^v}.$$

Then the hypothesis is equivalent to

$$k\eta \equiv \mu \pmod{2^{\gamma-2}}.$$

Since $k = 2^\tau k_0$ and $\tau = \gamma - 2$, it follows that μ is divisible by 2^τ. Therefore, there exists ξ, such that

$$k\eta \equiv \mu \pmod{2^{v-2}},$$

which implies that $x^k \equiv m \pmod{2^v}$. □

Lemma 4.7. *If the congruence*

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^\gamma}$$

has a solution with $x_1, \ldots, x_s$ not all divisible by p, then $\chi(p) > 0$.

Proof. We may suppose

$$a_1^k + \cdots + a_s^k \equiv N \pmod{p^\gamma} \quad \text{and} \quad p \text{ does not divide } a_1.$$

For $v > \gamma$: We choose $x_2, \ldots, x_s$ arbitrarily in $p^{(v-\gamma)(k-1)}$ ways, such that

$$x_j \equiv a_j \pmod{p^\gamma}, \quad 0 < x_j \leq p^v.$$

Then, by previous lemma, we can choose $0 < x_1 \leq p^v$, such that

$$x_1^k \equiv N - x_2^k - \cdots - x_s^k \pmod{p^v}.$$

Since we have that many choices for $x_2, \ldots, x_s$, we have

$$M(p^v) \geq p^{(v-\gamma)(s-1)} = C_p p^{v(s-1)},$$

where $C_p = p^{-\gamma(s-1)} > 0$ and independent of v. We then can use this to obtain

$$\chi(p) = \lim_{v\to\infty} M(p^v) p^{-v(s-1)} \geq C_p > 0.$$

□

Lemma 4.8. *If $s \geq 2k$ for k odd or $s \geq 4k$ for k even, then $\chi(p) > 0$ for all primes p and all N.*

Proof. By previous lemma, we only need to show the congruence

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^\gamma} \tag{4.2}$$

is soluble with $x_1, \ldots, x_s$ not all divisible by p. If p does not divide N, then the latter requirement is satisfied. If p divides N, then we only need to solve the congruence

$$x_1^k + \cdots + x_{s-1}^k + 1^k \equiv N \pmod{p^\gamma}.$$

Thus we have reduced the problem to solve the congruence (4.2) for $s \geq 2k - 1$ (k odd) or $s \geq 4k - 1$ (k even) when p does not divide N.

We start with the general case $p > 2$: We consider all N satisfying

$$0 < N < p^\gamma \quad \text{and} \quad N \not\equiv 0 \pmod{p},$$

and there are $\varphi(p^\gamma) = p^{\gamma-1}(p-1)$ of them. Let $s(N)$ denote the least s for which the congruence (4.2) is soluble. We observe that if $N \equiv z^k N' \pmod{p^\gamma}$, then $s(N) = s(N')$. Therefore, if we partition the numbers N into classes according to the value of $s(N)$, then the number in each class is at least equal to the number of distinct values assumed by z^k when $\gcd(z, p) = 1$. If we put $z \equiv g^\zeta \pmod{p^\gamma}$, and $a \equiv g^\alpha \pmod{p^\gamma}$, we can see that the congruence $z^k \equiv a \pmod{p^\gamma}$ is soluble if and only if α is divisible by $p^\tau \delta$, where $\delta = \gcd(k, p-1)$. Since $\tau = \gamma - 1$, then the number of distinct values for $\alpha \pmod{p^{\gamma-1}(p-1)}$, which is also equal to the number of distinct values for $a \pmod{p^\gamma}$, is

$$\frac{p^{\gamma-1}(p-1)}{p^{\gamma-1}\delta} = \frac{p-1}{\delta} = r.$$

Therefore, each class of values of N includes at least r elements.

Now, we may enumerate first all N, for which $s(N) = 1$:

$$N_1^{(1)} < N_2^{(1)} < \cdots < N_{r_1}^{(1)}, \quad \text{where } r_1 \geq r.$$

Then we may enumerate all N, for which $s(N) = 2$:

$$N_1^{(2)} < N_2^{(2)} < \cdots < N_{r_2}^{(2)}, \quad \text{where } r_2 \geq r,$$

and so on. We will see that even if some of these sets may be empty, but two consecutive sets cannot be empty at the same time: Consider the least N' not divisible by p, which is not in any of the first $j-1$ sets. Then, either $N'-1$ or $N'-2$ does not divide p, and being less than N', it must be in one of the first $j-1$ sets. We may represent N' as

$$(N'-1)+1^k \quad \text{and} \quad (N'-2)+1^k+1^k,$$

and can deduce that $s(N') \leq j+1$. Hence the sets for which $s(N)=j$ and $s(N)=j+1$ cannot both be empty.

Suppose the last set in this enumeration with $s(N)=m$. Then at least $\frac{1}{2}(m-1)$ of the first $m-1$ sets are not empty, and the m-th set is not empty, making at least $\frac{1}{2}(m+1)$ non-empty sets.

Since each set contains at least r numbers, we have

$$\frac{1}{2}r(m+1) \leq \varphi(p^\gamma) = p^{\gamma-1}(p-1).$$

We further observe

$$m+1 \leq \frac{2p^{\gamma-1}(p-1)}{r} = 2p^{\gamma-1}\delta = 2p^\tau \gcd(k_0, p-1) \leq 2k.$$

So we obtain that $m \leq 2k-1$, whence $s(N) \leq 2k-1$, for all N. Therefore, for $p > 2$, the congruence (4.2) is soluble for $s \geq 2k-1$.

In the case of $p=2$: If $\tau = 0$, or equivalently k is odd, then the congruence (4.2) is soluble for p does not divide N when $s=1$. This proves the conclusion of this lemma, since then the only restriction on s comes from the primes $p > 2$.

Now we may suppose $\tau \geq 1$, so that k is even. Without loss of generality, we may suppose that $0 < N < 2^\gamma$, since N is odd. If we take all the x_i in (4.2) to be 0 or 1, then we can solve the congruence if $s \geq 2^\gamma - 1$. Now, we have

$$2^\gamma - 1 = 2^{\tau+2} - 1 \leq 4k-1.$$

Thus it suffices if $s \geq 4k-1$, and proves the conclusion of this lemma in the case of k being even. □

In the style of Hardy and Littlewood, we set $\Gamma(k)$ to be the least value of s, such that the congruence

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^\gamma}$$

is soluble with x_i not all divisible by p, for all p and N. We have seen so far that

$$\Gamma(k) \leq \begin{cases} 2k & \text{if } k \text{ is odd,} \\ 4k & \text{if } k \text{ is even.} \end{cases}$$

Now, we are ready to prove the following important theorem:

Theorem 4.9. *If $s \geq 2^k + 1$, then*

$$\mathfrak{S}(N) \geq C_1(k, s) > 0,$$

where $C_1(k, s)$ is some constant, for all N.

Proof. By Lemma 4.2, if $s \geq 2^k + 1$, then

$$\mathfrak{S}(N) = \prod_p \chi(p).$$

The assumption $s \geq 2^k + 1$ implies the conditions of Lemma 4.8, hence in all cases, each factor $\chi(p)$ is strictly positive. Corollary 4.3 implies that, under the condition $s \geq 2^k + 1$, there exists some finite cut-off prime $p_0 = p_0(k)$, such that

$$\frac{1}{2} \leq \prod_{p > p_0} \chi(p) \leq \frac{3}{2}.$$

Again, by Lemma 4.2,

$$\mathfrak{S}(N) = \prod_p \chi(p) = \prod_{p \leq p_0} \chi(p) \cdot \prod_{p > p_0} \chi(p) \geq \prod_{p \leq p_0} \chi(p) \cdot \frac{1}{2} > 0.$$

□

This theorem is a necessary supplement to Theorem 3.6, as it shows that the main term in the asymptotic formula is $\gg N^{s/k-1}$, and thus, $r(N)$ tends to infinity as N tends to infinity.

Combining all these results, we obtain the following main theorem:

Theorem 4.10. *Every sufficiently large number can be written as the sum of s positive integral k-th powers for $s \geq 2^k + 1$.*

Chapter 5

The singular series continued

Note that we have only established absolute convergence for the singular series $\mathfrak{S}(N)$ when $s \geq 2^k + 1$, which we will improve to $s \geq 2k+1$ in this chapter.

Lemma 5.1. *If p does not divide a and $\delta = \gcd(k, p-1)$, then*

$$|S_{a,p}| \leq (\delta - 1)p^{\frac{1}{2}}$$

Proof. We first observe that $x^k \equiv m \pmod{p}$ and $x^\delta \equiv m \pmod{p}$ have the same number of solutions: Let g be a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of order $p-1$, so every non-zero element modulo p can be written as g^r for some integer r.

Therefore, the equation

$$x^k \equiv m \pmod{p}$$

can be written as

$$g^{ks} = g^t \Longrightarrow ks \equiv t \pmod{p-1},$$

where we set $x = g^s$ and $m = g^t$.

Similarly, the equation

$$x^\delta \equiv m \pmod{p}$$

would be

$$\delta s \equiv t \pmod{p-1}.$$

Because $\delta = \gcd(k, p-1)$, both congruences either have δ solutions in s or no solutions at all. Hence, for each $m = g^t$, the number of x solving $x^k \equiv m$ is the same as the number of x solving $x^\delta \equiv m$.

By the definition of $S_{a,q}$, we then have

$$S_{a,p} \coloneqq \sum_{1 \le x \le p} e\left(\frac{ax^k}{p}\right) = \sum_{x \pmod p} e\left(\frac{ax^\delta}{p}\right).$$

Let χ be a primitive character modulo p of order δ. Then we observe

$$\#\{x \pmod p : x^\delta \equiv t \pmod p\} = 1 + \chi(t) + \cdots + \chi^{\delta-1}(t),$$

which follows immediately from the orthogonality relations for Dirichlet characters.

With this at hand, we then can write

$$S_{a,p} = \sum_{0 \le n \le \delta - 1} \sum_{x \pmod p} \chi^n(t) e\left(\frac{a}{p} t\right). \tag{5.1}$$

If ψ is any non-principal character modulo p, then the sum

$$T(\psi) = \sum_{t \pmod p} \psi(t) e\left(\frac{a}{p} t\right)$$

is called a *Gauss sum.* It is a classical result due to Gauss that $|T(\psi)| = p^{1/2}$, which we repeat here for completeness: We consider

$$\begin{aligned} |T(\psi)|^2 &= \sum_t \sum_u \psi(t) \overline{\psi}(u) e\left(\frac{a}{p}(t-u)\right) \\ &= \sum_t \sum_{u \ne 0} \psi(t) e\left(\frac{a}{p} u(t-1)\right). \end{aligned}$$

We notice that the inner sum is $p-1$ if $t = 1$ and $-\psi(t)$ otherwise, hence

$$|T(\psi)|^2 = p\psi(1) - \sum_t \psi(t) = p.$$

We are done after taking the square root and using this in (5.1) for $\psi = \chi, \ldots, \chi^{\delta-1}$. □

Lemma 5.2. *Suppose p does not divide a and p does not divide k. Then, for $1 < v \le k$, we have*

$$S_{a,p^v} = p^{v-1},$$

and for $v > k$, we have

$$S_{a,p^v} = p^{k-1} S_{a,p^{v-k}}.$$

Proof. By definition,

$$S_{a,p^v} = \sum_{x=0}^{p^v-1} e\left(\frac{a}{p^v}x^k\right).$$

If we put $x = p^{v-1}y + z$, where $0 \le y < p$ and $0 \le z < p^{v-1}$, then

$$x^k \equiv (p^{v-1}y + z)^k \equiv z^k + kp^{v-1}z^{k-1}y \pmod{p^v}.$$

We then obtain

$$S_{a,p^v} = \sum_{z=0}^{p^{v-1}-1} \sum_{y=0}^{p-1} e\left(\frac{az^k}{p^v} + \frac{akz^{k-1}y}{p}\right).$$

Note that by assumption p does not divide ak, and the inner sum is 0 unless p divides z. Thus, we can write $z = pw$ and get

$$S_{a,p^v} = p\sum_{w=0}^{p^{v-2}-1} e\left(\frac{aw^k}{p^{v-k}}\right).$$

We notice that if $v \le k$, then we are just summing up ones and would get $S_{a,p^v} = p^{v-1}$. If $v > k$, we observe that we are summing up a function of period p^{v-k}, so we have

$$S_{a,p^v} = pp^{k-2}S_{a,p^{v-k}}.$$

We are now done. □

Lemma 5.3. *The second result of Lemma 5.2 holds as well when $p \mid k$, that is,*

$$S_{a,p^v} = p^{k-1}S_{a,p^{v-k}}.$$

Proof. As before, we put $k = p^\tau k_0$, and note since $v > k$, we have

$$v > k = p^\tau k_0 \ge 2^\tau \ge \tau + 1,$$

thus $v \ge \tau + 2$. Also, we have $k \ge \tau + 2$, since $k \ge 6$ if $\tau = 1$.

We then follow the idea of previous proof with minor modifications: We write

$$x = p^{v-\tau-1}y + z \quad \text{for } 0 \le y < p^{\tau+1} \quad \text{and} \quad 0 \le z < p^{v-\tau-1}.$$

We wish to prove, and assume for now, we have

$$x^k \equiv z^k + kp^{v-\tau-1}z^{k-1}y \pmod{p}. \tag{5.2}$$

Then the proof can be completed in a similar fashion as before: We have

$$S_{a,p^v} = \sum_{z=0}^{p^{v-\tau-1}-1} \sum_{y=0}^{p^{\tau+1}-1} e\left(\frac{az^k}{p^v} - \frac{ak_0 z^{k-1} y}{p}\right).$$

Note that once again the inner sum vanishes unless p divides z, thus

$$S_{a,p^v} = p^{\tau+1} \sum_{w=0}^{p^{v-\tau-2}-1} e\left(\frac{aw^k}{p^{v-k}}\right) = p^{\tau+1} p^{k-\tau-2} \cdot S_{a,p^{v-k}},$$

which proves the theorem.

It remains to prove the congruence (5.2): It suffices to show that

$$(p^{v-\tau-1}y + z)^{p^\tau} \equiv z^{p^\tau} + p^{v-1} z^{p^\tau - 1} y \pmod{p^v},$$

as raising both sides to the power k_0 presents no difficulty. If we put $\lambda \coloneqq v - \tau - 1$, then we need to prove

$$(p^\lambda y + z)^{p^\tau} \equiv z^{p^\tau} + p^{\lambda+\tau} z^{p^\tau - 1} y \pmod{p^{\lambda+\tau+1}}.$$

Since not all the binomial coefficients in the expansion of $(A+B)^{p^\tau}$ are divisible by p^τ, we need to continue by induction on τ.

The starting point is $\tau = 1$: In this case, we have $\lambda \geq 1$ (if $p > 2$) and $\lambda \geq 2$ (if $p = 2$). We only need to examine the last term in the binomial expansion, which is $p^{\lambda p} y^p$. For this we need to show that $\lambda p \geq \lambda + 2$, which is true under the hypothesis.

We continue the induction step: For $y_1 \equiv y \pmod{p}$, we have

$$\begin{aligned}(z + p^\lambda y)^{p^\tau} &= (z^{p^{\tau-1}} + p^{\lambda+\tau-1} z^{p^{\tau-1}-1} y_1)^p \\ &\equiv z^{p^\tau} + p^{\lambda+\tau} z^{p^\tau - 1} y_1 \pmod{p^{\lambda+\tau+1}} \\ &\equiv z^{p^\tau} + p^{\lambda+\tau} z^{p^\tau - 1} y \pmod{p^{\lambda+\tau+1}}.\end{aligned}$$

This holds true by assumptions on λ and we are done. □

Lemma 5.4. *For* $\gcd(a,q) = 1$, *we have*

$$|S_{a,q}| \ll q^{1-\frac{1}{k}}.$$

Proof. We write

$$T(a,q) = q^{-1+a/k} S_{a,q}.$$

We now wish to prove that $T(a,q)$ is bounded independently of q. If $q = p_1^{v_1}p_2^{v_2}\cdots$, then by the multiplicativity established earlier, we have

$$T(a,q) = T(a_1, p_1^{v_1})T(a_2, p_2^{v_2})\cdots ,$$

for suitable $a_1, a_2, \ldots$, each of which is relatively prime to each corresponding p^v. By previous two lemmas, we have

$$T(a, p^v) = T(a, p^{v-k}),$$

for $v > k$. Applying this repeatedly allows us to assume that $v_i \leq k$.

By Lemma 5.1, we have

$$T(a,p) \leq kp^{1/2}p^{-(1-1/k)} \leq kp^{-1/6},$$

and by the first part of Lemma 5.2, we have

$$T(a,p^v) = p^{v-1}p^{-v(1-1/k)} \leq 1 \quad \text{for } a < v \leq k.$$

Thus, $T(a,p^v) \leq 1$ except when $v = 1$ and $p \leq k^6$. Therefore, we have

$$T(a,q) \leq \prod_{p \leq k^6} (kp^{-1/6}),$$

and the number on the right is independent of q. □

Theorem 5.5. *The singular series $\mathfrak{S}(N)$ and the product $\prod_p \chi(P)$ are absolutely convergent if $s \geq 2k+1$, and we have*

$$\mathfrak{S}(N) \geq C_1(k,s) > 0,$$

where $C_1(k,s)$ is some constant, if $s \geq 2k+1$ for k odd or $s \geq 4k$ for k even.

Proof. The absolute convergence of the singular series $\mathfrak{S}(N)$ follows as before in (3.5): If $s \geq 2k+1$, then by Lemma 5.4, we have

$$\left|\left(q^{-1} \cdot S_{a,q}\right)^s e\left(-N\frac{a}{q}\right)\right| \leq \left|\left(q^{-1} \cdot S_{a,q}\right)^s\right| \ll q^{-\frac{s}{k}} \ll q^{-2-\frac{1}{k}}.$$

The rest follows in a similar fashion as in the proof of Theorem (4.9). □

Chapter 6

Conclusion

In this thesis, we have conducted an in-depth study of the application of the circle method to Waring's problem, achieving both a re-derivation of classical results and a deeper understanding of the underlying analytic machinery.

First, we established the key exponential sum estimates — Weyl's inequality (Lemma 2.2) and Hua's inequality (Lemma 2.3) — which are instrumental in handling the "minor arc" contributions. These inequalities provided rigorous upper bounds on exponential sums of k-th powers, ensuring that the total contribution of the minor arcs in our singular integral is $o(1)$ relative to the main term. Next, using a major/minor arc decomposition of the integral that counts representations of N as $x_1^k + \cdots + x_s^k$, we derived the *asymptotic formula* for the number of such representations $R_s^{(k)}(N)$ when the number of variables is $s \geq 2^k + 1$. In particular, we showed that for s above this threshold, the formula takes the shape

$$R_s^{(k)}(N) \sim C_{k,s} N^{s/k-1} \mathfrak{S}(N),$$

where $C_{k,s}$ is an explicit constant (coming from the gamma-function and volume of the solution set on the major arcs) and $\mathfrak{S}(N)$ is the *singular series*. We verified that under the same condition ($s \geq 2^k+1$), the singular series $\mathfrak{S}(N)$ converges absolutely and satisfies $\mathfrak{S}(N) \geq \gamma > 0$ for some fixed γ independent of N. This non-vanishing of $\mathfrak{S}(N)$ is crucial, as it confirms that the main term in the asymptotic formula is asymptotically bounded away from zero.

One of the key findings of this thesis is a self-contained proof that $G(k) \leq 2^k + 1$ for all k (recovering Hua's classical result in a modern presentation). We also examined the nature of the singular series in detail, showing how it factorizes into p-adic densities and how mild growth conditions ensure its convergence. In doing so, we addressed subtleties of interchanging summations and integrating term-by-term, thereby firming up the rigour behind the heuristic major/minor arc arguments. Overall, the thesis reinforced how the circle method successfully yields not just *qualitative* solutions but also *quantitative* and *asymptotic information* about the distribution of such representations.

6.1 Broader Implications

Beyond the specific proofs, the broader implications of these findings resonate with several central themes in analytic number theory. The work illustrates the efficacy of the circle method as a bridge between additive combinatorics and analysis: the ability to convert an additive problem into an integral and exponential sum problem is what allows us to bring powerful analytic tools to bear. The success of the method in deriving an asymptotic formula for Waring's problem solidifies the circle method's reputation as a cornerstone technique in the field.

Many other problems in analytic number theory share a similar outline: One seeks to show that a certain generating function's coefficients have the expected size, often by locating the dominant contributions from certain "major" regions of integration and controlling the rest. The present work on sums of k-th powers is a paradigmatic example of this approach.

Moreover, the role of the singular series $\mathfrak{S}(N)$ highlights a unifying principle: To solve a global problem (like representing all large N), one must account for local obstructions and densities at every prime. The fact that $\mathfrak{S}(N)$ is positive in our case means there are no local obstructions, and this principle carries over to other additive problems – whenever a singular series (or analogous product of local factors) vanishes, it signals a deeper obstruction that no analytic method can overcome. In Waring's problem, our confirmation that $\mathfrak{S}(N)$ stays bounded away from zero for $s \geq 2k + 1$ is thus a confirmation that the only hurdle to expressing large N in the desired form was an analytic one (overcome by our estimates), not a fundamental arithmetic obstruction.

6.2 Future Directions

While this thesis has resolved the targeted questions and reproduced a landmark result, it also opens the door to several future directions and unresolved problems:

- **Tightening the Bound on $G(k)$**: There is considerable interest in further reducing the number of summands required in Waring's problem. The best known bound for large k is $G(k) \leq k(\log k + \log\log k + O(1))$, but proving the conjectural bound $G(k) = k + 1$ remains open.

- **Waring's Problem for Small k and Exact Values**: For small k, exact values of $g(k)$ and $G(k)$ remain difficult to determine, as the circle method gives only asymptotic for large N. Future research can refine error bounds or combine analytic methods with computational verification.

- **Refinements of the Circle Method**: New developments in harmonic analysis (such as Wooley's efficient congruence and decoupling techniques) offer avenues to further refine minor arc estimates and singular series evaluations.

- **Applications to Other Additive Problems**: The circle method has been applied to problems like Goldbach's conjecture and sums of polygonal numbers. Future research can explore its adaptation to other additive questions involving prime variables or mixed power sums.

In conclusion, this thesis has reaffirmed the power of the circle method by concretely demonstrating its use on Waring's problem, and it has highlighted how each piece of the method contributes to the final result. The key findings provide a solid foundation and reference point for anyone looking to enter this area of research. At the same time, the discussion of open problems and future directions shows that there is ample room to push these ideas further. The circle method, deeply rooted in the work of Hardy, Littlewood, and their successors, remains very much alive. Continued research in this area promises not only to inch closer to the ultimate resolution of Waring's problem (in its various forms) but also to enrich the toolkit of analytic number theory, enabling us to tackle a wider array of problems about expressing numbers as sums of structured sets of terms. The ongoing developments stand as a testament to the enduring legacy and adaptability of the circle method in the pursuit of understanding additive properties of integers.

Bibliography

[Hil09] David Hilbert. “Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahlnter Potenzen (Waringsches Problem)”. In: *Mathematische Annalen* 67.3 (1909), pp. 281–300. ISSN: 1432-1807. DOI: 10.1007/BF01450405. URL: https://doi.org/10.1007/BF01450405.

[HR18] G. H. Hardy and S. Ramanujan. “Asymptotic Formulaæ in Combinatory Analysis”. In: *Proceedings of the London Mathematical Society* s2-17.1 (1918), pp. 75–115. DOI: https://doi.org/10.1112/plms/s2-17.1.75. eprint: https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/plms/s2-17.1.75. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/plms/s2-17.1.75.

[HL20] G. H. Hardy and J. E. Littlewood. “Some problems of ’Partitio numerorum’; I: A new solution of Waring‘s problem”. In: *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* 1920 (1920), pp. 33–54. URL: http://eudml.org/doc/59073.

[HUA38] LOO-KENG HUA. “ON WARING’S PROBLEM”. In: *The Quarterly Journal of Mathematics* os-9.1 (Jan. 1938), pp. 199–202. ISSN: 0033-5606. DOI: 10.1093/qmath/os-9.1.199. eprint: https://academic.oup.com/qjmath/article-pdf/os-9/1/199/4460503/os-9-1-199.pdf. URL: https://doi.org/10.1093/qmath/os-9.1.199.

[Vin47] Ivan Matveevich Vinogradov. “The method of trigonometrical sums in the theory of numbers”. In: *Trudy Matematicheskogo Instituta imeni VA Steklova* 23 (1947), pp. 3–109.

[Dav05] Harold Davenport. *Analytic Methods for Diophantine Equations and Diophantine Inequalities*. Ed. by T. D. Browning. Cambridge Mathematical Library. Online publication date: January 2010. Cambridge University Press, 2005. ISBN: 9780511542893. DOI: 10.1017/CBO9780511542893. URL: https://doi.org/10.1017/CBO9780511542893.

[BDG16] Jean Bourgain, Ciprian Demeter, and Larry Guth. “Proof of the main conjecture in Vinogradov’s mean value theorem for degrees higher than three”. In: *Annals of Mathematics* (2016), pp. 633–682.

Ich habe die Arbeit selbständig verfasst, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt und bisher keiner anderen Prüfungsbehörde vorgelegt. Außerdem bestätige ich hiermit, dass die vorgelegten Druckexemplare und die vorgelegte elektronische Version der Arbeit identisch sind und dass ich von den in § 26 Abs. 6 vorgesehenen Rechtsfolgen Kenntnis habe.