An Exposition of The Circle Method

Tomasz Ślusarczyk, Allen Lin, Alek Westover

March 2024

Abstract

The circle method is a powerful technique in analytic number theory for estimating integrals over the circle $\mathbb{R}/\mathbb{Z}$. Often when dealing with a f function derived from a number-theoretical object on $\mathbb{R}/\mathbb{Z}$ the following will occur: (1) at reals α which are far from all fractions of small denominator the value $f(\alpha)$ is relatively small, (2) at reals α which are very close to a fraction of small denominator $f(\alpha)$ grows very large. When dealing with such a situation it is often productive to split the integral into "major arcs": parts of the circle close to fractions of small denominator, and "minor arcs": parts of the circle far from all fractions of small denominator.

In this note, we give an exposition of an early application of the circle method: namely, Waring's Problem of finding the number of ways a number n can be expressed as the sum of a fixed number s of k-th powers. In addition to being an exposition of the circle method this note aims to give an introduction to several useful tools and paradigms in analytic number theory such as inequalities for bounding exponential sums and techniques for bounding integrals. The main proof exposition is based on chapter 5 of Nathanson's excellent book [Nat13], which is a simplification of the original proof by Vinogradov [Vin28].

1 Motivation

A major topic in additive number theory is the following question: "Given a set $A \subseteq \mathbb{N}$, can every sufficiently large positive integer be expressed as the sum of a bounded number of elements of A?" If the answer is positive we may be more ambitious and ask "In how many ways can number n be represented as the sum of s elements from A?" We say that the set A is an ***additive basis*** of order s if every positive integer can be written as the sum of at most s elements from A.

Here are some famous examples of problems of this form:

- Lagrange's four-square theorem states that all numbers can be written as the sum of four squares. That is, the set of squares are an additive basis of order 4 [Nat13].
- Goldbach's Conjecture states that the primes are an additive basis of order 2. This remains an open question. However, using circle method techniques Helfgott proved [Hel14] that the primes are an additive basis of order at most 3.
- Waring's problem ([Woo23]), the focus of this paper, asks whether the set of k-th powers is an additive basis of finite order. See [VW02] for a discussion of the best known bounds of what the order is for each value of k.

Our goal in this paper is to understand the following quantity:

Definition 1.1. Let $r_{k,s}(N)$ be the number of $x_1, x_2 \ldots, x_s \in \mathbb{N}$ such that $\sum_{i=1}^{s} x_i^k = N$.

To show that the k-th powers are an additive basis of order at most s it suffices to show that $r_{k,s}(N) > 0$ for sufficiently large N. We will show a much stronger statement: a precise asymptotic formula for $r_{k,s}(N)$. Specifically our goal is to show:

Theorem 1.2. [Hardy-Littlewood] For any $k, s \in \mathbb{N}$ with $s \geq 2^k + 1$ we have

$$r_{k,s}(N) = \Theta(N^{s/k-1}).$$

To get a feel for why this size is intuitive, notice that $|[\lceil N^{1/k} \rceil]^s| = \Theta(N^{s/k})$.

2 Preliminaries

We write $a \perp b$ to denote that $\gcd(a, b) = 1$. We write $f(n) \lesssim g(n)$ or $f(n) \leq O(g(n))$ to denote that $f(n) \leq Cg(n)$ for some constant C, and we write $f(n) < o(g(n))$ means $\lim_{n\to\infty} f(n)/g(n) = 0$. We define $[n]$ to be $\{1, 2, \ldots, n\}$.

Now we develop some basic tools for bounding ***exponential sums***. Exponential sums play a central role in using analytic tools to control the behavior of combinatorial objects. The most basic type of exponential sum is an exponential sum with "linear phase". Define $e(x) = e^{2\pi i x}$. A basic and important fact is (see [Gut22]):

Fact 2.1. Let $a, b \in \mathbb{N}$. Then

$$\sum_{n=1}^{b} e(n \cdot a/b) = 0.$$

If $\alpha \notin \mathbb{Q}$ then for large enough N we expect $[N] \cdot \alpha$ to be fairly uniformly distributed on the circle $\mathbb{R}/\mathbb{Z}$. For $\alpha \in \mathbb{R}$, let $\|\alpha\|_{\mathbb{Z}}$ denote the distance from α to the closest integer. We have:

Lemma 2.2. Let $\alpha \in \mathbb{R}$. Then

$$\left|\sum_{n=1}^{N} e(\alpha n)\right| \lesssim \min\left(N, \|\alpha\|_{\mathbb{Z}}^{-1}\right).$$

Proof. Note that $|e(\alpha n)| = 1$ for each $n \in \{1, \ldots, N\}$, giving the bound

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

by the triangle inequality. On the other hand, note that the sum is a geometric series and $|1 - e(\alpha)| \geq \|\alpha\|_{\mathbb{Z}}/5$, so

$$\left|\sum_{n=1}^{N} e(\alpha n)\right| = \left|\frac{e(\alpha) - e(\alpha)^{N+1}}{1 - e(\alpha)}\right| \leq \frac{2}{|1 - e(\alpha)|} \lesssim \frac{1}{\|\alpha\|_{\mathbb{Z}}},$$

as required. □

Now we turn our attention to understanding exponential sums of with higher-order polynomial phases. We have the following important theorem:

Theorem 2.3 (Weyl's Inequality)**.** Let $\alpha \in \mathbb{R}$ and $k \in \mathbb{N}$. Suppose f is a polynomial of degree k with leading coefficient α. Then

$$\left|\sum_{n=1}^{N} e(f(n))\right|^{2^{k-1}} \lesssim N^{2^{k-1}-k} \sum_{|d|\leq k!N^{k-1}} \min\left(N, \|d\alpha\|_{\mathbb{Z}}^{-1}\right).$$

Proof. We proceed with induction on the degree of the polynomial. The base case $k = 1$ holds by Lemma 2.2. Now assume the theorem holds for polynomials of degree $k-1$, that is, for polynomials f of degree $k-1$ with leading coefficient α,

$$\left|\sum_{n=1}^{N} e(f(n))\right|^{2^{k-2}} \lesssim N^{2^{k-2}-(k-1)} \sum_{|d|\leq (k-1)!N^{k-2}} \min\left(N, \|d\alpha\|_{\mathbb{Z}}^{-1}\right).$$

Now let f be a polynomial of degree k with leading coefficient α. Note that

$$\left|\sum_{n=1}^{N} e(f(n))\right|^2 = \left(\sum_{n_1=1}^{N} e(f(n_1))\right)\left(\sum_{n_2=1}^{N} e(-f(n_2))\right) = \sum_{n_1,n_2=1}^{N} e(f(n_1)-f(n_2)).$$

We sum over $[1,N]^2$ by summing over all diagonals $d = n_2 - n_1$, where for each d the possible range of values for $n = n_1$ are $[N_1(d), N_2(d)] \subseteq [N]$. Hence

$$\left|\sum_{n=1}^{N} e(f(n))\right|^2 = \sum_{n_1,n_2=1}^{N} e(f(n_1)-f(n_2)) = \sum_{|d|\leq N} \sum_{n=N_1(d)}^{N_2(d)} e(f(n+d)-f(n))$$

noting $f(n+d)-f(n)$ is a polynomial of degree $k-1$ with leading coefficient $kd\alpha$. Applying the Cauchy-Schwarz inequality $k-2$ times and the inductive hypothesis gives

$$\begin{aligned}
\left|\sum_{n=1}^{N} e(f(n))\right|^{2^{k-1}} &\leq N^{2^{k-2}-1}\left(\sum_{|d|\leq N}\left|\sum_{n=N_1(d)}^{N_2(d)} e(f(n+d)-f(n))\right|^{2^{k-2}}\right) \\
&\lesssim N^{2^{k-2}-1}\left(\sum_{|d|\leq N} N^{2^{k-2}-(k-1)} \sum_{|d|\leq (k-1)!N^{k-2}} \min\left(N, \|kd\alpha\|_{\mathbb{Z}}^{-1}\right)\right) \\
&= N^{2^{k-1}-k}\left(\sum_{|d|\leq (k-1)!N^{k-1}} \min\left(N, \|kd\alpha\|_{\mathbb{Z}}^{-1}\right)\right) \\
&= N^{2^{k-1}-k}\left(\sum_{|d|\leq k!N^{k-1}} \min\left(N, \|d\alpha\|_{\mathbb{Z}}^{-1}\right)\right),
\end{aligned}$$

which completes the induction. □

The following corollary is proved in [Nat13]

Corollary 2.4. Let $a \perp q, k \geq 2$.

$$S(q,a) = \sum_{r=1}^{q} e(ar^k/q) \lesssim q^{1-1/K+\varepsilon}.$$

The following lemma, concerning integrals of exponential sums, will also be useful.

Theorem 2.5 (Hua's Lemma)**.** Let

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

Then for any fixed $\varepsilon > 0$,

$$\int_0^1 |T(\alpha)|^{2^j}\, d\alpha \lesssim N^{2^j - j + \varepsilon}.$$

Proof. Fix $\varepsilon > 0$. We proceed by induction on j. When $j = 1$, the induction becomes

$$\begin{aligned}\int_0^1 |T(\alpha)|^2\, d\alpha &= \int_0^1 T(\alpha)T(-\alpha)\, d\alpha \\ &= \int_0^1 \sum_{n_1,n_2=1}^{N} e\left(\alpha\left(n_1^k - n_2^k\right)\right) d\alpha = N \lesssim N^{1+\varepsilon}.\end{aligned}$$

Now assume the statement holds for some $j < k$, that is,

$$\int_0^1 |T(\alpha)|^{2^j}\, d\alpha \lesssim N^{2^j - j + \varepsilon}.$$

Using the differencing technique as in the proof of Weyl's inequality, we find

$$|T(\alpha)|^{2^j} \leq (2n)^{2^j - j - 1} \sum_{|d_1| \leq N} \cdots \sum_{|d_j| \leq N} \sum_{n = N_1(d_1,\ldots,d_j)}^{N_2(d_1,\ldots,d_j)} e(p(n)),$$

where $p(n)$ is a polynomial of degree $k - j$ with leading coefficient $k \cdots (k-j+1) \cdot d_1 \cdots d_j \alpha$. Hence

$$\begin{aligned}\int_0^1 |T(\alpha)|^{2^{j+1}}\, d\alpha &= \int_0^1 T(\alpha)^{2^{J-1}} T(-\alpha)^{2^{J-1}} |T(\alpha)|^{2^j}\, d\alpha \\ &= (2N)^{2^j - j - 1} \\ &\quad \times \sum_{|d_1| \leq N} \cdots \sum_{|d_j| \leq N} \sum_{n = N_1(d_1,\ldots,d_j)}^{N_2(d_1,\ldots,d_j)} \int_0^1 T(\alpha)^{2^{j-1}} T(-\alpha)^{2^{j-1}} e(p(n))\, d\alpha.\end{aligned}$$

Because $1 \leq N_1, N_2 \leq N$, the sum is bounded above by the number of solutions of

$$\sum_{i=1}^{2^{j-1}} \left(u_i^k - v_i^k\right) = \frac{p(n)}{\alpha}$$

where $1 \le u_i, v_i \le N$. An analysis (which we have omitted) shows that the number of solutions is $\le N^{2^j+\varepsilon}$; hence the estimate becomes

$$\int_0^1 |T(\alpha)|^{2^{j+1}}\, d\alpha \le (2N)^{2^j-j-1} \cdot N^{2^j+\varepsilon} \lesssim N^{2^{j+1}-(j+1)+\varepsilon},$$

completing the induction. □

Another useful basic fact of calculus is:

Fact 2.6. For any $m, n \in \mathbb{N}$,

$$\int_0^1 e(tm)e(tn)dt = \begin{cases} 1 & m = -n \\ 0 & \text{else.} \end{cases}$$

Now we present some more general tools for estimating sums. The following lemma is often useful for estimating "convolutions against exponential functions". In particular, one should think of $u(m)$ as being an exponential function. The machinery developed above is well-suited for analyzing $U(x) = \sum_{m \le x} u(m)$. The following lemma, an analogue of integration by parts, lets us trade a complicated sum involving $u(m)$ for a nicer expression involving $U(x)$.

Lemma 2.7 (Abel's identity)**.** Let $U(x) = \sum_{m \le x} u(m)$, and assume g has a continuous derivative on the interval $[a, b]$. Then

$$\sum_{m=a+1}^{b} u(m)g(m) = U(b)g(b) - U(a)g(a) - \int_a^b U(x)g'(x)dx$$

Proof sketch. The following discrete version of the lemma is immediate: For any sequences f_k, g_k we have

$$\sum_{k=a}^{b} f_k(g_{k+1} - g_k) + \sum_{k=a}^{b} g_{k+1}(f_{k+1} - f_k) = f_{b+1}g_{b+1} - f_a g_a.$$

This can be extended to the continuous version of the lemma using standard techniques in calculus; we omit the proof, see [Nat13] for a proof. □

Finally, a trivial but extremely useful fact is:

Fact 2.8 (Triangle Inequality)**.** $\left|\int_a^b f dt\right| \le \int_a^b |f|\, dt$.

Fact 2.9 (Dirichlet's Approximation Theorem.)**.** Let $\alpha \in \mathbb{R}$. Then for all $Q \ge 1$, there exists some $a/q \in \mathbb{Q}$, $(a, q) = 1$, and $1 \le q \le Q$ such that $|\alpha - a/q| \le 1/(qQ)$.

Proof. Consider the residues $\{q\alpha \bmod 1\}_{q=1}^{Q}$ and the integers $\{\lfloor q\alpha \rfloor\}_{q=1}^{Q}$. The pigeonhole principle implies that there exist two distinct $q_1, q_2 \in \{1, \dots, Q\}$ such that

$$|(q_1\alpha - q_2\alpha) \bmod 1| < \frac{1}{Q}.$$

But

$$(q_1\alpha - q_2\alpha) \bmod 1 = (q_1 - q_2)\alpha - (\lfloor q_1\alpha \rfloor - \lfloor q_2\alpha \rfloor),$$

so combining the two previous equations implies

$$\left|\alpha - \frac{\lfloor q_1\alpha \rfloor - \lfloor q_2\alpha \rfloor}{q_1 - q_2}\right| < \frac{1}{Q(q_1 - q_2)}.$$

Choosing $a = \lfloor q_1\alpha \rfloor - \lfloor q_2\alpha \rfloor$ and $q = q_1 - q_2$ gives the desired result. □

3 The Circle Method

Now we show how to formulate the problem of determining $r_{k,s}(N)$ analytically, so that we can apply the powerful tools developed in Section 2. Define $P = \lceil N^{1/k} \rceil$ and

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

The polynomial $F(\alpha)^s$ is a sum of many terms of the form $e(\alpha(n_1^k + \cdots + n_s^k))$. The quantity $r_{k,s}(N)$ is precisely the coefficient of $e(\alpha N)$ in this sum. We can extract this using the orthogonality relations for exponential functions described in Fact 2.6:

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

We cannot hope to actually compute this integral. Instead we will use our tools for understanding exponential sums to get precise asymptotics for this integral. The crux of the circle method is the decision to decompose the integral into contributions from ***major arcs*** and ***minor arcs***. For $q \in [P^{0.01}]$, $a \in [q], a \perp q$ define

$$\mathfrak{M}(q,a) = \left\{ \alpha \in [0,1] \;\middle|\; |\alpha - a/q| \leq 1/P^{k-0.01} \right\},$$

$$\mathfrak{M} = \bigcup_{q \leq P^v} \bigcup_{a \in [q], a \perp q} \mathfrak{M}(q,a).$$

We call $\mathfrak{M}$ the major ars. The minor arcs are the left over parts of $[0,1]$:

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

We remark that the major arcs have small total measure, but will end up contributing the leading term to $r_{k,s}(N)$.

4 Minor Arcs

We start by bounding the minor arcs. The minor arcs turn out to contribute only a low-order term to $r_{k,s}(N)$. Informally this is because the exponential sum $F(\alpha)$ is small when α is far from being a fraction with small denominator. The following theorem formalizes this intuition.

Theorem 4.1.

$$\int_{\mathfrak{m}} F(\alpha)^s e(-\alpha N) d\alpha < o(N^{s/k-1}).$$

Proof. For any $\alpha \in [0,1]$ by Dirichlet's approximation theorem (Fact 2.9) there exists integer $q \in [P^{k-0.01}]$ and $a \in [q], a \perp q$ such that

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{q P^{k-0.01}}.$$

Because $\alpha \in \mathfrak{m}$ we must have $a \neq 0$. Also we must have $q > P^{0.01}$. Applying Weyl's Inequality (Theorem 2.3) gives:

$$F(\alpha) \lesssim P^{1+\varepsilon-0.01/2^k}.$$

Now applying Hua's Lemma (Theorem 2.5) and the triangle inequality gives:

$$\begin{aligned}\int_{\mathfrak{m}} F(\alpha)^s e(-\alpha N) d\alpha &\leq \sup_{\alpha \in \mathfrak{m}} |F(\alpha)|^{s-2^k} \cdot \int_0^1 |F(\alpha)|^{2^k} d\alpha \\ &< o(N^{s/k-1}).\end{aligned}$$

□

5 Major Arcs

Define

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

$$S(q,a) = \sum_{r=1}^{q} e(ar^k/q).$$

We will show that if α is in the major arc $\mathfrak{M}(q,a)$ then $F(\alpha)$ is $v(\alpha - a/q) \cdot S(q,a)/q$ plus a small error term. Eventually we want to show that the contribution of the Major arcs to the integral constitutes the highest order term. To start we estimate v, S.

Proposition 5.1. $S(q,a)/q \lesssim q^{-1/K+\varepsilon}$ and if $|\beta| \leq 1/2$ then $v(\beta) \lesssim \min(P, |\beta|^{-1/k})$.

Proof. In Corollary 2.4 we have already shown $S(q,a)/q \lesssim q^{-1/K+\varepsilon}$. By the triangle inequality we have

$$v(\beta) \leq N \cdot N^{1/k-1} \lesssim P.$$

If $|\beta| \leq 1/N$ then $P \lesssim |\beta|^{-1/k}$. All that remains to be shown is that if $|\beta| > 1/N$ then $v(\beta) \lesssim |\beta|^{-1/k}$. Let $M = \lfloor |\beta^{-1}| \rfloor$. Then $M \leq 1/|\beta| < M+1 \leq N$.

Now we use the telescoping decomposition (Lemma 2.7). Let $f(t)$ denote the first term: $\frac{1}{k} t^{1/k-1}$. Let $u(t) = e(\beta t)$ and let $U(t) = \sum_{m \leq t} e(\beta m)$. By our bound on exponential sums with linear phases (Lemma 2.2) we know $|U(t)| \lesssim |\beta|^{-1}$. Using the triangle inequality in Lemma 2.7 gives

$$\sum_{m=M+1}^{N} f(m)u(m) \lesssim |\beta|^{-1/k}. \tag{1}$$

We do the trivial bound for the first M terms:

$$\sum_{m=1}^{M} f(m)u(m) \leq \max_{m \in [M]} |f(m)u(m)| \lesssim M^{1/k} \lesssim |\beta|^{-1/k}.$$

Combined with (1) this gives the desired bound:

$$v(\beta) = \sum_{m=1}^{N} f(m)u(m) \lesssim |\beta|^{-1/k}.$$

□

Theorem 5.2. Let $\alpha \in \mathfrak{M}(q,a)$ with $q \in [P^{0.01}], a \in [q], a \perp q$. Then,

$$|F(\alpha) - [S(q,a)/q] \cdot v(\alpha - a/q)| \leq O(P^{0.02}).$$

Proof. Define $\beta = \alpha - a/q$. Our goal is to show that the following difference is small:

$$\begin{aligned} F(\alpha) - \frac{S(q,a)}{q} v(\beta) &= \sum_{m=1}^{P} e(\alpha m^k) - \frac{S(q,a)}{q} \sum_{m=1}^{N} \frac{1}{k} m^{1/k-1} e(\beta m) \\ &= \sum_{m=1}^{P} e(m^k(\alpha - a/q)) e(m^k a/q) - \frac{S(q,a)}{q} \sum_{m=1}^{N} \frac{1}{k} m^{1/k-1} e(\beta m) \\ &= \sum_{m=1}^{N} u(m) e(\beta m), \end{aligned} \tag{2}$$

where

$$u(m) = \begin{cases} e(am/q) - (S(q,a)/q) k^{-1} m^{1/k-1} & m \text{ is a } k\text{-th power} \\ -(S(q,a)/q) k^{-1} m^{1/k-1} & \text{else.} \end{cases}$$

This decomposition is productive because the sums $U(t) = \sum_{m \leq t} u(m)$ are well controlled, and because the "convolution" of (2) can be controlled with the telescoping technique (Lemma 2.7).

Now we show that $U(t)$ is controlled. First, observe that for any y,

$$\begin{aligned} \sum_{m=1}^{y} e(am^k/q) &= \sum_{r=1}^{q} e(ar^k/q) \left|\{m \in [y] \mid m \equiv r \mod q\}\right| \\ &= S(q,a) \cdot (y/q + O(1)) \\ &= yS(q,a)/q + O(q). \end{aligned}$$

Thus,

$$\begin{aligned} U(t) &= \sum_{m \leq t^{1/k}} e(am^k/q) - \frac{S(q,a)}{q} \sum_{m \leq t} \frac{1}{k} m^{1/k-1} \\ &= t^{1/k} \frac{S(q,a)}{q} + O(q) - \frac{S(q,a)}{q}(t^{1/k} + O(1)) \\ &= O(q). \end{aligned}$$

Now using this bound on $U(t)$ we apply Lemma 2.7 to (2):

$$\begin{aligned} \left|\sum_{m=1}^{N} u(m) e(\beta m)\right| &\leq |e(\beta N) U(N)| + \left|2\pi i \beta \int_1^N e(\beta t) U(t) dt\right| \\ &\lesssim q + |\beta| \int_1^N q dt \\ &\lesssim q + |\beta| N q. \end{aligned} \tag{3}$$

Finally, because $\alpha \in \mathfrak{M}(q,a)$ we have $\beta \leq 1/P^{k-0.01} = P^{0.01}/N$. Using this in (3) gives:

$$\left|F(\alpha) - \frac{S(q,a)}{q} v(\beta)\right| \lesssim P^{0.02}.$$

□

Now we use the form of $F(\alpha)$ determined in Theorem 5.2 to bound the integral of $F(\alpha)^s e(-N\alpha)$ over the major arcs. We have:

Theorem 5.3. Let

$$\mathfrak{S}(N,Q) = \sum_{q \le Q} \sum_{a \in [q], a \perp q} (S(q,a)/q)^s e(-Na/q),$$

and

$$J^*(N) = \int_{-P^{0.01-k}}^{P^{v-k}} v(\beta)^s e(-N\beta) d\beta.$$

Then

$$\left| \int_{\mathfrak{M}} F(\alpha)^s e(-N\alpha)\ d\alpha - \mathfrak{S}(N, P^{0.01}) J^*(N) \right| \le o(N^{s/k-1}).$$

Proof. Let $\alpha \in \mathfrak{M}(q,a)$ and define $\beta = \alpha - a/q$. Let

$$V = V(\alpha, q, a) = (S(q,a)/q) v(\beta).$$

Trivially $|S(q,a)| \le q$ so $|V| \lesssim |v(\beta)| \lesssim P$ by Proposition 5.1. Let $F = F(\alpha)$; Trivially $|F| \le P$. By Theorem 5.2 we have $|F - V| \le \mathcal{O}(P^{0.02})$. Thus,

$$|F^s - V^s| = |(F-V)(F^{s-1} + F^{s-2}V + \cdots V^{s-1})| \lesssim P^{s-1+0.02}.$$

Observe that

$$\mu(\mathfrak{M}) \le P^{0.02} \mu(\mathfrak{M}(q,a)) \le P^{0.02}/P^{k-0.01}.$$

Thus,

$$\int_{\mathfrak{M}} |F^s - V^s|\, d\alpha \lesssim \mu(\mathfrak{M}) \cdot P^{s-1+0.02} \lesssim P^{s-k-1+0.05} < o(N^{s/k-1}).$$

Now we use this to bound the desired integral:

$$\begin{aligned} \int_{\mathfrak{M}} F(\alpha)^s e(-N\alpha)\ d\alpha &= \int_{\mathfrak{M}} V(\alpha,q,a)^s e(-N\alpha)\ d\alpha \pm o(N^{s/k-1}) \\ &= \sum_{q \le P^{0.01}} \sum_{a \in [q], a \perp q} \int_{\mathfrak{M}(q,a)} V(\alpha,q,a)^s e(-N\alpha)\ d\alpha \pm o(N^{s/k-1}). \end{aligned}$$

Now we manipulate the main term to be of the form claimed in the theorem. For $q \ge 2$, we have

$$\begin{aligned} \int_{\mathfrak{M}(q,a)} V(\alpha,q,a)^s e(-N\alpha)\ d\alpha &= \int_{a/q - P^{0.01-k}}^{a/q + P^{0.01-k}} V(\alpha,q,a)^s e(-N\alpha)\ d\alpha \\ &= \int_{-P^{0.01-k}}^{P^{0.01-k}} V(\beta + a/q, q, a)^s e(-N(\beta + a/q))\ d\beta \\ &= (S(q,a)/q)^s e(-Na/q) \int_{-P^{0.01-k}}^{P^{0.01-k}} v(\beta)^s e(-N\beta)\ d\beta \\ &= (S(q,a)/q)^s e(-Na/q) J^*(N). \end{aligned}$$

For $q = 1$ there are only two arcs $\mathfrak{M}(1,0)$ and $\mathfrak{M}(1,1)$. Their total contribution is $J^*(N)$. Combining our bounds on the integral over each arc $\mathfrak{M}(q,a)$ gives:

$$\begin{aligned}\int_{\mathfrak{M}} F(\alpha)^s e(-N\alpha)\ d\alpha &= \sum_{q \le P^{0.01}} \sum_{a \in [q], a \perp q} (S(q,a)/q)^s e(-Na/q) J^*(N) \pm o(N^{s/k-1}) \\ &= \mathfrak{S}(N, P^{0.01}) J^*(N) \pm o(N^{s/k-1}).\end{aligned}$$

□

5.1 Singular Integral

We are interested in controlling the contribution of $J^*(N)$ to the main order term. Recall that

$$J^*(N) := \int_{-P^{0.01-k}}^{P^{0.01-k}} v(\beta)^s e(-N\beta)\ d\beta\,.$$

Recall from Proposition 5.1 that $v(\beta) \lesssim \beta^{-1/k}$, so that the expression $v(\beta)e(-N\beta)$ becomes negligibly small for large β. In fact, it turns out that expanding the range of integration to a constant length changes the value of the integral only negligibly. Let us introduce the following integral.

Definition 5.4. The integral

$$J(N) = \int_{-1/2}^{1/2} v(\beta)^s e(-\beta N)\ d\beta$$

is called the *singular integral* for the Waring's problem.

As we discussed, we expect $J(N) \approx J^*(N)$ since the contribution of $|\beta| > P^{0.01-k}$ should be small compared to $J^*(N)$. Indeed, we have the following lemma.

Lemma 5.5.

$$|J^*(N) - J(N)| < o(N^{s/k-1}).$$

Proof. We have

$$\begin{aligned}|J(N) - J^*(N)| &= \left| \int_{P^{0.01-k} \le |\beta| \le 1/2} v(\beta)^s e(-N\beta)\ d\beta \right| \\ &\lesssim \int_{P^{0.01-k}}^{1/2} |v(\beta)^s|\, d\beta \\ &\lesssim \int_{P^{0.01-k}}^{1/2} \beta^{-s/k}\ d\beta \\ &\lesssim P^{(k-0.01)(s/k-1)} \\ &< o(N^{s/k-1}).\end{aligned}$$

□

We will need the following lemma.

Lemma 5.6. Let α and β be real numbers such that $0 < \beta < 1$ and $\alpha \geq \beta$. Then

$$\sum_{m=1}^{N-1} m^{\beta-1}(N-m)^{\alpha-1} = N^{\alpha+\beta-1}\frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)} + O_\beta(N^{\alpha-1})$$

where the implied constant in $O_\beta(\cdot)$ depends only on β (and Γ denotes the usual Γ function).

Proof. For large N it is natural to try to bound the sum on the left side by an integral, i.e. trying to establish bounds of the form

$$\sum_{m=1}^{N-1} m^{\beta-1}(N-m)^{\alpha-1} \approx \int_0^N x^{\beta-1}(N-x)^{\alpha-1}\ dx.$$

Indeed, the main term on the right is precisely the value of this integral. Let

$$g(x) = m^{\beta-1}(N-m)^{\alpha-1}$$

which is positive and continuous on $(0, N)$. Then

$$\begin{aligned}
\int_0^N g(x)\ dx &= \int_0^N x^{\beta-1}(N-x)^{\alpha-1}\ dx \\
&= N^{\alpha+\beta-1}\int_0^1 t^{\beta-1}(t-t)^{\alpha-1}\ dt \\
&= N^{\alpha+\beta-1}B(\alpha,\beta) \\
&= N^{\alpha+\beta-1}\frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}
\end{aligned}$$

where $B(\alpha,\beta)$ is the Beta function.

Notice that

$$g'(x) = g(x)\left(\frac{\beta-1}{x} - \frac{\alpha-1}{N-x}\right).$$

Now if $\alpha \geq 1$, then $g'(x) < 0$, so g is decreasing and thus

$$\int_1^N g(x)\ dx \leq \sum_{m=1}^{N-1} g(x) \leq \int_0^{N-1} g(x)\ dx\,.$$

We now simply bound

$$\begin{aligned}
0 &< \int_0^N g(x)dx - \sum_{m=1}^{N-1} g(m) \\
&< \int_0^1 g(x)\ dx \\
&= \int_0^1 x^{\beta-1}(N-x)^{\alpha-1}\ dx \\
&\leq N^{\alpha-1}\int_0^1 x^{\beta-1}\ dx \\
&= \frac{N^{\alpha-1}}{\beta} \\
&= O(N^{\alpha-1}) \qquad (4)
\end{aligned}$$

as desired. So let's assume now $0 \leq \alpha < 1$. Now $\alpha + \beta < 2$ and g has a local minimum at

$$c = \frac{(1-\beta)N}{2-\alpha-\beta} \in [N/2, N)$$

(by inspecting $g'(x)$). Moreover, $g(x)$ is strictly decreasing on $(0, c]$ and strictly increasing on $[c, n)$, so we can repeat the bound similar to (4) separately on these intervals and add them up. For $(0, c]$ (where g is decreasing), we have

$$\sum_{m=1}^{\lfloor c \rfloor} g(m) < \int_0^c g(x)\ dx$$

and

$$\begin{aligned}\sum_{m=1}^{\lfloor c \rfloor} g(m) &\geq \int_1^{[c]} g(x)\ dx + g([c]) \\ &> \int_1^c g(x)\ dx \\ &> \int_0^c g(x)\ dx - \frac{N^{\alpha-1}}{\beta}\end{aligned}$$

where we used $\int_0^1 g(x)\ dx < \frac{N^{\alpha-1}}{\beta}$ from (4).

Similarly, for $[c, N)$ where g is increasing it follows that

$$\sum_{m=[c]+1}^{N-1} g(m) < \int_c^N g(x)\ dx$$

and

$$\begin{aligned}\sum_{m=[c]+1}^{N-1} g(m) &\geq \int_{[c]+1}^{N-1} g(x)\ dx + g([c]+1) \\ &> \int_c^{N-1} g(x)\ dx \\ &> \int_c^N g(x)\ dx - \frac{N^{\beta-1}}{\alpha}\end{aligned}$$

where we used the bound $\int_{N-1}^N g(x)\ dx < \frac{N^{\beta-1}}{\alpha}$ which is obtained identically to $\int_0^1 g(x)\ dx < \frac{N^{\alpha-1}}{\beta}$ after reversing the direction $x \to N - x$ and swapping α and β.

All in all we have

$$0 < \int_0^N g(x)\ dx - \sum_{m=1}^{N-1} < \frac{N^{\alpha-1}}{\beta} + \frac{N^{\beta-1}}{\alpha} \leq \frac{2N^{\alpha-1}}{\beta}$$

which finishes the proof.

□

Armed with this technical result, we can prove the main result of this section.

Theorem 5.7. If $s \geq 2$, then

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

Proof. Let us make the dependence of J on s explicit and denote

$$J(N) = J_s(N) = \int_{-1/2}^{1/2} v(\beta)^s e(-N\beta)\, d\beta$$

for $s \geq 1$. We will now compute this integral by induction on s. Recall that

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

so that

$$v(\beta)^2 = k^{-2} \sum_{m_1=1}^{N} \sum_{m_2=1}^{N} (m_1 m_2)^{1/k-1} e\big((m_1+\cdots+m_s)\beta\big)$$

so that

$$\begin{aligned} J_2(N) &= k^{-2} \sum_{m_1=1}^{N} \sum_{m_2=1}^{N} (m_1 m_2)^{1/k-1} \int_{-1/2}^{1/2} e\big((m_1+\cdots+m_s-N)\beta\big)\, d\beta \\ &= k^{-2} \sum_{\substack{m_1+m_2=N \\ 1\leq m_1,m_2\leq N}} (m_1 m_2)^{1/k-1} \\ &= k^{-2} \sum_{x=1}^{N-1} x^{1/k-1}(N-x)^{1/k-1}. \end{aligned}$$

Thus we can apply Lemma 5.6 with $\alpha = \beta = 1/k$ and obtain

$$\begin{aligned} J_2(N) &= k^{-2} \sum_{x=1}^{N-1} x^{1/k-1}(N-x)^{1/k-1} \\ &= \frac{\Gamma(1/k)^2}{k^2\Gamma(2/k)} N^{2/k-1} + O(N^{1/k-1}) \\ &= \frac{\Gamma(1+1/k)^2}{\Gamma(2/k)} N^{2/k-1} + O(N^{1/k-1}) \end{aligned}$$

which establishes the base case of induction ($s = 2$).

Now assume $s \geq 2$ and the result holds for s. We have

$$\begin{aligned}
J_{s+1}(N) &= \int_{-1/2}^{1/2} v(\beta)^{s+1} e(-N\beta)\ d\beta \\
&= \int_{-1/2}^{1/2} v(\beta) v(\beta)^{s} e(-N\beta)\ d\beta \\
&= \int_{-1/2}^{1/2} \sum_{m=1}^{N} \frac{1}{k} m^{1/k-1} e(\beta m) v(\beta)^{s} e(-N\beta)\ d\beta \\
&= \sum_{m=1}^{N} \frac{1}{k} m^{1/k-1} \int_{-1/2}^{1/2} v(\beta)^{s} e\big(-(N-m)\beta\big)\ d\beta \\
&= \sum_{m=1}^{N} \frac{1}{k} m^{1/k-1} J_s(N-m) \\
&= \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} \sum_{m=1}^{N-1} \frac{1}{k} m^{1/k-1} (N-m)^{s/k-1} \\
&\quad + O\left(\sum_{m=1}^{N-1} \frac{1}{k} m^{1/k-1} (N-m)^{(s-1)/k-1} \right). \qquad (5)
\end{aligned}$$

We can now apply Lemma 5.6 again twice: to the main term (with $\alpha = s/k$ and $\beta = 1/k$) and to the error term (with $\alpha = (s-1)/k$ and $\beta = 1/k$) to obtain

$$\sum_{m=1}^{N-1} \frac{1}{k} m^{1/k-1} (N-m)^{s/k-1} = \frac{\Gamma(1/k)\Gamma(s/k)}{k\Gamma((s+1)/k)} N^{(s+1)/k-1} + O(N^{s/k-1})$$

(for the main term) and

$$\sum_{m=1}^{N-1} \frac{1}{k} m^{1/k-1} (N-m)^{(s-1)/k-1} = O(N^{s/k-1}).$$

Combining this with (5) gives

$$\begin{aligned}
J_{s+1}(N) &= \frac{\Gamma(1/k)\Gamma(s/k)}{k\Gamma((s+1)/k)} \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} N^{(s+1)/k-1} + O(N^{s/k-1}) \\
&= \frac{\Gamma(1+1/k)^{s+1}}{\Gamma((s+1)/k)} N^{(s+1)/k-1} + O(N^{s/k-1})
\end{aligned}$$

(where the implicit constants depend on k and s). This finishes the inductive step. □

Corollary 5.8.

$$J^*(N) = \Gamma\left(1+\frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} N^{s/k-1} \pm o(N^{s/k-1}).$$

Proof. By Lemma 5.5 we know that $J(N), J^*(N)$ differ by a most $o(N^{s/k-1})$. In Theorem 5.7 we have computed a formula for $J(N)$. Combining these results gives the desired formula for $J^*(N)$. □

5.2 Singular Series

Now that we have computed the singular integral it remains to compute $\mathfrak{S}(N, P^{0.01})$ and then we will understand the leading term behavior of $r_{k,s}(N)$. Define

$$A_N(q) = \sum_{a \in [q], a \perp q} (S(q,a)/q)^s e(-Na/q),$$

and also define the ***singular series***

$$\mathfrak{S}(N) = \sum_{q \geq 1} A_N(q).$$

We claim that $\mathfrak{S}(N)$ is a good estimate for $\mathfrak{S}(N, P^{0.01})$. Recall that in Proposition 5.1 we showed (via Weyl's inequality) that for any $\varepsilon > 0$:

$$S(q,a)/q \lesssim q^{-1/K+\varepsilon},$$

where the implied constant depends on ε, K. Thus,

$$A_N(q) \lesssim q \cdot q^{-s/K+s\varepsilon}.$$

Recall that we are considering $s \geq 2K+1$. Thus, for some constant $\eta > 0$ we have

$$A_N(q) \lesssim 1/q^{1+\eta}. \tag{6}$$

Thus, $\mathfrak{S}(N)$ converges absolutely, and also $\mathfrak{S}(N) \leq \mathcal{O}(1)$. We now deduce:

$$\begin{aligned} \mathfrak{S}(N) - \mathfrak{S}(N, P^{0.01}) &= \sum_{q > P^{0.01}} A_N(q) && (7)\\ &\lesssim \sum_{q > P^{0.01}} 1/q^{1+\eta} && (8)\\ &\lesssim P^{-0.01\eta}. && (9) \end{aligned}$$

To conclude the analysis we will show that $\mathfrak{S}(N)$ is a positive constant dependent only on k, s. By our analysis of $\mathfrak{S}(N) - \mathfrak{S}(N, P^{0.01})$ this will imply that $\mathfrak{S}(N, P^{0.01})$ is a positive constant as well.

It is straightforward to show that A_N is multiplicative, i.e.,

Lemma 5.9. If $q \perp r$ then $A_N(qr) = A_N(q)A_N(r)$.

Proof. First we show that

$$S(qr, ar+bq) = S(q,a)S(r,b). \tag{10}$$

Any number $m \in [qr]$ can be expressed uniquely as $xr + yq$ for $x \in [q]$ and $y \in [r]$. Thus, utilizing the fact that $e(z) = 1$ for any integer z we have

$$\begin{aligned} S(qr, ar+bq) &= \sum_{x \in [q], y \in [r]} e\left(\frac{(ar+bq)(xr+yq)^k}{qr}\right) && (11)\\ &= \sum_{x=1}^{q} e(a(xr)^k/q) \sum_{y=1}^{r} e(b(yq)^k/r). && (12) \end{aligned}$$

But of course $\{(xr)^k \mod q \mid x \in [q]\} = \{x^k \mid x \in [q]\}$ and $\{(yq)^k \mid y \in [r]\} = \{y^k \mid y \in [r]\}$, so (12) is equal to $S(q,a)S(r,b)$.

Now, observe that if $c \perp q$ then $c \equiv ar + bq \mod qr$ where $a \perp q, b \perp r$. Using this to re-parameterize the sum in the definition of $A_N(qr)$ gives

$$A_N(qr) = \sum_{a \in [q], a \perp q} \sum_{b \in [r], b \perp r} \left(\frac{S(qr, ar+bq)}{qr}\right)^s e\left(\frac{-(ar+bq)N}{qr}\right). \tag{13}$$

Using (10) in (13) we get $A_N(qr) = A_N(q)A_N(r)$. □

Define For prime p, define

$$\chi_N(p) = 1 + \sum_{h=1}^{\infty} A_N(p^h).$$

We now show that $\mathfrak{S}(N)$ can be decomposed in terms of the $\chi_N(p)$'s via the following product formula:

Lemma 5.10. $\mathfrak{S}(N) = \prod_p \chi_N(p)$.

Proof. This follows from the multiplicativity of $A_N(q)$. □

Thus, it suffices to lower bound the $\chi_N(p)$'s. For positive integer q let $M_N(q)$ denote the number of $x_1, \ldots, x_s \in [q]$ such that

$$x_1^k + \cdots + x_s^k \equiv N \mod q.$$

There is a simple formula for $\chi_N(p)$ in terms of M_N:

Lemma 5.11.

$$\chi_N(p) = \lim_{h \to \infty} \frac{M_N(p^h)}{p^{h(s-1)}}.$$

Proof. Note that $\frac{1}{q}\sum_{q \in [q]} e(am/q)$ is 1 if $m \equiv 0 \mod q$ and 0 otherwise. Thus, we can express $M_N(q)$ as

$$M_N(q) = \sum_{x_1, \ldots, x_s \in [q]} \frac{1}{q} \sum_{a=1}^{q} e\left(\frac{a(x_1^k + \cdots + x_s^k - N)}{q}\right) \tag{14}$$

$$= \frac{1}{q} \sum_{a=1}^{q} S(q,a)^s e(-aN/q) \tag{15}$$

$$= \frac{1}{q} \sum_{d \mid q} \sum_{a \in [q/d], a \perp q/d} S(q, ad)^s e(-adN/q). \tag{16}$$

It is easy to see that

$$S(qd, ad) = \sum_{r=1}^{qd} e(adr^k/(qd)) = d \sum_{r \in [q]} e(ar^k/q) = dS(q,a).$$

Using this in (16) gives:

$$M_N(q) = q^{s-1} \sum_{d|q} A_N(q/d). \tag{17}$$

Using this formula in the case of $q = p^h$ gives:

$$1 + \sum_{j=1}^{h} A_N(p^j) = \sum_{d|p^h} A_N(p^h/d) = p^{h(1-s)} M_N(p^h).$$

Thus,

$$\chi_N(p) = \lim_{h\to\infty} p^{h(1-s)} M_N(p^h).$$

□

Lemma 5.12. There exists a constant p_0 depending only on k, s such that

$$\prod_{p>p_0} \chi_N(p) \in [1/2, 3/2].$$

Proof. Using (6) we have

$$|\chi_N(p) - 1| \le \sum_{h=1}^{\infty} |A_N(p^h)| \lesssim \sum_{h=1}^{\infty} 1/p^{h(1+\eta)} \lesssim 1/p^{1+\eta}.$$

Thus, there is a constant c such that $\chi_N(p) \in [1 - c/p^{1+\eta}, 1 + c/p^{1+\eta}]$. The product $1/\zeta(s) = \prod_p (1 - p^{-s})$ is known to converge for all $s > 1$. Thus, taking sufficiently large p_0 we can make $\prod_{p>p_0}(1 \pm cp^{-1-\eta})$ as close to 1 as desired. □

Thus, to lower bound $\mathfrak{S}(N)$ it suffices to show that for each $p < p_0$, the value $\chi_N(p)$ is bounded away from 0. By Lemma 5.11 it is equivalent to show that for sufficiently large h the equation

$$x_1^k + \cdots + x_s^k \equiv N \mod p^h$$

has at least $\Omega(p^{h(s-1)})$ solutions. Notice that we have taken the Warring's problem over the integers and in a certain sense reduced it to the problem modulo prime powers! Fortunately the problem is substantially simpler modulo prime powers.

Let p be a prime and write $k = p^\tau k_0$ where $k_0 \perp p$. Define

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

Our strategy for lower bounding $\chi_N(p)$ is to demonstrate the existence of one solution and then "amplify" that solution to many solutions.

First we prove a variant of the Hensel lifting lemma discussed class:

Lemma 5.13. Let $m \perp p$. Suppose that $x^k \equiv m \mod p^\gamma$ for some integer x. Then, for any $h > \gamma$ there exists an integer y such that $y^k \equiv m \mod p^h$.

Proof. We proceed by induction. We are given the base case. We assume that for some $h > \gamma$ there is an integer x_0 such that $x_0^k \equiv m \mod p^{h-1}$. Now we aim to solve the equation modulo p^h. We consider solutions of the form $x_0 + \lambda p^{h-\tau-1}$. In order for this to be a solution we need

$$0 \mod p^h \equiv (x_0+\lambda p^{h-\tau-1})^k - m \equiv -m + x_0^k + k x_0^{k-1} \lambda p^{h-\tau-1} + \binom{k}{2} x_0^{k-2} (\lambda p^{h-\tau} - 1)^2 + \cdots .$$

Because $h \geq \gamma + 1$ and using the definition of γ (which is different for even and odd primes) we have that

$$k p^{2(h-\tau-1)} \equiv 0 \mod p^h, \quad p^{(h-\tau-1)k} \equiv 0 \mod p^h.$$

Thus, we have

$$(x_0 + \lambda p^{h-\tau-1})^k - m \equiv x_0^k - m + k x_0^{k-1} \lambda p^{h-\tau-1} \mod p^h. \tag{18}$$

We chose x_0 such that $x_0^k - m \equiv 0 \mod p^{h-1}$, thus $z = \frac{m - x_0^k}{p^{h-1}}$ is an integer. Furthermore, $\nu_p(k p^{h-\tau-1}) = h - 1$. Assume that $\nu_p(x_0^k - m) = p - 1$; if it is instead at least p then we can just use x_0 as our solution. Then, dividing (18) by p^{h-1} we have:

$$\lambda x_0^{k-1} \equiv k_0^{-1} z \mod p.$$

Finally, observe that $x_0 \perp p$ because $x_0 \equiv m \mod p$ and $m \perp p$. Hence, x_0 is also invertible and we can solve for λ. Thus, there is some λ such that $(x_0 + \lambda p^{h-\tau-1})^k \equiv m \mod p^h$, concluding the proof. □

Now we use this "lifting" lemma to amplify a single solution to many solutions.

Lemma 5.14. Suppose that there is some solution $a_1, \ldots, a_s$ to $\sum_{i=1}^s a_i^k \equiv N \mod p^\gamma$ with at least one a_i having $a_i \perp p$. Then

$$\chi_N(p) \geq 1/p^{\gamma(1-s)} > 0.$$

Proof. Without loss of generality let $a_s \perp p$. Fix $h > \gamma$. For each $i \in [s-1]$ there are $p^{h-\gamma}$ distinct choices for $x_i \mod p^h$ such that $x_i \equiv a_i \mod p^\gamma$. Fixing any such choice of x_i's we will have that

$$a_s^k \equiv N - \sum_{i=1}^{s-1} x_i^k \mod p^\gamma.$$

By assumption $a_s \perp p$. Thus, we can apply Lemma 5.13 to deduce that

$$y^k \equiv N - \sum_{i=1}^{s-1} x_i^k \mod p^h$$

also has a solution y. Thus, $M_N(p^h) \geq p^{(h-\gamma)(s-1)}$. Using this in Lemma 5.11 gives the desired bound on $\chi_N(p)$. □

Finally, we demonstrate the existence of a solution to conclude the desired lower bound on $\chi_N(p)$.

Lemma 5.15. For any p we have:

$$\chi_N(p) \geq 1/p^{\gamma(1-s)} > 0.$$

Proof. By Lemma 5.14 it suffices to demonstrate the existence of a single solution. If N is divisible by p then we set one of the variables to 1 and our new goal is to find $s-1$ k-th powers summing to $N-1$ modulo p^γ. Thus we may assume without loss of generality that $N \perp p$.

First we consider the case that $p \neq 2$. Let g be a primitive root modulo p^γ, i.e., an element with order $\phi(p^\gamma) = (p-1)p^{\gamma-1} = (p-1)p^\tau$; it is well known that primitive roots exist. Let $m = g^r$ be an arbitrary element of $(\mathbb{Z}/p^\gamma\mathbb{Z})^*$. Then, m is a k-th power mod p^γ if and only if there exists v such that

$$kv \equiv r \mod \phi(p^\gamma).$$

Recall our decomposition $k = k_0 p^\tau$. Let $d = \gcd(k_0, p-1)$. The congruence becomes

$$p^\tau d \cdot (k_0/d) \equiv r \mod dp^\tau((p-1)/d).$$

This congruence clearly has a solution if and only if $r \equiv 0 \mod p^\tau d$. Thus, the number k-th power residues modulo p^γ is

$$\frac{\phi(p^\gamma)}{dp^\tau} = (p-1)/d.$$

Let $s(N)$ denote the smallest s such that $\sum_{i=1}^s x_i^k \equiv N \mod p^\gamma$ has a solution; this is well defined because trivially $s(N) \leq N$. Let $C(j)$ denote the set of all congruence classes N modulo p^γ such that $N \perp p$ and $s(N) = j$. Observe that the sets $C(j)$ are closed under multiplication by k-th powers. Thus, if $C(j)$ is non-empty then it contains at least $(p-1)/d$ elements. Let n be the largest integer such that $C(n)$ is non-empty; this is well defined as $C(1)$ is the set of k-th powers, which is non-empty. Let $j < n$ and let N be the smallest integer such that $N \perp p$ and $s(N) > j$. Since p is odd it follows that $N - i \perp p$ for at least one of $i \in \{1, 2\}$ and that $s(N-i) \leq j$. Then, setting variables to 1 we have

$$j + 1 \leq s(N) \leq s(N-i) + 2 \leq j + 2.$$

Thus, $s(N-i) \in \{j, j-1\}$. This implies that no two consecutive sets $C(j)$ are nonempty for $j = 1, \ldots, n$, and so the number of nonempty sets $C(j)$ is at least $(n+1)/2$. Since the sets $C(j)$ are pairwise disjoint we have:

$$(p-1)p^\tau = \phi(p^\gamma) = \sum_{j \in [n], C(j) \neq \varnothing} |C(j)| \geq \frac{n+1}{2}\frac{p-1}{d}.$$

Thus,

$$n \leq 2dp^\tau - 1 \leq 2k - 1.$$

Hence $s(N) \leq 2k-1$.

Now consider the case $p = 2$. Recall that we are assuming $N \perp 2$, which was achieved by potentially setting one variable to 1. If k is odd then the k-th powers can make any odd residue, and so we have a solution. If k is even then $s \geq 2^k + 1 \geq 2^{\tau+2} - 1$. Thus, appropriately setting variables to either 0 or 1 will suffice to find a solution.

□

Corollary 5.16. $\mathfrak{S}(N, P^{0.01}) = \Theta_{s,k}(1)$.

Proof. We have shown in Lemma 5.12 that there is a constant p_0 such that $\prod_{p>p_0} \chi_N(p) \in [1/2, 3/2]$. By Lemma 5.15 we have that for all primes $p < p_0$, $\chi_N(p) \geq p^{\gamma(1-s)}$. Using (9) to relate $\mathfrak{S}(N, P^{0.01})$ to $\mathfrak{S}(N)$ and using Lemma 5.10 to relate $\mathfrak{S}(N)$ to $\prod_p \chi_N(p)$ we have:

$$\mathfrak{S}(N, P^{0.01}) \geq \mathfrak{S}(N) - o(1) \geq \prod_p \chi_N(p) > \frac{1}{2} \prod_{p<p_0} \chi_N(p) \geq \Omega(1) > 0.$$

□

5.3 Conclusion

Now we combine the analysis of major arcs and minor arcs, in particular combining our separate analyses of the singular series and singular integral to deduce the theorem:

Theorem 1.2. [Hardy-Littlewood] For any $k, s \in \mathbb{N}$ with $s \geq 2^k + 1$ we have

$$r_{k,s}(N) = \Theta(N^{s/k-1}).$$

Proof. As discussed we have

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

We decompose the integral into the major and minor arcs. For the minor arcs we have by Theorem 4.1 that

$$\int_{\mathfrak{m}} F(\alpha)^s e(-\alpha N) d\alpha < o(N^{s/k-1}).$$

For the major arcs we have by Theorem 5.3 that

$$\left| \int_{\mathfrak{M}} F(\alpha)^s e(-N\alpha)\ d\alpha - \mathfrak{S}(N, P^{0.01}) J^*(N) \right| \leq o(N^{s/k-1}).$$

By Corollary 5.8 we know $J^*(N) = \Theta_{s,k}(N^{s/k-1})$.
By Corollary 5.16 we know $\mathfrak{S}(N, P^{0.01}) = \Theta_{s,k}(1)$. Combining all these results gives

$$r_{k,s}(N) = \Theta_{s,k}(N^{s/k-1}).$$

□

References

[Gut22] Larry Guth. *Analytic Number Theory Class Notes, MIT 18.158*. Class Notes. 2022.

[Hel14] H. A. Helfgott. *The ternary Goldbach conjecture is true*. 2014. arXiv: 1312.7748 [math.NT].

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

[Vin28] M. Vinogradov. "On Waring's theorem". In: *Izv. Mat. Nauk.* (1928), pp. 393–400.

[VW02] RC Vaughan and TD Wooley. "Waring's problem: a survey". In: *Surveys in Number Theory* (2002), pp. 285–324.

[Woo23] Trevor D. Wooley. *Analytic Number Theory: Introduction to the Circle Method and Its Applications*. 2023.