The Hardy-Littlewood Formula

Johnny Chen

February 2024

1 Introduction

The Hardy-Littlewood asymptotic formula builds on the past few works of work. Waring's problem was to prove that every non-negative integer can be expressed as a sum of a bounded number of kth powers. We can let $r_{k,s}(N)$ denote the number of representations of N as the sum of s positive kth powers. Thus, we can re-express Waring's problem as

$$r_{k,s}(N) > 0.$$

for some s and for all sufficiently large N.

At its core, the Hardy-Littlewood asymptotic formula attempts to find an asymptotic formula for $r_{k,s}(N)$. We will see that while there is an explicit formula for $k = 1$, that there is no easy way to compute (or even estimate) $r_{k,s}(N)$ for $k \geq 2$. Hardy and Littlewood manage to obtain an asymptotic formula for $r_{k,s}(N)$ for all $k \geq 2$ and $s \geq s_0(k)$. In particular, I will prove the Hardy-Littlewood asymptotic formula for $s \geq 2^k + 1$. For $N \geq 2^k$, let

$$P = [N^{1/k}] \tag{I}$$

and

$$F(\alpha) = \sum_{m=1}^{P} e(\alpha m^k), \tag{II}$$

where (II) represents the generating function for representing N as the sum of kth powers. Building on what we saw in last week's talk, we can use the circle method to estimate the following integral to derive the Hardy-Littlewood asymptotic formula:

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

To find an estimate, we need to do a few steps. First, we have to decompose the interval $[0, 1]$ into two disjoint sets—-the major arc $\mathcal{M}$ and minor arcs m , where $\mathcal{M}$ is the set of all real numbers $\alpha \in [0, 1]$ that can be approximated by rational numbers, whereas the m contains the numbers $\alpha \in [0, 1]$ that can't. Then, we will compute the integral over the major arc using the "singular integral" $J(N)$ and the "singular series" $\mathfrak{G}(N)$, and use Weyl's inequality and Hua's lemme to compute the integral over the minor arcs.

Intuitive understanding of what we're doing:

Imagine we have a certain number N, and we want to see how many ways we can split it into a sum of other numbers raised to their k-th power. To do so, we use generating functions. Each part of the series here corresponds to different ways to split up the number N. When we analyze this on the complex plane, we can imagine "walking" in the unit circle. This "walk" has two parts: "major" parts, where the behavior is predictable, and "minor" parts, where it's more erratic. We can then use Cauchy's theorem to arrive at an approximation for $r_{k,s}(N)$

2 The Hardy-Littlewood Decomposition

When trying to compute integral (III), we realize that it cannot be computed explicitly in terms of elementary functions. Instead, we will approach it by decomposing the interval into two disjoint sets.

2.1 The Major Arcs

The intuition behind what we seek here is to find the set of all real numbers $\alpha \in [0,1]$ that can be "well-approximated" by rational numbers, the definition of which will be explained shortly.

Let $N \geq 2^k \Rightarrow P = [N^{1/k}] \geq 2$. Now, choose variables v, q, a such that:

$$\begin{aligned} &0 < v < \frac{1}{5} \\ &1 \leq q \leq P^v \\ &(a,q) = 1 \end{aligned}$$

Now let

$$\mathcal{M}(q,a) = \left\{ \alpha \in [0,1] \mid |\alpha - \frac{a}{q}| \leq \frac{1}{p^{k-v}} \right\}$$

and, correspondingly,

$$\mathcal{M} = \bigcup_{1 \leq q \leq P^v} \bigcup_{a=0}^{q} \mathcal{M}(q,a),$$

where $\mathcal{M}(q,a)$ is *a* major arc, and $\mathcal{M}$ is the set of *all* major arcs. We then observe that

$$\begin{aligned} \mathcal{M}(1,0) &= \left[0, \frac{1}{P^{k-v}}\right], \\ \mathcal{M}(1,1) &= \left[1 - \frac{1}{P^{k-v}}, 1\right], \end{aligned}$$

and, more generally, when $q \geq 2$

$$\mathcal{M}(q,a) = \left[\frac{a}{q} - \frac{1}{P^{k-v}}, \frac{a}{q} + \frac{1}{P^{k-v}}\right]$$

Now, the definition of "well-approximated" is clear: the major arcs consist of all real numbers $\alpha \in [0,1]$ that are within distance P^{v-k} to a rational number that has a denominator smaller than P^v. We can also show that the major arcs $\mathcal{M}(q,a)$ are all pairwise disjoint. To do so, take $\alpha \in \mathcal{M}(q,a) \cap \mathcal{M}(q',a')$, where $\frac{a}{q} \neq \frac{a'}{q'} \Rightarrow |aq' - a'q| \geq 1$. Then we have

$$\begin{aligned} \frac{1}{P^{2v}} &\leq \frac{1}{qq'} \\ &\leq \left|\frac{a}{q} - \frac{a'}{q'}\right| \\ &\leq \left|a - \frac{a}{q}\right| + \left|a - \frac{a'}{q'}\right| \\ &\leq \frac{2}{P^{k-v}}, \end{aligned}$$

which is clearly impossible whenever $P \geq 2$ and $k \geq 2$, which concludes the proof.

2.2 The Minor Arcs

Having defined the major arcs $\mathcal{M}$, the work of the minor arcs m is significantly easier. We simply define

$$m = [0,1] - \mathcal{M}$$

2.3 The Measure of the Arcs

We now take a moment to discuss the measures of the minor and major arcs. Since we have shown that the major arcs are pairwise disjoint, we can simply find the measure of $\mathcal{M}$ by summing up the individual major arcs. We note that the measure of a single major arc $\mathcal{M}$ is equivalent to the size of the interval

$$\left[\frac{a}{q} - \frac{1}{P^{k-v}}, \frac{a}{q} + \frac{1}{P^{k-v}}\right],$$

which is just

$$\frac{2}{P^{k-v}}$$

We can then find the sum of all major arcs. Since each major arc was constructed around a rational number $\frac{a}{q}$, where $(a,q) = 1$, we can use Euler's Totient Function $\phi(q)$ to count the number of possible unique fractions $\frac{a}{q}$ that form the "centers" of the major arcs. As such, we can calculate the total measure of $\mathcal{M}$ to be

$$\mu(\mathcal{M}) = \sum_{1 \le q \le P^v} \phi(q) \times \frac{2}{P^{k-v}} = \frac{2}{P^{k-v}} \sum_{1 \le q \le P^v} \phi(q)$$

Then, we can bound $\mu(\mathcal{M}$ by noting that $\phi(q)$ is at most q, and so we get

$$\mu(\mathcal{M}) = \frac{2}{P^{k-v}} \sum_{1 \le q \le P^v} \phi(q) \le \frac{2}{P^{k-v}} \sum_{1 \le q \le P^v} q$$

With some simple algebra, we can once again bound this by

$$\mu(\mathcal{M}) = \frac{2}{P^{k-v}} \sum_{1 \le q \le P^v} \phi(q) \le \frac{2}{P^{k-v}} \sum_{1 \le q \le P^v} q \le \frac{2}{P^{k-v}} \frac{P^v(P^v+1)}{2} \le \frac{2}{P^{k-3v}}$$

We can then define the measure of minor arcs to be

$$\mu(m) = 1 - \mu(\mathcal{M}) > 1 - \frac{2}{P^{k-3v}}$$

Interestingly, some of you may have noticed that as P tends to infinity, $\mu(\mathcal{M})$ tends to 0 and, as a consequence, $\mu(m)$ tends to 1. This may seem troublesome, as the minor arcs m behaves erratically, but we will show in the next section that it can be bounded relatively easily such that its contribution is negligible

3 Bounding the Minor Arc

In this section, I will show that the integral over the minor arcs is small.

Theorem 4.1: *Let $k \geq 2$ and $s \geq 2^k + 1$. Then there exists $\delta_1 > 0$ such that*

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

where the constant depends only on k and s.

To bound the minor arc, let us first recall Dirichlet's theorem:

Theorem 4.2 (Dirichlet): *Let α and Q be real numbers, $Q \geq 1$. Then there exists integers a and q where*

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

and

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

Let us take $Q = P^{k-v} \Rightarrow$ for every $\alpha \in \mathbb{R}$, there is a fraction $\frac{a}{q}$ such that

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

and

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

Thus, if $\alpha \in m$, then we necessarily have $q > P^v$. Recall this was a condition for being in the minor arc, you can visit pg. 128 for another in-depth proof that $q \in (P^v, P^{k-v}]$.

The next step involves Weyl's inequality and Hua's lemma, both illustrated here:

Weyl's inequality *Let $f(x) = \alpha x^k + \ldots$ be a polynomial of degree $k \geq 2$ with real coefficients, and suppose that α has the rational approximation α such that*

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

where $q \geq 1$ and $(a, q) = 1$. Let

$$S(f) = \sum_{n=1}^{N} e(f(n)).$$

Let $K = 2^{k-1}$ and $\varepsilon > 0$. Then

$$S(f) \ll N^{1+\varepsilon}\left(N^{-1} + q^{-1} + N^{-k}q\right)^{1/K},$$

where the implied constant depends on k and ε.

Hua's lemma *For $k \geq 2$, let*

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

Then

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

Using Weyl's inequality with $f(x) = \alpha x^k$, we have

$$\begin{aligned} F(\alpha) &\ll P^{1+\varepsilon}(P^{-1} + q^{-1} + P^{-k}q)^{1/K} \\ &\ll P^{1+\varepsilon}(P^{-1} + P^{-v} + P^{-k}P^{k-v})^{1/K} \\ &\ll P^{1+\varepsilon-v/k} \end{aligned}$$

This allows us to apply Hua's lemma with $T(\alpha) = F(\alpha)$

$$\begin{aligned} \left| \int_m F(\alpha)^s e(-N\alpha) d\alpha \right| &= \left| \int_m F(\alpha)^{s-2} F(\alpha)^2 e(-N\alpha) d\alpha \right| \\ &\leq \int_m |F(\alpha)|^{s-2} |F(\alpha)|^2 d\alpha \\ &\leq \max_{\alpha \in m} |F(\alpha)|^{s-2} \int_0^1 |F(\alpha)|^2 d\alpha \\ &\ll \left(P^{1+\varepsilon-v/K} \right)^{s-2} P^{2-\kappa+\varepsilon} \\ &= P^{s-\kappa-\delta_1}, \end{aligned}$$

where

$$\delta_1 = \frac{v(s-2\kappa)}{K} - (s-2\kappa+1)\varepsilon > 0$$

if $\varepsilon > 0$ is chosen sufficiently small. This completes the proof.

This may have seemed very confusing, but the overall logic here is that Dirichlet's Theorem gives us a way to measure how close our number α is to rational numbers with small denominators, Weyl's inequality then tells us that the sums of those numbers are small, and Hua's Lemma confirms that the negligible contribution is true for the entire integral.

4 The Major Arc

Now that we have established the negligible contribution of the minor arcs, we turn to estimate the integral along the major arcs. It turns out that the integral can be expressed roughly as the product of two components: the singular series $\mathfrak{G}(N, Q)$ and the singular integral $J^*(N)$. The full proof is highly technical, so I will only introduce the important definitions and state the lemmas. If you wish, the full proof is in pages 129-133 in the textbook.

We first introduce some auxiliary functions

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

and

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

From this, we will show that if α lies in the major arc $\mathcal{M}(q,a)$, then $F(\alpha)$ is the product of $S(q,a)/q$ and $v(\alpha - a/q)$ with a small error term.

We know that $S(q,a) \leq q$. Using Weyl's inequality again, we have

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

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

We now illustrate 2 lemmas that will allow us to complete the proof:

Lemma 4.1: *If $|\beta| \leq 1/2$, then*

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

Lemma 4.2: *Let q and a be integers such that $1 \leq q \leq P^v$, and $0 \leq a \leq q$, and $(a,q) = 1$. If $\alpha \in \mathcal{M}(q,a)$, then*

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

Theorem 4.3 *Let*

$$\mathfrak{G}(N,Q) = \sum_{1 \leq q \leq Q} \sum_{\substack{a \bmod q \\ (a,q)=1}} \left(\frac{S(q,a)}{q}\right)^s e\left(-\frac{Na}{q}\right)$$

and

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

Let $\mathcal{M}$ denote the set of major arcs. Then

$$\int_{\mathcal{M}} F(\alpha)^s e(-N\alpha) d\alpha = \mathfrak{G}(N,P) J^*(N) + O(P^{s-k-\delta_2}),$$

where $\delta_2 = (1-5v)/k > 0$.

Proof of Theorem 4.3 Let $\alpha \in \mathcal{M}(q,a)$ and $\beta = \alpha - \frac{a}{q}$.

Let

$$V = V(\alpha, q, a) = \frac{S(q,a)}{q}\left(v(\alpha - \frac{a}{q}) - v(\alpha)\right) = \frac{S(q,a)}{q} v(\beta).$$

Since $|S(q,a)| \leq q$, we have $|V| \ll kv(\beta)$ by Lemma 4.1. Let $F = F^*(\alpha)$. Then $|F| \leq P$. Since $F - v = O(P^{2v})$ by Lemma 4.2, it follows that

$$F^s - V^s = (F - V)(F^{s-1} + F^{s-2}V + \cdots + V^{s-1})$$

$$\ll P^{2v} P^{s-1} = P^{s-1+2v}.$$

Since $\mu(\mathcal{M}) < P^{3v-k}$, it follows that

$$\int_{\mathcal{M}} |F^s - V^s| d\alpha \ll P^{3v-k} P^{s-1+2v} = P^{s-k-\delta_2},$$

where $\delta_2 = 1 - 5v > 0$.

Therefore,

$$\begin{aligned}
&\int_{\mathcal{M}} F(\alpha)^s e(-N\alpha)d\alpha \\
&= \int_{\mathcal{M}} V(\alpha,q,a)e(-N\alpha)d\alpha + O(P^{s-k-\delta_2}) \\
&= \sum_{1\le q\le P^v} \sum_{\substack{a \bmod q \\ (a,q)=1}} \int_{\mathcal{M}(q,a)} V(\alpha,q,a)e(-N\alpha)d\alpha + O(P^{s-k-\delta_2}).
\end{aligned}$$

For $q \geq 2$, we have

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

For $q = 1$ we have $V(\alpha,1,0) = v(\alpha)$ and $V(\alpha,1,1) = v(\alpha-1)$. Therefore,

$$\begin{aligned}
&\int_{\mathcal{M}(1,0)} V(\alpha,q,a)^s e(-N\alpha)d\alpha + \int_{\mathcal{M}(1,1)} V(\alpha,q,a)^s e(-N\alpha)d\alpha \\
&= \int_0^{P^{v-k}} v(\alpha)^s e(-N\alpha)d\alpha + \int_{1-P^{v-k}}^{1} v(\alpha-1)^s e(-N\alpha)d\alpha \\
&= \int_0^{P^{v-k}} v(\beta)^s e(-N\beta)d\beta + \int_0^{P^{v-k}} v(\beta)^s e(-N\beta)d\beta \\
&= J^*(N).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\int_{\mathcal{M}} F(\alpha)^s e(-N\alpha)d\alpha &= \sum_{1\le q\le P^v} \sum_{\substack{a \bmod q \\ (a,q)=1}} \left(\frac{S(q,a)}{q}\right)^s e\left(-\frac{Na}{q}\right) J^*(N) + O\left(P^{s-k-\delta_2}\right). \\
&= \mathfrak{G}(N,P^v)J^*(N) + O\left(P^{s-k-\delta_2}\right).
\end{aligned}$$

This completes the proof. While technical, the general idea here is to look at two functions. First, $\mathfrak{G}(N,Q)$, where we sum over all q up to Q such that $(a,q) = 1$, taking a function $S(q,a)$ raised to an exponent s and multiplying by a complex exponential. Second, $J^*(N)$, an integral over a function $v(\beta)$ similar to $F(\alpha)$, which can be thought of as smoothing out the discrete jumps in G.

5 Calculating the Major Arc

5.1 The Singular Integral

To estimate the singular integral $J^*(N)$, we will first look at a slightly easier integral $J(N)$ and use it to explicitly estimate $J^*(N)$. We consider

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

Theorem 5.1: *There exists $\delta_3 > 0$ such that*

$$J(N) \ll P^{s-k}$$

and

$$J^*(N) = J(N) + O(P^{s-k-\delta_3})$$

Proof of Theorem 5.1 By Lemma 4.1,

$$\begin{aligned} J(N) &\ll \int_0^{1/2} \min(P, |\beta|^{-1/k})^s d\beta \\ &= \int_0^{1/N} \min(P, |\beta|^{-1/k})^s d\beta + \int_{1/N}^{1/2} \min(P, |\beta|^{-1/k})^s d\beta \\ &= \int_0^{1/N} P^s d\beta + \int_{1/N}^{1/2} \beta^{-s/k} d\beta \\ &\ll P^{s-k} \end{aligned}$$

and

$$\begin{aligned} J(N) - J^*(N) &= \int_{P^{v-k} \le |\beta| \le 1/2} v(\beta)^s e(-N\beta) d\beta \\ &\ll \int_{P^{v-k}}^{1/2} |v(\beta)^s d\beta \\ &\ll \int_{P^{v-k}}^{1/2} \beta^{-s/k} d\beta \\ &\ll P^{(k-v)s/(k-1)} \\ &= P^{s-k-\delta_3}. \end{aligned}$$

The motivation for doing so is that $J^*(N)$ is hard to estimate due to the $v(\beta)$ in it, which is difficult to evaluate as β approaches 0. However, by moving the domain of integration, and noting that $v(\beta)$ is bounded by $\min(P, |\beta|^{-1/k})$, we see that $v(\beta)^s$ is bounded by $|\beta|^{-s/k}$. Furthermore, $J(N)$ is easier to estimate because its domain restrictions avoid singularities and other erratic behavior that $J^*(N)$ has.

Now, we can calculate $J(N)$ with one more lemma, the proof of which is available on pages 134-135.

Lemma 5.1 Let α and β be real numbers such that $0 < \beta < 1$ and $\alpha > \beta$. Then

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

where the implied constant depends only on β.

Theorem 5.2 *If $s \geq 2$, then*

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

Proof of Theorem 5.2 Let

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

for $s \geq 1$. We shall compute this integral by induction on s. Since

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

it follows that

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

and so

$$\begin{aligned} J_s(N) &= k^{-s} \sum_{m_1=1}^{N} \cdots \sum_{m_s=1}^{N} (m_1 \cdots m_s)^{1/k-1} \int_{-1/2}^{1/2} e((m_1 + \cdots + m_s - N)\beta) d\beta \\ &= k^{-s} \sum_{\substack{1 \leq m_1, \ldots, m_s \leq N \\ 1 \leq m_i \leq N}} (m_1 \cdots m_s)^{1/k-1}. \end{aligned}$$

In particular, for $s = 2$, we apply Lemma 5.1 with $\alpha = \beta = 1/k$ and obtain

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

This proves the result in the case where $s = 2$. If $s \geq 2$ and the theorem holds for s, then

$$\begin{aligned} J_{s+1}(N) &= \int_{-1/2}^{1/2} v(\beta)^{s+1} e(-N\beta) d\beta \\ &= \int_{-1/2}^{1/2} v(\beta) v(\beta)^s e(-N\beta) d\beta \\ &= \int_{-1/2}^{1/2} \sum_{m=1}^{N} \frac{1}{k} m^{1/k-1} e(\beta m) v(\beta)^s e(-N\beta) d\beta \\ &= \int_{-1/2}^{1/2} \sum_{m=1}^{N} \frac{1}{k} m^{1/k-1} e(\beta m) v(\beta)^s e(-N\beta) d\beta \end{aligned}$$

$$= \sum_{m=1}^{N} \frac{1}{k} m^{1/k-1} \int_{-1/2}^{1/2} v(\beta)^s e(-(N-m)\beta) d\beta$$

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

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

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

Applying Lemma 5.3 to the main term (with $\alpha = s/k$ and $\beta = 1/k$) and the error term (with $\alpha = (s-1)/k$ and $\beta = 1/k$), we obtain

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

and

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

This gives

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

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

This completes the induction. And thus, we have shown how to estimate $J(N)$, and we know that $J^*(N)$ is within a very small error term away from $J(N)$.

5.2 The Singular Series

With the singular integral taken care of, we now turn to the singular series $\mathfrak{G}(N, Q)$. This section is highly technical, and many of the proofs (of the 7 lemmas, for example) can be found in pages 138-145. First, though, recall Theorem 4.3, where we introduced the function

$$\mathfrak{G}(N, Q) = \sum_{1 \leq q \leq Q} A_N(q),$$

with

$$A_N(q) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\frac{S(q,a)}{q} \right)^s e\left(\frac{-Na}{q} \right).$$

We then define the *singular series* as

$$\mathfrak{G}(N) = \sum_{q=1}^{\infty} A_N(q).$$

Let's back up a little bit to check for intuition. The function $A_N(q)$ is a weighted count of solutions to a congruence equation modulo q. $S(q,a)$ is an exponential sum that counts how the k-th terms are distributed modulo q, i.e. each term in $S(q,a)$ relates to a solution of the congruence $x^k \equiv N \pmod{q}$. The weighting is then given by the exponential function $e\left(\frac{-Na}{q}\right)$. Our next job, after defining the singular series, is to show that $\mathfrak{G}(N)$ can be well-approximated by $\mathfrak{G}(N, P^v)$, and thus bound $\mathfrak{G}(N)$.

Let

$$0 < \varepsilon < \frac{1}{sK}$$

Since we assumed $s \geq 2^k + 1 = 2K + 1$, we have

$$\frac{s}{K} - 1 - s\varepsilon \geq 1 + \frac{1}{K} - s\varepsilon = 1 + \delta_4,$$

where

$$\delta_4 = \frac{1}{K} - s\varepsilon > 0.$$

By Weyl's inequality, recall

$$\frac{S(q,a)}{q} \ll q^{-1/k+\varepsilon}$$

which tells us that

$$A_N(q) \ll \frac{q}{q^{s/k - s\varepsilon}} \leq \frac{1}{q^{1+\delta_4}},$$

which tells us that the series $\sum A_N(q)$ converges absolutely and uniformly with respect to N, which means there is a constant $c_2 = c_2(k,s)$ such that

$$|\mathfrak{G}(N)| < c_2$$

and moreover that

$$\begin{aligned} \mathfrak{G}(N) - \mathfrak{G}(N, P^v) &= \sum_{q > P^v} A_N(q) \\ &\ll \sum_{q > P^v} \frac{1}{q^{1+\delta_4}} \\ &\ll P^{-v\delta_4}. \end{aligned}$$

The following lemmas will allow us to build up towards the major proof of this section, where we will show that $\mathfrak{G}(N)$ is a positive real number for all N and that there exists a positive constant $c_1 = c_1(k,s)$ such that

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

Lemma 5.2 Let $(q, r) = 1$. Then

$$S(qr, ar + bq) = S(q, a)S(r, b).$$

Lemma 5.3 If $(q, r) = 1$, then

$$A_N(qr) = A_N(q)A_N(r),$$

that is, the function $A_N(q)$ is multiplicative.

Lemma 5.4 Let $s \geq 2^k + 1$. For every prime p, the series

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

converges, and

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

Lemma 5.5 If $s \geq 2^k + 1$, then

$$\mathfrak{G}(N) = \prod_p \chi_N(p).$$

Moreover, there exists a constant c_2 depending only on k and s such that

$$0 < \mathfrak{G}(N) < c_2$$

for all N, and there exists a prime p_0 depending only on k and s such that

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

for all $N \geq 1$.

Lemma 5.6 Let m be an integer not divisible by p. If the congruence $x^k \equiv m \pmod{p^\gamma}$ is solvable, then the congruence $y^k \equiv m \pmod{p^h}$ is solvable for every $h \geq \gamma$.

Lemma 5.7 Let p be prime. If there exist integers $a_1, \ldots, a_s$, not all divisible by p, such that

$$a_1^k + \ldots + a_s^k \equiv N \pmod{p^\gamma},$$

then

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

Lemma 5.8 If $s \geq 2k$ for k odd or $s \geq 4k$ for k even, then

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

And now we are finally ready to prove the theorem!

Theorem 5.6 *There exist positive constants* $c_1 = c_1(k,s)$ and $c_2 = c_2(k,s)$ *such that*

$$c_1 < \mathfrak{G}(N) < c_2.$$

Moreover, for all sufficiently large integers N *,*

$$\mathfrak{G}(N, P^v) = \mathfrak{G}(N) + O(P^{-v\delta_4}).$$

This result pretty much follows directly from the aforementioned lemmas; the only part not yet proved is the lower bound for $\mathfrak{G}(N)$. However, we have seen that there exists a prime $p_0 = p_0(k,s)$ such that

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

for all $N \geq 1$. Since

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

for all primes p and all N, it follows that

$$\mathfrak{G}(N) - \prod_p \chi_N(p) > \frac{1}{2} \prod_{p \leq p_0} \chi_N(p) \geq \frac{1}{2} \prod_{p \leq p_0} p^{\gamma(1-s)} = c_1 > 0.$$

which (finally) concludes the proof.

6 Proving the Hardy-Littlewood Formula

We are now finally ready to prove the Hardy-Littlewood Asymptotic Formula:

The Hardy-Littlewood Theorem Let $k \geq 2$ and $s \geq 2^k + 1$. Let $r_{k,s}(N)$ denote the number of representations of N as the sum of s kth powers of positive integers. There exists $\delta = \delta(k,s) > 0$ such that

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

where the implied constant depends only on k and s, and $\mathfrak{G}(N)$ is an arithmetic function such that

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

for all N, where c_1 and c_2 are positive constants that depend only on k and s.

Proof. Let $\delta_0 = \min(1, \delta_1, \delta_2, \delta_3, \delta_4)$. By all the past theorems, we have

$$\begin{aligned}
r_{k,s}(N) &= \int_0^1 F(\alpha)^s e(-\alpha N) d\alpha \\
&= \int_{\mathcal{M}} F(\alpha)^s e(-\alpha N) d\alpha + \int_m F(\alpha)^s e(-\alpha N) d\alpha \\
&= \mathfrak{G}(N, P^v) J^*(N) + O(P^{s-k-\delta_2}) + O(P^{s-k-\delta_1}) \\
&= (\mathfrak{G}(N) + O(P^{-v\delta_4}))(J(N) + O(P^{s-k-\delta_3})) + O(P^{s-k-\delta_2}) \\
&\quad + O(P^{s-k-\delta_1}) \\
&= \mathfrak{G}(N) J(N) + O(P^{s-k-\delta_0}) \\
&= \mathfrak{G}(N) \left(1 + \frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} N^{\frac{s}{k}-1} + O(N^{\frac{(s-1)}{k-1}}) \\
&\quad + O\left(N^{\frac{s}{k}-1-\delta_0/k}\right) \\
&= \mathfrak{G}(N) \Gamma\left(1 + \frac{1}{k}\right) \Gamma\left(\frac{s}{k}\right)^{-1} N^{\frac{s}{k}-1} + O\left(N^{\frac{s}{k}-1-\delta}\right),
\end{aligned}$$

where $\delta = \delta_0/k$. This completes the proof.

7 Appendix

7.1 Where does the integral for $r_{k,s}(N)$ come from?

Recall the original form of the circle method:

$$r_{A,s}(N) = \frac{1}{2\pi i} \int_{|z|=\rho} \frac{f(z)^s}{z^{N+1}} dz$$

for any ρ in $(0, 1)$.

Vinogradov greatly simplified and improved the circle method. He observed that in order to study $r_{A,s}(N)$, it is possible to replace the power series $f(z)$ with the polynomial

$$p(z) = \sum_{a \le N \in A} z^a.$$

Then

$$p(z)^s = \sum_{m=0}^{sN} r_{A,s}^{(N)}(m) z^m,$$

where $r_{A,s}^{(N)}(m)$ is the number of representations of m as the sum of s elements of A not exceeding N. In particular, since the elements of A are nonnegative, we have $r_{A,s}^{(N)}(m) = r_{A,s}(m)$ for $m \le N$ and $r_{A,s}^{(N)}(m) = 0$ for $m > sN$. If we let

$$z = e(\alpha) = e^{2\pi i \alpha},$$

then we obtain the trigonometric polynomial

$$F(\alpha) = p(e(\alpha)) = \sum_{a \in A} e(a\alpha),$$

and

$$F(\alpha)^s = \sum_{m=0}^{sN} r_{A,s}^{(N)}(m) e(m\alpha).$$

From the basic orthogonality relation for the functions $e(n\alpha)$,

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

we obtain

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

7.2 What is O?

O is commonly referred to as "Big-O" notation, and is used in asymptotic functions as an error term. Here are a few more points to ensure everyone understands:

- **Upper Bound:** When we say $f(x) = O(h(x))$ as $x \to \infty$, we mean that there exists some positive constant M and some value x_0 such that for all $x > x_0$, the absolute value of $f(x)$ is bounded above by M times the absolute value of $h(x)$, i.e., $|f(x)| \leq M|h(x)|$.
- **Informal Interpretation:** Informally, you can think of $f(x)$ as not growing faster than $h(x)$ times some constant factor when x is large.
- **Error Term:** In asymptotic expansions, $O(h(x))$ often represents the error term of an approximation, indicating that the error does not grow faster than some multiple of $h(x)$.
- **Not Exact Bounds:** It's important to note that $O(h(x))$ does not give an exact bound but rather an order of magnitude. For example, if $f(x) = 3x^2 + O(x)$, this means that the part of $f(x)$ that is not $3x^2$ grows no faster than some constant times x.

7.3 Other notational items

- $e(x)$ is simply the exponential function in the complex plane, with

  $$e(x) = e^{2\pi i x}$$

- $\Gamma(x)$ is the gamma function, which is defined for all numbers in the complex plane excluding the non-positive integers. For the positive integers n

  $$\Gamma(n) = (n-1)!,$$

  and for the rest of the complex plane with a positive real part,

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