WARING'S PROBLEM

ALEX RICE

Abstract. These are notes compiled from an independent study with two University of Rochester undergraduate students during the Spring 2016 semester, and a treatment of the same material in MTH 230: Number Theory during Fall 2016, in which we give a mostly self-contained exposition of the fact that if $s > 2^k$, then every sufficiently large natural number can be written as the sum of s perfect k-th powers, in close to the expected number of ways. As the notes were prepared for a course, some of the details are left as exercises, or are alluded to as previously completed exercises. The notes are aimed at an undergraduate audience, and the only strict prerequisites are differential and integral calculus, a small amount of elementary number theory, and a general awareness of complex numbers. While some experience and comfort with complex exponentials and Big-O notation will help, we make an effort to introduce and discuss all required tools. (Still in progress.)

1. Introduction

It is a well-known theorem of Lagrange that every natural number can be written as the sum of four squares. What about cubes? Or perfect 73-rd powers? In these notes we prove the following conjecture of Edward Waring from 1770:

Theorem W 1 (Waring's Problem, Qualitative)**.** *For every $k \in \mathbb{N}$, there exists $s = s(k) \in \mathbb{N}$ such that every natural number can be written as a sum of s perfect k-th powers.*

In this qualitative form, Theorem W1 was first proven by Hilbert in 1908, but here we follow the approach of Hardy and Littlewood from the early 1920s, utilizing the *Hardy-Littlewood Circle Method* to establish the following stronger result:

Theorem W 2 (Waring's Problem, Intermediate)**.** *If $s, k \in \mathbb{N}$ with $s > 2^k$, then all but finitely many natural numbers can be written as the sum of s perfect k-th powers.*

On the face of it, Theorem W2 may appear weaker than Theorem W1, but a moment's consideration reveals that to not be the case. Specifically, every $N \in \mathbb{N}$ that is *excluded* from the conclusion of Theorem W2 can clearly be written as a sum of N perfect k-th powers, because 1 is a perfect k-th power! Therefore, if N_0 is the largest number that is excluded, which exists because there are only finitely many exceptions, then the conclusion of Theorem W1 follows with $s = \max\{N_0, 2^k + 1\}$. One can ask more refined questions about the *optimal* values of s in the context of each theorem, and the answers are actually quite different, but we will not focus on that degree of precision here.

2. Counting Solutions to Integer Equations with Integrals

Recall that the exponential function e^z can be defined for all complex numbers by the convergent Taylor expansion

$$e^z = 1 + z + \frac{z^2}{2} + \frac{z^3}{6} + \cdots = \sum_{n=0}^{\infty} \frac{z^n}{n!},$$

and this function maintains maintains nice properties of the real exponential like

$$e^{z+w} = e^z e^w. \tag{1}$$

Further, if the exponent is purely imaginary we have Euler's formula

$$e^{\mathrm{i}t} = \cos(t) + \mathrm{i}\sin(t),$$

which is just the point on the unit circle in the complex plane corresponding to angle t. In particular, as a function of a single real variable we have

$$\frac{d}{dt}\left(e^{\mathrm{i}t}\right) = -\sin(t) + \mathrm{i}\cos(t) = \mathrm{i}e^{\mathrm{i}t}. \tag{2}$$

The principal idea of the Hardy-Littlewood circle method, as it relates to number theoretic questions, is to accurately count, or at least assert the existence of, solutions to certain diophantine equations (like $n_1^k + \cdots + n_s^k = N$) by analyzing certain *exponential sums* (like $\sum_{1\le n\le M} e^{2\pi \mathrm{i} n^k \alpha}$) and their integrals over the unit circle in the complex plane, here parametrized by $0 \le \alpha < 1$.

But how does this work? What is the bridge between the a priori unrelated inquiries of counting solutions to integer equations and integrating exponential sums over the circle? The key is *orthogonality*.

Lemma W 3 (Orthogonality Relation)**.**

$$\int_0^1 e^{2\pi \mathrm{i} n\alpha} \mathrm{d}\alpha = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n \in \mathbb{Z} \setminus \{0\} \end{cases}$$

Proof. If $n = 0$, the exponential is identically $e^0 = 1$, integrated over an interval of length 1, so the equality is trivial. If $n \neq 0$, then by (2) and the Fundamental Theorem of Calculus we have

$$\int_0^1 e^{2\pi \mathrm{i} n\alpha} \mathrm{d}\alpha = \left[\frac{e^{2\pi \mathrm{i} n\alpha}}{2\pi \mathrm{i} n}\right]_0^1 = \frac{e^{2\pi \mathrm{i} n} - 1}{2\pi \mathrm{i} n}.$$

Further, if $n \in \mathbb{Z}$, then $e^{2\pi \mathrm{i} n} = 1$, and the lemma follows. □

Lemma W3 allows us to use an integral of an exponential over the circle as a perfect "detector" of whether an integer equation is solved or not, which is exactly the bridge that we need. Specifically, suppose $s, k, N \in \mathbb{N}$ and we want to count exactly how many ways N can be written as a sum of s perfect k-th powers. To that end, we define

$$r_{s,k}(N) = \left|\{(n_1, n_2, \ldots, n_s) \in \mathbb{N}^s : n_1^k + n_2^k + \cdots + n_s^k = N\}\right|,$$

and we observe the following formula:

Lemma W 4 (Integral Formula for $r_{s,k}$)**.** *For $s, k, N \in \mathbb{N}$, we have*

$$r_{s,k}(N) = \int_0^1 e^{-2\pi \mathrm{i} N\alpha} \left(S_M(\alpha)\right)^s \mathrm{d}\alpha,$$

where $M = N^{1/k}$ and

$$S_M(\alpha) = \sum_{1\le n\le M} e^{2\pi \mathrm{i} n^k \alpha}.$$

Proof. Fix $s, k, N \in \mathbb{N}$ and let $M = N^{1/k}$. We first note that for each solution we are trying to count, all of $n_1, \ldots, n_s$ are at most M. Therefore, by applying Lemma W3, exchanging the order of the sums and integral, and applying (1), we have

$$r_{s,k}(N) = \sum_{1\le n_1,\dots,n_s\le M} \begin{cases} 1 & \text{if } n_1^k + \cdots n_s^k = N \\ 0 & \text{else} \end{cases}$$

$$= \sum_{1\le n_1,\dots,n_s\le M} \int_0^1 e^{2\pi \mathrm{i}(n_1^k+\cdots+n_s^k-N)\alpha} \mathrm{d}\alpha$$

$$= \int_0^1 e^{-2\pi \mathrm{i} N\alpha} \sum_{1\le n_1,\dots,n_s\le M} e^{2\pi \mathrm{i} n_1^k\alpha}\cdots e^{2\pi \mathrm{i} n_s^k\alpha} \mathrm{d}\alpha$$

$$= \int_0^1 e^{-2\pi \mathrm{i} N\alpha} \left(\sum_{1\le n_1\le M} e^{2\pi \mathrm{i} n_1^k\alpha}\right)\cdots\left(\sum_{1\le n_s\le M} e^{2\pi \mathrm{i} n_s^k\alpha}\right) \mathrm{d}\alpha$$

$$= \int_0^1 e^{-2\pi \mathrm{i} N\alpha} \left(S_M(\alpha)\right)^s \mathrm{d}\alpha,$$

as required. □

3. Big-O notation, Vinogradov Symbols, and Asymptotic Estimation

Exhibiting an exact, explicit formula for $r_{s,k}(N)$ is beyond our capabilities, but to prove Theorem W2, we only need to show that $r_{s,k}(N) > 0$ provided $s > 2^k$ and N is sufficiently large with respect to s and k. Therefore, it is good enough for our purposes to estimate $r_{s,k}(N)$ with decent accuracy for fixed s, k and growing values of N.

To this end, recall that if $f, g : \mathbb{R} \to \mathbb{C}$, we say that

$$f(x) = O\left(g(x)\right)$$

(as $x \to \infty$) if there exist constants C and x_0 with

$$|f(x)| \le C|g(x)| \quad \text{for all } x > x_0.$$

Morally speaking, this means that as x tends to infinity, $f(x)$ grows at most as quickly, or shrinks at least as fast, as $g(x)$. To recall an example we have discussed in class, if $\pi(x)$ denotes the number of primes that are at most x, then

$$\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right),$$

meaning that there exists a constant C such that

$$\left|\pi(x) - \frac{x}{\log x}\right| \le C\frac{x}{(\log x)^2} \quad \text{for all } x \ge 2.$$

Note that in this case (and for us, most other cases) we can replace $x > x_0$ with $x \ge 2$ by taking an appropriate maximum and potentially changing the constant, since the functions are continuous and nonzero for $x \ge 2$.

This *asymptotic formula* is meaningful because, even though there is an implied constant in the "Big-O" term, it is still the case that if x is large enough, then the first term (which we call the *main term*) will be much, much larger than the second term (which we call the *error term*), so the main term is a good approximation as x tends to infinity.

A very convenient property of Big-O notation is that if you have several Big-O terms added together, and one of them grows faster (or shrinks slower) than the rest, then you can ignore all of the smaller ones. For example,

$$O\left(\frac{x}{(\log x)^2}\right) + O(x^{0.99}) + O((\log x)^{100}) = O\left(\frac{x}{(\log x)^2}\right).$$

Further, if you multiply a Big-O term by a regular term, than you can absorb the regular term into the Big-O and ignore all constants, for example

$$17435x^{-.05} \cdot O(x^{1.01}) = O(x^{0.96}).$$

When a Big-O term is alone on one side of an equation, we often use the alternative, less onerous *Vinogradov symbol* $\ll$. Specifically, we write

$$f(x) \ll g(x)$$

if $f(x) = O(g(x))$, and we write $f(x) \gg g(x)$ if $g(x) = O(f(x))$. We also use subscripts to clarify what parameters the implied constants are allowed to depend on. For example, Theorem 33 from class is equivalent to the statement that the Euler totient function $\phi(n)$ satisfies $\phi(n) \gg_\epsilon n^{1-\epsilon}$ for every $\epsilon > 0$.

4. Discrete and Continuous Triangle Inequalities

Recall that for any vectors $\mathbf{v}_1, \dots, \mathbf{v}_\ell \in \mathbb{R}^d$, we have the *triangle inequality*

$$|\mathbf{v}_1 + \cdots + \mathbf{v}_\ell| \leq |\mathbf{v}_1| + \cdots + |\mathbf{v}_\ell|.$$

Further, this also holds for continuous sums, also known as integrals, in that for any continuous function $f : \mathbb{R} \to \mathbb{C}$ (one can phrase things much more generally, but we will just state what we need), and any $a, b \in \mathbb{R}$, we have

$$\left|\int_a^b f(x)\mathrm{d}x\right| \leq \int_a^b |f(x)|\mathrm{d}x.$$

Assuming we are sticking to Riemann integration (which is most appropriate for the goals of this exposition), the integral version follows from writing the integral as a limit of Riemann sums, and applying the original triangle inequality to each Riemann sum.

In the context of the circle method, both versions of the triangle inequality are used a great deal, often in conjunction with the fact that $|e^{\mathrm{i}t}| = 1$ for all $t \in \mathbb{R}$, to effectively bound error terms. For example, for any sequences of real numbers $a_1, \dots, a_\ell$ and $t_1, \dots, t_\ell$, we have

$$\left|\sum_{n=1}^{\ell} a_n e^{\mathrm{i}t_n}\right| \leq \sum_{n=1}^{\ell} |a_n|,$$

and for any continuous functions $f : \mathbb{R} \to \mathbb{C}$, $g : \mathbb{R} \to \mathbb{R}$, and any $a, b \in \mathbb{R}$, we have

$$\left|\int_a^b f(x)e^{\mathrm{i}g(x)}\mathrm{d}x\right| \leq \int_a^b |f(x)|\mathrm{d}x.$$

We use both of these facts freely and frequently.

5. Heuristic and Main Result

We now fix $s, k \in \mathbb{N}$ for the remainder of our discussion, and we think of $r_{s,k}(N)$ as a function only of N, with N growing to infinity. In particular, all constants, including those implied by Big-O terms and Vinogradov symbols, are allowed to depend on s, k, and any other fixed parameters, but are NEVER allowed to depend on N. With this preemptive clarification, we will not use any subscripts on our Vinogradov symbols in the context of our proof, but rather only when stating lemmas that are independent of our proof.

Now that we are on board with the idea of estimating $r_{s,k}(N)$ with a main term, roughly how big do we think that main term should be? There are approximately $N^{1/k}$ possible choices for each of the natural numbers $n_1, \dots, n_s$, totaling about $N^{s/k}$ s-tuples where $n_1^k + \cdots + n_s^k$ has a chance to equal N. Each of these sums lies between 1 and sN, so if we make the leap of faith that they are somewhat "uniformly distributed", we might guess that about a $1/N$ (ignoring constants) portion of these sums are equal to N. This leads us to predict that the order of magnitude of $r_{s,k}(N)$ for large N is like $N^{s/k}(1/N) = N^{\frac{s}{k}-1}$. There are ways to refine this heuristic to more accurately predict the main term and not just its order of growth, but we will stick with this.

Our main result is the following asymptotic formula for $r_{s,k}(N)$, which in particular implies Theorem W2.

Theorem W 5 (Waring's Problem, Quantitative)**.** *If $s > 2^k$, then*

$$r_{s,k}(N) = \Theta(N)N^{\frac{s}{k}-1} + O(N^{\frac{s}{k}-1-\epsilon}), \tag{3}$$

for some $\epsilon > 0$, where $0 < c_1 < \Theta(N) < c_2$ for some constants c_1, c_2.

In fact, we will explicitly describe $\Theta(N)$, writing it as a product of an integral that depends only on s and k and an infinite series that depends on N but converges absolutely independent of N, but we save those details for later. Note that this certainly implies Theorem W2, and even gives the predicted order of growth, because we have that

$$r_{s,k}(N) > c_1 N^{\frac{s}{k}-1} - CN^{\frac{s}{k}-1-\epsilon},$$

which for example is larger than $(c_1/2)N^{\frac{s}{k}-1}$ if N is large enough in terms of all of the constants.

6. Partitioning the Circle: Defining the Major and Minor Arcs

The key philosophy of the circle method is that an exponential sum like $S_M(\alpha)$ should be very small, except when α is very close to a rational number with small denominator. Therefore, the main contributions to the integral expression for $r_{s,k}(N)$ given by Lemma W4 should come from these very small intervals around rationals, and the contribution from the remaining portion of the circle should be absorbed into an error term. This philosophy inspires the following definition, for which we also fix a sufficiently small positive constant δ (think $\delta = .01$).

Definition. Suppose $M > 0$. For $a, q \in \mathbb{N}$, we define

$$\mathbf{M}_{a,q} = \{\alpha \in [0,1] : |\alpha - a/q| < M^{\delta-k}\}.$$

Further, we define $\mathfrak{M}$, the *major arcs*, by

$$\mathfrak{M} = \bigcup_{1 \le q \le M^\delta} \bigcup_{a=0}^{q} \mathbf{M}_{a,q},$$

and $\mathfrak{m}$, the *minor arcs*, by

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

We note that these objects certainly depend on M, but we suppress that dependence in the notation.

Exercise W 1. Prove that if $a, q, b, r \in \mathbb{N}$, $a/q \neq b/r$, and $\mathbf{M}_{a,q} \cap \mathbf{M}_{b,r} \neq \emptyset$, then

$$\max\{q, r\} \geq (M^{k-\delta}/2)^{1/2}.$$

In particular, this means that the distinct major arcs in $\mathfrak{M}$ are pairwise disjoint if M is large.

Our task for proving Theorem W5 can now be broken into two pieces. Specifically, assuming $s > 2^k$, we show for any $M > 0$ that

$$\int_{\mathfrak{m}} |S_M(\alpha)|^s \, \mathrm{d}\alpha \ll M^{s-k-\frac{\delta}{2^{k+1}}}, \tag{4}$$

and then fixing $N \in \mathbb{N}$ and letting $M = N^{1/k}$ we show that

$$\int_{\mathfrak{M}} e^{-2\pi \mathrm{i} N\alpha} \left(S_M(\alpha)\right)^s \, \mathrm{d}\alpha = \sum_{1 \leq q \leq M^\delta} \sum_{\substack{0 \leq a \leq q \\ \gcd(a,q)=1}} \int_{\mathbf{M}_{a,q}} e^{-2\pi \mathrm{i} N\alpha} \left(S_M(\alpha)\right)^s \, \mathrm{d}\alpha \tag{5}$$

satisfies the desired asymptotic formula, where the equality in (5) follows from Exercise W1.

7. The Minor Arcs: Weyl's Inequality and Hua's Lemma

This section is dedicated to establishing (4), and for the remainder of our discussion we let

$$S_M(\alpha) = \sum_{1 \leq n \leq M} e^{2\pi \mathrm{i} n^k \alpha}$$

for any $M > 0$. We note that this section and the next are self-contained and make sense independent of having our original task in mind. In particular, there is no need for the parameter N. To bound $S_M(\alpha)$ on the minor arcs, we utilize the following century-old estimate, which provides a nontrivial upper bound on an exponential sum over a polynomial, provided the leading coefficient can be approximated with a rational number whose denominator is neither too small nor too large.

Lemma W 6 (Weyl's Inequality)**.** *Suppose $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ with $\alpha_k \neq 0$, $a, q \in \mathbb{N}$ with $\gcd(a, q) = 1$, and $x, \epsilon > 0$. If $|\alpha_k - a/q| < q^{-2}$, then*

$$\sum_{1 \leq n \leq x} e^{2\pi \mathrm{i}(\alpha_1 n + \cdots + \alpha_k n^k)} \ll_{k,\epsilon} x^{1+\epsilon} \left(x^{-1} + q^{-1} + qx^{-k}\right)^{2^{1-k}}.$$

Proof. Following [2], we provide a proof in the case of $k = 2$, and discuss the extension to higher values of k at the end.

Suppose $x \geq 1$ (the left hand side in the lemma is 0 otherwise) and $P(n) = \alpha n^2 + \beta n$ for $\alpha, \beta \in \mathbb{R}$, $\alpha \neq 0$. Suppose further that $|\alpha - a/q| < q^{-2}$ for $a, q \in \mathbb{N}$ with $\gcd(a, q) = 1$, and let

$$W = \sum_{1 \leq n \leq x} e^{2\pi \mathrm{i} P(n)}.$$

Recall that for $z = x + iy \in \mathbb{C}$, we write $\Re(z) = x$, $\Im(z) = y$, and $\overline{z} = x - iy$. Using the facts that $z\overline{z} = |z|^2$ for $z \in \mathbb{C}$ and $\overline{e^{\mathrm{i}t}} = e^{-\mathrm{i}t}$ for $t \in \mathbb{R}$, we have

$$|W|^2 = \sum_{1 \leq n, m \leq x} e^{2\pi \mathrm{i}(P(n) - P(m))}. \tag{6}$$

We now observe that there are exactly $\lfloor x \rfloor \leq x$ terms in this double sum with $n = m$, and they each contribute $e^0 = 1$. Further, each pair $1 \leq m < n \leq x$ has a "partner" where n and m play the opposite roles. Using the fact that $z + \overline{z} = 2\Re(z)$, each of these "pairs of pairs" contributes

$$e^{2\pi \mathrm{i}(P(n)-P(m))} + e^{2\pi \mathrm{i}(P(m)-P(n))} = 2\Re\left(e^{2\pi \mathrm{i}(P(n)-P(m))}\right).$$

Combining these observations with (6), we have

$$|W|^2 \leq x + 2\Re\left(\sum_{1\leq m<n\leq x} e^{2\pi \mathrm{i}(P(n)-P(m))}\right). \tag{7}$$

To bound the double sum in the parentheses in (7), we make the substitution $n = m + h$, note that $P(m+h) - P(m) = 2\alpha mh + \beta h + h^2$, exchange the order of summation, and then apply the triangle inequality to the outer sum only, yielding

$$\begin{aligned}
\left|\sum_{1\leq m<n\leq x} e^{2\pi \mathrm{i}(P(n)-P(m))}\right| &= \left|\sum_{1\leq m\leq x}\sum_{1\leq h\leq x-m} e^{2\pi \mathrm{i}(P(m+h)-P(m))}\right| \\
&= \left|\sum_{1\leq h\leq x-1}\sum_{1\leq m\leq x-h} e^{2\pi \mathrm{i}(2\alpha mh+\beta h+h^2)}\right| \\
&\leq \sum_{1\leq h\leq x-1}\left|\sum_{1\leq m\leq x-h} e^{2\pi \mathrm{i}(2\alpha h)m}\right|.
\end{aligned}$$

From (7) we now have

$$|W|^2 \leq x + 2\sum_{1\leq h\leq x-1}\left|\sum_{1\leq m\leq x-h} e^{2\pi \mathrm{i}(2\alpha h)m}\right|. \tag{8}$$

The sum inside the absolute value in (8) is merely a geometric series with common ratio $r = e^{2\pi \mathrm{i}(2\alpha h)}$, which is bounded by $x - h \leq x$ by the triangle inequality. Further, we have the geometric series formula

$$\sum_{m=1}^{K} r^m = \frac{r - r^{K+1}}{1 - r}.$$

In our case, the numerator is bounded by 2 in absolute value, and for the denominator we note that the straight line distance between two points on the unit circle is at least $2/\pi$ times the length of the shortest path along the circle between those points, which is just the distance between the angle and the nearest multiple of 2π. In particular,

$$\left|1 - e^{2\pi \mathrm{i}(2\alpha h)}\right| \geq \frac{2}{\pi} 2\pi \|2\alpha h\| = 4\|2\alpha h\|,$$

where $\|\cdot\|$ denotes distance to the nearest integer. Therefore, from our two ways of bounding this sum, we have

$$\sum_{1\leq m\leq x-h} e^{2\pi \mathrm{i}(2\alpha h)m} \leq \min\left\{x, \frac{1}{2\|2\alpha h\|}\right\},$$

which combined with (8) gives

$$|W|^2 \ll x + \sum_{1\le h\le x-1} \min\left\{x, \frac{1}{\|2\alpha h\|}\right\} \le x + \sum_{1\le h\le 2x} \min\left\{x, \frac{1}{\|\alpha h\|}\right\}, \tag{9}$$

where the last inequality is simply the introduction of the odd as well as even integers into the sum. Breaking the sum in h into intervals of length q, which is motivated by the assumpton that α is close to a/q, we have

$$\sum_{1\le h\le 2x} \min\left\{x, \frac{1}{\|\alpha h\|}\right\} \le \sum_{1\le j\le 2x/q} \sum_{s=0}^{q-1} \min\left\{x, \frac{1}{\|\alpha(qj+s)\|}\right\}. \tag{10}$$

We now write $\alpha = a/q + O(1/q^2)$, which we assumed, so if $j \in \mathbb{N}$ and $0 \le s \le q-1$, we have

$$\alpha(qj+s) = qj\alpha + \frac{sa}{q} + O\left(\frac{1}{q}\right). \tag{11}$$

Further, if we let b be the nearest integer to $q^2 j\alpha$, then we have $q^2 j\alpha = b + O(1)$ and hence $qj\alpha = b/q + O(1/q)$. Together with (11), this gives

$$\alpha(qj+s) = \frac{sa+b}{q} + O\left(\frac{1}{q}\right). \tag{12}$$

Since $\gcd(a,q) = 1$, as s runs over all residues modulo q, so does $sa+b$, so using the trivial bound of x for the $O(1)$ terms where the error term dominates, we have

$$\begin{aligned}\sum_{s=0}^{q-1} \min\left\{x, \frac{1}{\|\alpha(qj+s)\|}\right\} &\ll x + \sum_{s=1}^{q-1} \frac{1}{\|s/q\|} \\ &\le x + 2\sum_{1\le s\le q/2} \frac{q}{s} \\ &\ll x + q\log q,\end{aligned}$$

where the last inequality is the standard comparison of the harmonic series with the integral of $f(t) = 1/t$. Since the conclusion of the lemma (for $k = 2$) is trivial if $q > x^2$, we can assume $\log q \le 2\log x$, so this observation pairs with (10) to give

$$\sum_{1\le h\le 2x} \min\left\{x, \frac{1}{\|\alpha h\|}\right\} \ll \sum_{1\le j\le 2x/q} (x + q\log x) \le (2x/q+1)(x+q\log x). \tag{13}$$

Combining (9) with (13), we finally have

$$|W|^2 \ll x\log x + x^2/q + q\log x \le x^2 \log x(x^{-1} + q^{-1} + qx^{-2}). \tag{14}$$

Taking square roots and noting that $\log x \ll_\epsilon x^\epsilon$ for every $\epsilon > 0$, we have established the inequality in the case of $k = 2$. □

Establishing Lemma W6 for $k > 2$ is a matter of induction, and while the notation is somewhat clouding in the general case, the core techniques are all exhibited here. One simply iterates the process of squaring out the sum and making a substitution to reduce the degree of the polynomial by 1, a process known as *Weyl differencing*.

In addition to the $\log x$ term, the induction step gives rise to a power of the maximum value of the function $d(n)$, the number of positive divisors of n, for $1 \leq n \leq x$. For this, one just applies the estimate

$$d(n) \ll_\epsilon n^\epsilon \tag{15}$$

for all $\epsilon > 0$, which we proved in Theorem 34 in class. This is the reason for the x^ϵ factor, as opposed to just $\log x$, in the conclusion of Lemma W6 for general k.

Exercise W 2. Recall Dirichlet's Approximation Theorem, proven in Problem 7 of Homework 5, which says that if $\alpha \in \mathbb{R}$ and $Q \in \mathbb{N}$, then there exist integers a, q with $1 \leq q \leq Q$, $\gcd(a, q) = 1$, and

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

Use this theorem and Lemma W6 to show that

$$S_M(\alpha) \ll M^{1-\frac{\delta}{2^k}} \text{ for all } \alpha \in \mathfrak{m}. \tag{16}$$

Hint: Take $Q = \lceil M^{k-\delta} \rceil$.

While Lemma W6 allows us to beat the trivial upper bound on the sum $S_M(\alpha)$ by a small power of M, that is not good enough to establish (4). To complete the task, we use an upper bound on sufficiently high moments of an exponential sum over a polynomial, established by Hua in the late 1930s. But first, we need a bit of information to use as the base case of an induction.

Exercise W 3. Suppose $f : \mathbb{Z} \to \mathbb{C}$ has finite support, meaning $f(n) = 0$ for all but finitely many $n \in \mathbb{Z}$. (In particular, no need to worry about any convergence issues.) Use Lemma W3 to show that

$$\sum_{n \in \mathbb{Z}} |f(n)|^2 = \int_0^1 \left|\widehat{f}(\alpha)\right|^2 \mathrm{d}\alpha,$$

where

$$\widehat{f}(\alpha) = \sum_{x \in \mathbb{Z}} f(x) e^{2\pi \mathrm{i} x \alpha}.$$

This identity is known, more or less interchangeably, as *Plancherel's Identity* or *Parseval's Identity*.

Lemma W 7 (Hua's Lemma)**.** *If $M, \epsilon > 0$, then*

$$\int_0^1 |S_M(\alpha)|^{2^k} \mathrm{d}\alpha \ll_{k,\epsilon} M^{2^k - k + \epsilon}.$$

Proof. As in Lemma W6, we provide the full proof for the case $k = 2$, and discuss the extension to higher values of k afterward. We first note that if

$$f(n) = \begin{cases} 1 & \text{if } n = m^2 \text{ for some } 1 \leq m \leq M \\ 0 & \text{else} \end{cases},$$

then $\widehat{f}(\alpha)$, as defined in Exercise W3, is precisely $S_M(\alpha)$. Applying the conclusion of that exercise, we have

$$\int_0^1 |S_M(\alpha)|^2 \mathrm{d}\alpha = \sum_{n \in \mathbb{Z}} |f(n)|^2 \leq M. \tag{17}$$

Now, we note $|S_M(\alpha)|^2$ is a special case of the quantity $|W|^2$ estimated in (7). We apply this estimate, and also follow the proof of Lemma W6 in making the substitution $n = m + h$ and observing that $(m+h)^2 - m^2 = 2mh + h^2$, yielding

$$|S_M(\alpha)|^2 \leq M + 2\Re\left(\sum_{1\leq h\leq M-1}\sum_{1\leq m\leq M-h} e^{2\pi \mathrm{i}(2mh+h^2)\alpha}\right). \tag{18}$$

Multiplying both sides of (18) by $|S_M(\alpha)|^2$ and integrating from 0 to 1, and applying (17), we have

$$\int_0^1 |S_M(\alpha)|^4 \,\mathrm{d}\alpha \leq M^2 + 2\Re\left(\int_0^1 \sum_{1\leq h\leq M-1}\sum_{1\leq m\leq M-h} e^{2\pi \mathrm{i}(2mh+h^2)\alpha}|S_M(\alpha)|^2 \mathrm{d}\alpha\right). \tag{19}$$

Once again squaring out $|S_M(\alpha)|^2$, and exchanging the order of summation and integration, the integral on the right hand side of (19) is

$$\sum_{1\leq h\leq M-1}\sum_{1\leq m\leq M-h}\sum_{1\leq u,v\leq M}\int_0^1 e^{2\pi \mathrm{i}(2mh+h^2+u^2-v^2)\alpha}\mathrm{d}\alpha. \tag{20}$$

By Lemma W3, (20) is precisely the number of solutions to the equation

$$2mh + h^2 + u^2 - v^2 = 0,$$

where h, m, u, v are in the specified ranges. Once we chose one of the at most M^2 possibilities for the pair (u, v), the value of $2mh + h^2 = h(2m + h)$ is forced upon us, and in particular h must be a divisor of $v^2 - u^2$. Therefore, the number of choices for h is bounded by the maximum number of positive divisors of an integer up to M^2, which by (15) is at most $C_\epsilon M^\epsilon$ for every $\epsilon > 0$. Further, once h is chosen, there is at most one possible value of m that solves the equation, since $2m + h$ is strictly increasing in m. Putting all this together we have

$$\sum_{1\leq h\leq M-1}\sum_{1\leq m\leq M-h}\sum_{1\leq u,v\leq M}\int_0^1 e^{2\pi \mathrm{i}(2mh+h^2+u^2-v^2)\alpha}\mathrm{d}\alpha \ll_\epsilon M^{2+\epsilon}$$

for every $\epsilon > 0$, and the lemma follows in the case that $k = 2$. □

The additional requirements for extending Lemma W7 to $k > 2$ are even less fundamental then those for Lemma W6. In particular, we saw that this time we needed to apply the divisor function bound (15) even when $k = 2$. Truly, the only difference in the induction for larger k is the development of notation to reflect iterated applications of Weyl differencing rather than a single application.

Exercise W 4. Use (16) and Lemma W7 to establish that (4) holds provided $s > 2^k$.

8. The Major Arcs

In this section, in dichotomy with the previous, we estimate $S_M(\alpha)$ when α is very close to a rational with very small denominator. We make use of the following continuous/discrete hybrid analog of integration by parts, and then we jump right in.

Lemma W 8 (Abel's Partial Summation Formula, Homework 6 Problem 5)**.** *If $f : \mathbb{R} \to \mathbb{C}$ is continuously differentiable, $a : \mathbb{N} \to \mathbb{C}$, and $A(x) = \sum_{1\leq n\leq x} a(n)$, then*

$$\sum_{1\leq n\leq x} f(n)a(n) = f(x)A(x) - \int_0^x A(t)f'(t)\mathrm{d}t.$$

Lemma W 9 (Major Arc Estimate)**.** *If $M > 0$, $a, q \in \mathbb{N}$, $\alpha \in \mathbb{R}$, and $\beta = \alpha - a/q$, then*

$$S_M(\alpha) = q^{-1}G(a,q)\int_0^M e^{2\pi \mathrm{i} x^k \beta}\mathrm{d}x + O\left(q(1+M^k|\beta|)\right),$$

where

$$G(a,q) = \sum_{r=0}^{q-1} e^{2\pi \mathrm{i} r^k a/q}.$$

Proof. Fixing $\alpha = a/q + \beta$, we first apply (1) and write

$$S_M(\alpha) = \sum_{1\le n\le M} e^{2\pi \mathrm{i} n^k a/q}\cdot e^{2\pi \mathrm{i} n^k \beta}.$$

Then, we apply Lemma W8 with $a(n) = e^{2\pi \mathrm{i} n^k a/q}$ and $f(n) = e^{2\pi \mathrm{i} n^k \beta}$ to observe

$$S_M(\alpha) = e^{2\pi \mathrm{i} M^k \beta}S_M(a/q) - \int_0^M S_x(a/q)(2\pi \mathrm{i} k x^{k-1}\beta)e^{2\pi \mathrm{i} x^k \beta}\mathrm{d}x. \tag{21}$$

As an aside, we note that since $e^{2\pi i t}$ is a 1-periodic function of t, the value of $e^{2\pi \mathrm{i} n^k a/q}$ is completely determined by the residue of n modulo q. In particular, this means that for any $x > 0$ we have

$$\begin{aligned} S_x(a/q) &= \sum_{1\le n\le x} e^{2\pi \mathrm{i} n^k a/q} \\ &= \sum_{r=0}^{q-1} e^{2\pi \mathrm{i} r^k a/q}\,|\{1\le n\le x : n\equiv r \mod q\}| \\ &= \sum_{r=0}^{q-1} e^{2\pi \mathrm{i} r^k a/q}(x/q + O(1)) \\ &= \frac{x}{q}G(a,q) + O(q). \end{aligned}$$

Inputting this estimate into both terms of (21), then collecting error terms together, we have

$$\begin{aligned} S_M(\alpha) &= e^{2\pi \mathrm{i} M^k\beta}\left(\frac{M}{q}G(a,q) + O(q)\right) - \int_0^M \left(\frac{x}{q}G(a,q) + O(q)\right)(2\pi \mathrm{i} k x^{k-1}\beta)e^{2\pi \mathrm{i} x^k\beta}\mathrm{d}x \\ &= q^{-1}G(a,q)\left(Me^{2\pi \mathrm{i} M^k\beta} - \int_0^M x\cdot(2\pi \mathrm{i} k x^{k-1}\beta)e^{2\pi \mathrm{i} x^k\beta}\mathrm{d}x\right) \\ &\quad + O\left(q\left(1 + \int_0^M |(2\pi \mathrm{i} k x^{k-1}\beta)e^{2\pi \mathrm{i} x^k\beta}|\mathrm{d}x\right)\right). \end{aligned}$$

Finally, we observe that the difference in the main term is precisely the result of applying integration by parts with $u = e^{2\pi \mathrm{i} x^k\beta}$ and $\mathrm{d}v = \mathrm{d}x$, while the integral in the error term is certainly $O(M^k|\beta|)$.

This leads to the desired estimate

$$S_M(\alpha) = q^{-1}G(a,q)\int_0^M e^{2\pi i x^k\beta}\mathrm{d}x + O\left(q(1+M^k|\beta|)\right).$$

□

Exercise W 5. Use Lemma W9 to show that if $M > 0$, $a, q \in \mathbb{N}$ with $q \le M^\delta$, and $\alpha = a/q + \beta$ with $|\beta| < M^{\delta-k}$, then

$$(S_M(\alpha))^s = \left(q^{-1}G(a,q)\int_0^M e^{2\pi i x^k\beta}\mathrm{d}x\right)^s + O(M^{s-1+2\delta}).$$

9. Establishing the Asymptotic Formula

We are now armed with all the tools necessary to establish an asymptotic formula for $r_{s,k}(N)$, and to that end we fix $N \in \mathbb{N}$ and let $M = N^{1/k}$. We note again that none of our constants, implied or otherwise, are allowed to depend on N, or consequently on M. Since we established (4) in Section 7, it suffices to provide an asymptotic formula for

$$\int_{\mathfrak{M}} e^{-2\pi i N\alpha}\,(S_M(\alpha))^s\,\mathrm{d}\alpha,$$

for which we use the tools developed in Section 8. With this goal in mind, if $q > 1$ and $0 < a < q$, then by substituting $\beta = \alpha - a/q$ we have

$$\int_{\mathbf{M}_{a,q}} e^{-2\pi i N\alpha}\,(S_M(\alpha))^s\,\mathrm{d}\alpha = \int_{-M^{\delta-k}}^{M^{\delta-k}} e^{-2\pi i N(a/q+\beta)}\,(S_M(a/q+\beta))^s\,\mathrm{d}\beta.$$

Further, since the functions we are integrating are 1-periodic, and the distance between α and 1 is the same as the distance between $\alpha - 1$ and 0, we can combine $\mathbf{M}_{0,1}$ and $\mathbf{M}_{1,1}$ and observe

$$\int_{\mathbf{M}_{0,1}\cup\mathbf{M}_{1,1}} e^{-2\pi i N\alpha}\,(S_M(\alpha))^s\,\mathrm{d}\alpha = \int_{-M^{\delta-k}}^{M^{\delta-k}} e^{-2\pi i N\beta}\,(S_M(\beta))^s\,\mathrm{d}\beta.$$

Combining these observations with (5) we have

$$\int_{\mathfrak{M}} e^{-2\pi i N\alpha}\,(S_M(\alpha))^s\,\mathrm{d}\alpha = \sum_{1\le q\le M^\delta}\sum_{\substack{0\le a\le q-1\\ \gcd(a,q)=1}}\int_{-M^{\delta-k}}^{M^{\delta-k}} e^{-2\pi i N(a/q+\beta)}\,(S_M(a/q+\beta))^s\,\mathrm{d}\beta. \tag{22}$$

Exercise W 6. Use (22) and Exercise W5 to show that

$$\int_{\mathfrak{M}} e^{-2\pi i N\alpha}\,(S_M(\alpha))^s\,\mathrm{d}\alpha = \underbrace{\left(\sum_{1\le q\le M^\delta}\sum_{\substack{0\le a\le q-1\\ \gcd(a,q)=1}}(q^{-1}G(a,q))^s e^{-2\pi i Na/q}\right)}_{(\star)}\cdot$$

$$\underbrace{\left(\int_{-M^{\delta-k}}^{M^{\delta-k}} e^{-2\pi i N\beta}\left(\int_0^M e^{2\pi i x^k\beta}\mathrm{d}x\right)^s\mathrm{d}\beta\right)}_{(\star\star)} + O(M^{s-k-1+5\delta}).$$

We notice that in the conclusion of Exercise W6, we have crucially separated the "discrete part" from the "continuous part" in the main term. Specifically, $(\star)$ is a sum over rationals a/q, and $(\star\star)$ is an integral that is completely independent of a and q. What we would now like to do is to separate or eliminate most if not all of the dependence on N in these terms.

For starters, the outer upper limit of summation in $(\star)$, certainly depends on N. What would be the error in extending the sum in q out to infinity? Applying Lemma W6 with $\alpha = a/q$, $x = q$, and sufficiently small ϵ, we see that

$$G(a,q) \ll q^{1-(2^{k-1}+1/8)^{-1}}. \tag{23}$$

In fact it is true that $G(a,q) \ll q^{1-1/k}$, and we may refer to this estimate later, but once again we will just stick to what we need for now. In particular, if $s > 2^k$, then (23) yields

$$(q^{-1}G(a,q))^s \ll q^{-(2^k+1)/(2^{k-1}+1/8)} \leq q^{-2-\frac{3}{4(2^{k-1}+1/8)}} \leq q^{-2-2^{-k}}. \tag{24}$$

Applying (24) and the triangle inequality yields

$$\begin{aligned}
\left| \sum_{q>M^\delta} \sum_{\substack{0\leq a\leq q-1 \\ \gcd(a,q)=1}} (q^{-1}G(a,q))^s e^{-2\pi \mathrm{i} Na/q} \right| &\leq \sum_{q>M^\delta} \sum_{\substack{0\leq a\leq q-1 \\ \gcd(a,q)=1}} \left|q^{-1}G(a,q)\right|^s \\
&\ll \sum_{q>M^\delta} \sum_{\substack{0\leq a\leq q-1 \\ \gcd(a,q)=1}} q^{-2-2^{-k}} \\
&\leq \sum_{q>M^\delta} q^{-1-2^{-k}} \\
&\ll \int_{M^\delta}^{\infty} x^{-1-2^{-k}} \mathrm{d}x \\
&\ll M^{-\delta/2^k},
\end{aligned}$$

where the second to last inequality is a standard comparison between an infinite series and an integral. From this bound on the tail of the sum in q, we conclude that

$$(\star) = \mathfrak{S}(N) + O(M^{-\delta/2^k}), \tag{25}$$

where

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{\substack{0\leq a\leq q-1 \\ \gcd(a,q)=1}} (q^{-1}G(a,q))^s e^{-2\pi \mathrm{i} Na/q}. \tag{26}$$

For the integral $(\star\star)$, we recall that $M^k = N$ and apply two successive substitutions $y = N\beta$ and $\xi = x/M$ to yield

$$\int_{-M^{\delta-k}}^{M^{\delta-k}} e^{-2\pi \mathrm{i} N\beta} \left(\int_0^M e^{2\pi \mathrm{i} x^k \beta} \mathrm{d}x \right)^s \mathrm{d}\beta = M^{-k} \int_{-M^\delta}^{M^\delta} e^{-2\pi \mathrm{i} y} \left(\int_0^M e^{2\pi \mathrm{i} x^k y/M^k} \mathrm{d}x \right)^s \mathrm{d}y$$

$$= M^{s-k} \int_{-M^\delta}^{M^\delta} e^{-2\pi \mathrm{i} y} \left(\int_0^1 e^{2\pi \mathrm{i} \xi^k y} \mathrm{d}\xi \right)^s \mathrm{d}y$$

Completely analogous to our treatment of the discrete part, we wish to estimate the error in extending the range of integration in y out to infinity. In other words, we have

$$(\star\star) = J_{s,k} M^{s-k} + O\left(M^{s-k} \int_{|y|>M^\delta} \left| \int_0^1 e^{2\pi \mathrm{i} \xi^k y} \mathrm{d}\xi \right|^s \mathrm{d}y \right), \tag{27}$$

where

$$J_{s,k} = \int_{-\infty}^{\infty} e^{-2\pi \mathrm{i} y} \left(\int_0^1 e^{2\pi \mathrm{i} \xi^k y} \mathrm{d}\xi \right)^s \mathrm{d}y, \tag{28}$$

and we need to bound the integral in the error term of (27). We accomplish this with the following upper bound on the inner integral.

Exercise W 7. Use two successive substitutions to show that

$$\int_0^1 e^{2\pi \mathrm{i} \xi^k y} \mathrm{d}\xi \ll |y|^{-1/k}.$$

You may also need to utilize Dirichlet's criterion, which says that if $f : [a, \infty) \to [0, \infty)$ and $g : [a, \infty) \to \mathbb{C}$ are continuous functions such that $f(t)$ decreases to 0 as $t \to \infty$ and

$$\left| \int_a^b g(t) \mathrm{d}t \right| \leq C$$

for some constant C and all $b > a \in \mathbb{R}$, then every improper integral

$$\int_a^\infty f(t) g(t) \mathrm{d}t$$

converges. If you have not seen this before, it is simply an analog of the "alternating series test" for improper integrals, and it follows from integration by parts.

From the conclusion of Exercise W7, we have that if $s \geq k + 1$, then

$$\left| \int_0^1 e^{2\pi \mathrm{i} \xi^k y} \mathrm{d}\xi \right|^s \ll |y|^{-1-1/k},$$

and hence

$$\int_{|y|>M^\delta} \left| \int_0^1 e^{2\pi \mathrm{i} \xi^k y} \mathrm{d}\xi \right|^s \mathrm{d}y \ll \int_{M^\delta}^\infty y^{-1-1/k} \mathrm{d}y \ll M^{-\delta/k}. \tag{29}$$

Finally, all the pieces can be put together, again recalling that $M = N^{1/k}$.

Exercise W 8. Combine Exercises W4 and W6 with (25), (27), and (29) to conclude that if $s > 2^k$, then

$$r_{s,k}(N) = \mathfrak{S}(N) J_{s,k} N^{\frac{s}{k}-1} + O(N^{\frac{s}{k}-1-\frac{\delta}{k2^k}}). \tag{30}$$

We note that this is a more precise formulation of Theorem 5, provided we can show that $J_{s,k} > 0$ and that $\mathfrak{S}(N)$ is bounded above and below by positive constants independent of N. We address these two issues, respectively, in the next two sections.

10. The Singular Series

We first note that directly from the definition of $\mathfrak{S}(N)$ we have

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} F(q),$$

where

$$F(q) = \sum_{\substack{0 \le a \le q-1 \\ \gcd(a,q)=1}} (q^{-1}G(a,q))^s e^{-2\pi i N a/q}. \tag{31}$$

Exercise W 9. Show that $F(q) \in \mathbb{R}$ for all $q \in \mathbb{N}$ by showing that $F(q) = \overline{F(q)}$.

From (24), we know that if $s > 2^k$, then

$$(q^{-1}G(a,q))^s \ll q^{-2-2^{-k}},$$

hence

$$F(q) \ll q^{-1-2^{-k}}, \tag{32}$$

and in particular $\mathfrak{S}(N)$ is an absolutely convergent series, bounded above independent of N.

To bound $\mathfrak{S}(N)$ from below, we need to investigate $F(q)$ more carefully, and we begin by observing that it is in fact a multiplicative function.

Lemma W 10. *The function $F : \mathbb{N} \to \mathbb{R}$ defined by (31) is multiplicative, meaning that*

$$F(q_1 q_2) = F(q_1)(q_2)$$

whenever $\gcd(q_1, q_2) = 1$.

Proof. Suppose $\gcd(q_1, q_2) = 1$ and let $q = q_1 q_2$. Suppose $\gcd(a, q) = 1$, and let b_1, b_2 be any integers satisfying

$$a = b_1 q_2 + b_2 q_1.$$

We know that such integers exists, and further that all other solutions (x, y) take the form $(b_1 - jq_1, b_2 + jq_2)$ for $j \in \mathbb{Z}$ (this is Theorem 4 from class). In other words, there are unique residue classes $0 \le a_1 \le q_1 - 1$ and $0 \le a_2 \le q_2 - 1$ satisfying

$$a \equiv a_1 q_2 + a_2 q_1 \mod q,$$

and hence

$$\frac{a}{q} = \frac{a_1}{q_1} + \frac{a_2}{q_2} + j \tag{33}$$

for some $j \in \mathbb{Z}$. Further, any common divisor of a_1 and q_1, or of a_2 and q_2, would also be a common divisor of a and q, so we know that $\gcd(a_1, q_1) = \gcd(a_2, q_2) = 1$. Finally, we know that every pair of units (a_1, a_2) will arise in this way, because the number of such pairs is equal to the number of units modulo q by the multiplicative formula for the Euler phi function, which in particular follows from the Chinese Remainder Theorem.

Exercise W 10. Use the decomposition above, along with another decomposition

$$r \equiv r_1 q_2 + r_2 q_1 \mod q$$

to show that if a, q, a_1, q_1, a_2, q_2 are as above, then

$$G(a,q) = \sum_{r=0}^{q-1} e^{2\pi i r^k a/q} = G(a_1,q_1)G(a_2,q_2),$$

where the first equality is just reminding you of the definition.

Ignoring the $j \in \mathbb{Z}$, as the exponentials are 1-periodic, we apply (33) and Exercise W10 to observe

$$\begin{aligned} F(q) &= \sum_{\substack{0\le a\le q-1\\ \gcd(a,q)=1}} (q^{-1}G(a,q))^s e^{-2\pi i N a/q} \\ &= \sum_{\substack{0\le a_1\le q_1-1\\ \gcd(a_1,q_1)=1}} \sum_{\substack{0\le a_2\le q_2-1\\ \gcd(a_2,q_2)=1}} ((q_1q_2)^{-1}G(a_1,q_1)G(a_2q_2))^s e^{-2\pi i N(\frac{a_1}{q_1}+\frac{a_2}{q_2})} \\ &= \left(\sum_{\substack{0\le a_1\le q_1-1\\ \gcd(a_1,q_1)=1}} (q_1^{-1}G(a_1,q_1))^s e^{-2\pi i N a_1/q_1}\right)\left(\sum_{\substack{0\le a_2\le q_2-1\\ \gcd(a_2,q_2)=1}} (q_2^{-1}G(a_2,q_2))^s e^{-2\pi i N a_2/q_2}\right), \end{aligned}$$

which is $F(q_1)F(q_2)$, as required. □

We now exploit the fact that since $\mathfrak{S}(N)$ is an absolutely convergent sum of a multiplicative function, it has an *Euler Product* expansion, the meaning of which is explained by the following lemma.

Lemma W 11 (Euler Product Formula)**.** *If $F : \mathbb{N} \to \mathbb{C}$ is a multiplicative function and $\sum_{q=1}^{\infty} F(q)$ converges absolutely, then*

$$\sum_{q=1}^{\infty} F(q) = \prod_p \left(1 + F(p) + F(p^2) + \cdots\right), \tag{34}$$

where the product is taken over all primes.

Proof. We start on the right hand side, noting that the terms that occur in the infinite product are precisely all terms of the form $F(p_1^{a_1})F(p_2^{a_2})\cdots F(p_\ell^{a_\ell})$ with $a_i \ge 0$. Since F is multiplicative, this product equals $F(p_1^{a_1}\cdots p_\ell^{a_\ell})$, and by the fundamental theorem of arithmetic, each $q \in \mathbb{N}$ is accounted for as one of these products of prime powers in exactly one way. Finally, because the series is absolutely convergent, the ordering of the terms does not matter, and the lemma follows. □

Using the following standard connection between infinite series and infinite products, we can relate positivity of the Euler product expression for $\mathfrak{S}(N)$ with the convergence of a particular infinite series.

Lemma W 12. *If $\{a_n\}$ is a sequence of real numbers with $1 + a_n > 0$, then $\prod_{n=1}^{\infty}(1+a_n)$ is convergent and positive provided $\sum_{n=1}^{\infty} a_n$ converges absolutely.*

Proof. Since $1 + a_n > 0$, we can take the logarithm of the product to get

$$\log\left(\prod_{n=1}^{\infty}(1+a_n)\right) = \sum_{n=1}^{\infty}\log(1+a_n).$$

Further, we know that

$$\lim_{x\to 0}\frac{\log(1+x)}{x} = 1,$$

so the two series

$$\sum_{n=1}^{\infty}|a_n| \quad \text{and} \quad \sum_{n=1}^{\infty}|\log(1+a_n)|$$

either both converge or both diverge by the limit comparison test. In particular, if $\sum_{n=1}^{\infty} a_n$ converges absolutely, then the product converges and

$$0 < e^{-\sum_{n=1}^{\infty}|\log(1+a_n)|} \leq \prod_{n=1}^{\infty}(1+a_n) \leq e^{\sum_{n=1}^{\infty}|\log(1+a_n)|} < \infty.$$

□

Letting

$$T(p) = F(p) + F(p^2) + \cdots = \sum_{j=1}^{\infty} F(p^j), \tag{35}$$

for prime p, where F is as defined in (31), we have from (32) and the geometric series formula that

$$|T(p)| \ll p^{-1-2^{-k}} + (p^{-1-2^{-k}})^2 + \cdots = \frac{p^{-1-2^{-k}}}{1-p^{-1-2^{-k}}} = \frac{1}{p^{1+2^{-k}}-1}. \tag{36}$$

Since

$$\sum_{p}\frac{1}{p^{1+2^{-k}}-1} \leq \sum_{n=1}^{\infty}\frac{1}{n^{1+2^{-k}}-1} < \infty,$$

we know that $\sum_p |T(p)|$ converges with each term in the sum bounded independent of N.

With this observation, we can apply Lemma W11 and Lemma W12 to reduce our task significantly. Specifically, noting that

$$\mathfrak{S}(N) = \prod_{p}(1+T(p)),$$

we have proven the following:

Lemma W 13. *Suppose $s > 2^k$ and T is as defined in (35). If there exists a constant $c > 0$ with*

$$1 + T(p) > c$$

for all primes p and all $N \in \mathbb{N}$, then there exists a constant $c' > 0$ with

$$\mathfrak{S}(N) > c'$$

for all $N \in \mathbb{N}$.

In particular, Lemma W13 follows from applying Lemma W12 with $a_p = \inf_{n\in\mathbb{N}} T(p)$, and letting $c' = \prod_p(1+a_p)$.

Lemma W 14 (Chapter 6, [1]). *If p is prime, $j \in \mathbb{N}$, and $p \nmid a$, then*

$$|G(a, p^j)| \leq \begin{cases} (\gcd(p-1,k)-1)p^{1/2} & \text{if } j = 1 \\ p^{j-1} & \text{if } 2 \leq j \leq k \\ p^{j(1-1/k)} & \text{if } j > k \end{cases}. \tag{37}$$

11. The Singular Integral

References

[1] H. Davenport, *Analytic methods for diophantine equations and diophantine intequalities*, Cambridge University Press, Second Edition, 2005.

[2] N. Lyall, *The Weyl inequality and quadratic polynomials.*

[3] R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge University Press, Second Edition, 1997.