Arithmetic Structure in Difference Sets

Julia Wolf

May 2003

Contents

1 Introduction

Much of this essay is based on the so-called Hardy-Littlewood method, which was developed by the distinguished English mathematicians G.H. Hardy and J.E. Littlewood in the early decades of the last century in order to estimate certain exponential sums. Using their method, they proved an asymptotic formula for the number of representations of an integer N as the sum of s kth powers in 1920, and thereby gave a rigorous formulation to a statement made in 1770 by Edward Waring, who claimed that 'every number is expressible as the sum of four squares, nine cubes, nineteen biquadrates and so on...'.

The Hardy-Littlewood or 'circle' method as it is often called, is a very powerful tool in analytic number theory with numerous applications and thus deserves our attention in its own right. We shall cover the asymptotic solution to Waring's Problem in almost full generality, but will ultimately be concerned with finding an estimate for the number of ways in which an integer can be expressed as the sum of six squares. The main aim of this essay is to prove a result concerning the arithmetic structure of sets of integers, and we shall see how the estimates obtained by the circle method will come in useful.

More precisely, we shall show that provided a set $A \subset \{1, ..., N\}$ has sufficiently large density, it contains two elements whose difference is a perfect square. This was first proved by Sárközy [S78a], but his argument is rather convoluted and we shall follow a much more transparent approach due to Green [Gre02].

In order to obtain Sárközy's Theorem in a fairly straightforward manner, we shall need to introduce the basic notions of Fourier analysis on finite Abelian groups. This rather heavy heading should not deter anyone from reading this essay as there is no advanced analysis involved, nor any abstract group theory. We shall simply be manipulating finite exponential sums.

In the final chapter we shall then attempt to adapt the Hardy-Littlewood method to prove that a sufficiently dense subset of $\{1, ..., N\}$ contains two distinct elements whose difference is a perfect square minus one. This variation on the main theorem was hinted at by Sárközy himself in [S78b], although he did not give an explicit proof. The one we present here is based on ideas of Green and will follow on nicely from our treatment of the Hardy-Littlewood method and Sárközy's theorem in the preceding chapters.

2 Waring's Problem

As mentioned in the introduction, the Hardy-Littlewood method has a range of applications in additive number theory. An example that has been of longstanding interest to mathematicians is Goldbach's problem. In a letter to Euler in 1742, Goldbach conjectured that every even number can be written as the sum of two primes. This remains unproved to date, although Hardy and Littelwood managed to show that the result is true for 'almost all' even numbers, where 'almost all' has a rigorous mathematical interpretation. The interested reader is referred to [V81].

One of the most famous problems to which the Hardy-Littlewood method can be applied is without doubt Waring's problem. Because of its relative simplicity it illustrates the main features of the method exceptionally well. In this chapter we shall give a brief historical introduction to Waring's problem for general s and k.

Let $r_{k,s}(N)$ denote the number of representations of N as the sum of s kth powers, i.e. the number of ordered s-tuples $(x_1, ..., x_s)$ such that $N = x_1^k + ... + x_s^k$, where we require $x_i > 0 \; \forall \; 1 \leq i \leq s$. Waring's Problem as stated in his *Meditationes Algebraicae* in 1770 was to show that, given any natural number k, there exists a natural number s such that $r_{k,s}(N) > 0$ for all sufficiently large N. This assertion was first proved by Hilbert in 1909 [Hi09]. In 1919 Hardy and Littlewood not only gave a different proof of this conjecture [HaLi19], they also established the following explicit asymptotic formula:

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

where Γ denotes the gamma function and $\mathfrak{S}$ is a real arithmetic function. In Hardy and Littlewood's original presentation of their method, they used the generating function $f(z)^s = \left(\sum_{n=0}^{\infty} z^{n^k}\right)^s$ $= \sum_{n=0}^{\infty} r_{k,s}(n)\, z^n$ and then expressed $r_{k,s}(N)$ in terms of this function using Cauchy's Integral formula, i.e.

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

where the integration runs over a circle of radius less than one (hence the name 'circle method'). Replacing power series by finite exponential sums, Vinogradov introduced an important technical simplification in 1928, and it would probably be more than justified to associate his name with the method in question. Indeed, we shall follow his approach in the remainder of this essay.
Let $e(t) = e^{2\pi i t}$, and write

$$T(\alpha) = \sum_{x=0}^{P} e\left(\alpha x^k\right)$$

where $P > 0$ is an integer and $T(\alpha)$ is understood to be a function of k and P.
Setting $P = \left\lfloor N^{1/k} \right\rfloor$, this yields

$$\begin{aligned}\int_0^1 T(\alpha)^s\, e(-\alpha N)\; d\alpha &= \int_0^1 \left(\sum_{x=0}^{P} e\left(\alpha x^k\right)\right)^s e(-\alpha N)\; d\alpha \\ &= \int_0^1 \sum_{x_1,...,x_s}^{P} e\left(\alpha\left(x_1^k + ... + x_s^k - N\right)\right)\; d\alpha\end{aligned}$$

It follows from the orthogonality relation $\int_0^1 e(m\alpha)\, e(-n\alpha)\, d\alpha = 1$ if $m = n$ and 0 otherwise, that

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

We observe that we have turned the number-theoretic problem of finding the number of representations of N as the sum of s kth powers into the analytic problem of evaluating the integral $\int_0^1 T(\alpha)^s\, e(-\alpha N)\; d\alpha$, or at the very least finding an asymptotic expansion for it.

3 Exponential Sum Estimates

Weyl's Inequality and Hua's Lemma, which we shall establish in this chapter, are indispensable analytic tools for a large number of number theoretic problems. They both concern exponential sums, and as such turn out to be invaluable when we start dealing with these objects in large quantities in our attempts to estimate (1). Both Vaughan [V81] and Nathanson [N96a] are good references for the topics covered in this chapter. However, I found the former rather too condensed while the latter shows a tendency to dwell on rather elementary points.

3.1 Difference Operators

For any function $f : \mathbb{R} \to \mathbb{C}$, define the *forward difference operator* $\Delta_h(f)$ by

$$\Delta_h(f)(x) = f(x+h) - f(x)$$

where $h \in \mathbb{R}$. Note that this operator is linear.
For $l \geq 2$, define the *iterated forward difference operator* $\Delta_{h_l,h_{l-1},...,h_1}$ by

$$\Delta_{h_l,h_{l-1},...,h_1} = \Delta_{h_l} \circ \Delta_{h_{l-1},...,h_1} = \Delta_{h_l} \circ ... \circ \Delta_{h_1}$$

Why would these operators be useful in the context of Waring's problem? As can be guessed from the introduction, we shall end up wanting to estimate the absolute value of exponential sums of the form

$$S(f) = \sum_{x=1}^{P} e(f(x)) \tag{2}$$

where f is a polynomial. For the moment let us assume for simplicity that its degree is 2, i.e. $f(x) = ax^2 + bx + c$. Squaring the modulus of (2) yields

$$|S(f)|^2 = \sum_{x=1}^{P}\sum_{y=1}^{P} e\left(a\left(x^2-y^2\right)+b(x-y)\right) = \sum_{x=1}^{P}\sum_{h=1-x}^{P-x} e\left(2axh+ah^2+bh\right) = \sum_{x=1}^{P}\sum_{h=1-x}^{P-x} e\left(\Delta_h f(x)\right)$$

Note that the degree of the poynomial in the exponent has been decreased by one, and in the case of squares we could now sum the geometric series over x. It turns out that this approach generalises to higher powers.
Indeed, by induction on l, it is straightforward to show that

$$\Delta_{h_l,...,h_1}\left(x^k\right) = \sum_{\substack{j_1+...+j_l+j=k \\ j\geq 0, j_1,...,j_l \geq 1}} \frac{k!}{j!j_1!...j_l!} h_1^{j_1}...h_l^{j_l} x^j \tag{3}$$

This can be rewritten as

$$\Delta_{h_l,...,h_1}\left(x^k\right) = h_1...h_l p_{k-l}(x) \tag{4}$$

where $p_{k-l}(x)$ is a polynomial of degree $k-l$ and leading coefficient $\frac{k!}{(k-l)!}$. Notice that when $h_1, ..., h_l$ are integers, then p_{k-l} is a polynomial with integer coefficients.
In particular,

$$\Delta_{h_{k-1},...,h_1}\left(x^k\right) = h_1...h_{k-1}k!\left(x + \frac{h_1+...+h_{k-1}}{2}\right) \tag{5}$$

Lemma 1. *Let $f(x)$ be a polynomial of degree k with leading coefficient $\alpha \in \mathbb{R}$. If $1 \leq l \leq k$, then*

$$\Delta_{h_l,...,h_1}(f)(x) = h_1...h_l \frac{k!}{(k-l)!}\alpha x^{k-l} + ...$$

and if $l > k$, then

$$\Delta_{h_l,...,h_1}(f)(x) = 0$$

In particular, if $l = k-1$, then

$$\Delta_{h_{k-1},...,h_1}(f)(x) = h_1...h_l k!\alpha x + c$$

some $c \in \mathbb{R}$.

Proof. This follows at once from the above observations and the linearity of Δ. □

The following additional observation will be needed in the proof of Hua's Lemma.

Lemma 2. *Let $1 \leq l \leq k$. Suppose $h_1, ..., h_l$ and x are all at most P in modulus. Then $\Delta_{h_l,...,h_1}\left(x^k\right) \ll_k P^k$.*

Proof.

$$\left|\Delta_{h_l,...,h_1}\left(x^k\right)\right| \leq \sum_{\substack{j_1+...+j_l+j=k \\ j\geq 0, j_1,...,j_l \geq 1}} \frac{k!}{j!j_1!...j_l!}P^{j_1+...+j_l+j} \leq \sum_{\substack{j_1+...+j_l+j=k \\ j,j_1,...,j_l \geq 0}} \frac{k!}{j!j_1!...j_l!}P^k \leq (l+1)^k P^k$$

and the result follows. □

3.2 Fractional Parts

We shall see that exponential sums of the form (2), or indeed higher order ones, exhibit a different behaviour according to whether the highest coefficient of the poynomial is close to a rational with small denominator or not. To see roughly why this is the case, consider $\alpha = 1/3$. In this case the sum will be pretty large because lots of the individual terms 'point' in the same direction, whereas if α is 'very' irrational they are all over the place and the sum will be small. Our attempt to make this intuitive notion rigorous serves as a justification for this short section, in which we shall discover the connection between the rational approximation of α and its fractional part.
Let $\{\alpha\}$ denote the *fractional part* of α, i.e. $\alpha = \lfloor \alpha \rfloor + \{\alpha\}$ with $\{\alpha\} \in [0,1)$. Let $\|\alpha\|$ denote the distance of the real number α to the nearest integer. Note that $\|\alpha\| \in [0, \frac{1}{2}]$. We shall also make ample use of Vinogradov's notation and take $A \ll B$ to mean $A = O(B)$. The symbol $\ll_k$ indicates a dependence of the implied constant on k.

Lemma 3. *Let $\alpha \in \mathbb{R}$ and let $Q < P \in \mathbb{N}$. Then*

$$\sum_{x=Q}^{P} e(\alpha x) \ll \min\left\{P - Q + 1, \frac{1}{2\|\alpha\|}\right\}$$

Proof. The bound $P - Q + 1$ is trivial. Suppose α is not an integer, so $\|\alpha\| > 0$ and $e(\alpha) \neq 1$. Summing the geometric progression, we obtain

$$\left|\sum_{x=N}^{P} e(\alpha x)\right| = \left|\frac{e(\alpha N) - e(\alpha(P+1))}{e(\alpha) - 1}\right| = \left|\frac{e(\alpha(N-P-1))}{e(\alpha) - 1}\right| \leq \frac{2}{|e(\alpha) - 1|} = \frac{1}{\sin \pi \|\alpha\|}$$

which implies the result, since for $\beta \in \left(0, \frac{1}{2}\right)$ we have $2\beta < \sin \pi\beta \ (< \pi\beta)$. □

Lemma 4. *Let α be a real number and let a, q be integers with $(a, q) = 1$ such that $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$. Then*

$$\sum_{1 \leq r \leq q/2} \frac{1}{\|\alpha r\|} \ll q \log q$$

Proof. If $q = 1$, $\sum_{1 \leq r \leq q/2} \frac{1}{\|\alpha r\|} = 0$. Hence assume without loss of generality that $q \geq 2$.
For each integer r, there exist integers $s(r) \in [0, \frac{q}{2}]$ and $m(r)$ such that

$$\left\|\frac{ar}{q}\right\| = \frac{s(r)}{q} = \pm\left(\frac{ar}{q} - m(r)\right)$$

Notice that $(a, q) = 1$ implies that $s(r) = 0 \Leftrightarrow r \equiv 0 \mod q$, so $s(r) \in [1, \frac{q}{2}]$ if $r \in [1, \frac{q}{2}]$.
Let $-1 \leq \theta \leq 1$ satisfy $\alpha - \frac{a}{q} = \frac{\theta}{q^2}$. Then

$$\|\alpha r\| = \left\|\frac{ar}{q} + \frac{\theta r}{q^2}\right\| = \left\|m(r) \pm \frac{s(r)}{q} + \frac{\theta r}{q^2}\right\| = \left\|\frac{s(r)}{q} \pm \frac{\theta r}{q^2}\right\| \geq \left\|\frac{s(r)}{q}\right\| - \left\|\frac{\theta r}{q^2}\right\| \geq \frac{s(r)}{q} - \frac{1}{2q}$$

as $\left|\frac{\theta r}{q^2}\right| \leq \frac{|\theta|}{2q} \leq \frac{1}{2q}$.
Since $(a, q) = 1$ we have $s(r_1) = s(r_2) \Leftrightarrow r_1 = r_2$, and it follows that

$$\sum_{1 \leq r \leq q/2} \frac{1}{\|\alpha r\|} \leq \sum_{1 \leq r \leq q/2} \frac{1}{\frac{s(r)}{q} - \frac{1}{2q}} = \sum_{1 \leq s \leq q/2} \frac{1}{\frac{s}{q} - \frac{1}{2q}} \leq 2q \sum_{1 \leq s \leq q/2} \frac{1}{s} \ll q \log q$$

as desired. □

Lemma 5. *Let V be a non-negative real number and let α be an integer with rational approximation $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$, where $q \geq 1, (a, q) = 1$. Then for any non-negative integer h, we have*

$$\sum_{r=1}^{q} \min\left\{V, \frac{1}{\|\alpha(hq + r)\|}\right\} \ll V + q \log q$$

Proof. As in the proof of the previous Lemma, let $\alpha = \frac{a}{q} + \frac{\theta}{q^2}$. Then

$$\alpha(hq+r) = ah + \frac{ar + \lfloor \theta h \rfloor + \delta(r)}{q}$$

where $-1 \leq \delta(r) = \{\theta h\} + \frac{\theta r}{q} < 2$. Clearly, for each $r = 1, ..., q$, there exists a unique $r' \in \mathbb{Z}$ such that

$$\{\alpha(hq+r)\} = \frac{ar + \lfloor \theta h \rfloor + \delta(r)}{q} - r'$$

and it is not hard to see that this implies that $ar - qr'$ lies in the half-open interval $(qt - \lfloor \theta h \rfloor - 2, qt - \lfloor \theta h \rfloor + 2]$. Thus for any $t \in [0, 1 - \frac{1}{q}]$, there are ≤ 4 integers $r \in [1, q]$ such that $\{\alpha(hq+r)\} \in [t, t + \frac{1}{q}]$. We also observe that

$$\|\alpha(hq+r)\| \in [t, t+\frac{1}{q}] \Leftrightarrow \text{ either } \{\alpha(hq+r)\} \in [t, t+\frac{1}{q}] \text{ or } \{\alpha(hq+r)\} \in [t', t'+\frac{1}{q}]$$

where $t' = 1 - \frac{1}{q} - t \in [0, 1 - \frac{1}{q}]$. We conclude that for any $t \in [0, 1 - \frac{1}{q}]$, there are ≤ 8 integers $r \in [1, q]$ such that $\|\alpha(hq+r)\| \in [t, t + \frac{1}{q}]$.
Hence, if $\|\alpha(hq+r)\| \in [0, \frac{1}{q}]$, we use $\min\left\{V, \frac{1}{\|\alpha(hq+r)\|}\right\} \leq V$, and if $\|\alpha(hq+r)\| \in [s, s + \frac{1}{q}]$ for some integer $s \geq 1$, we use $\min\left\{V, \frac{1}{\|\alpha(hq+r)\|}\right\} \leq \frac{1}{\|\alpha(hq+r)\|}$. Thus

$$\sum_{r=1}^{q} \min\left\{V, \frac{1}{\|\alpha(hq+r)\|}\right\} \leq 8V + 8 \sum_{1 \leq s \leq q/2} \frac{q}{s} \ll V + \log q$$

□

Lemma 6. *Let U, V be positive real numbers and let α be a real number with rational approximation as above. Then*

$$\sum_{x=1}^{U} \min\left\{V, \frac{1}{\|\alpha x\|}\right\} \ll \left(q + U + V + \frac{UV}{q}\right) \max\{1, \log q\}$$

Proof. We have

$$\begin{aligned} \sum_{x=1}^{U} \min\left\{V, \frac{1}{\|\alpha q\|}\right\} &\leq \sum_{0 \leq h \leq U/q} \sum_{r=1}^{q} \min\left\{V, \frac{1}{\|\alpha(hq+r)\|}\right\} \\ &\ll \left(\frac{U}{q} + 1\right)(V + q \log q) \end{aligned}$$

and the last term can easily be expressed in the required form. □

3.3 Weyl's Inequality and Hua's Lemma

The following Lemma is the key step in the proof of both Weyl's Inequality and Hua's Lemma, so it is worth our while stating it explicitly.

Key Lemma. *Let f be an arbitrary arithmetic function and let $S(f)$ be the exponential sum $S(f) = \sum_{x=1}^{P} e(f(x))$. Then*

$$|S(f)|^{2^j} \leq (2P)^{2^j-j-1} \sum_{|h_1|,\ldots,|h_j|<P} S_j$$

where

$$S_j = \sum_{x \in I_j} e\left(\Delta_{h_j,\ldots,h_1}(f)(x)\right)$$

and the intervals $I_j = I_j(h_1,\ldots,h_j)$ satisfy $I_1(h_1) \subset [1,P]$ and $I_j(h_1,\ldots,h_j) \subset I_{j-1}(h_1,\ldots,h_{j-1})$.

Proof. We proceed by induction on j. First consider the case $j = 1$. Clearly,

$$|S(f)|^2 = \sum_{x=1}^{P}\sum_{y=1}^{P} e(f(y) - f(x)) = \sum_{x=1}^{P}\sum_{h_1=1-x}^{P-x} e(\Delta_{h_1}(f(x))) = \sum_{h_1=1-P}^{P-1}\sum_{x \in I_1} e(\Delta_{h_1}(f(x)))$$

where $I_1 = [1,P] \cap [1-h_1, P-h_1]$.

Now assume the result for a particular value of j, i.e. suppose that

$$|S(f)|^{2^j} \leq (2P)^{2^j-j-1} \sum_{|h_1|,\ldots,|h_j|<P} S_j$$

Applying the Cauchy-Schwarz Inequality to $\sum S_j 1$, we find that

$$|S(f)|^{2^j} \leq (2P)^{2^j-j-1} \left((2P)^j \sum_{|h_1|,\ldots,|h_j|<P} |S_j|^2\right)^{1/2}$$

so

$$|S(f)|^{2^{j+1}} \leq (2P)^{2^{j+1}-2j-2} (2P)^j \sum_{|h_1|,\ldots,|h_j|<P} |S_j|^2$$

where

$$|S_j|^2 = \sum_{|h|<P}\sum_{x \in I_{j+1}} e\left(\Delta_{h_j,\ldots,h_1}(f)(x+h) - \Delta_{h_j,\ldots,h_1}(f)(x)\right) = \sum_{|h|<P}\sum_{x \in I_{j+1}} e\left(\Delta_{h,h_j,\ldots,h_1}(f)(x)\right)$$

and $I_{j+1} = I_j \cap \{x : x+h \in I_j\}$. □

Weyl's Inequality (1916). *Let $f(x)$ be a real polynomial of degree k with leading coefficient α, i.e. $f(x) = \alpha x^k + \dots$. Suppose that α has a rational approximation $\frac{a}{q}$ satisfying $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$ and $(a,q) = 1$, $q \geq 1$.*
Then for any $\epsilon > 0$, we have

$$|S(f)| = \left|\sum_{x=1}^{P} e(f(x))\right| \ll_{k,\epsilon} P^{1+\epsilon}\left(P^{-1/K} + q^{-1/K} + \left(\frac{P^k}{q}\right)^{-1/K}\right)$$

where $K = 2^{k-1}$.

Proof. Observe that the result is trivial when $q > P^k$. Thus we may assume without loss of generality that $1 \leq q \leq P^k$.
By the Key Lemma and Lemma 1 on difference operators, we have

$$|S(f)|^K \leq (2P)^{K-k} \sum_{|h_1|,\dots,|h_{k-1}|<P} \sum_{x \in I_{k-1}} e(h_1 \dots h_{k-1} k! \alpha x + c)$$

Note that the terms with $h_1 \dots h_{k-1} = 0$ contribute $\ll P^{k-1}$ to the total sum. Hence by Lemma 6,

$$\begin{aligned}
|S(f)|^K &\ll (2P)^{K-k}\left(P^{k-1} + P^{\epsilon}\right) \sum_{h=1}^{k!P^{k-1}} \min\left\{P, \frac{1}{\|\alpha h\|}\right\} \\
&\ll P^{K-k}\left(P^{k-1} + P^{\epsilon}\left(q + k!P^{k-1} + P + \frac{k!P^k}{q}\right)\max\{1, \log q\}\right) \\
&\ll P^{K-k}\left(P^{k-1} + P^{2\epsilon}\left(q + P^{k-1} + \frac{P^k}{q}\right)\right) \\
&\ll P^{K-k}P^{k+2\epsilon}\left(qP^{-k} + P^{-1} + q^{-1}\right)
\end{aligned}$$

so that

$$|S(f)| \ll_{k,\epsilon} P^{1+\epsilon}\left(qP^{-k} + P^{-1} + q^{-1}\right)^{1/K} \ll_{k,\epsilon} P^{1+\epsilon}\left(\left(\frac{P^k}{q}\right)^{-1/K} + P^{-1/K} + q^{-1/K}\right)$$

□

Corollary 1. *Set $S_{a,q} = \sum_{x=1}^{q} e\left(\frac{a}{q}x^k\right)$, where $(a,q) = 1$ and $q \geq 1$. Then*

$$|S_{a,q}| \ll q^{1-1/K+\epsilon}$$

Proof. This is immediate from Weyl's Inequality upon setting $P = q$. □

Hua's Inequality (1938). *Suppose* $1 \leq j \leq k$, *and let* $T(\alpha) = \sum_{x=1}^{P} e\left(\alpha x^k\right)$. *Then*

$$\int_0^1 |T(\alpha)|^{2^j} d\alpha \ll_{k,\epsilon} P^{2^j - j + \epsilon}$$

for any fixed $\epsilon > 0$.

Proof. We proceed by induction on j. The case $j = 1$ is trivial since we observe that

$$\int_0^1 |T(\alpha)|^2 d\alpha = \sum_{x=1}^{P} \sum_{y=1}^{P} \int_0^1 e\left(\alpha\left(x^k - y^k\right)\right) d\alpha = P$$

Suppose the result holds for some j with $1 \leq j \leq k-1$. By the Key Lemma with $f(x) = \alpha x^k$, we have

$$|T(\alpha)|^{2^j} \leq (2P)^{2^j - j - 1} \sum_{|h_1|,\ldots,|h_j| < P} \sum_{x \in I_j} e\left(\alpha h_1 \ldots h_j p_{k-j}(x)\right)$$

where $p_{k-j}(x)$ is a polynomial in x of degree $k-j$ with integer coefficients.
Hence

$$|T(\alpha)|^{2^j} \ll (2P)^{2^j - j - 1} \sum_h c_h e(\alpha h)$$

where c_h is the number of solutions to the equation $h_1 \ldots h_j p_{k-j}(x; h_1, \ldots, h_j) = h$ with $|h_i| < P$ and $x \in I_j$. It is not hard to see that $c_0 \ll P^j$, and using Lemma 2 we find that $c_h \ll P^\epsilon$ for $h \neq 0$ since the number of divisors $d(h)$ of h satisfies $d(h) \ll_\epsilon h^\epsilon$ (see for example [N00]).
Writing $|T(\alpha)|^{2^j} = |T(\alpha)|^{2^{j-1}} |T(\alpha)|^{2^{j-1}}$ we also obtain an expression

$$|T(\alpha)|^{2^j} = \sum_h b_h e(-\alpha h) \tag{6}$$

where b_h is the number of solutions to the equation $x_1^k + \ldots + x_{j-1}^k - y_1^k - \ldots - y_{j-1}^k = h$ with $x_i, y_i < P$. We observe that $\sum_h b_h = T(0)^{2^j} = P^{2^j}$, and by integrating (6) and substituting the induction hypothesis, we find that $b_0 = \int_0^1 |T(\alpha)|^{2^j} d\alpha \ll P^{2^j - j + \epsilon}$. Finally,

$$\begin{aligned}
\int_0^1 |T(\alpha)|^{2^{j+1}} d\alpha &= \int_0^1 |T(\alpha)|^{2^j} |T(\alpha)|^{2^j} d\alpha \\
&\ll P^{2^j - j - 1} \int_0^1 \sum_h c_h e(\alpha h) \sum_{h'} b_{h'} e(-\alpha h) d\alpha \\
&= P^{2^j - j - 1} \sum_h c_h b_h \\
&\ll P^{2^j - j - 1} P^j P^{2^j - j + \epsilon} + P^{2^j - j - 1} P^\epsilon \sum_{h \neq 0} b_h
\end{aligned}$$

and after applying the above estimates the result follows as stated. □

3.4 Remarks on Exponential Sums

Weyl originially studied exponential sums from a rather different perspective: He was primarily interested in the uniform distribution of sequences. We say that a sequence (x_n) is *uniformly distributed* in the interval $[0,1)$ if and only if the probability of x_n lying within an interval J coincides with the measure of that interval. Weyl's Criterion says that the uniformly distributed sequences (x_n) are exactly those which satisfy $\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}e(mx_n)=0$ for all $m=1,2,....$ We can easily deduce that the fractional part of αn for irrational α is uniformly distributed in the interval [0,1) (this is also known as *Kronecker's Approximation Theorem*, see [Hl84]). Let $x_n=n\alpha$. Since α is irrational, $m\alpha$ is never an integer and we can sum the geometric series $\sum_{n=1}^{N}e(mn\alpha)$ just like in Lemma 3.
It should be remarked that the methods for estimating exponential sums introduced in this chapter are amongst the most primitive ones. More advanced methods were developed by van der Corput and Vinogradov, and an excellent reference is [M94].
Indeed, for large k, Weyl's estimates are far from best possible. It is conjectured (see [M94]) that under the conditions of Weyl's Inequality,

$$|S(f)|=\left|\sum_{x=1}^{P}e(f(x))\right|\ll_{k,\epsilon}P^{1+\epsilon}\left(\frac{1}{q}+\frac{q}{P^k}\right)^{1/k}$$

We see that when $k=2$, this coincides with our estimate, but there is a huge discrepancy when k is large.

4 The Hardy-Littlewood Method

In this section we shall adopt the simplest possible approach to develop the asymptotic formula for the number of representations of an integer N as the sum of s kth powers

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

for $s\geq 2^k+1$. Since we shall exclusively be concerned with the case $s=6,k=2$ in chapters to come, this is no real restriction.
Recall from Chapter 2 that

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

where $T(\alpha)=\sum_{x=1}^{P}e\left(\alpha x^k\right)$ and $P=\left\lfloor N^{1/k}\right\rfloor$.
The great achievement of Hardy and Littlewood was to notice that the integrand shows a significant difference in behaviour according to whether α can or cannot be well approximated by a rational with small denominator. We shall call the set of values of α that can be 'well' approximated by a rational the *major arcs* and the set of α where this is not the case the *minor arcs*.
To make this notion more precise, pick $0<\nu<\frac{1}{5}$ and define for $1\leq q\leq P^{\nu}$, $0\leq a\leq q$ and $(a,q)=1$ the set $\mathfrak{M}_{a,q}$ by

$$\mathfrak{M}_{a,q}=\left\{\alpha\in[0,1]:\left|\alpha-\frac{a}{q}\right|\leq\frac{1}{P^{k-\nu}}\right\}$$

The the *major arcs* are then defined to be the set

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

The set $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$ defines the *minor arcs.*
We notice that the sets $\mathfrak{M}_{a,q}$ are disjoint, for suppose $\alpha \in \mathfrak{M}_{a,q} \cap \mathfrak{M}_{a',q'}$, then

$$\frac{1}{P^{2\nu}} \le \frac{1}{qq'} \le \left|\frac{a}{q} - \frac{a'}{q'}\right| \le \left|\alpha - \frac{a}{q}\right| + \left|\alpha - \frac{a'}{q'}\right| \le \frac{2}{P^{k-\nu}}$$

which is impossible for $P \ge 2$ and $k \ge 2$. It is not hard to see that the measure of the major arcs tends to zero as P tends to infinity and, correspondingly, the measure of the minor arcs tends to one. However, we shall show in the next section that the contribution to the integral from the minor arcs is negligible, while the major arcs, dealt with in the subsequent section, require an asymptotic expansion and contribute the main term in the asymptotic formula.

4.1 The Minor Arcs

Minor Arcs. *For $k \ge 2$ and $s \ge 2^k + 1$, we have*

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

where $\delta_1 > 0$ is a constant depending on k and s only.

Proof. Recall Dirichlet's Theorem on Diophantine approximation, which states that for every $\alpha \in \mathbb{R}$, there exist integers a, q with $1 \le q \le Q$ and $(a,q) = 1$ such that $\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}$. Taking $Q = P^{k-\nu}$, we find that for $\alpha \in \mathfrak{m}$ we must have $q > P^{\nu}$ since otherwise $\alpha \in \mathfrak{M}_{a,q}$ for some a, q. But for $\alpha \in \mathfrak{m}$, i.e. those α whose rational approximation has fairly large denominator, Weyl's Inequality bites and yields

$$\begin{aligned} T(\alpha) &\ll P^{1+\epsilon}\left(P^{-1} + q^{-1} + P^{-k}q\right)^{1/K} \\ &\ll P^{1+\epsilon}\left(P^{-1} + P^{-\nu} + P^{-k}P^{k-\nu}\right)^{1/K} \\ &\ll P^{1+\epsilon-\nu/K} \end{aligned}$$

for any positive constant ϵ, where again we have set $K = 2^{k-1}$.
But then by Hua's Lemma we have

$$\begin{aligned} \left|\int_{\mathfrak{m}} T(\alpha)^s e(-\alpha N)\, d\alpha\right| &\le \max_{\alpha \in \mathfrak{m}} |T(\alpha)|^{s-2^k} \int_0^1 |T(\alpha)|^{2^k}\, d\alpha \\ &\ll \left(P^{1+\epsilon-\nu/K}\right)^{s-2^k} P^{2^k-k+\epsilon} \\ &\ll P^{s-k-\delta_1} \end{aligned}$$

where δ_1 is positive provided ϵ was chosen small enough. $\square$

That was nice and easy, and hopefully the reader will agree that Chapter 3 was worth the effort.

4.2 The Major Arcs

The main feature that we will use to estimate the integral over the major arcs is that they are so short that $T(\alpha)$ behaves relatively smoothly on each interval.

Major Arcs I. *For $\alpha \in \mathfrak{M}_{a,q}$, put $\alpha = \frac{a}{q} + \beta$. We then have*

$$T(\alpha) = \frac{1}{q} S_{a,q} v(\beta) + O\left(P^{2\nu}\right) \tag{7}$$

where

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

and

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

Proof. Let $\beta \in \mathbb{R}$ be defined via $\alpha = \frac{a}{q} + \beta$, whence $|\beta| < \frac{1}{P^{k-\nu}}$, and let

$$c_m = \begin{cases} e\left(\frac{a}{q} m\right) - \frac{1}{q} S_{a,q} \frac{1}{k} m^{1/k-1} & \text{where m is a kth power} \\ -\frac{1}{q} S_{a,q} \frac{1}{k} m^{1/k-1} & \text{otherwise} \end{cases} \tag{8}$$

In order to obtain an immediate motivation for making this definition, let us calculate

$$\begin{aligned} \sum_{m \le P^k = N} c_m e(\beta m) &= \sum_{\substack{m \le P^k \\ \text{m a kth power}}} \left(e\left(\frac{a}{q} m\right) - \frac{1}{q} S_{a,q} \frac{1}{k} m^{1/k-1}\right) e(\beta m) \\ &\quad + \sum_{\substack{m \le P^k \\ \text{m not a kth power}}} \left(-\frac{1}{q} S_{a,q} \frac{1}{k} m^{1/k-1}\right) e(\beta m) \\ &= \sum_{m \le P} e\left(\left(\frac{a}{q} + \beta\right) m^k\right) - \frac{1}{q} S_{a,q} v(\beta) \end{aligned}$$

which is exactly the term we wish to estimate.

We make three important observations: By Weyl's Inequality,

$$S_{a,q} = \sum_{x=1}^{q} e\left(\frac{a}{q} x^k\right) \ll q^{1+\epsilon} \left(q^{-1} + q^{-1} + q^{-k} q\right)^{1/K} \ll q^{1-1/K+\epsilon} \tag{9}$$

$$\sum_{m\leq P^k=N} e\left(\frac{a}{q}m^k\right) = \sum_{r=1}^{q} e\left(\frac{a}{q}r^k\right) \sum_{\substack{m\leq P \\ m\equiv r \mod q}} 1 = \frac{P}{q}S_{a,q} + O(q) \tag{10}$$

$$\sum_{m\leq P^k=N} \frac{1}{k}m^{1/k-1} = \int_1^N \frac{1}{k}m^{1/k-1}dm + O(1) = P + O(1) \tag{11}$$

These equations imply that

$$\sum_{m\leq P^k=N} c_m = \sum_{m\leq P} e\left(\frac{a}{q}m^k\right) - \frac{1}{q}S_{a,q}\sum_{m\leq N}\frac{1}{k}m^{1/k-1} = \frac{P}{q}S_{a,q} + O(q) - \frac{S_{a,q}}{q}(P + O(1)) = O(q)$$

But by partial summation, a formula for which can be found in both [V81] (p. 13) and [N96a] (p. 131), we obtain

$$\sum_{m\leq P^k=N} c_m e(\beta m) = e(\beta N)\sum_{m\leq N} c_m - 2\pi i\beta\int_1^N e(\beta\gamma)\sum_{m\leq\gamma} c_m d\gamma \ll q\left(1 + |\beta| P^k\right) \ll P^{2\nu}$$

which proves the Lemma. □

Major Arcs II. *With the same paramenters as above, we have*

$$\int_{\mathfrak{M}} T(\alpha)^s e(-\alpha N)\, d\alpha = P^{s-k}\mathfrak{S}(N, P^\nu)\tilde{J}(N) + O\left(P^{s-k-\delta_2}\right) \tag{12}$$

where $\delta_2 > 0$ depends on ν and k only. Here

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

and

$$\tilde{J}(N) = \int_{|\beta|<P^{\nu-k}} v(\beta)^s e(-\beta N)\, d\beta$$

Proof. For $\alpha\in\mathfrak{M}_{a,q}$, let $\beta = \alpha - \frac{a}{q}$ and $V(\alpha, a, q) = \frac{1}{q}S_{a,q}v(\beta)$, where $S_{a,q}$ and v are defined as above. Then

$$T(\alpha)^s - V(\alpha, a, q)^s = (T(\alpha) - V(\alpha, a, q))\left(T(\alpha)^{s-1} + ... + V(\alpha, a, q)^{s-1}\right) \ll P^{s-1+2\nu}$$

Hence

$$\begin{aligned}\int_{\mathfrak{M}} |T(\alpha)^s - V(\alpha, a, q)^s|\, d\alpha &= \sum_{1\leq q\leq P^\nu}\sum_{\substack{a=1 \\ (a,q)=1}}^{q}\int_{\mathfrak{M}_{a,q}} |T(\alpha)^s - V(\alpha, a, q)^s|\, d\alpha \\ &\ll P^{2\nu}P^{-(\nu-k)}P^{s-1+2\nu} \\ &\ll P^{s-k-\delta_2}\end{aligned}$$

for $\delta_2 > 0$, and we see why we had to choose $0 < \nu < \frac{1}{5}$ in the first place. It follows that

$$\int_{\mathfrak{M}} T(\alpha)^s e(-\alpha N)\, d\alpha = \sum_{1 \le q \le P^\nu} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}_{a,q}} V(\alpha, a, q)^s e(-\alpha N)\, d\alpha + O\left(P^{s-k-\delta_2}\right)$$

but

$$\begin{aligned} \int_{\mathfrak{M}_{a,q}} V(\alpha, a, q)^s e(-\alpha N)\, d\alpha &= \int_{\frac{a}{q}-P^{\nu-k}}^{\frac{a}{q}+P^{\nu-k}} V(\alpha, a, q)^s e(-\alpha N)\, d\alpha \\ &= \int_{-P^{\nu-k}}^{P^{\nu-k}} V\left(\frac{a}{q}+\beta, a, q\right)^s e\left(-\left(\frac{a}{q}+\beta\right)N\right) d\beta \\ &= \left(\frac{S_{a,q}}{q}\right)^s e\left(-\frac{a}{q}N\right) \int_{-P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e(-\beta N)\, d\beta \end{aligned}$$

Summing over all appropriate a and q gives the result. □

Since we shall want to estimate the terms in (12) as precisely as possible, it will be convenient to replace the functions $\tilde{J}$ and $\mathfrak{S}(N, P^\nu)$ by the *singular integral*

$$J(N) = \int_{-1/2}^{1/2} v(\beta)^s e(-\beta N)\, d\beta \tag{13}$$

and the *singular series*

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} A(q) \tag{14}$$

respectively, where

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

4.3 The Singular Integral

As indicated at the end of the last section, we shall attempt to replace the range of integration in $\tilde{J}$ by a unit interval, as this will enable us to evaluate the integral explicitly. Before we can do so, however, we need a good bound on the size of $v(\beta)$ for $|\beta| \le \frac{1}{2}$.

Lemma 7. *For $|\beta| \le \frac{1}{2}$, we have*

$$v(\beta) \ll \min\left\{P, |\beta|^{-1/k}\right\} \tag{15}$$

Proof. We have remarked earlier that

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

so when $|\beta| \leq \frac{1}{N}$ the result follows at once.
Now suppose that $|\beta| > \frac{1}{N}$ and set $W = \left\lfloor \frac{1}{|\beta|} \right\rfloor$. Let $s_m = \sum_{r=1}^{m} e(\beta r)$ and $b_m = \frac{1}{k} m^{1/k-1}$. Note that $|s_m| \leq \frac{1}{2|\beta|}$ (by Lemma 3) and that the sequence b_m is decreasing. Then

$$\begin{aligned}
\sum_{m=1}^{N} \frac{1}{k} m^{1/k-1} e(\beta m) &= \sum_{m=1}^{W} \frac{1}{k} m^{1/k-1} e(\beta m) + \sum_{m=W+1}^{N} \frac{1}{k} m^{1/k-1} e(\beta m) \\
&\ll W^{1/k} + b_{N+1} s_N - b_{W+1} s_W + \sum_{m=W+1}^{N} (b_m - b_{m+1}) s_m \\
&\ll |\beta|^{-1/k} + b_{W+1} |\beta|^{-1} \\
&\ll |\beta|^{-1/k}
\end{aligned}$$

□

Next we shall show that we can replace $\tilde{J}$ by the singular integral J without great losses.

Singular Integral (Lemma). *We have*

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

and

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

for some $\delta_3 > 0$.

Proof.

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

Moreover,

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

where $\delta_3 = \nu\left(\frac{s}{k} - 1\right) > 0$. □

The following technical lemma has been isolated for the purpose of making the proof of the subsequent theorem more transparent.

Lemma 8. *For real numbers c and d with $c \geq d > 0$ and $d \leq 1$ we have*

$$\sum_{m=1}^{N-1} m^{d-1} (N-m)^{c-1} = N^{c+d-1} \frac{\Gamma(c)\Gamma(d)}{\Gamma(c+d)} + O\left(N^{c-1}\right) \tag{16}$$

Proof. Consider the function $g(y) y^{d-1} (N-y)^{c-1}$. On $(0,N)$, g has at most one stationary point, so we can split $(0,N)$ into two intervals $(0,X)$ and (X,N) (one of which may be empty) such that g is monotone on both bits, and then apply a standard result concerning the approximation of sums by integrals:

$$\begin{aligned}
\sum_{m=1}^{N-1} g(m) &= \int_0^N g(y)\, dy + O\left(N^{c-1} + N^{c+d-2}\right) \\
&= \int_0^N y^{d-1} (N-y)^{c-1}\, dy + O\left(N^{c-1} + N^{c+d-2}\right) \\
&= N^{c+d-1} \int_0^1 u^{d-1} (1-u)^{c-1}\, du + O\left(N^{c-1}\right) \\
&= N^{c+d-1} \frac{\Gamma(c)\Gamma(d)}{\Gamma(c+d)} + O\left(N^{c-1}\right)
\end{aligned}$$

□

Singular Integral (Theorem). *For $s \geq 2$,*

$$J(N) = \Gamma\left(1+\frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} N^{s/k-1} + O\left(N^{(s-1)/k-1}\right) \tag{17}$$

Proof. By induction on s. For $s \geq 1$, let $J_s(N) = \int_{-1/2}^{1/2} v(\beta)^s e(-\beta N)\, d\beta$. Note that

$$J_s(N) = \sum_{\substack{m_1=1 \\ m_1+\ldots+m_s=N}}^{N} \ldots \sum_{m_s=1}^{N} \left(\frac{1}{k}\right)^s (m_1 \ldots m_s)^{1/k-1}$$

In the case $j = 2$, the result follows immediately from the above Lemma. Suppose the result holds for some $s \geq 2$.

Then

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

where the last two lines follow from the preceeding lemma, which in this proof facilitates both the first and the general inductive step. □

4.4 The Singular Series

Similarly to the way we proceeded with the singular integral, we first show that we can replace the function $\mathfrak{S}(N, P^\nu)$ by the singular series $\mathfrak{S}(N)$ with relatively small error.

Singular Series (Lemma).

$$\mathfrak{S}(N) = \mathfrak{S}(N, P^\nu) + O\left(P^{-\nu\delta_4}\right)$$

where δ_4 is a positive constant.

Proof. Let $0 < \epsilon < \frac{1}{sK}$ and recall that by Weyl's Inequality $S_{a,q} \ll q^{1-1/K+\epsilon}$. This implies that

$$A(q) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\frac{S_{a,q}}{q}\right)^s e\left(-\frac{a}{q}N\right) \ll \frac{q}{q^{s/K-s\epsilon}} \leq \frac{1}{q^{1+\delta_4}} \tag{18}$$

where $\delta_4 = 1/K - s\epsilon$. Hence

$$\mathfrak{S}(N) - \mathfrak{S}(N, P^\nu) = \sum_{q>P^\nu} A(q) \ll \sum_{q>P^\nu} \frac{1}{q^{1+\delta_4}} \ll P^{-\nu\delta_4}$$

□

We deduce that the singular series converges absolutely and uniformly with respect to N. In particular, there exists a constant $C = C(k, s)$ such that $|\mathfrak{S}(N)| < C$ for all positive integers N. All that remains to show is that $\mathfrak{S}(N)$ is real and positive, and we will have reached the main aim of this section, which is

Singular Series (Theorem). *There exist a positive constant* $C = C(k,s)$ *such that*

$$0 < \mathfrak{S}(N) < C$$

We first show that the function $A(q)$ is multiplicative.

Lemma 9. *Let* $(q,r) = 1$. *Then*

$$S_{a,q}S_{b,r} = S_{ar+bq,qr}$$

Proof. Since every congruence class $\mod qr$ can be written uniquely as $xr + yq$ with $1 \le x \le q$ and $1 \le y \le r$, we can write

$$\begin{aligned}
S_{ar+bq,qr} &= \sum_{m=1}^{qr} e\left(\frac{(ar+bq)}{qr}m^k\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\frac{(ar+bq)(xr+yq)^k}{qr}\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\frac{(ar+bq)}{qr}\left((xr)^k+(yq)^k\right)\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\frac{a}{q}(xr)^k\right)e\left(\frac{b}{r}(yq)^k\right) \\
&= S_{a,q}S_{b,r}
\end{aligned}$$

□

Lemma 10. *Let* $(q,r) = 1$. *Then*

$$A(qr) = A(q)A(r)$$

Proof. If $(c,qr) = 1$, then $c \equiv ar + bq \mod qr$ for some a, b with $(a,q) = (b,r) = 1$. It follows from the preceding lemma that

$$\begin{aligned}
A(qr) &= \sum_{\substack{c=1\\(c,qr)=1}}^{qr}\left(\frac{S_{c,qr}}{qr}\right)^s e\left(-\frac{c}{qr}N\right) \\
&= \sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{\substack{b=1\\(b,r)=1}}^{r}\left(\frac{S_{ar+bq,qr}}{qr}\right)^s e\left(-\frac{(ar+bq)}{qr}N\right) \\
&= \sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{\substack{b=1\\(b,r)=1}}^{r}\left(\frac{S_{a,q}}{q}\right)^s e\left(-\frac{a}{q}N\right)\left(\frac{S_{b,r}}{r}\right)^s e\left(-\frac{b}{r}N\right)
\end{aligned}$$

and the result is immediate. □

Lemma 11. *Let $s \geq 2^k + 1$ and let $M(N,q)$ denote the number of solutions to the congruence $x_1^k + ... + x_s^k \equiv N \mod q$ in integers x_i such that $1 \leq x_i \leq q$ for all $i = 1, ..., s$. Then for every prime p, the series $\chi(N,p) = 1 + \sum_{j=1}^{\infty} A(p^j)$ converges, and*

$$\chi(N,p) = \lim_{j \to \infty} \frac{M(N,p^j)}{p^{j(s-1)}}$$

Proof. The convergence of the series follows from (18). Notice that

$$\begin{aligned}
M(N,q) &= \sum_{x_1=1}^{q} ... \sum_{x_s}^{q} \frac{1}{q} \sum_{a=1}^{q} e\left(\frac{a}{q}\left(x_1^k + ... + x_s^k - N\right)\right) \\
&= \frac{1}{q} \sum_{a=1}^{q} (S_{a,q})^s \, e\left(-\frac{a}{q}N\right) \\
&= \frac{1}{q} \sum_{d|q}^{q} \sum_{\substack{a=1 \\ (a,q)=d}}^{q} (S_{a,q})^s \, e\left(-\frac{a}{q}N\right) \\
&= \frac{1}{q} \sum_{d|q}^{q} \sum_{\substack{a=1 \\ (a,q)=d}}^{q} d^s \left(S_{a/d,q/d}\right)^s e\left(-\frac{a/d}{q/d}N\right) \\
&= \frac{1}{q} \sum_{d|q}^{q} \sum_{\substack{a=1 \\ (a,q)=d}}^{q} q^s \left(\frac{S_{a/d,q/d}}{q/d}\right)^s e\left(-\frac{a/d}{q/d}N\right) \\
&= q^{s-1} \sum_{d|q} A\left(\frac{q}{d}\right)
\end{aligned}$$

In particular,

$$M\left(N,p^j\right) = p^{j(s-1)} \sum_{d|p^j} A\left(\frac{p^j}{d}\right) = p^{j(s-1)} \left(1 + \sum_{h=1}^{j} A\left(p^h\right)\right)$$

so

$$\chi(N,p) = \lim_{j \to \infty} \left(1 + \sum_{h=1}^{j} A\left(p^h\right)\right) = \lim_{j \to \infty} \frac{M\left(N,p^j\right)}{p^{j(s-1)}}$$

□

Proof. (of Theorem) We had already established that $\sum A(q)$ is absolutely convergent (recall (18)) and that $A(q)$ is multiplicative. By standard properties of Euler products (the reader may wish to refer to the appendix of [N96a]) we find that

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

and that the latter product converges. In particular, $\chi(N,p) \neq 0$ for all N and p. But now it follows from Lemma 10 that $\chi(N,p)$ is in fact positive for all N and p. This immediately implies that $\mathfrak{S}(N)$ is positive. We also saw that $\mathfrak{S}(N) \leq \sum_{q=1}^{\infty} \frac{1}{q^{1+\delta_4}}$ (recall again (18)) which completes the proof of the Theorem. □

4.5 The Asymptotic Formula and a Special Case

Putting the results of the previous two sections together, we have shown that

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

where $\mathfrak{S}(N)$ is a bounded, real arithmetic function, and δ a positive constant.
Not much additional work is required to obtain a positive lower bound for $\mathfrak{S}(N)$, but since this is not in our immediate interest the reader is referred to [V81], [N96a] or [Dav62].
It should also be pointed out that the approach outlined in this chapter can be extended to find asymptotic formulae for the number of solutions to more general equations: Here we have considered the equation

$$x_1^k + ... + x_s^k = N$$

but with rather little additional effort one could derive an expression for the number of solutions to

$$c_1x_1^k + ... + c_sx_s^k = N$$

where the c_i are given positive integers. There is no difficulty in prinicple in extending the method to cover more general equations of additive type, say

$$f(x_1) + ... + f(x_s) = N$$

The book by Davenport [Dav62] is highly recommended for further reading.
Another point to note is that for sums of an even number of squares it is in fact possible to sum the singular series directly. We saw that it is sufficient to evaluate $A(q)$ for q a prime power, and that this can be done explicitly is shown in [Gro85]. Although it involves some nice results from analytic number theory (including the Riemann Zeta function), the actual calculations are rather tedious and therefore omitted. The interested reader is referred to Grosswald's book.
One recovers the formula for the number of representations of an integer as the sum of six squares which can be obtained by elementary means using a recursion formula (see [N00]), namely

$$r_{2,6}(n) = 16\sum_{d|n} l\left(\frac{n}{d}\right)d^2 - 4\sum_{d|n} l(d)\,d^2$$

where

$$l(d) = \begin{cases} 1 & d \equiv 1 \mod 4 \\ -1 & d \equiv 3 \mod 4 \\ 0 & \text{otherwise} \end{cases}$$

It is not very hard (again, see [N00]) to obtain an explicit bound on $r_{2,6}(N)$ via this formula. Indeed, one has

$$\frac{3}{2}N^2 \leq r_{2,6}(N) \leq 40N^2$$

For our purposes a less precise estimate suffices. It follows directly from the asymptotic formula and the fact that $\mathfrak{S}(N)$ is bounded above by a constant independently of N that

$$r_{2,6}(N) \ll N^2$$

This will be a crucial ingredient in proving Sárközy's Theorem for Squares in Chapter 6.

5 Introduction to Fourier Analysis on Finite Abelian Groups

Throughout this rather short chapter, we shall consider subsets of $\mathbb{Z}_N$ rather than subsets of $1, 2, ..., N$. The reason is that we shall want to do Fourier analysis on $\mathbb{Z}_N$, which is rather convenient as the Fourier transform will be defined on the same space as the function itself.
Indeed, given a function $f : \mathbb{Z}_N \to \mathbb{C}$ and $r \in \mathbb{Z}_N$, we define the *discrete Fourier transform* of f to be

$$\hat{f}(r) = \sum_{s \in \mathbb{Z}_N} f(s)\, e\left(\frac{rs}{N}\right)$$

where $e(x) = \exp(2\pi i x)$ as before.
Let us also define the *convolution* of two functions f and g, denoted by $f * g$. For $s \in \mathbb{Z}_N$, set

$$(f * g)(s) = \sum_{t \in \mathbb{Z}_N} f(t)\, g(s-t)$$

For convenience we shall henceforth assume that N is a prime, except when explicitly stated otherwise.
By means of elementary manipulation (using the fact that $\sum_{s \in \mathbb{Z}_N} \exp(-2\pi rs/N) = N$ if $r = 0$ and 0 otherwise) we arrive at the following basic identities:

$$\sum_r \left|\hat{f}(r)\right|^2 = N \sum_s |f(s)|^2 \qquad (Plancherel) \tag{19}$$

$$\sum_r \hat{f}(r)\, \overline{\hat{g}(r)} = N \sum_s f(s)\, \overline{g(s)} \qquad (Parseval) \tag{20}$$

$$\widehat{(f * g)}(r) = \hat{f}(r)\, \overline{\hat{g}(r)} \qquad (Convolution) \tag{21}$$

$$f(s) = \frac{1}{N} \sum_r \hat{f}(r)\, e(rs/N) \qquad (Inversion) \tag{22}$$

where all the sums are henceforth taken to be over $\mathbb{Z}_N$. As a brief motivation for why these concepts are useful in the study of number theoretic problems, consider the expression $\sum_r \left|\hat{A}(r)\right|^4$, where we have written A to denote both the set $A \subset \mathbb{Z}_N$ and its characteristic function. We find that

$$\begin{aligned}\sum_r \left|\hat{A}(r)\right|^4 &= \sum_r \hat{A}(r)^2 \hat{A}(-r)^2 \\ &= \sum_r \sum_{x,y,z,w} A(x) A(y) A(z) A(w) e((x+y-z-w) r/N) \\ &= N \sum_{a+b=c+d} A(a) A(b) A(c) A(d) \\ &= N \times \text{number of quadruples in } A \text{ s.t. } a+b=c+d\end{aligned}$$

This simple example shows that from the size of Fourier coefficients we can infer vital information about the additive structure of sets of integers.
Notice that we have just made explicit what we have met in slight disguise before. The reader may wish to recall that in the introduction to Waring's problem we had expressed

$$\begin{aligned}\int_0^1 T(\alpha)^s e(-\alpha N)\ d\alpha &= \int_0^1 \left(\sum_{x=0}^{P} e\left(\alpha x^k\right)\right)^s e(-\alpha N)\ d\alpha \\ &= \int_0^1 \sum_{x_1,\ldots,x_s}^{P} e\left(\alpha\left(x_1^k + \ldots + x_s^k - N\right)\right)\ d\alpha\end{aligned}$$

Here the integration over the interval $[0,1]$ corresponds to the summation over r.
Equipped with this knowledge, we shall now focus our attention on a beautiful application of Fourier analysis to number theory.

6 Sárközy's Theorem for Squares

Without any further preliminaries we state

Sárközy's Theorem for Squares. *Let $A \subset \{1,\ldots,N\}$ have size δN, where $1 \geq \delta > 0$. Then for all $N > N_1(\delta)$, one can find two distinct elements $x, y \in A$ whose difference $x-y$ is a perfect square.*

As indicated in the introduction, this theorem was first proved by Sárközy in [S78a]. Very recently a different and rather more elegant proof was dicovered by Green [Gre02]. Though it does not yield quite as good a bound as Sárközy's orginial proof, it has the advantage of being much shorter and infinitely more transparent. It should be noted that at around the same time as Sárközy, Furstenberg proved the result using ergodic theory. His approach has lead to a large number of generalisations, the only real drawback being that it is impossible to obtain explicit bounds via these methods.

It will be advantageous to have a rough idea of the iteration argument on which Green's proof is based before one gets too involved in the technicalities. The main idea, which is very similar to the one that lies at the heart of the new proof of Szemerédi's Theorem through W.T. Gowers [G01] (which itself is based on Roth's original argument [R53]) is the following: Suppose for contradiction that $A \subset \{1, ..., N\}$ with density α contains no two distinct elements whose difference is a perfect square. (In this case we say $A - A$ is *square-free.*) Set $A_0 = A$, $\alpha_0 = \alpha$ and $N_0 = N$.
At the ith stage of the iteration, we have a set $A_i \subset \{1, ..., N\}$ with density α such that $A_i - A_i$ is square-free. We shall see that this fact together with the upper bound for the number of representations of an integer as the sum of six squares derived in Chapter 4 implies that the characteristic function A_i has rather large Fourier coefficient at some non-zero $r \in \mathbb{Z}_N$. Subsequently a lemma (a proof of which can be found in [G01]; here stated only), enables us to find an arithmetic progression B_i with square common difference d_i^2 on which A_i has increased density. We then pass to that subprogression, i.e. set $A_{i+1} = A_i \cap B_i$, $N_{i+1} = |B_i|$ and $\alpha_{i+1} = \frac{|A_{i+1}|}{N_{i+1}}$. We observe that, fortunately, $A_{i+1} - A_{i+1}$ is also square-free, for if $x, y \in A_{i+1}$ such that $x - y = z^2$, then $d_i^2 x - d_i^2 y = d_i^2 z^2 \in A_i - A_i$.er bo
At each stage we shall obtain a density increment of a certain 'fixed' size (to be determined in the course of the proof). Hence if we could continue in this loop indefinitely, the density of the subset A we are looking at would increase above one, which is clearly nonsense. So we conclude that $A - A$ contained a square in the first place.

Proof. (see [Gre02], *slightly sketched)* For simplicity of notation, we shall drop the index i from the notation used in the above outline of the proof. Let $S = \left\{1, 4, 9, ..., m^2 : m = \left\lfloor \sqrt{\frac{N}{2}} \right\rfloor\right\}$, the set of squares less than $\frac{N}{2}$. Let $C = A \cap [0, \frac{N}{2}]$ and regard S, A and C as subsets of $\mathbb{Z}_N$. We can assume without loss of generality that $|C| \geq \alpha N/2$. Now if $a - a$ is square-free, it is easily seen that

$$\sum_{x,d} A(x)C(x+d)s(d) = 0$$

Applying Parseval's Theorem and the triangle identity, we find that

$$\frac{1}{4}\alpha^2 N^{5/2} \leq \left|\hat{S}(0)\right| \left|\hat{C}(0)\right| \left|\hat{A}(0)\right| \leq \sum_{r \neq 0} \left|\hat{S}(r)\right| \left|\hat{C}(r)\right| \left|\hat{A}(r)\right|$$

and the right-hand side is at most

$$\sup_{r \neq 0} \left|\hat{A}(r)\right|^{1/6} \sum_{r \neq 0} \left|\hat{S}(r)\right| \left|\hat{C}(r)\right| \left|\hat{A}(r)\right|^{5/6}$$

which by a general version of Hölder's Inequality, is at most

$$\sup_{r \neq 0} \left|\hat{A}(r)\right|^{1/6} \left(\sum_r \left|\hat{S}(r)\right|^{12}\right)^{1/12} \left(\sum_r \left|\hat{C}(r)\right|\right)^{1/2} \left(\sum_r \left|\hat{A}(r)\right|^{5/6}\right)^{5/12} \tag{23}$$

The latter two terms look very pleasant already, and we can give a decent estimate for them using Parseval once again, i.e. we have $\sum_r \left|\hat{A}(r)\right|^2$ and $\sum_r \left|\hat{C}(r)\right|^2$ at most αN^2. For the term involving the L^{12}-norm of $\hat{S}$, we observe that

$$\sum_r \left|\hat{S}(r)\right|^{12} = \left\|\hat{S}^6\right\|_2^2 = N \left\|S * ... * S\right\|_2^2 = N \sum_x \left(\sum_{a_1^2+...+a_6^2=x} S(a_1)...S(a_6) \right)^2 = N \sum_x R_{2,6}(x)^2$$

Where $R_{2,6}$ is the number of solutions to the equation $a_1^2 + ... + a_6^2 \equiv x \mod N$. It is not hard to see that $R_{2,6}$ is of the same order of magnitude as $r_{2,6}$, the number of solutions to $a_1^2 + ... + a_6^2 = x$ which we evaluated in Chapter 4. The reader may wish to recall that the bound obtained was a constant times N^2, so we can assert that

$$\sum_r \left|\hat{S}(r)\right|^{12} \leq c^6 N^6 \tag{24}$$

for some absolute constant c. We have thus established that (23) is at most

$$\sup_{r \neq 0} \left|\hat{A}(r)\right|^{1/6} \left(c^6 N^6\right)^{1/12} \left(\alpha N^2\right)^{1/2} \left(\alpha N^2\right)^{5/12}$$

which means there exists an $r \neq 0$ such that

$$\left|\hat{A}(r)\right| \geq \frac{\alpha^{11/2}}{2^{12} c^3} |A| \tag{25}$$

As indicated in the sketch of the proof above, this enables us to find a subprogression with square common difference on which A has increased density.

Here we quote [Gre02] Lemma 8, which states that for $r \in \mathbb{Z}_N$ and $N > 2^{2^{130}}$ there exists a $d \leq N^{1/4}$ such that $|rd^2| \leq N^{127/128}$. Now let $B = \left\{d^2, 2d^2, ..., Ld^2\right\}$, where L is to be determined later. Then

$$\begin{aligned} \left|\hat{B}(r)\right| &\geq L \sup_{x=1,...,L} \left(1 - \left|1 - e(rd^2x/N)\right|\right) \\ &\geq L \left(1 - \frac{2\pi |rd^2| L}{N}\right) \\ &\geq \frac{L}{2} \end{aligned}$$

where the last line can be achieved by setting $L = \left\lfloor \frac{1}{20} N^{1/128} \right\rfloor$. This immediately implies that

$$\begin{aligned} N \sum_x |A \cap (B + x)|^2 &= \sum \left|\hat{A}(r)\right|^2 \left|\hat{B}(r)\right|^2 \\ &\geq \left(1 + \frac{\alpha^{11}}{2^{26} c^6}\right) |A|^2 L^2 \end{aligned}$$

There is one last difficulty we have to overcome, which is a consequence of having translated everything into $\mathbb{Z}_N$: Some of the translates of B will split into smaller subprogressions when we translate things back into $\mathbb{Z}$. Call these values of x 'bad', and since B has diameter at most $N^{2/3}$ there are at most $N^{2/3}$ of them. Thus

$$N \sup_{x \text{ good}} |A \cap (B+x)||A|L \geq \left(1 + \frac{\alpha^{11}}{2^{27}c^6}\right)|A|^2 L^2$$

provided that $\alpha \geq CN^{-1/39}$ for some absolute constant C. We shall see at the end of this iteration argument that this is significantly larger than the lower bound on α we obtain.
We conclude that there is a 'good' x such that

$$|A \cap (B+x)| \geq \left(\alpha + \frac{\alpha^{12}}{2^{27}c^6}\right) L$$

which means that we have found a subprogression $B + x$ with square common difference on which A has increased density. Iterating this argument leads to a lower bound on α of

$$\alpha \geq \frac{c}{(\log\log N)^{1/11}}$$

The (rather messy) details are omitted. □

7 A Variation on Sárközy's Theorem

We would like to adapt the method of proof used in the preceding chapter to prove the corresponding result for a square minus one, i.e. we would like to prove

Sárközy's Theorem for Squares Minus One. *Let $A \subset \{1, ..., N\}$ have size αN, where $1 \geq \alpha > 0$. Then for all $N > N_2(\alpha)$, one can find two distinct elements $x, y \in A$ whose difference $x - y$ is a perfect square minus one.*

This will require a not insignificant modification of the Hardy-Littlewood argument used in the proof of the original theorem.
We first observe that the result would not be true if we replaced 'square minus one' by 'square plus one'. We leave it as an exercise for the reader to check that although the set of multiples of six has large density as a subset of $\{1, ..., N\}$, it does not contain a difference that is a perfect square plus one (consider the set of squares mod 3).
Sárközy alluded to this result in [S78b]. We hope that the new proof given here will be more elegant and easier to understand, in particular when read in conjunction with the intitial chapters of this essay.
In general, it is known that the set of squares may be replaced by the set $\{p(n) : n \in \mathbb{N}\}$, where p

is a polynomial that maps the natural numbers to itself and has an integer root. For an outline of the proof see [S78b].
Before attempting a proof, we need to work out in what important aspects it would have to differ from the one given in the preceding chapter. Most importantly, the iteration argument cannot be carried out in the same way since the rescaling does not work for the square-minus-one case, the '...'-free property is not preserved. It turns out that instead of considering the set of squares minus one, it is a good idea to work with the set

$$S = \left\{ n\left(n+2\right) : n \leq \left\lfloor \sqrt{N} \right\rfloor \right\}$$

which the reader will easily verify to be equivalent to set of squares minus one. Again, we find that A has large Fourier coefficient for some r if we assume that A is free of numbers of the form $n(n+2)$. This time we find a subprogression with common difference q on which A has increased density, where q is the denominator of a rational approximation of $\frac{r}{N}$. However, after rescaling, we find that A is free of numbers of the form $n(qn+2)$. Thus, in general, we shall consider the set

$$S = \left\{ n\left(\lambda n+2\right) : n \leq \left\lfloor \sqrt{\frac{N}{\lambda}} \right\rfloor \right\}$$

where λ is the product of all the qs from previous steps.
This has two important implications: We do not want λ to grow very fast, so we have to place a rather strong restriction on how large q can be. Secondly, it will be harder to establish the corresponding version of the L^{12} estimate, i.e. the bound $\sum_r \left|\hat{S}(r)\right|^{12} \ll N^6$.
We will also have to deal with slightly different exponential sums, and to make life easier for ourselves we shall deal with the technicalities first.

7.1 A Version of Weyl's Inequality

Suppose we are given $\left|\theta - \frac{a}{q}\right| \leq \frac{1}{q^2}$ with $N^\nu < q \leq N^{1-\nu}$ and need an estimate for the absolute value of

$$f\left(\theta\right) = \sum_{x=1}^{M} e\left(\theta\left(\lambda x^2 + 2x\right)\right)$$

This means we need Weyl's Inequality for a non-monic polynomial. Clearly, $\left|\theta\lambda - \frac{a\lambda}{q}\right| \leq \frac{\lambda}{q^2}$, but if we tried to work through the usual proof of Weyl's Inequality we would encounter problems since

$\frac{a\lambda}{q}$ need not always be a proper fraction. However, introducing a 'δ'-function, we can write

$$\begin{aligned}\sum_{x=1}^{M} e\left(\theta\left(\lambda x^2\right)\right) &= \sum_{\substack{u=0 \\ u\equiv 0 \bmod \lambda}}^{\sqrt{\lambda N}} e\left(\frac{\theta}{\lambda}u^2\right) \\ &= \frac{1}{\lambda}\sum_{u=0}^{\sqrt{\lambda N}}\sum_{j=1}^{\lambda} e\left(\frac{j}{\lambda}u\right) e\left(\frac{\theta}{\lambda}u^2\right) \\ &= \frac{1}{\lambda}\sum_{j=1}^{\lambda}\sum_{u=0}^{\sqrt{\lambda N}} e\left(\frac{\theta}{\lambda}u^2 + \frac{j}{\lambda}u\right)\end{aligned}$$

If we now follow through the usual proof of Weyl's Inequality using the fact that $\left\{0, \frac{\theta}{\lambda}, ..., \frac{q}{2}\frac{\theta}{\lambda}\right\}$ are $\frac{1}{2\lambda q}$ separated, we obtain

Lemma 12.

$$|f(\theta)| \leq 16\sqrt{\lambda}\log N N^{1/2-\nu/2} \tag{26}$$

It turns out that this will be good enough for our purposes since we hope that λ will be a very small power of N.

7.2 Gauss Sums

Carl Friedrich Gauss introduced the so-called *(quadratic) Gauss sum* in his *Disquisitiones Arithmeticae* in 1801. He defined them as

$$\sum_{x=1}^{q} e\left(mx^2/q\right)$$

They are not easy to evaluate exactly, but fortunately not too hard to estimate in size. We shall have to deal with Gauss sums with an additional linear term. Suppose we wish to estimate

$$S_{\lambda a,q} = \sum_{x=1}^{q} e\left(\frac{a}{q}\left(\lambda x^2 + 2x\right)\right)$$

Our main problem is again that λa and q are not necessarily coprime, so we write

$$S_{\lambda a,q} = \frac{q}{d}\sum_{x=1}^{d} e\left(\frac{b}{d}\left(x^2 + \frac{2}{\lambda}x\right)\right) = \frac{q}{d}S_{b,d} = (\lambda, q)\, S_{b,d}$$

where $d = \frac{q}{(\lambda,q)}$ and $b = \frac{\lambda a}{(\lambda,q)}$. For b and d coprime, we find that

$$\begin{aligned}
|S_{b,d}|^2 &= \sum_{x=1}^{d}\sum_{y=1}^{d} e\left(\frac{b}{d}\left(\left(y^2-x^2\right)+\frac{2}{\lambda}\left(y-x\right)\right)\right) \\
&= \sum_{x=1}^{d}\sum_{z=1}^{d} e\left(\frac{b}{d}\left(\left(z^2+2xz\right)+\frac{2}{\lambda}z\right)\right) \\
&= \sum_{z=1}^{d} e\left(\frac{b}{d}z^2+\frac{2}{\lambda}z\right)\sum_{x=1}^{d} e\left(\frac{b}{d}2xz\right) \\
&= d\sum_{\substack{z=1\\ d|2z}}^{d} e\left(\frac{b}{d}z^2+\frac{2}{\lambda}z\right) \\
&\leq 2d
\end{aligned}$$

We conclude that $|S_{b,d}| \leq \sqrt{d}$, but we had $d = \frac{q}{(\lambda,q)}$ so that

$$|S_{\lambda a,q}| = |(\lambda,q)\, S_{b,d}| \leq \sqrt{(\lambda,q)\, q}$$

But we observe that by Bezout's Theorem $\lambda x^2 + 2x$ runs through a complete set of residues $\mod q$ unless $(\lambda, q) \geq 2$. This means $S_{\lambda a,q} = 0$ unless $(\lambda, q) \leq 2$. We summarize what we have shown in

Lemma 13. *For all integers λ and coprime integers a, q, we have*

$$|S_{\lambda a,q}| \leq \sqrt{2q} \tag{27}$$

Proof. (of Theorem) At each step of the iteration, $A - A$ is free of numbers of the form $n\,(\lambda n + 2)$ so set

$$S = \left\{ n\,(\lambda n + 2) : n \leq \left\lfloor \sqrt{\frac{N}{\lambda}} \right\rfloor = M \right\}$$

Choose $P = \frac{10}{\alpha^2}$, $P' = N^{\nu}$ and $Q = N^{1-\nu}$, the exact value of ν to be chosen later. We note that $P \leq P'$ if $\alpha \geq \frac{\sqrt{10}}{N^{\nu/2}}$, and it turns out that this will always be the case.
By Dirichlet, every r satisfies $\left|\frac{r}{N} - \frac{a}{q}\right| \leq \frac{1}{qQ}$ for some q with $(a, q) = 1, q \leq Q$.
We shall say that

$$r \in \textit{arithmetic part}\ (\text{AP}) \text{ if } \quad q \leq P \quad (\textit{very major arcs})$$

$$r \in \textit{non-arithmetic part}\ (\text{NAP}) \text{ if } \quad P < q \leq Q$$

where we further distinguish between

$$P < q \leq P' \quad (\textit{majorish arcs}) \quad \text{and} \quad P' < q \leq Q \quad (\textit{minor arcs})$$

Our first aim is

Lemma 14.

$$r \in NAP \Rightarrow \left|\hat{S}(r)\right| \leq \frac{\alpha}{2}|S| \tag{28}$$

Proof. We shall deal with majorish and minor arcs separately.
Using the above version of Weyl's Inequality on the minor arcs, we get

$$\begin{aligned}\left|\hat{S}(r)\right| &= \left|\sum_{x=1}^{M} e\left(\frac{r}{N}\left(\lambda x^2+2x\right)\right)\right| \\ &\leq 16\lambda \log N M N^{-\nu/2} \\ &\leq 16 \log N N^{1/100-\nu/2} M \\ &\leq \frac{\alpha}{2} M\end{aligned}$$

where we have assumed that $\lambda \leq N^{1/100}$ and $\alpha \geq \frac{32\log N}{N^{1/25}}$. We shall see at the end of the proof that these conditions will always be satisfied.
Analogously to Waring's Problem, we find an asymptotic expansion for the majorish arcs

$$f(\theta) = \sum_{x=1}^{M} e\left(\theta\left(\lambda x^2+2x\right)\right) = \frac{1}{q} S_{\lambda a,q}\, v\left(\theta - \frac{a}{q}\right) + O\left(N^{2\nu}\right) \tag{29}$$

where

$$S_{\lambda a,q} = \sum_{x=1}^{q} e\left(\frac{a}{q}\left(\lambda x^2+2x\right)\right)$$

and

$$v\left(\theta-\frac{a}{q}\right) = \sum_{m=1}^{M^2} \frac{1}{2} m^{-1/2} e\left(\left(\theta-\frac{a}{q}\right)\left(\lambda m + 2\sqrt{m}\right)\right)$$

We find that $\left|v\left(\theta-\frac{a}{q}\right)\right| \leq 2M$ and $|S_{\lambda a,q}| \leq \sqrt{2q}$ by Lemma 27. Thus on the majorish arcs

$$\begin{aligned}\left|\hat{S}(r)\right| &\leq \frac{\sqrt{2q}}{q} 2M \\ &\leq \frac{\alpha}{2} M\end{aligned}$$

□

It follows immediately that from (28) that

$$\sum_{\substack{r\neq 0\\ r\in AP}} \left|\hat{A}\left(r\right)\right|^2 \left|\hat{S}\left(r\right)\right| \geq \frac{1}{2}\left|A\right|^2\left|S\right|$$

and similarly to the proof of Sárközy's Theorem for squares, we find that

$$\begin{aligned}\frac{1}{2}\alpha^2 N^2 M &\leq \sum_{\substack{r\neq 0\\ r\in AP}} \left|\hat{A}\left(r\right)\right|^2 \left|\hat{S}\left(r\right)\right| \\ &\leq \sup_{\substack{r\neq 0\\ r\in AP}} \left|\hat{A}(r)\right| \left(\sum_r \left|\hat{S}(r)\right|^{12}\right)^{1/12} \left(\sum_r \left|\hat{A}(r)\right|^2\right)^{1/2} \left(\sum_r \left|\hat{A}(r)\right|^2\right)^{5/12}\end{aligned}$$

7.3 An L^{12} estimate for general λ

Our aim is to show that

$$\sum_r \left|\hat{S}\left(r\right)\right|^{12} \leq c\left|S\right|^{12}$$

or equivalently, that

$$\int_0^1 \left|f\left(\theta\right)\right|^{12} d\theta \ll \frac{N^5}{\lambda^6} \tag{30}$$

with $f\left(\theta\right)$ as above.

Following Hardy-Littlewood, we split the interval $[0,1]$ into major and minor arcs:

Let $\delta > 0$ be 'small' and let

$$\mathfrak{M}_{a,q} = \left\{\theta \in [0,1] : \left|\theta - \frac{a}{q}\right| < \frac{1}{N^{1-\delta}}, (a,q) = 1, q \leq N^{\delta}\right\}$$

Then the *major arcs* are defined to be the set

$$\mathfrak{M} = \bigcup_{q=1}^{N^{\delta}} \bigcup_{\substack{a=1\\(a,q)=1}}^{q} \mathfrak{M}_{a,q}$$

and the *minor arcs*

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

On the minor arcs, modified Weyl yields

$$\left|f\left(\theta\right)\right| = \left|\sum_{x=1}^{M} e\left(\theta\left(\lambda x^2 + 2x\right)\right)\right| \ll \sqrt{\lambda}\log N N^{1/2-\delta/2} \ll_{\epsilon} N^{101/200-\delta/2+\epsilon}$$

We then have

$$\begin{aligned}\int_{\mathfrak{m}} |f(\theta)|^{12}\, d\theta &\leq \max_{\theta\in\mathfrak{m}} |f(\theta)|^{8} \int_0^1 |f(\theta)|^4\, d\theta \\ &\ll \left(N^{101/200-\delta/2+\epsilon}\right)^8 M^{2+\sigma} \\ &\ll \frac{1}{\lambda} N^{5+1/25-4\delta+8\epsilon+\sigma/2}\end{aligned}$$

where we have used Hua's Lemma, which holds for general polynomials [Hu38]. Thus if we choose $\delta > 1/30$ and ϵ, σ small enough so that $8\epsilon + \sigma/2 \leq \delta$, we have

$$\int_{\mathfrak{m}} |f(\theta)|^{12}\, d\theta \ll \frac{N^5}{\lambda^6}$$

as required.

As before, on the major arcs we obtain an asymptotic expansion

$$f(\theta) = \sum_{x=1}^{M} e\left(\theta\left(\lambda x^2 + 2x\right)\right) = \frac{1}{q} S_{\lambda a,q}\, v\left(\theta - \frac{a}{q}\right) + O\left(N^{2\delta}\right)$$

where

$$S_{\lambda a,q} = \sum_{x=1}^{q} e\left(\frac{a}{q}\left(\lambda x^2 + 2x\right)\right)$$

and

$$v\left(\theta - \frac{a}{q}\right) = \sum_{m=1}^{M^2} \frac{1}{2} m^{-1/2} e\left(\left(\theta - \frac{a}{q}\right)\left(\lambda m + 2\sqrt{m}\right)\right)$$

It follows that

$$\sum_{q=1}^{N^\delta} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}_{a,q}} \left| f(\theta)^{12} - \left(\frac{1}{q} S_{\lambda a,q}\, v\left(\theta - \frac{a}{q}\right)\right)^{12} \right| d\theta \ll \frac{N^5}{\lambda^6}$$

if we chose $\delta > 0$ at each stage such that $\lambda \ll N^{1-10\delta}$. If we assume that $\lambda \leq N^{1/100}$, then this only means that we want δ to be significantly less than $1/10$, $\delta = 1/20$ say.

Following Vaughan, we also find that

$$|v(\beta)| \ll \min\left\{M, \frac{1}{|\lambda\beta|^{1/2}}\right\}$$

which is a very good thing as the following calculation shows. We have

$$\begin{aligned}\int_{\mathfrak{M}}|f(\theta)|^{12} &= \int_{\mathfrak{M}}\left(\frac{1}{q}S_{\lambda a,q}v\left(\theta-\frac{a}{q}\right)\right)^{12}d\theta+\text{error}\\ &= \sum_{q\leq N^{\delta}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left(\frac{S_{\lambda a,q}}{q}\right)^{12}\int_{\mathfrak{M}_{a,q}}\left|v\left(\theta-\frac{a}{q}\right)\right|^{12}d\theta+\text{error}\\ &\ll \sum_{q\leq N^{\delta}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left(\frac{S_{\lambda a,q}}{q}\right)^{12}\int_{0}^{\frac{\lambda}{N}}\left(\min\left\{M,\frac{1}{|\lambda\beta|^{1/2}}\right\}\right)^{12}d\beta\\ &\ll \frac{N^5}{\lambda^6}\sum_{q\leq N^{\delta}}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left(\frac{S_{\lambda a,q}}{q}\right)^{12}\end{aligned}$$

and our estimate of $S_{\lambda a,q}$ gives us the desired estimate

$$\int_{\mathfrak{M}}|f(\theta)|^{12}d\theta\ll\frac{N^5}{\lambda^6}$$

Having obtained our L^{12} estimate, we deduce that there exists $r\neq 0, r\in AP$ for which

$$\left|\hat{A}(r)\right|\geq\frac{\alpha^{11/2}}{2\sqrt{c}}|A|$$

We now show that A has increased density on a subprogression with common difference q, where q satisfies $\left|\frac{r}{N}-\frac{a}{q}\right|\leq\frac{1}{qQ}$ and $q\leq\frac{10}{\alpha^2}$. Let $B=\{0,q,2q,...,Lq\}$ with L to be chosen later. Then

$$\left|\hat{B}(r)\right|=\left|\sum_{x=1}^{L}e\left(\frac{rqx}{N}\right)\right|=\left|\frac{\sin\pi\frac{rq}{N}\frac{L}{2}}{\sin\pi\frac{rq}{n}}\right|\geq\frac{2}{\pi}L$$

provided $L\leq\frac{1}{2}Q$.
Now

$$\begin{aligned}N\sum_{x}|A\cap(B+x)|^2 &= \sum_{m}\left|\hat{A}(m)\right|^2\left|\hat{B}(m)\right|^2\\ &\geq \frac{4}{\pi^2}L^2\left(\frac{\alpha^{11}}{4c}|A|^2\right)+L^2|A|^2\\ &= \left(1+\alpha^{11}\pi^2c\right)L^2|A|^2\end{aligned}$$

We are in good shape, except that unfortunately some of the translates of B will split into smaller subprogressions when we unravel $\mathbb{Z}_N$ to recover $\{1,...,N\}$. Call the set of x for which this does not happen 'good'.

7.4 Bounds

Setting $L = \alpha^2 N^{1/2}$, we find that the diameter of B is at most $10\sqrt{N}$, but also $L \geq N^{2/5}$ (anticipating once again the final lower bound on α).

We deduce that there are at most $\sqrt{N}$ 'bad' values of x, and their contribution to the above sum is at most $L^2 N^{3/2}$. Thus

$$\begin{aligned} N \sup_{x' good'} |A \cap (B+x)||A|L &\geq N \sum_x |A \cap (B+x)|^2 \\ &\geq \left(1 + \frac{\alpha^{11}}{2\pi^2 c}\right) L^2 |A|^2 \end{aligned}$$

provided $\alpha \geq \left(\frac{2\pi^2 c}{N^{1/2}}\right)^{1/13}$. It follows that there exists a 'good' x such that

$$|A \cap (B+x)| \geq \left(\alpha + \frac{\alpha^{12}}{2\pi^2 c}\right) L$$

We have thus established a density increase of $\frac{\alpha_m^{12}}{2\pi^2 c}$ at the mth step. The total number of steps T before we reach contradiction (i.e. density greater than one) is bounded above by $4\pi^2 c \alpha_0^{-11}$, which gives a lower bound on α of

$$\alpha \geq \frac{c}{(\log\log N)^{1/11}}$$

It remains to check that λ is indeed as small as we would like it to be. At each step, $q \leq \frac{10}{\alpha^2} \leq \frac{1}{100c}(\log\log N)^{1/11}$. We shall multiply at most T such q together, whence $\lambda \ll (\log\log N)^{T/11}$ which does not exceed $N^{\frac{1}{100}\left(\frac{2}{5}\right)^T}$ provided $\alpha \geq \frac{C}{(\log\log N)^{1/11}}$, for some (maybe larger) constant C.

□

Acknowledgements

I am greatly indebted to Dr Ben Green for his very valuable and generous help in producing this essay. He deserves full credit for the ideas underlying the final chapter. Any remaining errors are mine. I am grateful to Tom Sanders for pointing out the existence of the delta function to me after having been rudely awakened by a phone call at 11 am. Finally, I would like to thank Dominic Vella for moral support and his unbroken enthusiasm for Lemma 13.

References

[Dav62] H. Davenport, *Analytic methods for diophantine equations and diophantine inequalities*, Ann Arbor Publishers 1962

[G01] W.T. Gowers, *A new proof of Szemerdi's Theorem*, Geom. funct. anal. **11** (2001), 465-588

[Gre02] B.J. Green, *On arithmetic structures in dense set of integers*, Duke Math. Journal **114** (2002), 215-238

[Gro85] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer Verlag 1985

[HaLi19] G.H. Hardy and J.E. Littlewood, *A new solution of Waring's Problem*, Quart. J. Math. **48** (1919), 272-293

[Hi09] D. Hilbert, *Beweis für Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl von Potenzen (Waringsches Problem)*, Göttinger Nachrichten (1909), 17-36

[Hl84] E. Hlawka, *The Theory of Uniform Distribution*, A B Academic Publishers

[Hu38] L.K. Hua, *On Waring's Problem*, Quart. J. Math. Oxford **9** (1938), 199-202

[M94] H.L. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS Regional Conference Series in Mathematics **84** AMS 1994

[N96a] M.B. Nathanson, *Additive Number Theory: The Classical Bases*, Graduate Texts in Mathematics **164**, Springer Verlag, 1996

[N00] M.B. Nathanson *Elementary Methods in Number Theory*, Graduate Texts in Mathematics **195**, Springer Verlag 2000

[R53] K.F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104-109

[S78a] A. Sárközy, *On difference sets of sequences of integers I*, Acta Math. Acad. Sci. Hungar. **31** (1978), 125-149

[S78b] A. Sárközy, *On difference sets of sequences of integers III*, Acta Math. Acad. Sci. Hungar. **31** (1978), 355-386

[V81] R.C. Vaughan, *The Hardy-Littlewood Method*, Cambridge Tracts in Mathematics **80**, Cambridge University Press 1981