CHAPTER 1

Waring's Problem

1.1. Introduction

Lagrange's theorem that every natural number is a sum of 4 non-negative integer squares, leads naturally to the question of sums of cubes, biquadrates, primes, *etc.* Indeed, Waring conjectured that every natural number could be written as a sum of 9 non-negative integer cubes, a sum of 19 non-negative integer biquadrates, and so on.

The purpose of this chapter is to give a very brief introduction to a technique which enables one to study some of these and related questions. The method of Hardy and Littlewood was first used in the early 1900's to study the conjecture of Waring. Since then, the method has been modified and adapted in many different ways to study a variety of problems in additive number theory. Here we only provide a glimpse of the method.

More precisely, Waring's problem concerns the solubility, or otherwise, of the diophantine equation

$$n = x_1^k + \ldots + x_s^k, \tag{1.1}$$

where $k \geqslant 2$ is a fixed integer. Given any natural number $n \in \mathbb{N}$, the question is how large the integer s has to be in order to guarantee that there are non-negative integers $x_1, \ldots, x_s$ such that (1.1) holds.

The number $g(k)$ is defined to be the smallest value of s for which, given any $n \in \mathbb{N}$, there exist non-negative integers $x_1, \ldots, x_s$ such that (1.1) holds. Thus Lagrange's theorem states that $g(2) = 4$, and Waring conjectured that $g(3) = 9$, $g(4) = 19$, and so on.

However, the number $g(k)$ is greatly affected by the number of summands in (1.1) required when the natural number $n \in \mathbb{N}$ is relatively small. For example, it is now known that $g(3) = 9$, but apart from $n = 23$ and $n = 239$, every other natural number $n \in \mathbb{N}$ is a sum of 8 non-negative integer cubes. It is therefore more natural to consider the number $G(k)$ which is defined to be the smallest value of s for which, given any sufficiently large $n \in \mathbb{N}$, there exist non-negative integers $x_1, \ldots, x_s$ such that (1.1) holds. In other words, we allow a finite number of exceptional values of $n \in \mathbb{N}$ for which (1.1) is not soluble in non-negative integers $x_1, \ldots, x_s$. The only known values of $G(k)$ are $G(2) = 4$ and $G(4) = 16$.

We develop the basic ideas of the Hardy–Littlewood method and prove that $G(k) \leqslant 2^k + 1$ for every integer $k \geqslant 2$.

THEOREM 1.1. *Suppose that $k \geqslant 2$ is a fixed integer. Suppose further that the integer $s \geqslant 2^k + 1$. Then there exists N_0 such that for every natural number $n \in \mathbb{N}$ satisfying $n > N_0$, there exist non-negative integers $x_1, \ldots, x_s$ such that $n = x_1^k + \ldots + x_s^k$.*

We remark that Theorem 1.1 is not best possible. Note, for example, that it only gives $G(2) \leqslant 5$ and $G(4) \leqslant 17$. Indeed, Vinogradov showed that there exists a positive number C such that for all large values of k, the estimate

$$G(k) \leqslant (C + o(1))k \log k$$

is valid. In particular, he showed that one could take $C = 2$. However, there was no real progress on this problem for many years until Wooley showed in the late 1980's that for all large values of k, the

estimate

$$G(k) \leqslant k(\log k + \log\log k + O(1))$$

is valid. For small values of k, the best published results up to about 2005 are due to Vaughan and Wooley, with $G(5) \leqslant 17$, $G(6) \leqslant 21$, $G(7) \leqslant 33$, $G(8) \leqslant 42$ and $G(9) \leqslant 50$.

Throughout the chapter, the natural number $k \geqslant 2$ is chosen and fixed, and the natural number $s \geqslant 2^k + 1$. Also, δ denotes a positive real number, chosen to be small enough, and may differ from one occurrence to the next. Indeed, all estimates involving δ will hold with some fixed value of δ for all sufficiently large values of n.

Suppose that $m \in \mathbb{Z}$. Then

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

It follows that if $n, x_1, \dots, x_s \in \mathbb{N}$, then

$$\int_0^1 e((x_1^k + \dots + x_s^k - n)\alpha)\,\mathrm{d}\alpha = \begin{cases} 1, & \text{if } n = x_1^k + \dots + x_s^k, \\ 0, & \text{if } n \neq x_1^k + \dots + x_s^k. \end{cases}$$

For every $n \in \mathbb{N}$, let $R(n)$ denote the number of solutions of the equation (1.1), with $x_1, \dots, x_s \in \mathbb{N}$. Then clearly

$$R(n) = \sum_{x_1 \in \mathbb{N}} \dots \sum_{x_s \in \mathbb{N}} \int_0^1 e((x_1^k + \dots + x_s^k - n)\alpha)\,\mathrm{d}\alpha. \tag{1.2}$$

On the other hand, note that if $n = x_1^k + \dots + x_s^k$, then we must have $x_i \leqslant n^{1/k}$ for every $i = 1, \dots, s$. Hence the summation in (1.2) can be restricted to

$$1 \leqslant x_1, \dots, x_s \leqslant n^{1/k}$$

without altering the value of $R(n)$, so that

$$\begin{aligned} R(n) &= \sum_{1 \leqslant x_1 \leqslant n^{1/k}} \dots \sum_{1 \leqslant x_s \leqslant n^{1/k}} \int_0^1 e((x_1^k + \dots + x_s^k - n)\alpha)\,\mathrm{d}\alpha \\ &= \int_0^1 \sum_{1 \leqslant x_1 \leqslant n^{1/k}} \dots \sum_{1 \leqslant x_s \leqslant n^{1/k}} e((x_1^k + \dots + x_s^k - n)\alpha)\,\mathrm{d}\alpha \\ &= \int_0^1 \sum_{1 \leqslant x_1 \leqslant n^{1/k}} \dots \sum_{1 \leqslant x_s \leqslant n^{1/k}} e(\alpha x_1^k) \dots e(\alpha x_s^k) e(-\alpha n)\,\mathrm{d}\alpha \\ &= \int_0^1 \left(\sum_{1 \leqslant x_1 \leqslant n^{1/k}} e(\alpha x_1^k) \right) \dots \left(\sum_{1 \leqslant x_s \leqslant n^{1/k}} e(\alpha x_s^k) \right) e(-\alpha n)\,\mathrm{d}\alpha \\ &= \int_0^1 f^s(\alpha) e(-\alpha n)\,\mathrm{d}\alpha, \end{aligned} \tag{1.3}$$

where

$$f(\alpha) = \sum_{x=1}^{N} e(\alpha x^k),$$

with

$$N = [n^{1/k}].$$

The size of the integrand on the right hand side of (1.3) varies greatly as the value of α varies. Roughly speaking, the size is relatively large when α is close to rational numbers with small denominators, and relatively small otherwise.

The idea of Hardy and Littlewood is therefore to write

$$R(n) = \int_{\mathfrak{M}} f^s(\alpha) e(-\alpha n)\,\mathrm{d}\alpha + \int_{\mathfrak{m}} f^s(\alpha) e(-\alpha n)\,\mathrm{d}\alpha, \tag{1.4}$$

where the two sets $\mathfrak{M}$ and $\mathfrak{m}$ are disjoint and $\mathfrak{M}\cup\mathfrak{m}$ represents a unit interval – note that the integrand on the right hand side of (1.3) is periodic with period 1. Let ν be a sufficiently small positive real number, and write

$$P = N^{\nu}.$$

For every $a, q \in \mathbb{N}$ satisfying $1 \leqslant a \leqslant q \leqslant P$ and $(a, q) = 1$, let

$$\mathfrak{M}(q, a) = \{\alpha \in \mathbb{R} : |\alpha - a/q| \leqslant PN^{-k}\}.$$

The intervals $\mathfrak{M}(q, a)$ are called the major arcs, and are basically short intervals centred at rational numbers with small denominators. It is not difficult to show that the major arcs are pairwise disjoint, provided that ν is small enough. Indeed, if $a/q \neq a'/q'$, then

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| = \frac{|aq' - qa'|}{qq'} \geqslant \frac{1}{qq'} > 2PN^{-k},$$

provided that $\nu < 1/2$, say, and N is sufficiently large. We now write

$$\mathfrak{M} = \bigcup_{q \leqslant P} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}(q, a),$$

and let

$$\mathcal{U} = (PN^{-k}, 1 + PN^{-k}] \quad \text{and} \quad \mathfrak{m} = \mathcal{U} \setminus \mathfrak{M}.$$

We say that the intervals in $\mathfrak{m}$ form the minor arcs.

To prove Theorem 1.1, it suffices to show that $R(n) > 0$ for all sufficiently large $n \in \mathbb{N}$. Our strategy is to find some sufficiently small positive value of ν for which

$$\int_{\mathfrak{M}} f^s(\alpha) e(-\alpha n)\, \mathrm{d}\alpha \gg n^{s/k-1}$$

and

$$\int_{\mathfrak{m}} f^s(\alpha) e(-\alpha n)\, \mathrm{d}\alpha = o(n^{s/k-1}).$$

We do not give an explicit value for ν, but will indicate the restrictions on its size throughout our discussion.

In the remainder of this chapter, the implicit constants in estimates may depend on the value of the fixed integer k.

1.2. The Minor Arcs

In this section, we study the integral

$$\int_{\mathfrak{m}} f^s(\alpha) e(-\alpha n)\, \mathrm{d}\alpha.$$

It is easy to see that

$$\left|\int_{\mathfrak{m}} f^s(\alpha) e(-\alpha n)\, \mathrm{d}\alpha\right| \leqslant \int_{\mathfrak{m}} |f(\alpha)|^s\, \mathrm{d}\alpha \leqslant \left(\sup_{\alpha \in \mathfrak{m}} |f(\alpha)|\right)^{s-2^k} \int_0^1 |f(\alpha)|^{2^k}\, \mathrm{d}\alpha. \tag{1.5}$$

We use the following two estimates. Note that the implicit constants may depend on the choice of ϵ.

THEOREM 1.2 (Hua's lemma). *For every $j = 1, \dots, k$, we have*

$$\int_0^1 |f(\alpha)|^{2^j}\, \mathrm{d}\alpha \ll N^{2^j - j + \epsilon}. \tag{1.6}$$

THEOREM 1.3 (Weyl's inequality). *Suppose that $a, q \in \mathbb{N}$ satisfy $(a, q) = 1$. Suppose further that $\alpha \in \mathbb{R}$ satisfies $|\alpha - a/q| \leqslant q^{-2}$. Then*

$$|f(\alpha)| \ll N^{1+\epsilon}(q^{-1} + N^{-1} + qN^{-k})^{1/K},$$

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

To use Weyl's inequality, we need to study those values of $\alpha \in \mathfrak{m}$ more closely. We need the following famous result of Dirichlet on diophantine approximation.

THEOREM 1.4 (Dirichlet). *Suppose that $\alpha \in \mathbb{R}$. Then for every real number $X \geqslant 1$, there exist $a, q \in \mathbb{Z}$ satisfying $(a,q) = 1$ and $1 \leqslant q \leqslant X$ such that*

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{qX}.$$

PROOF. It clearly suffices to prove the result without the restriction $(a,q) = 1$. Consider the $[X]$ numbers

$$\{t\alpha\} = t\alpha - [t\alpha], \quad t = 1, \dots, [X],$$

and the $[X]+1$ intervals

$$I_j = \left[\frac{j-1}{[X]+1}, \frac{j}{[X]+1}\right), \quad j = 1, \dots, [X]+1.$$

If one of the $[X]$ numbers $\{t\alpha\}$ lies in I_1 or $I_{[X]+1}$, then the conclusion of the theorem holds with $q = t$. On the other hand, if I_1 and $I_{[X]+1}$ do not contain any of the $[X]$ numbers, then by the Dirichlet box principle, one of the remaining $[X]-1$ intervals must contain two of the $[X]$ numbers. In other words, there exist integers t', t'', satisfying $1 \leqslant t' < t'' \leqslant [X]$, and an integer $i = 2, \dots, [X]$, such that $\{t'\alpha\}, \{t''\alpha\} \in I_i$, so that

$$|\{t''\alpha\} - \{t'\alpha\}| \leqslant \frac{1}{[X]+1} \leqslant \frac{1}{X},$$

whence

$$|(t''-t)\alpha - ([t''\alpha] - [t'\alpha])| \leqslant \frac{1}{X}.$$

We now take $q = t'' - t'$ and $a = [t''\alpha] - [t'\alpha]$ to complete the proof. ◯

Suppose now that $\alpha \in \mathfrak{m}$. Using Dirichlet's theorem with $X = N^k P^{-1}$, we conclude that there exist $a, q \in \mathbb{Z}$ satisfying $(a,q) = 1$ and $1 \leqslant q \leqslant N^k P^{-1}$ such that $|\alpha - a/q| \leqslant q^{-1} P N^{-k}$. Since $\alpha \in \mathfrak{m} \subseteq (PN^{-k}, 1 - PN^{-k})$, it follows that $1 \leqslant a \leqslant q$. Furthermore, we must have $q > P$, for otherwise $\alpha \in \mathfrak{M}$. It now follows from Weyl's inequality that for every $\alpha \in \mathfrak{m}$, we must have

$$\begin{aligned} |f(\alpha)| &\ll N^{1+\epsilon}(q^{-1} + N^{-1} + qN^{-k})^{1/K} \\ &\ll N^{1+\epsilon}(P^{-1} + N^{-1} + P^{-1})^{1/K} \\ &\ll N^{1+\epsilon} P^{-1/K} = N^{1+\epsilon-\nu/K}, \end{aligned} \tag{1.7}$$

provided that ν is sufficiently small. Combining (1.5)–(1.7), we conclude that

$$\left|\int_{\mathfrak{m}} f^s(\alpha) e(-\alpha n)\, \mathrm{d}\alpha\right| \ll N^{(1+\epsilon-\nu/K)(s-2^k)} N^{2^k - k + \epsilon} \ll n^{s/k - 1 - \delta} \tag{1.8}$$

for some fixed positive real number δ, depending only on our choice of ν.

We prove Hua's lemma and Weyl's inequality in Section 1.6.

1.3. The Major Arcs

In this section, we study the integral

$$\int_{\mathfrak{M}(q,a)} f^s(\alpha) e(-\alpha n)\, \mathrm{d}\alpha,$$

where $a, q \in \mathbb{N}$ satisfy $1 \leqslant a \leqslant q \leqslant P$ and $(a,q) = 1$.

The first step in our argument is to find a suitable approximation to the generating function $f(\alpha)$. We introduce the functions

$$v(\beta) = \sum_{m=1}^{n} \frac{1}{k} m^{1/k-1} e(\beta m) \tag{1.9}$$

and

$$S(q,a) = \sum_{m=1}^{q} e\left(\frac{am^k}{q}\right). \tag{1.10}$$

Here v is obtained from f by replacing the characteristic function of the k-th powers by the probability that m is a k-th power, and $S(q,a)$ has to be introduced to overcome the handicap that the k-th powers are generally not uniformly distributed modulo q.

THEOREM 1.5. *Suppose that $a, q \in \mathbb{N}$ satisfy $1 \leqslant a \leqslant q \leqslant P$ and $(a,q) = 1$. Suppose further that $\alpha \in \mathfrak{M}(q,a)$, and*

$$V(\alpha, q, a) = q^{-1} S(q,a) v\left(\alpha - \frac{a}{q}\right). \tag{1.11}$$

Then

$$f(\alpha) = V(\alpha, q, a) + O(P^2).$$

PROOF. Write $\beta = \alpha - a/q$. Then

$$f(\alpha) = \sum_{1 \leqslant x \leqslant n^{1/k}} e\left(\frac{ax^k}{q}\right) e(\beta x^k) = \sum_{m=1}^{n} c(m) e\left(\frac{am}{q}\right) e(\beta m),$$

where

$$c(m) = \begin{cases} 1, & \text{if } m \text{ is a } k\text{-th power,} \\ 0, & \text{otherwise.} \end{cases}$$

It follows that

$$f(\alpha) - q^{-1} S(q,a) v\left(\alpha - \frac{a}{q}\right) = \sum_{m=1}^{n} a_m e(\beta m),$$

where

$$a_m = \begin{cases} e\left(\dfrac{am}{q}\right) - q^{-1} S(q,a) \dfrac{1}{k} m^{1/k-1}, & \text{if } m \text{ is a } k\text{-th power,} \\ -q^{-1} S(q,a) \dfrac{1}{k} m^{1/k-1}, & \text{otherwise.} \end{cases}$$

By partial summation (see Remark below), we have

$$\sum_{m=1}^{n} a_m e(\beta m) = e(\beta n) \sum_{m=1}^{n} a_m - 2\pi \mathrm{i} \beta \int_0^n e(\beta y) \left(\sum_{m \leqslant y} a_m \right) \mathrm{d}y.$$

Note that

$$\sum_{m \leqslant y} a_m = \sum_{x \leqslant y^{1/k}} e\left(\frac{ax^k}{q}\right) - q^{-1} S(q,a) \sum_{m \leqslant y} \frac{1}{k} m^{1/k-1}.$$

First of all, we have

$$\sum_{x \leqslant y^{1/k}} e\left(\frac{ax^k}{q}\right) = \sum_{r=1}^{q} e\left(\frac{ar^k}{q}\right) \sum_{\substack{x \leqslant y^{1/k} \\ x \equiv r \bmod q}} 1 = S(q,a)(y^{1/k} q^{-1} + O(1)) = y^{1/k} q^{-1} S(q,a) + O(q).$$

Secondly, we have, by the Integral test, that

$$\sum_{m \leqslant y} \frac{1}{k} m^{1/k-1} = \int_1^y \frac{1}{k} x^{1/k-1} \, \mathrm{d}x + O(1) = y^{1/k} + O(1).$$

It follows that

$$\sum_{m \leqslant y} a_m = O(q).$$

Note now that $|\beta| \leqslant PN^{-k}$. Hence

$$\sum_{m=1}^{n} a_m e(\beta m) \ll (1 + |\beta| n) q \ll (1 + PN^{-k} n) P \ll P^2.$$

The result follows immediately. ◯

REMARK. The following partial summation result is often used in analytic number theory, and can be proved by writing

$$F(m) = F(X) - \int_m^X F'(y)\,\mathrm{d}y,$$

and interchanging the order of summation and integration: Suppose that $a_1, a_2, a_3, \dots$ is a sequence of complex numbers. Suppose further that the function F has continuous derivative on the interval $[0, X]$. Then

$$\sum_{m\leqslant X} a_m F(m) = F(X)\sum_{m\leqslant X} a_m - \int_0^X F'(y)\left(\sum_{m\leqslant y} a_m\right)\mathrm{d}y. \tag{1.12}$$

It now follows from Theorem 1.5 that if $\alpha \in \mathfrak{M}(q,a)$, then

$$f^s(\alpha) - V^s(\alpha,q,a) \ll N^{s-1}|f(\alpha) - V(\alpha,q,a)| \ll N^{s-1}P^2.$$

Summing this error over all the major arcs, we obtain

$$\sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{\mathfrak{M}(q,a)} |f^s(\alpha) - V^s(\alpha,q,a)|\,\mathrm{d}\alpha \ll N^{s-k-1}P^5 \ll n^{s/k-1-1/k}P^5 \ll n^{s/k-1-\delta}$$

for some fixed positive number δ depending only on our choice of ν. If we now write

$$R_1(n) = \sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{\mathfrak{M}(q,a)} V^s(\alpha,q,a)e(-\alpha n)\mathrm{d}\alpha, \tag{1.13}$$

then

$$\int_{\mathfrak{M}} f^s(\alpha)e(-\alpha n)\,\mathrm{d}\alpha = R_1(n) + O(n^{s/k-1-\delta}). \tag{1.14}$$

Combining (1.11) and (1.13), we have

$$\begin{aligned}
R_1(n) &= \sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{\mathfrak{M}(q,a)} (q^{-1}S(q,a))^s v^s\left(\alpha - \frac{a}{q}\right)e(-\alpha n)\,\mathrm{d}\alpha \\
&= \sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{\mathfrak{M}(q,a)} (q^{-1}S(q,a))^s v^s\left(\alpha - \frac{a}{q}\right)e\left(-\left(\alpha - \frac{a}{q}\right)n\right)e\left(-\frac{an}{q}\right)\mathrm{d}\alpha \\
&= \sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}(q^{-1}S(q,a))^s e\left(-\frac{an}{q}\right)\int_{\mathfrak{M}(q,a)} v^s\left(\alpha - \frac{a}{q}\right)e\left(-\left(\alpha - \frac{a}{q}\right)n\right)\mathrm{d}\alpha \\
&= \sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}(q^{-1}S(q,a))^s e\left(-\frac{an}{q}\right)\int_{-PN^{-k}}^{PN^{-k}} v^s(\beta)e(-\beta n)\,\mathrm{d}\beta \\
&= \mathfrak{S}(n,P)J^*(n),
\end{aligned} \tag{1.15}$$

where

$$\mathfrak{S}(n,P) = \sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}(q^{-1}S(q,a))^s e\left(-\frac{an}{q}\right)$$

and

$$J^*(n) = \int_{-PN^{-k}}^{PN^{-k}} v^s(\beta)e(-\beta n)\,\mathrm{d}\beta. \tag{1.16}$$

Our next task is to complete the series to infinity and to replace the interval of integration by a unit interval.

Let us first of all consider the series $\mathfrak{S}(n,P)$. Write

$$S(q) = \sum_{\substack{a=1\\(a,q)=1}}^{q} (q^{-1}S(q,a))^s e\left(-\frac{an}{q}\right). \tag{1.17}$$

It is easily seen from Weyl's inequality that $S(q,a) \ll q^{1+\epsilon-1/K}$ provided that $(a,q)=1$. Hence $S(q) \ll q(q^{\epsilon-1/K})^s$, and so whenever $s \geqslant 2^k+1$ and $\epsilon > 0$ is sufficiently small, we can conclude that

$$S(q) \ll q^{-1-2^{-k}}.$$

Hence

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} S(q) \tag{1.18}$$

converges absolutely and uniformly with respect to n. Note that $P = N^\nu$, so

$$\mathfrak{S}(n,P) - \mathfrak{S}(n) \ll n^{-\delta} \tag{1.19}$$

for some fixed positive number δ depending only on our choice of ν. Combining (1.15) and (1.19), we conclude that

$$R_1(n) = (\mathfrak{S}(n) + O(n^{-\delta}))J^*(n) \quad \text{and} \quad \mathfrak{S}(n) \ll 1. \tag{1.20}$$

We consider next the integral $J^*(n)$. The reason that we can replace the interval of integration by the unit interval $[-1/2, 1/2]$ is that the function $v(\beta)$ decays rather rapidly away from $\beta = 0$. More precisley, we have the following estimate.

THEOREM 1.6. *Suppose that $\beta \in \mathbb{R}$ satisfies $|\beta| \leqslant 1/2$. Then*

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

PROOF. Suppose first of all that $|\beta| \leqslant 1/n$. Then

$$v(\beta) \ll \sum_{m=1}^{n} \frac{1}{k} m^{1/k-1} = \int_1^n \frac{1}{k} x^{1/k-1}\,\mathrm{d}x + O(1) \ll n^{1/k} = \min\{n^{1/k}, |\beta|^{-1/k}\}.$$

Suppose now that $|\beta| > 1/n$. Let $M = [|\beta|^{-1}]$, and write

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

Clearly the first term on the right hand side is $\ll M^{1/k} \ll \min\{n^{1/k}, |\beta|^{-1/k}\}$. To study the second term on the right hand side, we use Abel summation. Let

$$S_m = \sum_{r=1}^{m} e(\beta r) \quad \text{and} \quad c_m = \frac{1}{k} m^{1/k-1}.$$

Then

$$\begin{aligned}\sum_{m=M+1}^{n} \frac{1}{k} m^{1/k-1} e(\beta m) &= \sum_{m=M+1}^{n} c_m(S_m - S_{m-1}) = \sum_{m=M+1}^{n} c_m S_m - \sum_{m=M+1}^{n} c_m S_{m-1}\\ &= \sum_{m=M+1}^{n} c_m S_m - \sum_{m=M}^{n-1} c_{m+1} S_m\\ &= c_n S_n - c_{M+1} S_M + \sum_{m=M+1}^{n-1} (c_m - c_{m+1}) S_m.\end{aligned}$$

Since $S_m \ll |\beta|^{-1}$ and c_m is a decreasing sequence, it follows that

$$\sum_{m=M+1}^{n} \frac{1}{k} m^{1/k-1} e(\beta m) \ll c_{M+1}|\beta|^{-1} < |\beta|^{-1/k} = \min\{n^{1/k}, |\beta|^{-1/k}\}.$$

The conclusion follows immediately. ◯

Let

$$J(n) = \int_{-\frac{1}{2}}^{\frac{1}{2}} v^s(\beta) e(-\beta n)\,\mathrm{d}\beta. \tag{1.21}$$

Then it follows from (1.16) and (1.21) that

$$J(n) - J^*(n) \ll \int_{PN^{-k}}^{\frac{1}{2}} \beta^{-s/k}\,\mathrm{d}\beta \ll \int_{PN^{-k}}^{\infty} \beta^{-s/k}\,\mathrm{d}\beta \ll n^{s/k-1-\delta} \tag{1.22}$$

for some fixed positive number δ depending only on our choice of ν. Also,

$$J(n) \ll \int_0^{\infty} \min\{n^{s/k}, |\beta|^{-s/k}\}\,\mathrm{d}\beta \ll n^{s/k-1}. \tag{1.23}$$

Hence it follows from (1.20), (1.22) and (1.23) that

$$\begin{aligned} R_1(n) &= (\mathfrak{S}(n) + O(n^{-\delta}))J(n) + (\mathfrak{S}(n) + O(n^{-\delta}))(J^*(n) - J(n)) \\ &= \mathfrak{S}(n)J(n) + O(n^{-\delta}|J(n)|) + O(|J^*(n) - J(n)|) \\ &= \mathfrak{S}(n)J(n) + O(n^{s/k-1-\delta}) \end{aligned} \tag{1.24}$$

for some fixed positive number δ depending only on our choice of ν.

Finally, we combine (1.4), (1.8), (1.14) and (1.24) to obtain

$$R(n) = \mathfrak{S}(n)J(n) + O(n^{s/k-1-\delta}) \tag{1.25}$$

for some fixed positive number δ depending only on our choice of ν.

1.4. The Singular Integral

In this section, we study the integral

$$J(n) = \int_{-\frac{1}{2}}^{\frac{1}{2}} v^s(\beta) e(-\beta n)\,\mathrm{d}\beta.$$

THEOREM 1.7. *Suppose that $s \geqslant 2$. Then*

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

The proof of Theorem 1.7 depends on the following technical result.

THEOREM 1.8. *Suppose that $A, B \in \mathbb{R}$ satisfy $A \geqslant B > 0$ and $B \leqslant 1$. Then*

$$\sum_{m=1}^{n-1} m^{B-1}(n-m)^{A-1} = \Gamma(B)\Gamma(A)\Gamma^{-1}(B+A)n^{B+A-1} + O(n^{A-1}).$$

PROOF OF THEOREM 1.7. Note from (1.9) that

$$\begin{aligned} J(n) &= \int_{-\frac{1}{2}}^{\frac{1}{2}} \sum_{m_1=1}^{n} \dots \sum_{m_s=1}^{n} \frac{1}{k^s}(m_1 \dots m_s)^{1/k-1} e((m_1 + \dots + m_s - n)\beta)\,\mathrm{d}\beta \\ &= \sum_{m_1=1}^{n} \dots \sum_{m_s=1}^{n} \frac{1}{k^s}(m_1 \dots m_s)^{1/k-1} \int_{-\frac{1}{2}}^{\frac{1}{2}} e((m_1 + \dots + m_s - n)\beta)\,\mathrm{d}\beta. \end{aligned}$$

Since

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} e((m_1 + \dots + m_s - n)\beta)\,\mathrm{d}\beta = \begin{cases} 1, & \text{if } m_1 + \dots + m_s = n, \\ 0, & \text{otherwise,} \end{cases}$$

it follows that

$$J(n) = \sum_{\substack{m_1=1 \\ m_1+\dots+m_s=n}}^{n} \dots \sum_{m_s=1}^{n} \frac{1}{k^s}(m_1 \dots m_s)^{1/k-1}.$$

For every integer $s \geqslant 2$, write

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

We prove by induction on s that

$$J_s(n) = \Gamma^s\left(1+\frac{1}{k}\right)\Gamma^{-1}\left(\frac{s}{k}\right)n^{s/k-1} + O(n^{s/k-1/k-1}). \tag{1.26}$$

Using Theorem 1.8 with $A = B = 1/k$, we have

$$\begin{aligned} J_2(n) &= \sum_{\substack{m_1=1 \\ m_1+m_2=n}}^{n} \sum_{m_2=1}^{n} \frac{1}{k^2}(m_1 m_2)^{1/k-1} = \frac{1}{k^2}\sum_{m=1}^{n-1} m^{1/k-1}(n-m)^{1/k-1} \\ &= \left(\frac{1}{k}\Gamma\left(\frac{1}{k}\right)\right)^2 \Gamma^{-1}\left(\frac{2}{k}\right)n^{2/k-1} + O(n^{1/k-1}) = \Gamma^2\left(1+\frac{1}{k}\right)\Gamma^{-1}\left(\frac{2}{k}\right)n^{2/k-1} + O(n^{1/k-1}). \end{aligned}$$

Suppose now that (1.26) holds for some particular integer $s \geqslant 2$. Then

$$\begin{aligned} J_{s+1}(n) &= \sum_{\substack{m=1 \\ m+m_1+\ldots+m_s=n}}^{n} \sum_{m_1=1}^{n} \ldots \sum_{m_s=1}^{n} \frac{1}{k^{s+1}} m^{1/k-1}(m_1 \ldots m_s)^{1/k-1} \\ &= \sum_{m=1}^{n-1} \frac{1}{k} m^{1/k-1} \sum_{\substack{m_1=1 \\ m_1+\ldots+m_s=n-m}}^{n-m} \ldots \sum_{m_s=1}^{n-m} \frac{1}{k^s}(m_1 \ldots m_s)^{1/k-1} = \sum_{m=1}^{n-1} \frac{1}{k} m^{1/k-1} J_s(n-m) \\ &= \sum_{m=1}^{n-1} \frac{1}{k} m^{1/k-1}\Gamma^s\left(1+\frac{1}{k}\right)\Gamma^{-1}\left(\frac{s}{k}\right)(n-m)^{s/k-1} + O\left(\sum_{m=1}^{n-1} m^{1/k-1}(n-m)^{s/k-1/k-1}\right) \\ &= \frac{1}{k}\Gamma^s\left(1+\frac{1}{k}\right)\Gamma^{-1}\left(\frac{s}{k}\right)\sum_{m=1}^{n-1} m^{1/k-1}(n-m)^{s/k-1} + O\left(\sum_{m=1}^{n-1} m^{1/k-1}(n-m)^{s/k-1/k-1}\right). \end{aligned}$$

Using Theorem 1.8 with $A = s/k$ and $B = 1/k$ on the main term and with $A = (s-1)/k$ and $B = 1/k$ on the error term, we have

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

This completes the proof. ◯

Proof of Theorem 1.8. Note that the function $x^{B-1}(n-x)^{A-1}$ has at most one stationary point in the interval $(0,n)$. It follows that the interval $(0,n)$ can be divided into two intervals $(0,X)$ and (X,n), one of which may be empty, such that $x^{B-1}(n-x)^{A-1}$ is monotonic in each interval. Hence

$$\begin{aligned} \sum_{m=1}^{n-1} m^{B-1}(n-m)^{A-1} &= \int_0^n x^{B-1}(n-x)^{A-1}\,\mathrm{d}x + O(n^{A-1} + n^{B+A-2}) \\ &= n^{B+A-1}\int_0^1 y^{B-1}(1-y)^{A-1}\,\mathrm{d}y + O(n^{A-1} + n^{B+A-2}) \\ &= \Gamma(B)\Gamma(A)\Gamma^{-1}(B+A)n^{B+A-1} + O(n^{A-1}), \end{aligned}$$

as required. ◯

REMARK. The gamma function is defined for $t > 0$ by

$$\Gamma(t) = \int_0^\infty \mathrm{e}^{-x} x^{t-1}\,\mathrm{d}x.$$

Using integration by parts, it is easily shown that

$$t\Gamma(t) = \Gamma(1+t)$$

for every $t > 0$. We now attempt to show that for every $A, B > 0$, we have

$$\Gamma(B)\Gamma(A) = \Gamma(B+A)\int_0^1 y^{B-1}(1-y)^{A-1}\,\mathrm{d}y. \tag{1.27}$$

Note first of all that

$$\Gamma(B)\Gamma(A) = \int_0^\infty \mathrm{e}^{-x}x^{B-1}\,\mathrm{d}x\int_0^\infty \mathrm{e}^{-y}y^{A-1}\,\mathrm{d}y = \lim_{M\to\infty}\iint\limits_{S(M)} \mathrm{e}^{-(x+y)}x^{B-1}y^{A-1}\,\mathrm{d}x\,\mathrm{d}y,$$

where $S(M)$ denotes the square $[0,M]^2$. Let $T(M)$ denote the triangle with vertices $(0,0)$, $(M,0)$ and $(0,M)$. Using the substitution $x = u$ and $y = v-u$ and then writing $u = vy$ in the inner integral, it is easily seen that

$$\begin{aligned}\iint\limits_{T(M)} \mathrm{e}^{-(x+y)}x^{B-1}y^{A-1}\,\mathrm{d}x\,\mathrm{d}y &= \int_0^M\left(\int_0^v \mathrm{e}^{-v}u^{B-1}(v-u)^{A-1}\,\mathrm{d}u\right)\mathrm{d}v\\ &= \int_0^M \mathrm{e}^{-v}v^{B+A-1}\,\mathrm{d}v\int_0^1 y^{B-1}(1-y)^{A-1}\,\mathrm{d}y.\end{aligned}$$

On the other hand, we clearly have $S(M/2) \subseteq T(M) \subseteq S(M)$, and so

$$\iint\limits_{S(M/2)} \mathrm{e}^{-(x+y)}x^{B-1}y^{A-1}\,\mathrm{d}x\,\mathrm{d}y \leqslant \iint\limits_{T(M)} \mathrm{e}^{-(x+y)}x^{B-1}y^{A-1}\,\mathrm{d}x\,\mathrm{d}y \leqslant \iint\limits_{S(M)} \mathrm{e}^{-(x+y)}x^{B-1}y^{A-1}\,\mathrm{d}x\,\mathrm{d}y.$$

It follows that

$$\int_0^M \mathrm{e}^{-v}v^{B+A-1}\,\mathrm{d}v\int_0^1 y^{B-1}(1-y)^{A-1}\,\mathrm{d}y \to \Gamma(B)\Gamma(A)$$

as $M\to\infty$. On the other hand,

$$\int_0^M \mathrm{e}^{-v}v^{B+A-1}\,\mathrm{d}v \to \Gamma(B+A)$$

as $M\to\infty$. The identity (1.27) follows immediately.

1.5. The Singular Series

In our discussion of the minor arcs, and in our discussion of the major arcs so far, we have made use only of the size of the natural number n that we are trying to represent as a sum of s k-th powers of natural numbers. We have had no input about the arithmetic properties of the natural number n.

For an equation

$$n = x_1^k + \ldots + x_s^k$$

to hold, it is necessary that the corresponding congruence

$$n \equiv x_1^k + \ldots + x_s^k$$

must hold modulo q for any natural number q. The purpose of this section is to use information on the solubility of the congruence to gain information on the solubility of the equation.

In particular, we are interested in studying the behaviour of the series

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

Here

$$S(q,a) = \sum_{m=1}^{q} e\left(\frac{am^k}{q}\right).$$

Our task is to show that $\mathfrak{S}(n) \gg 1$. This, together with (1.25) and Theorem 1.7, will imply that $R(n) > 0$ for all sufficiently large natural numbers n.

For every prime p, let

$$T(p) = \sum_{h=0}^{\infty} S(p^h).$$

Our first task is to reduce the study of the series $\mathfrak{S}(n)$ to the study of the series $T(p)$ for only finitely many primes p.

THEOREM 1.9. *Suppose that $s \geqslant 2^k + 1$. Then*

(i) *for every prime p, the series $T(p)$ converges absolutely;*
(ii) *the infinite product $\prod_p T(p)$ converges absolutely, with*

$$\mathfrak{S}(n) = \prod_p T(p);$$

and
(iii) *there is a positive real number C, depending only on k, such that*

$$\frac{1}{2} < \prod_{p \geqslant C} T(p) < \frac{3}{2}.$$

It follows that the study of the series $\mathfrak{S}(n)$ is reduced to the study of the series $T(p)$ for the primes $p < C$.

PROOF OF THEOREM 1.9. The absolute convergence of $T(p)$ follows easily from our observation earlier that $S(q) \ll q^{-1-2^{-k}}$. On the other hand, if the function $S(q)$ is multiplicative, so that $S(qr) = S(q)S(r)$ whenever $(q,r) = 1$, then

$$\prod_p T(p) = \prod_p \sum_{h=0}^{\infty} S(p^h) = \prod_p (1 + S(p) + S(p^2) + \ldots) = \sum_{q=1}^{\infty} S(q)$$

is a simple result in the theory of multiplicative functions and follows as a consequence of the absolute and uniform convergence of $\mathfrak{S}(n)$. The last part of the theorem is then a simple consequence of the convergence of the product representation of $\mathfrak{S}(n)$. It remains to prove that $S(qr) = S(q)S(r)$ whenever $(q,r) = 1$. We first of all show that if $(a,q) = (b,r) = (q,r) = 1$, then

$$S(qr, ar + bq) = S(q,a)S(r,b). \tag{1.28}$$

To see this, recall that since $(q,r) = 1$, it follows that as t runs through a complete set of residues modulo q and u runs through a complete set of residues modulo r, $tr + uq$ runs through a complete set of residues modulo qr. Hence

$$\begin{aligned} S(qr, ar + bq) &= \sum_{m=1}^{qr} e\left(\frac{(ar+bq)m^k}{qr}\right) = \sum_{t=1}^{q}\sum_{u=1}^{r} e\left(\frac{(ar+bq)(tr+uq)^k}{qr}\right) \\ &= \sum_{t=1}^{q}\sum_{u=1}^{r} e\left(\frac{(ar+bq)(t^k r^k + u^k q^k)}{qr}\right) = \sum_{t=1}^{q}\sum_{u=1}^{r} e\left(\frac{at^k r^k}{q} + \frac{bu^k q^k}{r}\right) \\ &= \sum_{t=1}^{q} e\left(\frac{at^k r^k}{q}\right) \sum_{u=1}^{r} e\left(\frac{bu^k q^k}{r}\right) = S(q,a)S(r,b), \end{aligned}$$

where the last step follows from the observation that since $(q,r) = 1$, tr runs through a complete set of residues modulo q as r runs through a complete set of residues modulo q, and uq runs through a complete set of residues modulo r as u runs through a complete set of residues modulo r. Next,

note that as a and b run through reduced sets of residues modulo q and r respectively, $ar+bq$ runs through a reduced set of residues modulo qr. In view of (1.28), we have

$$\begin{aligned}
S(qr) &= \sum_{\substack{m=1\\(m,qr)=1}}^{qr} ((qr)^{-1}S(qr,m))^s e\left(-\frac{mn}{qr}\right)\\
&= \sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{\substack{b=1\\(b,r)=1}}^{r} ((qr)^{-1}S(qr,ar+bq))^s e\left(-\frac{(ar+bq)n}{qr}\right)\\
&= \sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{\substack{b=1\\(b,r)=1}}^{r} ((qr)^{-1}S(q,a)S(r,b))^s e\left(-\left(\frac{an}{q}+\frac{bn}{r}\right)\right)\\
&= \sum_{\substack{a=1\\(a,q)=1}}^{q} (q^{-1}S(q,a))^s e\left(-\frac{an}{q}\right)\sum_{\substack{b=1\\(b,r)=1}}^{r} (r^{-1}S(r,b))^s e\left(-\frac{bn}{r}\right)\\
&= S(q)S(r),
\end{aligned}$$

as required. ◯

Our next task is to show that there is a close connection between T and the number $M_n(q)$ of solutions of the congruence

$$m_1^k+\ldots+m_s^k \equiv n \bmod q, \quad 1\leqslant m_1,\ldots,m_s\leqslant q.$$

Indeed, we use the following result.

THEOREM 1.10. *For every prime p, we have*

$$T(p)=\lim_{\ell\to\infty} p^{\ell(1-s)}M_n(p^\ell).$$

In fact, we prove the following more general result. The special case of Theorem 1.10 follows on letting $q=p^\ell$ and letting $\ell\to\infty$.

THEOREM 1.11. *For every natural number $q\in\mathbb{N}$, we have*

$$\sum_{d|q} S(d)=q^{1-s}M_n(q).$$

PROOF. It is easy to check that

$$\frac{1}{q}\sum_{u=1}^{q} e\left(\frac{uh}{q}\right)=\begin{cases} 1, & \text{if } q\mid h,\\ 0, & \text{if } q\nmid h.\end{cases}$$

Using this, it follows that

$$\begin{aligned}
M_n(q) &= \sum_{m_1=1}^{q}\cdots\sum_{m_s=1}^{q}\frac{1}{q}\sum_{u=1}^{q} e\left(\frac{u(m_1^k+\ldots+m_s^k-n)}{q}\right)\\
&= \frac{1}{q}\sum_{u=1}^{q}\sum_{m_1=1}^{q}\cdots\sum_{m_s=1}^{q} e\left(\frac{um_1^k}{q}\right)\ldots e\left(\frac{um_s^k}{q}\right)e\left(-\frac{un}{q}\right)\\
&= \frac{1}{q}\sum_{u=1}^{q}\left(\sum_{m=1}^{q} e\left(\frac{um^k}{q}\right)\right)^s e\left(-\frac{un}{q}\right).
\end{aligned}$$

Suppose that

$$\frac{q}{(u,q)}=d. \tag{1.29}$$

Then writing $a = u/(u,q)$ and noting that every $m = 1, \dots, q$ can be written uniquely in the form $dy + x$, where $y = 0, \dots, q/d - 1$ and $x = 1, \dots, d$, we have

$$\sum_{m=1}^{q} e\left(\frac{um^k}{q}\right) = \sum_{m=1}^{q} e\left(\frac{am^k}{d}\right) = \sum_{y=0}^{q/d-1} \sum_{x=1}^{d} e\left(\frac{a(dy+x)^k}{d}\right)$$
$$= \sum_{y=0}^{q/d-1} \sum_{x=1}^{d} e\left(\frac{ax^k}{d}\right) = \frac{q}{d} \sum_{x=1}^{d} e\left(\frac{ax^k}{d}\right) = qd^{-1}S(d,a).$$

Now, for every $u = 1, \dots, q$, there exists a unique $d \mid q$ such that (1.29) holds. For this value of d, the condition (1.29) is equivalent to the condition $(a,d) = 1$. It follows that

$$M_n(q) = \frac{1}{q} \sum_{d|q} \sum_{\substack{a=1 \\ (a,d)=1}}^{d} (qd^{-1}S(d,a))^s e\left(-\frac{an}{d}\right)$$
$$= q^{s-1} \sum_{d|q} \sum_{\substack{a=1 \\ (a,d)=1}}^{d} (d^{-1}S(d,a))^s e\left(-\frac{an}{d}\right) = q^{s-1} \sum_{d|q} S(d),$$

as required. ◯

To use Theorem 1.10, we need to investigate, for every fixed prime p, congruences of the form

$$m_1^k + \ldots + m_s^k \equiv n \bmod p^\ell, \quad 1 \leqslant m_1, \dots, m_s \leqslant p^\ell, \tag{1.30}$$

for all sufficiently large natural numbers ℓ.

Naturally, we are seeking good lower bounds for $T(p)$. We therefore need to estimate from below the number $M_n(p^\ell)$ of solutions of the congruence (1.30). Indeed, we would like to estimate $M_n(p^\ell)$ for larger values of ℓ by using estimates of $M_n(p^\ell)$ for smaller values of ℓ. In practice, our strategy is slightly more complicated. We find a value γ so that the congruence (1.30) is soluble for $\ell = \gamma$ and with the extra condition that $(m_1, p^\gamma) = 1$. This extra condition makes it relatively simple to obtain good lower bounds for $M_n(p^\ell)$ when $\ell \geqslant \gamma$.

Before we embark on this strategy, we need to make a few comments on k-th power residues.

REMARKS. (i) Suppose that p is a prime and $\ell \in \mathbb{N}$. A number $a \in \mathbb{Z}$ is said to be a k-th power residue modulo p^ℓ if $p \nmid a$ and the congruence $x^k \equiv a \bmod p^\ell$ is soluble. The number of k-th power residues modulo p^ℓ is the number of integers $a \in \mathbb{Z}$ such that $1 \leqslant a \leqslant p^\ell$ and a is a k-th power residue modulo p^ℓ.

(ii) The number $\nu(p^\ell)$ of k-th power residues modulo p^ℓ satisfies

$$\nu(p^\ell) = \begin{cases} \dfrac{\phi(p^\ell)}{(k, \phi(p^\ell))}, & \text{if } p > 2 \text{ or } \ell = 1 \text{ or } k \text{ is odd,} \\ \dfrac{2^{\ell-2}}{(k, 2^{\ell-2})}, & \text{if } p = 2 \text{ and } \ell \geqslant 2 \text{ and } k \text{ is even.} \end{cases}$$

(iii) Suppose that $\tau \in \mathbb{Z}$ satisfies

$$p^\tau \mid k \quad \text{and} \quad p^{\tau+1} \nmid k.$$

It is convenient to define

$$\gamma = \begin{cases} \tau + 1, & \text{if } p > 2 \text{ or } \tau = 0, \\ \tau + 2, & \text{if } p = 2 \text{ and } \tau > 0. \end{cases}$$

Then

$$\nu(p^\gamma) = \frac{\phi(p^{\tau+1})}{(k, \phi(p^{\tau+1}))}.$$

(iv) The number of solutions of the congruence

$$x^k \equiv a \bmod p^\gamma$$

when $p \nmid a$ is either 0 or $p^{\gamma-\tau-1}(k, \phi(p^{\tau+1}))$.

(v) If a is a k-th power residue modulo p^γ, then it is a k-th power residue modulo p^ℓ for every natural number $\ell \in \mathbb{N}$.

For every natural number $q \in \mathbb{N}$, let $M_n^*(q)$ denote the number of solutions of the congruence

$$m_1^k + \ldots + m_s^k \equiv n \bmod q, \quad 1 \leqslant m_1, \ldots, m_s \leqslant q, \ (m_1, q) = 1.$$

THEOREM 1.12. *Suppose that $M_n^*(p^\gamma) > 0$. Then for every natural number $\ell \geqslant \gamma$, we have*

$$M_n(p^\ell) \geqslant p^{(\ell-\gamma)(s-1)}.$$

PROOF. Suppose that

$$x_1^k \equiv n - x_2^k - \ldots - x_s^k \bmod p^\gamma,$$

where $1 \leqslant x_1, \ldots, x_s \leqslant p^\gamma$ and $p \nmid x_1$. For every $j = 2, \ldots, s$, there are precisely $p^{\ell-\gamma}$ integers y_j satisfying $1 \leqslant y_j \leqslant p^\ell$ and $y_j \equiv x_j \bmod p^\gamma$. It follows that for each of the $p^{(\ell-\gamma)(s-1)}$ choices of $(s-1)$-tuples $(y_2, \ldots, y_s)$, the number $n - y_2^k - \ldots - y_s^k$ is a k-th power residue modulo p^γ, and so a k-th power residue modulo p^ℓ. Hence there exists y_1 satisfying $1 \leqslant y_1 \leqslant p^\ell$ and $p \nmid y_1$ such that

$$y_1^k \equiv n - y_2^k - \ldots - y_s^k \bmod p^\ell.$$

The result follows immediately. ◯

It now follows from Theorems 1.10 and 1.12 that if $M_n^*(p^\gamma) > 0$, then

$$T(p) = \lim_{\ell \to \infty} p^{\ell(1-s)} M_n(p^\ell) \geqslant p^{-\gamma(s-1)}.$$

If we now use this inequality for every prime $p < C$, then it follows from Theorem 1.9 that $\mathfrak{S}(n) \gg 1$. It therefore remains to prove the following result.

THEOREM 1.13. *Suppose that*

$$s \geqslant \begin{cases} \dfrac{p}{p-1}(k, p^\tau(p-1)), & \text{if } p > 2, \\ 2^{\tau+2}, & \text{if } p = 2 \text{ and } k > 2, \\ 5, & \text{if } p = 2 \text{ and } k = 2. \end{cases}$$

Then $M_n^*(p^\gamma) > 0$ for every natural number $n \in \mathbb{N}$.

The case $p = 2$ and $k = 2$ is very easy. If $p = 2$ and $k > 2$, then one has $s \geqslant 2^\gamma$, and the congruence

$$m_1^k + \ldots + m_s^k \equiv n \bmod 2^\gamma, \quad 1 \leqslant m_1, \ldots, m_s \leqslant 2^\gamma, \ 2 \nmid m_1,$$

can be satisfied by taking m_j to be 0 or 1. When p is odd, we apply the following result repeatedly.

THEOREM 1.14 (Cauchy–Davenport–Chowla). *Suppose that*

$$\mathcal{A} = \{x_1, \ldots, x_r\} \quad \text{and} \quad \mathcal{B} = \{y_1, \ldots, y_s\}$$

denote respectively r and s incongruent residue classes modulo q. Suppose further that $0 \in \mathcal{B}$ and that $(y_j, q) = 1$ for every $j = 1, \ldots, s$ satisfying $y_j \not\equiv 0 \bmod q$. If $\mathcal{A} + \mathcal{B}$ denote the set of residue classes of the form

$$x_i + y_j, \quad i = 1, \ldots, r, \ j = 1, \ldots, s,$$

then $\#(\mathcal{A} + \mathcal{B}) \geqslant \min\{q, r + s - 1\}$.

PROOF. We may suppose that $r + s - 1 \leqslant q$, for otherwise we simply remove some elements from $\mathcal{B}$. We may also assume that $r < q$ and $y_1 = 0$. The proof of the theorem is by induction on s. The case $s = 1$ is trivial. Suppose now that $s > 1$. We claim that there exist $x_\mu \in \mathcal{A}$ and $y_\nu \in \mathcal{B}$ such that $x_\mu + y_\nu \notin \mathcal{A}$; otherwise, for every $y_j \in \mathcal{B}$, $x_i + y_j$ would run over $\mathcal{A}$ as x_i ran over $\mathcal{A}$, so that

$$\sum_{i=1}^{r} (x_i + y_j) \equiv \sum_{i=1}^{r} x_i \bmod q,$$

and so $ry_j \equiv 0 \bmod q$ for every $j = 1, \ldots, s$, clearly an impossibility. Rearranging the elements of $\mathcal{A}$ and $\mathcal{B}$ if necessary, we may assume that $\mu = 1$ and that there exists $t = 2, \ldots, s$ such that

$$x_1 + y_j \begin{cases} \in \mathcal{A}, & \text{if } j = 1, \ldots, t-1, \\ \notin \mathcal{A}, & \text{if } j = t, \ldots, s. \end{cases}$$

Let

$$\mathcal{A}_1 = \mathcal{A} \cup (\{x_1\} + \{y_t, \dots, y_s\}) \quad \text{and} \quad \mathcal{B}_1 = \{y_1, \dots, y_{t-1}\}.$$

Then $1 \leqslant \#\mathcal{B}_1 < s$ and $\#\mathcal{A}_1 + \#\mathcal{B}_1 = r + s$. Also,

$$\begin{aligned}\mathcal{A}_1 + \mathcal{B}_1 &= (\mathcal{A} + \mathcal{B}_1) \cup (\{x_1\} + \{y_t, \dots, y_s\}) + \{y_1, \dots, y_{t-1}\}) \\ &= (\mathcal{A} + \mathcal{B}_1) \cup (\{x_1\} + \{y_1, \dots, y_{t-1}\}) + \{y_t, \dots, y_s\}) \\ &\subseteq \mathcal{A} + \mathcal{B}.\end{aligned}$$

The result follows. ◯

1.6. Weyl's Inequality and Hua's Lemma

The proofs of Weyl's inequality and Hua's lemma depend on an intermediate result best described in terms of the forward difference operator.

Suppose that ϕ is a real valued function of a real variable. For any $x, h_1 \in \mathbb{R}$, write

$$\Delta_1(\phi(x); h_1) = \phi(x + h_1) - \phi(x).$$

We now denote by Δ_j the j-th iterate of the forward difference operator Δ_1. In other words, we write

$$\Delta_{j+1}(\phi(x); h_1, \dots, h_{j+1}) = \Delta_1(\Delta_j(\phi(x); h_1, \dots, h_j); h_{j+1}).$$

Remark. It can be shown that for any natural numbers $j \leqslant k$, the j-th iterate Δ_j of the forward difference operator satisfies

$$\Delta_j(x^k; h_1, \dots, h_j) = \sum_{\substack{\ell_0 \geqslant 0, \ell_1 \geqslant 1, \dots, \ell_j \geqslant 1 \\ \ell_0 + \ell_1 + \dots + \ell_j = k}} \frac{k!}{\ell_0! \ell_1! \dots \ell_j!} x^{\ell_0} h_1^{\ell_1} \dots h_j^{\ell_j} = h_1 \dots h_j p_j(x; h_1, \dots, h_j),$$

where $p_j(x; h_1, \dots, h_j)$ is a polynomial in x with integer coefficients, of degree $k - j$ and with leading coefficient $k!/(k-j)!$.

Theorem 1.15. *Suppose that*

$$T(\phi) = \sum_{x=1}^{Q} e(\phi(x)),$$

where $\phi : \mathbb{N} \to \mathbb{R}$ is an arithmetic function. Then for any natural number $j \in \mathbb{N}$, we have

$$|T(\phi)|^{2^j} \leqslant (2Q)^{2^j - j - 1} \sum_{|h_1| < Q} \dots \sum_{|h_j| < Q} \sum_{x \in I_j} e(\Delta_j(\phi(x); h_1, \dots, h_j)),$$

where the intervals $I_j = I_j(h_1, \dots, h_j)$ satisfy the conditions

$$I_1(h_1) \subseteq [1, Q] \quad \text{and} \quad I_j(h_1, \dots, h_j) \subseteq I_{j-1}(h_1, \dots, h_{j-1}).$$

Proof. We proceed by induction on j. Suppose first of all that $j = 1$. Then

$$\begin{aligned}|T(\phi)|^2 &= \sum_{x=1}^{Q} \sum_{y=1}^{Q} e(\phi(y) - \phi(x)) = \sum_{x=1}^{Q} \sum_{h_1 = 1-x}^{Q-x} e(\phi(x + h_1) - \phi(x)) = \sum_{x=1}^{Q} \sum_{h_1 = 1-x}^{Q-x} e(\Delta_1(\phi(x); h_1)) \\ &= \sum_{h_1 = 1-Q}^{Q-1} \sum_{x \in I_1} e(\Delta_1(\phi(x); h_1)) = \sum_{|h_1| < Q} \sum_{x \in I_1} e(\Delta_1(\phi(x); h_1)),\end{aligned}$$

where $I_1 = [1, Q] \cap [1 - h_1, Q - h_1]$. Suppose now that the conclusion of the theorem holds for a particular natural number $j \in \mathbb{N}$, so that

$$|T(\phi)|^{2^j} \leqslant (2Q)^{2^j - j - 1} \sum_{|h_1| < Q} \dots \sum_{|h_j| < Q} \sum_{x \in I_j} e(\Delta_j(\phi(x); h_1, \dots, h_j)).$$

Then by Cauchy's inequality, we have

$$|T(\phi)|^{2^{j+1}} \leqslant (2Q)^{2^{j+1} - 2j - 2} (2Q - 1)^j \sum_{|h_1| < Q} \dots \sum_{|h_j| < Q} \left| \sum_{x \in I_j} e(\Delta_j(\phi(x); h_1, \dots, h_j)) \right|^2.$$

Note next that

$$\begin{aligned}\left|\sum_{x\in I_j} e(\Delta_j(\phi(x);h_1,\dots,h_j))\right|^2 &= \sum_{x\in I_j}\sum_{y\in I_j} e(\Delta_j(\phi(y);h_1,\dots,h_j)-\Delta_j(\phi(x);h_1,\dots,h_j))\\ &= \sum_{|h|<Q}\sum_{x\in I_{j+1}} e(\Delta_j(\phi(x+h);h_1,\dots,h_j)-\Delta_j(\phi(x);h_1,\dots,h_j))\\ &= \sum_{|h|<Q}\sum_{x\in I_{j+1}} e(\Delta_1(\Delta_j(\phi(x);h_1,\dots,h_j);h))\\ &= \sum_{|h|<Q}\sum_{x\in I_{j+1}} e(\Delta_{j+1}(\phi(x);h_1,\dots,h_j,h)),\end{aligned}$$

where $I_{j+1}=I_j\cap\{x: x+h\in I_j\}$. This gives the conclusion of the theorem with j replaced by $j+1$. ◯

The next step concerns an estimate which arises when we use Theorem 1.15 in the deduction of Weyl's inequality. It is stated in a more general form than we need here. The generality is necessary in our discussion of the ternary Goldbach problem in Chapter 2.

THEOREM 1.16. *Suppose that $X,Y,\alpha\in\mathbb{R}$ with $X,Y\geqslant 1$. Suppose further that $|\alpha-a/q|\leqslant q^{-2}$ with $(a,q)=1$. Then*

$$\sum_{x\leqslant X}\min\{XYx^{-1},\|\alpha x\|^{-1}\}\ll XY\left(\frac{1}{q}+\frac{1}{Y}+\frac{q}{XY}\right)\log(2Xq),$$

where $\|\beta\|=\min_{n\in\mathbb{Z}}|\beta-n|$ denotes the distance of β to the nearest integer.

PROOF. Write

$$S=\sum_{x\leqslant X}\min\{XYx^{-1},\|\alpha x\|^{-1}\}.$$

Clearly every natural number $x\leqslant X$ can be written in the form $qj+r$, where the integers j and r satisfy $0\leqslant j\leqslant X/q$ and $1\leqslant r\leqslant q$. Hence

$$S\leqslant\sum_{0\leqslant j\leqslant X/q}\sum_{r=1}^{q}\min\left\{\frac{XY}{qj+r},\|\alpha(qj+r)\|^{-1}\right\}.$$

We can write

$$\begin{aligned}\alpha(qj+r)=\alpha qj+\frac{ar}{q}+\left(\alpha-\frac{a}{q}\right)r &= \frac{[\alpha q^2j]+\{\alpha q^2j\}}{q}+\frac{ar}{q}+\frac{(q^2\alpha-qa)r}{q^2}\\ &= \frac{[\alpha q^2j]+ar}{q}+\frac{\{\alpha q^2j\}}{q}+\frac{(q^2\alpha-qa)r}{q^2}.\end{aligned}$$

Suppose first of all that $j=0$ and $r\leqslant q/2$. Then

$$\alpha(qj+r)=\frac{ar}{q}+\frac{(q^2\alpha-qa)r}{q^2}\quad\text{and}\quad\left|\frac{(q^2\alpha-qa)r}{q^2}\right|\leqslant\frac{r}{q^2}\leqslant\frac{1}{2q},$$

and so

$$\|\alpha(qj+r)\|\geqslant\left\|\frac{ar}{q}\right\|-\frac{1}{2q}\geqslant\frac{1}{2}\left\|\frac{ar}{q}\right\|.$$

On the other hand, we always have

$$\left|\frac{\{\alpha q^2j\}}{q}+\frac{(q^2\alpha-qa)r}{q^2}\right|\leqslant\frac{1}{q}+\frac{r}{q^2}\leqslant\frac{2}{q}.$$

For every j satisfying $0\leqslant j\leqslant X/q$, as r runs over a complete set of residues modulo q, $[\alpha q^2j]+ar$ also runs through a complete set of residues modulo q. It follows that for any j satisfying $0\leqslant j\leqslant X/q$, there are at most 7 values of r for which the inequality

$$\|\alpha(qj+r)\|\geqslant\frac{1}{2}\left\|\frac{[\alpha q^2j]+ar}{q}\right\|$$

fails to hold. Note also that $qj+r \gg q(j+1)$ if $j \neq 0$ or $r > q/2$. It follows that

$$\begin{aligned} S &\ll \sum_{1\leqslant r\leqslant \frac{1}{2}q} \left\| \frac{ar}{q} \right\|^{-1} + \sum_{0\leqslant j\leqslant X/q} \left(\frac{XY}{q(j+1)} + \sum_{\substack{r=1 \\ q\nmid [\alpha q^2 j]+ar}}^{q} \left\| \frac{[\alpha q^2 j]+ar}{q} \right\|^{-1} \right) \\ &\ll \frac{XY}{q} \sum_{0\leqslant j\leqslant X} \frac{1}{j+1} + \left(\frac{X}{q} + 1 \right) \sum_{1\leqslant h\leqslant \frac{1}{2}q} \left(\frac{h}{q} \right)^{-1} \\ &\ll \frac{XY}{q} \log(2X) + (X+q)\log q. \end{aligned}$$

The theorem follows immediately. ◯

Proof of Theorem 1.3. We apply Theorem 1.15 with $j = k-1$, $Q = N$ and $\phi(x) = \alpha x^k$ to obtain

$$|f(\alpha)|^K \leqslant (2N)^{K-k} \sum_{|h_1|<N} \dots \sum_{|h_{k-1}|<N} \sum_{x\in I_{k-1}} e(\Delta_{k-1}(\alpha x^k; h_1, \dots, h_{k-1})).$$

By the Remark preceding Theorem 1.15, we have

$$\Delta_{k-1}(\alpha x^k; h_1, \dots, h_{k-1}) = k!\alpha h_1 \dots h_{k-1} \left(x + \frac{h_1}{2} + \dots + \frac{h_{k-1}}{2} \right),$$

so that

$$|f(\alpha)|^K \leqslant (2N)^{K-k} \sum_{|h_1|<N} \dots \sum_{|h_{k-1}|<N} \sum_{x\in I_{k-1}} e\left(k!\alpha h_1 \dots h_{k-1} \left(x + \frac{h_1}{2} + \dots + \frac{h_{k-1}}{2} \right) \right).$$

The terms with $h_1 \dots h_{k-1} = 0$ contribute $\ll N^{k-1}$ to the sum. Hence

$$\begin{aligned} |f(\alpha)|^K &\ll (2N)^{K-k} \left(N^{k-1} + N^{\epsilon} \sum_{h=1}^{k!N^{k-1}} \min\{N, \|\alpha h\|^{-1}\} \right) \\ &\ll N^{K-k+\epsilon} \left(N^{k-1} + \sum_{h=1}^{k!N^{k-1}} \min\{k!N^k h^{-1}, \|\alpha h\|^{-1}\} \right), \end{aligned}$$

where the term N^{ϵ} is an upper bound on the number of solutions of the equation

$$k!h_1 \dots h_{k-1} = h, \quad 0 < |h_1|, \dots, |h_{k-1}| < N.$$

We now apply Theorem 1.16 with $X = k!N^{k-1}$ and $Y = N$ to obtain

$$\sum_{h=1}^{k!N^{k-1}} \min\{k!N^k h^{-1}, \|\alpha h\|^{-1}\} \ll N^k \left(\frac{1}{q} + \frac{1}{N} + \frac{q}{N^k} \right) \log(N^{k-1}q).$$

This gives

$$|f(\alpha)|^K \ll N^{K+2\epsilon}(q^{-1} + N^{-1} + qN^{-k})$$

if $q \leqslant N^k$. The proof is now complete on noting that the result is trivial if $q > N^k$. ◯

Proof of Theorem 1.2. We proceed by induction on j. Suppose first of all that $j = 1$. Then the integral

$$\int_0^1 |f(\alpha)|^2 \, \mathrm{d}\alpha$$

is equal to the number of solutions of the equation $x^k - y^k = 0$ in natural numbers $x, y \leqslant N$. Clearly there are precisely N solutions. Suppose now that the inequality (1.6) holds for some natural number j satisfying $1 \leqslant j < k$. We apply Theorem 1.15 with $Q = N$ and $\phi(x) = \alpha x^k$ to obtain

$$|f(\alpha)|^{2^j} \leqslant (2N)^{2^j - j - 1} \sum_{|h_1|<N} \dots \sum_{|h_j|<N} \sum_{x\in I_j} e(\Delta_j(\alpha x^k; h_1, \dots, h_j)),$$

where, by the Remark preceding Theorem 1.15,

$$\Delta_j(\alpha x^k; h_1, \dots, h_j) = \alpha h_1 \dots h_j p_j(x; h_1, \dots, h_j),$$

where $p_j(x; h_1, \dots, h_j)$ is a polynomial in x of degree $k-j$ and with integer coefficients. Hence

$$|f(\alpha)|^{2^j} \ll (2N)^{2^j-j-1} \sum_{h\in\mathbb{Z}} c_h e(\alpha h), \tag{1.31}$$

where, for every $h \in \mathbb{Z}$, c_h denotes the number of solutions of the equation

$$h_1 \dots h_j p_j(x; h_1, \dots, h_j) = h, \quad |h_1|, \dots, |h_j| < N,\ x \in I_j.$$

It is well known that $c_0 \ll N^j$ and $c_h \ll N^\epsilon$ if $h \neq 0$. On the other hand, we can write

$$|f(\alpha)|^{2^j} = (f(\alpha))^{2^{j-1}} (f(-\alpha))^{2^{j-1}} = \sum_{h\in\mathbb{Z}} b_h e(-\alpha h), \tag{1.32}$$

where, for every $h \in \mathbb{Z}$, b_h denotes the number of solutions of the equation

$$x_1^k + \dots + x_{2^{j-1}}^k - y_1^k + \dots - y_{2^{j-1}}^k = h, \quad 1 \leqslant x_1, \dots, x_{2^{j-1}}, y_1, \dots, y_{2^{j-1}} \leqslant N.$$

Hence

$$\sum_{h\in\mathbb{Z}} b_h = |f(0)|^{2^j} = N^{2^j}.$$

Also, by the induction hypothesis, we have

$$b_0 = \int_0^1 |f(\alpha)|^{2^j}\, \mathrm{d}\alpha \ll N^{2^j-j+\epsilon}.$$

It now follows from (1.31), (1.32) and Parseval's identity that

$$\int_0^1 |f(\alpha)|^{2^{j+1}}\, \mathrm{d}\alpha \ll (2N)^{2^j-j-1} \sum_{h\in\mathbb{Z}} c_h b_h.$$

Note now that

$$\sum_{h\in\mathbb{Z}} c_h b_h \ll c_0 b_0 + N^\epsilon \sum_{h\neq 0} b_h \ll N^j N^{2^j-j+\epsilon} + N^\epsilon N^{2^j},$$

so that

$$\int_0^1 |f(\alpha)|^{2^{j+1}}\, \mathrm{d}\alpha \ll N^{2^{j+1}-j-1+\epsilon}.$$

This completes the proof. ◯