SUMS OF FIFTH POWERS AND RELATED TOPICS

Koichi Kawada[1] and Trevor D. Wooley[2]

1. Introduction

In recent years our understanding of various problems of additive type involving sums of kth powers of integers has been advanced by corresponding progress in estimates for exponential sums. The bulk of these improvements have been engineered through the use of smooth Weyl sums and their close kin (see, for example, [8], [11] and [12]). In a recent memoir [4] devoted to various problems involving sums of biquadrates, the authors applied the identity

$$x^4 + y^4 + (x+y)^4 = 2(x^2 + xy + y^2)^2 \tag{1.1}$$

to obtain new conclusions beyond the reach of the current technology involving smooth Weyl sums. The key observation of [4] is that the identity (1.1) enables sums of three biquadrates to be treated as a square, at least in so far as mean value estimates for exponential sums are concerned. Thus we were able to employ in our investigations the extensive apparatus of the Hardy-Littlewood method devoted to mixed problems involving squares, biquadrates and so on. The purpose of this paper is to develop an analogous treatment for sums of fifth powers and related polynomials. Although for problems involving pure fifth powers our conclusions are not as sharp as those attainable through the use of smooth Weyl sums, in contrast to the latter methods we are able to treat sums of quite general quintic polynomials.

We illustrate our ideas with two theorems, the first of which we establish in §3.

Theorem 1. *Let $\phi(x)$ denote a quintic polynomial with rational coefficients taking integral values at integer values of the argument x. When X is a large real number, write $\mathcal{N}(X)$ for the number of integers n with $1 \le n \le X$ which are represented in the form*

$$n = \phi(x_1) + \phi(x_2) + \cdots + \phi(x_{10}), \tag{1.2}$$

1991 *Mathematics Subject Classification.* 11P05, 11P55.

Key words and phrases. Sums of fifth powers, quintic polynomials, Waring's problem.

[1]Written while the author visited the University of Michigan at Ann Arbor, and enjoyed the benefits of a Fellowship from the David and Lucile Packard Foundation.

[2]Packard Fellow and supported in part by NSF grant DMS-9622773. This paper was completed while the author was enjoying the hospitality of the Department of Mathematics at Princeton University.

with $x_i \in \mathbb{N}$ $(1 \le i \le 10)$ *or with* $-x_i \in \mathbb{N}$ $(1 \le i \le 10)$*. Then for each positive number* ε *one has*

$$\mathcal{N}(X) \gg_\varepsilon X^{1-\varepsilon}.$$

We note that in the special case in which the polynomials ϕ under consideration are pure fifth powers, one can establish sharper conclusions through the use of smooth Weyl sums (see [1], [10] and [11]). In particular, the latter techniques may be wielded to show that sums of 9 fifth powers have positive density. For arbitrary polynomials, the sharpest bounds hitherto available stem from the diminishing ranges techniques of Thanigasalam [6] and Vaughan [7], although such bounds are recorded in the literature only in the special case where the polynomials are fifth powers. In the latter circumstances, for example, [7, equation (3.20)] is tantamount to the lower bound

$$\mathcal{N}(X) \gg X^{0.99575}.$$

We investigate Waring's problem for quintic polynomials in §§4-9.

Theorem 2. *Let* $\phi(x)$ *and* $\psi(x)$ *denote polynomials with rational coefficients taking integral values at integer values of the argument* x*, and having respective degrees* 5 *and* $k \ge 2$*. Let* $\mathcal{L}$ *denote the set of positive integers,* n*, for which the congruence*

$$\sum_{i=1}^{20} \phi(x_i) + \psi(x_{21}) \equiv n \pmod q \tag{1.3}$$

has a solution for all $q \in \mathbb{N}$*. Then the set* $\mathcal{L}$ *has positive density, and every sufficiently large integer* n *with* $n \in \mathcal{L}$ *can be written in the form*

$$n = \sum_{i=1}^{20} \phi(x_i) + \psi(x_{21}), \tag{1.4}$$

with $x_i \in \mathbb{Z}$ $(1 \le i \le 21)$*.*

We note that in the special case in which the polynomials ϕ and ψ are both fifth powers, the number of summands may be reduced from 21 to 17 (see [11]). Moreover the aforementioned techniques of Thanigasalam [6] and Vaughan [7] should permit the conclusion of Theorem 2 to be established whenever $\psi(x)$ has degree $k \le 6$. However, the sharpest result along these lines available in the literature is apparently due to H. B. Yu [13], who proves an analogue of Theorem 2 which shows that whenever n is a sufficiently large natural number satisfying a local solubility hypothesis analogous to (1.3), then n can be written in the form

$$n = \sum_{i=1}^{24} \phi(x_i)$$

(we note that Yu also remarks on the possibility of applying the methods of Vaughan [7] so as to reduce the number of summands from 24 to 21). As an immediate consequence of Theorem 2 above one may reduce the number of summands in the latter representation from 24 to 21.

A few remarks are in order concerning the local solubility condition implicit in Theorem 2. Suppose that $\Phi(x)$ is a quintic polynomial with rational coefficients taking integral values at integer values of the argument x. We can easily assume that $\Phi(0) = 0$. Write d_Φ for the highest common factor amongst all the values of $\Phi(x)$ as x varies over $\mathbb{Z}$. Then whenever $d_\Phi > 1$, any integer represented as a sum of values of $\Phi(x)$ must necessarily be divisible by d_Φ. For the purposes of this discussion, therefore, it makes sense to define a new polynomial $\widetilde{\Phi}(x) = d_\Phi^{-1}\Phi(x)$ with $d_{\widetilde{\Phi}} = 1$, and to consider the representation of integers n in the form

$$n = \widetilde{\Phi}(x_1) + \widetilde{\Phi}(x_2) + \cdots + \widetilde{\Phi}(x_s). \tag{1.5}$$

When

$$\widetilde{\Phi}(x) = 16F_5(x) - 8F_4(x) + 4F_3(x) - 2F_2(x) + F_1(x), \tag{1.6}$$

in which

$$F_i(x) = x(x-1)\dots(x-i+1)/i! \quad (1 \le i \le 5),$$

it follows from work of Hua [3] that whenever $s < 31$, there is a certain arithmetic progression of integers n for which the equation (1.5) is locally insoluble. Consequently, at least when the polynomial $\psi(x)$ is equal to the quintic polynomial $\phi(x)$, the local solubility condition described in the statement of Theorem 2 is necessary. However, rather recent work of Yu [13] shows that Hua's example (1.6) is essentially the only barrier to local solubility when $s \ge 16$. Thus, if $\phi(x)$ satisfies the hypothesis that $d_\phi = 1$, and

$$2 \nmid \phi(1) \quad \text{and} \quad \phi(x) \equiv \phi(1)\widetilde{\Phi}(x) \pmod{32}, \tag{1.7}$$

in which $\widetilde{\Phi}(x)$ is defined by (1.6), then the congruence

$$n \equiv \phi(x_1) + \phi(x_2) + \cdots + \phi(x_s) \pmod{q} \tag{1.8}$$

is soluble for each natural number q whenever $s \ge 31$, and when $s < 31$ there is an arithmetic progression of integers, and a modulus q, for which (1.8) is insoluble. Meanwhile, if the polynomial $\phi(x)$ does not satisfy (1.7), then the congruence (1.8) is soluble for each natural number q whenever $s \ge 16$. Consequently, for polynomials $\phi(x)$ satisfying $d_\phi = 1$, the local solubility condition implicit in (1.3) may be ignored provided only that $\phi(x)$ does not satisfy (1.7) (and, moreover, this conclusion is independent of the polynomial $\psi(x)$).

In its simplest form, the polynomial identity underlying our proofs of Theorems 1 and 2 takes the shape

$$\begin{aligned}(h+x)^5 + (h+y)^5 + (h+x+y)^5 + (h-x)^5 + (h-y)^5 + (h-x-y)^5 \\ = 2h\left(10(x^2+xy+y^2)^2 + 20h^2(x^2+xy+y^2) + 3h^4\right),\end{aligned} \tag{1.9}$$

an identity which one can recognise as being closely related to (1.1) through the observation that for a fixed h, the polynomial $(h+x)^5+(h-x)^5$ takes the quartic shape at^4+bt^2+c amenable to (1.1). Our idea is to use (1.9) to specialise 6 fifth powers (or more generally 6 quintic polynomials) in such a way that their sum may be treated as a cubic polynomial with a linear factor. Although one of the variables occurring in the latter polynomial is restricted to the values of the binary quadratic form x^2+xy+y^2, the integers represented by the latter polynomial are rather dense amongst the rational integers. Thus, by making use of the identity (1.9) within suitable mean values of exponential sums, one may wield the tools applicable to such mixed problems familiar to practitioners of the Hardy-Littlewood method. Of course, in order to handle quite general quintic polynomials one must adjust the scheme described above, but it transpires that such adjustments are not fatal to our proposed course of action.

Throughout, the letter k denotes a fixed integer exceeding 1. We adopt the convention that whenever the letter ε appears in a statement, either explicitly or implicitly, then we assert that the statement holds for every sufficiently small positive number ε. The "value" of ε may consequently change from statement to statement. The implicit constants in Vinogradov's notation $\ll$ and $\gg$, and in Landau's notation, will depend at most on k, ε and the coefficients of the polynomials ϕ and ψ, unless stated otherwise. When x is a real number, we write $[x]$ for the greatest integer not exceeding x, and when n is an integer and p is a prime number we write $p^r\|n$ when $p^r|n$ but $p^{r+1}\nmid n$. Finally, we adopt the convention throughout that any variable denoted by the letter p is implicitly assumed to be a prime number.

2. Preliminaries

We begin with some simplifying observations which ease our subsequent deliberations. We also exploit this opportunity to record some notation. Let $\phi(x)$ and $\psi(x)$ be polynomials satisfying the hypotheses of Theorem 2 (of course, the hypotheses of the statement of Theorem 1 are then automatically satisfied by $\phi(x)$). Let c be the least natural number with the property that $c\psi(x)\in\mathbb{Z}[x]$, and when q is a natural number, define the integer $\lambda(q)=\lambda(q,\psi)$ by

$$\lambda(q,\psi)=q\prod_{\substack{p|q\\ p^t\|c}}p^t. \tag{2.1}$$

Let b be the least natural number with the property that $b\phi(x)\in\mathbb{Z}[x]$. Then on observing that the representation (1.4) of the integer n is equivalent to

$$\sum_{j=1}^{20} b(\phi(x_j)-\phi(0))+b\psi(x)=b(n-20\phi(0)),$$

it is evident that there is no loss of generality in assuming that the polynomial $\phi(x)$ has integer coefficients, and that $\phi(0)=0$. We may also suppose without loss of generality that the leading coefficient of $\phi(x)$ is positive, for we may replace $\phi(x)$ by $\phi(-x)$ whenever necessary.

Having made the transformations described in the previous paragraph, let d denote the least common divisor of the coefficients of $\phi(x)$. Suppose that the integer n which we seek to represent in the form (1.4) satisfies $n \equiv r \pmod{d}$, with $1 \le r \le d$. Then in view of the presumed solubility of the congruence (1.3), there exists an integer s with $1 \le s \le \lambda(d)$ such that whenever $x \equiv s \pmod{\lambda(d)}$, one has $\psi(x) \equiv r \pmod{d}$. But if we write

$$\psi_1(x) = d^{-1}(\psi(\lambda(d)x + s) - r),$$

then we find that the representation (1.4) of n is derived from the representation of the integer $(n-r)/d$ provided by

$$\sum_{j=1}^{20} d^{-1}\phi(x_j) + \psi_1(x_{21}) = (n-r)/d.$$

We may consequently suppose without loss of generality that $d = 1$, by simply replacing $\phi(x)$ by $\phi(x)/d$, and $\psi(x)$ by $\psi_1(x)$.

In conclusion, it suffices to establish Theorem 2 when $\phi(x)$ takes the form

$$\phi(x) = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x, \tag{2.2}$$

where $a_j \in \mathbb{Z}$ $(1 \le j \le 5)$, $a_5 > 0$ and $(a_1, a_2, a_3, a_4, a_5) = 1$. We henceforth assume that the latter is indeed the case. Note that we may make the same simplifications also in the proof of Theorem 1. Also, the positivity of the density of $\mathcal{L}$ for the general case follows easily from that when the polynomial $\phi(x)$ takes the simplified form (2.2).

Before moving on to establish Theorems 1 and 2, we first record some additional notation. We take N to be a large real parameter, and consider large real numbers P and Q (which we fix later) satisfying

$$N^{1/5} \ll P \ll N^{1/5} \quad \text{and} \quad N^{1/k} \ll Q \ll N^{1/k}. \tag{2.3}$$

We write

$$\begin{aligned}\Phi(x,y,z) =& \phi(z+x) + \phi(z+y) + \phi(z+x+y)\\ &+ \phi(z-x) + \phi(z-y) + \phi(z-x-y),\end{aligned} \tag{2.4}$$

and define the exponential sums

$$f(\alpha) = \sum_{P/2<x\le P} e(\phi(x)\alpha), \quad g(\alpha) = \sum_{\sqrt{Q}<y\le Q} e(\psi(y)\alpha), \tag{2.5}$$

and

$$F(\alpha) = \sum_{1\le x,y\le P/3}\ \sum_{P<z\le 2P} e(\Phi(x,y,z)\alpha). \tag{2.6}$$

3. A mean value estimate

We next establish a mean value estimate fundamental to our proof of Theorem 2, and from which Theorem 1 follows as an immediate corollary.

Lemma 3.1. *One has*

$$\int_0^1 |F(\alpha)^2 f(\alpha)^8| d\alpha \ll P^{9+\varepsilon}.$$

Proof. On applying Cauchy's inequality to (2.6), we obtain

$$|F(\alpha)|^2 \le P F_1(\alpha), \tag{3.1}$$

where

$$\begin{aligned} F_1(\alpha) &= \sum_{P<z\le 2P} \Big| \sum_{1\le x,y\le P/3} e(\Phi(x,y,z)\alpha) \Big|^2 \\ &= \sum_{P<z\le 2P} \sum_{1\le x_1,y_1\le P/3} \sum_{1\le x_2,y_2\le P/3} e(\Phi_1(\mathbf{x},\mathbf{y},z)\alpha), \end{aligned}$$

and

$$\Phi_1(\mathbf{x},\mathbf{y},z) = \Phi(x_1,y_1,z) - \Phi(x_2,y_2,z). \tag{3.2}$$

It therefore follows from (3.1) and orthogonality that

$$\begin{aligned} \int_0^1 |F(\alpha)^2 f(\alpha)^8| d\alpha &\le P \int_0^1 F_1(\alpha) |f(\alpha)|^8 d\alpha \\ &= P V_1(P), \end{aligned} \tag{3.3}$$

where $V_1(P)$ denotes the number of solutions of the diophantine equation

$$\Phi_1(\mathbf{x},\mathbf{y},z) = \sum_{j=1}^4 (\phi(v_j) - \phi(w_j)), \tag{3.4}$$

with

$$1 \le x_i, y_i \le P/3 \quad (i=1,2), \tag{3.5}$$

and

$$P < z \le 2P, \quad \tfrac{1}{2}P < v_j, w_j \le P \quad (1 \le j \le 4). \tag{3.6}$$

We next note that as a consequence of Taylor's theorem, one has

$$\phi(z+x) + \phi(z-x) = 2\phi(z) + \phi''(z)x^2 + \tfrac{1}{12}\phi''''(z)x^4.$$

Then on recalling the identity (1.1) together with the simpler identity

$$x^2 + y^2 + (x+y)^2 = 2(x^2 + xy + y^2),$$

we deduce from (2.4) that

$$\Phi(x,y,z)=6\phi(z)+2\phi''(z)(x^2+xy+y^2)+\tfrac{1}{6}\phi''''(z)(x^2+xy+y^2)^2. \tag{3.7}$$

We remark that the identity (3.7) constitutes the promised generalisation of (1.9). But on substituting (3.7) into (3.2), we obtain

$$\Phi_1(\mathbf{x},\mathbf{y},z)=2(u_1-u_2)\left(\phi''(z)+2(5a_5z+a_4)(u_1+u_2)\right),$$

where

$$u_j=x_j^2+x_jy_j+y_j^2 \quad (j=1,2).$$

Consequently, on noting that for any positive integer n, the number of solutions of the diophantine equation $x^2+xy+y^2=n$ is $O(n^\varepsilon)$ (see, for example, [2]), we deduce from (3.4)-(3.6) that

$$V_1(P)\ll P^\varepsilon V_2(P), \tag{3.8}$$

where $V_2(P)$ denotes the number of solutions of the diophantine equation

$$s\left(\phi''(z)+t(5a_5z+a_4)\right)=\sum_{j=1}^{4}(\phi(v_j)-\phi(w_j)) \tag{3.9}$$

with z, $\mathbf{v}$ and $\mathbf{w}$ satisfying (3.6), and with

$$|s|\le P^2 \quad \text{and} \quad 1\le t\le 2P^2. \tag{3.10}$$

We divide into cases, writing $V_3(P)$ for the number of solutions of (3.9) counted by $V_2(P)$ in which

$$\sum_{j=1}^{4}(\phi(v_j)-\phi(w_j)) \tag{3.11}$$

is zero, and writing $V_4(P)$ for the corresponding number of solutions in which the expression (3.11) is non-zero. Thus, on recalling (3.3) and (3.8), one has

$$\int_0^1|F(\alpha)^2f(\alpha)^8|d\alpha\ll P^{1+\varepsilon}(V_3(P)+V_4(P)). \tag{3.12}$$

Consider first the solutions $s,t,z,\mathbf{v},\mathbf{w}$ counted by $V_3(P)$. From (3.6), the number of available choices for z is at most P, and, moreover, since P is large one necessarily has that $5a_5z+a_4$ is non-zero. But if the expression (3.11) is zero, then it follows from (3.9) either that s is zero, or else that the integer

$$t=-\frac{\phi''(z)}{5a_5z+a_4}$$

is non-zero. Hence it follows from (3.10) that for a fixed choice of z, the total number of available choices for s and t counted by $V_3(P)$ is $O(P^2)$. But the number of choices for $\mathbf{v}$ and $\mathbf{w}$ for which the expression (3.11) is zero may be bounded by means of Hua's Lemma (see [9, Lemma 2.5]). Thus one obtains

$$V_3(P) \ll P^3 \int_0^1 |f(\alpha)|^8 d\alpha \ll P^{8+\varepsilon}. \tag{3.13}$$

Next consider the solutions $s, t, z, \mathbf{v}, \mathbf{w}$ counted by $V_4(P)$. Plainly, there are at most P^8 possible choices of $\mathbf{v}$ and $\mathbf{w}$ for which the expression (3.11) is non-zero. Fix any one such, and write m for the corresponding value of (3.11). From (3.9) we have that s is a divisor of the non-zero integer m, whence by elementary estimates for the divisor function there are at most $O(P^\varepsilon)$ possible choices for s. Fix any one such value of s, and substitute $\tilde{z} = 5a_5 z + a_4$ into (3.9). With a modicum of computation, one obtains

$$\tilde{z}(4\tilde{z}^2 + A_1 + 25a_5^2 t) = 25a_5^2 m/s - A_0, \tag{3.14}$$

where

$$A_0 = 8a_4^3 - 30a_3a_4a_5 + 50a_2a_5^2 \quad \text{and} \quad A_1 = 30a_3a_5 - 12a_4^2.$$

Since z is large, one has that $\tilde{z}$ is large, and so the positivity of t ensures that the expression on the left hand side of (3.14) is non-zero. Consequently the integer $m' = 25a_5^2 m/s - A_0$ is also non-zero. But $\tilde{z}$ is a divisor of this fixed integer m', whence there are at most $O(P^\varepsilon)$ possible choices for $\tilde{z}$, and hence for z. For any fixed choice of z, one may determine t from the non-trivial linear equation following from (3.14), namely

$$t = (m'/\tilde{z} - A_1 - 4\tilde{z}^2)/(25a_5^2).$$

Thus we may conclude that the total number of solutions $s, t, z, \mathbf{v}, \mathbf{w}$ of this type is

$$V_4(P) \ll P^8(P^\varepsilon)^2 = P^{8+2\varepsilon}. \tag{3.15}$$

Recalling (3.12), the conclusion of the lemma is obtained by combining (3.13) and (3.15).

We are now equipped to complete the proof of Theorem 1 in routine manner. Recall the notation concluding §2, and fix P by taking $P = \frac{1}{4}(N/a_5)^{1/5}$. When n is a positive integer, denote by $r(n)$ the number of representations of n in the form

$$n = \Phi(x, y, z) + \sum_{i=1}^{4} \phi(v_i),$$

with

$$1 \le x, y \le P/3, \quad P < z \le 2P \quad \text{and} \quad P/2 < v_i \le P \quad (1 \le i \le 4). \tag{3.16}$$

Then on recalling the notation of the statement of Theorem 1, it follows from (2.4) that whenever $r(n) > 0$, one has that n is represented in the form (1.2). Thus

$$\mathcal{N}(N) \geq \sum_{\substack{1 \leq n \leq N \\ r(n) > 0}} 1. \tag{3.17}$$

But on considering the underlying diophantine equation, one has from Lemma 3.1 that

$$\sum_{1 \leq n \leq N} r(n)^2 = \int_0^1 |F(\alpha)^2 f(\alpha)^8| d\alpha \ll P^{9+\varepsilon}. \tag{3.18}$$

Since, moreover, it follows from Cauchy's inequality that

$$\Big(\sum_{1 \leq n \leq N} r(n) \Big)^2 \leq \Big(\sum_{\substack{1 \leq n \leq N \\ r(n) > 0}} 1 \Big) \Big(\sum_{1 \leq n \leq N} r(n)^2 \Big),$$

we deduce from (3.16)-(3.18) that

$$\mathcal{N}(N) \gg (P^7)^2 (P^{9+\varepsilon})^{-1} \gg N^{1-\varepsilon}.$$

This completes the proof of Theorem 1.

4. An auxiliary singular series: initial skirmishing

Rather than employing the exponential sum $F(\alpha)$ defined by (2.6) in a full frontal attack on the proof of Theorem 2 through the medium of the Hardy-Littlewood method, we aim to outflank the difficulties inherent in handling such exponential sums by considering the major arc contribution arising from the problem of representing the integer n in the form

$$n = \sum_{i=1}^{8} \phi(x_i) + \psi(x_9).$$

In principal, only conventional weapons are required in such a manoeuvre, but difficulties associated with controlling the singular series require extra discipline to achieve a successful conclusion. The object of the next four sections is to seize control of this singular series.

Before proceeding further, we arm ourselves with some notation useful in subsequent operations. Recall the notation $\lambda(q) = \lambda(q, \psi)$ defined in (2.1). When $q \in \mathbb{N}$ and $a \in \mathbb{Z}$, write

$$S(q,a) = \sum_{r=1}^{q} e(a\phi(r)/q) \quad \text{and} \quad S_1(q,a) = \sum_{r=1}^{\lambda(q)} e(a\psi(r)/q). \tag{4.1}$$

Lemma 4.1. *When $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ satisfy $(a,q)=1$, one has*

$$S(q,a) \ll q^{4/5+\varepsilon} \quad \textit{and} \quad S_1(q,a) \ll q^{1-1/k+\varepsilon}.$$

Further, when p is a prime number and $p \nmid a$, then

$$S(p,a) \ll p^{1/2} \quad \textit{and} \quad S_1(p,a) \ll p^{1/2}.$$

Proof. The estimates provided by the lemma are by now well-known; see, for example, [9, Theorem 7.1] and [5, Corollary 2F of Chapter II].

When q and m are natural numbers, define next

$$\mathcal{S}(q,m) = q^{-8}\lambda(q)^{-1} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S(q,a)^8 S_1(q,a) e(-am/q), \tag{4.2}$$

and when p is a prime number, write

$$T(p,m) = \sum_{h=0}^{\infty} \mathcal{S}(p^h, m). \tag{4.3}$$

We then define the auxiliary singular series $\mathfrak{S}(m)$ central to our subsequent investigations by

$$\mathfrak{S}(m) = \sum_{q=1}^{\infty} \mathcal{S}(q,m). \tag{4.4}$$

Finally, denote by $M_m(q)$ the number of solutions of the congruence

$$\phi(w_1) + \dots + \phi(w_8) + \psi(w_9) \equiv m \pmod{q}, \tag{4.5}$$

with

$$1 \le w_j \le q \quad (1 \le j \le 8) \quad \text{and} \quad 1 \le w_9 \le \lambda(q).$$

As experts will anticipate, the singular series $\mathfrak{S}(m)$ has sufficiently rapid convergence that it may be expressed as a product of local densities, as we now show.

Lemma 4.2. *Let m be an integer. Then the following hold.*

(i) *For each prime number p the series $T(p,m)$ is absolutely convergent, and*

$$T(p,m) = 1 + O(p^{-6/5}).$$

Moreover, the sum $\mathfrak{S}(m)$ is absolutely convergent, the product $\prod_p T(p,m)$ is absolutely convergent, and

$$\mathfrak{S}(m) = \prod_p T(p,m).$$

(ii) *One has*

$$\sum_{q=1}^{\infty} q^{1/k} |\mathcal{S}(q,m)| \ll 1.$$

(iii) *One has $0 \le \mathfrak{S}(m) \ll 1$.*

Proof. Let m be a natural number. Then when p is a prime number, it follows from (4.2) together with Lemma 4.1 that

$$\mathcal{S}(p,m) \ll p^{-7/2}. \tag{4.6}$$

When q is an arbitrary natural number, meanwhile, again from Lemma 4.1,

$$\mathcal{S}(q,m) \ll q^{-9}(q)(q^{4/5+\varepsilon})^8(q^{1-1/k+\varepsilon}) \ll q^{-\frac{3}{5}-\frac{1}{k}+9\varepsilon}. \tag{4.7}$$

It therefore follows from (4.3) that $T(p,m)$ is absolutely convergent. Further, on substituting (4.6) and (4.7) into (4.3), we deduce that

$$T(p,m) - 1 \ll p^{-7/2} + \sum_{h=2}^{\infty} p^{-(\frac{3}{5}+\frac{1}{k}-\varepsilon)h} \ll p^{-6/5},$$

and consequently the standard theory of Euler products shows that $\prod_p T(p,m)$ is absolutely convergent. But the standard theory of exponential sums (see, for example, [9, §2.6]) shows that $\mathcal{S}(q,m)$ is a multiplicative function of q. Then on recalling (4.4), the absolute convergence of $\prod_p T(p,m)$ ensures that $\mathfrak{S}(m)$ is absolutely convergent, and also that $\mathfrak{S}(m) = \prod_p T(p,m)$. This completes the proof of part (i) of the lemma.

In order to establish part (ii), we have only to note that by (4.6) and (4.7), for each prime p one has

$$\sum_{h=0}^{\infty} p^{h/k}|\mathcal{S}(p^h,m)| - 1 \ll p^{\frac{1}{k}-\frac{7}{2}} + \sum_{h=2}^{\infty} p^{-(3/5-\varepsilon)h} \ll p^{2\varepsilon-6/5},$$

and hence the multiplicativity of $\mathcal{S}(q,m)$ ensures that

$$\sum_{q=1}^{\infty} q^{1/k}|\mathcal{S}(q,m)| = \prod_p \Big(\sum_{h=0}^{\infty} p^{h/k}|\mathcal{S}(p^h,m)|\Big) \ll 1.$$

Finally, on recalling (4.1), the argument of the proof of Lemma 2.12 of [9] shows that for every natural number H, one has

$$\sum_{h=0}^{H} \mathcal{S}(p^h,m) = p^{-7H}(\lambda(p^H))^{-1}M_m(p^H). \tag{4.8}$$

On recalling (4.3) and (4.5), therefore, we find that for each prime p, one has $T(p,m) \geq 0$, whence also

$$\mathfrak{S}(m) = \prod_p T(p,m) \geq 0.$$

The proof of part (iii) of the lemma is completed on noting that part (ii) leads immediately from (4.4) to the upper bound $\mathfrak{S}(m) \ll 1$.

The estimates provided by Lemma 4.2 suffice for our analysis of the local factors of the singular series for larger primes, but for smaller primes we must work harder. The following lemma shows that the existence of suitable solutions to the congruence (4.5) suffices to provide a useful lower bound on $T(p,m)$.

Lemma 4.3. *Let ρ be a positive integer, and suppose that γ and δ are non-negative integers with $\rho = 2\gamma + 1 - \delta$ and $\gamma \geq 2\delta - 1$. Let m be a natural number and p be a prime number. Suppose that when $q = p^\rho$, the congruence* (4.5) *is soluble with*

$$p^\gamma \| \phi'(w_1) \quad \textit{and} \quad p^\delta | \tfrac{1}{2}\phi''(w_1). \tag{4.9}$$

Then one has

$$T(p, m) \gg p^{-8\rho}.$$

Proof. Suppose that the hypotheses of the statement of the lemma are satisfied, and that for some integer l and a natural number H with $H \geq \rho$, one has $\phi(w_1) \equiv l \pmod{p^H}$. Write

$$\alpha = p^{-H}(\phi(w_1) - l) \quad \text{and} \quad \beta = p^{-\gamma}\phi'(w_1).$$

Then one has $\alpha \in \mathbb{Z}$, and in view of (4.9) one has also $\beta \in \mathbb{Z}$ and $(\beta, p) = 1$. Thus, since

$$H - \gamma \geq \gamma + 1 - \delta \geq \max\{1, \delta\}, \tag{4.10}$$

it follows from the Binomial Theorem that for each integer t one has

$$\phi(w_1 + p^{H-\gamma}t) \equiv \phi(w_1) + p^{H-\gamma}\phi'(w_1)t + p^{2(H-\gamma)}\frac{\phi''(w_1)}{2}t^2 \pmod{p^{3(H-\gamma)}},$$

whence by (4.9),

$$\phi(w_1 + p^{H-\gamma}t) \equiv l + (\alpha + \beta t)p^H \pmod{p^{2(H-\gamma)+\delta}}. \tag{4.11}$$

But $(\beta, p) = 1$, so that one may solve the congruence $\alpha + \beta t \equiv 0 \pmod{p}$, say with $t = \bar{t}$. Moreover, by (4.10) one has

$$2(H - \gamma) + \delta \geq (H - \gamma + \delta) + (\gamma + 1 - \delta) = H + 1,$$

and thus by (4.11),

$$\phi(w_1 + p^{H-\gamma}\bar{t}) \equiv l \pmod{p^{H+1}}. \tag{4.12}$$

Applying the Binomial Theorem again, one obtains from (4.9) also

$$\phi'(w_1 + p^{H-\gamma}\bar{t}) \equiv \phi'(w_1) + p^{H-\gamma}\phi''(w_1)\bar{t} \equiv \phi'(w_1) \pmod{p^{H-\gamma+\delta}}.$$

Thus, on noting that (4.10) yields $H - \gamma + \delta \geq \gamma + 1$, it follows from (4.9) that

$$p^\gamma \| \phi'(w_1 + p^{H-\gamma}\bar{t}). \tag{4.13}$$

Further, again applying the Binomial Theorem in combination with (4.9) and (4.10), one has

$$\tfrac{1}{2}\phi''(w_1 + p^{H-\gamma}\bar{t}) \equiv \tfrac{1}{2}\phi''(w_1) \equiv 0 \pmod{p^\delta}. \tag{4.14}$$

On collecting together (4.12)-(4.14), we conclude that if the congruence

$$\phi(w_1) \equiv l \pmod{p^H} \tag{4.15}$$

has a solution w_1 satisfying (4.9) for some H with $H \geq 2\gamma + 1 - \delta$, then such holds also with H replaced by $H + 1$. Consequently, by induction on H, we deduce that the congruence (4.15) has a solution w_1 satisfying (4.9) for every integer H with $H \geq 2\gamma + 1 - \delta$.

Suppose next that when $q = p^\rho$, the congruence (4.5) has a solution $\mathbf{w}$ satisfying the hypotheses of the statement of the lemma. We take v_j $(2 \leq j \leq 9)$ to be any integers with

$$v_j \equiv w_j \pmod{p^\rho} \quad (2 \leq j \leq 8) \quad \text{and} \quad v_9 \equiv w_9 \pmod{\lambda(p^\rho)}. \tag{4.16}$$

Write

$$l = m - \sum_{j=2}^{8} \phi(v_j) - \psi(v_9).$$

Then by assumption, the congruence $\phi(w_1) \equiv l \pmod{p^\rho}$ is satisfied with the conditions (4.9) holding. Thus, as a consequence of the discussion of the previous paragraph, the congruence $\phi(\xi) \equiv l \pmod{p^H}$ has a solution ξ for every integer H with $H \geq \rho$. Summing over all possible choices of v_j $(2 \leq j \leq 9)$ satisfying (4.16), we deduce that for each $H \geq \rho$ one has

$$M_m(p^H) \geq (p^{H-\rho})^7 \left(\lambda(p^H)/\lambda(p^\rho)\right) = p^{8(H-\rho)}.$$

We therefore conclude from (4.8) that for each $H \geq \rho$, one has

$$\sum_{h=0}^{H} \mathcal{S}(p^h, m) \geq p^{H-8\rho}(\lambda(p^H))^{-1} \gg p^{-8\rho},$$

and so it follows from (4.3) that $T(p, m) \gg p^{-8\rho}$. This concludes the proof of the lemma.

5. An auxiliary singular series: the contribution of the larger primes

We must now grapple with the problem of showing that the singular series $\mathfrak{S}(m)$ is bounded away from zero. We begin by dismissing the larger primes in routine manner, following a little notation. When s and q are natural numbers, denote by $\mathcal{K}(q, s) = \mathcal{K}(q, s; \phi)$ the set of residue classes modulo q that can be represented in the form

$$\phi(w_1) + \cdots + \phi(w_s) \tag{5.1}$$

with $w_j \in \mathbb{Z}$ $(1 \leq j \leq s)$. Similarly, denote by $\mathcal{K}^*(q, s) = \mathcal{K}^*(q, s; \phi)$ the set of residue classes modulo q that are represented in the form (5.1) with $w_j \in \mathbb{Z}$ $(1 \leq j \leq s)$ and $(\phi'(w_1), q) = 1$. We then define

$$K(q, s) = \text{card}(\mathcal{K}(q, s)) \quad \text{and} \quad K^*(q, s) = \text{card}(\mathcal{K}^*(q, s)).$$

Note that in view of the vanishing of the constant term of $\phi(x)$ provided by (2.2), we may suppose that $0 \in \mathcal{K}(q, s)$.

Lemma 5.1. *For each natural number m, one has*

$$\prod_{p\geq 7} T(p,m) \gg 1.$$

Proof. By Lemma 4.2(i), one has for each natural number m and prime p the estimate

$$T(p,m) = 1 + O(p^{-6/5}),$$

and thus there is a real number C exceeding 7, depending only on k and the coefficients of ϕ and ψ, such that

$$\prod_{p\geq C} T(p,m) \geq \tfrac{1}{2}. \tag{5.2}$$

In order to establish the conclusion of the lemma, therefore, it suffices to consider primes p with $7 \leq p < C$.

Suppose that p is a prime with $p \geq 7$. On recalling (2.2), we see that for each integer n, the congruence $\phi(x) \equiv n \pmod{p}$ has at most 5 solutions modulo p. Moreover, since $p > 5$ the congruence $\phi'(x) \equiv 0 \pmod{p}$ has at most 4 solutions modulo p. Consequently,

$$K(p,1) \geq p/5 \quad \text{and} \quad K^*(p,1) \geq (p-4)/5,$$

so that since $p \geq 7$,

$$K(p,1) \geq [p/5] + 1 \quad \text{and} \quad K^*(p,1) \geq [p/5].$$

On applying the Cauchy-Davenport theorem (see [9, Lemma 2.14]), we therefore deduce that

$$K^*(p,8) \geq \min\{p, \kappa(p)\}, \tag{5.3}$$

where

$$\kappa(p) = K^*(p,1) + 7(K(p,1) - 1) \geq 8[p/5]. \tag{5.4}$$

But it follows from (5.4) that whenever $p \geq 11$, one has

$$\kappa(p) \geq 8(p-4)/5 \geq p,$$

and moreover a direct calculation from (5.4) yields $\kappa(7) \geq 8$. Thus we deduce from (5.3) that $K^*(p,8) = p$, whence for every integer m, the hypotheses of Lemma 4.3 are satisfied with $\gamma = \delta = 0$. We therefore conclude from Lemma 4.3 that whenever $p \geq 7$ one has $T(p,m) \gg p^{-8}$, whence

$$\prod_{7\leq p<C} T(p,m) \gg 1. \tag{5.5}$$

The conclusion of the lemma follows by combining (5.2) and (5.5).

We conclude this section by considering the contribution of the prime 5.

Lemma 5.2. *Let $\mathcal{L}$ be defined as in the statement of Theorem* 2*. Then whenever $n \in \mathcal{L}$, for any integers x_j, y_j, z_j $(j = 1, 2)$ one has*

$$T(5, n - \Phi(x_1, y_1, z_1) - \Phi(x_2, y_2, z_2)) \gg 1.$$

Proof. We suppose first that $K(5, 1) \geq 2$, and further that for some integer x one has $5 \nmid \phi'(x)$. Then by the Cauchy-Davenport theorem (see [9, Lemma 2.14]) we have $K(5, 4) = 5$, whence $K^*(5, 8) = 5$. Thus we deduce that the hypotheses of Lemma 4.3 are satisfied with $\gamma = \delta = 0$. We may therefore conclude from Lemma 4.3 that for every integer m, one has $T(5, m) \gg 1$.

Next suppose that $K(5, 1) = 1$, and that for some integer x one has $5 \nmid \phi'(x)$. In view of the vanishing of the constant term in (2.2), we therefore have that $5|\phi(y)$ for every integer y, whence by (2.4) it follows that whenever $u, v, w \in \mathbb{Z}$, one has

$$5|\Phi(u, v, w). \tag{5.6}$$

Notice that when $n \in \mathcal{L}$, the solubility of the congruence (1.3), together with the observation that $5|\phi(x_i)$ $(1 \leq i \leq 20)$, implies that the congruence $\psi(\xi) \equiv n \pmod 5$ is soluble. We are therefore forced to conclude that when $n \in \mathcal{L}$ and $m \equiv n \pmod 5$, then the congruence (4.5) is soluble when $q = 5$, and, moreover, soluble with $5 \nmid \phi'(w_1)$. Thus the hypotheses of Lemma 4.3 are satisfied with $\gamma = \delta = 0$, whence by Lemma 4.3 one has $T(5, m) \gg 1$. In this case, therefore, it follows from (5.6) that whenever $n \in \mathcal{L}$, for any integers x_j, y_j, z_j $(j = 1, 2)$, one has

$$T(5, n - \Phi(x_1, y_1, z_1) - \Phi(x_2, y_2, z_2)) \gg 1.$$

Finally, we suppose that $5|\phi'(x)$ for every integer x. By referring to (2.2), a simple calculation yields

$$\begin{aligned} a_1 &= \phi'(0), \\ 24a_2 &= 8(\phi'(1) - \phi'(-1)) - (\phi'(2) - \phi'(-2)), \\ 72a_3 &= 16(\phi'(1) + \phi'(-1)) - (\phi'(2) + \phi'(-2)) - 30\phi'(0), \\ 48a_4 &= -2(\phi'(1) - \phi'(-1)) + (\phi'(2) - \phi'(-2)), \\ 120a_5 &= -4(\phi'(1) + \phi'(-1)) + (\phi'(2) + \phi'(-2)) + 6\phi'(0). \end{aligned} \tag{5.7}$$

Since by hypothesis we have $5|\phi'(x)$ for each x, it follows from (5.7) that $5|a_j$ for $1 \leq j \leq 4$. By our assumption following (2.2) that $(a_1, a_2, a_3, a_4, a_5) = 1$, therefore, we have also $5 \nmid a_5$. Suppose next that $25|\phi'(x)$ for each integer x. Then the last equation of (5.7) implies that $5|a_5$, a contradiction which ensures the existence of an integer x with $25 \nmid \phi'(x)$. On referring to (2.2) once again, moreover, one finds that the above observations ensure that for every integer x, one has $5|\frac{1}{2}\phi''(x)$. But $\phi(x) \equiv a_5x^5 \equiv a_5x \pmod 5$, so that $\mathcal{K}(25, 1)$ contains at least 4 residue classes coprime to 5, as well as the zero residue class. Consequently, an application of the Cauchy-Davenport theorem (see [9, Lemma 2.14]) yields $K(25, 6) = 25$. In view of the discussion contained in this paragraph, therefore, it follows that for every integer m, the hypotheses of Lemma 4.3 are satisfied with $\gamma = \delta = 1$ and $p = 5$. We therefore deduce from Lemma 4.3 that for every integer m one has $T(5, m) \gg 1$.

Collecting together the conclusions of the preceding three paragraphs, the proof of the lemma is complete.

6. An auxiliary singular series: the contribution of the prime 3

When it comes to estimating $T(p,m)$ for $p=2$ and 3, we pay heavily for the use of the identity (3.7), and our arguments become considerably more complicated than those of the previous section. We tackle the prime 3 in this section, beginning with a lemma of a somewhat combinatorial flavour concerning the simultaneous solubility modulo 3 of the congruences

$$\begin{aligned} &t_j+r_j\equiv u_{6j-5},\quad t_j+s_j\equiv u_{6j-3},\quad t_j+r_j+s_j\equiv u_{6j-1},\\ &t_j-r_j\equiv u_{6j-4},\quad t_j-s_j\equiv u_{6j-2},\quad t_j-r_j-s_j\equiv u_{6j}. \end{aligned} \tag{6.1}$$

Lemma 6.1. *Suppose that $u_1,\dots,u_{16}$ are integers. Then there exists a relabelling of the u_i $(1\le i\le 16)$, and there exist integers r_j,s_j,t_j $(j=1,2)$, with the property that for $j=1,2$ the congruences* (6.1) *are satisfied simultaneously modulo* 3.

Proof. Suppose that $u_1,\dots,u_{16}$ are integers. By the pigeon-hole principle, amongst any 7 integers there must be three integers mutually congruent modulo 3. Consequently, by applying this observation twice and relabelling the u_i $(1\le i\le 16)$, we may suppose that for $j=1,2$ one has

$$u_{6j-5}\equiv u_{6j-3}\equiv u_{6j}\pmod 3\quad\text{and}\quad u_{6j-4}\equiv u_{6j-2}\equiv u_{6j-1}\pmod 3.$$

Then the dozen congruences (6.1) are satisfied modulo 3 with

$$r_j=s_j=2u_{6j-5}+u_{6j-4}\quad\text{and}\quad t_j=-(u_{6j-5}+u_{6j-4})\quad(j=1,2).$$

This completes the proof of the lemma.

We now estimate $T(3,m)$.

Lemma 6.2. *Let $\mathcal{L}$ be defined as in the statement of Theorem* 2*, and suppose that $n\in\mathcal{L}$. Then there exist integers r_j,s_j,t_j $(j=1,2)$ such that whenever x_j,y_j,z_j $(j=1,2)$ are integers satisfying the congruences*

$$x_j\equiv r_j\pmod 3,\quad y_j\equiv s_j\pmod 3\quad\text{and}\quad z_j\equiv t_j\pmod 3\quad(j=1,2), \tag{6.2}$$

one has

$$T(3,n-\Phi(x_1,y_1,z_1)-\Phi(x_2,y_2,z_2))\gg 1. \tag{6.3}$$

Proof. We divide our argument into a number of cases.

(a) *Suppose that $3\nmid\phi'(x)$ for some integer x.* On the one hand, if $K(3,1)\ge 2$, then it follows from the Cauchy-Davenport theorem (see [9, Lemma 2.14]) that $K(3,2)=3$, whence for every integer m the hypotheses of Lemma 4.3 are satisfied with $\gamma=\delta=0$ and $p=3$. We therefore conclude from Lemma 4.3 that in such circumstances one has $T(3,m)\gg 1$ for every integer m. On the other hand, if $K(3,1)=1$, then it follows from (2.2) that for every integer x one has $3|\phi(x)$. Moreover, similarly, it follows from (2.4) that for all integers u,v,w one has

$$3|\Phi(u,v,w). \tag{6.4}$$

Notice that when $n \in \mathcal{L}$, the solubility of the congruence (1.3), together with the observation that $3|\phi(x_i)$ $(1 \le i \le 20)$, implies that the congruence $\psi(\xi) \equiv n \pmod 3$ is soluble. We are therefore forced to conclude that when $n \in \mathcal{L}$ and $m \equiv n \pmod 3$, then the congruence (4.5) is soluble when $q = 3$, and further, that it is soluble with $3 \nmid \phi'(w_1)$. Thus the hypotheses of Lemma 4.3 are satisfied with $\gamma = \delta = 0$ and $p = 3$, whence by Lemma 4.3 one has $T(3, m) \gg 1$. In this case, therefore, it follows from (6.4) that whenever $n \in \mathcal{L}$, the lower bound (6.3) holds for any integers x_j, y_j, z_j $(j = 1, 2)$.

(b) *Suppose that* $3|\phi'(x)$ *for every integer* x*, but that for some integer* y *one has* $9 \nmid \phi'(y)$. Observe that it follows from (2.2) that for every integer x one has

$$\phi'(x) \equiv 2a_5x^2 + (a_4 - a_2)x + a_1 \equiv 0 \pmod 3,$$

whence by our initial hypothesis one necessarily has

$$a_5 \equiv a_1 \equiv 0 \pmod 3 \quad \text{and} \quad a_4 \equiv a_2 \pmod 3. \tag{6.5}$$

In particular, for every integer x,

$$\phi''(x) = 20a_5x^3 + 12a_4x^2 + 6a_3x + 2a_2 \equiv 2a_4 \pmod 3. \tag{6.6}$$

We subdivide our argument into further cases, according to whether or not $3|a_4$.

(i) *Suppose that* $3|a_4$. In view of (6.5) one has $3|a_j$ for $j = 1, 2, 4, 5$, so that by our assumption following (2.2) that $(a_5, a_4, a_3, a_2, a_1) = 1$, one has $3 \nmid a_3$. Consequently, it follows from (2.2) that $\phi(x) \equiv a_3x \pmod 3$ for every integer x. Since $3 \nmid a_3$, therefore, the set $\mathcal{K}(9, 1)$ contains at least 2 residue classes coprime to 3, as well as the zero residue class. Then an application of the Cauchy-Davenport theorem (see [9, Lemma 2.14]) shows that $K(9, 4) = 9$. But by hypothesis, the congruence (6.6) implies that for every integer x one has $3|\phi''(x)$. We therefore conclude that for every integer m the hypotheses of Lemma 4.3 are satisfied with $\gamma = \delta = 1$ and $p = 3$. It therefore follows from Lemma 4.3 that $T(3, m) \gg 1$ for each integer m, whence the lower bound (6.3) again follows.

(ii) *Suppose that* $3 \nmid a_4$. In view of (2.2) and (6.5), one has

$$\phi(\pm 3) \equiv 9(a_4 \pm a_1/3) \pmod{27}, \tag{6.7}$$

whence, on recalling our hypothesis that $3 \nmid a_4$, it follows that we may choose an integer ξ_0 with $\xi_0 = \pm 3$ such that

$$9 \| \phi(\xi_0). \tag{6.8}$$

Next we observe that if both $\phi(1)$ and $\phi(-1)$ are divisible by 3, then in view of (2.2) and (6.5) one has $a_3 \equiv a_4 \pmod 3$ and $a_3 \equiv -a_4 \pmod 3$, whence $3|a_4$. This contradicts our initial hypothesis, so plainly one has either

$$3 \nmid \phi(1) \quad \text{or} \quad 3 \nmid \phi(-1). \tag{6.9}$$

Also, we observe that by (6.6) and the Binomial Theorem, one has for every ξ,

$$\begin{aligned}\phi(\xi\pm 3)&\equiv \phi(\xi)\pm 3\phi'(\xi)+9\phi''(\xi)/2 \pmod{27}\\ &\equiv \phi(\xi)+9(a_4\pm \phi'(\xi)/3) \pmod{27}. \qquad (6.10)\end{aligned}$$

Let ω denote the choice of ± 1 which in (6.9) provides that $3\nmid \phi(\omega)$. Then we claim that there exists a residue ξ, with $\xi\equiv \omega \pmod 3$, which satisfies

$$\phi'(\xi)\equiv a_1 \pmod 9. \qquad (6.11)$$

In order to verify this assertion, write

$$\begin{aligned}g(\xi)&=(\phi'(\xi)-a_1)/\xi\\ &=2a_2+3a_3\xi+4a_4\xi^2+5a_5\xi^3, \qquad (6.12)\end{aligned}$$

and observe that the claimed solubility of the congruence (6.11) is equivalent to the solubility, with $\xi\equiv\omega \pmod 3$, of the congruence $g(\xi)\equiv 0 \pmod 9$. But in view of (6.5), it follows from (6.12) that $g(\omega)\equiv 0 \pmod 3$. Moreover, again from (6.12), one has

$$g'(\omega)=3a_3+8a_4\omega+15a_5\omega^2\equiv 8a_4\omega \pmod 3,$$

whence by hypothesis one has $3\nmid g'(\omega)$. Thus we may conclude from Hensel's Lemma that there exists a residue ξ with $\xi\equiv\omega \pmod 3$ and $g(\xi)\equiv 0 \pmod 9$. This establishes the desired solubility of (6.11).

Take ξ_1 to be the choice of ξ supplied by the solubility of (6.11), and note that in view of the choice of ω in the previous paragraph, one has $3\nmid\phi(\xi_1)$. Then by (6.7), (6.10) and (6.11), one has

$$\phi(\xi_1+\xi_0)\equiv \phi(\xi_1)+\phi(\xi_0) \pmod{27}.$$

On recalling (6.8), therefore, we may conclude that there exist integers ξ_0,ξ_1,ξ_2 with $\xi_0=\pm 3$, $3\nmid \xi_1$, $\xi_2=\xi_1+\xi_0$ and

$$9\|\phi(\xi_0),\quad 3\nmid\phi(\xi_1),\quad \phi(\xi_2)\equiv\phi(\xi_1)+\phi(\xi_0) \pmod{27}. \qquad (6.13)$$

Observe next that every residue class modulo 27 is represented in the form $\mu\phi(\xi_1)+\nu\phi(\xi_0)$ with $0\le\mu\le 8$ and $1\le\nu\le 3$. In order to confirm this observation, it suffices to show that whenever

$$\mu\phi(\xi_1)+\nu\phi(\xi_0)\equiv \mu'\phi(\xi_1)+\nu'\phi(\xi_0) \pmod{27}, \qquad (6.14)$$

with $0\le\mu,\mu'\le 8$ and $1\le\nu,\nu'\le 3$, then necessarily $\mu=\mu'$ and $\nu=\nu'$. But in view of (6.13), the congruence (6.14) implies that $(\mu-\mu')\phi(\xi_1)\equiv 0 \pmod 9$, whence $\mu=\mu'$, and thus also $(\nu-\nu')\phi(\xi_0)\equiv 0 \pmod{27}$, whence $\nu=\nu'$. Consequently, given any integer l, there exist integers μ and ν satisfying

$$l\equiv \mu\phi(\xi_1)+\nu\phi(\xi_0) \pmod{27},$$

and with $0 \le \mu \le 8$ and $1 \le \nu \le 3$. On making use of (6.13) we may reformulate the latter congruence in the shapes

$$l \equiv (\mu-\nu)\phi(\xi_1) + \nu\phi(\xi_2) + (8-\mu)\phi(0) \pmod{27}$$

and

$$l \equiv \mu\phi(\xi_1) + \nu\phi(\xi_0) + (8-\mu-\nu)\phi(0) \pmod{27}.$$

It follows that the congruence

$$\phi(w_1) + \cdots + \phi(w_8) \equiv l \pmod{27} \tag{6.15}$$

has the solution $\mathbf{w}$ given by

$$w_j = \begin{cases} \xi_1, & \text{when } 1 \le j \le \mu-\nu, \\ \xi_2, & \text{when } \mu-\nu+1 \le j \le \mu, \\ 0, & \text{when } \mu+1 \le j \le 8, \end{cases}$$

whenever $\mu > \nu$, and has the solution $\mathbf{w}$ given by

$$w_j = \begin{cases} \xi_1, & \text{when } 1 \le j \le \mu, \\ \xi_0, & \text{when } \mu+1 \le j \le \mu+\nu, \\ 0, & \text{when } \mu+\nu+1 \le j \le 8, \end{cases}$$

when $\mu \le \nu$.

Consider now the solution of (6.15) provided by the above choices of $\mathbf{w}$. In the former instance, one necessarily has $\mu-\nu \ge 1$ and $\nu \ge 1$, and in the latter instance one has $\nu \ge 1$ and $8-\mu-\nu \ge 2$. Consequently, in the former case there are w_i equal to ξ_1 and w_j equal to ξ_2, for some i and j, and in the latter case there are w_i equal to ξ_0 and w_j equal to 0, for some i and j. Next note that by (6.6), for every integer x it follows from the Binomial Theorem that

$$\phi'(x \pm 3) \equiv \phi'(x) \pm 3\phi''(x) \equiv \phi'(x) \pm 6a_4 \pmod 9.$$

By hypothesis, moreover, one has $3 \nmid a_4$. Consequently, in view of our definitions of ξ_0, ξ_1, ξ_2, one has $3\|\phi'(\xi_1)$ or $3\|\phi'(\xi_2)$, and also $3\|\phi'(0)$ or $3\|\phi'(\xi_0)$. Then in either of the above instances, there is a solution $\mathbf{w}$ of the congruence (6.15) in which, for some j, one has $3\|\phi'(w_j)$. By relabelling variables, therefore, there is no loss of generality in supposing that for every integer l, the congruence (6.15) is soluble with $3\|\phi'(w_1)$. For every integer m, therefore, the hypotheses of Lemma 4.3 are satisfied with $\gamma = 1$, $\delta = 0$ and $p = 3$. We therefore conclude from Lemma 4.3 that $T(3,m) \gg 1$ for every integer m, whence the lower bound (6.3) follows immediately.

(c) *Suppose that* $9|\phi'(x)$ *for every integer* x. On recalling (5.7), we find that our initial hypothesis implies that $9|a_1$, and that $3|a_j$ for $j = 2, 4, 5$. By our assumption following (2.2) that $(a_1, a_2, a_3, a_4, a_5) = 1$, therefore, we have also $3 \nmid a_3$. Moreover, on noting that our initial hypothesis dictates that

$$\phi'(1) + \phi'(-1) \equiv 10a_5 + 6a_3 + 2a_1 \equiv 0 \pmod 9,$$

we deduce that $a_5 \equiv 3a_3 \pmod 9$, whence for every integer x one has

$$\phi''(x) = 20a_5x^3 + 12a_4x^2 + 6a_3x + 2a_2 \equiv 2(6a_3x + a_2) \pmod 9. \tag{6.16}$$

Similarly, one has for every integer x that

$$\phi'''(x) = 60a_5x^2 + 24a_4x + 6a_3 \equiv 6a_3 \pmod 9,$$

whence by the Binomial Theorem together with (6.16),

$$\begin{aligned}\phi(x \pm 3) &\equiv \phi(x) \pm 3\phi'(x) + 9\phi''(x)/2 \pm 27\phi'''(x)/6 \pmod{81} \\ &\equiv \phi(x) + 27((2a_3x + a_2/3) \pm (a_3 + \phi'(x)/9)) \pmod{81}.\end{aligned} \tag{6.17}$$

Next observe that since $3 \nmid a_3$, there exists an integer ξ for which $3 \nmid (2a_3\xi + a_2/3)$. But then one cannot have

$$(2a_3\xi + a_2/3) + \omega(\phi'(\xi)/9 + a_3) \equiv 0 \pmod 3$$

for both $\omega = 1$ and $\omega = -1$. Consequently, for some $\omega_1, \omega_2 \in \{+1, -1\}$, it follows from (6.17) that

$$\phi(\xi + 3\omega_1) \equiv \phi(\xi) + 27\omega_2 \pmod{81},$$

whence there exist integers ξ_1 and ξ_2 with

$$\phi(\xi_2) \equiv \phi(\xi_1) + 27 \pmod{81}. \tag{6.18}$$

Finally, observe also that if $27|\phi'(x)$ for every integer x, then the equations (5.7) provide that $3|a_3$, leading to a contradiction. Thus there exists an integer ξ_0 with $27 \nmid \phi'(\xi_0)$, and in view of our initial hypothesis the latter implies that

$$9 \| \phi'(\xi_0). \tag{6.19}$$

Next, since for every integer x one has $\phi(x) \equiv a_3x \pmod 3$, we notice that the set $\mathcal{K}(27, 1)$ contains at least 2 residue classes coprime to 3, as well as the zero residue class. Consequently, an application of the Cauchy-Davenport theorem (see [9, Lemma 2.14]) yields $K(27, 13) = 27$, whence for any integers v and n, there exist integers u_j $(1 \le j \le 17)$ satisfying

$$\phi(u_1) + \phi(u_2) + \dots + \phi(u_{17}) + 2\phi(\xi_1) + \phi(\xi_0) + \psi(v) \equiv n \pmod{27}. \tag{6.20}$$

By relabelling variables, therefore, it follows from Lemma 6.1 that there exist integers r_j, s_j, t_j $(j = 1, 2)$ with the property that for $j = 1, 2$, the congruences (6.1) hold simultaneously modulo 3. For these integers r_j, s_j, t_j $(j = 1, 2)$, suppose that $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are integers satisfying the congruences (6.2). Then on noting that the congruence (6.17) ensures that whenever $x \equiv y \pmod 3$, one has $\phi(x) \equiv \phi(y) \pmod{27}$, we find from (2.4) and (6.1) that the congruence

$$\Phi(x_1, y_1, z_1) + \Phi(x_2, y_2, z_2) \equiv \phi(u_1) + \cdots + \phi(u_{12}) \tag{6.21}$$

holds modulo 27. Then (6.20) implies that

$$\begin{aligned}\phi(u_{13}) + \cdots + &\phi(u_{17}) + 2\phi(\xi_1) + \phi(\xi_0) + \psi(v)\\ &\equiv n - \Phi(x_1, y_1, z_1) - \Phi(x_2, y_2, z_2) \pmod{27},\end{aligned}$$

whence there exists a choice for d with $d \in \{0, 27, 54\}$ such that

$$\begin{aligned}\phi(u_{13}) + \cdots + &\phi(u_{17}) + 2\phi(\xi_1) + \phi(\xi_0) + \psi(v) + d\\ &\equiv n - \Phi(x_1, y_1, z_1) - \Phi(x_2, y_2, z_2) \pmod{81}.\end{aligned} \tag{6.22}$$

But by (6.18), we have

$$\phi(\xi_1) + \phi(\xi_2) \equiv 2\phi(\xi_1) + 27 \pmod{81},$$

and

$$2\phi(\xi_2) \equiv 2\phi(\xi_1) + 54 \pmod{81},$$

and so it is apparent from (6.22) that the congruence

$$\phi(w_1) + \cdots + \phi(w_8) + \psi(w_9) \equiv n - \Phi(x_1, y_1, z_1) - \Phi(x_2, y_2, z_2) \tag{6.23}$$

is soluble modulo 81 with

$$w_1 = \xi_0, \quad w_i \in \{\xi_1, \xi_2\} \quad (i = 2, 3), \quad w_j = u_{j+9} \quad (4 \le j \le 8) \quad \text{and} \quad w_9 = v.$$

On recalling (6.16) and (6.19), therefore, which imply that $9 \| \phi'(\xi_0)$ and $3 | \phi''(\xi_0)$, we conclude that the hypotheses of Lemma 4.3 are satisfied for the integer

$$m = n - \Phi(x_1, y_1, z_1) - \Phi(x_2, y_2, z_2) \tag{6.24}$$

with $\gamma = 2$, $\delta = 1$ and $p = 3$. We therefore deduce from Lemma 4.3 that $T(3, m) \gg 1$, whence the lower bound (6.3) follows immediately.

This completes the proof of the lemma.

7. An auxiliary singular series: the contribution of the prime 2

We now bound $T(2,m)$ from below, the analysis here being somewhat more delicate than in the previous section. We begin with a combinatorial lemma similar to Lemma 6.1.

Lemma 7.1. *The following hold.*

(i) *Suppose that $u_1,\dots,u_{16}$ are integers with $u_{2j-1}\equiv u_{2j} \pmod 4$ for $1\le j\le 8$. Then there exists a relabelling of the u_i $(1\le i\le 16)$, and there exist integers r_j,s_j,t_j $(j=1,2)$, with the property that for $j=1,2$, the congruences* (6.1) *hold simultaneously modulo* 4.

(ii) *Suppose that $u_1,\dots,u_{19}$ are integers. Then there exists a relabelling of the u_i $(1\le i\le 19)$, and there exist integers r_j,s_j,t_j $(j=1,2)$, with the property that for $j=1,2$, the congruences* (6.1) *hold simultaneously modulo* 4.

(iii) *Suppose that $u_1,\dots,u_{18}$ are integers, and suppose that there is an integer u with the property that $u_j\not\equiv u \pmod 4$ $(1\le j\le 18)$. Then there exists a relabelling of the u_i $(1\le i\le 18)$, and there exist integers r_j,s_j,t_j $(j=1,2)$, with the property that for $j=1,2$, the congruences* (6.1) *hold simultaneously modulo* 4.

Proof. We begin by establishing part (i) of the lemma. Suppose that $u_1,\dots,u_{16}$ are integers. By the pigeon-hole principle, amongst any 5 integers there are three of the same parity, and at least two of the latter integers are mutually congruent modulo 4. Applying this observation to the integers u_{2j} with $1\le j\le 8$, it follows from the hypothesis of part (i) of the lemma that there is a relabelling of the u_i $(1\le i\le 16)$ such that for $j=1,2$ one has

$$u_{6j-5}\equiv u_{6j-4}\equiv u_{6j-3}\equiv u_{6j-2} \pmod 4,$$
$$u_{6j-1}\equiv u_{6j} \pmod 4 \quad\text{and}\quad u_{6j-5}\equiv u_{6j-1} \pmod 2.$$

Thus the dozen congruences (6.1) are satisfied simultaneously modulo 4 with

$$r_j=s_j=u_{6j-5}-u_{6j-1}\quad\text{and}\quad t_j=u_{6j-1}\quad (j=1,2).$$

Next we establish part (ii). Suppose that $u_1,\dots,u_{19}$ are integers. Again, by the pigeon-hole principle, amongst any 5 integers there are two integers mutually congruent modulo 4. Thus we may relabel the u_i $(1\le i\le 19)$ so that $u_{2j-1}\equiv u_{2j} \pmod 4$ for $1\le j\le 8$. Consequently, the hypotheses of part (i) of the lemma are now satisfied, and the desired conclusion follows from the previous paragraph.

Finally we consider part (iii). Suppose that $u_1,\dots,u_{18}$ are integers satisfying the hypotheses of part (iii). Then because these integers omit a congruence class modulo 4, amongst any 4 such integers there are two which are mutually congruent modulo 4. Thus we may relabel the u_i $(1\le i\le 18)$ so that $u_{2j-1}\equiv u_{2j} \pmod 4$ for $1\le j\le 8$. We therefore conclude that the hypotheses of part (i) of the lemma are again satisfied, whence the desired conclusion again follows immediately.

This completes the proof of the lemma.

We now launch our offensive on the prime 2.

Lemma 7.2. *Let $\mathcal{L}$ be defined as in the statement of Theorem 2, and suppose that $n \in \mathcal{L}$. Then there exist integers r_j, s_j, t_j $(j = 1, 2)$ such that whenever x_j, y_j, z_j $(j = 1, 2)$ are integers satisfying the congruences*

$$x_j \equiv r_j \pmod 4, \quad y_j \equiv s_j \pmod 4 \quad \text{and} \quad z_j \equiv t_j \pmod 4 \quad (j = 1, 2), \tag{7.1}$$

then one has

$$T(2, n - \Phi(x_1, y_1, z_1) - \Phi(x_2, y_2, z_2)) \gg 1. \tag{7.2}$$

Proof. We divide our proof into a plethora of cases.

(a) *Suppose that $2 \nmid \phi'(x)$ for some integer x.* On the one hand, if $K(2, 1) = 2$, then it follows immediately that for every integer m, the hypotheses of Lemma 4.3 are satisfied with $\gamma = \delta = 0$ and $p = 2$. Thus we deduce from Lemma 4.3 that $T(2, m) \gg 1$ for every integer m. On the other hand, if $K(2, 1) = 1$, then necessarily $\phi(x)$ is even for every integer x, and thus it follows from (2.4) that $\Phi(u, v, w)$ is even for all integers u, v, w. But if $n \in \mathcal{L}$, then by the solubility of the congruence (1.3) one has that the congruence $\psi(\xi) \equiv n \pmod 2$ must be soluble. Then whenever $n \in \mathcal{L}$ and $m \equiv n \pmod 2$, one sees that the hypotheses of Lemma 4.3 are satisfied with $\gamma = \delta = 0$ and $p = 2$, whence Lemma 4.3 shows that $T(2, m) \gg 1$. Then in either case one has the lower bound (7.2).

(b) *Suppose that $2|\phi'(x)$ for every integer x, and for some integer y one has $4 \nmid \phi'(y)$.* Since for every integer x one has

$$\phi'(x + 2) \equiv \phi'(x) + 2\phi''(x) \equiv \phi'(x) \pmod 4,$$

our initial hypothesis implies that either $4 \nmid \phi'(0)$ or $4 \nmid \phi'(1)$. Suppose initially that in fact $2\|\phi'(x)$ for all even integers x. Then whenever $n \in \mathcal{L}$, the solubility of the congruence (1.3) ensures that there exist integers u_j $(1 \le j \le 20)$ and v satisfying

$$\phi(u_1) + \cdots + \phi(u_{20}) + \psi(v) \equiv n \tag{7.3}$$

modulo 8. But our initial hypothesis ensures that for every integer x,

$$\phi(x + 4) \equiv \phi(x) + 4\phi'(x) \equiv \phi(x) \pmod 8, \tag{7.4}$$

so that we may suppose without loss that $0 \le u_j \le 3$ $(1 \le j \le 20)$. If $u_j \in \{1, 3\}$ $(1 \le j \le 20)$ then at least 10 of the u_j are equal to some single value, whence by relabelling the u_j $(1 \le j \le 20)$, we may suppose that $u_{13} = u_{14} = \cdots = u_{20}$. But then one has

$$\phi(u_{13}) + \cdots + \phi(u_{20}) \equiv 0 \pmod 8, \tag{7.5}$$

and so we may solve the congruence (7.3) with $u_j = 0$ $(13 \le j \le 20)$. There is no loss of generality, therefore, in supposing that u_{20} is even, whence $2\|\phi'(u_{20})$. In the contrary case in which $2\|\phi'(x)$ for all odd integers x, we may proceed in like manner. In this instance, if the congruence (7.3) is soluble with $u_j \in \{0, 2\}$

$(1 \le j \le 20)$, then we may relabel variables so that $u_{13} = u_{14} = \cdots = u_{20}$, and (7.5) again holds. But then we may solve the congruence (7.3) with $u_j = 1$ $(13 \le j \le 20)$. There is no loss of generality in this second case, therefore, in supposing that u_{20} is odd, whence $2\|\phi'(u_{20})$. Thus in either case we may suppose that (7.3) possesses a solution with $2\|\phi'(u_{20})$.

Next we observe that by applying Lemma 7.1(ii) to the integers $u_1, \ldots, u_{19}$ occurring in (7.3), it follows by relabelling the u_i $(1 \le i \le 19)$ that there exist integers r_j, s_j, t_j $(j = 1, 2)$ satisfying the dozen congruences (6.1) simultaneously modulo 4. For these integers r_j, s_j, t_j $(j = 1, 2)$, suppose that $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are integers satisfying the congruences (7.1). Then by (7.4) one has that the congruence (6.21) is satisfied modulo 8, and on recalling the conclusion of the previous paragraph, we deduce that the congruence (6.23) possesses a solution modulo 8 with

$$w_j = u_{21-j} \quad (1 \le j \le 8), \quad w_9 = v \quad \text{and} \quad 2\|\phi'(w_1).$$

Consequently, the hypotheses of Lemma 4.3 are satisfied for the integer m given by (6.24) with $\gamma = 1$, $\delta = 0$ and $p = 2$. It therefore follows from Lemma 4.3 that $T(2, m) \gg 1$, whence the lower bound (7.2) follows immediately.

(c) *Suppose that* $4|\phi'(x)$ *for every integer* x*, and for some integer* y *one has* $8 \nmid \phi'(y)$*.* Observe that by (2.2) one has

$$\tfrac{1}{2}\phi''(x) \equiv a_3 x + a_2 \pmod 2 \quad \text{and} \quad \tfrac{1}{2}\phi'''(x) \equiv a_3 \pmod 2. \tag{7.6}$$

Thus, by the Binomial Theorem, for every integer x one has

$$\begin{aligned} \phi(x+4) &\equiv \phi(x) + 4\phi'(x) + 8\phi''(x) \pmod{32} \\ &\equiv \phi(x) + 4\phi'(x) + 16(a_3 x + a_2) \pmod{32}, \end{aligned} \tag{7.7}$$

$$\begin{aligned} \phi(x+2) &\equiv \phi(x) + 2\phi'(x) + 2\phi''(x) \pmod 8 \\ &\equiv \phi(x) + 4(a_3 x + a_2) \pmod 8, \end{aligned} \tag{7.8}$$

and

$$\begin{aligned} \phi'(x+2) &\equiv \phi'(x) + 2\phi''(x) + 2\phi'''(x) \pmod 8 \\ &\equiv \phi'(x) + 4(a_3 x + a_2 + a_3) \pmod 8. \end{aligned} \tag{7.9}$$

Further, on noting that (7.7) implies that $\phi(x+4) \equiv \phi(x) \pmod{16}$ for every integer x, it follows from the definition of $\mathcal{L}$ that for every $n \in \mathcal{L}$, there exist integers u_j $(1 \le j \le 20)$ and v with the property that the congruence (7.3) holds modulo 16, and moreover $0 \le u_j \le 3$ $(1 \le j \le 20)$.

We subdivide our argument according to the respective parities of a_2 and a_3.

(i) *Suppose that both* a_2 *and* a_3 *are odd.* It follows from (7.6) that for odd x one has $4|\phi''(x)$. Further, the relation (7.9) implies that $\phi'(3) \equiv \phi'(1) + 4 \pmod 8$, so that either $8 \nmid \phi'(1)$ or $8 \nmid \phi'(3)$. Suppose temporarily that the former is the case, whence by hypothesis we have $4 \| \phi'(1)$. Consider a solution $\mathbf{u}$, v of the congruence (7.3) modulo 16, of the type ensured by the argument above. Since (7.8) shows that $2\phi(3) \equiv 2\phi(1) \pmod{16}$, it follows that whenever two of the u_j are equal to 3, then we may replace both by 1 without affecting the validity of the congruence (7.3). Suppose next that at most one of the u_j is equal to 3, and that none are equal to 1. Then we may relabel variables so that for some ν with $0 \le \nu \le 19$, one has that $u_j = 0$ for $1 \le j \le \nu$, and $u_j = 2$ for $\nu + 1 \le j \le 19$. Moreover, since (7.8) shows that $4\phi(0) \equiv 4\phi(2) \pmod{16}$, it follows that whenever $\nu \ge 4$ we may adjust the values of the u_j so that $u_j = 2$ for $\nu - 3 \le j \le \nu$, without altering the validity of (7.3). Thus we may suppose that $0 \le \nu \le 3$. But then $u_j = 2$ for $4 \le j \le 19$, and so we may replace these 16 values of u_j by 1 without altering the validity of (7.3) modulo 16. In any case, we may suppose that at least one of the u_j is equal to 1, and by relabelling variables we may suppose further that $u_{20} = 1$ without loss of generality. If in fact $8 \nmid \phi'(3)$, whence $4 \| \phi'(3)$, then we may proceed along the same path, mutatis mutandis, and conclude that $u_{20} = 3$ via a relabelling of variables. Thus in either case it follows that with $\xi_0 = 1$ or 3, one may relabel variables so that $u_{20} = \xi_0$ and $4 \| \phi'(u_{20})$.

Next observe that by applying Lemma 7.1(ii) to the integers $u_1, \ldots, u_{19}$, we may guarantee that by suitably relabelling variables, there exist integers r_j, s_j, t_j $(j = 1, 2)$ satisfying the dozen congruences (6.1) simultaneously modulo 4. For these integers r_j, s_j, t_j $(j = 1, 2)$, suppose that $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are integers satisfying the congruences (7.1). Then by (7.7) one finds that the congruence (6.21) is satisfied modulo 16, and hence, on recalling the conclusion of the previous paragraph, it follows that the congruence (6.23) modulo 16 possesses a solution with

$$w_j = u_{21-j} \quad (1 \le j \le 8), \quad w_9 = v, \quad 4 \| \phi'(w_1) \quad \text{and} \quad 2 | \tfrac{1}{2}\phi''(w_1).$$

Consequently, the hypotheses of Lemma 4.3 are satisfied for the integer m defined by (6.24) with $\gamma = 2$, $\delta = 1$ and $p = 2$. We therefore obtain from Lemma 4.3 the lower bound $T(2, m) \gg 1$, whence (7.2) follows immediately.

(ii) *Suppose that a_2 is even and a_3 is odd.* We may again apply (7.9), in this instance to deduce that $\phi'(2) \equiv \phi'(0) + 4 \pmod 8$. Further, the congruence (7.8) implies that $\phi(2) \equiv \phi(0) \pmod 8$ and $\phi(3) \equiv \phi(1) \pmod 4$. Also, it follows from (7.6) that for even integers x one has $4 | \phi''(x)$. On interchanging the roles of $\{1, 3\}$ and $\{0, 2\}$, therefore, we find that the argument of part (i) may be applied, mutatis mutandis, in order to establish the lower bound (7.2) also in this case.

(iii) *Suppose that both a_2 and a_3 are even.* It now follows from (7.6) that for every integer x one has $4 | \phi''(x)$. Also, on noting that our hypothesis (c) implies that $4 | \phi'(0)$ and $4 | \phi'(1)$, and recalling (2.2), we find that necessarily both a_1 and a_5 are even. Then our assumption following (2.2) that $(a_1, a_2, a_3, a_4, a_5) = 1$ leads to the conclusion that a_4 is odd. Consequently $\phi(1)$ must be odd, and so $\mathcal{K}(16, 1)$ contains at least two elements, namely 0 and $\phi(1)$. We therefore deduce from the Cauchy-Davenport theorem (see [9, Lemma 2.14]) that $K(16, 15) = 16$. By the hypothesis (c), there is an integer ξ_0 with $4 \| \phi'(\xi_0)$. We take $u_{20} = \xi_0$, and then solve the congruence (7.3) modulo 16 for u_j $(1 \le j \le 19)$ and v. The latter is possible in view of our earlier observation that $K(16, 15) = 16$. We now find ourselves in a position essentially identical with that holding at the start of the concluding paragraph of case (i) above, and thus we may apply an identical argument to establish the desired lower bound (7.2).

(iv) *Suppose that a_2 is odd and a_3 is even.* We begin by noting that (7.9) implies that for every integer x one has

$$\phi'(x+2) \equiv \phi'(x) + 4 \pmod 8. \tag{7.10}$$

Moreover, if y is an integer with $8|\phi'(y)$, then by (7.7) one has

$$\phi(y+4) \equiv \phi(y) + 16 \pmod{32}. \tag{7.11}$$

Consequently, if w_1 and w_2 are integers with $w_1 \equiv w_2 + 2 \pmod 4$, then by suitably relabelling variables, we may suppose without loss of generality that

$$\phi(w_1+4) \equiv \phi(w_1) + 16 \pmod{32} \quad \text{and} \quad 4\|\phi'(w_2). \tag{7.12}$$

For if $8|\phi'(w_1)$, then the first relation in (7.12) follows from (7.11), and the second relation follows from (7.10). Meanwhile, if $8 \nmid \phi(w_1)$, then by the hypothesis (c) we have $4\|\phi'(w_1)$, and it follows from (7.10) that $8|\phi'(w_2)$, whence from (7.11) we have $\phi(w_2+4) \equiv \phi(w_2) + 16 \pmod{32}$.

Consider next a solution $\mathbf{u}$, v of the congruence (7.3) modulo 16, of the type ensured by the conclusion of the opening paragraph of case (c) above. Since $0 \le u_j \le 3$ $(1 \le j \le 20)$, an application of the pigeon-hole principle guarantees that at least 5 of the u_j are equal, whence by relabelling variables we may suppose that

$$u_{16} = u_{17} = \dots = u_{20}.$$

On recalling (7.8), one has that $4\phi(u_{20}) \equiv 4\phi(u_{20} \pm 2) \pmod{16}$, and thus if we replace u_j by $u_{20} + 2$ for $16 \le j \le 19$, or by $u_{20} - 2$ for $16 \le j \le 19$, then the congruence (7.3) remains valid modulo 16. Thus, by the argument leading to (7.12), we may relabel variables so that

$$u_{19} \equiv u_{20} + 2 \pmod 4, \tag{7.13}$$

$$\phi(u_{19}+4) \equiv \phi(u_{19}) + 16 \pmod{32} \quad \text{and} \quad 4\|\phi'(u_{20}). \tag{7.14}$$

Applying the pigeon-hole principle once again with the integers u_j $(1 \le j \le 18)$, we find that we may relabel the u_j with $1 \le j \le 18$ so that $u_{2j-1} = u_{2j}$ $(1 \le j \le 7)$. It is possible that two of the u_j with $15 \le j \le 18$ are equal, in which case we relabel the latter variables so that $u_{15} = u_{16}$. Otherwise, the sets $\{u_{15}, u_{16}, u_{17}, u_{18}\}$ and $\{0, 1, 2, 3\}$ are necessarily equal, and by (7.13) and (7.14) we may relabel the u_j with $15 \le j \le 20$ so that $u_{15} = u_{20}$, $u_{16} \equiv u_{17} + 2 \pmod 4$, and moreover so that $4\|\phi'(u_{16})$. In this latter case we relabel variables so as to interchange u_{16}

and u_{20}, and similarly u_{17} and u_{19}. Consequently, in any case, we can assume that the congruence (7.3) modulo 16 has a solution $\mathbf{u}$, v satisfying (7.14), and with $u_{2j-1} = u_{2j}$ $(1 \le j \le 8)$. By relabelling the variables u_j $(1 \le j \le 16)$, therefore, it follows from Lemma 7.1(i) that there exist integers r_j, s_j, t_j $(j = 1, 2)$ with the property that the dozen congruences (6.1) hold simultaneously modulo 4. For these integers r_j, s_j, t_j $(j = 1, 2)$, suppose that $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ are integers satisfying the congruences (7.1). Then by (7.7) one finds that the congruence (6.21) is satisfied modulo 16, and hence, by (7.14), that the congruence (6.23) modulo 16 possesses a solution with

$$w_j = u_{21-j} \quad (1 \le j \le 8), \quad w_9 = v,$$

$$4 \| \phi'(w_1) \quad \text{and} \quad \phi(w_2 + 4) \equiv \phi(w_2) + 16 \pmod{32}. \tag{7.15}$$

But the final relation of (7.15) permits us, if necessary, to adjust the value of w_2 so as to replace the congruence (6.23) modulo 16 by the stronger congruence (6.23) modulo 32. Thus the hypotheses of Lemma 4.3 are satisfied for the integer m given by (6.24) with $\gamma = 2$, $\delta = 0$ and $p = 2$. We therefore conclude from Lemma 4.3 that $T(2, m) \gg 1$, whence the lower bound (7.2) follows immediately.

(d) *Suppose that* $8 | \phi'(x)$ *for every integer* x. On recalling (2.2), we find that

$$\phi'(0) = a_1 \equiv 0 \pmod 8, \quad \phi'(1) - \phi'(-1) \equiv 4a_2 \equiv 0 \pmod 8,$$

$$\phi'(2) \equiv 12a_3 + 4a_2 + a_1 \equiv 0 \pmod 8,$$

$$\phi'(1) + \phi'(-1) = 10a_5 + 6a_3 + 2a_1 \equiv 0 \pmod 8.$$

Consequently, one has that a_5, a_3, a_2, a_1 are all even. Then by our assumption following (2.2) that $(a_5, a_4, a_3, a_2, a_1) = 1$, one has that a_4 is odd. Thus we deduce from (2.2) that for every integer x one has

$$\phi''(x) \equiv (4 + 6a_3)x + 2a_2 \pmod 8 \quad \text{and} \quad \phi'''(x) \equiv 6a_3 \pmod 8. \tag{7.16}$$

An application of the Binomial Theorem now reveals that for every integer x one has

$$\begin{aligned}\phi(x+4) &\equiv \phi(x) + 4\phi'(x) + 8\phi''(x) \pmod{64} \\ &\equiv \phi(x) + 4\phi'(x) + 16((2 + 3a_3)x + a_2) \pmod{64},\end{aligned} \tag{7.17}$$

$$\begin{aligned}\phi(x+2) &\equiv \phi(x) + 2\phi'(x) + 2\phi''(x) + 4\phi'''(x)/3 \pmod{16} \\ &\equiv \phi(x) + 4((2 + 3a_3)x + a_2) \pmod{16},\end{aligned} \tag{7.18}$$

$$\begin{aligned}\phi'(x+2) &\equiv \phi'(x) + 2\phi''(x) + 2\phi'''(x) + 4\phi''''(x)/3 \pmod{16} \\ &\equiv \phi'(x) + (8 + 12a_3)x + 4a_2 + 12a_3 \pmod{16}.\end{aligned} \tag{7.19}$$

We divide our argument according to the respective residue classes of a_3 and a_2 modulo 4.

(i) *Suppose that* $a_3 \equiv 2 \pmod 4$ *and* $a_2 \equiv 0 \pmod 4$. In this case it follows from (7.16)-(7.19) that for every integer x, one has

$$\phi''(x) \equiv 0 \pmod 8, \quad \phi(x+2) \equiv \phi(x) \pmod{16}, \tag{7.20}$$

$$\phi'(x+2) \equiv \phi'(x) + 8 \pmod{16}, \quad \phi(x+4) \equiv \phi(x) \pmod{32}. \tag{7.21}$$

Notice, in particular, that by hypothesis the first congruence of (7.21) implies that for every integer x, one has either

$$8 \| \phi'(x) \quad \text{or} \quad 8 \| \phi'(x+2). \tag{7.22}$$

Observe next that whenever $n \in \mathcal{L}$, the solubility of the congruence (1.3) implies that there exist integers u_j $(1 \le j \le 20)$ and v for which the congruence (7.3) is soluble modulo 32. In view of the second congruence of (7.21), moreover, we may suppose without loss of generality that $0 \le u_j \le 3$ $(1 \le j \le 20)$ in the latter solution. On noting (7.20), we may apply the argument of the second paragraph of case (iv) of part (c) to show, subject to a suitable relabelling of the u_j $(1 \le j \le 20)$, that there exists a solution $\mathbf{u}$, v of the congruence (7.3) modulo 32 with the property that $u_{19} \equiv u_{20} + 2 \pmod 4$. In view of (7.22), therefore, we may relabel the u_j $(1 \le j \le 20)$ in such a way that $8 \| \phi'(u_{20})$. By relabelling the u_j with $1 \le j \le 19$, it now follows from Lemma 7.1(ii) that there exist integers r_j, s_j, t_j $(j = 1, 2)$ with the property that the dozen congruences (6.1) hold simultaneously modulo 4. For these integers r_j, s_j, t_j $(j = 1, 2)$, suppose that $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are integers satisfying the congruences (7.1). Then by (7.21) one finds that the congruence (6.21) is satisfied modulo 32, and hence, by the above argument, that the congruence (6.23) modulo 32 possesses a solution with $8 \| \phi'(w_1)$. On recalling (7.20), we find that the hypotheses of Lemma 4.3 are satisfied for the integer m given by (6.24) with $\gamma = 3$, $\delta = 2$ and $p = 2$. We therefore conclude from Lemma 4.3 that $T(2, m) \gg 1$, whence the lower bound (7.2) follows immediately.

(ii) *Suppose that* $a_3 \equiv 0 \pmod 4$ *and* $a_2 \equiv 2 \pmod 4$. We begin by noting that all the residue classes modulo 32 are represented in the form $\mu\phi(1) + \nu\phi(2)$ with $0 \le \mu \le 7$ and $0 \le \nu \le 3$. In order to establish this claim, it suffices to show that whenever

$$\mu\phi(1) + \nu\phi(2) \equiv \mu'\phi(1) + \nu'\phi(2) \pmod{32} \tag{7.23}$$

with $0 \le \mu, \mu' \le 7$ and $0 \le \nu, \nu' \le 3$, then necessarily $\mu = \mu'$ and $\nu = \nu'$. But in view of our earlier hypotheses, the congruence (7.18) implies that $8 \| \phi(2)$, and further $\phi(1) \equiv a_4 \pmod 2$, whence $\phi(1)$ is odd. Thus (7.23) implies that $(\mu - \mu')\phi(1) \equiv 0 \pmod 8$, whence $\mu = \mu'$. Consequently, one has $(\nu - \nu')\phi(2) \equiv 0 \pmod{32}$, so that in view of our earlier observation that $8 \| \phi(2)$ we have $\nu = \nu'$.

Observe next that by hypothesis, it follows from (7.19) that $\phi'(2) \equiv \phi'(0) + 8 \pmod{16}$. Further, if x is even and $16 | \phi'(x)$, then by (7.17) one has $\phi(x+4) \equiv \phi(x) + 32 \pmod{64}$. Thus there exist even integers u_{19}, u_{20} satisfying

$$\phi(u_{19} + 4) \equiv \phi(u_{19}) + 32 \pmod{64} \quad \text{and} \quad 8 \| \phi'(u_{20}). \tag{7.24}$$

Fix these choices of u_{19} and u_{20}, and fix also any choice of v and n. Then it follows from the discussion of the previous paragraph that there are integers μ and ν with $0 \le \mu \le 7$ and $0 \le \nu \le 3$, such that the congruence (7.3) is satisfied modulo 32 with

$$u_j = \begin{cases} 1, & \text{when } 1 \le j \le \mu, \\ 2, & \text{when } \mu + 1 \le j \le \mu + \nu, \\ 0, & \text{when } \mu + \nu + 1 \le j \le 18. \end{cases} \tag{7.25}$$

Notice that the choice of u_j $(1 \le j \le 18)$ provided by (7.25) has the property that $u_j \not\equiv 3 \pmod 4$ for $1 \le j \le 18$. Then it follows from Lemma 7.1(iii) that by relabelling the u_j with $1 \le j \le 18$, there exist integers r_j, s_j, t_j $(j = 1, 2)$ with the property that the dozen congruences (6.1) hold simultaneously modulo 4. For these integers r_j, s_j, t_j $(j = 1, 2)$, suppose that $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are integers satisfying the congruences (7.1). Notice that by making use of our hypotheses in (7.17) one finds that $\phi(x + 4) \equiv \phi(x) \pmod{32}$ for every integer x. Thus the congruence (6.21) is satisfied modulo 32, and hence, by (7.24), the congruence (6.23) modulo 32 possesses a solution with

$$w_j = u_{21-j} \quad (1 \le j \le 8), \quad w_9 = v,$$

$$8 \| \phi'(w_1) \quad \text{and} \quad \phi(w_2 + 4) \equiv \phi(w_2) + 32 \pmod{64}. \tag{7.26}$$

But the final relation of (7.26) permits us, if necessary, to adjust the value of w_2 so as to replace the congruence (6.23) modulo 32 by the stronger congruence (6.23) modulo 64. On recalling (7.16), it follows from the hypothesis (ii) that the hypotheses of Lemma 4.3 are satisfied for the integer m given by (6.24) with $\gamma = 3$, $\delta = 1$ and $p = 2$. We therefore conclude from Lemma 4.3 that $T(2, m) \gg 1$, whence the lower bound (7.2) follows immediately.

(iii) *Suppose that* $a_3 \equiv a_2 \equiv 0 \pmod 4$. We again have that $\phi(1)$ is odd, and further the congruence (7.18) in this instance shows that $8 \| (\phi(3) - \phi(1))$. In this case, therefore, we find that all residue classes modulo 32 are represented in the form $\mu\phi(1) + \nu(\phi(3) - \phi(1))$ for some integers μ and ν satisfying $0 \le \nu \le 3 \le \mu \le 10$. Consequently, given an integer m, the congruence

$$\phi(u_1) + \cdots + \phi(u_{18}) \equiv m \pmod{32}$$

possesses a solution of the form

$$u_j = \begin{cases} 1, & \text{when } 1 \le j \le \mu - \nu, \\ 3, & \text{when } \mu - \nu + 1 \le j \le \mu, \\ 0, & \text{when } \mu + 1 \le j \le 18. \end{cases}$$

Also, by (7.19) one has $\phi'(3) \equiv \phi'(1) + 8 \pmod{16}$, and by (7.17) we have that whenever x is odd and $16 | \phi'(x)$, then $\phi(x + 4) \equiv \phi(x) + 32 \pmod{64}$. Then we may conclude that there are odd integers u_{19} and u_{20} satisfying (7.24). On interchanging the roles of the sets $\{0, 1, 2\}$ and $\{0, 1, 3\}$, therefore, we may apply the argument concluding our treatment of the previous case, mutatis mutandis, in order to establish the lower bound (7.2) in the present case.

(iv) *Suppose that* $a_3 \equiv a_2 \equiv 2 \pmod 4$. In this case (7.18) shows that $8\|\phi(2)$, and (7.19) shows that for all integers x one has

$$\phi'(x+2) \equiv \phi'(x) \pmod{16}. \tag{7.27}$$

Regrettably, at this stage we are forced to subdivide our argument still further.

(1) *Suppose that* $\phi'(0) \equiv \phi'(1) \equiv 8 \pmod{16}$. Then for all integers x, the congruence (7.27) shows that $8\|\phi'(x)$. By (7.17), moreover, for every integer x one has

$$\phi(x+4) \equiv \phi(x) \pmod{64}. \tag{7.28}$$

Since all residue classes modulo 64 can now be represented in the form $\mu\phi(1)+\nu\phi(2)$ with $0 \le \mu, \nu \le 7$, it is immediate that $K(64,14) = 64$. Consequently, for every integer n, the congruence (7.3) is soluble modulo 64. By relabelling the u_j with $1 \le j \le 19$, it now follows from Lemma 7.1(ii) that there exist integers r_j, s_j, t_j $(j=1,2)$ with the property that the dozen congruences (6.1) hold simultaneously modulo 4. For these integers r_j, s_j, t_j $(j=1,2)$, suppose that $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are integers satisfying the congruences (7.1). Then by (7.28) one finds that the congruence (6.21) is satisfied modulo 64, and hence that the congruence (6.23) modulo 64 possesses a solution. Further, since $8\|\phi'(x)$ for every x, the latter solution necessarily satisfies $8\|\phi'(w_1)$. On recalling (7.16), it follows from the hypothesis (iv) that the hypotheses of Lemma 4.3 are satisfied for the integer m given by (6.24) with $\gamma = 3$, $\delta = 1$ and $p = 2$. We therefore conclude from Lemma 4.3 that $T(2,m) \gg 1$, whence the lower bound (7.2) follows immediately.

(2) *Suppose that* $\phi'(0) \equiv 8 \pmod{16}$ *and* $\phi'(1) \equiv 0 \pmod{16}$, *or* $\phi'(0) \equiv 0 \pmod{16}$ *and* $\phi'(1) \equiv 8 \pmod{16}$. As in the previous case, all residue classes modulo 64 are represented in the form $\mu\phi(1)+\nu\phi(2)$ with $0 \le \mu, \nu \le 7$, and it is immediate that $K(64,14) = 64$. We take $u_{19} = 1$ and $u_{20} = 0$, or $u_{19} = 0$ and $u_{20} = 1$, in the respective cases, and observe that (7.17) implies that $\phi(u_{19}+4) \equiv \phi(u_{19})+32 \pmod{64}$. Consequently, on noting our initial hypothesis, we find that the conditions (7.24) are satisfied, and thus we may apply the argument of case (d)(ii) above without further alteration in order to establish the lower bound (7.2).

(3) *Suppose that* $\phi'(0) \equiv \phi'(1) \equiv 0 \pmod{16}$. Then it follows from (7.27) that $16|\phi'(x)$ for every integer x, and so on recalling the hypothesis (iv), it follows from (7.17) that for every integer x one has

$$\phi(x+4) \equiv \phi(x) + 32 \pmod{64}. \tag{7.29}$$

Next, again recalling the hypothesis (iv), we find from (7.16) that for every integer x one has $\phi''(x) \equiv 4 \pmod 8$ and $\phi'''(x) \equiv 0 \pmod 4$. Consequently, by the Binomial Theorem, for every integer x one has

$$\phi'(x+4) \equiv \phi'(x) + 4\phi''(x) + 8\phi'''(x) \equiv \phi'(x) + 16 \pmod{32}. \tag{7.30}$$

When $n \in \mathcal{L}$, it follows from the solubility of the congruence (1.3) that there are integers u_j $(1 \le j \le 20)$ and v such that the congruence (7.3) is satisfied modulo 32. On applying Lemma 7.1(ii) to the integers u_j $(1 \le j \le 19)$, we deduce that there exist integers r_j, s_j, t_j $(j = 1, 2)$ for which the dozen congruences (6.1) hold simultaneously modulo 4. For these integers r_j, s_j, t_j $(j = 1, 2)$, suppose that $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are integers satisfying the congruences (7.1). Then by (7.29) one finds that the congruence (6.21) is satisfied modulo 32. Define the integer m as in (6.24). Also, set $w_9 = v$, and set $w_1 = u_{13}$ or $w_1 = u_{13} + 4$ in such a way that $16 \| \phi'(w_1)$. The latter is possible, of course, by (7.30). Then in view of (7.29), we obtain

$$\phi(w_1) + \phi(u_{14}) + \cdots + \phi(u_{20}) + \psi(w_9) \equiv m - 32l \pmod{256}, \tag{7.31}$$

for some integer l.

Next, for $14 \le j \le 20$, we put

$$\xi_j = (\phi(u_j + 4) - \phi(u_j))/32, \tag{7.32}$$

and define $\mathcal{C}_j = \{0, \xi_j\}$. It follows from (7.29) that ξ_j is odd for every j, and thus repeated application of the Cauchy-Davenport theorem (see [9, Lemma 2.14]) shows that every residue class modulo 8 is represented in the form $\eta_{14} + \cdots + \eta_{20}$ with $\eta_j \in \mathcal{C}_j$ $(14 \le j \le 20)$. Thus, given the integer l occurring in (7.31), there exists a set $\mathcal{J} \subseteq \{14, 15, \dots, 20\}$ with the property that

$$\sum_{j \in \mathcal{J}} \xi_j \equiv l \pmod{8},$$

whence by (7.32),

$$\sum_{j \in \mathcal{J}} \phi(u_j + 4) + \sum_{\substack{j \notin \mathcal{J} \\ 14 \le j \le 20}} \phi(u_j) \equiv \sum_{j=14}^{20} \phi(u_j) + 32l \pmod{256}. \tag{7.33}$$

On putting $w_{j-12} = u_j + 4$ or $w_{j-12} = u_j$ according to whether or not $j \in \mathcal{J}$ for $14 \le j \le 20$, we deduce from (7.31) and (7.33) that

$$\phi(w_1) + \cdots + \phi(w_8) + \psi(w_9) \equiv m \pmod{256}.$$

In view of our earlier observations to the effect that $\phi''(x) \equiv 4 \pmod 8$ for every x, and $16 \| \phi'(w_1)$, we may conclude that the hypotheses of Lemma 4.3 are satisfied with $\gamma = 4$, $\delta = 1$ and $p = 2$. We thus deduce from Lemma 4.3 that $T(2, m) \gg 1$, whence the lower bound (7.2) follows immediately.

This concludes the proof of the lemma.

8. Averaging the auxiliary singular series, and the density of $\mathcal{L}$

In this section we conclude our discussion of the auxiliary singular series by extracting the consequences of the above discussion necessary for our proof of Theorem 2. We begin with an estimate concerning a suitable average of the auxiliary singular series. When P is a large real number and n is a natural number, we define the averaged singular series $\widetilde{\mathfrak{S}}(n;P)$ by

$$\widetilde{\mathfrak{S}}(n;P)=\sum_{\substack{1\le x_1,y_1\le P/3\\ 1\le x_2,y_2\le P/3}}\sum_{P<z_1,z_2\le 2P}\mathfrak{S}(n-\Phi(x_1,y_1,z_1)-\Phi(x_2,y_2,z_2)).$$

Lemma 8.1. *Let P be a large real number. Then whenever $n\in\mathcal{L}$, one has $\widetilde{\mathfrak{S}}(n;P)\gg P^6$.*

Proof. Suppose that P is a large real number and $n\in\mathcal{L}$. Then by the Chinese Remainder Theorem, it follows from Lemmata 6.2 and 7.2 that there exist integers r_j,s_j,t_j $(j=1,2)$ such that whenever x_j,y_j,z_j $(j=1,2)$ are integers satisfying the congruences

$$x_j\equiv r_j\pmod{12},\quad y_j\equiv s_j\pmod{12}\quad\text{and}\quad z_j\equiv t_j\pmod{12}\quad(j=1,2),\tag{8.1}$$

then one has

$$T(p,n-\Phi(x_1,y_1,z_1)-\Phi(x_2,y_2,z_2))\gg 1\tag{8.2}$$

for both $p=2$ and $p=3$. Then on recalling Lemmata 5.1 and 5.2, and making use of Lemma 4.2(i), we deduce that whenever $\mathbf{x},\mathbf{y},\mathbf{z}$ satisfy (8.1), one has

$$\mathfrak{S}(n-\Phi(x_1,y_1,z_1)-\Phi(x_2,y_2,z_2))\gg 1.$$

We therefore conclude from Lemma 4.2(iii) that

$$\widetilde{\mathfrak{S}}(n;P)\gg\sum_{1\le x_1,y_1\le P/3}\sum_{1\le x_2,y_2\le P/3}\sum_{P<z_1,z_2\le 2P}1,$$

where we now restrict the summation to be over $\mathbf{x},\mathbf{y},\mathbf{z}$ satisfying (8.1). Consequently, one has $\widetilde{\mathfrak{S}}(n;P)\gg P^6$, and so the proof of the lemma is complete.

We complete this section by demonstrating that the set $\mathcal{L}$ has positive density, and this we achieve cheaply by making use of the discussion in §§5-7. We take a to be a large positive integer, and define the integer n_0 by $n_0=20\phi(a)+\psi(1)$. Then plainly we have $n_0\in\mathcal{L}$. Observe that by (4.3) and (4.8), it follows that whenever $T(p,m)>0$, then necessarily the congruence (4.5) is soluble with $q=p^h$ for every natural number h. In particular, Lemma 5.1 shows that the congruence (4.5) is soluble with $q=p^h$ for every prime p with $p\ge 7$, and every natural number h. Next write $q_0=2^8\cdot 3^4\cdot 5^2$, and take p to be one of 2, 3 and 5. Observe that since $n_0\in\mathcal{L}$, then the arguments of the proofs of Lemmata 5.2, 6.2 and 7.2 show that whenever $n \equiv n_0 \pmod{q_0}$, then there exist integers x_j, y_j, z_j $(j = 1, 2)$ such that the lower bound (8.2) holds. It follows that the congruence (4.5) is soluble with the integer m given by (6.24), and with $q = p^h$ for every natural number h. On recalling (2.4), therefore, we may conclude that whenever $n \equiv n_0 \pmod{q_0}$, then the congruence (1.3) is soluble with $q = p^h$, for any prime p and natural number h, whence by the Chinese Remainder Theorem, the same must hold for every natural number q. Thus $\mathcal{L}$ contains, at least, the arithmetic progression $n \equiv n_0 \pmod{q_0}$, and consequently $\mathcal{L}$ has positive density. Thus we have established the first claim of Theorem 2.

9. Application of the Hardy-Littlewood method

Our analysis of the auxiliary singular series now complete, we may move on to apply the Hardy-Littlewood method. We begin by recalling some consequences of well-known estimates for the exponential sums $f(\alpha)$ and $g(\alpha)$. When $\beta \in \mathbb{R}$, we write

$$v(\beta) = \int_{P/2}^{P} e(\phi(t)\beta)dt \quad \text{and} \quad v_1(\beta) = \int_{\sqrt{Q}}^{Q} e(\psi(t)\beta)dt.$$

Lemma 9.1. *Let $\alpha \in \mathbb{R}$, and suppose that $\beta \in \mathbb{R}$, $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ satisfy $\alpha = \beta + a/q$ and $(a, q) = 1$. Then*

$$f(\alpha) = q^{-1}S(q, a)v(\beta) + O(q(1 + N|\beta|)) \tag{9.1}$$

and

$$g(\alpha) = (\lambda(q))^{-1}S_1(q, a)v_1(\beta) + O(q(1 + N|\beta|)). \tag{9.2}$$

Further, when $\beta \in \mathbb{R}$ one has

$$v(\beta) \ll P(1 + N|\beta|)^{-1/5} \quad \textit{and} \quad v_1(\beta) \ll Q(1 + N|\beta|)^{-1/k}. \tag{9.3}$$

Proof. The estimates (9.1) and (9.2) are immediate from [9, Theorem 7.2], and the estimates (9.3) follow from [9, Theorem 7.3].

Let $n \in \mathcal{L}$, and write $\mathcal{R}(n)$ for the number of representations of n in the form (1.4) with $x_i \in \mathbb{Z}$ $(1 \le i \le 21)$. If $\mathcal{R}(n)$ is infinite, of course, then there is nothing left to prove, so we suppose that $\mathcal{R}(n)$ is finite. Then by considering the underlying diophantine equation, it follows from (2.4) via orthogonality that

$$\mathcal{R}(n) \ge \int_0^1 F(\alpha)^2 f(\alpha)^8 g(\alpha) e(-n\alpha) d\alpha. \tag{9.4}$$

When $\mathfrak{B} \subseteq [0, 1)$, write

$$\mathcal{R}(n; \mathfrak{B}) = \int_{\mathfrak{B}} F(\alpha)^2 f(\alpha)^8 g(\alpha) e(-n\alpha) d\alpha. \tag{9.5}$$

Write $X = Q^{1/(15k)}$, and define the major arcs $\mathfrak{M}$ by

$$\mathfrak{M} = \bigcup_{\substack{0\le a\le q\le X\\(a,q)=1}} \mathfrak{M}(q,a),$$

where

$$\mathfrak{M}(q,a) = \{\alpha \in [0,1) \ : \ |\alpha - a/q| \le q^{-1}XN^{-1}\}.$$

Notice that the $\mathfrak{M}(q,a)$ comprising $\mathfrak{M}$ are mutually disjoint. Also, define the minor arcs $\mathfrak{m}$ by $\mathfrak{m} = [0,1)\setminus\mathfrak{M}$. By (9.4) and (9.5), therefore, we have

$$\mathcal{R}(n) \ge \mathcal{R}(n;\mathfrak{M}) + \mathcal{R}(n;\mathfrak{m}). \tag{9.6}$$

The minor arcs may be swiftly disposed of. By Weyl's inequality (see [9, Lemma 2.4]), one has

$$\sup_{\alpha\in\mathfrak{m}} |g(\alpha)| \ll Q^{1+\varepsilon}X^{-2^{1-k}} \ll Q^{1-2\eta},$$

where $\eta = (k2^{k+4})^{-1}$. Then by Lemma 3.1, it follows from (9.5) that

$$\mathcal{R}(n;\mathfrak{m}) \le \sup_{\alpha\in\mathfrak{m}} |g(\alpha)| \int_0^1 |F(\alpha)^2 f(\alpha)^8|d\alpha \ll P^9Q^{1-\eta}. \tag{9.7}$$

On recalling (2.6), we next find from (9.5) that

$$\mathcal{R}(n;\mathfrak{M}) = \sum_{\substack{1\le x_1,y_1\le P/3\\1\le x_2,y_2\le P/3}} \sum_{P<z_1,z_2\le 2P} \mathcal{T}(n-\Phi(x_1,y_1,z_1)-\Phi(x_2,y_2,z_2)), \tag{9.8}$$

where for each integer m we write

$$\mathcal{T}(m) = \int_{\mathfrak{M}} f(\alpha)^8 g(\alpha) e(-m\alpha)d\alpha. \tag{9.9}$$

Write

$$J(m) = \int_{-\infty}^{\infty} v(\beta)^8 v_1(\beta)e(-m\beta)d\beta, \tag{9.10}$$

$$J(m;q,X) = \int_{-X/(qN)}^{X/(qN)} v(\beta)^8 v_1(\beta)e(-m\beta)d\beta \tag{9.11}$$

and

$$\mathcal{T}(m;X) = \sum_{1\le q\le X} \mathcal{S}(q,m)J(m;q,X), \tag{9.12}$$

where $\mathcal{S}(q,m)$ is defined as in (4.2). By Lemma 9.1, whenever $\alpha\in\mathfrak{M}(q,a)\subseteq\mathfrak{M}$, one has

$$f(\alpha) - q^{-1}S(q,a)v(\alpha-a/q) \ll q(1+N|\alpha-a/q|) \ll X$$

and

$$g(\alpha) - (\lambda(q))^{-1} S_1(q,a) v_1(\alpha - a/q) \ll q(1 + N|\alpha - a/q|) \ll X.$$

Thus, on making use of trivial estimates for $f(\alpha)$ and $g(\alpha)$, we find that whenever $\alpha \in \mathfrak{M}(q,a) \subseteq \mathfrak{M}$, one has

$$f(\alpha)^8 g(\alpha) - (\lambda(q))^{-1} q^{-8} S(q,a)^8 S_1(q,a) v(\alpha - a/q)^8 v_1(\alpha - a/q) \ll XP^8 + XP^7 Q.$$

Since the measure of $\mathfrak{M}$ is $O(X^2 N^{-1})$, we deduce from (2.3) and (9.9)-(9.12) that

$$\mathcal{T}(m) - \mathcal{T}(m;X) \ll X^3 P^8 N^{-1} + X^3 P^7 Q N^{-1} \ll P^3 Q X^{-1}. \tag{9.13}$$

Also, again by Lemma 9.1, when $q \le X$ one has

$$J(m;q,X) - J(m) \ll P^8 Q \int_{X/(qN)}^{\infty} (1 + N\beta)^{-\frac{8}{5} - \frac{1}{k}} d\beta \ll P^3 Q (q/X)^{1/k}. \tag{9.14}$$

Further, by (4.4) and Lemma 4.2(ii) one has

$$|\mathfrak{S}(m) - \sum_{1 \le q \le X} \mathcal{S}(q,m)| \ll \sum_{q > X} (q/X)^{1/k} |\mathcal{S}(q,m)| \ll X^{-1/k}. \tag{9.15}$$

Furthermore, it follows from Lemma 4.2(iii) and Lemma 9.1 that

$$\mathfrak{S}(m) \ll 1 \quad \text{and} \quad J(m) \ll P^3 Q. \tag{9.16}$$

Combining the estimates (9.14)-(9.16) together with (9.12), we deduce that

$$\begin{aligned} \mathcal{T}(m;X) - \mathfrak{S}(m) J(m) &= \sum_{1 \le q \le X} \mathcal{S}(q,m)(J(m;q,X) - J(m)) \\ &\quad - J(m)\Big(\mathfrak{S}(m) - \sum_{1 \le q \le X} \mathcal{S}(q,m)\Big) \\ &\ll P^3 Q X^{-1/k} \Big(1 + \sum_{1 \le q \le X} q^{1/k} |\mathcal{S}(q,m)|\Big). \end{aligned}$$

Then by (9.13) and Lemma 4.2(ii), we have

$$\mathcal{T}(m) = \mathfrak{S}(m) J(m) + O(P^3 Q X^{-1/k}). \tag{9.17}$$

Substituting (9.17) into (9.8), we obtain

$$\mathcal{R}(n;\mathfrak{M}) = \mathcal{U}(n) + O(P^9 Q X^{-1/k}), \tag{9.18}$$

where

$$\mathcal{U}(n) = \sum_{\substack{1\le x_1,y_1\le P/3\\ 1\le x_2,y_2\le P/3}} \sum_{P<z_1,z_2\le 2P} \mathfrak{S}(m)J(m), \tag{9.19}$$

and here m is the integer defined in (6.24).

We must now analyse the singular integral $J(m)$. Since P and Q are large, we may suppose without loss of generality that $\phi(t)$ is monotone for $t \ge \frac{1}{2}P$, and similarly that $\psi(t)$ is monotone for $t \ge \sqrt{Q}$. A change of variable therefore yields

$$v(\beta) = \int_{\phi(P/2)}^{\phi(P)} \frac{e(u\beta)}{\phi'(\phi^{-1}(u))} du \quad \text{and} \quad v_1(\beta) = \int_{\psi(\sqrt{Q})}^{\psi(Q)} \frac{e(u\beta)}{\psi'(\psi^{-1}(u))} du.$$

Consequently,

$$v(\beta)^8 v_1(\beta) = \int_{-\infty}^{\infty} \tilde{J}(u)e(u\beta)du,$$

where

$$\tilde{J}(u) = \int_{\mathcal{B}(u)} (\Xi(u;\mathbf{u}))^{-1} d\mathbf{u}, \tag{9.20}$$

$$\Xi(u;\mathbf{u}) = |\psi'(\psi^{-1}(u-u_1-u_2-\cdots-u_8))| \prod_{i=1}^{8} \phi'(\phi^{-1}(u_i)), \tag{9.21}$$

and $\mathcal{B}(u)$ is the region defined by the inequalities

$$\phi(P/2) \le u_i \le \phi(P) \quad (1\le i\le 8) \quad \text{and} \quad u-\psi_1 \le u_1+\cdots+u_8 \le u-\psi_2, \tag{9.22}$$

where

$$\psi_1 = \max\{\psi(\sqrt{Q}),\psi(Q)\} \quad \text{and} \quad \psi_2 = \min\{\psi(\sqrt{Q}),\psi(Q)\}.$$

Thus it follows from Fourier's integral formula that $J(m) = \tilde{J}(m)$. We now fix P and Q by taking

$$50\phi(3P) = N \quad \text{and} \quad \psi(Q) = N$$

when the leading coefficient of ψ is positive, and by taking

$$\phi(P/2) = N \quad \text{and} \quad \psi(Q) = -20\phi(3P)$$

when the leading coefficient of ψ is negative. These equations determine P and Q uniquely, and plainly these choices for P and Q satisfy (2.3). Suppose that m is an integer satisfying

$$\tfrac{1}{2}N - 12\phi(3P) \le m \le N.$$

Then we have

$$m-\psi_1 \le 8\phi(P/2) \quad \text{and} \quad m-\psi_2 \ge 8\phi(P),$$

and so it follows from (9.20)-(9.22) that

$$\tilde{J}(m) = \int_{[\phi(P/2),\phi(P)]^8} (\Xi(m;\mathbf{u}))^{-1} d\mathbf{u} \gg (P^{-4})^8 Q^{1-k} (\phi(P) - \phi(P/2))^8.$$

Consequently,

$$J(m) \gg P^3 Q. \tag{9.23}$$

Suppose now that $N/2 < n \le N$. Then when $1 \le x_i, y_i \le P/3$ $(i = 1, 2)$ and $P < z_1, z_2 \le 2P$, it is apparent that

$$\tfrac{1}{2}N - 12\phi(3P) \le n - \Phi(x_1, y_1, z_1) - \Phi(x_2, y_2, z_2) \le N.$$

Then by Lemma 4.2(iii) together with (9.19) and (9.23), we have

$$\mathcal{U}(n) \gg P^3 Q \sum_{\substack{1 \le x_1, y_1 \le P/3 \\ 1 \le x_2, y_2 \le P/3}} \sum_{P < z_1, z_2 \le 2P} \mathfrak{S}(n - \Phi(x_1, y_1, z_1) - \Phi(x_2, y_2, z_2)),$$

whence by Lemma 8.1, whenever $n \in \mathcal{L} \cap [N/2, N]$ one has $\mathcal{U}(n) \gg P^9 Q$. On recalling (9.6), (9.7) and (9.18), therefore, we may conclude that when $n \in \mathcal{L} \cap [N/2, N]$ one has $\mathcal{R}(n) \gg P^9 Q$, and thus the proof of Theorem 2 is complete.

References

1. J. Brüdern, *On Waring's problem for fifth powers and some related topics*, Proc. London Math. Soc. (3) **61** (1990), 457–479.
2. T. Estermann, *Einige Sätze über quadratfrei Zahlen*, Math. Ann. **105** (1931), 653–662.
3. L.-K. Hua, *On a generalized Waring problem. II*, J. Chinese Math. Soc. **2** (1940), 175–191.
4. K. Kawada and T. D. Wooley, *Sums of fourth powers and related topics* (submitted).
5. W. M. Schmidt, *Equations over finite fields. An elementary approach. Lecture Notes in Mathematics*, vol. 536, Springer-Verlag, Berlin, 1976.
6. K. Thanigasalam, *Improvement on Davenport's iterative method and new results in additive number theory. III*, Acta Arith. **48** (1987), 97–116.
7. R. C. Vaughan, *On Waring's problem for smaller exponents*, Proc. London Math. Soc. (3) **52** (1986), 445–463.
8. R. C. Vaughan, *A new iterative method in Waring's Problem*, Acta Math. **162** (1989), 1–71.
9. R. C. Vaughan, *The Hardy–Littlewood Method, second edition*, Cambridge University Press, 1997.
10. R. C. Vaughan and T. D. Wooley, *Waring's problem: some refinements*, Proc. London Math. Soc. (3) **63** (1991), 35–68.
11. R. C. Vaughan and T. D. Wooley, *Further improvements in Waring's Problem*, Acta Math. **174** (1995), 147–240.
12. T. D. Wooley, *Large improvements in Waring's problem*, Ann. Math. **135** (1992), 131–164.
13. H. B. Yu, *On Waring's problem with polynomial summands*, Acta Arith. **76** (1996), 131–144.

Kawada: Department of Mathematics, Faculty of Education, Iwate University, Morioka, 020 JAPAN

E-mail address: `kawada@iwate-u.ac.jp`

Wooley: Department of Mathematics, University of Michigan, East Hall, 525 East University Avenue, Ann Arbor, MI 48109-1109, U.S.A.

Current address: Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544-1000, U.S.A.

E-mail address: `wooley@math.lsa.umich.edu, wooley@math.princeton.edu`