

## SLIM EXCEPTIONAL SETS FOR SUMS OF FOUR SQUARES

TREVOR D. WOOLEY

### 1. Introduction

The celebrated theorem of Lagrange, to the effect that all natural numbers are the sum of four squares of integers, remains to this day one of the brightest in the firmament of additive number theory. Problems in which the squares are restricted in various ways have provided an attractive menu of possible extensions of Lagrange's theorem. Perhaps the most tempting such problem asserts that all large integers congruent to 4 modulo 24 are the sum of four squares of prime numbers, the congruence condition arising naturally from the observation that when  $p$  is a prime number exceeding 3, one has  $p^2 \equiv 1 \pmod{24}$ . Although progress has been made in a number of related problems (a topic we discuss below), the best approximation at present to this Waring–Goldbach problem for four squares shows only that the desired conclusion holds almost always. Let  $E(N)$  denote the number of positive integers not exceeding  $N$  that are congruent to 4 modulo 24, yet cannot be written as the sum of four squares of prime numbers. Then a refinement by Schwarz [19] of an earlier conclusion of Hua [11] implies that for any positive number  $A$ , one has  $E(N) \ll N(\log N)^{-A}$ , thereby justifying our earlier assertion. Even the substantially sharper bound  $E(N) \ll N^{13/15+\varepsilon}$ , valid for each  $\varepsilon > 0$ , very recently established by J. Liu and M.-C. Liu [16], seems somewhat disappointing given that an exceptional set of size  $O(N(\log N)^{-A})$ , for any  $A > 0$ , had already been established by Schwarz [19] in the analogous problem involving only three squares of prime numbers. In this paper we seek to exploit effectively the ‘excess’ fourth square of a prime so as to improve substantially this most recent bound for  $E(N)$ . It transpires that the ideas underlying this progress permit estimates for exceptional sets in a variety of additive problems to be significantly slimmed whenever sufficiently many excess variables are available. We illustrate such ideas within this paper for sums of squares, deferring to a future occasion a more comprehensive investigation of accessible applications.

Our improved estimate for  $E(N)$ , which we describe in the following theorem, is established in §2 below.

**THEOREM 1.1.** *For each  $\varepsilon > 0$ , one has  $E(N) \ll N^{13/30+\varepsilon}$ .*

The bound recorded in Theorem 1.1 should be compared with the aforementioned estimate  $E(N) \ll N^{13/15+\varepsilon}$  due to Liu and Liu [16]. Various authors have considered alternative approximations to the conjecture that all large integers

---

Received 2 January 2001; revised 24 July 2001.

2000 *Mathematics Subject Classification* 11P32, 11P05, 11P55.

The author is a Packard Fellow, and supported in part by NSF grant DMS-9970440.

congruent to 4 modulo 24 may be written as the sum of four squares of prime numbers. Thus Hua [11] showed that all large integers congruent to 5 modulo 24 may be written as the sum of five squares of prime numbers, and Brüdern and Fouvry [2] have shown that this conjecture holds when almost-primes are substituted for the primes (here, the almost-primes may have as many as 34 prime factors). Meanwhile, Shields [20], Plaksin [17] and Kovalchik [15] have obtained an asymptotic formula for the number of representations of an integer as the sum of two squares of integers and two squares of prime numbers (see Greaves [7] for an earlier non-trivial lower bound for the number of such representations). Current technology apparently lacks the power to establish the validity of the expected asymptotic formula for the number of representations of an integer as the sum of a square of an integer, and three squares of prime numbers. We are able, however, to show that such an asymptotic formula holds almost always, with rather few possible exceptions.

In order to state the latter conclusion precisely, we require some notation. When  $n$  is a natural number, denote by  $R(n)$  the number of representations of  $n$  as the sum of a square of an integer and three squares of prime numbers. Also, let  $\mathfrak{S}(n)$  denote the associated singular series corresponding to  $n$ , which we define by

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^q (q^{-1}S(q, a))(\phi(q)^{-1}S^*(q, a))^3 e(-an/q), \quad (1.1)$$

where  $\phi(q)$  denotes Euler's totient function, we write

$$S(q, a) = \sum_{r=1}^q e(ar^2/q) \quad \text{and} \quad S^*(q, a) = \sum_{\substack{t=1 \\ (t,q)=1}}^q e(at^2/q), \quad (1.2)$$

and, as usual,  $e(z)$  denotes  $e^{2\pi iz}$ . We remark that  $\mathfrak{S}(n) = 0$  unless  $n \equiv 3, 4, 7, 12, 15$  or  $19$  modulo 24, in which case one has  $1 \ll \mathfrak{S}(n) \ll \log \log n$ . When  $\psi(t)$  is a function of a positive variable  $t$ , denote by  $E^*(N; \psi)$  the number of integers  $n$  with  $1 \leq n \leq N$  for which

$$|R(n) - \tfrac{1}{2}\pi^2 \mathfrak{S}(n)n(\log n)^{-3}| > n(\log n)^{-3}\psi(n)^{-1}. \quad (1.3)$$

**THEOREM 1.2.** *Suppose that  $\psi$  is a function of a positive variable  $t$ , increasing monotonically to infinity, and satisfying the condition that for some fixed number  $A$  with  $1 > A > 0$ , for large values of  $t$  one has  $\psi(t) = O((\log t)^A)$ . Then one has*

$$E^*(N; \psi) \ll \psi(N)^4 (\log N)^6.$$

As a final illustration of our methods we consider sums of squares of integers possessing only small prime divisors. Sárközy has conjectured that for each positive number  $\varepsilon$ , every sufficiently large natural number  $N$  is the sum of four squares of integers, the largest prime divisors of which are all smaller than  $N^\varepsilon$ . Harcos [9] has made some progress in the direction of this conjecture by establishing such a conclusion for almost all natural numbers  $N$ . Let  $P(n)$  denote the largest prime divisor of  $n$ , and write  $L(t) = \exp((\log t \log \log t)^{1/2})$ . Then Harcos established that for almost all integers  $m$  with  $1 \leq m \leq N$  and  $8 \nmid m$ , the equation  $n_1^2 + n_2^2 + n_3^2 + n_4^2 = m$  possesses a solution with  $P(n_1 n_2 n_3 n_4) < L(m)^{20}$ . Indeed,

Harcos shows that the number of possible exceptions is at most  $O(NL(N)^{-1/16})$ . By modestly weakening the smoothness parameter and applying the ideas underlying the proof of Theorem 1.1 above, we sharpen considerably the latter conclusion.

**THEOREM 1.3.** *Define  $\mathcal{E}(N; \beta)$  to be the number of positive integers  $m$  not exceeding  $N$  for which the equation*

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 = m$$

*fails to possess a solution with  $P(n_1 n_2 n_3 n_4) < m^\beta$ . Then for every sufficiently small positive number  $\eta$ , one has  $\mathcal{E}(N; \eta) \ll N^{1/2-\eta/1600}$ .*

In contrast to the conclusion of Harcos [9], we do not impose any conditions concerning divisibility by 8, for as we see in §4, such issues are essentially irrelevant to the estimation of the exceptional set. We note also that at the cost of greater effort, the smoothness parameter  $m^\eta$  implicit in the statement of Theorem 1.3 may be replaced by  $\exp(c \log m / \log \log m)$ , for a suitable positive constant  $c$ .

The principles underlying our approach to these exceptional set problems are clearly illustrated in our proof of Theorem 1.1 in §2 below. Roughly speaking, we replace the conventional argument, involving Bessel's inequality, with one in which the set of 'exceptions' appears explicitly within our application of the Hardy–Littlewood method. In this respect, our argument draws inspiration from recent work of Brüdern, Kawada and Wooley concerning exceptional sets in polynomial sequences (see, for example, [3, 4]). Equipped with sufficiently many excess variables (and with four squares one has one such variable), one may exploit one or more of these excess variables within a mean value incorporating an exponential sum over the exceptional set. Under favourable conditions, this mean value is dominated by the diagonal contribution, and thus one achieves square-root cancellation in the exponential sum over this squared variable. By comparison, in the traditional approach via Bessel's inequality, one makes use of these excess variables through available Weyl estimates. For exponential sums over squares of primes, for example, such estimates are far from achieving square-root cancellation. In this way one profits handsomely in the estimation of the associated exceptional set.

Throughout, the letter  $\varepsilon$  will denote a sufficiently small positive number. We use  $\ll$  and  $\gg$  to denote Vinogradov's well-known notation, implicit constants depending at most on  $\varepsilon$ , unless otherwise indicated. When  $\alpha$  is a real number, we write  $[\alpha]$  for the greatest integer not exceeding  $\alpha$ . Also, we denote the number of divisors of a positive integer  $n$  by  $d(n)$ . In an effort to simplify our analysis, we adopt the convention that whenever  $\varepsilon$  appears in a statement, then we are implicitly asserting that for each  $\varepsilon > 0$  the statement holds for sufficiently large values of the main parameter. Note that the 'value' of  $\varepsilon$  may consequently change from statement to statement, and hence also the dependence of implicit constants on  $\varepsilon$ .

## 2. Four squares of primes

Our proof of Theorem 1.1 is accomplished without serious technical discussion, but such concision demands recourse to the literature. We begin by recording some notation. Let  $\delta$  be a sufficiently small positive number, and let  $N$  be a

positive number sufficiently large in terms of  $\delta$ . Following the notation introduced by Liu and Liu in [16], we write

$$X = N^{1/2}, \quad P = N^{2/15-\delta} \quad \text{and} \quad Q = NP^{-1}(\log N)^{-14}. \quad (2.1)$$

We define the set of major arcs  $\mathfrak{M}$  as the union of the intervals

$$\mathfrak{M}(q, a) = \{\alpha \in [0, 1) : |q\alpha - a| \leq Q^{-1}\},$$

with  $0 \leq a \leq q \leq P$  and  $(a, q) = 1$ . We then denote the corresponding set of minor arcs by  $\mathfrak{m} = [0, 1) \setminus \mathfrak{M}$ . Finally, we define the weighted exponential sum  $g(\alpha)$  by

$$g(\alpha) = \sum_{p \leq X} (\log p) e(p^2 \alpha),$$

where here, and throughout, the letter  $p$  denotes a prime number.

LEMMA 2.1. *Whenever  $\frac{1}{2}N < n \leq N$  and  $n \equiv 4 \pmod{24}$ , one has*

$$\int_{\mathfrak{M}} g(\alpha)^4 e(-n\alpha) d\alpha \gg N.$$

*Proof.* The desired lower bound is an immediate consequence of Theorem 2 of Liu and Liu [16].

*The proof of Theorem 1.1.* Denote by  $\mathcal{Z}(N)$  the set of integers  $n$  with  $\frac{1}{2}N < n \leq N$  for which  $n \equiv 4 \pmod{24}$ , and yet the equation

$$p_1^2 + p_2^2 + p_3^2 + p_4^2 = n$$

has no solution in prime numbers  $p_1, \dots, p_4$ . Define the exponential sum

$$K(\alpha) = \sum_{n \in \mathcal{Z}(N)} e(n\alpha),$$

and, for the sake of convenience, write  $Z = \text{card}(\mathcal{Z}(N))$ . In view of the definition of  $\mathcal{Z}(N)$ , it is evident from orthogonality that

$$\int_0^1 g(\alpha)^4 K(-\alpha) d\alpha = \sum_{n \in \mathcal{Z}(N)} \int_0^1 g(\alpha)^4 e(-n\alpha) d\alpha = 0.$$

But by Lemma 2.1, one has

$$\int_{\mathfrak{M}} g(\alpha)^4 K(-\alpha) d\alpha = \sum_{n \in \mathcal{Z}(N)} \int_{\mathfrak{M}} g(\alpha)^4 e(-n\alpha) d\alpha \gg ZN,$$

and thus we deduce that

$$\left| \int_{\mathfrak{m}} g(\alpha)^4 K(-\alpha) d\alpha \right| \gg ZN. \quad (2.2)$$

We estimate the integral over the minor arcs in (2.2) by applying Schwarz's inequality. Thus we deduce that

$$\left| \int_{\mathfrak{m}} g(\alpha)^4 K(-\alpha) d\alpha \right| \leq \left( \sup_{\alpha \in \mathfrak{m}} |g(\alpha)| \right) I_1^{1/2} I_2^{1/2}, \quad (2.3)$$

where

$$I_1 = \int_0^1 |g(\alpha)K(\alpha)|^2 d\alpha \quad \text{and} \quad I_2 = \int_0^1 |g(\alpha)|^4 d\alpha.$$

The mean value  $I_1$  counts the number of solutions of the equation

$$p_1^2 - p_2^2 = n_1 - n_2,$$

with  $p_i \leq X$  ( $i = 1, 2$ ) and  $n_j \in \mathcal{Z}(N)$  ( $j = 1, 2$ ), where each solution is counted with weight  $(\log p_1)(\log p_2)$ . There are plainly  $O(ZX/\log X)$  solutions of this equation with  $n_1 = n_2$  and  $p_1^2 = p_2^2$ . Given any one of the  $O(Z^2)$  available choices of  $n_1$  and  $n_2$  with  $n_1 \neq n_2$ , on the other hand, one may apply an elementary estimate for the divisor function to show that there are  $O(X^\varepsilon)$  possible choices for  $p_1 - p_2$  and  $p_1 + p_2$ , whence also for  $p_1$  and  $p_2$ . Thus we conclude that

$$I_1 \ll (\log N)^2 (ZX/\log X + X^\varepsilon Z^2) \ll N^\varepsilon (ZX + Z^2). \quad (2.4)$$

By arguing similarly, or instead applying Hua's Lemma (see Lemma 2.5 of Vaughan [21]), one finds that

$$I_2 \ll (\log N)^4 X^{2+\varepsilon} \ll N^\varepsilon X^2. \quad (2.5)$$

Finally, we note that Theorem 2 of Ghosh [6] supplies the bound

$$\sup_{\alpha \in \mathfrak{M}} |g(\alpha)| \ll X^{1+\varepsilon} (P^{-1} + X^{-1/2} + QX^{-2})^{1/4} \ll X^{1+\varepsilon} P^{-1/4}. \quad (2.6)$$

On recalling (2.2) and substituting the estimates (2.4)–(2.6) into (2.3), we deduce from (2.1) that

$$\begin{aligned} ZN &\ll N^\varepsilon X P^{-1/4} (XZ + Z^2)^{1/2} (X^2)^{1/2} \\ &\ll ZN^{1+\varepsilon} P^{-1/4} + Z^{1/2} N^{5/4+\varepsilon} P^{-1/4}. \end{aligned} \quad (2.7)$$

But in view of the definition of  $P$  in (2.1), the first term on the right-hand side of (2.7) is of smaller order of magnitude than the left-hand side, and thus we may conclude that

$$Z \ll N^{1/2+\varepsilon} P^{-1/2} \ll N^{1/2-1/15+\delta}.$$

The consequent upper bound  $\text{card}(\mathcal{Z}(N)) \ll N^{13/30+\delta}$  leads to the conclusion of Theorem 1.1 on summing over dyadic intervals.

We remark that an argument almost identical to that establishing Theorem 1.1 provides an analogous conclusion for sums of three squares of primes and a  $k$ th power of a prime. In this instance, the associated exceptional set may be shown to be at most  $O(N^{1/2-c/(k2^k)})$ , where  $c$  is a suitable positive number. Combining the use of equation (2.6) of Bauer, Liu and Zhan [1] with modern estimates for trigonometric sums over prime numbers (see, for example, Lemma 3.3 of Kawada and Wooley [14]), one may show that any number  $c$  with  $c < \frac{9}{80}$  is permissible. Indeed, a more refined analysis shows that when  $k \geq 4$ , any number  $c$  with  $c < 1$  is permissible.

### 3. Three squares of primes and an integral square

Although the skeleton of our proof of Theorem 1.2 retains the key elements of the argument described in §2, we are forced by the precision claimed in the

statement of this theorem to indulge in a pruning process of medium difficulty. A full account of the technical details involved in such a treatment would occupy considerable space, and we therefore take the short cut of making use of recent work of Bauer, Liu and Zhan [1] concerning sums of three squares of prime numbers. We start by introducing some notation. Let  $\delta$  be a sufficiently small positive number, let  $E$  be a positive number sufficiently large in terms of  $A$ , and let  $N$  be a positive number sufficiently large in terms of  $\delta$  and  $E$ . Following the notation introduced by Bauer, Liu and Zhan in [1], we write

$$X = N^{1/2}, \quad P = N^{9/80-\delta} \quad \text{and} \quad Q = NP^{-1}(\log N)^{-E}.$$

We define the set of major arcs  $\mathfrak{N}$  to be the union of the intervals

$$\mathfrak{N}(q, a) = \{\alpha \in [0, 1) : |q\alpha - a| \leq Q^{-1}\},$$

with  $0 \leq a \leq q \leq P$  and  $(a, q) = 1$ . We then denote the corresponding set of minor arcs by  $\mathfrak{n} = [0, 1) \setminus \mathfrak{N}$ .

Before recording the estimate of Bauer, Liu and Zhan [1] of which we make use, we recall the exponential sum  $S^*(q, a)$  defined in (1.2), and define

$$\mathfrak{S}^*(n, P) = \sum_{1 \leq q \leq P} \sum_{\substack{a=1 \\ (a, q)=1}}^q \phi(q)^{-3} S^*(q, a)^3 e(-na/q). \quad (3.1)$$

Finally, we define the exponential sum

$$h(\alpha) = \sum_{M < p \leq X} (\log p) e(p^2 \alpha),$$

where we write  $M = X(\log N)^{-4E-4}$ .

LEMMA 3.1. *Whenever  $1 \leq n \leq N$ , one has*

$$\int_{\mathfrak{N}} h(\alpha)^3 e(-n\alpha) d\alpha = \frac{1}{4} \pi \mathfrak{S}^*(n, P) n^{1/2} + O((|\mathfrak{S}^*(n, P)| + 1) X (\log N)^{-2E}).$$

Furthermore, when  $-N \leq n < 0$  one has

$$\int_{\mathfrak{N}} h(\alpha)^3 e(-n\alpha) d\alpha \ll X (\log N)^{-2E}.$$

Finally, one has

$$\int_{\mathfrak{N}} h(\alpha)^3 d\alpha \ll PX.$$

*Proof.* Write

$$\tilde{h}(\alpha) = \sum_{M < m \leq X} \Lambda(m) e(m^2 \alpha),$$

where  $\Lambda(\cdot)$  denotes the well-known von Mangoldt function. Then one finds that for each non-zero integer  $n$  with  $|n| \leq N$ , the argument of Bauer, Liu and Zhan [1] leading to equation (2.6) of that paper is easily modified to yield the asymptotic relation

$$\int_{\mathfrak{N}} \tilde{h}(\alpha)^3 e(-n\alpha) d\alpha = \frac{1}{8} \mathfrak{S}^*(n, P) \mathfrak{J}(n) + O(X (\log N)^{-2E}), \quad (3.2)$$

where we write

$$\mathfrak{J}(n) = \sum_{\substack{m_1 + m_2 + m_3 = n \\ M^2 < m_i \leq N \ (i=1,2,3)}} (m_1 m_2 m_3)^{-1/2}.$$

Here we remark that the condition  $M^2 < m_i \leq N$  in the above replaces a corresponding condition that would read  $\frac{1}{12}N < m_i \leq N$  in [1]. This wider range for the  $m_i$  is, however, easily accommodated within the argument of [1]. Next, on employing Lemma 2.9 of Vaughan [21], for example, we find that when  $1 \leq n \leq N$  one has

$$\begin{aligned} \mathfrak{J}(n) &= \frac{\Gamma(\frac{1}{2})^3}{\Gamma(\frac{3}{2})} n^{1/2} + O(X(\log N)^{-2E}) \\ &= 2\pi n^{1/2} + O(X(\log N)^{-2E}). \end{aligned}$$

Thus we deduce that

$$\begin{aligned} \int_{\mathfrak{N}} \tilde{h}(\alpha)^3 e(-n\alpha) d\alpha &= \frac{1}{4} \pi \mathfrak{S}^*(n, P) n^{1/2} \\ &\quad + O((|\mathfrak{S}^*(n, P)| + 1) X(\log N)^{-2E}). \end{aligned} \quad (3.3)$$

Finally, on accounting for squares and higher powers of primes, one finds that

$$|\tilde{h}(\alpha) - h(\alpha)| \ll X^{1/2} \log X.$$

But the measure of  $\mathfrak{N}$  is  $O(P^2 N^{\varepsilon-1})$ , and thus the trivial estimate  $|\tilde{h}(\alpha)| \ll X$  leads to the relation

$$\begin{aligned} \int_{\mathfrak{N}} h(\alpha)^3 e(-n\alpha) d\alpha - \int_{\mathfrak{N}} \tilde{h}(\alpha)^3 e(-n\alpha) d\alpha &\ll (X^{5/2} \log X)(P^2 N^{\varepsilon-1}) \\ &\ll X^{19/20+2\varepsilon}. \end{aligned} \quad (3.4)$$

The conclusion of the lemma is now immediate from (3.3) for  $1 \leq n \leq N$ . When  $-N \leq n < 0$ , on the other hand, it is apparent from (3.2) that

$$\int_{\mathfrak{N}} \tilde{h}(\alpha)^3 e(-n\alpha) d\alpha \ll X(\log N)^{-2E},$$

and thus the desired conclusion again follows from (3.4). Finally, by applying Hua's lemma (see Lemma 2.5 of Vaughan [21]) in combination with Hölder's inequality, one finds that

$$\begin{aligned} \int_{\mathfrak{N}} h(\alpha)^3 d\alpha &\leq \left( \int_0^1 |h(\alpha)|^4 d\alpha \right)^{3/4} \left( \int_{\mathfrak{N}} d\alpha \right)^{1/4} \\ &\ll (X^{2+\varepsilon})^{3/4} (P^2 N^{\varepsilon-1})^{1/4} \ll PX. \end{aligned}$$

Before discussing the major arc contribution for sums of a square and three squares of prime numbers, we pause to analyse the singular series  $\mathfrak{S}^*(n, P)$ , and also the singular series  $\mathfrak{S}(n)$  defined in (1.1).

LEMMA 3.2. *Suppose that  $n$  is a natural number with  $\frac{1}{2}N < n \leq N$ . Then*

- (i) *the singular series  $\mathfrak{S}(n)$  defined in (1.1) is absolutely convergent, and one has  $0 \leq \mathfrak{S}(n) \ll \log \log n$ ; moreover, provided only that  $n \equiv 3, 4, 7, 12, 15$  or  $19$  modulo  $24$ , one has  $\mathfrak{S}(n) \gg 1$ ;*

(ii) *there is an absolute constant  $C$  with the property that*

$$\sum_{1 \leq m < \sqrt{n}} |\mathfrak{S}^*(n - m^2, P)| \ll X(\log N)^C.$$

*Proof.* We begin by discussing the conclusion of part (i). Write

$$A(q, n) = \sum_{\substack{a=1 \\ (a, q)=1}}^q (\phi(q)^{-1} S^*(q, a))^3 (q^{-1} S(q, a)) e(-na/q), \quad (3.5)$$

so that in view of (1.1), one has

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} A(q, n).$$

We observe that whenever  $(t, q) = 1$ , a change of variables readily establishes that

$$\begin{aligned} A(q, n) &= \sum_{\substack{a=1 \\ (a, q)=1}}^q (\phi(q)^{-1} S^*(q, at^2))^3 (q^{-1} S(q, at^2)) e(-nat^2/q) \\ &= \sum_{\substack{a=1 \\ (a, q)=1}}^q (\phi(q)^{-1} S^*(q, a))^3 (q^{-1} S(q, a)) e(-nat^2/q), \end{aligned}$$

whence

$$A(q, n) = q^{-1} \phi(q)^{-4} \sum_{\substack{a=1 \\ (a, q)=1}}^q S(q, a) S^*(q, a)^3 S^*(q, -na). \quad (3.6)$$

But when  $(b, q) = 1$ , the estimate  $S(q, b) \ll q^{1/2}$  follows from Theorem 4.2 of Vaughan [21], and the corresponding bound  $S^*(q, b) \ll q^{1/2+\varepsilon}$  follows from Lemma 1.3 of Hua [10]. Thus we deduce that for every positive number  $Y$  one has

$$\begin{aligned} \sum_{q > Y} |A(q, n)| &\ll \sum_{q=1}^{\infty} (q/Y)^{1/4} |A(q, n)| \ll Y^{-1/4} \sum_{q=1}^{\infty} q^{-7/6} (q, n)^{1/2} \\ &\leq Y^{-1/4} \sum_{d|n} \sum_{\substack{q=1 \\ d|q}}^{\infty} q^{-7/6} d^{1/2} \leq Y^{-1/4} \sum_{m=1}^{\infty} m^{-7/6} \sum_{d|n} d^{-2/3} \\ &\ll N^{\varepsilon} Y^{-1/4}. \end{aligned} \quad (3.7)$$

In particular, the singular series  $\mathfrak{S}(n)$  is absolutely convergent.

Next define  $\gamma = \gamma(p)$  by taking  $\gamma = 3$  when  $p = 2$ , and otherwise by taking  $\gamma = 1$ . Then it follows from Lemma 8.3 of Hua [12] that  $S^*(p^h, a) = 0$  when  $(p, a) = 1$  and  $h > \gamma(p)$ . Furthermore, the standard theory of exponential sums demonstrates that  $A(q, n)$  is a multiplicative function of  $q$  (see Lemma 8.1 of Hua [12] and § 2.6 of Vaughan [21]). But when  $(b, p) = 1$ , Lemma 4.3 of Vaughan [21] leads to the estimates  $|S(p, b)| = \sqrt{p}$  and  $|S^*(p, b)| \leq \sqrt{p} + 1$ . It therefore

follows from (3.6) that when  $p > 2$ ,

$$\sum_{h=0}^{\infty} A(p^h, n) = 1 + A(p, n) = 1 + O(np^{-3/2}),$$

whence the infinite product

$$\prod_p \left( \sum_{h=0}^{\infty} A(p^h, n) \right)$$

is absolutely convergent. Moreover, one also obtains the upper bound

$$\begin{aligned} \mathfrak{S}(n) &\ll (8, n) \prod_{p>2} (1 + A(p, n)) \\ &\ll \left( \prod_{\substack{p|n \\ p>2}} \left( 1 + \left( \frac{\sqrt{p}+1}{p-1} \right)^3 \sqrt{p} \right) \right) \left( \prod_{\substack{p \nmid n \\ p>2}} (1 + 21p^{-3/2}) \right) \\ &\ll \prod_{p|n} (1 + 1/p) \ll \log \log n. \end{aligned}$$

Furthermore, on noting that

$$\phi(p^\gamma)^3 \sum_{h=0}^{\gamma} A(p^h, n)$$

counts the number of solutions of the congruence

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv n \pmod{p^\gamma},$$

with  $1 \leq x_i \leq p^\gamma$  ( $1 \leq i \leq 4$ ) and  $(x_i, p) = 1$  ( $2 \leq i \leq 4$ ), it is evident that this expression is real and non-negative for each prime  $p$ , whence also  $\mathfrak{S}(n) \geq 0$ . Also, when  $n \equiv 3, 4, 7, 12, 15$  or  $19$  modulo  $24$ , it is easily verified that the above congruence possesses at least one solution of the required type for every prime  $p$ . Here one may proceed directly when  $p = 2$  or  $3$ , and for larger primes  $p$  one may appeal to the Cauchy–Davenport lemma (see, for example, Lemma 2.14 of Vaughan [21]). But for every reduced residue  $b$  modulo  $p$ , one has  $S(p, b) - S^*(p, b) = 1$  and  $S(p, -b) = \pm S(p, b)$ . On employing our earlier estimates, we therefore obtain

$$|S^*(p, b)^3 S(p, b) - |S(p, b)|^4| \leq 7(\sqrt{p} + 1)^3.$$

Then we may proceed as above to deduce that for a sufficiently large but fixed positive number  $p_0$ , one has

$$\begin{aligned} \mathfrak{S}(n) &\gg \left( \prod_{\substack{p|n \\ p>p_0}} (1 + p^{-1}(p-1)^{-2}(p^2 - 7(\sqrt{p}+1)^3)) \right) \left( \prod_{\substack{p \nmid n \\ p>p_0}} (1 - 21p^{-3/2}) \right) \\ &\gg \prod_{p|n} (1 + 1/p) \gg 1. \end{aligned}$$

This completes the proof of part (i) of the lemma.

For the proof of part (ii), we initially proceed as in part (i) to deduce that

$$\mathfrak{S}^*(n, P) = \sum_{1 \leq q \leq P} B(q, n),$$

where

$$\begin{aligned} B(q, n) &= \sum_{\substack{a=1 \\ (a, q)=1}}^q (\phi(q)^{-1} S^*(q, a))^3 e(-na/q) \\ &= \phi(q)^{-4} \sum_{\substack{a=1 \\ (a, q)=1}}^q S^*(q, a)^3 S^*(q, -na). \end{aligned}$$

Thus, just as in part (i), we deduce that

$$\begin{aligned} |\mathfrak{S}^*(n, P)| &\ll \left( \prod_{\substack{2 < p \leq P \\ p|n}} \left( 1 + \left( \frac{\sqrt{p}+1}{p-1} \right)^3 p \right) \right) \left( \prod_{\substack{2 < p \leq P \\ p \nmid n}} \left( 1 + \left( \frac{\sqrt{p}+1}{p-1} \right)^4 p \right) \right) \\ &\ll \left( \prod_{p|n} (1 + p^{-1/2}) \right) \left( \prod_{p \leq P} (1 + p^{-1}) \right) \ll d(n) \log P. \end{aligned}$$

But then it follows from van der Corput's lemma (see, for example, Theorem 3 of Hua [12]) that

$$\sum_{1 \leq m < \sqrt{n}} |\mathfrak{S}^*(n - m^2, P)| \ll (\log N) \sum_{1 \leq m < \sqrt{n}} d(n - m^2) \ll \sqrt{n} (\log N)^C,$$

where  $C$  is an absolute constant. The conclusion of part (ii) of the lemma is now immediate.

In order to make further progress we must equip ourselves with the additional exponential sum

$$f(\alpha) = \sum_{m \leq X} e(m^2 \alpha).$$

LEMMA 3.3. *Suppose that  $n$  is an integer with  $\frac{1}{2}N < n \leq N$ . Then one has*

$$\int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha = \frac{1}{16} \pi^2 \mathfrak{S}(n) n + O(N(\log N)^{-E}).$$

*Proof.* We begin by transforming the integral in question into one more closely resembling that in the statement of Lemma 3.1. We observe that

$$\int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha = \sum_{1 \leq m \leq X} \int_{\mathfrak{N}} h(\alpha)^3 e(-(n - m^2)\alpha) d\alpha.$$

Then it follows from Lemma 3.1 that whenever  $\frac{1}{2}N < n \leq N$ , one has

$$\int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha = R_1 + O(R_2), \quad (3.8)$$

where

$$R_1 = \frac{1}{4} \pi \sum_{1 \leq m < \sqrt{n}} \mathfrak{S}^*(n - m^2, P) (n - m^2)^{1/2}$$

and

$$R_2 = \sum_{1 \leq m < \sqrt{n}} (|\mathfrak{S}^*(n - m^2, P)| + 1) X(\log N)^{-2E}.$$

We first dispose of the contribution of  $R_2$  within (3.8), noting that as a consequence of Lemma 3.2(ii), there is an absolute constant  $C$  with the property that

$$R_2 \ll (X(\log N)^C)(X(\log N)^{-2E}).$$

Thus, provided that  $E$  is chosen sufficiently large, as we may assume, it follows that

$$R_2 \ll N(\log N)^{-E}. \quad (3.9)$$

Next we deal with  $R_1$ . On splitting the sum over  $m$  into arithmetic progressions modulo  $q$ , and recalling the definition (3.1), one finds that

$$\begin{aligned} \sum_{1 \leq m < \sqrt{n}} \mathfrak{S}^*(n - m^2, P)(n - m^2)^{1/2} \\ = \sum_{1 \leq q \leq P} \sum_{\substack{a=1 \\ (a,q)=1}}^q \phi(q)^{-3} S^*(q, a)^3 e(-na/q) U(q, a; n), \end{aligned} \quad (3.10)$$

where

$$U(q, a; n) = \sum_{r=1}^q \sum_{0 \leq u < (\sqrt{n}-r)/q} e(a(qu+r)^2/q) (n - (qu+r)^2)^{1/2}.$$

But on considering lattice points in an associated ellipse, one may apply an elementary counting argument to establish that

$$\sum_{0 \leq u < (\sqrt{n}-r)/q} (n - (qu+r)^2)^{1/2} = \frac{1}{4} \pi (n/q + O(n^{1/2})),$$

whence, on recalling (1.2), one finds that

$$U(q, a; n) = \frac{1}{4} \pi q^{-1} S(q, a) n + O(qn^{1/2}).$$

On substituting into (3.10) and recalling (3.5), one deduces that

$$\sum_{1 \leq m < \sqrt{n}} \mathfrak{S}^*(n - m^2, P)(n - m^2)^{1/2} = \frac{1}{4} \pi n \sum_{1 \leq q \leq P} A(q, n) + O(n^{1/2} P^3). \quad (3.11)$$

In order to complete the singular series implicit in (3.11), we recall (3.7), and deduce that

$$\sum_{q > P} A(q, n) \ll N^\varepsilon P^{-1/4}.$$

We therefore conclude from (3.8), (3.9) and (3.11) that whenever  $\frac{1}{2}N < n \leq N$ , one has

$$\int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha = \frac{1}{16} \pi^2 n (\mathfrak{S}(n) + O(N^\varepsilon P^{-1/4})) + O(N(\log N)^{-E}).$$

The conclusion of the lemma now follows immediately.

Our final preparation for the proof of Theorem 1.2 involves a sieve upper bound associated with the number of representations of an integer as a sum of four squares of primes.

LEMMA 3.4. *When  $k$  is a non-zero integer with  $|k| \leq N$ , one has*

$$\int_0^1 |h(\alpha)|^4 e(-k\alpha) d\alpha \ll X^2.$$

*Proof.* By orthogonality, one has

$$\int_0^1 |h(\alpha)|^4 e(-k\alpha) d\alpha \leq (\log X)^4 r(k),$$

where  $r(k)$  denotes the number of solutions of the equation

$$p_1^2 + p_2^2 - p_3^2 - p_4^2 = k,$$

with  $p_i \leq X$ . Let  $\mathcal{B}$  denote the sequence of integers

$$\mathcal{B} = \{x_1 x_2 x_3 x_4 \in \mathbb{N} : 1 \leq x_i \leq X \ (1 \leq i \leq 4) \text{ and } x_1^2 + x_2^2 - x_3^2 - x_4^2 = k\},$$

and write

$$S(\mathcal{B}, z) = \sum_{\substack{n \in \mathcal{B} \\ p|n \Rightarrow p > z}} 1.$$

We apply the technology of Brüdern and Fouvry [2] to engineer a four-dimensional sieve, and thereby demonstrate that for a suitable positive number  $\delta$ , with  $0 < \delta < \frac{1}{2}$ , one has

$$S(\mathcal{B}, X^\delta) \ll_\delta X^2 (\log X)^{-4}.$$

Since  $S(\mathcal{B}, X^\delta)$  plainly provides an upper bound for  $r(k)$ , the desired conclusion will follow immediately.

In order to justify our claimed bound on  $S(\mathcal{B}, X^\delta)$ , we observe that the argument on p. 81 of Brüdern and Fouvry [2] applies, with simple modifications, to the present situation. On p. 212 of Halberstam and Richert [8], one finds a sieving limit 9.32 for dimension 4, and thus the analogue of Lemma 9 of Brüdern and Fouvry [2] relevant to the current problem, combined with the upper bound for  $S(\mathcal{B}, z)$  provided by Theorem 1 of Iwaniec [13], demonstrates that

$$S(\mathcal{B}, X^\delta) \ll X^2 (\log X)^{-4} + X^{2-\varepsilon}.$$

This establishes our earlier claim, and hence also the conclusion of the lemma.

We may now launch our campaign against the proof of Theorem 1.2. Let  $R_0(n)$  denote the number of representations of  $n$  in the form

$$n = x^2 + p_1^2 + p_2^2 + p_3^2, \tag{3.12}$$

with  $x \in \mathbb{N}$ , with  $p_i$  ( $i = 1, 2, 3$ ) prime numbers exceeding  $M$ , and with each solution counted with weight  $(\log p_1)(\log p_2)(\log p_3)$ . Then by orthogonality, whenever  $\frac{1}{2}N < n \leq N$  one has

$$R_0(n) = \int_0^1 f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha. \tag{3.13}$$

Consider a fixed function  $\psi(t)$  of the type described in the statement of Theorem 1.2, and define  $\mathcal{Z}(N)$  to be the set of integers  $n$  with  $\frac{1}{2}N < n \leq N$  for which the inequality

$$|R_0(n) - \frac{1}{16}\pi^2 \mathfrak{S}(n)n| > \frac{1}{10}n\psi(n)^{-1} \quad (3.14)$$

holds. We aim to show that  $\text{card}(\mathcal{Z}(N)) \ll \psi(N)^4 (\log N)^5$ , whence the conclusion of Theorem 1.2 follows with little additional effort.

By virtue of Lemma 3.3, we find that for  $n \in \mathcal{Z}(N)$ , one has

$$\left| R_0(n) - \int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha \right| > \frac{1}{30}N\psi(N)^{-1} + O(N(\log N)^{-E}),$$

whence by (3.13),

$$\left| \int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha \right| > \frac{1}{60}N\psi(N)^{-1}. \quad (3.15)$$

Define the complex numbers  $\eta_n$  by taking  $\eta_n = 0$  for  $n \notin \mathcal{Z}(N)$ , and when  $n \in \mathcal{Z}(N)$  by means of the equation

$$\left| \int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha \right| = \eta_n \int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha.$$

In view of (3.15), one obtains

$$\begin{aligned} N\psi(N)^{-1} \text{card}(\mathcal{Z}(N)) &\ll \sum_{N/2 < n \leq N} \eta_n \int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 e(-n\alpha) d\alpha \\ &= \int_{\mathfrak{N}} f(\alpha) h(\alpha)^3 K(-\alpha) d\alpha, \end{aligned} \quad (3.16)$$

where we write

$$K(\alpha) = \sum_{N/2 < n \leq N} \eta_n e(n\alpha). \quad (3.17)$$

Observe next that by Dirichlet's theorem on Diophantine approximation, the set  $[0, 1)$  is contained in the union of the intervals

$$\mathfrak{P}(q, a) = \{\alpha \in [0, 1): |q\alpha - a| \leq X^{-1}\}$$

with  $0 \leq a \leq q \leq X$  and  $(a, q) = 1$ . As a special case of Theorem 1 of Vaughan [22], whenever  $a \in \mathbb{Z}$ ,  $q \in \mathbb{N}$  and  $\beta = \alpha - a/q$ , one has

$$|f(\alpha)| \ll |q^{-1}S(q, a)v(\beta)| + (qX^2|\beta|)^{1/2} + q^{1/2} \log(2q),$$

where  $S(q, a)$  is defined as in (1.2) and  $v(\beta) = \int_0^X e(\beta t^2) dt$ . Define the function  $\Delta(\alpha)$  for  $\alpha \in [0, 1)$  by taking

$$\Delta(\alpha) = \min\{(q + N|q\alpha - a|)^{-1}\},$$

where the minimum is taken over the values of  $a \in \mathbb{Z}$  and  $q \in \mathbb{N}$  with  $0 \leq a \leq q \leq X$ ,  $(a, q) = 1$  and  $|q\alpha - a| \leq X^{-1}$ . Then on applying Theorem 4.2 of Vaughan [21] together with the estimate

$$v(\beta) \ll X(1 + X^2|\beta|)^{-1/2}$$

that is immediate from partial integration, one finds that whenever  $0 \leq a \leq q \leq X$ ,

$(a, q) = 1$  and  $\alpha \in \mathfrak{P}(q, a)$ , one has

$$|f(\alpha)| \ll X(q + X^2|q\alpha - a|)^{-1/2} + X^{1/2} + q^{1/2} \log(2q).$$

Consequently, one has the estimate

$$|f(\alpha)| \ll X\Delta(\alpha)^{1/2} + X^{1/2} \log X$$

uniformly for  $\alpha \in [0, 1)$ . On substituting this estimate into (3.16), we therefore obtain

$$N\psi(N)^{-1}Z \ll I_1 + I_2, \quad (3.18)$$

where we write  $Z = \text{card}(\mathcal{Z}(N))$ ,

$$I_1 = X^{1/2}(\log N) \int_0^1 |h(\alpha)^3 K(\alpha)| d\alpha \quad (3.19)$$

and

$$I_2 = X \int_{\mathfrak{n}} \Delta(\alpha)^{1/2} |h(\alpha)^3 K(\alpha)| d\alpha. \quad (3.20)$$

Next, on applying Schwarz's inequality to (3.19), one deduces that

$$I_1 \leq X^{1/2}(\log N) I_3^{1/2} I_4^{1/2}, \quad (3.21)$$

where

$$I_3 = \int_0^1 |h(\alpha)|^4 d\alpha \quad \text{and} \quad I_4 = \int_0^1 |h(\alpha) K(\alpha)|^2 d\alpha.$$

But as a consequence of Rieger [18, Satz 3], one has

$$I_3 \ll X^2(\log X)^2 \quad (3.22)$$

(see, for example, Liu and Liu [16, equation (6.10)]). Also, as in the argument leading to the estimate (2.4) above, one finds that

$$I_4 \ll (\log N)^2 (ZX / \log X + X^\varepsilon Z^2). \quad (3.23)$$

On substituting (3.22) and (3.23) into (3.21), we conclude that

$$I_1 \ll N(\log N)^{5/2} Z^{1/2} + N^{3/4+\varepsilon} Z. \quad (3.24)$$

We estimate  $I_2$  through the medium of Hölder's inequality, obtaining from (3.20) the upper bound

$$I_2 \leq I_3^{1/2} I_5^{1/4} I_6^{1/4}, \quad (3.25)$$

where

$$I_5 = \int_0^1 |h(\alpha)^4 K(\alpha)^2| d\alpha \quad \text{and} \quad I_6 = X^4 \int_{\mathfrak{n}} \Delta(\alpha)^2 |K(\alpha)|^2 d\alpha.$$

Here we note immediately that on making use of (3.22) for the diagonal contribution in  $I_5$ , and employing Lemma 3.4 for the corresponding off-diagonal contribution, one obtains

$$\begin{aligned} I_5 &\leq Z \int_0^1 |h(\alpha)|^4 d\alpha + \sum_{\substack{k_1, k_2 \in \mathcal{Z}(N) \\ k_1 \neq k_2}} \int_0^1 |h(\alpha)|^4 e((k_1 - k_2)\alpha) d\alpha \\ &\ll ZX^2(\log X)^2 + Z^2 X^2. \end{aligned} \quad (3.26)$$

On recalling the definitions of  $\mathfrak{n}$  and  $\Delta(\alpha)$ , meanwhile, one finds that

$$I_6 \ll X^4(T_1 + T_2), \quad (3.27)$$

where

$$T_1 = \sum_{P < q \leq X} \sum_{\substack{a=1 \\ (a,q)=1}}^q \int_{-\infty}^{\infty} \frac{|K(\beta + a/q)|^2}{(q + qN|\beta|)^2} d\beta$$

and

$$T_2 = \sum_{1 \leq q \leq P} \sum_{\substack{a=1 \\ (a,q)=1}}^q \int_{|\beta| > (qQ)^{-1}} \frac{|K(\beta + a/q)|^2}{(q + qN|\beta|)^2} d\beta.$$

Let  $c_q(m)$  be Ramanujan's sum, which we define by

$$c_q(m) = \sum_{\substack{a=1 \\ (a,q)=1}}^q e(am/q).$$

Then it follows that

$$\sum_{\substack{a=1 \\ (a,q)=1}}^q |K(\beta + a/q)|^2 = \sum_{n_1, n_2 \in \mathcal{Z}(N)} \eta_{n_1} \bar{\eta}_{n_2} c_q(n_1 - n_2) e(\beta(n_1 - n_2)).$$

The familiar estimate  $|c_q(m)| \leq (q, m)$  (note the convention that  $(q, 0) = q$ ) therefore leads to the estimates

$$T_1 \ll N^{-1} \sum_{P < q \leq X} q^{-2} \sum_{n_1, n_2 \in \mathcal{Z}(N)} (q, n_1 - n_2)$$

and

$$T_2 \ll QN^{-2} \sum_{1 \leq q \leq P} q^{-1} \sum_{n_1, n_2 \in \mathcal{Z}(N)} (q, n_1 - n_2).$$

On isolating the diagonal contribution, we deduce that

$$T_1 \ll N^{-1} Z \sum_{P < q \leq X} q^{-1} + N^{-1} \sum_{\substack{n_1, n_2 \in \mathcal{Z}(N) \\ n_1 \neq n_2}} \sum_{d | (n_1 - n_2)} \sum_{\substack{P < q \leq X \\ d | q}} dq^{-2}.$$

But on making an elementary divisor function estimate, one finds that when  $m \neq 0$  one has

$$\sum_{d | m} \sum_{\substack{P < q \leq X \\ d | q}} dq^{-2} \leq P^{-1} \sum_{d | m} \sum_{P/d < t \leq X/d} t^{-1} \ll m^\varepsilon P^{-1} \log X.$$

Thus we conclude that

$$T_1 \ll ZN^{-1} \log X + P^{-1} N^{\varepsilon-1} Z^2, \quad (3.28)$$

and by a similar argument,

$$\begin{aligned} T_2 &\ll QN^{-2} Z \sum_{1 \leq q \leq P} 1 + QN^{-2} \sum_{\substack{n_1, n_2 \in \mathcal{Z}(N) \\ n_1 \neq n_2}} \sum_{d | (n_1 - n_2)} \sum_{\substack{1 \leq q \leq P \\ d | q}} dq^{-1} \\ &\ll ZPQN^{-2} + QN^{\varepsilon-2} Z^2 \ll ZN^{-1} + P^{-1} N^{\varepsilon-1} Z^2. \end{aligned} \quad (3.29)$$

On substituting (3.28) and (3.29) into (3.27), recalling (3.22) and (3.26), and incorporating these estimates into (3.25), we arrive at the upper bound

$$\begin{aligned} I_2 &\ll (X^2(\log X)^2)^{1/2}(ZX^2(\log X)^2 + Z^2X^2)^{1/4} \\ &\quad \times (ZN(\log X) + Z^2P^{-1}N^{1+\varepsilon})^{1/4} \\ &\ll Z^{1/2}N(\log N)^{7/4} + Z^{3/4}N(\log N)^{5/4} + ZN^{1+\varepsilon}P^{-1/4}. \end{aligned}$$

In view of (3.18) and (3.24), therefore, one has

$$N\psi(N)^{-1}Z \ll Z^{1/2}N(\log N)^{5/2} + Z^{3/4}N(\log N)^{5/4} + ZN^{1+\varepsilon}P^{-1/4}.$$

We thus conclude that  $\text{card}(\mathcal{Z}(N)) \ll \psi(N)^4(\log N)^5$ , as desired. In order to complete the proof of Theorem 1.2, it remains now only to remove the logarithmic weights, complete the intervals containing the primes, and sum the contributions from a set of dyadic intervals covering  $[1, N]$ .

In order to remove the weights, note that when  $M < p \leq X$ , one has  $\log p = \log X + O(\log \log N)$ . Thus, whenever  $\frac{1}{2}N < n \leq N$ , each solution of (3.12) counted by (3.13) appears with weight  $\frac{1}{8}(\log n)^3 + O((\log n)^{2+\varepsilon})$ . Let  $R^*(n)$  denote the number of representations of  $n$  in the form (3.12) with  $x \in \mathbb{N}$ , and with  $p_i$  ( $i = 1, 2, 3$ ) prime numbers exceeding  $M$ . Then from (3.14) and the definition of  $\mathcal{Z}(N)$ , it follows that the inequality

$$|R^*(n) - \frac{1}{2}\pi^2 \mathfrak{S}(n)n(\log n)^{-3}| > \frac{5}{6}n(\log n)^{-3}\psi(n)^{-1}$$

holds for at most  $O(\psi(N)^4(\log N)^5)$  of the integers  $n$  with  $\frac{1}{2}N < n \leq N$ .

We finish by showing that the contribution to  $R(n)$  arising from prime variables  $p_i$ , with  $p_i \leq M$  for  $i = 1, 2$  or  $3$ , is negligible compared to  $R^*(n)$ . In order to see this, note that the total number of such solutions is bounded above by

$$3 \int_0^1 |f(\alpha)b(\alpha)B(\alpha)^2| d\alpha,$$

where we write

$$b(\alpha) = \sum_{p \leq M} e(p^2\alpha) \quad \text{and} \quad B(\alpha) = \sum_{p \leq X} e(p^2\alpha).$$

But in view of Rieger [18, Satz 3], one has

$$\int_0^1 |b(\alpha)|^4 d\alpha \ll M^2(\log M)^{-2} \quad \text{and} \quad \int_0^1 |B(\alpha)|^4 d\alpha \ll X^2(\log X)^{-2},$$

and moreover a classical estimate yields

$$\int_0^1 |f(\alpha)|^4 d\alpha \ll X^2 \log X.$$

Then an application of Hölder's inequality yields the bound

$$\begin{aligned}
& \int_0^1 |f(\alpha)b(\alpha)B(\alpha)^2| d\alpha \\
& \leq \left( \int_0^1 |f(\alpha)|^4 d\alpha \right)^{1/4} \left( \int_0^1 |b(\alpha)|^4 d\alpha \right)^{1/4} \left( \int_0^1 |B(\alpha)|^4 d\alpha \right)^{1/2} \\
& \ll (X^2 \log X)^{1/4} (M^2 (\log M)^{-2})^{1/4} (X^2 (\log X)^{-2})^{1/2} \\
& \ll X^{3/2} M^{1/2} (\log N)^{-5/4} \ll N (\log N)^{-2E}.
\end{aligned}$$

Whenever  $\psi(N) = O((\log N)^E)$ , therefore, the contribution of these small primes is negligible compared to  $N(\log N)^{-3}\psi(N)^{-1}$ . It follows that the lower bound (1.3) holds for at most  $O(\psi(N)^4(\log N)^5)$  of the integers  $n$  with  $\frac{1}{2}N < n \leq N$ . On summing over dyadic intervals, we conclude that (1.3) holds for at most  $O(\psi(N)^4(\log N)^6)$  of the integers  $n$  with  $1 \leq n \leq N$ , and this completes the proof of Theorem 1.2.

#### 4. Four smooth squares

The key features of our method, so far as it applies to sums of squares, are already evident from the discussion of §§ 2 and 3, and so we will be as brief as possible in our proof of Theorem 1.3. It is expedient to make use of the treatment provided by Harcos in [9], although this weighted version of the circle method is not the most direct approach (see Brüdern and Wooley [5] for an alternative weightless argument). We begin by introducing some notation in the spirit of Harcos [9], and we note here that the notation of previous sections is now discarded. Let  $\eta$  be a sufficiently small positive number, and let  $N$  be a positive number sufficiently large in terms of  $\eta$ . We define  $w = N^{\eta/56}$ ,  $y = w^{27}$  and  $z = y^{8/27} = w^8$ . Let

$$X = N^{1/2}, \quad Q = Nz^{-1/4}, \quad U = [4N/y] + 1,$$

and

$$\mathcal{L} = \{l \in \mathbb{N}: \frac{9}{10}Xy^{-1} \leq l \leq Xy^{-1} \text{ and } p \mid l \Rightarrow z < p \leq y\}.$$

After introducing the weights

$$d_n = \sum_{\substack{ml=n \\ m \leq y \\ l \in \mathcal{L}}} 1,$$

for  $1 \leq n \leq X$ , we define

$$f(\alpha) = \sum_{1 \leq n \leq X} d_n e(n^2 \alpha), \quad u(\alpha) = U^{-1} \sum_{n=0}^{U-1} e(n\alpha),$$

and

$$h(\alpha) = f(\alpha)u(\alpha) = \sum_{n=1}^{N+U-1} h_n e(n\alpha),$$

where

$$h_n = U^{-1} \sum_{n-U < j^2 \leq n} d_j.$$

A weighted lower bound for the number of representations of a natural number  $M$  as the sum of four squares of integers, all of whose prime divisors are at most  $y$ , is provided by

$$J(M) = \int_0^1 f(\alpha)^4 e(-M\alpha) d\alpha. \quad (4.1)$$

Harcos [9] estimates  $J(M)$  on average by comparing this integral with

$$I(M) = \int_0^1 h(\alpha)^4 e(-M\alpha) d\alpha. \quad (4.2)$$

We require a Hardy–Littlewood dissection, and this we define as follows. We take  $\mathfrak{M}$  to be the union of the intervals

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

with  $0 \leq a \leq q \leq z$  and  $(a, q) = 1$ , and write  $\mathfrak{m} = [0, 1) \setminus \mathfrak{M}$ . We extract from the discussion of Harcos [9] a consequence of the major arc treatment relevant to our deliberations here.

**LEMMA 4.1.** *Suppose that  $M$  is an integer with  $\frac{1}{2}N < M \leq N$ , such that  $8 \nmid M$  and  $J(M) = 0$ . Then one has*

$$\left| \int_{\mathfrak{m}} f(\alpha)^4 e(-M\alpha) d\alpha \right| + \left| \int_{\mathfrak{m}} h(\alpha)^4 e(-M\alpha) d\alpha \right| \gg Nw^{-4/27-\varepsilon}.$$

*Proof.* We note that our definitions of  $w$  and  $z$  differ from those of Harcos [9], but that the increased sizes of  $w$ ,  $z$  and  $y$  do not invalidate the accompanying analysis (indeed, much of the analysis would become somewhat easier to execute in detail). The lower bound

$$I(M) \geq Nw^{-4/27-\varepsilon} \quad (4.3)$$

follows from the argument of Harcos [9] leading to [9, equation (4)]. Also, on examining the argument of [9] leading to equation (3) of that paper, one finds that

$$\left| \int_{\mathfrak{M}} f(\alpha)^4 e(-M\alpha) d\alpha - \int_{\mathfrak{M}} h(\alpha)^4 e(-M\alpha) d\alpha \right| \ll Nz^{-1/4}w^\varepsilon. \quad (4.4)$$

Furthermore, our hypothesis that  $J(M) = 0$  leads from (4.1) to the conclusion that

$$\int_{\mathfrak{M}} f(\alpha)^4 e(-M\alpha) d\alpha = - \int_{\mathfrak{m}} f(\alpha)^4 e(-M\alpha) d\alpha. \quad (4.5)$$

On combining (4.2) and (4.5), we deduce that

$$\begin{aligned} I(M) - \int_{\mathfrak{M}} h(\alpha)^4 e(-M\alpha) d\alpha + \int_{\mathfrak{M}} f(\alpha)^4 e(-M\alpha) d\alpha \\ = \int_{\mathfrak{m}} h(\alpha)^4 e(-M\alpha) d\alpha - \int_{\mathfrak{m}} f(\alpha)^4 e(-M\alpha) d\alpha, \end{aligned}$$

whence by applying the triangle inequality in combination with (4.3) and (4.4), we deduce that

$$\left| \int_{\mathfrak{m}} h(\alpha)^4 e(-M\alpha) d\alpha - \int_{\mathfrak{m}} f(\alpha)^4 e(-M\alpha) d\alpha \right| \geq Nw^{-4/27-\varepsilon} + O(Nz^{-1/4}w^\varepsilon).$$

The conclusion of the lemma follows immediately by means of a second application of the triangle inequality.

*The proof of Theorem 1.3.* Let  $\mathcal{Z}_1(N)$  denote the set of integers  $M$  with  $\frac{1}{2}N < M \leq N$  satisfying  $8 \nmid M$ , with  $J(M) = 0$ , and such that

$$\left| \int_{\mathfrak{m}} f(\alpha)^4 e(-M\alpha) d\alpha \right| \geq \left| \int_{\mathfrak{m}} h(\alpha)^4 e(-M\alpha) d\alpha \right|. \quad (4.6)$$

Also, let  $\mathcal{Z}_2(N)$  denote the corresponding set of integers  $M$  in which the inequality (4.6) is reversed. We aim to show that  $\text{card}(\mathcal{Z}_i(N)) \ll N^{1/2}w^{-1/28}$  ( $i = 1, 2$ ), whence by summing over dyadic intervals it follows that there are  $O(N^{1/2}w^{-1/28})$  integers  $M$  with  $1 \leq M \leq N$  and  $8 \nmid M$  which fail to admit a representation as the sum of four integral squares, all of whose prime divisors are at most  $M^\eta$ . If  $M$  is an integer with  $8 \mid M$ , and one has  $M = x_1^2 + x_2^2 + x_3^2 + x_4^2$ , then necessarily  $2 \mid x_i$  ( $1 \leq i \leq 4$ ). Thus  $M$  fails to admit a representation of the desired type precisely when  $\frac{1}{4}M$  fails to admit such a representation. Either  $8 \nmid \frac{1}{4}M$ , or else we may again extract a factor of 4 from  $\frac{1}{4}M$ . In this way, one finds that the integers divisible by 8 contribute a set of exceptions of the shape  $4^j\xi$ , with  $\xi$  an exceptional integer with  $8 \nmid \xi$ . Since each such  $\xi$  contributes at most  $\log N$  exceptional integers not exceeding  $N$ , the conclusion of Theorem 1.3 follows from our claimed bounds on  $\text{card}(\mathcal{Z}_i(N))$ .

The argument required to treat  $\mathcal{Z}_2(N)$  is essentially the same as that for  $\mathcal{Z}_1(N)$ , so we discuss here only the treatment associated with the latter. On recalling Lemma 4.1, it follows from (4.6) that whenever  $M \in \mathcal{Z}_1(N)$ , one has

$$\left| \int_{\mathfrak{m}} f(\alpha)^4 e(-M\alpha) d\alpha \right| \gg Nw^{-4/27-\varepsilon}. \quad (4.7)$$

Define the complex numbers  $\eta_M$  by taking  $\eta_M = 0$  for  $M \notin \mathcal{Z}_1(N)$ , and when  $M \in \mathcal{Z}_1(N)$  by means of the equation

$$\left| \int_{\mathfrak{m}} f(\alpha)^4 e(-M\alpha) d\alpha \right| = \eta_M \int_{\mathfrak{m}} f(\alpha)^4 e(-M\alpha) d\alpha.$$

In view of (4.7), one obtains

$$\begin{aligned} Nw^{-4/27-\varepsilon} \text{card}(\mathcal{Z}_1(N)) &\ll \sum_{N/2 < M \leq N} \eta_M \int_{\mathfrak{m}} f(\alpha)^4 e(-M\alpha) d\alpha \\ &= \int_{\mathfrak{m}} f(\alpha)^4 K(-\alpha) d\alpha, \end{aligned} \quad (4.8)$$

where  $K(\alpha)$  is defined as in (3.17).

Next, applying Schwarz's inequality to (4.8), we find that

$$Nw^{-4/27-\varepsilon} \text{card}(\mathcal{Z}_1(N)) \ll \left( \sup_{\alpha \in \mathfrak{m}} |f(\alpha)| \right) J_1^{1/2} J_2^{1/2}, \quad (4.9)$$

where

$$J_1 = \int_0^1 |f(\alpha)|^4 d\alpha \quad \text{and} \quad J_2 = \int_0^1 |f(\alpha)K(\alpha)|^2 d\alpha.$$

On the one hand, it follows as in Lemma 5 of Harcos [9] that  $J_1 \ll Nw^\varepsilon$ . Meanwhile, on considering the underlying diophantine equation, we see that  $J_2$  is bounded above by the number of solutions of the equation  $x_1^2 - x_2^2 = M_1 - M_2$ , with  $M_i \in \mathcal{Z}_1(N)$  ( $i = 1, 2$ ),  $1 \leq x_j \leq X$  ( $j = 1, 2$ ), and with each solution counted with a weight bounded above, as in Lemma 1 of Harcos [9], by  $w^\varepsilon$ . Consequently, on writing  $Z = \text{card}(\mathcal{Z}_1(N))$ , we find just as in the argument leading to (2.4) above that

$$J_2 \ll w^\varepsilon (XZ + Z^2).$$

On substituting these estimates into (4.9), and adding the upper bound

$$\sup_{\alpha \in \mathfrak{m}} |f(\alpha)| \ll Xz^{-1/48} w^\varepsilon,$$

immediate from Lemma 4 of Harcos [9], we find that

$$Nw^{-4/27-\varepsilon}Z \ll w^\varepsilon N^{1/2}Xz^{-1/48}(XZ + Z^2)^{1/2}.$$

Thus we obtain

$$Z \ll z^{-1/48} w^{4/27+\varepsilon} N^{1/4} Z^{1/2} + z^{-1/48} w^{4/27+\varepsilon} Z,$$

so that in view of the relative sizes of  $z$  and  $w$ , it follows that

$$\text{card}(\mathcal{Z}_1(N)) \ll N^{1/2} w^{-1/28}.$$

On recalling our earlier comments, it is apparent that the proof of Theorem 1.3 is now complete.

### References

1. C. BAUER, M.-C. LIU and T. ZHAN, ‘On a sum of three prime squares’, *J. Number Theory* 85 (2000) 336–359.
2. J. BRÜDERN and É. FOUVRY, ‘Lagrange’s four squares theorem with almost prime variables’, *J. Reine Angew. Math.* 454 (1994) 59–96.
3. J. BRÜDERN, K. KAWADA and T. D. WOOLEY, ‘Additive representation in thin sequences, I: Waring’s problem for cubes’, *Ann. Sci. École Norm. Sup.* (4) 34 (2001) 471–501.
4. J. BRÜDERN, K. KAWADA and T. D. WOOLEY, ‘Additive representation in thin sequences, III: asymptotic formulae’, *Acta Arith.* 100 (2001) 267–289.
5. J. BRÜDERN and T. D. WOOLEY, ‘On Waring’s problem for cubes and smooth Weyl sums’, *Proc. London Math. Soc.* (3) 82 (2001) 89–109.
6. A. GHOSH, ‘The distribution of  $\alpha p^2$  modulo 1’, *Proc. London Math. Soc.* (3) 42 (1981) 252–269.
7. G. GREAVES, ‘On the representation of a number in the form  $x^2 + y^2 + p^2 + q^2$  where  $p$  and  $q$  are odd primes’, *Acta Arith.* 29 (1976) 257–274.
8. H. HALBERSTAM and H. E. RICHERT, *Sieve methods* (Academic Press, London, 1974).
9. G. HARCOS, ‘On sums of four smooth squares’, *J. Number Theory* 77 (1999) 145–154.
10. L.-K. HUA, ‘On the representation of numbers as the sums of the powers of primes’, *Math. Z.* 44 (1938) 335–346.
11. L.-K. HUA, ‘Some results in the additive prime number theory’, *Quart. J. Math. Oxford* 9 (1938) 68–80.
12. L.-K. HUA, *Additive theory of prime numbers* (American Mathematical Society, Providence, RI, 1965).
13. H. IWANIEC, ‘Rosser’s sieve’, *Acta Arith.* 36 (1980) 171–202.
14. K. KAWADA and T. D. WOOLEY, ‘On the Waring–Goldbach problem for fourth and fifth powers’, *Proc. London Math. Soc.* (3) 83 (2001) 1–50.

15. F. B. KOVALCHIK, 'Analogues of the Hardy–Littlewood equation', *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov* 116 (1982) 86–95.
16. J. LIU and M.-C. LIU, 'The exceptional set in the four prime squares problem', *Illinois J. Math.* 44 (2000) 272–293.
17. V. A. PLAKSIN, 'Asymptotic formula for the number of solutions of an equation with primes', *Izv. Akad. Nauk SSSR Ser. Mat.* 45 (1981) 321–397.
18. G. J. RIEGER, 'Über die Summe aus einem Quadrat und einem Primzahlquadrat', *J. Reine Angew. Math.* 231 (1968) 89–100.
19. W. SCHWARZ, 'Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen II: Darstellungen für "fast alle" Zahlen', *J. Reine Angew. Math.* 206 (1961) 78–112.
20. P. SHIELDS, 'Some applications of sieve methods in number theory', Thesis, University of Wales, 1979.
21. R. C. VAUGHAN, *The Hardy–Littlewood method*, 2nd edn (Cambridge University Press, 1997).
22. R. C. VAUGHAN, 'On generating functions in additive number theory, I', Preprint, Pennsylvania State University, 2001.

*Trevor D. Wooley*  
*Department of Mathematics*  
*University of Michigan*  
*East Hall*  
*525 East University Avenue*  
*Ann Arbor*  
*Michigan 48109-1109*  
*USA*  
[wooley@math.lsa.umich.edu](mailto:wooley@math.lsa.umich.edu)