

ON SUMS OF FOUR SQUARES OF PRIMES

ANGEL KUMCHEV AND LILU ZHAO

ABSTRACT. Let $E(N)$ denote the number of positive integers $n \leq N$, with $n \equiv 4 \pmod{24}$, which cannot be represented as the sum of four squares of primes. We establish that $E(N) \ll N^{11/32}$, thus improving on an earlier result of Harman and the first author, where the exponent $7/20$ appears in place of $11/32$.

1. INTRODUCTION

Let

$$\mathcal{A} = \{n \in \mathbb{N} : n \equiv 4 \pmod{24}\}.$$

It is conjectured that every sufficiently large integer $n \in \mathcal{A}$ can be represented as the sum of four squares of primes. Since this conjecture appears to lie beyond the reach of present methods, several approximations to it have been studied. One of those recasts the question in terms of the set of possible exceptions. Let \mathcal{E} denote the set of $n \in \mathcal{A}$ that have no representations as the sum of four squares of primes. Hua [8] was the first to prove that this exceptional set is “thin.” Write $E(N)$ for the cardinality of $\mathcal{E} \cap [1, N]$. Hua showed that

$$E(N) \ll N(\log N)^{-A} \tag{1.1}$$

for some absolute constant $A > 0$. Later, Schwarz [16] refined Hua’s result and showed that the power of the logarithm in (1.1) can be chosen arbitrarily large.

A couple of breakthroughs occurred at the cusp between the last and current centuries. First, Liu and Zhan [14] discovered a new technique for dealing with the major arcs in the application of the circle method. That was followed closely by a clever observation of Wooley [18] that greatly improved some minor arc estimates. Those ideas led to a series of improvements on (1.1) (see [11, 12, 13, 18]), culminating in the result of Liu, Wooley and Yu [13] that

$$E(N) \ll N^{3/8+\epsilon} \tag{1.2}$$

for any fixed $\epsilon > 0$. Subsequently, Harman and the first author [6, 7] adapted Harman’s alternative sieve method [2, 3, 5] to further improve (1.2). In particular, they proved [7] the sharpest bound for $E(N)$ to date:

$$E(N) \ll N^{7/20+\epsilon} \tag{1.3}$$

for any fixed $\epsilon > 0$. The purpose of this paper is to improve on (1.3) by establishing the following result.

Theorem 1.1. *One has*

$$E(N) \ll N^{11/32}. \tag{1.4}$$

2010 *Mathematics Subject Classification.* 11P32.

Key words and phrases. Circle method, sieve method.

L. Zhao is supported by the National Natural Science Foundation of China (Grant No. 11401154).

The improvement in our theorem has two sources. First, we simplify significantly the treatment of the major arcs in the application of the circle method. That removes a barrier to the sieve method that was artificially imposed in [7] to avoid certain technical difficulties on the major arcs. By itself, this idea allows us to “squeeze” a little more out of the sieve method in [7] and to reduce the exponent $7/20$ in (1.3) to approximately 0.347 . Our second innovation is a new bound for a triple exponential sum, Lemma 3.2 below, which allows us to strengthen some of the sieve estimates in [7]. The stronger sieve is responsible for the further reduction of the exponent in (1.4) to $11/32$. We remark that, in contrast to earlier work, the exponent $11/32$ in (1.4) is only a convenient approximation to the best possible exponent. In fact, in order to have an ϵ -free bound, we establish a slightly stronger result with exponent $11/32 - 10^{-4} + \epsilon$, whereas the actual limit of the method is the exponent $11/32 - \eta + \epsilon$ for some $\eta \approx 3.6 \times 10^{-4}$.

The history of the above problem is intertwined with that of the companion question about sums of three squares of primes, and results often come in pairs. Indeed, in [6, 7], Harman and the first author obtained simultaneously bounds for $E(N)$ and for the related quantity $E_3(N)$, which counts the integers $n \leq N$, with $n \equiv 3 \pmod{24}$ and $5 \nmid n$, that cannot be expressed as a sum of three squares of primes. Based on such history and on “conventional wisdom” about the circle method, the informed reader may expect that, together with (1.4), we should be able to establish also the bound

$$E_3(N) \ll N^{27/32}.$$

That, however, is not the case. It is true that our minor arc estimates can be adapted for the proof of such a result, but our treatment of the major arcs relies on the presence of four variables in the problem and does not extend to the ternary problem. Thus, in that problem, we still face the same artificial barrier as in the first author’s work with Harman.

Notation. Throughout the paper, the letter ϵ denotes a sufficiently small positive real number. Any statement in which ϵ occurs holds for each fixed $\epsilon > 0$, and any implied constant in such a statement is allowed to depend on ϵ . The letter p , with or without subscripts, is reserved for prime numbers; c denotes an absolute constant, not necessarily the same in all occurrences. As usual in number theory, $\mu(n)$, $\phi(n)$ and $\tau(n)$ denote, respectively, the Möbius function, the Euler totient function and the number of divisors function. Also, if $n \in \mathbb{N}$ and $z \geq 2$, we define

$$\psi(n, z) = \begin{cases} 1 & \text{if } n \text{ is divisible by no prime } p < z, \\ 0 & \text{otherwise.} \end{cases} \quad (1.5)$$

It is also convenient to extend the function $\psi(n, z)$ to all real $n \geq 1$ by setting $\psi(n, z) = 0$ for $n \notin \mathbb{Z}$. We write $e(x) = \exp(2\pi i x)$, $e_q(x) = e(x/q)$, and $(a, b) = \gcd(a, b)$, and we use $m \sim M$ as an abbreviation for the condition $M < m \leq 2M$.

2. OUTLINE OF THE PROOF

The theorem will follow by a standard dyadic argument, if we show that

$$|\mathcal{E} \cap (N/2, N]| \ll N^{11/32} \quad (2.1)$$

for all sufficiently large N . Thus, we fix a large N and define

$$P = \frac{2}{3}N^{1/2}, \quad L = \log P, \quad \mathcal{I} = [P/2, P].$$

We shall construct functions ρ_j , $1 \leq j \leq 3$, such that

$$\psi(m, P^{1/2})\psi(k, P^{1/2}) \geq \rho_1(m)\psi(k, P^{1/2}) - \rho_3(m)\rho_2(k), \quad (2.2)$$

where $\psi(m, z)$ is defined by (1.5). Note that for integers $m \in \mathcal{I}$, m is prime if and only if $\psi(m, P^{1/2}) = 1$. Therefore, when $n \in \mathcal{A} \cap (N/2, N]$, (2.2) yields

$$\sum_{\substack{p_1^2+p_2^2+p_3^2+p_4^2=n \\ p_j \in \mathcal{I}}} 1 \geq S_1 - S_2, \quad (2.3)$$

where

$$S_1 = \sum_{\substack{m_1^2+p_2^2+p_3^2+p_4^2=n \\ m_1, p_2, p_3, p_4 \in \mathcal{I}}} \rho_1(m_1),$$

$$S_2 = \sum_{\substack{m_1^2+m_2^2+p_3^2+p_4^2=n \\ m_1, m_2, p_3, p_4 \in \mathcal{I}}} \rho_3(m_1)\rho_2(m_2).$$

We study S_1 and S_2 by the circle method.

Let ρ_0 denote the characteristic function of the set of primes. For $0 \leq j \leq 3$, we define

$$f_j(\alpha) = \sum_{m \in \mathcal{I}} \rho_j(m) e(m^2 \alpha). \quad (2.4)$$

By orthogonality,

$$\sum_{\substack{m_1^2+m_2^2+p_3^2+p_4^2=n \\ m_1, m_2, p_3, p_4 \in \mathcal{I}}} \rho_j(m_1)\rho_k(m_2) = \int_0^1 f_j(\alpha) f_k(\alpha) f_0(\alpha)^2 e(-n\alpha) d\alpha. \quad (2.5)$$

The evaluation of the integral on the right side of (2.5) uses that the sieve weights ρ_j , $1 \leq j \leq 3$, have properties that are somewhat similar to the properties of the indicator function of the primes. In particular, our construction in §4 will yield functions ρ_j with the following three properties:

- (i) If $m \in \mathcal{I}$, one has $\rho_j(m) = 0$ unless $\psi(m, P^{0.06}) = 1$.
- (ii) Let $A, B > 0$ be fixed. For any non-principal Dirichlet character χ modulo $q \leq L^B$ and for any $u, v \in \mathcal{I}$, one has

$$\sum_{u < m \leq v} \rho_j(m) \chi(m) \ll PL^{-A}.$$

- (iii) Let $A > 0$ be fixed. There exist smooth functions ϱ_j and constants C_j such that, for any $u, v \in \mathcal{I}$, one has

$$\begin{aligned} \sum_{u < m \leq v} \rho_j(m) &= \sum_{u < m \leq v} \varrho_j(m) + O(PL^{-A}) \\ &= C_j(v - u)L^{-1} + O(PL^{-2}). \end{aligned}$$

We remark that these properties are well-known in the case $j = 0$ (the indicator function of the primes): (ii) is then a form of the Siegel–Walfisz theorem, whereas (iii) with $C_0 = 1$ and $\rho_0(m) = (\log m)^{-1}$ is the Prime Number Theorem with a rather weak error term.

For $1 \leq Q \leq P$, we introduce the collection of major arcs

$$\mathfrak{M}(Q) = \bigcup_{q \leq Q} \bigcup_{\substack{a=1 \\ (a,q)=1}}^q \left[\frac{a}{q} - \frac{Q}{qP^2}, \frac{a}{q} + \frac{Q}{qP^2} \right]. \quad (2.6)$$

To apply the circle method to the right side of (2.5), we dissect the unit interval into sets of major and minor arcs, defined as

$$\mathfrak{M} = \mathfrak{M}(P^{0.01}) \quad \text{and} \quad \mathfrak{m} = [P^{-1.99}, 1 + P^{-1.99}] \setminus \mathfrak{M}. \quad (2.7)$$

We remark that this choice of major and minor arcs differs from those made by earlier authors, who required significantly larger sets of major arcs (e.g., the major arcs in [7] are given by $\mathfrak{M} = \mathfrak{M}(P^{0.3-\epsilon})$). The modest size of our set of major arcs allows us to use standard techniques from [6, 11] to estimate the contribution of \mathfrak{M} to the right side of (2.5). In §5.1, we show that if ρ_j and ρ_k satisfy hypotheses (i)–(iii) above, plus another technical hypothesis, then

$$\int_{\mathfrak{M}} f_j(\alpha) f_k(\alpha) f_0(\alpha)^2 e(-n\alpha) d\alpha = (C_j C_k + o(1)) \mathfrak{S}(n) \mathfrak{I}(n/N) NL^{-4}. \quad (2.8)$$

Here, $\mathfrak{S}(n)$ and $\mathfrak{I}(t)$ are, respectively, the singular series and the singular integral of the problem, defined by

$$\begin{aligned} \mathfrak{S}(n) &= \sum_{q=1}^{\infty} \frac{1}{\phi^4(q)} \sum_{\substack{a=1 \\ (a,q)=1}}^q \left(\sum_{\substack{r=1 \\ (r,q)=1}}^q e_q(ar^2) \right)^4 e_q(-an), \\ \mathfrak{I}(t) &= \int_{-\infty}^{\infty} \left(\int_{1/3}^{2/3} e(x^2\gamma) dx \right)^4 e(-t\gamma) d\gamma. \end{aligned}$$

To estimate the contribution from the minor arcs, we employ an auxiliary decomposition of the unit interval:

$$\mathfrak{N} = \mathfrak{M}(P^{2/3}), \quad \mathfrak{n} = [P^{-4/3}, 1 + P^{-4/3}] \setminus \mathfrak{N}.$$

Suppose that the sieve weights are constructed so that the constants C_j in (iii) above satisfy

$$C_1 - C_3 C_2 > 0, \quad (2.9)$$

and that for some σ , $3/20 < \sigma < 1/6$, we have

$$\sup_{\alpha \in \mathfrak{n}} |f_j(\alpha)| \ll P^{1-\sigma+\epsilon} \quad (j = 1, 2). \quad (2.10)$$

In §5.2, we show that (2.5)–(2.10) yield the bound

$$S_1 - S_2 \gg NL^{-4}$$

for all but $O(N^{1/2-\sigma+\epsilon})$ values of $n \in \mathcal{A} \cap (N/2, N]$. To complete the proof of the theorem, we show in §5.2 that the sieve construction in §4 yields weights that satisfy both (2.9) and (2.10) with $\sigma = 5/32 + 10^{-4}$.

3. EXPONENTIAL SUM ESTIMATES

In this section, we collect the exponential sum estimates needed on the minor arcs. In particular, we establish a new estimate for certain triple sums—Lemma 3.2 below—that is likely to find applications beyond the proof of our main result. In all results, the set \mathfrak{m}_σ is the set of minor arcs defined by

$$\mathfrak{m}_\sigma = [QX^{-2}, 1 + QX^{-2}] \setminus \mathfrak{M}(Q), \quad Q = X^{4\sigma}.$$

In particular, our lemmas apply to any α that appears on the left side of (2.10).

Lemma 3.1. *Let $0 < \sigma < 1/6$, $\alpha \in \mathfrak{m}_\sigma$, and let ξ_r be complex numbers with $|\xi_r| \ll r^\epsilon$. Then*

$$\sum_{r \sim R} \sum_{rm \sim X} \xi_r e(\alpha r^2 m^2) \ll X^{1-\sigma+\epsilon},$$

provided that $R \ll X^{1-3\sigma}$.

Proof. This bound is established by Harman [4]. In particular, as a part of its proof, Harman shows that if $\alpha \in \mathfrak{m}_\sigma$ and $U \leq X^{2\sigma} \leq R \leq X^{1-3\sigma}$, then

$$\#\{(r, u) \in \mathbb{Z}^2 : r \sim R, u \sim U, \|\alpha r u^2\| < R^2 X^{2\sigma-2}\} \ll RU^{1/2} X^{-\sigma+\epsilon}. \quad (3.1)$$

□

Lemma 3.2. *Let $0 < \sigma < 1/6$, $\alpha \in \mathfrak{m}_\sigma$, and let $\xi_{r,s}$ be complex numbers with $|\xi_{r,s}| \ll (rs)^\epsilon$. Then*

$$\Sigma = \sum_{r \sim R} \sum_{s \sim S} \sum_{rsm \sim X} \xi_{r,s} e(\alpha r^2 s^2 m^2) \ll X^{1-\sigma+\epsilon},$$

provided that $R \ll X^{1-3\sigma}$ and $RS^2 \leq 0.1X^{1-2\sigma}$.

Proof. We may assume that $RS \geq X^{1-3\sigma}$, for otherwise the result follows from Lemma 3.1. Note that together with the hypothesis $RS^2 \ll X^{1-2\sigma}$, this assumption yields $S \ll X^\sigma$ and $R \gg X^{1-4\sigma} \gg X^{2\sigma}$. When $RS \ll X^{1-2\sigma}$, standard estimates for the inner sum (Lemma 2.4 and Theorem 4.1 in [17]) yield

$$\Sigma \ll \sum_{(r,s) \in \mathcal{S}} \frac{u^{-1/2} X^{1+\epsilon} / (RS)}{1 + (X/RS)^2 |\alpha r^2 s^2 - b/u|} + X^{1-\sigma+\epsilon},$$

where \mathcal{S} denotes the set of pairs $(r, s) \in \mathbb{Z}^2$ with $r \sim R$, $s \sim S$, for which there exist integers b, u with

$$1 \leq u \leq X^{2\sigma}, \quad (b, u) = 1, \quad |\alpha u r^2 s^2 - b| < (RS)^2 X^{2\sigma-2}. \quad (3.2)$$

Suppose that $(r, s) \in \mathcal{S}$. By Dirichlet's theorem on Diophantine approximations, there exist integers b_1, u_1 such that

$$1 \leq u_1 \leq 10S^2 X^{2\sigma}, \quad (b_1, u_1) = 1, \quad |\alpha u_1 r^2 - b_1| < 0.1S^{-2} X^{-2\sigma}. \quad (3.3)$$

Combining (3.2), (3.3) and the hypothesis $RS^2 \leq 0.1X^{1-2\sigma}$, we get

$$|b_1 u s^2 - b u_1| < 0.1u(2S)^2 S^{-2} X^{-2\sigma} + 10S^2 X^{2\sigma} (RS)^2 X^{2\sigma-2} \leq 0.5,$$

whence

$$\frac{b}{u} = \frac{b_1 s^2}{u_1}, \quad u = \frac{u_1}{(u_1, s^2)}.$$

Thus,

$$\begin{aligned} \Sigma &\ll \sum_{r \sim R} \frac{u_1^{-1/2} X^{1+\epsilon} / (RS)}{1 + (X/R)^2 |\alpha r_1^2 - b_1/u_1|} \sum_{s \sim S} (u_1, s^2)^{1/2} + X^{1-\sigma+\epsilon} \\ &\ll \sum_{r \sim R} \frac{u_1^{-1/2} X^{1+\epsilon} / R}{1 + (X/R)^2 |\alpha r_1^2 - b_1/u_1|} + X^{1-\sigma+\epsilon}, \end{aligned}$$

on using standard divisor estimates (see Lemma 2.3 in [10]). If either $u_1 \geq X^{2\sigma}$ or $|\alpha u_1 r^2 - b_1| \geq R^2 X^{2\sigma-2}$ this yields the desired bound. Otherwise, we have

$$\Sigma \ll X^{1+\epsilon} U^{-1/2} R^{-1} |\mathcal{R}| + X^{1-\sigma+\epsilon},$$

where \mathcal{R} is the set of integers $r \sim R$ for which there exists an integer $u_1 \sim U$, $1 \leq U \leq X^{2\sigma}$, such that $\|\alpha u_1 r^2\| < R^2 X^{2\sigma-2}$. Recalling that $X^{2\sigma} \ll R \ll X^{1-3\sigma}$, we see that the desired bound then follows from (3.1). \square

Lemma 3.3. *Let $0 < \sigma < 1/6$, $\alpha \in \mathfrak{m}_\sigma$, and let ξ_r, η_s be complex numbers with $|\xi_r| \ll r^\epsilon$, $|\eta_s| \ll s^\epsilon$. Then*

$$\sum_{r \sim R} \sum_{rs \sim X} \xi_r \eta_s e(\alpha r^2 s^2) \ll X^{1-\sigma+\epsilon},$$

provided that $X^{2\sigma} \ll R \ll X^{1-4\sigma}$.

This is a classical bound due to Ghosh [1].

Lemma 3.4. *Let $0 < \sigma < 1/6$, $\alpha \in \mathfrak{m}_\sigma$, and let ξ_r, η_s be complex numbers with $|\xi_r| \ll r^\epsilon$, $|\eta_s| \ll s^\epsilon$. Then*

$$\Sigma = \sum_{r \sim R} \sum_{s \sim S} \sum_{rsm \sim X} \xi_r \eta_s \psi(m, z) e(\alpha r^2 s^2 m^2) \ll X^{1-\sigma+\epsilon},$$

provided that $R \leq X^{2\sigma}$, $S \leq X^{2\sigma}$, $RS \ll X^{1-3\sigma}$, and $z \leq X^{1-6\sigma}$.

Proof. Let $\Pi = \prod_{p < z} p$. We have

$$\Sigma = \sum_{r \sim R} \sum_{s \sim S} \sum_{d | \Pi} \sum_{drsm \sim X} \xi_r \eta_s \mu(d) e(\alpha r^2 s^2 m^2 d^2),$$

where μ is the Möbius function. We break Σ into several subsums depending on the relative sizes of d, R, S .

Case 1: $dRS \leq X^{1-3\sigma}$. The corresponding terms of Σ form a Type I sum that can be estimated using Lemma 3.1.

Case 2: $dRS > X^{4\sigma}$, or $dR > X^{2\sigma}$, or $dS > X^{2\sigma}$. Then we can use the argument in Harman [5, Theorem 3.1] to split the corresponding terms of Σ into $\ll (\log X)^2$ subsums of Type II that can be estimated using Lemma 3.3. For example, when $R \leq X^{2\sigma} < dR$ and $d | \Pi$, d can be factored as $d = d_1 d_2$ so that $X^{2\sigma} \ll d_1 R \ll X^{1-4\sigma}$.

Case 3: $dR \leq X^{2\sigma}$, $dS \leq X^{2\sigma}$, $X^{1-3\sigma} < dRS \leq X^{4\sigma}$. Then Σ can be split into $\ll \log N$ sums of the form in Lemma 3.2 with $(r, s) = (rs, d)$. Indeed, we have

$$RS \ll X^{1-3\sigma}, \quad RSd^2 \leq (dR)(dS) \leq X^{4\sigma} \leq 0.1X^{1-2\sigma}. \quad \square$$

4. SIEVE CONSTRUCTION

In this section, we present our sieve construction, which has a lot in common with the one used in [7] by Harman and the first author. We construct arithmetic functions g_1, g_2, b_1, b_2, b_3 such that

$$\psi(m, P^{1/2}) = g_1(m) - b_1(m) + b_2(m), \quad (4.1)$$

$$\psi(m, P^{1/2}) = g_2(m) - b_3(m), \quad (4.2)$$

where $b_i(m) \geq 0$ and we can apply Lemmas 3.3 and 3.4 to estimate the exponential sums $\sum_m g_i(m) e(\alpha m^2)$. Our decompositions are based on Buchstab's identity

$$\psi(m, z_1) = \psi(m, z_2) - \sum_{z_2 \leq p < z_1} \psi(m/p, p) \quad (2 \leq z_2 < z_1). \quad (4.3)$$

For $3/20 < \sigma < 1/6$, put

$$z = P^{1-6\sigma}, \quad V = P^{2\sigma}, \quad W = P^{1-4\sigma}, \quad Y = P^{1-3\sigma}.$$

The reader will recognize these quantities as the various limits on the sizes of the summation variables in the exponential sum bounds from §3. We treat σ as a numerical parameter to be chosen later in the proof of our theorem; its value will eventually be set to $\sigma = 5/32 + 10^{-4}$.

We first describe the identity (4.1). By (4.3),

$$\begin{aligned} \psi(m, P^{1/2}) &= \psi(m, z) - \left\{ \sum_{z \leq p < V} + \sum_{V \leq p \leq W} + \sum_{W < p < P^{1/2}} \right\} \psi(m/p, p) \\ &= \psi_1(m) - \psi_2(m) - \psi_3(m) - \psi_4(m), \quad \text{say.} \end{aligned} \quad (4.4)$$

In this decomposition, ψ_1 and ψ_3 will contribute to g_1 and ψ_4 will be a part of b_1 ; we decompose ψ_2 further. Another application of Buchstab's identity gives

$$\begin{aligned}\psi_2(m) &= \sum_{z \leq p_1 < V} \left\{ \psi(m/p_1, z) - \sum_{z \leq p_2 < p_1 < V} \psi(m/(p_1 p_2), p_2) \right\} \\ &= \psi_5(m) - \psi_6(m), \quad \text{say.}\end{aligned}\tag{4.5}$$

We now write

$$\psi_6(m) = \psi_7(m) + \cdots + \psi_{10}(m),\tag{4.6}$$

where ψ_i is the part of ψ_6 subject to the following extra conditions on the product pq :

- $\psi_7(m)$: $p_1 p_2 < V$;
- $\psi_8(m)$: $V \leq p_1 p_2 \leq W$;
- $\psi_9(m)$: $W < p_1 p_2 \leq Y$;
- $\psi_{10}(m)$: $p_1 p_2 > Y$.

In our final decomposition, ψ_5 and ψ_8 contribute to g_1 and ψ_{10} contributes to b_2 ; we give further decompositions of ψ_7 and ψ_9 .

We apply (4.3) twice more to ψ_7 :

$$\begin{aligned}\psi_7(m) &= \sum_{p_1, p_2} \left\{ \psi(m/(p_1 p_2), z) - \sum_{z \leq p_3 < p_2} \psi(m/(p_1 p_2 p_3), z) \right. \\ &\quad \left. + \sum_{z \leq p_4 < p_3 < p_2} \psi(m/(p_1 p_2 p_3 p_4), p_4) \right\} \\ &= \psi_{11}(m) - \psi_{12}(m) + \psi_{13}(m), \quad \text{say.}\end{aligned}\tag{4.7}$$

We next apply Buchstab's identity to ψ_9 and obtain

$$\begin{aligned}\psi_9(m) &= \sum_{p_1, p_2} \left\{ \psi(m/(p_1 p_2), z) \right. \\ &\quad \left. - \sum_{z \leq p_3 < p_2} \left(\sum_{p_1 p_2 p_3 \leq Y} + \sum_{p_1 p_2 p_3 > Y} \right) \psi(m/(p_1 p_2 p_3), p_3) \right\} \\ &= \psi_{14}(m) - \psi_{15}(m) - \psi_{16}(m), \quad \text{say.}\end{aligned}\tag{4.8}$$

Note that the summation conditions in ψ_{15} imply $p_2 p_3 \leq P^{2/3-2\sigma} \leq W$. Thus, a final application of (4.3) yields

$$\begin{aligned}\psi_{15}(m) &= \sum_{p_1, p_2, p_3} \left\{ \sum_{p_2 p_3 \geq V} + \sum_{p_2 p_3 < V} \right\} \psi(m/(p_1 p_2 p_3), p_3) \\ &= \psi_{17}(m) + \sum_{\substack{p_1, p_2, p_3 \\ p_2 p_3 < V}} \left\{ \psi(m/(p_1 p_2 p_3), z) - \sum_{z \leq p_4 < p_3} \psi(m/(p_1 \cdots p_4), p_4) \right\} \\ &= \psi_{17}(m) + \psi_{18}(m) - \psi_{19}(m), \quad \text{say.}\end{aligned}\tag{4.9}$$

Finally, we split ψ_{13} , ψ_{16} , and ψ_{19} into "good" and "bad" parts, which we denote ψ_j^g and ψ_j^b , respectively. We collect in ψ_j^g the terms in ψ_j in which a subproduct of $p_1 p_2 p_3 p_4$ lies within the ranges $[V, W]$ or $[P/W, P/V]$; they will contribute to g_1 . The remaining terms in ψ_j are placed in ψ_j^b and will contribute to b_1 or b_2 , depending on the value of j .

Combining (4.4)–(4.9), we now have (4.1) with

$$\begin{aligned} g_1(m) &= \psi_1(m) - \psi_3(m) - \psi_5(m) + \psi_8(m) + \psi_{11}(m) - \psi_{12}(m) + \psi_{13}^g(m) \\ &\quad + \psi_{14}(m) - \psi_{16}^g(m) - \psi_{17}(m) - \psi_{18}(m) + \psi_{19}^g(m), \\ b_1(m) &= \psi_4(m) + \psi_{16}^b(m), \quad b_2(m) = \psi_{10}(m) + \psi_{13}^b(m) + \psi_{19}^b(m). \end{aligned}$$

We remark that each term ψ_j that appears in g_1 leads to an exponential sum that can be estimated using Lemmas 3.3 or 3.4, and that each term $\psi_j^g(m)$ leads to a sum that can be estimated using Lemma 3.3.

We now turn to (4.2). We have

$$\psi_2(m) = \left\{ \sum_{z \leq p \leq Y^{1/2}} + \sum_{Y^{1/2} < p < V} \right\} \psi(m/p, p) = \psi_{20}(m) + \psi_{21}(m), \quad \text{say.} \quad (4.10)$$

The term ψ_{21} will contribute to b_3 ; we apply (4.3) twice to ψ_{20} . That gives

$$\begin{aligned} \psi_{20}(m) &= \sum_{z \leq p_1 \leq Y^{1/2}} \left\{ \psi(m/p_1, z) - \sum_{z \leq p_2 < p_1} \psi(m/(p_1 p_2), z) \right. \\ &\quad \left. + \sum_{z \leq p_3 < p_2 < p_1} \psi(m/(p_1 p_2 p_3), p_3) \right\} \\ &= \psi_{22}(m) - \psi_{23}(m) + \psi_{24}(m), \quad \text{say.} \end{aligned} \quad (4.11)$$

We split ψ_{24} into “good” and a “bad” parts, and then further split $\psi_{24}^b(m)$ in two:

$$\begin{aligned} \psi_{24}^b(m) &= \sum_{p_1, p_2, p_3} \left\{ \sum_{p_1 p_2 p_3^2 \leq Y} + \sum_{p_1 p_2 p_3^2 > Y} \right\} \psi(m/(p_1 p_2 p_3), p_3) \\ &= \psi_{25}(m) + \psi_{26}(m), \quad \text{say.} \end{aligned} \quad (4.12)$$

We apply Buchstab’s identity two more times to ψ_{25} :

$$\begin{aligned} \psi_{25}(m) &= \sum_{p_1, p_2, p_3} \left\{ \psi(m/(p_1 p_2 p_3), z) - \sum_{z \leq p_4 < p_3} \psi(m/(p_1 \cdots p_4), z) \right. \\ &\quad \left. + \sum_{z \leq p_5 < p_4 < p_3} \psi(m/(p_1 \cdots p_5), p_5) \right\} \\ &= \psi_{27}(m) - \psi_{28}(m) + \psi_{29}(m), \quad \text{say.} \end{aligned} \quad (4.13)$$

Finally, we split ψ_{26} and ψ_{29} into “good” and “bad” subsums. We remark that the summation conditions in ψ_{25} imply $p_1 p_3 \leq W$. (Otherwise, we would have $p_2 p_3 \leq P^\sigma$, whence $p_3 \leq P^{\sigma/2}$ and $p_1 p_3 \leq P^{1/2-\sigma}$; the latter contradicts the assumption $p_1 p_3 > W$ when $\sigma < 1/6$.) Therefore, the exponential sums with coefficients ψ_{27} and ψ_{28} can be estimated either by Lemma 3.3 (when $p_1 p_3 \geq V$) or by Lemma 3.4 (when $p_1 p_3 < V$). Combining (4.4) and (4.10)–(4.13), we have (4.2) with

$$\begin{aligned} g_2(m) &= \psi_1(m) - \psi_3(m) - \psi_5(m) - \psi_{22}(m) + \psi_{23}(m) - \psi_{24}^g(m) \\ &\quad - \psi_{26}^g(m) - \psi_{27}(m) + \psi_{28}(m) - \psi_{29}^g(m), \\ b_3(m) &= \psi_4(m) + \psi_{21}(m) + \psi_{26}^b(m) + \psi_{29}^b(m). \end{aligned}$$

It follows from (4.1) and (4.2) that

$$\psi(m, P^{1/2})\psi(k, P^{1/2}) \geq g_1(m)\psi(k, P^{1/2}) - b_1(m)g_2(k).$$

Thus, we may choose the sieve functions ρ_j , $1 \leq j \leq 3$, in (2.2) as

$$\rho_1 = g_1, \quad \rho_2 = g_2 \quad \text{and} \quad \rho_3 = b_1.$$

It is clear from the above construction that this choice leads to respective generating functions f_1 and f_2 that satisfy inequality (2.10). Furthermore, all three functions are supported on integers m with $\psi(m, z) = 1$, so hypothesis (i) in §2 is satisfied as long as $\sigma < 0.1566\dots$

5. THE PROOF OF THEOREM 1.1

In this section, we demonstrate that the functions ρ_1, ρ_2, ρ_3 above with $\sigma = 5/32 + \delta$, where $\delta > 0$ is a fixed, sufficiently small constant, have all the properties postulated in §2.

5.1. The major arcs. We first justify the major arc approximation (2.8). As explained above, the sieve weights satisfy hypothesis (i) in §2, provided that $\delta \leq 10^{-4}$, for example. The hypotheses (ii) and (iii) on the distribution of the ρ_j 's follow by partial summation from the Prime Number Theorem and from the Siegel–Walfisz theorem in the form given by Iwaniec and Kowalski [9, (5.79)]. In particular, the constants C_j in hypothesis (iii) arise as linear combinations of multiple integrals corresponding to the different functions ψ_j^* in §4. For example, our choice of ρ_3 results in

$$C_3 = \log \left(\frac{4\sigma}{1-4\sigma} \right) + \iiint_{D_{16}} \omega \left(\frac{1-u_1-u_2-u_3}{u_3} \right) \frac{du_1 du_2 du_3}{u_1 u_2 u_3^2},$$

where ω is the so-called Buchstab function from sieve theory and D_{16} is the set in \mathbb{R}^3 defined by the conditions

$$1 - 6\sigma \leq u_3 \leq u_2 \leq u_1 \leq 2\sigma, \quad 1 - 4\sigma \leq u_1 + u_2 \leq 1 - 3\sigma \leq u_1 + u_2 + u_3,$$

no subsum of $u_1 + u_2 + u_3$ lies in the set $[2\sigma, 1 - 4\sigma] \cup [4\sigma, 1 - 2\sigma]$.

The reader will find the definition of ω and a thorough explanation of the nature of the approximations in (iii) in Harman's monograph [5, pp. 15–16]. A numerical evaluation of the constants C_j reveals that when $\sigma = 5/32 + 10^{-4}$, we have

$$C_1 > 1.665, \quad C_2 < 2.096, \quad \text{and} \quad C_3 < 0.769,$$

and so (2.9) holds when $\delta = 10^{-4}$.

Beyond properties (i)–(iii) in §2, we also need an additional, more technical arithmetic hypothesis on the functions ρ_j :

(iv) The function ρ_j can be expressed as a linear combination of $O(L^c)$ bilinear sums of the form

$$\sum_{uv=m} \alpha_u \beta_v,$$

where $|\alpha_u| \leq \tau(u)^c$, $|\beta_v| \leq \tau(v)^c$, and either $P^{0.06} \leq v \leq P^{0.94}$ (type II), or $v \geq P^{0.06}$ and $\beta_v = 1$ for all v (type I).

Note that in the case $j = 0$ (i.e., when ρ_j is the indicator function of the primes), we can obtain such a decomposition by applying Vaughan's or Heath-Brown's combinatorial identities for von Mangoldt's function. Hypothesis (iv) states that our sieve functions can be similarly decomposed. Indeed, with the exception of $\psi_1(m)$, every other arithmetic function $\psi_j^*(m)$ in §4 can be viewed as a type II sum under hypothesis (iv). Finally, in the notation of Lemma 3.4, we have

$$\psi_1(m) = \sum_{\substack{m=dv \\ d|\Pi}} \mu(d),$$

and the sum on the right can be split into $O(L)$ subsums, each either of type II, or of type I with $v \geq P^{0.94}$.

We next sketch how hypotheses (i)–(iv) lead to a proof of (2.8). The proof of (2.8) in the case $j = k = 0$ is by now a standard matter: see for example Liu [11], where he establishes such a result for $\mathfrak{M} = \mathfrak{M}(P^{0.4-\epsilon})$. Harman and the first author [6, 7] showed that the arguments from [11] can be applied to more general integrals of the above type, though at the cost of some technical complications. The major inconvenience in those works is the possibility (not present in [11]) that when α is on a major arc centered at a/q , $(a, q) = 1$, the denominator q need not be relatively prime to all the integers in the support of the sieve weights (see [6, pp. 6–7] and [7, p. 1974]). Our choice of major arcs (2.7) and hypothesis (i), however, rule out that possibility in the present context. Therefore, we can follow the argument in [11] almost verbatim except for the estimation of the quantity $J(g)$ in [11, §3], which we need to replace by

$$J(g) = \sum_{r \sim R} [r, g]^{-1+\epsilon} \sum_{\chi \bmod r}^* \max_{|\beta| \leq P^{-1.99}} \left| \sum_{m \in \mathcal{I}} \rho_j(m) \chi(m) e(\beta m^2) \right|,$$

where $1 \leq R \leq P^{0.01}$, g is an integer with $1 \leq g \leq N$, and the middle sum is over all primitive Dirichlet characters χ modulo r . The estimation of this average can be handled using the modification of Liu’s argument outlined in [6, (4.10)–(4.12)]. Using hypothesis (iv), we can replace [11, Lemma 2.1] with the inequality (cf. [6, (4.12)])

$$\sum_{r \sim R} \sum_{\chi \bmod r}^* \int_{-T}^T |F_j(1/2 + it, \chi)| dt \ll L^\epsilon (P^{1/2} + RT^{1/2} P^{0.47} + R^2 T), \quad (5.1)$$

where $F_j(s, \chi)$ is the Dirichlet polynomial

$$F_j(s, \chi) = \sum_{m \in \mathcal{I}} \rho_j(m) \chi(m) m^{-s}.$$

Once we have (5.1) at our disposal, we follow the argument in [6, p. 8] to obtain the needed variants of [11, Lemmas 3.1 and 3.2] and complete the proof of (2.8).

5.2. The minor arcs. We write $\mathcal{E}_N = \mathcal{E} \cap (N/2, N]$,

$$F(\alpha) = f_1(\alpha) f_0(\alpha) - f_3(\alpha) f_2(\alpha), \quad K(\alpha) = \sum_{n \in \mathcal{E}_N} e(-\alpha n).$$

In particular, we have

$$S_1 - S_2 = \int_0^1 F(\alpha) f_0(\alpha)^2 e(-\alpha n) d\alpha. \quad (5.2)$$

For $n \in (N/2, N] \cap \mathcal{A}$, one has

$$\mathfrak{S}(n) \gg 1 \quad \text{and} \quad \mathfrak{I}(n/N) \gg 1. \quad (5.3)$$

From (2.3), (2.8), (2.9), (5.2), and (5.3), we deduce that

$$- \int_{\mathfrak{m}} F(\alpha) f_0(\alpha)^2 e(-n\alpha) d\alpha \gg NL^{-4}$$

for all $n \in \mathcal{E}_N$. Summing these inequalities over n , we obtain

$$|\mathcal{E}_N| NL^{-4} \ll \left| \int_{\mathfrak{m}} F(\alpha) f_0(\alpha)^2 K(\alpha) d\alpha \right|. \quad (5.4)$$

Recall that by the construction of ρ_1 and ρ_2 , we can use Lemmas 3.3 and 3.4 to establish (2.10). Thus, we obtain from (2.10) that

$$\int_{\mathfrak{n}} F(\alpha) f_0^2(\alpha) K(\alpha) d\alpha \ll P^{1-\sigma+\epsilon} (I_1 + I_2), \quad (5.5)$$

where

$$I_1 = \int_0^1 |f_0^3(\alpha)K(\alpha)| d\alpha, \quad I_2 = \int_0^1 |f_3(\alpha)f_0^2(\alpha)K(\alpha)| d\alpha.$$

We now define a function Δ on \mathfrak{N} by

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

when $|q\alpha - a| \leq P^{-4/3}$, with $1 \leq a \leq q \leq P^{2/3}$ and $(a, q) = 1$. By the main result in Ren [15], when $\alpha \in \mathfrak{N}$, we have

$$f_0(\alpha) \ll P^{1+\epsilon}\Delta(\alpha)^{1/2} + P^{5/6+\epsilon}. \quad (5.6)$$

From (5.6), we deduce that

$$\int_{\mathfrak{m} \cap \mathfrak{N}} F(\alpha)f_0(\alpha)^2 K(\alpha) d\alpha \ll P^{5/6+\epsilon}I_3 + P^{1+\epsilon}I_4, \quad (5.7)$$

where

$$I_3 = \int_0^1 |F(\alpha)f_0(\alpha)K(\alpha)| d\alpha,$$

$$I_4 = \int_{\mathfrak{m} \cap \mathfrak{N}} |F(\alpha)f_0(\alpha)\Delta(\alpha)^{1/2}K(\alpha)| d\alpha.$$

We can estimate I_1, I_2 and I_3 similarly to Wooley [18, (3.21)–(3.23)]. This yields the bounds

$$I_1, I_2, I_3 \ll N^{3/4+\epsilon}|\mathcal{E}_N|^{1/2} + N^{1/2+\epsilon}|\mathcal{E}_N|. \quad (5.8)$$

Moreover, an argument similar to that in Wooley [18, (3.27)–(3.29)] gives

$$I_4 \ll P^{1+\epsilon}|\mathcal{E}_N|^{3/4} + P^{1+\epsilon}Q^{-1/2}|\mathcal{E}_N|, \quad (5.9)$$

where $Q = P^{0.01}$. We conclude from (5.5) and (5.7)–(5.9) that

$$\int_{\mathfrak{m}} F(\alpha)f_0(\alpha)^2 K(\alpha) d\alpha \ll N^{5/4-\sigma/2+\epsilon}|\mathcal{E}_N|^{1/2} + N^{1+\epsilon}|\mathcal{E}_N|^{3/4} + N^{0.998}|\mathcal{E}_N|$$

$$\ll N^{5/4-\sigma/2+\epsilon}|\mathcal{E}_N|^{1/2} + N^{0.998}|\mathcal{E}_N|. \quad (5.10)$$

Finally, combining (5.4) and (5.10) and recalling that $\sigma = 5/32 + 10^{-4}$, we obtain

$$|\mathcal{E}_N| \ll N^{1/2-\sigma+\epsilon} \ll N^{11/32}.$$

This establishes (2.1) and completes the proof of the theorem.

Acknowledgment. This collaboration originated during the workshop on Analytic Number Theory at Oberwolfach, October 20–26, 2013. The authors would like to thank the Mathematics Institute and the organizers of that meeting for their hospitality and the stimulating working environment. Moreover, A. Kumchev wants to express his gratitude to the Morningside Center for Mathematics at the Chinese Academy of Sciences for hospitality during the Workshop on Number Theory, July 20–28, 2014, when work on this project was completed.

REFERENCES

- [1] A. Ghosh, *The distribution of xp^2 modulo 1*, Proc. London Math. Soc. (3) **42** (1981), 252–269.
- [2] G. Harman, *On the distribution of xp modulo one*, J. London Math. Soc. (2) **27** (1983), 9–18.
- [3] ———, *On the distribution of xp modulo one II*, Proc. London Math. Soc. (3) **72** (1996), 241–260.
- [4] ———, *The values of ternary quadratic forms at prime arguments*, Mathematika **51** (2004), 83–96.
- [5] ———, *Prime Detecting Sieves*, Princeton University Press, 2007.
- [6] G. Harman and A. V. Kumchev, *On sums of squares of primes*, Math. Proc. Cambridge Phil. Soc. **140** (2006), 1–13.

- [7] ———, *On sums of squares of primes II*, J. Number Theory. **130** (2010), 1969–2002.
- [8] L. K. Hua, *Some results in additive prime number theory*, Quart. J. Math. Oxford **9** (1938), 68–80.
- [9] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society, 2004.
- [10] 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.
- [11] J. Y. Liu, *On Lagrange’s theorem with prime variables*, Quart. J. Math. Oxford (2) **54** (2003), 453–462.
- [12] J. Y. Liu and M. C. Liu *The exceptional set in the four prime squares problem*, Illinois J. Math. **44** (2000), 272–293.
- [13] J. Y. Liu, T. D. Wooley and G. Yu, *The quadratic Waring-Goldbach problem*, J. Number Theory **107** (2004), 298–321.
- [14] J. Y. Liu and T. Zhan *Sums of five almost equal prime squares II*, Sci. China **41** (1998), 710–722.
- [15] X. Ren, *On exponential sum over primes and application in Waring-Goldbach problem*, Sci. China Ser. A Math. (6) **48** (2005), 785–797.
- [16] W. Schwarz, *Zur Darstellun von Zahlen durch Summen von Primzahlpotenzen*, J. reine angew. Math. **206** (1961), 78–112.
- [17] R. C. Vaughan, *The Hardy-Littlewood Method*, Second ed., Cambridge University Press, 1997.
- [18] T. D. Wooley, *Slim exceptional sets for sums of four squares*, Proc. London Math. Soc. (3) **85** (2002), 1–21.

DEPARTMENT OF MATHEMATICS, TOWSON UNIVERSITY, 7800 YORK ROAD, TOWSON, MD 21252, U.S.A.
E-mail address: akumchev@towson.edu

SCHOOL OF MATHEMATICS, HEFEI UNIVERSITY OF TECHNOLOGY, HEFEI, 230009, CHINA
E-mail address: zhaolilu@gmail.com