BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 62, No. 3, 2014

NUMBER THEORY

Sums of Squares Coprime in Pairs

by

Jörg BRÜDERN

Presented by Andrzej SCHINZEL

Summary. Asymptotic formulae are provided for the number of representations of a natural number as the sum of four and of three squares that are pairwise coprime.

1. Introduction. In a recent contribution to this journal Professor Schinzel established that all sufficiently large natural numbers in the union $\mathfrak{A}$ of the congruence classes 3, 4, 7, 12, 15 and 19 modulo 24 are sums of four integral squares that are coprime in pairs [6]. The numbers in the remaining classes cannot be represented in the proposed manner, as is readily checked by considering squares modulo 24. The argument invokes the Siegel–Walfisz theorem, so that no bound can be named for the size of the exceptions in Schinzel's theorem. The object of this note is to respond affirmatively to his inquiries whether the result can be demonstrated effectively, and whether sums of three pairwise coprime squares could be treated in like manner, the necessary congruence condition now being that the number to be represented is in one of the classes 2, 3, 6, 11, 14 and 18 modulo 24. When $s = 3$ or 4, our argument yields asymptotic formulae for the number $R_s(n)$ of natural numbers $x_1, \dots, x_s$ with

$$x_1^2 + x_2^2 + \dots + x_s^2 = n, \quad (x_i, x_j) = 1 \quad (1 \le i < j \le s),$$

and with these in hand, we are able to deduce the following.

THEOREM 1. *There exist positive numbers c, n_0 such that $R_4(n) \ge cn$ for all natural numbers $n \in \mathfrak{A}$ with $n \ge n_0$. Further, for any $\varepsilon > 0$ there are positive numbers $c(\varepsilon)$, $n_0(\varepsilon)$ such that $R_3(n) \ge c(\varepsilon) n^{1/2-\varepsilon}$ for all natural numbers $n \ge n_0(\varepsilon)$ with $n + 1 \in \mathfrak{A}$.*

2010 *Mathematics Subject Classification*: Primary 11E25; Secondary 11D85.
Key words and phrases: sums of squares, Kloosterman method, ternary quadratic forms.

DOI: 10.4064/ba62-3-3

Our estimations of $R_4(n)$ are effective, and it would be possible to assign a numerical value to n_0. Schinzel has conjectured that for all $n > 268$ with $n \in \mathfrak{A}$ one has $R_4(n) \geq 1$. With a refined version of our approach and the help of machine computation, it is perhaps possible to check this. In contrast, our lower bound for $R_3(n)$ stems from Siegel's theorem, and is therefore ineffective.

Throughout this paper, the letter p denotes a prime.

2. Large common factors. The evaluation of $R_s(n)$ depends on an auxiliary upper bound for the number of representations of n as the sum of s squares with a large common factor between two of the squares involved. Such representations are rare, but when $s = 3$ a proof of this fact requires some care.

LEMMA 1. *Let c and m be natural numbers, and let $\varrho_c(m)$ denote the number of solutions of $x^2 + cy^2 = m$ in non-negative numbers x, y. Then the bound $\varrho_c(m) \ll m^{\varepsilon}$ holds uniformly in all c that are expressible as the sum of two integral squares.*

Proof. When $c > m$, we have $\varrho_c(m) \leq 1$. When $c \leq m$, write $c = c_1 c_2^2$ with squarefree c_1 to see that $\varrho_c(m) \leq \varrho_{c_1}(m)$. Since c is a sum of two squares, it follows that c_1 is divisible by no prime congruent to 3 mod 4. Hence, $-4c_1$ is a fundamental discriminant, and Satz 8.3 of Zagier [10] implies that

$$\varrho_{c_1}(m) \leq 6 \sum_{d|m} \left(\frac{-4c_1}{d} \right).$$

A divisor function estimate completes the proof of the lemma. ∎

LEMMA 2. *Let $s = 3$ or 4, and let $1 \leq D \leq n^{1/6}$. Let $T_s(n, D)$ denote the number of solutions in positive integers of $x_1^2 + x_2^2 + \cdots + x_s^2 = n$ with $(x_1, x_2) \geq D$. Then $T_s(n, D) \ll n^{s/2-1+\varepsilon} D^{-1}$.*

Proof. Note that for all $\mathbf{x}$ counted here one has $x_i \leq n^{1/2}$. Hence, the number of choices for x_1, x_2 with $(x_1, x_2) \geq D$ does not exceed $4nD^{-1}$. For any fixed such choice of x_1, x_2, Lemma 1 shows that the number of solutions in x_3, x_4 of $x_3^2 + x_4^2 = n - x_1^2 - x_2^2$ is $O(n^{\varepsilon})$. This proves Lemma 2 when $s = 4$.

More care is required when $s = 3$. Let $U(n, d)$ denote the number of solutions in natural numbers of $x_1^2 + x_2^2 + x_3^2 = n$ with $(x_1, x_2) = d$. Then

$$T_3(n, D) = \sum_{D \leq d \leq n^{1/2}} U(n, d). \tag{1}$$

For any $d \leq n^{1/2}$, consider a prime p with $p^e \parallel (d^2, n)$, and suppose that e is odd. Then $p^e \parallel n$ and $p^{e+1} \mid d^2$. For any solution $\mathbf{x}$ counted by $U(n, d)$ it

follows that $x_3^2 \equiv n \bmod p^{e+1}$, and further that $p^e \parallel x_3^2$, which is impossible. We conclude that $U(n,d) = 0$ in all cases where (d^2, n) is not a square.

We may now suppose that $(d^2, n) = u^2$, and hence that $d = uv$. For any solution $\mathbf{x}$ counted by $U(n,d)$, we have $(d^2, n) \mid x_3^2$, whence $u \mid x_3$. Now $x_i = dy_i$ $(i = 1, 2)$ and $x_3 = uz$ with natural numbers y_1, y_2, z. It follows that $U(n,d)$ does not exceed the number of solutions in y_1, y_2, z of

$$v^2(y_1^2 + y_2^2) + z^2 = nu^{-2}. \tag{2}$$

Note that $(nu^{-2}, v) = 1$. Equation (2) implies $z \le n^{1/2}u^{-1}$ and $z^2 \equiv nu^{-2} \bmod v^2$, forcing z into no more than $O(v^\varepsilon)$ congruence classes modulo v^2. Hence, the number of choices for z does not exceed $\ll v^\varepsilon(n^{1/2}u^{-1}v^{-2} + 1)$, and for any chosen z, Lemma 1 shows that the number of solutions of (2) in y_1, y_2 is bounded by $O(n^\varepsilon)$. This yields $U(n,d) \ll n^\varepsilon(n^{1/2}u^{-1}v^{-2} + 1)$ and

$$\sum_{D \le d \le n^{1/3}} U(n,d) \ll n^\varepsilon \sum_{u^2 \mid n} \sum_{D/u \le v \le n^{1/3}/u} \frac{n^{1/2}}{uv^2} + n^{1/3+\varepsilon} \ll \frac{n^{1/2+2\varepsilon}}{D} + n^{1/3+\varepsilon},$$

which is acceptable. The above discussion also shows that the sum

$$U = \sum_{n^{1/3} < d \le n^{1/2}} U(n,d)$$

does not exceed the number of solutions of (2) in natural numbers y_1, y_2, z, u, v with $u^2 \mid n$, $(y_1, y_2) = 1$, $(v, nu^{-2}) = 1$ and $uv > n^{1/3}$. For the solutions counted here, (2) implies that $y_i \le n^{1/2}/(uv) \le n^{1/6}$, so that there are at most $n^{1/3}$ choices for the pairs y_1, y_2. For any fixed choice of y_1, y_2, we infer from Lemma 1 that the number of solutions of (2) in v and z is $O(n^\varepsilon)$. Hence $U \ll n^{1/3+\varepsilon}$, and the desired bound for $T_3(n,D)$ follows from (1). ∎

3. Initial transformation. The opening game begins with the obvious identity

$$R_s(n) = \sum_{x_1^2 + \cdots + x_s^2 = n} \sum_{\substack{d_{ij} \mid (x_i, x_j) \\ 1 \le i < j \le s}} \mu(d_{ij}). \tag{3}$$

In the interest of brevity, let $\mathbf{d} = (d_{ij})_{1 \le i < j \le s}$, and put

$$\mu(\mathbf{d}) = \prod_{1 \le i < j \le s} \mu(d_{ij}), \quad |\mathbf{d}| = \max_{1 \le i < j \le s} |d_{ij}|. \tag{4}$$

In the later proceedings, we will use this notation also for vectors of different format. Now choose a number θ with $0 < \theta < 1/6$. Let $R_s'(n)$ denote the portion of the sum in (3) where $|\mathbf{d}| \le n^\theta$, and let $R_s''(n)$ be the complementary part where $|\mathbf{d}| > n^\theta$. By symmetry and a divisor function estimate, one

has $R_s''(n) \ll n^{\varepsilon} T_s(n, n^{\theta})$. Hence, by Lemma 2,

$$R_s(n) = R_s'(n) + O(n^{s/2-1-\theta+\varepsilon}). \tag{5}$$

Further, one infers directly from the definition that $R_s'(n)$ equals

$$\sum_{|\mathbf{d}|\le n^{\theta}} \mu(\mathbf{d}) \#\{\mathbf{x} \in \mathbb{N}^s : x_1^2+\cdots+x_s^2 = n,\ d_{ij} \,|\, (x_i, x_j)\ (1 \le i < j \le s)\}. \tag{6}$$

For $1 \le l \le s$, set

$$C_l = \prod_{1\le i<l} d_{il} \prod_{l<j\le s} d_{lj}, \quad c_l = \prod_{p \mid C_l} p. \tag{7}$$

For squarefree d_{ij}, the simultaneous conditions $d_{ij} \,|\, (x_i, x_j)$ $(1 \le i < j \le s)$ are equivalent to $c_l \,|\, x_l$ for $1 \le l \le s$. Hence, if $r_{\mathbf{c}}(n)$ denotes the number of solutions of

$$c_1^2 y_1^2 + \cdots + c_s^2 y_s^2 = n$$

in natural numbers $y_1, \dots, y_s$, we find from (5) and (6) that

$$R_s(n) = \sum_{|\mathbf{d}|\le n^{\theta}} \mu(\mathbf{d}) r_{\mathbf{c}}(n) + O(n^{s/2-1-\theta+\varepsilon}). \tag{8}$$

Here $\mathbf{c}$ is defined in terms of $\mathbf{d}$ via (7). For later use, we summarise certain properties of the mapping $\mathbf{d} \mapsto \mathbf{c}$ in the next lemma. It features the set $\mathscr{U} = \{u \in \mathbb{N} : p \,|\, u \Rightarrow p^2 \,|\, u\}$ of squareful numbers.

LEMMA 3. *Let $s = 3$ or 4, and suppose that $\mathbf{d} = (d_{ij})_{1\le i<j\le s}$ with $\mu(\mathbf{d})^2 = 1$ and $\mathbf{c} \in \mathbb{N}^s$ correspond via (7). Then $\mu(\mathbf{c})^2 = 1$ and $c_1 \cdots c_s \in \mathscr{U}$. Further $|\mathbf{c}| \le |\mathbf{d}|^{s-1}$.*

Proof. Let p be a prime with $p \,|\, c_1$. Then there is some $j \in \{2, \dots, s\}$ with $p \,|\, d_{1j}$, and it follows that $p \,|\, c_j$. By symmetry, this argument shows that $c_1 \cdots c_s$ is squareful. The other claims are immediate from (7). ∎

4. Sums of four squares. At this point, the treatment of the cases $s = 3$ and $s = 4$ can no longer be performed in parallel. For $s = 4$, the case on which we concentrate first, the method rests on results obtained in collaboration with Fouvry [3]. Let

$$S(q, a) = \sum_{x=1}^{q} e(ax^2/q) \tag{9}$$

and

$$A(q, \mathbf{c}, n) = q^{-4} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(-an/q) \prod_{j=1}^{4} S(q, ac_j^2). \tag{10}$$

As a special case of [3, Lemma 1], we recall the estimate

$$A(q,\mathbf{c},n) \ll q^{\varepsilon-3/2}\big((q,n)(q,c_1^2)(q,c_2^2)(q,c_3^2)(q,c_4^2)\big)^{1/2}. \tag{11}$$

It follows that the series

$$\mathfrak{S}(\mathbf{c},n) = \sum_{q=1}^{\infty} A(q,\mathbf{c},n) \tag{12}$$

converges absolutely. The next lemma is a simplified version of [3, Theorem 3].

LEMMA 4. *There is a positive number δ such that uniformly for all $\mathbf{c} \in \mathbb{N}^4$ with $\mu(\mathbf{c})^2 = 1$ and $|\mathbf{c}| \le n^{1/24}$ one has*

$$r_{\mathbf{c}}(n) = \left(\frac{\pi}{4}\right)^2 \frac{\mathfrak{S}(\mathbf{c},n)n}{c_1c_2c_3c_4} + O(n^{1-2\delta}).$$

We may take $\delta \le 1/4$ and $\theta = \delta/6$. Then, by (8) and Lemma 4,

$$R_4(n) = \left(\frac{\pi}{4}\right)^2 n \sum_{|\mathbf{d}|\le n^{\theta}} \mu(\mathbf{d}) \frac{\mathfrak{S}(\mathbf{c},n)}{c_1c_2c_3c_4} + O(n^{1-\theta+\varepsilon}). \tag{13}$$

Here and in similar expressions later, $\mathbf{c}$ is defined in terms of $\mathbf{d}$ via (7).

LEMMA 5. *For natural numbers n the multiple series*

$$V(n) = \sum_{\mathbf{d}\in\mathbb{N}^6} \mu(\mathbf{d})^2 |\mathbf{d}|^{1/4} \frac{|\mathfrak{S}(\mathbf{c},n)|}{c_1c_2c_3c_4}$$

converges, and $V(n) \ll n^{\varepsilon}$.

Equipped with this lemma, we see that the *singular series*

$$\mathfrak{E}_4(n) = \sum_{\mathbf{d}\in\mathbb{N}^6} \mu(\mathbf{d})^2 \frac{\mathfrak{S}(\mathbf{c},n)}{c_1c_2c_3c_4} \tag{14}$$

converges absolutely, and that this expression differs from its truncated version in (13) by an amount not exceeding $V(n)n^{-\theta/4} \ll n^{-\theta/5}$. By (13), we may conclude as follows.

THEOREM 2. *There is a positive number η with the property that*

$$R_4(n) = \left(\frac{\pi}{4}\right)^2 \mathfrak{E}_4(n)n + O(n^{1-\eta}).$$

It remains to establish Lemma 5. By (11) and (12),

$$V(n) \ll \sum_{q=1}^{\infty} q^{\varepsilon-3/2}(q,n)^{1/2} F(q) \tag{15}$$

where

$$F(q) = \sum_{\mathbf{d}\in\mathbb{N}^6} \mu(\mathbf{d})^2 |\mathbf{d}|^{1/4} \frac{\big((q,c_1^2)(q,c_2^2)(q,c_3^2)(q,c_3^2)\big)^{1/2}}{c_1c_2c_3c_4}.$$

When all d_{ij} are squarefree, we infer from (7) that $d_{ij} \,|\, c_i$ and $d_{ij} \,|\, c_j$. This implies $d_{ij} \le (c_ic_j)^{1/2}$, whence $|\mathbf{d}| \le (c_1c_2c_3c_4)^{1/2}$, and consequently

$$F(q) \le \sum_{\mathbf{d}\in\mathbb{N}^6} \mu(\mathbf{d})^2 \frac{\big((q,c_1^2)(q,c_2^2)(q,c_3^2)(q,c_3^2)\big)^{1/2}}{(c_1c_2c_3c_4)^{7/8}}. \tag{16}$$

We now wish to bound the right hand side above by a sum over $\mathbf{c}$. Let

$$\mathscr{C} = \{\mathbf{c} \in \mathbb{N}^4 : \mu(\mathbf{c})^2 = 1,\ c_1c_2c_3c_4 \in \mathscr{U}\}.$$

Then, by Lemma 3, all $\mathbf{c}$ that occur on the right hand side of (16) are in $\mathscr{C}$. In the reverse direction, let $\mathbf{c} \in \mathscr{C}$. Then any $\mathbf{d}$ with $\mu(\mathbf{d})^2 = 1$ corresponding to $\mathbf{c}$ via (7) satisfies $d_{ij} \,|\, c_i$, $d_{ij} \,|\, c_j$ for all $1 \le i < j \le 4$. Hence, the number of $\mathbf{d}$ that yield the same $\mathbf{c}$ is bounded by $O(|\mathbf{c}|^{\varepsilon})$. Therefore, by (16),

$$F(q) \ll \sum_{\mathbf{c}\in\mathscr{C}} \mu(\mathbf{c})^2 \frac{\big((q,c_1^2)(q,c_2^2)(q,c_3^2)(q,c_3^2)\big)^{1/2}}{(c_1c_2c_3c_4)^{6/7}} \ll \sum_{u\in\mathscr{U}} u^{-6/7} f_q(u) \tag{17}$$

where

$$f_q(u) = \sum_{\substack{\mathbf{c}\in\mathbb{N}^4\\ c_1c_2c_3c_4=u}} \mu(\mathbf{c})^2 \big((q,c_1^2)(q,c_2^2)(q,c_3^2)(q,c_3^2)\big)^{1/2}. \tag{18}$$

It is immediate that the function $f_q(u)$ is multiplicative in u. Also, for a prime p and $l \in \mathbb{N}$, the solutions of $c_1c_2c_3c_4 = p^l$ with $\mu(\mathbf{c})^2 = 1$ have exactly l of the c_j equal to p, and the remaining ones equal to 1. Hence $f_q(p^l) = 0$ for all $l \ge 5$. Rewriting the right hand side of (17) as an Euler product yields

$$F(q) \ll \prod_p \big(1 + p^{-12/7} f_q(p^2) + p^{-18/7} f_q(p^3) + p^{-24/7} f_q(p^4)\big). \tag{19}$$

The remark preceding (19) together with (18) also shows that for $p \nmid q$ one has $f_q(p^l) \le 6$ for $2 \le l \le 4$, whence the corresponding Euler factors in (19) are of the form $1 + O(p^{-12/7})$. Further, when $p \parallel q$ and $2 \le l \le 4$, we again find from (18) that

$$f_q(p^l) = f_p(p^l) = \sum_{c_1c_2c_3c_4=p^l} \mu(\mathbf{c})^2 \big((p,c_1)(p,c_2)(p,c_3)(p,c_4)\big)^{1/2} \le 6p^{l/2}.$$

Similarly, when $p^2 \,|\, q$, one finds that

$$f_q(p^l) = f_{p^2}(p^l) = \sum_{c_1c_2c_3c_4=p^l} \mu(\mathbf{c})^2 \big((p^2,c_1^2)(p^2,c_2^2)(p^2,c_3^2)(p^2,c_4^2)\big)^{1/2} \le 6p^l.$$

On collecting together, one derives from (19) that

$$F(q) \ll \prod_{p\|q}(1+18p^{-5/7}) \prod_{p^2|q}(1+18p^{4/7}) \ll q^{\varepsilon} q_2^{2/7}$$

where $q_2 \in \mathscr{U}$ is defined through the unique factorisation $q = q_1 q_2$ with $(q_1, q_2) = 1$, $\mu(q_1)^2 = 1$. By (15) we now see that

$$V(n) \ll \sum_{q_1=1}^{\infty} \mu(q_1)^2 q_1^{\varepsilon-3/2} (q_1, n)^{1/2} \sum_{q_2 \in \mathscr{U}} q_2^{\varepsilon-17/14} (q_2, n)^{1/2} \ll n^{\varepsilon}.$$

This completes the proof of Lemma 5.

5. The quaternary singular product. The definition of $\mathfrak{E}_4(n)$ in (14) involves an oscillating sum that stems from the use of the inclusion-exclusion principle in the transition to (8) in Section 2. This disguises the arithmetical information typically encoded in a singular series. In fact, $\mathfrak{E}_4(n)$ should be related to the number $M_n(q)$ of incongruent solutions of

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv n \bmod q, \qquad (x_i, x_j, q) = 1 \qquad (1 \le i < j \le 4) \tag{20}$$

in x_1, x_2, x_3, x_4. In this section, such a relation is established by a method that, in some sense, reverses the manipulations leading from (3) to (8). The argument will also present $\mathfrak{E}_4(n)$ as an Euler product from which a lower bound can be deduced along very familiar lines.

LEMMA 6. *For all $n \in \mathbb{N}$ the function $M_n(q)$ is multiplicative in q.*

Proof. Observe that if $d \in \mathbb{N}$ is coprime to q then the mapping $\mathbf{x} \mapsto d\mathbf{x}$ is a bijection between the solutions counted by $M_n(q)$ and $M_{nd^2}(q)$. In particular, one then has $M_n(q) = M_{nd^2}(q)$.

Next suppose that $q = q'q''$ with $(q', q'') = 1$, and choose natural numbers n', n'' with $n \equiv q''^2 n' \bmod q'$ and $n \equiv q'^2 n'' \bmod q''$. We now apply the Chinese remainder theorem and write $\mathbf{x} = q'\mathbf{x}'' + q''\mathbf{x}'$ in (20) to see that the mapping $\mathbf{x} \mapsto (\mathbf{x}', \mathbf{x}'')$ is a bijection between the solutions $\mathbf{x}$ counted by $M_n(q)$ and the pairs $(\mathbf{x}', \mathbf{x}'')$ counted by $M_{n'}(q')$ and $M_{n''}(q'')$, respectively. The two remarks together establish the lemma. ∎

LEMMA 7. *Let $p_1, \dots, p_t$ be distinct primes and write $\Pi = p_1 \cdots p_t$. Further, let $h \ge 5$ and $Q = \Pi^h$. Then*

$$\sum_{\substack{d_{ij}|Q \\ 1\le i<j\le 4}} \frac{\mu(\mathbf{d})}{c_1 c_2 c_3 c_4} \sum_{q|Q} A(q, \mathbf{c}, n) = Q^{-3} M_n(Q). \tag{21}$$

Proof. As in (3), we find that

$$M_n(Q) = \sum_{\substack{x_1,x_2,x_3,x_4=1\\ x_1^2+x_2^2+x_3^2+x_4^2\equiv n \bmod Q}}^{Q} \sum_{\substack{d_{ij}\mid(x_i,x_j,Q)\\ 1\le i<j\le 4}} \mu(\mathbf{d}) = \sum_{\substack{d_{ij}\mid Q\\ 1\le i<j\le 4}} \mu(\mathbf{d}) W_n(Q,\mathbf{c})$$

where $W_n(Q,\mathbf{c})$ is the number of solutions of $x_1^2+x_2^2+x_3^2+x_4^2 \equiv n \bmod Q$ with $1 \le x_i \le Q$ and $c_i \mid x_i$ $(1 \le i \le 4)$. We write $x_i = c_i y_i$ and note that by (7) the c_i are squarefree numbers that divide Π. It follows that $W_n(Q,\mathbf{c})$ equals the number of solutions of $c_1^2y_1^2 + \cdots + c_4^2y_4^2 \equiv n \bmod Q$ with $1 \le y_i \le Q/c_i$. By the theory of quadratic congruences, the number $N_n(Q,\mathbf{c})$ of solutions of $c_1^2y_1^2+\cdots+c_4^2y_4^2 \equiv n \bmod Q$ with $1 \le y_i \le Q$ equals $c_1c_2c_3c_4W_n(\mathbf{c},Q)$, so that we now have

$$M_n(Q) = \sum_{\substack{d_{ij}\mid Q\\ 1\le i<j\le 4}} \frac{\mu(\mathbf{d})}{c_1c_2c_3c_4} N_n(Q,\mathbf{c}). \tag{22}$$

Further, by orthogonality,

$$QN_n(Q,\mathbf{c}) = \sum_{A=1}^{Q} S(Q,Ac_1^2)S(Q,Ac_2^2)S(Q,Ac_3^2)S(Q,Ac_4^2)e\Big(-\frac{An}{Q}\Big).$$

This sum is rearranged according to the value of $(A,Q) = Q/q$ for $q \mid Q$. Since $q^{-1}S(q,a)$ is a function of a/q, this produces

$$\frac{N_n(Q,\mathbf{c})}{Q^3} = \sum_{q\mid Q} \frac{1}{q^4} \sum_{\substack{A=1\\ (A,Q)=Q/q}}^{Q} S(q,ac_1^2)S(q,ac_2^2)S(q,ac_3^2)S(q,ac_4^2)e\Big(-\frac{an}{q}\Big)$$

where a is defined by $A/Q = a/q$. By (10), we infer that

$$Q^{-3}N_n(Q,\mathbf{c}) = \sum_{q\mid Q} A(q,\mathbf{c},n),$$

and Lemma 7 follows from (22). ∎

We are ready to embark on the main argument. First we take $t = 1$ in Lemma 7 which then asserts that for any prime p one has

$$p^{-3h}M_n(p^h) = \sum_{\substack{d_{ij}\mid p\\ 1\le i<j\le 4}} \frac{\mu(\mathbf{d})}{c_1c_2c_3c_4} \sum_{l=0}^{h} A(p^l,\mathbf{c},n).$$

By (11), it follows that the limit

$$E_4(p,n) = \lim_{h\to\infty} p^{-3h}M_n(p^h) \tag{23}$$

exists. We now apply Lemma 7 again, this time with $p_1, \dots, p_t$ the complete list of primes not exceeding a parameter P. In Lemma 6 we take $Q = (p_1 \dots p_t)^h$ to see that the right hand side of (21) equals

$$Q^{-3} M_n(Q) = \prod_{p \le P} p^{-3h} M_n(p^h). \tag{24}$$

Moreover, by (12) and (14), the sum on the left hand side of (21) is a portion of the absolutely convergent series (14). By unique factorisation, the nested limit $h \to \infty$ followed by $P \to \infty$ of the expression on the left hand side of (21) equals $\mathfrak{E}_4(n)$. Now we take $h \to \infty$ in (24), apply (23) and then take $P \to \infty$ to infer the desired identity

$$\mathfrak{E}_4(n) = \prod_p E_4(p, n). \tag{25}$$

The deduction of a lower bound for $\mathfrak{E}_4(n)$ depends on a precise evaluation of $M_n(p)$ for odd primes p. Let $H_s(p, n)$ denote the number of incongruent solutions of $x_1^2 + \dots + x_s^2 \equiv n \bmod p$ with $p \nmid x_j$ $(1 \le j \le s)$. By symmetry and an inspection of (20), one then finds that $M_n(p) = H_4(p, n) + 4H_3(p, n)$. Further, by (9) and orthogonality,

$$pH_s(p, n) = \sum_{a=1}^{p} (S(p, a) - 1)^s e\Big(-\frac{an}{p}\Big).$$

Here we single out the term with $a = p$ and use the trivial identity

$$(X - 1)^4 + 4(X - 1)^3 = X^4 - 6X^2 + 8X - 3$$

twice to infer that

$$pM_n(p) = p^4 - 6p^2 + 8p - 3 + \Gamma, \tag{26}$$

where

$$\Gamma = \sum_{a=1}^{p-1} \big(S(p, a)^4 - 6S(p, a)^2 + 8S(p, a) - 3\big) e\Big(-\frac{an}{p}\Big).$$

We now recall some identities from the elementary theory of Gauß sums. When p is an odd prime and $p \nmid a$, then

$$S(p, a) = \Big(\frac{a}{p}\Big) S(p, 1), \qquad S(p, a)^2 = \Big(\frac{-1}{p}\Big) p, \qquad S(p, 1) = \sum_{a=1}^{p-1} \Big(\frac{a}{p}\Big) e\Big(\frac{a}{p}\Big) \tag{27}$$

(see Rose [5, Theorems 2.2 and 2.3 and formula $(*)$ on p. 108]). In particular, it follows that

$$\Gamma = \Big(p^2 - 6\Big(\frac{-1}{p}\Big)p - 3\Big) \sum_{a=1}^{p-1} e\Big(-\frac{an}{p}\Big) + 8 \sum_{a=1}^{p-1} S(p, a) e\Big(-\frac{an}{p}\Big). \tag{28}$$

When $p \nmid n$, one finds from (27) that

$$\sum_{a=1}^{p-1} S(p,a)e\Big(-\frac{an}{p}\Big) = S(p,1)\sum_{a=1}^{p-1}\Big(\frac{a}{p}\Big)e\Big(-\frac{an}{p}\Big) = \Big(\frac{n}{p}\Big)|S(p,1)|^2 = \Big(\frac{n}{p}\Big)p,$$

and by (26) and (28), we deduce an explicit formula for $M_n(p)$ that implies the inequality

$$|M_n(p) - p^3 + 7p| \le 22. \tag{29}$$

When $p \mid n$, orthogonality and (9) produce

$$\sum_{a=1}^{p-1} S(p,a)e\Big(-\frac{an}{p}\Big) = \sum_{a=1}^{p-1} S(p,a) = 0,$$

so that

$$\Gamma = (p-1)\Big(p^2 - 6\Big(\frac{-1}{p}\Big)p - 3\Big).$$

By (26), we see that $M_n(5) \ge 1$. Also, it follows that $\Gamma \ge 3$ for $p \ge 7$, and by (26) this shows that $M_n(p) \ge p^3 - 6p + 8$. In combination with (29) we may now deduce the following.

LEMMA 8. *Let $p \ge 7$ be a prime, and let n be a natural number. Then $M_n(p) \ge p^3 - 7p - 22$. Further, $M_n(5) \ge 1$. If $n \not\equiv 2 \bmod 3$, then $M_n(3) \ge 1$. If n is in one of the residue classes 3, 4 or 7 modulo 8, then $M_n(8) \ge 1$.*

Proof. The claims for $p \ge 5$ have already been established, and the claims concernings $M_n(3)$ and $M_n(8)$ can be checked by hand. ∎

A lower bound for $\mathfrak{E}_4(n)$ is now easily available. For odd primes p, the argument of proof for Lemma 2.13 of Vaughan [9] yields $M_n(p^h) \ge p^{3h-3}M_n(p)$ for $h \ge 1$, and similarly $M_n(2^h) \ge 2^{3h-9}M_n(8)$ for $h \ge 3$. Hence, by Lemma 8 and (23), we find that for $p \ge 7$ one has $E_4(p,n) \ge 1 - 6p^{-2} - 22p^{-3}$, and also that $E_4(5,n) \ge 5^{-3}$. Further, if n satisfies the congruence conditions in Lemma 8, then $E_4(3,n) \ge 1/27$ and $E_4(2,n) \ge 1/512$. By the Chinese remainder theorem and (25), it follows that $\mathfrak{E}_4(n) \gg 1$ uniformly in $n \in \mathfrak{A}$. The case $s = 4$ of Theorem 1 now follows from Theorem 2.

6. Sums of three squares. Our approach to $R_4(n)$ easily extends to sums of more than four squares. The problem with three squares, however, is more difficult. The arithmetic of ternary quadratic forms is more involved, and the singular series associated with a ternary form no longer converges absolutely. Thus, the manipulations of certain multiple series that we performed in Sections 4 and 5 are harder to verify in the new context, if at all possible. Instead, we turn to an alternative method where the desired conclusion is inferred from the representation of the singular series as an Euler product.

We begin by recalling some basic facts from the analytic theory of positive definite ternary quadratic forms. Throughout, let $c_1, c_2, c_3 \in \mathbb{N}$ with $\mu(\mathbf{c})^2 = 1$. For a prime p and $n \in \mathbb{N}$, the limit

$$\chi_p(\mathbf{c}, n) = \lim_{h\to\infty} p^{-2h} \#\{1 \le x_j \le p^h : c_1^2x_1^2 + c_2^2x_2^2 + c_3^2x_3^2 \equiv n \bmod p^h\} \tag{30}$$

exists, and whenever $p \nmid 2c_1c_2c_3n$, one has

$$\chi_p(\mathbf{c}, n) = 1 + \left(\frac{-n}{p}\right)\frac{1}{p} \tag{31}$$

(see Siegel [8], in particular Hilfssatz 12). Elementary prime number theory shows that the limit

$$\mathfrak{S}(\mathbf{c}, n) = \lim_{P\to\infty} \prod_{p\le P} \chi_p(\mathbf{c}, n) \tag{32}$$

also exists. Let $\mathbf{e} = (1, 1, 1)$ and write $\mathfrak{S}(n) = \mathfrak{S}(\mathbf{e}, n)$. Then (31) computes $\chi_p(\mathbf{e}, n)$ for all $p \nmid 2n$, and for odd primes p with $p \mid n$, Hilfssatz 16 of Siegel [8] yields

$$1 - \frac{1}{p} \le \chi_p(\mathbf{e}, n) \le 1 + \frac{1}{p}. \tag{33}$$

Further, whenever $n + 1 \in \mathfrak{A}$, then n is in one of the classes 2, 3 or 6 modulo 8, so that $x_1^2 + x_2^2 + x_3^2 \equiv n \bmod 8$ has a solution with $x_1 = 1$. An argument similar to that in the ultimate paragraph in Section 5 now shows that $\chi_2(\mathbf{e}, n) > 1/512$. For $n + 1 \in \mathfrak{A}$ this gives $\chi_p(\mathbf{e}, n) > 0$ for all p, and for these n we may now define

$$\omega(\mathbf{c}, n) = \prod_{p\mid c_1c_2c_3} \frac{\chi_p(\mathbf{c}, n)}{\chi_p(\mathbf{e}, n)}. \tag{34}$$

For $p \nmid c_1c_2c_3$, the substitution $y_i = c_ix_i$ in (30) shows that $\chi_p(\mathbf{c}, n) = \chi_p(\mathbf{e}, n)$. Hence, by (32) and (34), we have

$$\mathfrak{S}(\mathbf{c}, n) = \mathfrak{S}(n)\omega(\mathbf{c}, n). \tag{35}$$

Finally, by (31)–(33), the singular product $\mathfrak{S}(n)$ factors into a Dirichlet L-function to a quadratic character modulo $4n$ at 1 and a product over primes $p \mid 2n$ of factors satisfying (33) when p is odd. Hence, for $n + 1 \in \mathfrak{A}$, Siegel's theorem [7] yields

$$\mathfrak{S}(n) \gg n^{-\varepsilon}. \tag{36}$$

LEMMA 9. *Let $n + 1 \in \mathfrak{A}$, and let $c_1, c_2, c_3 \in \mathbb{N}$ with $\mu(\mathbf{c})^2 = 1$ and $c_1c_2c_3 \in \mathscr{U}$. Then, whenever $c_1c_2c_3 \le n^{1/8}$, one has*

$$r_{\mathbf{c}}(n) = \frac{\pi n^{1/2}}{4c_1c_2c_3}\mathfrak{S}(\mathbf{c}, n) + O\big(n^{13/28+\varepsilon}(c_1c_2c_3)^{5/2}\big).$$

Proof. This is similar to [2, Lemma 2.2]. First suppose that $c_1c_2c_3$ is even. Then, by hypotheses, at least two of the c_j are even. By symmetry, we may suppose that c_1 and c_2 are even. Further, $n+1 \in \mathfrak{A}$ implies that n is in one of the congruence classes 2, 3 or 6 modulo 8. It follows that $c_1^2x_1^2 + c_2^2x_2^2 + c_3^2x_3^2 \equiv n \bmod 4$ has no solution $\mathbf{x} \in \mathbb{Z}^3$, and consequently $r_{\mathbf{c}}(n) = \chi_2(\mathbf{c}, n) = 0$. By (32), this confirms the claim in the lemma.

Next suppose that $c_1c_2c_3$ is odd. Then, since $\mu(\mathbf{c})^2 = 1$, it follows from [4, (102:10)] that the spinor genus of $c_1^2x_1^2 + c_2^2x_2^2 + c_3^2x_3^2$ coincides with the genus of this form. According to Siegel [8], the average of representations in a genus is the product of local densities. Also $4 \nmid n$, so that Blomer [1, (2.8)] is applicable. On combining this with the aforementioned result of Siegel, we find that the estimate

(37)
$$\#\{\mathbf{x} \in \mathbb{Z}^3 : c_1^2x_1^2+c_2^2x_2^2+c_3^2x_3^2 = n\} = \frac{2\pi n^{1/2}}{c_1c_2c_3}\mathfrak{S}(\mathbf{c}, n) + O\big(n^{13/28+\varepsilon}(c_1c_2c_3)^{5/2}\big)$$

holds uniformly for all $\mathbf{c}$ with $\mu(\mathbf{c})^2 = 1$ and $c_1c_2c_3 \le n^{1/8}$. The left hand side of (37) differs from $8r_{\mathbf{c}}(n)$ by the number of solutions of $c_1^2x_1^2+c_2^2x_2^2+c_3^2x_3^2 = n$ with at least one of x_1, x_2, x_3 equal to 0, and by Lemma 1 the latter is bounded by $O(n^{\varepsilon})$, uniformly in $\mathbf{c}$. This establishes the lemma. ∎

We are ready to proceed to an asymptotic formula for $R_3(n)$. The procedure is similar to that used in Section 4. We take $s = 3$ and $\theta = 1/600$ in (8), and apply Lemma 9 to replace $r_{\mathbf{c}}(n)$. This is possible because by Lemma 3 we see that $c_1c_2c_3 \le n^{6\theta}$ for all $\mathbf{c}$ that occur on the right hand side of (8). It follows that whenever $n+1 \in \mathfrak{A}$, then

$$R_3(n) = \sum_{|\mathbf{d}| \le n^{\theta}} \mu(\mathbf{d}) \bigg(\frac{\pi n^{1/2}}{4c_1c_2c_3}\mathfrak{S}(\mathbf{c}, n) + O\big(n^{13/28+\varepsilon}(c_1c_2c_3)^{5/2}\big) \bigg) + O(n^{1-\theta+\varepsilon}).$$

We use the bound $c_1c_2c_3 \le n^{6\theta}$ again and apply (34) to simplify this to

$$R_3(n) = \frac{\pi}{4}\mathfrak{S}(n)n^{1/2} \sum_{|\mathbf{d}| \le n^{\theta}} \frac{\mu(\mathbf{d})\omega(\mathbf{c}, n)}{c_1c_2c_3} + O(n^{1-\theta+\varepsilon}). \tag{38}$$

Lemma 10. *For natural numbers n with $n+1 \in \mathfrak{A}$ the multiple series*

$$W(n) = \sum_{\mathbf{d} \in \mathbb{N}^3} \mu(\mathbf{d})^2 |\mathbf{d}|^{1/2} \frac{\omega(\mathbf{c}, n)}{c_1c_2c_3}$$

converges, and $W(n) \ll n^{\varepsilon}$.

With this lemma in hand, we deduce that the series

$$\mathfrak{T}(n) = \sum_{\mathbf{d} \in \mathbb{N}^3} \mu(\mathbf{d}) \frac{\omega(\mathbf{c}, n)}{c_1c_2c_3} \tag{39}$$

converges absolutely, and that it differs from the sum on the right hand side of (38) by an amount not exceeding $O(n^{-\theta/3})$. From (38) we now deduce the following.

THEOREM 3. *Let $n+1 \in \mathfrak{A}$. Then*

$$R_3(n) = \frac{\pi}{4}\mathfrak{S}(n)\mathfrak{T}(n)n^{1/2} + O(n^{999/2000}).$$

The proof of Lemma 10 depends on estimates for $\omega(\mathbf{c}, n)$ that we now derive. Suppose that $n+1 \in \mathfrak{A}$ and $\mu(\mathbf{c})^2 = 1$. Let $\mathbf{e}_1(p) = (p, 1, 1)$, $\mathbf{e}_2 = (p, p, 1)$ and $\mathbf{e}_3(p) = (p, p, p)$. Then, as on p. 510 of [2], one infers from (30) and (34) that

$$\omega(\mathbf{c}, n) = \prod_{p^\nu \mid c_1c_2c_3} \frac{\chi_p(\mathbf{e}_\nu(p), n)}{\chi_p(\mathbf{e}, n)}. \tag{40}$$

Whenever $\mathbf{c}$ is the image of some $\mathbf{d}$, then $c_1c_2c_3 \in \mathscr{U}$ (by Lemma 3), so that it suffices to consider $\chi_p(\mathbf{e}_\nu(p), n)$ for $\nu = 2$ and $\nu = 3$.

When $\nu = 3$ and $p^2 \nmid n$, it follows from (30) that $\chi_p(\mathbf{e}_3(p), n) = 0$. When $p^2 \mid n$, an appropriate rearrangement of (30) gives $\chi_p(\mathbf{e}_3(p), n) = p^2\chi_p(\mathbf{e}, n)$, and (33) then shows that $\chi_p(\mathbf{e}_3(p), n) \le 2p^2$. Now let $\nu = 2$ and $p \nmid n$. Then (30) shows that $\chi_p(\mathbf{e}_2(p), n) = 0$ unless $\left(\frac{n}{p}\right) = 1$. In this last case, the congruence $p^2x_1^2 + p^2x_2^2 + x_3^2 \equiv n \bmod p$ has exactly $2p^2$ solutions with $1 \le x_j \le p$ $(1 \le j \le 3)$, and an application of Hensel's lemma gives $\chi_p(\mathbf{e}_2(p), n) = 2$. Finally, consider the case $\nu = 2$ and $p \mid n$. Then, by (30), we have $\chi_p(\mathbf{e}_2(p), n) = 0$ unless the congruence $p^2x_1^2 + p^2x_2^2 + x_3^2 \equiv n \bmod p^h$ is soluble for any fixed h. This last condition implies $p \mid x_3$, and further that $p^2 \mid n$. Another obvious rearrangement in (30) now shows that $\chi_p(\mathbf{e}_2(p), n) = p\chi_p(\mathbf{e}, n/p^2)$. In particular, the bounds in (33) now suffice to conclude that there is a constant $C \ge 1$ with the property that

$$0 \le \omega(\mathbf{c}, n) \le \prod_{p^\nu \| c_1c_2c_3} \omega_\nu(p, n) \tag{41}$$

where $\omega_2(2, n) = \omega_3(2, n) = C$ and, for odd primes p,

$$\omega_2(p, n) = \begin{cases} 2(1-1/p)^{-2}, \\ p(1-1/p)^{-2}, \end{cases} \qquad \omega_3(p, n) = \begin{cases} 0 & \text{for } p^2 \nmid n, \\ Cp^2 & \text{for } p^2 \mid n. \end{cases}$$

We are ready to complete the proof of Lemma 10. As in the proof of Lemma 5, we note that (7) yields $|\mathbf{d}| \le (c_1c_2c_3)^{1/2}$, and that at most $(c_1c_2c_3)^\varepsilon$ triplets $\mathbf{d} \in \mathbb{N}^3$ with $\mu(\mathbf{d})^2 = 1$ produce the same $\mathbf{c}$. Hence, by the argument leading to (17),

$$W(n) \ll \sum_{c_1c_2c_3 \in \mathscr{U}} \mu(\mathbf{c}) \frac{\omega(\mathbf{c}, n)}{(c_1c_2c_3)^{3/4-\varepsilon}}.$$

We now combine (41) with the bounds obtained for $\omega(\mathbf{c},n)$ to infer that

$$W(n) \ll \sum_{u\in\mathscr{U}} u^{-5/7}g(u)$$

where g is the multiplicative function defined on $\mathscr{U}$ by $g(p^\nu)=\omega_\nu(p,n)$ whenever p is a prime. The required estimate now follows from

$$W(n) \ll \prod_p \big(1+p^{-10/7}g(p^2)+p^{-15/7}g(p^3)\big) \ll \prod_{p^2\mid n}(1+4p^{-3/7}+Cp^{-1/7}).$$

7. The correcting factor. In this section, we bound $\mathfrak{T}(n)$ from below, thereby establishing the case $s=3$ of Theorem 1. The first step is to convert $\mathfrak{T}(n)$ into an Euler product. We continue to import notation from Section 3, but set $s=3$. Thus, when $\mathbf{d}=(d_{12},d_{13},d_{23})\in\mathbb{N}^3$ with $\mu(\mathbf{d})^2=1$, we let $\mathbf{c}=(c_1,c_2,c_3)$ be the vector defined by (7). For $q\in\mathbb{N}$, let

$$\mathscr{D}(q)=\{\mathbf{d}\in\mathbb{N}^3 : \mu(\mathbf{d})^2=1,\ c_1c_2c_3=q\}. \tag{42}$$

By (7), we have $d_{ij}\mid q$ so that $\mathscr{D}(q)$ is a finite set. When $n+1\in\mathfrak{A}$, let

$$h(q,n)=\sum_{\mathbf{d}\in\mathscr{D}(q)}\mu(\mathbf{d})\omega(\mathbf{c},n). \tag{43}$$

On rearranging the absolutely convergent series (39) according to the value of $c_1c_2c_3$ we infer from (43) that

$$\mathfrak{T}(n)=\sum_{q=1}^{\infty}q^{-1}h(q,n).$$

Lemma 11. *For any $n+1\in\mathfrak{A}$, the function $h(q,n)$ is multiplicative in q. For $\nu=1$ and for $\nu\ge 4$ one has $h(p^\nu,n)=0$.*

From this lemma, we now conclude that

$$\mathfrak{T}(n)=\prod_p\left(1+\frac{h(p^2,n)}{p^2}+\frac{h(p^3,n)}{p^3}\right). \tag{44}$$

We now establish Lemma 11. At the same time, we will determine $h(p^2,n)$ and $h(p^3,n)$. First observe that the vectors $\mathbf{c}$ coming from some $\mathbf{d}$ via (7) have squarefree coordinates with $c_1c_2c_3$ squareful. Hence $\mathscr{D}(q)=\emptyset$ unless q is squareful and free of fourth powers. Next, we demonstrate that whenever $q=p^\nu q'$ with $p\nmid q'$, then

$$h(q,n)=h(p^\nu,n)h(q',n). \tag{45}$$

By induction on the number of prime factors, this suffices to confirm that $h(q,n)$ is multiplicative in q. Since $\mathscr{D}(q)=\emptyset$ implies $h(q,n)=0$, we see that (45) reduces to the trivial identity $0=0$ unless q is squareful and free from fourth powers. In this remaining case, we have $\nu=2$ or $\nu=3$, and

we proceed to compute $\mathscr{D}(p^2)$ and $\mathscr{D}(p^3)$ explicitly. When $c_1c_2c_3 = p^2$ with all c_j squarefree, then there are i, j with $1 \le i < j \le 3$ and $c_i = c_j = p$, and the remaining c_l is 1. By (7), we see that we must have $d_{ij} = p$, and that the remaining coordinates of $\mathbf{d}$ must be 1. Hence

$$\mathscr{D}(p^2) = \{(p,1,1),(1,p,1),(1,1,p)\}. \tag{46}$$

An analogous reasoning shows that $c_1c_2c_3 = p^3$ implies $\mathbf{c} = (p,p,p)$, and that this is possible only when at least two components of $\mathbf{d}$ equal p, the remaining one being p or 1. Hence

$$\mathscr{D}(p^2) = \{(p,p,1),(p,1,p),(1,p,p),(p,p,p)\}. \tag{47}$$

Now suppose that $q = p^2q'$ with $p \nmid q'$. If $c_1c_2c_3 = p^2q'$ with $\mu(\mathbf{c})^2 = 1$, then there is exactly one pair i, j with $1 \le i < j \le 3$ and $p \,|\, c_i$, $p \,|\, c_j$ but $p \nmid c_l$ where $\{i,j,l\} = \{1,2,3\}$. Write $c_i' = c_i/p$, $c_j' = c_j/p$, $c_l' = c_l$. Then $c_1'c_2'c_3' = q'$. Also, (7) shows that $p \nmid d_{ij}$, but p does not divide any other coordinate of $\mathbf{d}$. We may define $\mathbf{d}'$ as the vector obtained from $\mathbf{d}$ by replacing d_{ij} with d_{ij}/p. Then, by construction, $\mathbf{d}' \in \mathscr{D}(q')$, and unique factorisation implies that this defines a bijection

$$\mathscr{D}(q) \to \mathscr{D}(q') \times \mathscr{D}(p^2), \qquad \mathbf{d} \mapsto (\mathbf{d}', \mathbf{e}'),$$

where $\mathbf{e}' \in \mathscr{D}(p^2)$ is the vector that has i, j coordinate p. Since $\mu(\mathbf{d}') = -\mu(\mathbf{d})$ and $\mu(\mathbf{e}') = -1$, it follows from (43) that

$$h(q,n) = \sum_{\mathbf{d}' \in \mathscr{D}(q')} \sum_{\mathbf{e}' \in \mathscr{D}(p^2)} \mu(\mathbf{d}')\mu(\mathbf{e}')\omega(\mathbf{c},n).$$

By (40) we also see that $\omega(\mathbf{c},n) = \omega(\mathbf{c}',n)\omega((p,p,1),n)$. The identity (45) now follows immediately when $\nu = 2$. The case where $\nu = 3$ is very similar, and we may omit the details. This concludes the proof of Lemma 11.

To complete the discussion of $\mathfrak{T}(n)$, we note that it follows from (43), (46), (47) and (40) that

$$h(p^2,n) = -3\omega((p,p,1),n), \qquad h(p^3,n) = 2\omega((p,p,p),n).$$

By (43), this implies that

$$\mathfrak{T}(n) = \prod_p E_p(n)$$

where

$$E_p(n) = 1 - 3\frac{\omega(\mathbf{e}_2(p),n)}{p^2} + 2\frac{\omega(\mathbf{e}_3(p),n)}{p^3}.$$

We proceed to establish lower bounds for $E_p(n)$. First suppose that $p \ge 5$ and $p^2 \nmid n$. Then, by (41), we have $\omega(\mathbf{e}_3(p),n) \ge 0$ and $\omega(\mathbf{e}_2(p),n) \le$

$2p/(p-1)$ so that

$$E_p(n) \ge 1 - \frac{6}{p(p-1)}.$$

For $p \ge 5$ with $p^2 \mid n$ the same reasoning produces

$$E_p(n) \ge 1 - \frac{3}{(p-1)},$$

and consequently

$$\mathfrak{T}(n) \gg E_2(n)E_3(n)(\log n)^{-3}. \tag{48}$$

Now consider $E_3(n)$. Since $n+1 \in \mathfrak{A}$, we have $n \equiv 0$ or $2 \bmod 3$. If $n \equiv 2 \bmod 3$, then the argument preceding (41) shows that $\chi_3(\mathbf{e}_2(3), n) = 2$. Also, by (31), we have $\chi_3(\mathbf{e}, n) = 4/3$. It follows that $\omega(\mathbf{e}_2(3), n) = 3/2$ and $E_3(n) \ge 1/2$. This leaves the case where $3 \mid n$. If $3 \parallel n$ then it is immediate that $\chi_3(\mathbf{e}_2(3), n) = \chi_3(\mathbf{e}_3(3), n) = 0$, and this shows that $E_3(n) = 1$. Finally, when $9 \mid n$, it is also immediate from (30) that $\chi_3(\mathbf{e}_3(3), n) = 9\chi_3(\mathbf{e}, n/9)$. From (40) we then see that

$$E_3(n) = 1 - \frac{\chi_3(\mathbf{e}, n/9)}{\chi_3(\mathbf{e}, n)}.$$

By Lemma 16 of Siegel [8] we know that both $\chi_3(\mathbf{e}, n/9)$ and $\chi_3(\mathbf{e}, n)$ are in the interval $[2/3, 4/3]$ so that $E_3(n) \ge 2/3$. It has now been demonstrated for all n with $n+1 \in \mathfrak{A}$ one has $E_3(n) \ge 1/2$. The reader may check that for these n, a similar argument gives $E_2(n) \ge 2^{-7}$. We now deduce from (48) and (36) that $\mathfrak{S}(n)\mathfrak{T}(n) \gg n^{-\varepsilon}$ for all n with $n+1 \in \mathfrak{A}$. The conclusion in Theorem 1 concerning $R_3(n)$ now follows from Theorem 3.

References

[1] V. Blomer, *Ternary quadratic forms, and sums of three squares with restricted variables*, in: Anatomy of Integers, CRM Proc. Lecture Notes 46, Amer. Math. Soc., Providence, RI, 2008, 1–17.

[2] V. Blomer and J. Brüdern, *A three squares theorem with almost primes*, Bull. London Math. Soc. 37 (2005), 507–513.

[3] J. Brüdern and E. Fouvry, *Lagrange's four squares theorem with almost prime variables*, J. Reine Angew. Math. 454 (1994), 59–96.

[4] O. T. O'Meara, *Introduction to Quadratic Forms*, 3rd printing, Grundlehren Math. Wiss. 117, Springer, New York, 1973.

[5] H. E. Rose, *A Course in Number Theory*, 2nd ed., Oxford Univ. Press, Oxford, 1994.

[6] A. Schinzel, *On sums of four coprime squares*, Bull. Polish Acad. Sci. Math. 61 (2013), 109–111.

[7] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), 83–86.

[8] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. (2) 36 (1935), 527–606.
[9] R. C. Vaughan, *The Hardy–Littlewood Method*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.
[10] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer, Berlin, 1981.

Jörg Brüdern
Mathematisches Institut
Bunsenstrasse 3–5
D-37073 Göttingen, Germany
E-mail: bruedern@uni-math.gwdg.de

Received December 13, 2014 (8003)