DE GRUYTER OPEN

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/tmmp-2014-0015
Tatra Mt. Math. Publ. **59** (2014), 1–26

ON THE EQUATION $x_1^2 + x_2^2 + x_3^2 + x_4^2 = N$ WITH VARIABLES SUCH THAT $x_1x_2x_3x_4 + 1$ IS AN ALMOST-PRIME

T. L. Todorova* — D. I. Tolev**

ABSTRACT. We consider Lagrange's equation $x_1^2+x_2^2+x_3^2+x_4^2 = N$, where N is a sufficiently large and odd integer, and prove that it has a solution in natural numbers $x_1, \dots, x_4$ such that $x_1x_2x_3x_4 + 1$ has no more than 48 prime factors.

1. Introduction and statement of the result

In 1770 Lagrange proved that for any positive integer N the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = N \tag{1}$$

has a solution in integers $x_1, \dots, x_4$ and later Jacobi found an exact formula for the number of the solutions (see [6, Ch. 20]). Many researchers studied the equation (1) for solvability in integers satisfying additional conditions. There is a conjecture stating that if N is sufficiently large and $N \equiv 4 \pmod{24}$, then (1) has a solution in primes. This conjecture has not been proved so far, but several weaker statements have been established.

Greaves [5], Plaksin [15], Shields [16] and Kowalchik [13] considered (1) with two prime and two integer variables. Brüdern and Fouvry [2], Heath-Brown and Tolev [8], Tolev [17], Yinhchun Cai [18] studied (1) with multiplicative restrictions imposed on all of the variables—with four almost-primes or with one prime and three almost-primes. (We say that the integer n is an almost-prime of order r if n has at most r prime factors, counted with multiplicity. We denote by $\mathcal{P}_r$ the set of all almost-primes of order r).

2010 Mathematics Subject Classification: 11P05, 11N36.
Keywords: Lagrange's equation, almost-primes.
*Supported by Sofia University Grant 015/2014.
**Supported by Sofia University Grant 59/2014.

Y i n h c h u n C a i established in [18] the solvability of (1) in:

- x_1 prime and $x_2, x_3, x_4 \in \mathcal{P}_{42}$;
- x_1 prime and x_2, x_3, x_4 satisfying $x_2x_3x_4 \in \mathcal{P}_{121}$;
- $x_1, x_2, x_3, x_4 \in \mathcal{P}_{13}$;
- x_1, x_2, x_3, x_4 satisfying $x_1x_2x_3x_4 \in \mathcal{P}_{41}$.

We should also mention the result of B l o m e r and B r ü d e r n [1] which states that every sufficiently large integer, satisfying certain natural congruence conditions, can be represented in the form $x_1^2+x_2^2+x_3^2$ with integers $x_1, x_2, x_3 \in \mathcal{P}_{521}$. Later L ü G u a n g s h i [14] considered the same problem, but with integers such that $x_1x_2x_3 \in \mathcal{P}_{551}$. Obviously from these results one obtains information about the solvability of (1) in three almost-prime variables and one variable of any nature.

Having in mind the results mentioned above one may consider the following problem. For a given polynomial $f \in \mathbb{Z}[x_1, \dots, x_4]$ study the arithmetical properties of the integers $f(x_1, \dots, x_4)$, where $x_1, \dots, x_4$ are solutions of (1) and, in particular, study the solvability of (1) in integers $x_1, \dots, x_4$ such that $f(x_1, \dots, x_4)$ is an almost-prime of a given order.

In the present paper we consider the polynomial $f = x_1x_2x_3x_4 + 1$ and prove the following:

Theorem 1. *Suppose that N is a sufficiently large odd integer. Then the equation* (1) *has a solution in natural numbers $x_1, \dots, x_4$ such that $x_1x_2x_3x_4+1$ has no more than 48 prime factors. The number of such solutions is greater than $\frac{cN}{\log N}$ for some constant $c > 0$.*

A similar result holds if N is even, but having a large odd divisor. (If N is a power of 2 then, according to the Jacobi theorem [6, Ch. 20], the equation (1) has exactly 24 solutions in integers and in this case our method does not work). Using the method of the proof one may study this problem with an arbitrary polynomial $f \in \mathbb{Z}[x_1, \dots, x_4]$, satisfying certain natural conditions.

In the present paper we use the following notations.

We denote by N a sufficiently large odd integer. Letters a, b, k, l, m, n, v are always integers, q is a natural number and p is always a prime number. By $(n_1, \dots, n_k)$ we denote the greatest common divisor of $n_1, \dots, n_k$. If $q \in \mathbb{N}$ and $a \in \mathbb{Z}$, $(a, q) = 1$, then we denote by $\overline{(a)_q}$ the inverse of a modulo q, i.e., the solution of the congruence $ax \equiv 1 \pmod q$. If the value of the modulus is clear from the context then we write $\overline{a}$ for simplicity. If $p^l \mid m$, but $p^{l+1} \nmid m$, then we write $p^l \parallel m$. We denote by $\vec{n}$ four dimensional vectors and let

$$|\vec{n}| = \max(|n_1|, \dots, |n_4|). \tag{2}$$

For an odd q we denote by $\left(\frac{\cdot}{q}\right)$ the Jacobi symbol. As usual $\mu(q)$ is the Möbius function, $\varphi(q)$ is the Euler function and $\tau(q)$ is the number of positive divisors of q. Sometimes we write $a\equiv b(q)$ as an abbreviation of $a\equiv b\pmod q$. We write $\sum_{x(q)}$ for a sum over a complete system of residues modulo q and, respectively, $\sum_{x(q)^*}$ is a sum over a reduced system of residues modulo q. We also denote $e(t)=e^{2\pi it}$.

We use Vinogradov's notation $A\ll B$, which is equivalent to $A=O(B)$. If we have simultaneously $A\ll B$ and $B\ll A$ then we write $A\asymp B$. By ε we denote arbitrarily small positive number, which is not the same in different formulas. The constants in the O-terms and $\ll$-symbols are absolute or depend on ε.

2. Results about exponential and character sums and integrals

Consider first some classical exponential sums.

The Gauss sum is defined by

$$G(q,m,n)=\sum_{x\ (q)} e\left(\frac{mx^2+nx}{q}\right). \tag{3}$$

We denote also

$$G(q,m)=G(q,m,0). \tag{4}$$

The Gauss sum has the following properties.

If $(q,m)=d$, then

$$G(q,m,n)=\begin{cases} d\,G\left(\frac{q}{d},\frac{m}{d},\frac{n}{d}\right) & \text{if } d\mid n,\\ 0 & \text{otherwise.}\end{cases} \tag{5}$$

For any q we have

$$G(q,1)=\frac{1+i^{-q}}{1+i^{-1}}\sqrt{q}. \tag{6}$$

If $(q,2m)=1$, then

$$G(q,m,n)=e\left(-\frac{\overline{4m}\,n^2}{q}\right)\left(\frac{m}{q}\right)G(q,1). \tag{7}$$

If $2\nmid m$ and $k\ge 2$, then

$$G(2^k,m,n)=\begin{cases} e\left(-\frac{\overline{m}(n/2)^2}{2^k}\right)2^{\frac{k+1}{2}}c(m,k) & \text{if } 2\mid n,\\ 0 & \text{otherwise,}\end{cases} \tag{8}$$

where

$$c(m,k)=\begin{cases} \frac{1+i^m}{\sqrt{2}} & \text{if } 2\mid k,\\ e\left(\frac{m}{8}\right) & \text{if } 2\nmid k.\end{cases} \tag{9}$$

In particular, we have

$$c(m,k)^4 = -1. \tag{10}$$

If $p > 2$ is a prime, then for any m we have

$$\sum_{x \ (p)} \left(\frac{x}{p}\right) e\left(\frac{mx}{p}\right) = \left(\frac{m}{p}\right) G(p,1). \tag{11}$$

The proofs of formulas (5)–(11) are available in [3, Sec. 6] and [9, Ch. 7].

For $\vec{n} \in \mathbb{Z}^4$ we denote

$$G(q,m,\vec{n}) = \prod_{j=1}^{4} G(q,m,n_j). \tag{12}$$

The Kloosterman sum is defined by

$$K(q,m,n) = \sum_{x(q)^*} e\left(\frac{mx + n\overline{x}}{q}\right). \tag{13}$$

We use A. Weil's bound

$$|K(q,m,n)| \le \tau(q)\, q^{\frac{1}{2}}\, (q,m,n)^{\frac{1}{2}}. \tag{14}$$

A proof of (14) is available in [10, Ch. 11].

The Ramanujan sum is defined by

$$c_q(m) = K(q,m,0) \tag{15}$$

and we have

$$c_q(m) = \frac{\mu\left(\frac{q}{d}\right)}{\varphi\left(\frac{q}{d}\right)} \varphi(q), \qquad \text{where} \quad d = (q,m). \tag{16}$$

For a proof see [6, Ch. 16].

We need also an estimate for a special character sum. Suppose that $p > 2$ is a prime and $f \in \mathbb{F}_p[x]$ is a polynomial of degree k, which is not of the form $cg^2(x)$, where c is a constant and $g \in \mathbb{F}_p[x]$. Then we have

$$\left| \sum_{x \ (p)} \left(\frac{f(x)}{p}\right) \right| \le (k-1)\sqrt{p}. \tag{17}$$

For a proof we refer the reader to [10, Ch. 11].

Consider now some exponential integrals.

We take the infinitely many times differentiable function

$$\omega_0(t) = \begin{cases} \exp \frac{1}{\left(t-\frac{1}{2}\right)^2 - \frac{1}{16}} & \text{for } \ t \in \left(\frac{1}{4}, \frac{3}{4}\right), \\ 0 & \text{otherwise} \end{cases} \tag{18}$$

and define

$$J(\gamma, u) = \int_{-\infty}^{\infty} \omega_0(x)\, e(\gamma x^2 + ux)\, dx. \tag{19}$$

We have

$$J(\gamma, u) \ll \min\left(1, |\gamma|^{-\frac{1}{2}}\right). \tag{20}$$

A proof can be found for example in [11, Ch. 1].

For $\vec{u} \in \mathbb{R}^4$ we define

$$J(\gamma, \vec{u}) = \prod_{j=1}^{4} J(\gamma, u_j). \tag{21}$$

We specify the constant $\varkappa$ by

$$\varkappa = \int_{-\infty}^{\infty} e(-\gamma)\, J(\gamma, \vec{0})\, d\gamma. \tag{22}$$

Using the standard technique of the circle method (see for example [11, Ch. 11]) one can establish that

$$\varkappa > 0. \tag{23}$$

If $\vec{u} \in \mathbb{R}^4$ and $|\vec{u}| > 0$ (see (2) for the definition of $|\vec{u}|$), then we have

$$\int_{-\infty}^{\infty} |J(\gamma, \vec{u})|\, d\gamma \ll |\vec{u}|^{-1+\varepsilon}. \tag{24}$$

The proof of this estimate is available in [8, Lemma 10].

3. Proof of the theorem

3.1. Beginning of the proof

We denote

$$P = \sqrt{N} \tag{25}$$

and let

$$\omega(t) = \omega_0\left(\frac{t}{P}\right), \tag{26}$$

where $\omega_0(t)$ is defined by (18).

Suppose that $\eta > 0$ is a constant, which will be specified later and let

$$z = N^{\eta}, \qquad P(z) = \prod_{2<p<z} p. \tag{27}$$

Consider the sum

$$\Gamma = \sum_{\substack{x_1^2+\dots+x_4^2=N \\ (x_1x_2x_3x_4+1,P(z))=1}} \omega(x_1)\dots\omega(x_4). \tag{28}$$

If we prove the inequality

$$\Gamma \gg \frac{N}{\log N}, \tag{29}$$

then we will establish that there is a constant $c>0$ such that the equation (1) has at least $\frac{cN}{\log N}$ solutions satisfying $\big(x_1x_2x_3x_4+1, P(z)\big)=1$ and such that $x_1x_2x_3x_4+1 \asymp N^2$. We also note that $2 \nmid x_1x_2x_3x_4+1$ because in the opposite case we would have $2 \nmid x_j$ for all j which would imply $2 \mid N$, but this contradicts our assumption. Hence for every such solution the integer $x_1x_2x_3x_4+1$ does not have prime factors less than z and therefore this integer has at most $2/\eta$ prime factors. So, to prove Theorem 1, we have to choose $\eta = \frac{1}{24}-\omega$, where $\omega>0$ is a sufficiently small constant, and to establish (29).

To find the lower bound (29) we apply the linear sieve and that is why we need information about the sums

$$F(N,d) = \sum_{\substack{x_1^2+\dots+x_4^2=N \\ x_1x_2x_3x_4+1\equiv 0 \ (d)}} \omega(x_1)\dots\omega(x_4), \tag{30}$$

where d is squarefree and odd. Applying the Kloosterman form of the Hardy--Littlewood circle method, we find that for small d the sum (30) can be approximated by the quantity

$$M(N,d) = \varkappa\, N\, a(N)\, \Psi(N,d), \tag{31}$$

where the terms in the right-hand side of (31) are defined as follows.

The constant $\varkappa$ is given by (22).

Further

$$a(N) = \prod_{p>2} \left(1+\frac{1}{p}\right)\left(1-\frac{1}{p^{1+\xi_p(N)}}\right), \tag{32}$$

where $\xi_p(N)$ is the non-negative integer defined by

$$p^{\xi_p(N)} \parallel N. \tag{33}$$

Next we have

$$\Psi(N,d) = \frac{\alpha(N,d)\,\mathcal{L}(N,d)}{d^3}, \tag{34}$$

where

$$\alpha(N,d) = \prod_{p\mid d} \left(1+\frac{1}{p}\right)^{-1}\left(1-\frac{1}{p^{1+\xi_p(N)}}\right)^{-1} \tag{35}$$

and where $\mathcal{L}(N,d)$ is the number of solutions of the system of congruences

$$b_1^2 + \cdots + b_4^2 \equiv N \pmod{d}, \qquad b_1 b_2 b_3 b_4 + 1 \equiv 0 \pmod{d}. \tag{36}$$

We denote by $R(N,d)$ the error which arises when we approximate $F(N,d)$ by $M(N,d)$, that is

$$F(N,d) = M(N,d) + R(N,d). \tag{37}$$

To prove our theorem we have to study the arithmetic properties of the main term and to estimate the error term.

3.2. An estimate for a special exponential sum

An important role in our analysis plays the exponential sum

$$\begin{aligned} V_q &= V_q(N,d,v,\vec{b},\vec{n}) \\ &= \sum_{a\ (q)^*} e\left(\frac{a(b_1^2 + \cdots + b_4^2 - N) + \overline{a}v}{q}\right) G(q, ad^2, 2ad\vec{b} + \vec{n}), \end{aligned} \tag{38}$$

where $\vec{b} = \langle b_1, \ldots, b_4\rangle \in \mathbb{Z}^4$. It is analogous to the sum, considered in [2, Sec. 1].

To estimate $V_q(N,d,v,\vec{b},\vec{n})$ we use the properties of the Gauss sum and the Kloosterman sum and prove following:

Lemma 1. *Suppose that $N,d,q \in \mathbb{N}$, $v \in \mathbb{Z}$, $2 \nmid Nd$, $\mu^2(d) = 1$ and $\vec{n} = \langle n_1, \ldots, n_4\rangle \in \mathbb{Z}^4$, $\vec{b} = \langle b_1, \ldots, b_4\rangle \in \mathbb{Z}^4$. Then we have*

$$V_q(N,d,v,\vec{b},\vec{n}) \ll \tau(q)\, q^{\frac{5}{2}}\, (q,N)^{\frac{1}{2}}\, (q, N - b_1^2 - \cdots - b_4^2)^{\frac{1}{2}}\, (q,d^2)^2, \tag{39}$$

where the constant in the $\ll$-symbol is absolute. Further, if some of the conditions

$$(q,d) \mid n_j, \qquad j = 1, \ldots, 4 \tag{40}$$

do not hold, then $V_q(N,d,v,\vec{b},\vec{n}) = 0$.

Proof. Suppose that $(q,d) \nmid n_j$ for some j. It follows from (5) that

$$G(q, ad^2, 2adb_j + n_j) = 0$$

and having in mind (12) and (38) we see that $V_q = 0$.

From this point onwards we assume that (40) holds and we begin the proof of (39).

First we note that the sum V_q is multiplicative with respect to q in the following sense: If $(q', q'') = 1$, then we have

$$\begin{aligned} &V_{q'q''}(N,d,v,\vec{b},\vec{n}) \\ &= V_{q'}\left(N, q''d, \overline{(q'')_{q'}}^2 v, \vec{b}, \vec{n}\right)\, V_{q''}\left(N, q'd, , \overline{(q')_{q''}}^2 v, \vec{b}, \vec{n}\right). \end{aligned} \tag{41}$$

We leave the routine calculations to the reader.

Having in mind the identity (41) we see that it is enough to estimate $V_{p^s}(N, Ad, Bv, \vec{b}, \vec{n})$, where $A, B \in \mathbb{Z}$ and $p \nmid A$.

Consider first the case $p > 2$, $p \nmid d$. Applying (7) we find

$$G\left(p^s, aA^2d^2, 2aAdb_j + n_j\right) = e\left(-\frac{\overline{4aA^2d^2}n_j^2 + \overline{Ad}n_jb_j + ab_j^2}{p^s}\right)\left(\frac{a}{p^s}\right)G(p^s, 1).$$

Therefore, using (6), (12), (13) and (38) we get

$$V_{p^s}(N, Ad, Bv, \vec{b}, \vec{n}) = p^{2s}\, e\left(-\frac{\overline{Ad}(n_1b_1 + \cdots + n_4b_4)}{p^s}\right) K\left(p^s, -N, M\right), \tag{42}$$

where

$$M \equiv Bv - \overline{4A^2d^2}(n_1^2 + \cdots + n_4^2) \pmod{p^s}.$$

Using (14) and (42) we find

$$|V_{p^s}(N, Ad, Bv, \vec{b}, \vec{n})| \le (s+1)\left(p^s\right)^{\frac{5}{2}}\left(p^s, N\right)^{\frac{1}{2}} \qquad \text{for} \quad p \nmid 2d. \tag{43}$$

Consider now the case $p \mid d$. Since d is squarefree, we may write

$$d = pd', \qquad \text{where} \quad p \nmid d'. \tag{44}$$

If $s = 1$ then, using (40), we see that $G\left(p, aA^2d^2, 2aAdb_j + n_j\right) = p$ and, having in mind (12), we find $G(p, aA^2d^2, 2aAd\vec{b} + \vec{n}) = p^4$. Therefore, from (13) and (38) it follows that

$$V_p(N, Ad, Bv, \vec{b}, \vec{n}) = p^4 K\left(p, b_1^2 + \cdots + b_4^2 - N, Bv\right).$$

Noting that $(p, d^2) = p$ and using (14) we find

$$|V_p(N, Ad, Bv, \vec{b}, \vec{n})| \le 2p^{\frac{5}{2}}\left(p, N - b_1^2 - \cdots - b_4^2\right)^{\frac{1}{2}}\left(p, d^2\right)^2 \qquad \text{for} \quad p \mid d. \tag{45}$$

In the case $s \ge 2$ we use the following observation. From (5) it follows that

$$G\left(p^s, aA^2d^2, 2aAdb_j + n_j\right) = 0$$

unless

$$\left(p^s, aA^2d^2\right) \mid 2aAdb_j + n_j.$$

Since $p \nmid aA^2$, we see that the later condition is equivalent to

$$\left(p^s, d^2\right) \mid 2aAdb_j + n_j. \tag{46}$$

(The last formula implies, in particular, that $p \mid n_j$, but we already know this because of the assumption (40)). Hence we may write

$$n_j = pn_j', \quad n_j' \in \mathbb{Z}, \quad 1 \le j \le 4 \tag{47}$$

because otherwise $V_q = 0$.

Suppose that $s=2$. Then from (46) it follows that $p^2 \mid 2aAdb_j+n_j$, hence using (12) we get

$$G\big(p^2, aA^2d^2, 2aAd\vec{b}+\vec{n}\big)=p^8.$$

Now we take into account (13) and (38) to find

$$V_{p^2}(N, Ad, Bv, \vec{b}, \vec{n})=p^8K\big(p^2, b_1^2+\cdots+b_4^2-N, Bv\big).$$

Noting that $(p^2, d^2)=p^2$ and using (14) we find

$$\begin{aligned}&|V_{p^2}(N, Ad, Bv, \vec{b}, \vec{n})|\\ &\le 3(p^2)^{\frac{5}{2}}\big(p^2, N-b_1^2-\cdots-b_4^2\big)^{\frac{1}{2}}\big(p^2, d^2\big)^2 \qquad \text{for} \quad p\mid d. \end{aligned} \tag{48}$$

Consider now the case $s\ge 3$. Having in mind (44), (46) and (47) we denote

$$\frac{2aAd'b_j+n_j'}{p}=h_j\in\mathbb{Z}. \tag{49}$$

Using that $(p^s, d^2)=p^2$ and applying (5) we find

$$\begin{aligned}G\big(p^s, aA^2d^2, 2aAdb_j+n_j\big)&=p^2\,G(p^{s-2}, aA^2d'^2, h_j)\\ &=p^2e\left(-\frac{\overline{(4aA^2d'^2)_{p^{s-2}}}h_j^2}{p^{s-2}}\right)\left(\frac{a}{p^{s-2}}\right)G(p^{s-2}, 1).\end{aligned}$$

It is obvious that $\overline{(M)_{p^{s-2}}}\equiv\overline{(M)_{p^s}} \pmod{p^{s-2}}$ for any integer M with $p\nmid M$. Hence, using the definition of h_j given by (49), we find

$$\begin{aligned}&G\big(p^s, aA^2d^2, 2aAdb_j+n_j\big)\\ &=p^2e\left(-\frac{\overline{4aA^2d'^2}n_j'^2+\overline{Ad'}n_j'b_j+ab_j^2}{p^s}\right)\left(\frac{a}{p^{s-2}}\right)G\big(p^{s-2}, 1\big),\end{aligned}$$

where the inverses are already taken modulo p^s. Therefore, using (6) and (12) we find

$$\begin{aligned}&G\big(p^s, aA^2d^2, 2aAd\vec{b}+\vec{n}\big)\\ &=p^{2s+4}e\left(-\frac{\overline{4aA^2d'^2}\sum_{j=1}^4 n_j'^2+\overline{Ad'}\sum_{j=1}^4 n_j'b_j+a\sum_{j=1}^4 b_j^2}{p^s}\right).\end{aligned}$$

From this formula, (13) and (38) we find

$$V_{p^s}(N, Ad, Bv, \vec{b}, \vec{n})=p^{2s+4}e\left(-\frac{\overline{Ad'}\sum_{j=1}^4 n_j'b_j}{p^s}\right)K(p^s, -N, M),$$

where $M\equiv Bv-\overline{4A^2d'^2}\sum_{j=1}^4 n_j'^2 \pmod{p^s}$. Therefore, using (14) we obtain

$$|V_{p^s}(N, Ad, Bv, \vec{b}, \vec{n})|\le (s+1)(p^s)^{\frac{5}{2}}(p^s, N)^{\frac{1}{2}}\big(p^s, d^2\big)^2 \quad \text{for} \quad p\mid d,\ s\ge 3. \tag{50}$$

Combining (43), (45), (48) and (50) we see that for any prime $p \nmid 2A$ and for any positive integer s we have

$$\begin{aligned}&|V_{p^s}(N, Ad, Bv, \vec{b}, \vec{n})| \\ &\le \tau(p^s)(p^s)^{\frac{5}{2}}\big(p^s, N - b_1^2 - \cdots - b_4^2\big)^{\frac{1}{2}}(p^s, N)^{\frac{1}{2}}\big(p^s, d^2\big)^2. \end{aligned} \tag{51}$$

Consider now the case $p = 2$. We have $2 \nmid dN$ and suppose also that $2 \nmid A$. We shall prove that for all positive integers s we have

$$|V_{2^s}(N, Ad, Bv, \vec{b}, \vec{n})| \le 4(s+1)\,(2^s)^{\frac{5}{2}}. \tag{52}$$

From (38) it follows that (52) is obvious for $s = 1$. Suppose now that $s \ge 2$. From (8), (12) and (38) we see that V_{2^s} vanishes if $2 \nmid n_j$ for some j. Hence we may assume that $2 \mid n_j$ for all j, so we may write

$$n_j = 2n_j', \qquad \text{where} \quad n_j' \in \mathbb{Z}, \quad 1 \le j \le 4.$$

Using these formulas, as well as (8) and (10), it is easy to verify that

$$\begin{aligned}&G\big(2^s, aA^2d^2, 2aAd\vec{b} + \vec{n}\big) \\ &= -2^{2s+2}e\left(-\frac{\overline{Ad}(n_1b_1 + \cdots + n_4b_4)}{2^s}\right) \\ &\quad \times e\left(-\frac{\overline{aA^2d^2}({n_1'}^2 + \cdots + {n_4'}^2)}{2^s}\right)e\left(-\frac{a(b_1^2 + \cdots + b_4^2)}{2^s}\right).\end{aligned}$$

Hence using (13) and (38) we find

$$\begin{aligned}V_{2^s}(N, Ad, Bv, \vec{b}, \vec{n}) = &-2^{2s+2}\,e\left(-\frac{\overline{Ad}\,(n_1b_1 + \cdots + n_4b_4)}{2^s}\right) \\ &\times K\Big(2^s, -N, Bv - \overline{A^2d^2}\big({n_1'}^2 + \cdots + {n_4'}^2\big)\Big).\end{aligned}$$

It remains to apply (14) and we prove (52).

From (41), (51) and (52) we obtain (39) and the proof of the lemma is complete. □

3.3. The error term

In this section we study the quantity $R(N, d)$ defined by (37). Recall that $\mathcal{L}(N, d)$ is the number of $\vec{b} = \langle b_1, b_2, b_3, b_4\rangle \in \mathbb{Z}^4$ satisfying

$$1 \le b_1, b_2, b_3, b_4 \le d, \quad b_1b_2b_3b_4 + 1 \equiv 0 \pmod d, \quad b_1^2 + b_2^2 + b_3^2 + b_4^2 \equiv N \pmod d. \tag{53}$$

We prove the following

Lemma 2. *Suppose that N is sufficiently large, d is squarefree, $2\nmid dN$ and*

$$d\le N^{\frac{1}{12}}. \tag{54}$$

Then we have

$$R(N,d)\ll \mathcal{L}(N,d)\,N^{\frac{3}{4}+\varepsilon}. \tag{55}$$

P r o o f. We write the sum $F(N,d)$ specified by (30) in the form

$$F(N,d)=\sum_{\vec{b}(53)}\Phi(N,d,\vec{b}), \tag{56}$$

where the summation in (56) is taken over $\vec{b}$ satisfying (53) and where

$$\Phi(N,d,\vec{b}) \;=\sum_{\substack{x_1^2+\dots+x_4^2=N\\ x_i\equiv b_i(d),\ i=1,\dots,4}}\omega(x_1)\dots\omega(x_4). \tag{57}$$

We express the sum (57) as

$$\Phi(N,d,\vec{b})=\int_{\mathcal{I}} e(-N\alpha)\prod_{j=1}^{4}S_{d,b_j}(\alpha)\,d\alpha, \tag{58}$$

where the integration is taken over the interval $\mathcal{I}=\big((1+[P])^{-1},1+(1+[P])^{-1}\big]$ and

$$S_{d,b}(\alpha)\;=\sum_{\substack{x\in\mathbb{Z}\\ x\equiv b\,(d)}}\omega(x)e\big(\alpha x^2\big). \tag{59}$$

Using the properties of the Farey fractions (see [6, Ch. 3]) we represent $\mathcal{I}$ as an union of disjoint intervals in the following way:

$$\mathcal{I}=\bigcup_{q\le P}\ \bigcup_{\substack{1\le a\le q\\ (a,q)=1}}\mathfrak{L}(q,a), \tag{60}$$

where

$$\mathfrak{L}(q,a)=\left(\frac{a}{q}-\frac{1}{q(q+q')},\frac{a}{q}+\frac{1}{q(q+q'')}\right]$$

and where the integers q',q'' are specified by

$$P<q+q',q+q''\le q+P,\quad aq'\equiv 1\pmod q,\quad aq''\equiv -1\pmod q. \tag{61}$$

We apply (58), (60) and change the variable of integration to get

$$\Phi(N,d,\vec{b})=\sum_{q\le P}\sum_{\substack{a=1\\ (a,q)=1}}^{q}e\left(-\frac{aN}{q}\right)\int_{\mathfrak{M}(q,a)}e\left(-\beta N\right)\prod_{j=1}^{4}S_{d,b_j}\left(\frac{a}{q}+\beta\right)d\beta, \tag{62}$$

where

$$\mathfrak{M}(q,a)=\left(-\frac{1}{q(q+q')},\frac{1}{q(q+q'')}\right]. \tag{63}$$

Working as in the proof of [8, Lemma 12], we find that for $\beta \in \mathfrak{M}(q,a)$ we have

$$S_{d,b_j}\left(\frac{a}{q}+\beta\right) = \frac{P}{dq} e\left(\frac{ab_j^2}{q}\right) \sum_{|n|\le dP^{\varepsilon}} e\left(\frac{nb_j}{dq}\right) J\Big(\beta N, -\frac{nP}{dq}\Big) \times G(q, ad^2, 2ab_j d + n) + O\left(P^{-A}\right),$$

where $G(q,m,n)$ and $J(\gamma,u)$ are defined respectively by (3) and (19), A is an arbitrarily large constant, $\varepsilon > 0$ is arbitrarily small and the constant in the O-term depends only on A and ε. We leave the verification of the last formula to the reader.

Therefore we may write the integrand in (62) in the form

$$e(-\beta N)\frac{P^4}{d^4q^4} e\left(\frac{a(b_1^2+\cdots+b_4^2)}{q}\right) \sum_{|\vec{n}|\le dP^{\varepsilon}} e\left(\frac{n_1b_1+\cdots+n_4b_4}{dq}\right) J\Big(\beta N, -\frac{P}{dq}\vec{n}\Big) \times G\big(q, ad^2, 2ad\vec{b}+\vec{n}\big) + O\left(P^{-A}\right),$$

where $G(q,m,\vec{n})$ and $J(\beta,\vec{u})$ are defined respectively by (12) and (21) and where the meaning of $|\vec{n}|$ is explained in (2).

We substitute the above expression for the integrand in (62), change the variable $\beta N = \gamma$ and use (63) to find

$$\Phi(N,d,\vec{b}) = \tilde{\Phi}(N,d,\vec{b}) + O(1), \tag{64}$$

where

$$\tilde{\Phi}(N,d,\vec{b}) = \frac{P^2}{d^4}\sum_{q\le P} q^{-4} \sum_{\substack{a=1\\(a,q)=1}}^{q} e\left(\frac{a(b_1^2+\cdots+b_4^2-N)}{q}\right) \sum_{|\vec{n}|\le dP^{\varepsilon}} e\left(\frac{n_1b_1+\cdots+n_4b_4}{dq}\right) \times G(q, ad^2, 2ad\vec{b}+\vec{n}) \int\limits_{\mathfrak{N}(q,a)} e(-\gamma) J\left(\gamma, -\frac{P}{dq}\vec{n}\right) d\gamma \tag{65}$$

and where

$$\mathfrak{N}(q,a) = \left(-\frac{N}{q(q+q')}, \frac{N}{q(q+q'')}\right]. \tag{66}$$

We note that from (61) and (66) follows

$$\left(-\frac{P}{2q}, \frac{P}{2q}\right] \subset \mathfrak{N}(q,a) \subset \left[-\frac{P}{q}, \frac{P}{q}\right]. \tag{67}$$

Therefore we may represent the expression in (65) as

$$\tilde{\Phi}(N,d,\vec{b}) = \Phi'(N,d,\vec{b}) + \Phi''(N,d,\vec{b}), \tag{68}$$

where in $\Phi'(N,d,\vec{b})$ the integration is taken over $\gamma \in \left[-\frac{P}{2q}, \frac{P}{2q}\right]$ and, respectively, in $\Phi''(N,d,\vec{b})$ we integrate over $\gamma \in \mathfrak{N}(q,a) \setminus \left[-\frac{P}{2q}, \frac{P}{2q}\right]$.

Consider first $\Phi''(N,d,\vec{b})$. We change the order of summation over a and integration over γ. Using (67) we conclude that in the new expression for Φ'' the domain of integration is $\frac{P}{2q}\le|\gamma|\le\frac{P}{q}$ and in the domain of summation over a is imposed the additional condition $\mathfrak{N}(q,a)\ni\gamma$. The later condition may be expressed using the idea of K l o o s t e r m a n [12] and an explanation of this method is available also in [7, Sec. 3].

There exists a function $\sigma(v,q,\gamma)$, defined for $q\le P$, $|\gamma|\le\frac{P}{q}$, $-\frac{q}{2}<v\le\frac{q}{2}$, integrable with respect to γ, satisfying

$$|\sigma(v,q,\gamma)|\le(1+|v|)^{-1} \tag{69}$$

and also

$$\sum_{-\frac{q}{2}<v\le\frac{q}{2}} e\left(\frac{\overline{a}v}{q}\right)\sigma(v,q,\gamma)=\begin{cases}1 & \text{if } \gamma\in\mathfrak{N}(q,a),\\ 0 & \text{otherwise.}\end{cases} \tag{70}$$

Hence using (67) and (70) we may write Φ'' in the form

$$\Phi''(N,d,\vec{b})=\frac{P^2}{d^4}\sum_{q\le P}q^{-4}\sum_{|\vec{n}|\le dP^{\varepsilon}}e\left(\frac{n_1b_1+\cdots+n_4b_4}{dq}\right)\int\limits_{\frac{P}{2q}\le|\gamma|\le\frac{P}{q}}e(-\gamma)J\left(\gamma,-\frac{P}{dq}\vec{n}\right)$$
$$\times\sum_{\substack{a=1\\(a,q)=1}}^{q}e\left(\frac{a(b_1^2+\cdots+b_4^2-N)}{q}\right)G(q,ad^2,2ad\vec{b}+\vec{n})\sum_{-\frac{q}{2}<v\le\frac{q}{2}}e\left(\frac{\overline{a}v}{q}\right)\sigma(v,q,\gamma)\,d\gamma. \tag{71}$$

Now we change the order of integration and summation over v and use (38) to get

$$\Phi''(N,d,\vec{b})=\frac{P^2}{d^4}\sum_{q\le P}q^{-4}\sum_{|\vec{n}|\le dP^{\varepsilon}}e\left(\frac{n_1b_1+\cdots+n_4b_4}{dq}\right)\sum_{-\frac{q}{2}<v\le\frac{q}{2}}V_q(N,d,v,\vec{b},\vec{n})$$
$$\times\int\limits_{\frac{P}{2q}\le|\gamma|\le\frac{P}{q}}e(-\gamma)J\left(\gamma,-\frac{P}{dq}\vec{n}\right)\sigma(v,q,\gamma)\,d\gamma. \tag{72}$$

From (69) and (72) it follows that

$$\Phi''(N,d,\vec{b})\ll\frac{P^2}{d^4}\sum_{q\le P}q^{-4}\sum_{|\vec{n}|\le dP^{\varepsilon}}\sum_{-\frac{q}{2}<v\le\frac{q}{2}}\frac{|V_q(N,d,v,\vec{b},\vec{n})|}{1+|v|}$$
$$\times\int\limits_{\frac{P}{2q}\le|\gamma|\le\frac{P}{q}}\left|J\left(\gamma,-\frac{P}{dq}\vec{n}\right)\right|d\gamma.$$

Using (20) and (21) we find that the integral in the above formula is

$$\ll \int_{\frac{P}{2q}}^{\infty} \gamma^{-2} d\gamma \ll \frac{q}{P},$$

hence

$$\Phi''(N,d,\vec{b}) \ll \frac{P}{d^4} \sum_{q\le P} q^{-3} \sum_{|\vec{n}|\le dP^{\varepsilon}} \sum_{-\frac{q}{2}<v\le\frac{q}{2}} \frac{|V_q(N,d,v,\vec{b},\vec{n})|}{1+|v|}. \tag{73}$$

Next we apply the estimate for V_q given by the inequality (39) from Lemma 1. We also notice that the sum over v produces a factor $\log P$ and, having in mind that V_q vanishes unless the conditions (40) hold, we see that the summation over $\vec{n}$ produces a factor

$$\sum_{\substack{|\vec{n}|\le dP^{\varepsilon}\\ n_j\equiv 0\ ((q,d))\\ 1\le j\le 4}} 1 \ll \left(\frac{dP^{\varepsilon}}{(q,d)}\right)^4.$$

Therefore we find

$$\begin{aligned}\Phi''(N,d,\vec{b}) &\ll \frac{P^{1+\varepsilon}}{d^4} \sum_{q\le P} q^{-\frac12} \left(\frac{dP^{\varepsilon}}{(q,d)}\right)^4 (q,N)^{\frac12}\big(q,N-b_1^2-\cdots-b_4^2\big)^{\frac12}\big(q,d^2\big)^2\\ &\ll P^{1+\varepsilon} \sum_{q\le P} q^{-\frac12}(q,N)^{\frac12}\big(q,N-b_1^2-\cdots-b_4^2\big)^{\frac12}\\ &\ll P^{1+\varepsilon} \sum_{q\le P} q^{-\frac12}\Big(q,N\big(N-b_1^2-\cdots-b_4^2\big)\Big). \end{aligned}\tag{74}$$

For any positive integer M we have

$$\sum_{q\le P} q^{-\frac12}(q,M) \ll P^{\frac12}\tau(M) \tag{75}$$

(we leave the easy proof to the reader). From the conditions (53) and (54) imposed on d and b_j we find that $N-b_1^2-\cdots-b_4^2\in\mathbb{N}$. Hence using (74) and (75) we find

$$\Phi''(N,d,\vec{b}) \ll P^{\frac32+\varepsilon}. \tag{76}$$

Consider now $\Phi'(N,d,\vec{b})$. We remind that the expression for it is similar to the expression in the right-hand side of (65), but the integration is taken over the interval $\big[-\frac{P}{2q},\frac{P}{2q}\big]$. We have

$$\Phi'(N,d,\vec{b}) = \Phi_0(N,d,\vec{b}) + \Phi^*(N,d,\vec{b}), \tag{77}$$

where Φ_0 denotes the contribution of the terms with $\vec{n}=\vec{0}$, that is

$$\Phi_0(N,d,\vec{b})=\frac{P^2}{d^4}\sum_{q\le P}q^{-4}\sum_{a\ (q)^*}e\left(\frac{a(b_1^2+\cdots+b_4^2-N)}{q}\right)\times G\big(q,ad^2,2ad\vec{b}\big)\int\limits_{|\gamma|\le\frac{P}{2q}}e(-\gamma)J\left(\gamma,\vec{0}\right)d\gamma. \quad (78)$$

Respectively, Φ^* is the contribution coming from the other terms:

$$\Phi^*(N,d,\vec{b})=\frac{P^2}{d^4}\sum_{q\le P}q^{-4}\sum_{a\ (q)^*}e\left(\frac{a(b_1^2+\cdots+b_4^2-N)}{q}\right)\sum_{1\le|\vec{n}|\le dP^{\varepsilon}}e\left(\frac{n_1b_1+\cdots+n_4b_4}{dq}\right)\times G(q,ad^2,2ad\vec{b}+\vec{n})\int\limits_{|\gamma|\le\frac{P}{2q}}e(-\gamma)J\left(\gamma,-\frac{P}{dq}\vec{n}\right)d\gamma. \quad (79)$$

Consider first Φ^*. Using (38) and (79) we find

$$\Phi^*(N,d,\vec{b})\ll\frac{P^2}{d^4}\sum_{q\le P}q^{-4}\sum_{1\le|\vec{n}|\le dP^{\varepsilon}}|V_q(N,d,0,\vec{b},\vec{n})|\int\limits_{|\gamma|\le\frac{P}{2q}}\left|J\left(\gamma,-\frac{P}{dq}\vec{n}\right)\right|d\gamma.$$

We apply (24) to get

$$\int\limits_{|\gamma|\le\frac{P}{2q}}\left|J\left(\gamma,-\frac{P}{dq}\vec{n}\right)\right|d\gamma\ll\left(\frac{P}{qd}\,|\vec{n}|\right)^{-1+\varepsilon},$$

hence

$$\Phi^*(N,d,\vec{b})\ll\frac{P^{1+\varepsilon}}{d^3}\sum_{q\le P}q^{-3}\sum_{1\le|\vec{n}|\le dP^{\varepsilon}}\frac{|V_q(N,d,0,\vec{b},\vec{n})|}{|\vec{n}|}.$$

Now we apply Lemma 1 and find

$$\Phi^*(N,d,\vec{b})\ll\frac{P^{1+\varepsilon}}{d^3}\sum_{q\le P}\frac{(q,N)^{\frac12}\,(q,N-b_1^2-\cdots-b_4^2)^{\frac12}\,(q,d^2)^2}{q^{\frac12}}\sum_{\substack{1\le|\vec{n}|\le dP^{\varepsilon}\\ n_j\equiv0\ ((q,d))\\ 1\le j\le4}}\frac{1}{|\vec{n}|}. \quad (80)$$

It is clear that the sum over $\vec{n}$ in the expression above is

$$\ll \sum_{\substack{1\le n_4\le dP^{\varepsilon}\\ n_4\equiv 0((q,d))}} \frac{1}{n_4}\left(\sum_{\substack{|n|\le n_4\\ n\equiv 0((q,d))}} 1\right)^3 \ll \sum_{1\le h\le \frac{dP^{\varepsilon}}{(q,d)}} \frac{h^2}{(q,d)} \ll \frac{d^3P^{\varepsilon}}{(q,d)^4},$$

which, together with (80), gives

$$\begin{aligned}\Phi^*(N,d,\vec{b}) &\ll P^{1+\varepsilon}\sum_{q\le P}\frac{(q,N)^{\frac12}(q,N-b_1^2-\cdots-b_4^2)^{\frac12}}{q^{\frac12}}\\ &\ll P^{1+\varepsilon}\sum_{q\le P}\frac{(q,N(N-b_1^2-\cdots-b_4^2))}{q^{\frac12}}.\end{aligned}$$

The last expression coincides with the expression in (74), so we get

$$\Phi^*(N,d,\vec{b}) \ll P^{\frac32+\varepsilon}. \tag{81}$$

Consider now the quantity $\Phi_0(N,d,\vec{b})$, defined by (78). We use (21) and (38) to write it in the form

$$\Phi_0(N,d,\vec{b}) = \frac{P^2}{d^4}\sum_{q\le P}\frac{V_q(N,d,0,\vec{b},\vec{0})}{q^4}\int\limits_{|\gamma|\le\frac{P}{2q}} e(-\gamma)J(\gamma,\vec{0})\,d\gamma.$$

Using the estimate (20) we find that the integral in the above formula is equal to $\varkappa + O\left(\frac{q}{P}\right)$, where $\varkappa$ is defined by (22). We combine this with the estimate for V_q, given in Lemma 1, and working as above we get

$$\Phi_0(N,d,\vec{b}) = \varkappa\frac{P^2}{d^4}\sum_{q\le P}\frac{V_q(N,d,0,\vec{b},\vec{0})}{q^4} + O\left(P^{\frac32+\varepsilon}\right).$$

Now we extend the summation over q to infinity. Using again Lemma 1 and the estimate

$$\sum_{q>P}\frac{(q,N)^{\frac12}(q,N-b_1^2-\cdots-b_4^2)^{\frac12}}{q^{\frac32-\varepsilon}} \ll \sum_{q>P}\frac{\left(q,N(N-b_1^2-\cdots-b_4^2)\right)}{q^{\frac32-\varepsilon}} \ll P^{-\frac12+\varepsilon}$$

(we leave the details to the reader), we find

$$\Phi_0(N,d,\vec{b}) = \varkappa\frac{P^2}{d^4}\,\sigma(N,d,\vec{b}) + O\left(P^{\frac32+\varepsilon}\right), \tag{82}$$

where

$$\sigma(N,d,\vec{b}) = \sum_{q=1}^{\infty} A_q(N,d,\vec{b}), \quad A_q(N,d,\vec{b}) = \frac{V_q(N,d,0,\vec{b},\vec{0})}{q^4}. \tag{83}$$

From (64), (68), (76), (77), (81) and (82) we obtain

$$\Phi(N,d,\vec{b}) = \varkappa\frac{P^2}{d^4}\,\sigma(N,d,\vec{b}) + O\left(P^{\frac{3}{2}+\varepsilon}\right). \tag{84}$$

Now we use (56) and (84) to get

$$F(N,d) = \varkappa\frac{P^2}{d^4}\,\mathcal{H}(N,d) + O\left(\mathcal{L}(N,d)\,P^{\frac{3}{2}+\varepsilon}\right), \tag{85}$$

where

$$\mathcal{H}(N,d) = \sum_{\vec{b}\in\mathbb{Z}^4\,:\,(53)} \sigma(N,d,\vec{b}). \tag{86}$$

It remains to prove that

$$\mathcal{H}(N,d) = d^4 a(N)\Psi(N,d), \tag{87}$$

where $a(N)$ and $\Psi(N,d)$ are defined respectively by (32) and (34). If we establish this identity and use (31), (37) and (85) we obtain (55) and finish the proof of Lemma 2.

To prove (87) we find an explicit formula for $\sigma(N,d,\vec{b})$. We have already established that the series in (83) is absolutely convergent. Further, the function $A_q(N,d,\vec{a})$ is multiplicative with respect to q. Indeed, from (41) we find that if $(q',q'')=1$ then

$$V_{q'q''}(N,d,0,\vec{b},\vec{0}) = V_{q'}(N,q''d,0,\vec{b},\vec{0})\,V_{q''}(N,q'd,0,\vec{b},\vec{0}).$$

However it is easy to see that

$$V_{q'}(N,q''d,0,\vec{b},\vec{0}) = V_{q'}(N,d,0,\vec{b},\vec{0})$$

and

$$V_{q''}(N,q'd,0,\vec{b},\vec{0}) = V_{q''}(N,d,0,\vec{b},\vec{0})$$

and it remains to apply (83).

Hence we have

$$\sigma(N,d,\vec{b}) = \prod_p \chi_p(N,d,\vec{b}), \tag{88}$$

where

$$\chi_p(N,d,\vec{b}) = 1+\sum_{s=1}^{\infty} A_{p^s}(N,d,\vec{b}). \tag{89}$$

We shall now compute the quantities $\chi_p(N,d,\vec{b})$.

Consider first the case $p\nmid 2d$. A straightforward calculation, based on (6), (7), (12), (15), (38) and (83), shows that

$$A_{p^s}(N,d,\vec{b}) = p^{-2s}c_{p^s}(N).$$

Using (16) and (33) we find that

$$A_{p^s}(N,d,\vec{b}) = \begin{cases} 0 & \text{for } s \geq \xi_p(N)+2, \\ -\frac{1}{p^{\xi_p(N)+2}} & \text{for } s = \xi_p(N)+1, \\ \frac{1}{p^s} - \frac{1}{p^{s+1}} & \text{for } s \leq \xi_p(N). \end{cases} \tag{90}$$

(The third case in (90) is applicable only if $\xi_p(N) \geq 1$).

From (89) and (90) we find

$$\chi_p(N,d,\vec{b}) = \left(1+\frac{1}{p}\right)\left(1-\frac{1}{p^{\xi_p(N)+1}}\right) \quad \text{for } p \nmid 2d. \tag{91}$$

Suppose now that $p \mid d$. From (53) it follows that $p \mid N - b_1^2 - \cdots - b_4^2$ and using (5), (12), (38) and (83), we easily find that

$$A_p(N,d,\vec{b}) = p-1 \qquad \text{for } p \mid d. \tag{92}$$

Suppose now that $s \geq 2$. In this case we have $(p^s, ad^2) = p^2$. However $p \nmid b_j$ for any j because of the condition $d \mid b_1b_2b_3b_4 + 1$ imposed in (53). This implies that $p^2 \nmid 2adb_j$ and using (5) we find $G(p^s, ad^2, 2adb_j) = 0$. Therefore from (38) and (83) we find

$$A_{p^s}(N,d,\vec{b}) = 0 \qquad \text{for } s \geq 2, \ \ p \mid d. \tag{93}$$

From (89), (92) and (93) we obtain

$$\chi_p(N,d,\vec{b}) = p \qquad \text{for } p \mid d. \tag{94}$$

It remains to consider the case $p = 2$. Using (3), (8), (10), (15), (16), (38), (83) and our assumption $2 \nmid N$ we easily get

$$A_{2^s}(N,d,\vec{b}) = 0 \qquad \text{for } s \geq 1$$

(we leave the verification to the reader). This formula and (89) imply

$$\chi_2(N,d,\vec{b}) = 1. \tag{95}$$

From (88), (91), (94) and (95) we get

$$\sigma(N,d,\vec{b}) = d \prod_{p \nmid 2d} \left(1+\frac{1}{p}\right)\left(1-\frac{1}{p^{\xi_p(N)+1}}\right) \tag{96}$$

and bearing in mind the definitions (32) and (35) we obtain

$$\sigma(N,d,\vec{b}) = d\, a(N)\, \alpha(N,d). \tag{97}$$

From (34), (86) and (97) we find that the quantity $\mathcal{H}(N,d)$ satisfies (87) and the proof of Lemma 2 is complete. □

3.4. The main term

To apply the sieve method and prove the theorem we have to study the properties of the main term $M(N,d)$ defined by (31). We already mentioned that the constant $\varkappa$ satisfies (23). Further, from (32) we easily find

$$1 \ll a(N) \ll \log\log N. \tag{98}$$

More care is needed about the quantity $\Psi(N,d)$ defined by (34). We have the following

Lemma 3. *The function $\Psi(N,d)$ is multiplicative with respect to d. We also have*

$$\Psi(N,p) < 0.9 \qquad \textit{for} \qquad p > 2 \tag{99}$$

and

$$0 < \Psi(N,p) \qquad \textit{for} \qquad p > 1000. \tag{100}$$

Finally, for all z_1, z_2 with $2 < z_1 < z_2$ we have

$$\prod_{z_1 \le p < z_2} \big(1 - \Psi(N,p)\big)^{-1} \le \frac{\log z_2}{\log z_1}\left(1 + \frac{L}{\log z_1}\right), \tag{101}$$

where $L > 0$ is an absolute constant.

P r o o f. Obviously, the function $\alpha(N,d)$, defined by (35) is multiplicative with respect to d and it is easy to see that the same property possesses $\mathcal{L}(N,d)$, which, by definition, is the number of solutions of the system (36). This proves the multiplicativity of $\Psi(N,d)$.

We shall now study $\Psi(N,p)$ for $p > 2$.

It is easy to verify that for any prime $p > 2$ we have

$$\frac{3}{4} \le \alpha(N,p) \le \frac{9}{8}. \tag{102}$$

Consider $\mathcal{L} = \mathcal{L}(N,p)$. We shall prove that for $p > 2$ we have

$$\mathcal{L} \le 4(p-1)^2 \tag{103}$$

and

$$\big|\mathcal{L} - p^2\big| \le 30p^{\frac{3}{2}}. \tag{104}$$

Suppose that the integers $b_1, \dots, b_4$ satisfy

$$b_1^2 + \dots + b_4^2 \equiv N \pmod p, \quad b_1 b_2 b_3 b_4 + 1 \equiv 0 \pmod p.$$

From the second of these congruences we conclude that $b_4 \equiv -\overline{b_1 b_2 b_3} \pmod p$, hence $\mathcal{L}$ is equal to the number of triples $b_1, b_2, b_3 \in \{1, 2, \dots, p-1\}$ satisfying

$$b_1^2 + b_2^2 + b_3^2 + \overline{b_1 b_2 b_3}^{\,2} \equiv N \pmod p,$$

or equivalently,

$$b_1^2 b_2^2 b_3^2 \left(b_1^2 + b_2^2 + b_3^2 - N\right) + 1 \equiv 0 \pmod{p}. \tag{105}$$

For fixed b_1, b_2 there are at most 4 admissible values of b_3, hence (103) is correct.

Using the definition of $\Psi(N,p)$ given by (34) as well as (102), (103) we establish (99).

To establish (100) we first prove (104) in the following elementary way. For any integer a the number of solutions of $x^2 \equiv a \pmod{p}$ is equal to $1+\left(\frac{a}{p}\right)$, so we may write

$$\mathcal{L} = \sum_{\substack{a_1,a_2,a_3 \ (p)^* \\ (106)}} \left(1+\left(\frac{a_1}{p}\right)\right)\left(1+\left(\frac{a_2}{p}\right)\right)\left(1+\left(\frac{a_3}{p}\right)\right),$$

where the summation is taken over variables a_1, a_2, a_3 satisfying

$$a_1 a_2 a_3 \left(a_1 + a_2 + a_3 - N\right) + 1 \equiv 0 \pmod{p}. \tag{106}$$

It is clear that

$$\mathcal{L} = \mathcal{L}_1 + 3\mathcal{L}_2 + 3\mathcal{L}_3 + \mathcal{L}_4, \tag{107}$$

where $\mathcal{L}_1$ is the number of solutions of (106),

$$\mathcal{L}_2 = \sum_{\substack{a_1,a_2,a_3 \ (p)^* \\ (106)}} \left(\frac{a_1}{p}\right), \quad \mathcal{L}_3 = \sum_{\substack{a_1,a_2,a_3 \ (p)^* \\ (106)}} \left(\frac{a_1 a_2}{p}\right), \quad \mathcal{L}_4 = \sum_{\substack{a_1,a_2,a_3 \ (p)^* \\ (106)}} \left(\frac{a_1 a_2 a_3}{p}\right). \tag{108}$$

Consider $\mathcal{L}_4$. We use the identity

$$\sum_{h \ (p)} e\left(\frac{mh}{p}\right) = \begin{cases} p & \text{if } p \mid m, \\ 0 & \text{otherwise} \end{cases} \tag{109}$$

and find

$$\mathcal{L}_4 = \frac{1}{p} \sum_{h,a_1,a_2,a_3 \ (p)^*} \left(\frac{a_1 a_2 a_3}{p}\right) e\left(\frac{h\left(a_1 a_2 a_3 (a_1 + a_2 + a_3 - N) + 1\right)}{p}\right).$$

For fixed a_2, a_3, h we change the variable a_1 to a_4, where $a_1 a_2 a_3 \equiv a_4 \pmod{p}$. We find

$$\mathcal{L}_4 = \frac{1}{p} \sum_{h,a_2,a_3,a_4 \ (p)^*} \left(\frac{a_4}{p}\right) e\left(\frac{h\left(a_4 (\overline{a_2 a_3} a_4 + a_2 + a_3 - N) + 1\right)}{p}\right).$$

Next we change the variable h to t, where $h \equiv a_2 t \pmod p$, and use (3) to get

$$\begin{aligned}\mathcal{L}_4 &= \frac{1}{p} \sum_{t,a_2,a_3,a_4 \ (p)^*} \left(\frac{a_4}{p}\right) e\left(\frac{t\left(\overline{a_3}a_4^2 + a_4a_2^2 + (a_3a_4 - a_4N + 1)a_2\right)}{p}\right) \\ &= \frac{1}{p} \sum_{t,a_3,a_4 \ (p)^*} \left(\frac{a_4}{p}\right) e\left(\frac{t\overline{a_3}a_4^2}{p}\right) \big(G\big(p, ta_4, t(a_3a_4 - a_4N + 1)\big) - 1\big).\end{aligned}$$

Clearly, the contribution of the term -1 in the brackets above vanishes. Therefore, using (7) we find

$$\mathcal{L}_4 = \frac{G(p,1)}{p} \sum_{t,a_3,a_4 \ (p)^*} \left(\frac{t}{p}\right) e\left(\frac{t\left(\overline{a_3}a_4^2 - \overline{4a_4}(a_3a_4 - a_4N + 1)^2\right)}{p}\right).$$

We write the summation over t inside and applying (6) and (11) we find

$$\begin{aligned}\mathcal{L}_4 &= \frac{G^2(p,1)}{p} \sum_{a_3,a_4 \ (p)^*} \left(\frac{\overline{a_3}a_4^2 - \overline{4a_4}(a_3a_4 - a_4N + 1)^2}{p}\right) \\ &= (-1)^{\frac{p-1}{2}} \sum_{a_4 \ (p)^*} \left(\frac{a_4}{p}\right) \sum_{a_3 \ (p)} \left(\frac{4a_3a_4^3 - a_3^2(a_3a_4 - a_4N + 1)^2}{p}\right).\end{aligned}$$

We estimate the character sum over a_3 using (17) and find that its modulus does not exceed $3\sqrt{p}$. Hence we obtain

$$|\mathcal{L}_4| \le 3p^{\frac{3}{2}}. \tag{110}$$

Consider now $\mathcal{L}_3$. From (3), (106), (108) and (109) we find

$$\begin{aligned}\mathcal{L}_3 &= \frac{1}{p} \sum_{h,a_1,a_2,a_3 \ (p)^*} \left(\frac{a_1a_2}{p}\right) e\left(\frac{h\left(a_1a_2a_3(a_1 + a_2 + a_3 - N) + 1\right)}{p}\right) \\ &= \frac{1}{p} \sum_{h,a_1,a_2 \ (p)^*} \left(\frac{a_1a_2}{p}\right) e\left(\frac{h}{p}\right) \Big(G\big(p, ha_1a_2, ha_1a_2(a_1 + a_2 - N)\big) - 1\Big).\end{aligned}$$

Clearly, the contribution of the term -1 in the brackets above vanishes. Now we apply (7) to find

$$\mathcal{L}_3 = \frac{G(p,1)}{p} \sum_{h,a_1,a_2 \ (p)^*} \left(\frac{h}{p}\right) e\left(\frac{h\left(1 - \overline{4}a_1a_2(a_1 + a_2 - N)^2\right)}{p}\right).$$

We insert the summation over h inside and use (11) to get

$$\mathcal{L}_3 = \frac{G^2(p,1)}{p} \sum_{a_1,a_2 \ (p)^*} \left(\frac{1 - \overline{4} a_1 a_2 (a_1 + a_2 - N)^2}{p} \right).$$

Applying (17) for the sum over a_2 and having also in mind (6) we obtain

$$|\mathcal{L}_3| \le 3p^{\frac{3}{2}}. \tag{111}$$

In the same manner we consider $\mathcal{L}_2$ and find

$$|\mathcal{L}_2| \le 3p^{\frac{3}{2}}. \tag{112}$$

It remains to study $\mathcal{L}_1$. We use (109) and find

$$\begin{aligned} \mathcal{L}_1 &= \frac{1}{p} \sum_{a_1,a_2,a_3 \ (p)^*} \sum_{h \ (p)} e\left(\frac{h\left(a_1 a_2 a_3 (a_1 + a_2 + a_3 - N) + 1\right)}{p} \right) \\ &= \frac{(p-1)^3}{p} + \Delta, \end{aligned} \tag{113}$$

where

$$\Delta = \frac{1}{p} \sum_{h,a_1,a_2,a_3 \ (p)^*} e\left(\frac{h\left(a_1 a_2 a_3 (a_1 + a_2 + a_3 - N) + 1\right)}{p} \right).$$

Now we apply (3), (7) and (11) to get

$$\begin{aligned} \Delta &= \frac{1}{p} \sum_{h,a_1,a_2 \ (p)^*} e\left(\frac{h}{p}\right) \Big(G\big(p, h a_1 a_2, h a_1 a_2 (a_1 + a_2 - N)\big) - 1 \Big) \\ &= \frac{G(p,1)}{p} \sum_{h,a_1,a_2 \ (p)^*} \left(\frac{h a_1 a_2}{p}\right) e\left(\frac{h\left(1 - \overline{4} a_1 a_2 (a_1 + a_2 - N)^2\right)}{p} \right) + \frac{(p-1)^2}{p} \\ &= \frac{G^2(p,1)}{p} \sum_{a_1,a_2 \ (p)^*} \left(\frac{a_1 a_2 \left(4 - a_1 a_2 (a_1 + a_2 - N)^2\right)}{p} \right) + \frac{(p-1)^2}{p}. \end{aligned}$$

We estimate the sum over a_2 using (17) and having in mind (6) we get

$$|\Delta| \le 4p^{\frac{3}{2}}. \tag{114}$$

From (107), (110)–(114) we obtain (104).

The inequality (100) for $\Psi(N,p)$ follows from (34), (102) and (104).

It remains to prove (101). From (34), (35) and (104) we see that

$$\Psi(N,p) = \frac{p^2 + O(p^{\frac{3}{2}})}{p^3 (1 + \frac{1}{p})(1 - \frac{1}{p^{1+\xi_p(N)}})} = \frac{1}{p} + O\left(\frac{1}{p^{\frac{3}{2}}}\right), \tag{115}$$

with an absolute constants in the O-terms. We apply Mertens's prime number theorem (see [6, Ch. 22]) and after some simple calculations, which we leave to the reader, we establish (101). □

3.5. End of the proof of Theorem 1

Here we use the terminology and results from [4, Ch. 12].

We write the quantity $P(z)$ given by (27) in the form

$$P(z) = C_0\, P^*(z), \tag{116}$$

where

$$C_0 = \prod_{2<p<1000} p, \quad P^*(z) = \prod_{1000<p<z} p. \tag{117}$$

Suppose that

$$D = N^{\delta}, \quad 0 < \delta < \frac{1}{12} \tag{118}$$

and let $\lambda(d)$ be the lower bound Rosser weights of level D, hence

$$|\lambda(d)| \le 1; \quad \lambda(d) = 0 \qquad \text{for} \quad d > D \quad \text{or} \quad \mu^2(d) = 0. \tag{119}$$

Then for the sum Γ, defined by (28), we have

$$\begin{aligned}\Gamma &= \sum_{x_1^2+x_2^2+x_3^2+x_4^2=N} \omega(x_1)\dots\omega(x_4) \sum_{\delta\mid(x_1x_2x_3x_4+1,C_0)} \mu(\delta) \sum_{t\mid(x_1x_2x_3x_4+1,P^*(z))} \mu(t)\\ &\ge \sum_{x_1^2+x_2^2+x_3^2+x_4^2=N} \omega(x_1)\dots\omega(x_4) \sum_{\delta\mid(x_1x_2x_3x_4+1,C_0)} \mu(\delta) \sum_{t\mid(x_1x_2x_3x_4+1,P^*(z))} \lambda(t).\end{aligned}$$

Now we change the order of summation and find

$$\Gamma \ge \sum_{d\mid P(z)} \theta(d)\, F(N,d), \tag{120}$$

where $F(N,d)$ is defined by (30) and

$$\theta(d) = \sum_{\substack{\delta\mid C_0\\ t\mid P^*(z)\\ \delta t=d}} \mu(\delta)\lambda(t). \tag{121}$$

We apply (37) and (120) and find that

$$\Gamma \ge \Gamma_1 + R, \tag{122}$$

where

$$\Gamma_1 = \sum_{d\mid P(z)} \theta(d)\, M(N,d), \quad R = \sum_{d\mid P(z)} \theta(d)\, R(N,d). \tag{123}$$

From (119) and (121) we see that $\theta(d) \ll 1$ and also that $\theta(d)$ is supported on the set of squarefree odd integers $d \le C_0 D$. Therefore using Lemma 2 we get

$$R \ll \sum_{\substack{d \le C_0 D \\ 2 \nmid d}} \mu^2(d)\, |R(N,d)| \ll N^{\frac{3}{4}+\varepsilon} \sum_{\substack{d \le C_0 D \\ 2 \nmid d}} \mu^2(d)\, \mathcal{L}(N,d).$$

Having in mind (104) we see that for any squarefree odd d we have

$$\mathcal{L}(N,d) \le d^2 \prod_{p \mid d} \left(1 + 30 p^{-\frac{1}{2}}\right) \ll d^2 \tau(d).$$

Hence using (118) we get

$$R \ll D^3 N^{\frac{3}{4}+\varepsilon} \ll \frac{N}{\log^2 N}. \tag{124}$$

Consider now the sum Γ_1. Using (31) we write it as

$$\Gamma_1 = \varkappa N\, a(N)\, \Gamma_2, \tag{125}$$

where

$$\Gamma_2 = \sum_{d \mid P(z)} \theta(d)\, \Psi(N,d).$$

Using the muptiplicativity with respect to d of $\Psi(N,d)$ and having in mind (121) we find

$$\Gamma_2 = \sum_{\substack{\delta \mid C_0 \\ t \mid P^*(z)}} \mu(\delta)\lambda(t)\Psi(N,\delta t) = \Gamma_3\, \Gamma_4, \tag{126}$$

where

$$\Gamma_3 = \sum_{\delta \mid C_0} \mu(\delta)\, \Psi(N,\delta), \quad \Gamma_4 = \sum_{t \mid P^*(z)} \lambda(t)\, \Psi(N,t).$$

Using (99) and (117) we find

$$\Gamma_3 \;=\; \prod_{2<p<1000} (1 - \Psi(N,p)) \gg 1, \tag{127}$$

where the constant in Vinogradov's symbol is absolute.

Consider now Γ_4. We apply the lower bound linear sieve and having in mind the properties of $\Psi(N,d)$ mentioned in Lemma 3 we obtain

$$\Gamma_4 \ge \Pi(z) \left(f(s_0) + O\big((\log D)^{-\frac{1}{3}}\big)\right), \tag{128}$$

where

$$\Pi(z) \;=\; \prod_{1000<p<z} \big(1 - \psi(N,p)\big), \tag{129}$$

$$s_0 = \frac{\log D}{\log z} = \frac{\delta}{\eta} \tag{130}$$

and where $f(s)$ is the lower function of the linear sieve, for which we know that

$$f(s) = 2e^{\gamma} s^{-1} \log(s-1) \qquad \text{for} \quad s \in (2,3) \tag{131}$$

(γ is the Euler constant).

We choose

$$\eta = \frac{1}{24} - 10^{-4}, \quad \delta = \frac{1}{12} - 10^{-4}. \tag{132}$$

Then from (27), (115) and (132) it follows that

$$\Pi(z) \asymp (\log z)^{-1} \asymp (\log N)^{-1}. \tag{133}$$

On the other hand from (130) and (132) we find $s_0 \in (2,3)$ and having in mind (131) we find that

$$f(s_0) > 0. \tag{134}$$

From (118), (128), (133) and (134) we find

$$\Gamma_4 \gg (\log N)^{-1}$$

and having also in mind (98), (122), (124)–(127) we obtain (29). It remains to notice that for the number η given by (132) we have $48 < \frac{2}{\eta} < 49$ and the theorem is proved.

□

REFERENCES

[1] BLOMER, V.—BRÜDERN, J.: *A three squares theorem with almost primes*, Bull. London Math. Soc. **37** (2005), 507–513.

[2] BRÜDERN, J.—FOUVRY, E.: *Lagranges four squares theorem with almost prime variables*, J. Reine Angew. Math. **454** (1994), 59–96.

[3] ESTERMANN, T.: *A new application of the Hardy-Littlewood-Kloosterman method*, Proc. London Math. Soc. **12** (1962), 425–444.

[4] FRIEDLANDER, J.—IWANIEC, H.: *Opera de Cribro*, in: Amer. Math. Soc. Colloq. Publ., Vol. 57, Providence, RI, 2010.

[5] GRIEVES, G.: *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.

[6] HARDY, G. H.—WRIGHT, E. M.: *An Introduction to the Theory of Numbers* (5th ed.), Oxford Univ. Press, 1979.

[7] HEATH-BROWN, D. R.: *Cubic forms in ten variables*, Proc. London Math. Soc. **47** (1983), 225–257.

[8] HEATH-BROWN, D. R.—TOLEV, D. I.: *Lagranges four squares theorem with one prime and three almost-prime variables*, J. Reine Angew. Math. **558** (2003), 159–224.

[9] HUA, L. K.: *Introduction to Number Theory*. Springer, Berlin, 1982.

[10] IWANIEC, H.—KOWALSKI, E.: *Analytic Number Theory*, in: Amer. Math. Soc. Colloq. Publ., Vol. 53, Providence, RI, 2004.

[11] KARATSUBA, A. A.: *Basic Analytic Number Theory*. Springer, Berlin, 1993.

[12] KLOOSTERMAN, H. D.: *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta Math. **49** (1926), 407–464.

[13] KOWALCHIK, F. B.: *Analogues of the Hardy–Litlewood equation*, Zap. Nauchn. Sem. LOMI **116** (1982), 86–95.
[14] LÜ, G.: *Gauss's three squares theorem with almost prime variables*, Acta Arith. **128** (2007), 391–399.
[15] PLAKSIN, V. A.: *An asymptotic formula for the number of solutions of a nonlinear equation for prime numbers*, Math. USSR Izv. **18** (1982), 275–348.
[16] SHIELDS, P.: *Some Applications of the Sieve Methods in Number Theory*. Thesis, University of Wales, Cardiff, UK, 1979.
[17] TOLEV, D. I.: *Lagranges four squares theorem with variables of special type*, in: Proceedings of the Session in Analytic Number Theory and Diophantine Equations (D. R. Heath-Brown et al., eds.), Bonn, 2002, Bonner Math. Schriften, Vol. 360, Univ. Bonn, Bonn, 2003, 17 pp.
[18] CAI, Y.: *Lagranges four squares theorem with variables of special type*, Intern. J. Number Theory **6** (2010), 1801–1817.

Received June 22, 2014

T. L. Todorova
Faculty of Mathematics and Informatics
Sofia University "St. Kl. Ohridsky"
5 J. Bourchier
1164 Sofia
BULGARIA
E-mail: tlt@fmi.uni-sofia.bg

D. I. Tolev
Institute of Mathematica and
Informatics, BAS
8 Acad. G. Bonchev
1113 Sofia
BULGARIA

Faculty of Mathematics and Informatics
Sofia University "St. Kl. Ohridsky"
5 J. Bourchier
1164 Sofia
BULGARIA
E-mail: dtolev@fmi.uni-sofia.bg