ACTA ARITHMETICA
128.4 (2007)

Gauss's three squares theorem with almost prime variables

by

Guangshi Lü (Jinan)

1. Introduction and main results. Gauss proved that all integers n not of the form $4^k(8m+7)$ can be written as a sum of three integral squares, i.e.

$$n = x_1^2 + x_2^2 + x_3^2. \tag{1.1}$$

This is one of the most elegant and subtle theorems in number theory. It is also conjectured that (1.1) still holds if we restrict the variables to prime numbers, as long as there are no local obstructions and n is large enough. Here "no local obstructions" means

$$n \equiv 3 \pmod{24} \quad \text{and} \quad 5 \nmid n. \tag{1.2}$$

Current technology apparently lacks the power to establish this conjecture. However, various approximations to it have been studied. Let $E(N)$ denote the number of all positive integers $n \le N$ satisfying (1.2) that cannot be written as a sum of three squares of primes. Hua [6] proved that $E(N) \ll N \log^{-A} N$ for some positive integer A. The study of the size of $E(N)$ received attention of many authors, including Schwarz [10], Leung and Liu [7], Bauer, Liu and Zhan [1], Liu and Zhan [8], and Ren [9]. The best result is due to Harman and Kumchev [5]: $E(N) \ll N^{6/7+\varepsilon}$.

By using the vector sieve, the theory of theta functions and modular forms, Blomer and Brüdern [2] considered (1.1) with sufficiently large n satisfying $n \equiv 3 \pmod{24}$ with $5 \nmid n$. They found a lower bound on the number of solutions in integers x_i with no more than 521 prime factors each. For simplicity, throughout this paper we shall use P_r to denote an integer which has at most r prime factors. Thus their result implies that the equation (1.1) holds true provided that the product $x_1x_2x_3$ is P_{1563}.

2000 *Mathematics Subject Classification*: 11P32, 11P05, 11P55, 11N36.

Key words and phrases: three squares theorem, weighted sieve of dimension exceeding one, almost prime.

Supported by Tianyuan Mathematics Foundation (Grant No. 10526028), and by the NSF of China (Grant No. 10571107).

The goal of this note is to attack the problem in a different direction, i.e. to make the number of prime factors of the product $x_1x_2x_3$ as small as possible. Unlike [2], where the vector sieve is used, we shall use the weighted three-dimensional sieve procedure to study the equation (1.1). It turns out that the weighted sieve of dimension exceeding one gives more savings on the number of prime divisors of the product $x_1x_2x_3$, although not so good to reduce the number of prime divisors for the single variables x_j. This observation, together with a mean-value theorem proved in [2] (see Lemma 3.3 below), leads to the following result.

THEOREM 1.1. *Every sufficiently large integer n with $n \equiv 3 \pmod{24}$ and $5 \nmid n$ can be represented in the form* (1.1), *such that the product $x_1x_2x_3$ is P_{551}. Moreover if n is square-free, the equation* (1.1) *holds true provided that the product $x_1x_2x_3x_4$ is P_{397}.*

Notation. Throughout the paper we use boldface letters to denote three-dimensional integral vectors; for example, we write $\mathbf{x} = (x_1, x_2, x_3)$ and $\mathbf{l} = (l_1, l_2, l_3)$. The notation $p \mid n \Leftrightarrow p \mid m$ means that m and n have the same prime factors. We also use $p^v \parallel n$ to denote that $p^v \mid n$ but $p^{v+1} \nmid n$.

2. The weighted sieve of dimension exceeding one. In this section we recall some basic facts on the weighted sieve of dimension exceeding one. Let $\mathcal{A}$ be a finite integer sequence whose members are not necessarily all positive or distinct. Let $\mathcal{P}$ be a set of primes, $\mathcal{P}^c$ its complement with respect to the set of all primes, and suppose that no members of $\mathcal{A}$ has a prime factor from $\mathcal{P}^c$. Some basic assumptions about the pair $\mathcal{A}$ and $\mathcal{P}$ are required. Loosely speaking, we require the probability of a member a from $\mathcal{A}$ being divisible by a prime p from $\mathcal{P}$ to be no larger than κ/p on average, where $\kappa > 1$ is a constant. We also require $\mathcal{A}$ to be well distributed among the arithmetic progressions $0 \bmod d$ as a runs over an extensive range of square-free numbers coprime with $\mathcal{P}^c$.

Suppose there exists an approximation X to the cardinality $|\mathcal{A}|$ of $\mathcal{A}$ and a non-negative multiplicative arithmetic function $\omega(\cdot)$ satisfying

$$\omega(1) = 1, \quad \omega(p) = 0 \quad \text{if } p \in \mathcal{P}^c, \tag{2.1}$$

$$0 \le \omega(p) < p \quad \text{if } p \in \mathcal{P}, \tag{2.2}$$

and for some constants $\kappa > 1$, $A \ge 2$,

$$\prod_{z_1 \le p < z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \le \left(\frac{\log z}{\log z_1}\right)^{\kappa} \left(1 + \frac{A}{\log z_1}\right) \quad \text{if } 2 \le z_1 < z, \tag{2.3}$$

such that the remainders

$$R_d := |\{a \in \mathcal{A} : a \equiv 0 \pmod{d}\}| - \frac{\omega(d)}{d} X$$

are small on average in the sense that for some constants τ, $0 < \tau \le 1$, $A_1 \ge 1$ and $A_2 \ge 2$,

$$\sum_{\substack{d<X^\tau \\ (d,\mathcal{P}^c)=1}} \mu^2(d)4^{v(d)}|R_d| \le A_2 \frac{X}{(\log X)^{\kappa+1}}, \tag{2.4}$$

where $v(d)$ denotes the number of prime factors of d. Finally, we introduce a constant μ such that

$$\max_{a\in\mathcal{A}} |a| \le X^{\tau\mu}, \tag{2.5}$$

where τ is the constant in (2.4).

The following two lemmas are essentially Theorems 0 and 1 in Diamond, Halberstam and Richert [4].

LEMMA 2.1. *Let $\kappa > 1$ be given, and let $\sigma_\kappa(u)$ be the continuous solution of the differential-difference problem*

$$\begin{cases} u^{-\kappa}\sigma(u) = A_\kappa^{-1} & \text{for } 0 < u \le 2, \quad A_\kappa = (2e^\gamma)^\kappa \Gamma(\kappa+1), \\ (u^{-\kappa}\sigma(u))' = -\kappa u^{-\kappa-1}\sigma(u-2) & \text{for } 2 < u; \end{cases} \tag{2.6}$$

here γ denotes the Euler constant. Then there exist two numbers α_κ and β_κ satisfying

$$\alpha_\kappa \ge \beta_\kappa \ge 2$$

such that the simultaneous differential-difference system

$$\begin{cases} F(u) = 1/\sigma(u) & \text{for } 0 < u \le \alpha_\kappa, \\ f(u) = 0 & \text{for } 0 < u \le \beta_\kappa, \\ (u^\kappa F(u))' = \kappa u^{\kappa-1} f(u-1) & \text{for } u > \alpha_\kappa, \\ (u^\kappa f(u))' = \kappa u^{\kappa-1} F(u-1) & \text{for } u > \beta_\kappa, \end{cases} \tag{2.7}$$

has continuous solutions $F_\kappa(u)$ and $f_\kappa(u)$ with the properties that

$$F_\kappa(u) = 1 + O(e^{-u}), \qquad f_\kappa(u) = 1 + O(e^{-u}), \tag{2.8}$$

and $F_\kappa(u)$ and $f_\kappa(u)$, respectively, decreases and increases towards 1 as $u \to \infty$.

LEMMA 2.2. *Let $\mathcal{A}$ and $\mathcal{P}$ be as described above. For any two real numbers u and v satisfying*

$$\tau^{-1} < u < v, \qquad \beta_\kappa < \tau v,$$

we have

$$|\{P_r : P_r \in \mathcal{A}\}| \gg X \prod_{p<X^{1/v}} \left(1 - \frac{\omega(p)}{p}\right) \tag{2.9}$$

provided only that

$$r > \tau\mu u - 1 + \frac{\kappa}{f_\kappa(\tau v)} \int_1^{v/u} F_\kappa(\tau v - s)\left(1 - \frac{u}{v}\, s\right)\frac{ds}{s}. \tag{2.10}$$

3. Preliminaries. We want to sift the sequence

$$\mathcal{A} = \{x_1x_2x_3 : x_1^2 + x_2^2 + x_3^2 = n,\ x_i \in \mathbb{N}\}, \tag{3.1}$$

where $\mathbb{N}$ denotes the set of positive integers. Any sieve requires information on the distribution in arithmetic progressions of the sequence which is to be sifted. Therefore we write $\mathcal{A}_d$ for the set of all $a \in \mathcal{A}$ divisible by d, where d is a square-free integer. We want to establish the necessary approximation information on $|\mathcal{A}_d|$. To this end, we take the short cut of making use of the work of Blomer and Brüdern [2].

As in [2], for $n \equiv 3 \pmod 8$, we also introduce the sequences

$$\mathcal{B} = \{\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{N}^3 : x_1^2 + x_2^2 + x_3^2 = n\}, \tag{3.2}$$

$$\mathcal{B}_{\mathbf{l}} = \{\mathbf{x} = (x_1, x_2, x_3) \in \mathcal{B} : \mathbf{x} \equiv 0 \pmod{\mathbf{l}}\}, \tag{3.3}$$

where the boldface letter $\mathbf{l}$ denotes the vector (l_1, l_2, l_3) and the congruence $\mathbf{x} \equiv 0 \pmod{\mathbf{l}}$ means the simultaneous conditions

$$x_i \equiv 0 \pmod{l_i}, \qquad i = 1, 2, 3.$$

The theory of theta functions and modular forms suggest that the number of elements in $\mathcal{B}_{\mathbf{l}}$, which equals the number of solutions $\mathbf{y} \in \mathbb{N}^3$ of the equation

$$l_1^2y_1^2 + l_2^2y_2^2 + l_3^2y_3^2 = n,$$

has the main term

$$\frac{\pi}{4}\,\frac{n^{1/2}}{l_1l_2l_3}\sum_{q=1}^{\infty} q^{-3} \sum_{\substack{a=1\\(a,q)=1}}^{q} e\left(-\frac{an}{q}\right)\prod_{j=1}^{3} S(q, al_j^2), \tag{3.4}$$

where

$$S(q, a) = \sum_{x=1}^{q} e\left(\frac{ax^2}{q}\right). \tag{3.5}$$

We let

$$\mathfrak{G}(n, \mathbf{l}) = \sum_{q=1}^{\infty} q^{-3} \sum_{\substack{a=1\\(a,q)=1}}^{q} e\left(-\frac{an}{q}\right)\prod_{j=1}^{3} S(q, al_j^2), \qquad \mathfrak{G}(n) = \mathfrak{G}(n, (1, 1, 1)),$$

and

$$\omega(\mathbf{l}, n) = \mathfrak{G}(n, \mathbf{l})\mathfrak{G}(n)^{-1}. \tag{3.6}$$

Therefore we write

$$|\mathcal{B}_{\mathbf{l}}| = \frac{\omega(\mathbf{l},n)}{l_1l_2l_3}\,\frac{\pi}{4}\,\mathfrak{G}(n)n^{1/2} + R(n,\mathbf{l}), \tag{3.7}$$

where $R(n,\mathbf{l})$ is the assumed error term.

For the application of the sieve method it is important to investigate the behavior of the function $\omega(\mathbf{l},n)$. We let

$$A(q,\mathbf{l},n) = q^{-3}\sum_{\substack{a=1\\(a,q)=1}}^{q} e\Big(-\frac{an}{q}\Big)\prod_{j=1}^{3} S(q,al_j^2). \tag{3.8}$$

Then $\mathfrak{G}(n,\mathbf{l})$ has the form

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

It is easy to show that $A(q,\mathbf{l},n)$ is multiplicative in q. Thus

$$\mathfrak{G}(n,\mathbf{l}) = \prod_{p}\chi_p(n,\mathbf{l}),$$

where

$$\chi_p(n,\mathbf{l}) = \sum_{k=0}^{\infty} A(p^k,\mathbf{l},n). \tag{3.9}$$

Let $\mathbf{e}_1(p) = (p,1,1)$, $\mathbf{e}_2(p) = (p,p,1)$, and $\mathbf{e}_3(p) = (p,p,p)$. By (3.5), we have $S(q,at^2) = S(q,a)$ when $(q,t) = 1$. Hence, by (3.8) we can deduce that $A(p^k,\mathbf{l},n) = A(p^k,\mathbf{e}_v(p),n)$ if $p^v \parallel l_1l_2l_3$. By (3.6) and (3.9) it follows that

$$\omega(\mathbf{l},n) = \prod_{\substack{p^v\parallel l_1l_2l_3\\v\ge 1}} \frac{\chi_p(n,\mathbf{e}_v(p))}{\chi_p(n,\mathbf{e})} = \prod_{\substack{p^v\parallel l_1l_2l_3\\v\ge 1}} \omega_v(p), \tag{3.10}$$

where $\mathbf{e} = (1,1,1)$ and $\omega_v(p) = \omega(\mathbf{e}_v(p),n)$. It is clear that $\omega_v(2) = 0$ for $v \ge 1$ and $n \equiv 3 \pmod 8$.

Lemmas 3.1 and 3.2 in Blomer and Brüdern [2] give explicit information on $\omega_v(p)$.

LEMMA 3.1. *Suppose that $p^v \parallel l_1l_2l_3$ and $\mu(l_1)^2\mu(l_2)^2\mu(l_3)^2 = 1$. If $p \nmid n$ then*

$$\omega_v(p) = \begin{cases} \dfrac{p - \left(\frac{-1}{p}\right)}{p + \left(\frac{-n}{p}\right)} & \text{if } v = 1,\\[2ex] \dfrac{p\left(1 + \left(\frac{n}{p}\right)\right)}{p + \left(\frac{-n}{p}\right)} & \text{if } v = 2,\\[2ex] 0 & \text{if } v = 3. \end{cases}$$

LEMMA 3.2. *Let $p^\theta \| n$ with $\theta \ge 1$ and write*

$$f_\theta(p) = \begin{cases} p^{-1} - p^{-(\theta+1)/2} - p^{-(\theta+3)/2} & \text{if } \theta \text{ is odd,} \\ p^{-1} - p^{-(\theta+2)/2} - \left(\frac{-np^{-\theta}}{p}\right)p^{-(\theta+2)/2} & \text{if } \theta \text{ is even.} \end{cases}$$

Then

$$\omega_v(p) = \begin{cases} \dfrac{1 + \left(\frac{-1}{p}\right)\frac{p-1}{p} + pf_\theta(p)}{1 + f_\theta(p)} & \text{if } v = 1, \\ \dfrac{1 + p^2 f_\theta(p)}{1 + f_\theta(p)} & \text{if } v = 2, \\ \dfrac{p + p^3 f_\theta(p)}{1 + f_\theta(p)} & \text{if } v = 3. \end{cases}$$

From these lemmas, it is easy to see that

$$\omega_1(p) \le \begin{cases} \dfrac{p+1}{p-1} & \text{if } p \nmid n, \\ \dfrac{p+1}{p} & \text{if } p \mid n \text{ and } p \equiv -1 \pmod 4, \\ 3 & \text{if } p \mid n \text{ and } p \equiv 1 \pmod 4, \end{cases}$$

$$\omega_2(p) < p \quad \text{if } p \mid n,$$

$$\omega_3(p) < p^2 \quad \text{if } p \mid n.$$

Then for primes p, we define the multiplicative function Ω by

$$\Omega(p) = 3\omega_1(p) - 3\,\frac{\omega_2(p)}{p} + \frac{\omega_3(p)}{p^2}. \tag{3.11}$$

Thus for $n \equiv 3 \pmod{24}$ and $5 \nmid n$, we have

$$0 \le \Omega(p) < p. \tag{3.12}$$

In addition, by Mertens' theorem, there is a constant $A \ge 2$ such that

$$\prod_{z_1 \le p < z} \left(1 - \frac{\Omega(p)}{p}\right)^{-1} \le \left(\frac{\log z}{\log z_1}\right)^3 \left(1 + \frac{A}{\log z_1}\right) \quad \text{for } 2 \le z_1 \le z. \tag{3.13}$$

4. Proof of Theorem 1.1. Now we begin to prove Theorem 1.1. First we transform the information concerning $\mathcal{B}_{\mathbf{l}}$ into that on $\mathcal{A}_d$. For square-free d, the inclusion-exclusion principle yields

$$|\mathcal{A}_d| = \mu(d) \sum_{\substack{\mathbf{l} \in \mathbb{N}^3 \\ p \mid l_1 l_2 l_3 \Leftrightarrow p \mid d}} \mu(l_1)\mu(l_2)\mu(l_3)|\mathcal{B}_{\mathbf{l}}|. \tag{4.1}$$

We replace $|\mathcal{B}_{\mathbf{l}}|$ with the approximation formula (3.7) to obtain

$$|\mathcal{A}_d| = \frac{\pi}{4}\Bigg(\mu(d) \sum_{\substack{\mathbf{l}\in\mathbb{N}^3 \\ p|l_1l_2l_3 \Leftrightarrow p|d}} \mu(l_1)\mu(l_2)\mu(l_3)\,\frac{\omega(\mathbf{l},n)}{l_1l_2l_3}\Bigg)\mathfrak{G}(n)n^{1/2} + R_d(\mathcal{A}), \tag{4.2}$$

where

$$R_d(\mathcal{A}) \le \sum_{\substack{\mathbf{l}\in\mathbb{N}^3 \\ p|l_1l_2l_3 \Leftrightarrow p|d}} \mu(l_1)^2\mu(l_2)^2\mu(l_3)^2|R(n,\mathbf{l})|. \tag{4.3}$$

Using the notations (3.10) and (3.11), we see that the coefficient of the main term in (4.2) transforms into

$$\prod_{p|d}\left(\frac{3\omega_1(p)}{p} - \frac{3\omega_2(p)}{p^2} + \frac{\omega_3(p)}{p^3}\right) = \prod_{p|d}\frac{\Omega(p)}{p} =: \frac{\Omega(d)}{d}.$$

We further write

$$X = \frac{\pi}{4}\,\mathfrak{G}(n)n^{1/2}. \tag{4.4}$$

Therefore we can rewrite the formula (4.2) as

$$|\mathcal{A}_d| = \frac{\Omega(d)}{d}\,X + R_d(\mathcal{A}). \tag{4.5}$$

For the assumed error term $R_d(\mathcal{A})$, we have

LEMMA 4.1. *Suppose $n \equiv 3 \pmod{24}$ and $5 \nmid n$ and $\tau < 1/177$. Then for any sufficiently small $\varepsilon > 0$,*

$$\sum_{d\le(n^{1/2})^\tau} \mu^2(d)4^{v(d)}|R_d(\mathcal{A})| \ll n^{1/2-\varepsilon}. \tag{4.6}$$

Moreover, if n is square-free, then (4.6) also holds true for $\tau < 1/126$.

Proof. In essence this lemma is Lemma 2.2 in Blomer and Brüdern [2]. Following similar arguments to those in Section III of [3], we can easily transform Lemma 2.2 in [2] into the present case.

From (3.12), (3.13), (4.5) and (4.6), we see that our present case satisfies all requirements in Lemmas 2.1 and 2.2 with $\kappa = 3$. In particular, for $a \in \mathcal{A}$, the inequality (2.5) holds with

$$\tau\mu = 3.$$

Therefore from Lemma 2.2, for any two real numbers u and v satisfying

$$\tau^{-1} < u < v, \qquad \beta_3 < \tau v,$$

we have

$$|\{P_r : P_r \in \mathcal{A}\}| \gg X \prod_{p<X^{1/v}}\left(1 - \frac{\Omega(p)}{p}\right) \tag{4.7}$$

provided only that

$$r > \tau\mu u - 1 + \frac{3}{f_3(\tau v)} \int_1^{v/u} F_3(\tau v - s)\left(1 - \frac{u}{v}\, s\right) \frac{ds}{s}. \tag{4.8}$$

Note that

$$\beta_3 = 6.6408,$$

by Appendix III on p. 345 in [4]. Our aim is to find the smallest r satisfying (4.8).

Although it is difficult to compute $F_3(u)$ and $f_3(u)$, there is a slightly weaker version of (4.8), which states that for any $0 < \zeta < \beta_3$, we have

$$r > (1+\zeta)\mu - 1 + (3+\zeta)\log\frac{\beta_3}{\zeta} - 3 - \zeta\,\frac{\mu - 3}{\beta_3} =: m(\zeta). \tag{4.9}$$

It is easy to find that, for $\tau = 1/177$,

$$\min_{0<\zeta<\beta_3} m(\zeta) = m(0.00655868\ldots) = 550.767\ldots; \tag{4.10}$$

and for $\tau = 1/126$,

$$\min_{0<\zeta<\beta_3} m(\zeta) = m(0.00917128\ldots) = 396.764\ldots \tag{4.11}$$

Thus $r = 551$ is acceptable unconditionally, and $r = 397$ under the condition that n is square-free. This completes the proof of Theorem 1.1.

Acknowledgements. The author would like to thank Professor Jianya Liu for his comments and suggestions. The author is grateful to the referee for a careful reading of the manuscript and valuable suggestions.

References

[1] C. Bauer, M. C. Liu and T. Zhan, *On sums of three prime squares*, J. Number Theory 85 (2000), 336–359.

[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] H. Diamond, H. Halberstam and H. E. Richert, *Combinatorial sieves of dimension exceeding 1*, J. Number Theory 28 (1988), 306–346.

[5] G. Harman and A. V. Kumchev, *On sums of squares of primes*, Math. Proc. Cambridge Philos. Soc. 140 (2006), 1–13.

[6] L. K. Hua, *Some results in the additive prime number theory*, Quart. J. Math. (Oxford) 9 (1938), 68–80.

[7] M. C. Leung and M. C. Liu, *On generalized quadratic equations in three prime variables*, Monatsh. Math. 115 (1993), 133–169.

[8] J. Y. Liu and T. Zhan, *The exceptional set in Hua's theorem for three squares of primes*, Acta Math. Sin. (Engl. Ser.) 21 (2005), 207–228.

[9] X. M. Ren, *Exponential sums over primes and applications to the Waring–Goldbach problem*, Sci. China (Ser. A) 35 (2005), 252–264.
[10] W. Schwarz, *Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen, II*, J. Reine Angew. Math. 206 (1961), 78–112.

Department of Mathematics
Shandong University
Jinan, Shandong, 250100, P.R. China
E-mail: gslv@sdu.edu.cn

Received on 25.1.2007
and in revised form on 17.4.2007 (5379)