arXiv:2010.02067v1 [math.NT] 5 Oct 2020

PROOF OF A CONJECTURE OF SUN ON SUMS OF FOUR SQUARES

YUE-FENG SHE AND HAI-LIANG WU

ABSTRACT. In 2016, while studying restricted sums of integral squares, Sun posed the following conjecture: Every positive integer n can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N} = \{0, 1, \dots\})$ with x + 3y a square. In this paper, we confirm this conjecture via some arithmetic theory of ternary quadratic forms.

1. INTRODUCTION

The Lagrange four-square theorem states that every positive integer can be written as the sum of four integral squares. Along this line, in 1917, Ramanujan [8] claimed that there are at most 55 positive definite integral diagonal quaternary quadratic forms that can represent all positive integers. Later in the paper [2] Dickson confirmed that Ramanujan's claim is true for 54 forms in Ramanujan's list and pointed out that the quaternary form $x^2+2y^2+5z^2+5w^2$ included in his list represents all positive integers except 15.

In 2016, Sun [10] studied some refinements of Lagrange's theorem. For instance, he showed that for any $k \in \{4, 5, 6\}$, each positive integer n can be written as $x^k + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$. In addition, let P(x, y, z, w) be an integral polynomial. Sun called P(x, y, z, w) a suitable polynomial if every positive integer n can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N})$ with P(x, y, z, w) a square. In the same paper, Sun showed that the polynomials x, 2x, x - y, 2x - 2y are all suitable. Also, he showed that every positive integer n can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{Z})$ with x + 2ya square and he conjectured that x + 2y is a suitable polynomial. This conjecture was later confirmed by Sun and his cooperator Y.-C. Sun in [9]. Readers may consult [6, 9, 11, 13] for the recent progress on this topic. Moreover, Sun [10] investigated the polynomial x + 3y, and he [10, Theorem 1.3(ii)] obtained the following result:

Theorem 1.1 (Sun). Assuming the GRH (Generalized Riemann Hypothesis), every positive integer n can be written as $x^2+y^2+z^2+w^2$ $(x, y, z, w \in \mathbb{Z})$ with x + 3y a square.

²⁰¹⁰ Mathematics Subject Classification. Primary 11E25; Secondary 11E12, 11E20. Key words and phrases. sums of four squares, ternary quadratic forms.

Based on calculations, Sun [10, Conjecture 4.1] posed the following conjecture.

Conjecture 1.2. x + 3y is a suitable polynomial, i.e., each positive integer n can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N})$ with x + 3y a square.

Remark 1.3. With the help of computer, Sun [12] verified this conjecture up to 10^8 . For example,

$$9996 = 58^2 + 14^2 + 6^2 + 80^2$$
 and $58 + 3 \times 14 = 10^2$.
 $99992 = 286^2 + 66^2 + 68^2 + 96^2$ and $286 + 3 \times 66 = 22^2$.

In this paper, we confirm this conjecture via some arithmetic theory of ternary quadratic forms.

Theorem 1.4. Every positive integer n can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N})$ with x + 3y a square.

In Section 2 we will introduce some notations and prove some lemmas which are key elements in our proof of Theorem 1.4. We shall give the detailed proof of Theorem 1.4 in Section 3.

2. NOTATIONS AND SOME PREPARATIONS

Throughout this paper, for any prime p, we let \mathbb{Z}_p denote the ring of p-adic integers, and let \mathbb{Z}_p^{\times} denote the group of invertible elements in \mathbb{Z}_p . In addition, we set $\mathbb{Z}_p^{\times 2} = \{x^2 : x \in \mathbb{Z}_p^{\times}\}$ and let $M_3(\mathbb{Z}_p)$ denote the ring of 3×3 matrices with entries contained in \mathbb{Z}_p . We also adopt the standard notations of quadratic forms (readers may refer to [1, 5, 7] for more details). Let

$$f(x, y, z) = ax^{2} + by^{2} + cz^{2} + ryz + szx + txy$$

be an integral positive definite ternary quadratic form. Its associated matrix is

$$M_f := \begin{pmatrix} a & t/2 & s/2 \\ t/2 & b & r/2 \\ s/2 & r/2 & c \end{pmatrix}$$

Let p be an arbitrary prime. We introduce the following notations.

$$q(f) := \{ f(x, y, z) : (x, y, z) \in \mathbb{Z}^3 \}.$$
$$q_p(f) := \{ f(x, y, z) : (x, y, z) \in \mathbb{Z}_p^3 \}.$$

In addition, let p > 2 be a prime. We say that f is unimodular over \mathbb{Z}_p if its associated matrix $M_f \in M_3(\mathbb{Z}_p)$ and is invertible. We also let gen(f) denote the set of quadratic forms which are in the genus of f.

3

For any positive integer n, we say that n can be represented by gen(f)if there exists a form $f^* \in gen(f)$ such that $n \in q(f^*)$. When this occurs, we write $n \in q(gen(f))$. By [1, Theorem 1.3, p. 129] we know that

(2.1)
$$n \in q(gen(f)) \Leftrightarrow n \in q_p(f) \text{ for all primes } p.$$

We now state our first lemma involving local representations over \mathbb{Z}_2 (cf. [4, pp. 186–187]).

Lemma 2.1 (Jones). Let f be an integral positive definite ternary quadratic form, and let n be a positive integer. Then $n \in q_2(f)$ if and only if

$$f(x, y, z) \equiv n \pmod{2^{r+1}}$$

is solvable, where r is the 2-adic order of 4n.

We now give our next lemma which concerns the global representations by the form $x^2 + 10y^2 + 10z^2$.

Lemma 2.2. (i) Let $n \equiv 1, 2 \pmod{4}$ be a positive integer, and let $0 < \lambda \le \sqrt{10n}$ be an odd integer with $5 \nmid \lambda$. Then there exist $x, y, z \in \mathbb{Z}$ such that

$$10n - \lambda^2 = x^2 + 10y^2 + 10z^2.$$

(ii) Let $n \equiv 3 \pmod{4}$ be a positive integer, and let $0 < \delta \leq \sqrt{10n}$ be an integer with $4 \mid \delta$ and $5 \nmid \delta$. Then there are $x, y, z \in \mathbb{Z}$ such that

$$10n - \delta^2 = x^2 + 10y^2 + 10z^2$$

(iii) Let n be a positive odd integer, and let $0 < \mu \leq \sqrt{10n}$ be an integer with $\mu \equiv 2 \pmod{4}$ and $5 \nmid \mu$. Then there are $x, y, z \in \mathbb{Z}$ such that

$$10n - \mu^2 = x^2 + 10y^2 + 10z^2$$

Proof. (i). Let $f(x, y, z) = x^2 + 10y^2 + 10z^2$. For any prime $p \neq 2, 5$, it is clear that f(x, y, z) is unimodular over \mathbb{Z}_p and hence $q_p(f) = \mathbb{Z}_p$. As $5 \nmid \lambda$, it is easy to see that $10n - \lambda^2 \in q_5(f)$. When p = 2, since $n \equiv 1, 2 \pmod{4}$, we have $10n - \lambda^2 \equiv 1, 3 \pmod{8}$. By the local square theorem (cf. [7, 63:1]) we obtain that $10n - \lambda^2 \in \mathbb{Z}_2^{\times 2}$ if $n \equiv 1 \pmod{4}$ and that $10n - \lambda^2 \in 3\mathbb{Z}_2^{\times 2}$ if $n \equiv 2 \pmod{4}$. This implies $10n - \lambda^2 \in q_2(f)$ and hence $10n - \lambda^2 \in q(\operatorname{gen}(f))$.

There are two classes in gen(f) and the one not containing f has a representative $g(x, y, z) = 4x^2 + 5y^2 + 6z^2 + 4zx$. By (2.1) we have either $10n - \lambda^2 \in q(f)$ or $10n - \lambda^2 \in q(g)$. If $10n - \lambda^2 \in q(f)$, then we are done. Suppose now $10n - \lambda^2 \in q(g)$, i.e., there are $x, y, z \in \mathbb{Z}$ such that

$$10n - \lambda^2 = g(x, y, z) = 4x^2 + 5y^2 + 6z^2 + 4zx.$$

Then clearly $2 \nmid y$. As $10n - \lambda^2 \equiv 2n - 1 \equiv 5 + 2z^2 \pmod{4}$, we obtain $z \equiv n + 1 \pmod{2}$. If $n \equiv 1 \pmod{4}$, then we have $10n - \lambda^2 \equiv 1 \equiv 4x^2 + 5 \pmod{8}$ and hence $x \equiv 1 \pmod{2}$. Hence in the case $n \equiv 1 \pmod{4}$, we have $x - y - z \equiv 0 \pmod{2}$. In the case $n \equiv 2 \pmod{4}$, as $z \equiv 1 \pmod{2}$, by the equality

(2.2)
$$g(x, y, z) = g(x + z, y, -z),$$

there exist $x', y', z' \in \mathbb{Z}$ with $2 \mid x' - y' - z'$ such that $10n - \lambda^2 = g(x', y', z')$. One can easily verify the following equality:

(2.3)
$$f(x, y, z) = g\left(\frac{x - y - z}{2}, -y + z, y + z\right).$$

By this equality and the above discussion, it is easy to see that $10n - \lambda^2 \in q(f)$.

(ii). Let notations be as above. With the same reasons as in (i), we have $10n - \delta^2 \in q_p(f)$ for any prime $p \neq 2$. When p = 2, by the local square theorem we have

$$\mathbb{Z}_{2}^{\times} \subseteq \{2x^{2} + 5y^{2} + 5z^{2} : x, y, z \in \mathbb{Z}_{2}\}$$

Hence $5n - \delta^2/2 \equiv 2x^2 + 5y^2 + 5z^2 \pmod{8}$ is solvable. This implies that the congruence equation $10n - \delta^2 \equiv f(x, y, z) \pmod{16}$ is solvable. By Lemma 2.1 and the above, we obtain $10n - \delta^2 \in q(\text{gen}(f))$.

By (2.1) we have either $10n - \delta^2 \in q(f)$ or $10n - \delta^2 \in q(g)$. If $10n - \delta^2 \in q(f)$, then we are done. Suppose now $10n - \delta^2 \in q(g)$, i.e., there are x, y, z such that $10n - \delta^2 = g(x, y, z)$. Then clearly $2 \mid y$. As $10n - \delta^2 \equiv 2 \equiv 2z^2 \pmod{4}$, we obtain $2 \nmid z$. Hence by Eq. (2.2) there must exist $x', y', z' \in \mathbb{Z}$ with $x' - y' - z' \equiv 0 \pmod{2}$ such that $10n - \delta^2 = g(x', y', z')$. By Eq. (2.3) we clearly have $10n - \delta^2 \in q(f)$.

(iii) Let notations be as above. Clearly we have $10n - \mu^2 \in q_p(f)$ for any prime $p \neq 2$. When p = 2, as

$$\mathbb{Z}_{2}^{\times} \subseteq \{2x^{2} + 5y^{2} + 5z^{2} : x, y, z \in \mathbb{Z}_{2}\}.$$

The equation $5n - \mu^2/2 \equiv 2x^2 + 5y^2 + 5z^2 \pmod{8}$ is solvable. This implies that the equation $10n - \mu^2 \equiv x^2 + 10y^2 + 10z^2 \pmod{16}$ is solvable. By Lemma 2.1 and the above, we have $10n - \mu^2 \in q(\operatorname{gen}(f))$.

By (2.1) we have either $10n - \mu^2 \in q(f)$ or $10n - \mu^2 \in q(g)$. If $10n - \mu^2 \in q(f)$, then we are done. Suppose now $10n - \mu^2 \in q(g)$, i.e., there are x, y, z such that $10n - \mu^2 = g(x, y, z)$. Then clearly $2 \mid y$. Since $10n - \mu^2 \equiv 2 \equiv 2z^2 \pmod{4}$, we get $2 \nmid z$. Then by Eq. (2.2) there are $x', y', z' \in \mathbb{Z}$ with $x' - y' - z' \equiv 0 \pmod{2}$ such that $10n - \mu^2 = g(x', y', z')$. By Eq. (2.3) we clearly have $10n - \mu^2 \in q(f)$. This completes the proof.

Sun and his cooperator [9, Theorem 1.1(ii)] proved that every positive integer n can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N})$ with x + 2ya square. Motivated by this, we obtain the following stronger result which we need in the next Section.

Lemma 2.3. Every odd integer $n \ge 8 \times 10^6$ can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N})$ with $x \le y$ and x + 2y a square.

Proof. We first note that

$$8 \times 10^6 > \left[\left(\frac{2}{5^{1/4} - (4.5)^{1/4}} \right)^4 \right],$$

where $[\cdot]$ denotes the floor function. If $n \ge 8 \times 10^6$, then $(5n)^{1/4} - (4.5n)^{1/4} > 2$ and hence there is an integer $(4.5n)^{1/4} \le m \le (5n)^{1/4}$ such that $m \equiv \frac{n-1}{2} \pmod{2}$.

Now let $h(x, y, z) = x^2 + 5y^2 + 5z^2$. By [3, pp. 112–113] we have (2.4) $q(h) = \{x \in \mathbb{N} : x \not\equiv \pm 2 \pmod{5} \text{ and } x \neq 4^k(8l+7) \text{ for any } k, l \in \mathbb{N}\}.$

As $5n - m^4 \ge 0$, $5n - m^4 \equiv 1$, 2 (mod 4) and $5n - m^4 \not\equiv \pm 2 \pmod{5}$, we have $5n - m^4 \in q(h)$ by (2.4). Hence there exist $s \in \mathbb{Z}$ and $z, w \in \mathbb{N}$ such that $5n - m^4 = s^2 + 5z^2 + 5w^2$. Clearly $-\sqrt{5n - m^4} \le s \le \sqrt{5n - m^4}$. Replacing s by -s if necessary, we may assume that $s \in \mathbb{Z}$ and $s \equiv -2m^2 \pmod{5}$. By the inequality

$$s + 2m^2 \ge -\sqrt{5n - m^4} + 2m^2 = \frac{5m^4 - 5n}{\sqrt{5n - m^4} + 2m^2} > 0$$

we may write $s + 2m^2 = 5y$ for some $y \in \mathbb{N}$. This gives

$$5n - m^4 = (5y - 2m^2)^2 + 5z^2 + 5w^2,$$

and hence we get

(2.5)
$$n = (m^2 - 2y)^2 + y^2 + z^2 + w^2.$$

Let $x := m^2 - 2y$. Then we have

$$5x = 5m^2 - 10y = m^2 - 2s \ge m^2 - 2\sqrt{5n - m^4} = \frac{5(m^4 - 4n)}{m^2 + 2\sqrt{5n - m^4}} > 0.$$

This gives x > 0. Moreover,

$$5(y-x) = 3s + m^2 \ge -3\sqrt{5n - m^4} + m^2 = \frac{10(m^4 - 4.5n)}{m^2 + 3\sqrt{5n - m^4}} \ge 0$$

This gives $x \leq y$. In view of the above, we can write $n = x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}, x \leq y$ and $x + 2y = m^2$. This completes the proof. \Box

We conclude this section with the following lemma.

Lemma 2.4. For every integer $n \not\equiv 0 \pmod{4}$ with $n \geq 4 \times 10^8$, we can write $n = x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N})$ with $x + 3y = 2m^2$ for some $m \in \mathbb{N}$.

Proof. We divide our proof into the following two cases.

Case 1. $n \equiv 2 \pmod{4}$.

In this case, we write n = 2n' for some odd integer $n' \ge 4 \times 10^7$. By Lemma 2.3 we can write $n' = x'^2 + y'^2 + z'^2 + w'^2$ $(x', y', z', w' \in \mathbb{N})$ with $x' \le y', z' \le w'$ and $x' + 2y' = m_0^2$ for some $m_0 \in \mathbb{N}$. Then

$$n = 2n' = (y' - x')^{2} + (y' + x')^{2} + (w' - z')^{2} + (z' + w')^{2}.$$

Letting x := y' - x', y := y' + x', z := w' - z' and w := z' + w', we obtain that

$$n = x^2 + y^2 + z^2 + w^2$$

with $x + 3y = (y' - x') + 3(y' + x') = 2(x' + 2y') = 2m_0^2$.

Case 2. n is odd.

We first note that

$$4 \times 10^8 > \left[\left(\frac{4\sqrt{2}}{10^{1/4} - 9^{1/4}} \right)^4 \right].$$

If $n \ge 4 \times 10^8$, then we have $\frac{(10n)^{1/4}}{\sqrt{2}} - \frac{(9n)^{1/4}}{\sqrt{2}} > 4$ and hence there exists an integer $\frac{(9n)^{1/4}}{\sqrt{2}} \le m \le \frac{(10n)^{1/4}}{\sqrt{2}}$ such that $2 \nmid m$ and $5 \nmid m$. By Lemma 2.2 (iii) there exist $t \in \mathbb{Z}$ and $z, w \in \mathbb{N}$ such that

$$10n - 4m^4 = t^2 + 10z^2 + 10w^2.$$

Clearly $-\sqrt{10n - 4m^4} \le t \le \sqrt{10n - 4m^4}$. Replacing t by -t if necessary, we may assume $t \equiv -6m^2 \pmod{10}$. By the inequality

$$t + 6m^2 \ge -\sqrt{10n - 4m^4} + 6m^2 = \frac{10(4m^4 - n)}{6m^2 + \sqrt{10n - 4m^4}} > 0$$

we can write $t + 6m^2 = 10y$ for some $y \in \mathbb{N}$. This implies

$$10n - 4m^4 = (10y - 6m^2)^2 + 10z^2 + 10w^2$$

and hence we get

$$n = (2m^2 - 3y)^2 + y^2 + z^2 + w^2.$$

Let $x := 2m^2 - 3y$. Then we have

$$10x = 2m^2 - 3t \ge 2m^2 - 3\sqrt{10n - 4m^4} = \frac{10(4m^4 - 9n)}{2m^2 + 3\sqrt{10n - 4m^4}} \ge 0.$$

This gives $x \ge 0$. In view of the above, we can write $n = x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N})$ with $x + 3y = 2m^2$.

This completes the proof of Lemma 2.4.

3. Proof of the main result

Proof of Theorem 1.4. We prove our result by induction on n. When $n < 4 \times 10^9$, we can verify the desired result by computer. Assume now $n > 4 \times 10^9$. We divide our remaining proof into following cases.

Case 1. $n \equiv 0 \pmod{4}$.

If 16 | n, then the desired result follows immediately from the induction hypothesis. We now assume 16 \nmid n. Then we can write n = 4n' with $n' \not\equiv 0 \pmod{4}$. By Lemma 2.4 there exist $x_1, y_1, z_1, w_1, m_1 \in \mathbb{N}$ such that $n' = x_1^2 + y_1^2 + z_1^2 + w_1^2$ and $x_1 + 3y_1 = 2m_1^2$. Clearly we can write $n = 4n' = x^2 + y^2 + z^2 + w^2$ with $x + 3y = (2m_1)^2$, where $x = 2x_1, y = 2y_1, z = 2z_1, w = 2w_1 \in \mathbb{N}$.

Case 2. $n \equiv 1, 2, 3 \pmod{4}$.

We first note that

$$4 \times 10^9 > \left[\left(\frac{8}{10^{1/4} - 9^{1/4}} \right)^4 \right] > \left[\left(\frac{4}{10^{1/4} - 9^{1/4}} \right)^4 \right].$$

If $n \ge 4 \times 10^9$, then we have $(10n)^{1/4} - (9n)^{1/4} > 8$. Hence we can find an integer $(9n)^{1/4} \le m \le (10n)^{1/4}$ satisfying the following condition:

$$\begin{cases} 2 \nmid m \text{ and } 5 \nmid m & \text{if } n \equiv 1,2 \pmod{4}, \\ 4 \mid m \text{ and } 5 \nmid m & \text{if } n \equiv 3 \pmod{4}. \end{cases}$$

By Lemma 2.2 there exist $u \in \mathbb{Z}$ and $z, w \in \mathbb{N}$ such that

$$10n - m^4 = u^2 + 10z^2 + 10w^2.$$

Clearly $-\sqrt{10n - m^4} \le u \le \sqrt{10n - m^4}$. Replacing u by -u if necessary, we may assume that $u \in \mathbb{Z}$ and $u \equiv -3m^2 \pmod{10}$. By the inequality

$$u + 3m^2 \ge -\sqrt{10n - m^4} + 3m^2 = \frac{10(m^4 - n)}{\sqrt{10n - m^4} + 3m^2} > 0$$

we can write $s + 3m^2 = 10y$ for some $y \in \mathbb{N}$. This gives

$$10n - m^4 = (10y - 3m^2)^2 + 10z^2 + 10w^2,$$

and hence

$$n = (m^2 - 3y)^2 + y^2 + z^2 + w^2.$$

Let $x := m^2 - 3y$. Then we have

$$10x = m^2 - 3u \ge m^2 - 3\sqrt{10n - m^4} = \frac{10(m^4 - 9n)}{m^2 + 3\sqrt{10n - m^4}} \ge 0.$$

This gives $x \ge 0$ and hence we have $n = x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N})$ with $x + 3y = m^2$.

In view of the above, we complete the proof.

Acknowledgements. This research was supported by the National Natural Science Foundation of China (grant 11971222).

Y.-F. SHE AND H.-L. WU

References

- [1] J. W. S. Cassels, Rational Quadratic Forms, Academic Press, London, 1978.
- [2] L. E. Dickson, Quaternary quadratic forms representing all integers, Amer. J. Math. 49 (1927), 39–56.
- [3] L. E. Dickson, Modern Elementary Theory of Numbers, Univ. Chicago Press, Chicago, 1939.
- [4] B. W. Jones, The Arithmetic Theory of Quadratic Forms, Math. Assoc. Amer., Carus Math. Mono. 10, Buffalo, New York, 1950.
- [5] Y. Kitaoka, Arithmetic of Quadratic Forms, Cambridge Tracts in Math., Vol. 106, 1993.
- [6] D. Krachun and Z.-W. Sun, On sums of four pentagonal numbers with coefficients, Electron. Res. Arch. 28 (2020), 559–566.
- [7] O. T. O'Meara, Introduction to Quadratic Forms, Springer, New York, 1963.
- [8] S. Ramanujan, On the expression of a number in the form $ax^2 + by^2 + cz^2 + dw^2$, Proc. Cambridge Philos. Soc. **19** (1917), 11–21.
- [9] Y.-C. Sun and Z.-W. Sun, Some variants of Lagrange's four squares theorem, Acta Arith. 183 (2018), 339–356.
- [10] Z.-W. Sun, Refining Lagrange's four-square theorem, J. Number Theory 175 (2017), 169–190.
- [11] Z.-W. Sun, Restricted sums of four squares, Int. J. Number Theory 15 (2019), 1863– 1893.
- [12] Z.-W. Sun, Sequence A300666, in OEIS, http://oeis.org.
- [13] H.-L. Wu and Z.-W. Sun, On the 1-3-5 conjecture and related topics, Acta Arith.
 193 (2020), 253-268.

(YUE-FENG SHE) DEPARTMENT OF MATHEMATICS, NANJING UNIVERSITY, NAN-JING 210093, PEOPLE'S REPUBLIC OF CHINA Email address: she.math@smail.nju.edu.cn

(HAI-LIANG WU) SCHOOL OF SCIENCE, NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS, NANJING 210023, PEOPLE'S REPUBLIC OF CHINA *Email address*: whl.math@smail.nju.edu.cn