A talk given at 2020 Westlake Number Theory Symp. (Oct. 29, 2020).

Various Refinements of Lagrange's Four-Square Theorem

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

October 29, 2020

Abstract

Lagrange's four-square theorem asserts that any $n \in \mathbb{N} = \{0, 1, 2, \dots\}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$. In 2016 the speaker formulated many conjectural refinements of this classical theorem; for example, his 1-3-5 conjecture states that we may require additionally that $x + 3y + 5z$ is a square.

In this talk, we review various problems and results refining Lagrange's four-square theorem. In particular, we will introduce the recent nice proof of the 1-3-5 conjecture given by A. Machiavelo and N. Tsopanidis, which involves the Lipschitz integers related to Hamilton quaternions.

Part I. Classical Results on Sums of Four Squares

Lagrange's Four-square Theorem

Four-Square Theorem. Each $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ can be written as the sum of four squares.

Examples. $3 = 1^2 + 1^2 + 1^2 + 0^2$ and $7 = 2^2 + 1^2 + 1^2 + 1^2$.

A. Diophantus (AD 299-215, or AD 285-201) was aware of this theorem as indicated by examples given in his book *Arithmetica*.

In 1621 Bachet translated Diophantus' book into Latin and stated the theorem in the notes of his translation.

In 1748 L. Euler found the four-square identity

$$\begin{aligned}
&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\
=&(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3)^2\\
&+ (x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2)^2 + (x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2)^2.
\end{aligned}$$

and hence reduced the theorem to the case with n prime.

On the basis of Euler's work, in 1770 J. L. Lagrange first completed the proof of the four-square theorem. The celebrated theorem is now known as *Lagrange's Four-square Theorem*.

The representation function $r_4(n)$

Jacobi used his triple-product formula

$$\prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}z)(1+q^{2n-1}z^{-1}) = \sum_{n=-\infty}^{+\infty} z^n q^{n^2} \ \ (|q|<1,\ z\neq 0)$$

to study the fourth power of $\varphi(q)=\sum_{n=-\infty}^{\infty} q^{n^2}$, and this led him to deduce that

$$r_4(n) = 8\sum_{d\mid n\ \&\ 4\nmid d} d \quad \text{for all } n\in\mathbb{Z}^+,$$

where

$$r_4(n) := |\{(w,x,y,z)\in\mathbb{Z}^4:\ w^2+x^2+y^2+z^2=n\}|.$$

This is related to modular forms of weight two. Let τ be a complex number with positive real part and set $\theta(\tau)=\varphi(e^{2\pi i\tau})$. Then

$$\theta\left(\frac{\tau}{4\tau+1}\right)=\sqrt{4\tau+1}\,\theta(\tau) \text{ and hence } \theta^4\left(\frac{\tau}{4\tau+1}\right)=(4\tau+1)^2\theta^4(\tau).$$

Ramanujan's observation

S. Ramanujan's Observation (confirmed by L.E. Dickson in 1927). There are totally 54 quadruples $(a, b, c, d) \in (\mathbb{Z}^+)^4$ with $a \leqslant b \leqslant c \leqslant d$ such that each $n \in \mathbb{N}$ can be written as $aw^2 + bx^2 + cy^2 + dz^2$ with $w, x, y, z \in \mathbb{Z}$. The 54 quadruples are

$(1,1,1,1)$, $(1,1,1,2)$, $(1,1,2,2)$, $(1,2,2,2)$, $(1,1,1,3)$, $(1,1,2,3)$,
$(1,2,2,3)$, $(1,1,3,3)$, $(1,2,3,3)$, $(1,1,1,4)$, $(1,1,2,4)$, $(1,2,2,4)$,
$(1,1,3,4)$, $(1,2,3,4)$, $(1,2,4,4)$, $(1,1,1,5)$, $(1,1,2,5)$, $(1,2,2,5)$,
$(1,1,3,5)$, $(1,2,3,5)$, $(1,2,4,5)$, $(1,1,1,6)$, $(1,1,2,6)$, $(1,2,2,6)$,
$(1,1,3,6)$, $(1,2,3,6)$, $(1,2,4,6)$, $(1,2,5,6)$, $(1,1,1,7)$, $(1,1,2,7)$,
$(1,2,2,7)$, $(1,2,3,7)$, $(1,2,4,7)$, $(1,2,5,7)$, $(1,1,2,8)$, $(1,2,3,8)$,
$(1,2,4,8)$, $(1,2,5,8)$, $(1,1,2,9)$, $(1,2,3,9)$, $(1,2,4,9)$, $(1,1,5,9)$,
$(1,1,2,10)$, $(1,2,3,10)$, $(1,2,4,10)$, $(1,2,5,10)$, $(1,1,2,11)$, $(1,2,4,11)$,
$1,1,2,12)$, $(1,2,4,12)$, $(1,1,2,13)$, $(1,2,4,13)$, $(1,1,2,14)$, $(1,2,4,14)$.

Sums of three squares

Gauss-Legendre Theorem. $n \in \mathbb{N}$ can be written as the sum of three squares if and only if n is not of the form $4^k(8l+7)$ with $k, l \in \mathbb{N}$.

Euler's Observation (June 9, 1750). Any positive odd integer can be written as $x^2+y^2+z^2+w^2$ with $x, y, z, w \in \mathbb{Z}$ and $x+y+z+w=1$.

This follows from the Gauss-Legendre Theorem.

Part II. New Problems for Sums of Four Squares

Universal sums over $\mathbb{N}$

Let $f(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$. If any $n \in \mathbb{N}$ can be written as $f(x_1, \ldots, x_k)$ with $x_1, \ldots, x_k$ in $\mathbb{N}$ (or $\mathbb{Z}$), then we say that f is *universal over* $\mathbb{N}$ (or $\mathbb{Z}$).

Suppose that $a_1 x_1^{n_1} + \ldots + a_k x_k^{n_k}$ (with $a_1, \ldots, a_k \in \mathbb{Z}^+$) is universal over $\mathbb{N}$. For any positive integer N, each $n = 0, \ldots, N-1$ can be written as $\sum_{i=1}^k a_i x_i^{n_i}$ with $x_i \in \mathbb{N}$, thus

$$|\{(x_1, \ldots, x_k) \in \mathbb{N}^k : \ a_1 x_1^{n_1} < N, \ \ldots, \ a_k x_k^{n_k} < N\}| \geqslant N$$

and hence

$$N \leqslant \prod_{i=1}^k \left(1 + \left(\frac{N}{a_i}\right)^{1/n_i}\right).$$

As this holds for any $N \in \mathbb{Z}^+$, we must have

$$\sum_{i=1}^k \frac{1}{n_i} \geqslant 1.$$

Universal sums of four mixed powers

Theorem (Sun [J. Number Theory 175(2017)]). For any $a \in \{1, 4\}$ and $k \in \{4, 5, 6\}$, $aw^k + x^2 + y^2 + z^2$ is universal over $\mathbb{N}$.

Theorem (Z.-W. Sun [Nanjing Univ. J. Math. Biquarterly 34(2017)]). Let $a, b, c, d \in \mathbb{Z}^+$ with $a \leqslant b \leqslant c \leqslant d$, and let $h, i, j, k \in \{2, 3, \ldots\}$ with at most one of h, i, j, k equal to two. Suppose that $h \leqslant i$ if $a = b$, $i \leqslant j$ if $b = c$, and $j \leqslant k$ if $c = d$. If $f(w, x, y, z) = aw^h + bx^i + cy^j + dz^k$ is universal over $\mathbb{N}$, then $f(w, x, y, z)$ must be among the following 9 polynomials

$$w^2 + x^3 + y^4 + 2z^3,\ w^2 + x^3 + y^4 + 2z^4,\ w^2 + x^3 + 2y^3 + 3z^3,$$
$$w^2 + x^3 + 2y^3 + 3z^4,\ w^2 + x^3 + 2y^3 + 4z^3,\ w^2 + x^3 + 2y^3 + 5z^3,$$
$$w^2 + x^3 + 2y^3 + 6z^3,\ w^2 + x^3 + 2y^3 + 6z^4,\ w^3 + x^4 + 2y^2 + 4z^3.$$

Conjecture (Sun [Nanjing Univ. J. Math. Biquarterly 34(2017)]). All the 9 polynomials are universal over $\mathbb{N}$.

Discoveries on April 8, 2016

Motivated by my conjecture that any $n \in \mathbb{N}$ can be written as

$$x_1^3 + x_2^3 + 2x_3^3 + 2x_4^3 + 3x_5^3 \quad (x_1, x_2, x_3, x_4, x_5 \in \mathbb{N})$$

(which is stronger than the result $g(3) = 9$ for Waring's problem), on April 8, 2016 I considered to write $n \in \mathbb{N}$ as $\sum_{i=1}^5 a_i x_i^2$ $(x_i \in \mathbb{N})$ with certain restrictions on $x_1, \ldots, x_5$.

Conjecture (Z.-W. Sun) Let $n > 1$ be an integer.

(i) n can be written as

$$x_1^2+x_2^2+x_3^2+2x_4^2+2x_5^2 = x_1^2+x_2^2+x_3^2+(\underline{x_4+x_5})^2+(x_4-x_5)^2 \ (x_i \in \mathbb{N})$$

with $x_1 + x_2 + x_3 + \underline{x_4 + x_5}$ prime.

(ii) We can write n as

$$x_1^2 + 2x_2^2 + 3x_3^2 + 4x_4^2 + 5x_5^2 \quad (x_1, x_2, x_3, x_4, x_5 \in \mathbb{N})$$

with $x_1 + x_2 + x_3 + x_4$ a square.

Remark. Squares are sparser than prime numbers.

1-3-5-Conjecture (1350 US dollars for the first solution)

1-3-5-Conjecture (Z.-W. Sun, April 9, 2016): Any $n \in \mathbb{N}$ can be written as $x^2+y^2+z^2+w^2$ with $x,y,z,w \in \mathbb{N}$ such that $x+3y+5z$ is a square.

Examples.

$$\begin{aligned}7 =&1^2+1^2+1^2+2^2 \text{ with } 1+3\times 1+5\times 1=3^2,\\ 8 =&0^2+2^2+2^2+0^2 \text{ with } 0+3\times 2+5\times 2=4^2,\\ 31 =&5^2+2^2+1^2+1^2 \text{ with } 5+3\times 2+5\times 1=4^2,\\ 43 =&1^2+5^2+4^2+1^2 \text{ with } 1+3\times 5+5\times 4=6^2.\end{aligned}$$

The conjecture has been verified by Qing-Hu Hou for all $n \leqslant 10^{10}$.

We guess that, if a,b,c are positive integers with $\gcd(a,b,c)$ squarefree such that any $n \in \mathbb{N}$ can be written as $x^2+y^2+z^2+w^2$ $(x,y,z,w \in \mathbb{N})$ with $ax+by+cz$ a square, then we must have $\{a,b,c\}=\{1,3,5\}$.

无　解

数字几时有，
把酒问青天。
一二三四五，
自然藏玄机。

四个平方和，
遍历自然数。
奇妙一三五，
更上一层楼。

苍天捉弄人，
数论妙无穷。
吾辈虽努力，
难解一三五!

时势唤英雄，
攻关需豪杰。
人间若无解，
天神会证否？

Diagonal ternary quadratic forms

For $a, b, c \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, we define

$$E(a, b, c) := \{n \in \mathbb{N} : \ n \neq ax^2 + by^2 + cz^2 \text{ for any } x, y, z \in \mathbb{N}\}.$$

It is known that $E(a, b, c)$ is an infinite set.

There are totally 102 diagonal ternary quadratic forms $ax^2 + by^2 + cz^2$ with $a, b, c \in \mathbb{Z}^+$ and $\gcd(a, b, c) = 1$ for which the structure of $E(a, b, c)$ is known explicitly. For example,

$$\begin{aligned}
E(1,1,1) =& \{4^k(8l+7) : \ k, l \in \mathbb{N}\},\\
E(1,1,2) =& \{4^k(16l+14) : \ k, l \in \mathbb{N}\},\\
E(1,1,5) =& \{4^k(8l+3) : \ k, l \in \mathbb{N}\},\\
E(1,2,3) =& \{4^k(16l+10) : \ k, l \in \mathbb{N}\},\\
E(1,2,6) =& \{4^k(8l+5) : \ k, l \in \mathbb{N}\}.
\end{aligned}$$

Sums of a fourth power and three squares

Theorem (Z.-W. Sun, March 27, 2016). Each $n \in \mathbb{N}$ can be written as $w^4 + x^2 + y^2 + z^2$ with $w, x, y, z \in \mathbb{N}$.

Proof. For $n = 0, 1, 2, \ldots, 15$, the result can be verified directly. Now let $n \geqslant 16$ be an integer and assume that the result holds for smaller values of n.

Case 1. $16 \mid n$.
By the induction hypothesis, we can write

$$\frac{n}{16} = x^4 + y^2 + z^2 + w^2 \quad \text{with } x, y, z, w \in \mathbb{N}.$$

It follows that $n = (2x)^4 + (4y)^2 + (4z)^2 + (4w)^2$.

Case 2. $n = 4^k q$ with $k \in \{0, 1\}$ and $q \equiv 7 \pmod 8$.
In this case, $n - 1 \notin E(1, 1, 1)$, and hence $n = 1^4 + y^2 + z^2 + w^2$ for some $y, z, w \in \mathbb{N}$.

Case 3. $16 \nmid n$ and $n \neq 4^k(8l + 7)$ for any $k \in \{0, 1\}$ and $l \in \mathbb{N}$.
In this case, $n \notin E(1, 1, 1)$ and hence there are $y, z, w \in \mathbb{N}$ such that $n = 0^4 + y^2 + z^2 + w^2$.

Suitable polynomials

Definition (Z.-W. Sun, 2016). A polynomial $P(x, y, z, w)$ with integer coefficients is called *suitable* if any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ such that $P(x, y, z, w)$ is a square.

We have seen that both x and $2x$ are suitable polynomials. The 1-3-5-Conjecture says that $x + 3y + 5z$ is suitable.

We conjecture that there only finitely many $a, b, c, d \in \mathbb{Z}$ with $\gcd(a, b, c, d)$ squarefree such that $ax + by + cz + dw$ is suitable, and we have found all such quadruples (a, b, c, d).

$x - y$ and $2x - 2y$ are suitable

Let $a \in \{1, 2\}$. We claim that any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ such that $a(x - y)$ is a square, and want to prove this by induction.

For every $n = 0, 1, \ldots, 15$, we can verify the claim directly.

Now we fix an integer $n \geqslant 16$ and assume that the claim holds for smaller values of n.

Case 1. $16 \mid n$.
In this case, by the induction hypothesis, there are $x, y, z, w \in \mathbb{N}$ with $a(x - y)$ a square such that $n/16 = x^2 + y^2 + z^2 + w^2$, and hence $n = (4x)^2 + (4y)^2 + (4z)^2 + (4w)^2$ with $a(4x - 4y)$ a square.

Case 2. $16 \nmid n$ and $n \notin E(1, 1, 2)$.
In this case, there are $x, y, z, w \in \mathbb{N}$ with $x = y$ and $n = x^2 + y^2 + z^2 + w^2$, thus $a(x - y) = 0^2$ is a square.

$x - y$ and $2x - 2y$ are suitable

Case 3. $16 \nmid n$ and $n \in E(1,1,2) = \{4^k(16l+14):\ k,l \in \mathbb{N}\}$.

In this case, $n = 4^k(16l+14)$ for some $k \in \{0,1\}$ and $l \in \mathbb{N}$. Note that $n/2 - (2/a)^2 \notin E(1,1,1)$. So, $n/2 - (2/a)^2 = t^2 + u^2 + v^2$ for some $t,u,v \in \mathbb{N}$ with $t \geqslant u \geqslant v$. As $n/2 - (2/a)^2 \geqslant 8 - 4 > 3$, we have $t \geqslant 2 \geqslant 2/a$. Thus

$$\begin{aligned} n =& 2\left(\left(\frac{2}{a}\right)^2 + t^2\right) + 2(u^2+v^2) \\ =& \left(t+\frac{2}{a}\right)^2 + \left(t-\frac{2}{a}\right)^2 + (u+v)^2 + (u-v)^2 \end{aligned}$$

with

$$a\left(\left(t+\frac{2}{a}\right) - \left(t-\frac{2}{a}\right)\right) = 2^2.$$

This proves that $x - y$ and $2x - 2y$ are both suitable.

Suitable polynomials of the form $ax \pm by$

Conjecture (Z.-W. Sun, April 14, 2016) Let $a, b \in \mathbb{Z}^+$ with $\gcd(a, b)$ squarefree.

(i) The polynomial $ax + by$ is suitable if and only if $\{a, b\} = \{1, 2\}, \{1, 3\}, \{1, 24\}$.

(ii) The polynomial $ax - by$ is suitable if and only if (a, b) is among the ordered pairs

$$(1, 1),\ (2, 1),\ (2, 2),\ (4, 3),\ (6, 2).$$

Remark. In 2016, I proved that any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}$ such that $x + 2y$ is a square (or a cube). In a joint paper with my student Yu-Chen Sun [Acta Arith. 183(2018)], we managed to show that $x + 2y$ is indeed suitable.

Write $n = x^2 + y^2 + z^2 + w^2$ with $x + 3y$ a square

In 1916 Ramanujan conjectured that

(1) *the only positive even numbers not of the form* $x^2 + y^2 + 10z^2$ *are those* $4^k(16l + 6)$ $(k, l \in \mathbb{N})$

and

(2) *sufficiently large odd numbers are of the form* $x^2 + y^2 + 10z^2$.

In 1927 L. E. Dickson [Bull. AMS] proved (1). In 1990 W. Duke and R. Schulze-Pillot [Invent. Math.] confirmed (2). In 1997 K. Ono and K. Soundararajan [Invent. Math.] proved that under the GRH (Generalized Riemann Hypothesis) any odd number greater than 2719 has the form $x^2 + y^2 + 10z^2$.

Z.-W. Sun [J. Number Theory 175(2017)]: Under the GRH, any $n \in \mathbb{N}$ can be written as $n = x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{Z})$ with $x + 3y$ a square.

Yue-Feng She and Hai-Liang Wu [arXiv:2010.02067]: $x + 3y$ is suitable (via the arithmetic theory of ternary quadratic forms).

Suitable $ax - by - cz$ or $ax + by - cz$

Conjecture (Z.-W. Sun, April 14, 2016): (i) Let $a, b, c \in \mathbb{Z}^+$ with $b \leqslant c$ and $\gcd(a, b, c)$ squarefree. Then $ax - by - cz$ is suitable if and only if (a, b, c) is among the five triples

$$(1,1,1),\ (2,1,1),\ (2,1,2),\ (3,1,2),\ (4,1,2).$$

(ii) Let $a, b, c \in \mathbb{Z}^+$ with $a \leqslant b$ and $\gcd(a, b, c)$ squarefree. Then $ax + by - cz$ is suitable if and only if (a, b, c) is among the following 52 triples

$(1,1,1),\ (1,1,2),\ (1,2,1),\ (1,2,2),\ (1,2,3),\ (1,3,1),$
$(1,3,3),\ (1,4,4),\ (1,5,1),\ (1,6,6),\ (1,8,6),\ (1,12,4),\ (1,16,1),$
$(1,17,1),\ (1,18,1),\ (2,2,2),\ (2,2,4),\ (2,3,2),\ (2,3,3),\ (2,4,1),$
$(2,4,2),\ (2,6,1),\ (2,6,2),\ (2,6,6),\ (2,7,4),\ (2,7,7),\ (2,8,2),$
$(2,9,2),\ (2,32,2),\ (3,3,3),\ (3,4,2),\ (3,4,3),\ (3,8,3),\ (4,5,4),$
$(4,8,3),\ (4,9,4),\ (4,14,14),\ (5,8,5),\ (6,8,6),\ (6,10,8),\ (7,9,7),$
$(7,18,7), (7,18,12),\ (8,9,8),\ (8,14,14),\ (8,18,8),\ (14,32,14),$
$(16,18,16),\ (30,32,30),\ (31,32,31),\ (48,49,48),\ (48,121,48).$

$n = x^2 + y^2 + z^2 + w^2$ with $x + y + z$ a square (or a cube)

Theorem (Z.-W. Sun [J. Number Theory 175(2017)]). Any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}$ such that $x + y + z$ is a square (or a cube).

Theorem (Z.-W. Sun [Int. J. Number Theory 15(2019)]).

(i) Any $n \in \mathbb{Z}^+$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ and $|x + y - z| \in \{4^k : k \in \mathbb{N}\}$.

(ii) Any $n \in \mathbb{Z}^+$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ such that

$$x + y - z \in \{\pm 8^k : k \in \mathbb{N}\} \cup \{0\} \subseteq \{t^3 : t \in \mathbb{Z}\}.$$

Remark. The speaker is unable to show that $x + y - z$ (or $x - y - z$) is suitable.

Suitable $ax+by+cz-dw$ or $ax+by-cz-dw$

Conjecture (Z.-W. Sun, April 14, 2016): Let $a,b,c,d\in\mathbb{Z}^+$ with $a\leqslant b\leqslant c$ and $\gcd(a,b,c,d)$ squarefree. Then $ax+by+cz-dw$ is suitable if and only if (a,b,c,d) is among the 12 quadruples

$$(1,1,2,1),\ (1,2,3,1),\ (1,2,3,3),\ (1,2,4,2),\\ (1,2,4,4),\ (1,2,5,5),\ (1,2,6,2),\ (1,2,8,1),\\ (2,2,4,4),\ (2,4,6,4),\ (2,4,6,6),\ (2,4,8,2).$$

Conjecture (Z.-W. Sun, April 14, 2016): Let $a,b,c,d\in\mathbb{Z}^+$ with $a\leqslant b$ and $c\leqslant d$, and $\gcd(a,b,c,d)$ squarefree. Then $ax+by-cz-dw$ is suitable if and only if (a,b,c,d) is among the 9 quadruples

$$(1,2,1,1),\ (1,2,1,2),\ (1,3,1,2),\ (1,4,1,3),\\ (2,4,1,2),\ (2,4,2,4),\ (8,16,7,8),\ (9,11,2,9),\ (9,16,2,7).$$

A general theorem joint with Yu-Chen Sun

Theorem (Yu-Chen Sun and Z.-W. Sun [Acta Arith. 183(2018)]). Let $a, b, c, d \in \mathbb{Z}$ with a, b, c, d not all zero. Let $\lambda \in \{1, 2\}$ and $m \in \{2, 3\}$ Then any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}/(a^2 + b^2 + c^2 + d^2)$ such that $ax + by + cz + dw = \lambda r^m$ for some $r \in \mathbb{N}$.

Proof. Let $n \in \mathbb{N}$. By a result of Z.-W. Sun, we can write $(a^2 + b^2 + c^2 + d^2)n$ as $(\lambda r^m)^2 + t^2 + u^2 + v^2$ with $r, t, u, v \in \mathbb{N}$. Set $s = \lambda r^m$, and define x, y, z, w by

$$\begin{cases} x = \frac{as-bt-cu-dv}{a^2+b^2+c^2+d^2}, \\ y = \frac{bs+at+du-cv}{a^2+b^2+c^2+d^2}, \\ z = \frac{cs-dt+au+bv}{a^2+b^2+c^2+d^2}, \\ w = \frac{ds+ct-bu+av}{a^2+b^2+c^2+d^2}. \end{cases}$$

Proof of the general theorem

Then

$$\begin{cases} ax + by + cz + dw = & s, \\ ay - bx + cw - dz = & t, \\ az - bw - cx + dy = & u, \\ aw + bz - cy - dx = & v. \end{cases}$$

With the help of Euler's four-square identity,

$$x^2 + y^2 + z^2 + w^2 = \frac{s^2 + t^2 + u^2 + v^2}{a^2 + b^2 + c^2 + d^2} = n$$

and

$$ax + by + cz + dw = s = \lambda r^m.$$

This concludes the proof.

Joint work with Yu-Chen Sun

Theorem (Y.-C. Sun and Z.-W. Sun [Acta Arith. 183(2018)])

(i) Let $m \in \mathbb{Z}^+$. Then any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{Z})$ with $x + y + z + w$ an m-th power if and only if $m \leqslant 3$.

(ii) Any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}$ such that $x + 2y + 3z$ is a square (or a cube).

(iii) (Progress on the 1-3-5-Conjecture) Any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, 5z, 5w \in \mathbb{Z}$ such that $x + 3y + 5z$ is a square (or a cube).

A Lemma

The proof of the Theorem needs several lemmas and some previous results of Z.-W. Sun. Here is one of them.

Lemma. Define

$$\begin{cases} x = \frac{s-t-u-2v}{7}, \\ y = \frac{s+t+2u-v}{7}, \\ z = \frac{s-2t+u+v}{7}, \\ w = \frac{2s+t-u+v}{7}. \end{cases}$$

Then

$$x^2 + y^2 + z^2 + w^2 = \frac{s^2 + t^2 + u^2 + v^2}{7}.$$

Also,

$$\begin{aligned} x + y + z + 2w &= s, \\ w + 2x + 3z &= s - t, \\ x + 3y + 5w &= 2s + t. \end{aligned}$$

Joint work with Hai-Liang Wu

Besides the 1-3-5 conjecture, I also conjectured that any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ such that

$$|x + 3y - 5z| \in \{4^k : \ k \in \mathbb{N}\}.$$

In 2017, Hai-Liang Wu and the speaker used the theory of ternary quadratic forms and modular forms to obtain the following progress on the 1-3-5 conjecture.

Theorem (H.-L. Wu and Z.-W. Sun [Acta Arith. 193(2020)]). Any sufficiently large integer n not divisible by 16 can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}$ such that $x + 3y + 5z \in \{1, 4\}$.

In the proof we split $\{n \in \mathbb{N} : \ 16 \nmid n\}$ into two sets

$$A = \bigcup_{k \in \mathbb{N}} \{4k+1, 4k+2, 8k+4\} \ \text{ and } \ B = \bigcup_{k \in \mathbb{N}} \{4k+3, 16k+8\}.$$

Suitable polynomials of the form $ax^2 + by^2 + cz^2$

Conjecture (Z.-W. Sun, April 9, 2016).

(i) Any natural number can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ and $x \geqslant y$ such that $x^2 + 8y^2 + 16z^2$ is a square. Both $x^2 + 3y^2 + 12z^2$ and $3x^2 + 4y^2 + 9z^2$ are suitable.

(ii) If a, b, c are positive integers with $ax^2 + by^2 + cz^2$ suitable, then a, b, c cannot be pairwise coprime.

Conjecture (Z.-W. Sun, March 13-14, 2018):

$$(3x)^2+(4y)^2+(12z)^2,\ (12x)^2+(15y)^2+(20z)^2,\ (12x)^2+(21y)^2+(28z)^2$$

are suitable.

Suitable polynomials related to Pythagorean triples

Conjecture (Z.-W. Sun, April 12, 2016). Any $n \in \mathbb{Z}^+$ can be written as $w^2 + x^2 + y^2 + z^2$ with $w \in \mathbb{Z}^+$ and $x, y, z \in \mathbb{N}$ such that $(10w + 5x)^2 + (12y + 36z)^2$ is a square.

Remark. Yu-Chen Sun and Z.-W. Sun [Acta Arith. 183(2018)] proved that any $n \in \mathbb{N}$ can be written as $w^2 + x^2 + y^2 + z^2$ with w, x, y, z *integers* such that $(10w + 5x)^2 + (12y + 36z)^2$ is a square.

Theorem (Z.-W. Sun, May 16, 2016). Any $n \in \mathbb{Z}^+$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ and $y > 0$ such that $x + 4y + 4z$ and $9x + 3y + 3z$ are the two legs of a right triangle with positive integer sides.

Conjectures involving cubic diophantine equations

Conjecture (Z.-W. Sun, March 2017).

(i) Each $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ such that $x^3 + (y - z)^3$ is a square.

(ii) Every $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{Z})$ such that $x^3 + 2y^3$ is a square.

Remark. We have some other similar conjectures.

Suitable polynomials of the form $ax^4 + by^3z$

The following conjecture sounds very mysterious!

Conjecture (Z.-W. Sun, 2016) Let a and b be nonzero integers with $\gcd(a, b)$ squarefree. Then the polynomial $ax^4 + by^3z$ is suitable if and only if (a, b) is among the ordered pairs

$$(1,1),\ (1,15),\ (1,20),\ (1,36),\ (1,60),\ (1,1680) \text{ and } (9,260).$$

Examples:

$$9983 = 63^2 + 54^2 + 17^2 + 53^2$$

with $63^4 + 54^3 \times 17 = 4293^2$, and

$$20055 = 47^2 + 6^2 + 77^2 + 109^2$$

with $47^4 + 1680 \times 6^3 \times 77 = 5729^2$.

Some other conjectures

Conjecture (Z.-W. Sun, 2016). Any $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ such that $xy + 2zw$ or $xy - 2zw$ is a square.

Conjecture (Z.-W. Sun, 2016). All the following polynomials

$$4x^2 + 5y^2 + 20zw,\ x^2 + 3y^2 + 5z^2 - 8w^2,$$
$$36x^2y + 12y^2z + z^2x,\ w^2x^2 + 3x^2y^2 + 2y^2z^2,$$
$$w^2x^2 + 5x^2y^2 + 80y^2z^2 + 20z^2w^2$$

are suitable.

Theorem (Z.-W. Sun [J. Number Theory 175(2017)]). All the polynomials

$$x^2y^2 + y^2z^2 + z^2x^2,\ x^2y^2 + 4y^2z^2 + 4z^2x^2,\ x^4 + 8y^3z + 8yz^3$$

are suitable.

Restrictions involving powers of four

Theorem (Z.-W. Sun [Int. J. Number Theory 15(2019)]) (i) Any $n \in \mathbb{Z}^+$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ and $|x - 2y| \in \{4^k : k \in \mathbb{N}\}$.

(ii) Any $n \in \mathbb{Z}^+$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}$ and $x + y + 2z \in \{4^k : k \in \mathbb{N}\}$.

(iii) Any $n \in \mathbb{Z}^+$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}$ and $x + 2y + 2z \in \{4^k : k \in \mathbb{N}\}$.

Conjecture (Z.-W. Sun, 2016). Any $n \in \mathbb{Z}^+$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ such that

$$x + 2y - 2z \in \{4^k : k \in \mathbb{N}\}.$$

Remark. Qing-Hu Hou has verified this for n up to 10^9.

The 24-conjecture with \$2400 prize

24-Conjecture (Z.-W. Sun, Feb. 4, 2017). Each $n \in \mathbb{N}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ such that both x and $x + 24y$ are squares.

Remark. Qing-Hu Hou has verified this for $n \leqslant 10^{10}$. I would like to offer 2400 US dollars as the prize for the first proof.

$$
\begin{aligned}
12 &= 1^2 + 1^2 + 1^2 + 3^2 \text{ with } 1 = 1^2 \text{ and } 1 + 24 \times 1 = 5^2,\\
23 &= 1^2 + 2^2 + 3^2 + 3^2 \text{ with } 1 = 1^2 \text{ and } 1 + 24 \times 2 = 7^2,\\
24 &= 4^2 + 0^2 + 2^2 + 2^2 \text{ with } 4 = 2^2 \text{ and } 4 + 24 \times 0 = 2^2,\\
47 &= 1^2 + 1^2 + 3^2 + 6^2 \text{ with } 1 = 1^2 \text{ and } 1 + 24 \times 1 = 5^2,\\
71 &= 1^2 + 5^2 + 3^2 + 6^2 \text{ with } 1 = 1^2 \text{ and } 1 + 24 \times 5 = 11^2,\\
168 &= 4^2 + 4^2 + 6^2 + 10^2 \text{ with } 4 = 2^2 \text{ and } 4 + 24 \times 4 = 10^2,\\
344 &= 4^2 + 0^2 + 2^2 + 18^2 \text{ with } 4 = 2^2 \text{ and } 4 + 24 \times 0 = 2^2,\\
632 &= 0^2 + 6^2 + 14^2 + 20^2 \text{ with } 0 = 0^2 \text{ and } 0 + 24 \times 6 = 12^2,\\
1724 &= 25^2 + 1^2 + 3^2 + 33^2 \text{ with } 25 = 5^2 \text{ and } 25 + 24 \times 1 = 7^2.
\end{aligned}
$$

Write $n \in \mathbb{Z}^+$ as $4^k(1+x^2+y^2)+z^2$

Conjecture (Z.-W. Sun, August 2016). Any $n \in \mathbb{Z}^+$ can be written as $w^2(1+x^2+y^2)+z^2$ with $w \in \mathbb{Z}^+$, $x, y, z \in \mathbb{Z}$ and $x \equiv y \pmod 2$. Moreover, when $n \neq 449$ we may require further that w is a power of two.

Remark. I can show this under the GRH.

Theorem (Z.-W. Sun [J. Number Theory 175(2017)]). Any positive integer can be written as $4^k(1+4x^2+y^2)+z^2$ with $k, x, y, z \in \mathbb{N}$.

Unify the four-square theorem and the twin prime conjecture

The following conjecture implies the twin prime conjecture.

Conjecture (Z.-W. Sun, August 23, 2017). Any positive odd integer can be written as $x^2+y^2+z^2+w^2$ with $x,y,z,w\in\mathbb{Z}$ such that $p=x^2+3y^2+5z^2+7w^2$ and $p-2$ are twin prime.

Example.

$$39=1^2+3^2+5^2+2^2$$

with $1^2+3\cdot3^2+5\cdot5^2+7\cdot2^2=181$ and $181-2=179$ twin prime. Also,

$$123=7^2+3^2+7^2+4^2$$

with $7^2+3\cdot3^2+5\cdot7^2+7\cdot4^2=433$ and $433-2=431$ twin prime.

Restricted sums of four squares involving primes

Conjecture (Z.-W. Sun, August 19, 2017). Any positive odd integer can be written as $x^2 + y^2 + z^2 + 4w^2$ with $x, y, z, w \in \mathbb{N}$ such that $2^x + 2^y + 2^z + 1$ is prime.

Example. $143 = 1^2 + 5^2 + 9^2 + 4 \cdot 3^2$ with $2^1 + 2^5 + 2^9 + 1 = 547$ prime.

Conjecture (Z.-W. Sun, August 20, 2017). Any odd integer $n > 1$ can be written as $x^2 + y^2 + z^2 + w^2$ $(x, y, z, w \in \mathbb{N})$ such that $2^{x+y} + 2^{z+w} + 1$ is prime.

Example. $197 = 6^2 + 6^2 + 2^2 + 11^2$ with $2^{6+6} + 2^{2+11} + 1 = 12289$ prime. And

$$2 \times 6998538 + 1 = 122^2 + 220^2 + 208^2 + 3727^2$$

with $2^{122+220} + 2^{208+3727} + 1 = 2^{342} + 2^{3935} + 1$ a prime of 1185 decimal digits.

I have verified both conjectures for positive odd integers not more than 2×10^7.

Part III. Solution of the 1-3-5 Conjecture

1-3-5 Conjecture was proved in 2020

In 2019 Detlev Hoffmann released arXiv:1902.07109 in which the author claimed to prove the integer version of the 1-3-5 conjecture by using Mordell's result. I pointed out that the proof is wrong.

In 2020, Prof. António Machiavelo and his PhD student Nikolaos Tsopanidis (Greek) at Porto Univ. posted their paper

Zhi-Wei Sun's 1-3-5 Conjecture and Variations, arXiv:2003.02592

to arXiv in which they reduced the 1-3-5 Conjecture to verifying it up to

$$c = 105103560126 \approx 1.051 \times 10^{11}.$$

In their computational report joint with Rogério Reis

Report on Zhi-Wei Sun's 1-3-5 Conjecture and some of its Refinements, arXiv:2005.13526

the 1-3-5 Conjecture was reported to be verified up to c.

Thus 1-3-5 Conjecture has been completed proved!

Hamliton quaternions

The Hamilton quaternions have the form

$$\zeta = a + bi + cj + dk \text{ with } a, b, c, d \in \mathbb{R}$$

with the multiplication rule

$$ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

All the Hamiltion quaternions form a skew field (division ring).

For a Hamiltion quaternion $\zeta = a + bi + cj + dk$, its *conjugate* is $\bar{\zeta} = a - bi - cj - dk$, and its *norm* is

$$N(\zeta) = \zeta\bar{\zeta} = a^2 + b^2 + c^2 + d^2.$$

By Euler's four-square identity, for any two Hamliton quaternions α, β we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

Real parts of Hamliton quaternions

For a Hamliton quaternion

$$\zeta = a + bi + cj + dk \quad \text{with } a, b, c, d \in \mathbb{R},$$

we call $\Re(\zeta) = a$ the *real part* of ζ.

For two Hamiltion quaternions ζ and $\rho \neq 0$, clearly

$$\overline{\rho^{-1}\zeta\rho} = N(\rho^{-1}\zeta\rho)(\rho^{-1}\zeta\rho)^{-1} = N(\zeta)\rho^{-1}\zeta^{-1}\rho = \rho^{-1}\bar{\zeta}\rho,$$

thus

$$2\Re(\rho^{-1}\zeta\rho) = \rho^{-1}\zeta\rho + \overline{\rho^{-1}\zeta\rho} = \rho^{-1}(\zeta + \bar{\zeta})\rho = \rho^{-1}2\Re(\zeta)\rho = 2\Re(\zeta)$$

and hence

$$\Re(\rho^{-1}\zeta\rho) = \Re(\zeta).$$

Hurwitz integers

The ring of Hurwitz integers is

$$\mathcal{H} = \left\{ a + bi + cj + dk : \; a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \frac{1}{2} + \mathbb{Z} \right\}.$$

This ring is left (or right) Euclidean, i.e., for any $\alpha, \beta \in \mathcal{H}$ with $\beta \neq 0$, there are $\eta, \gamma \in \mathcal{H}$ such that

$$\alpha = \beta\eta + \gamma \quad \text{and} \quad N(\gamma) < N(\alpha).$$

Lagrange's four-square theorem can be proved via Hurwitz integers, but its proof is essentially equivalent to the usual proof of Lagrange.

Lipschitz integers

The ring of Lipschitz integers is

$$\mathcal{L} = \{a + bi + cj + dk : \ a, b, c, d \in \mathbb{Z}\}.$$

This ring is neither left nor right Euclidean. This is why it is less known than the ring of Hurwitz integers.

For $\alpha, \beta \in \mathcal{L}$, if $\alpha = \gamma\beta$ for some $\gamma \in \mathcal{L}$ then we call β a *right divisor* of α.

G. Pall published two papers to study factorizations in $\mathcal{L}$:

1. G. Pall, et al., *On the factorization of generalized quaternions*, Duke Math. J. **4** (1938), 696–704.

2. G. Pall, *On the arithmetic of quaternions*, Trans. Amer. Math. Soc. **47** (1940), 487–500.

Pall's theorem

Pall's Theorem (G. Pall [Trans. Amer. Math. Soc. 47(1940)]). Let $v = v_0 + v_1 i + v_2 j + v_3 k \in \mathcal{L}$ and let m be a positive integer dividing $N(v)$. Then there is a unique, up to left multiplication by units, right divisor of v of norm m, provided one of the following conditions:

(i) $2 \nmid m$ and $\gcd(v_0, v_1, v_2, v_3, m) = 1$.

(ii) $2 \mid m$, $2 \nmid \frac{N(v)}{m}$, and $\gcd(v_0, v_1, v_2, v_3) = 1$.

Pall's Theorem implies the following result.

Theorem. Let $Q = a + bi + cj + dk \in \mathcal{L}$ and suppose that $N(Q) = p_1 \ldots p_r$, where $p_1, \ldots, p_r$ are primes. There there are $P_1, \ldots, P_r \in \mathcal{L}$ with $N(P_i) = p_i$ for all $i = 1, \ldots, r$ such that $P_1 \ldots P_r = Q$.

A general theorem

Theorem (Machiavelo and Tsopanidis, 2020). Let $m, n.\ell \in \mathbb{N}$ with $m\ell - n^4 \in \mathbb{N} \setminus E$, where $E = \{4^s(8t+7) : \ s, t \in \mathbb{N}\}$. Then, for some $a, b, c, d \in \mathbb{N}$ with $a^2 + b^2 + c^2 + d^2 = \ell$, the system

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = m, \\ ax + by + cz + dw = n^2 \end{cases}$$

has integer solutions.

Proof. By the Gauss-Legendre theorem, $m\ell - n^4 = A^2 + B^2 + C^2$ for some $A, B, C \in \mathbb{Z}$. Let $\delta = n^2 + Ai + Bj + Ck \in \mathcal{L}$. Then $N(\delta) = m\ell$. Suppose that $\ell = p_1 \dots p_r$ and $m = q_1 \dots q_s$, where $p_1, \dots, p_r, q_1, \dots, q_s$ are primes. As $N(\delta) = p_1 \dots p_r q_1 \dots q_s$, there are $P_1, \dots, P_r, Q_1, \dots, Q_s \in \mathcal{L}$ with

$$N(P_1) = p_1, \dots, N(P_r) = p_r, \ N(Q_1) = q_1, \dots, N(Q_s) = q_s$$

such that $\delta = P_1 \dots P_r Q_1 \dots Q_s$.

Continue the proof

Write $P_1 \dots P_r = a - bi - cj - dk$ with $a, b, c, d \in \mathbb{Z}$, and $Q_1 \dots Q_s = x_0 + y_0 i + z_0 j + w_0 k$ with $x_0, y_0, z_0, w_0 \in \mathbb{Z}$. Set

$$\zeta = a + bi + cj + dk \text{ and } \xi = x_0 + y_0 i + z_0 j + w_0 k.$$

Then

$$a^2 + b^2 + c^2 + d^2 = N(\zeta) = N(\bar{\zeta}) = N(P_1 \dots P_r) = p_1 \dots p_r = \ell,$$

$$x_0^2 + y_0^2 + z_0^2 + w_0^2 = N(\xi) = N(Q_1 \dots Q_s) = q_1 \dots q_s = m.$$

Note that $\bar{\zeta}\xi = P_1 \dots P_r Q_1 \dots Q_s = \delta$ and

$$\zeta \cdot \xi = ax_0 + by_0 + cz_0 + dw_0 = \Re(\bar{\zeta}\xi) = \Re(\delta) = n^2.$$

Choose $x \in \{\pm x_0\}$, $y \in \{\pm y_0\}$, $z \in \{\pm z_0\}$ and $w \in \{\pm w_0\}$ so that $ax_0 = |a|x,\ by_0 = |b|y,\ cz_0 = |c|z,\ dw_0 = |d|w$. Then $x^2 + y^2 + z^2 + w^2 = m$ and $|a|x + |b|y + |c|z + |d|w = n^2$.

Application to the 1-3-5 Conjecture

There are exactly two ways to write $\ell = 35$ as a sum of four squares:

$$35 = 1^2 + 3^2 + 5^2 + 0^2 = 1^2 + 3^2 + 3^2 + 4^2.$$

So, by the general theorem we obtain the following consequence.

Corollary (Machiavelo and Tsopanidis). Let $m, n \in \mathbb{N}$ with $35m - n^4 \in \mathbb{N} \setminus E$. Then, either the system

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = m, \\ x + 3y + 5z = n^2 \end{cases} \tag{1-3-5}$$

has integer solutions, or the system

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = m, \\ x + 3y + 3z + 4w = n^2 \end{cases} \tag{1-3-3-4}$$

has integer solutions.

Application to the 1-3-5 Conjecture

There are exactly two ways to write $\ell = 35$ as a sum of four squares:

$$35 = 1^2 + 3^2 + 5^2 + 0^2 = 1^2 + 3^2 + 3^2 + 4^2.$$

So, by the general theorem we obtain the following consequence.

Corollary (Machiavelo and Tsopanidis). Let $m, n \in \mathbb{N}$ with $35m - n^4 \in \mathbb{N} \setminus E$. Then, either the system

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = m, \\ x + 3y + 5z = n^2 \end{cases} \tag{1-3-5}$$

has integer solutions, or the system

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = m, \\ x + 3y + 3z + 4w = n^2 \end{cases} \tag{1-3-3-4}$$

has integer solutions.

From (1-3-3-4) to (1-3-5)

For $\alpha, \alpha' \in \mathcal{L}$, we write $\alpha \sim \alpha'$ if we can obtain α' from α by permutating and changing the signs of the coordinates of α.

Let

$$\alpha = 1 + 3i + 5j \ \text{ and } \ \beta = 1 + 3i + 3j + 4k.$$

Suppose that (1-3-3-4) has a solution with $x, y, z, w \in \mathbb{Z}$. Let $\gamma = x - yi - zj - wk$. Then $\Re(\gamma\beta) = x + 3y + 3z + 4w = n^2$ and $N(\gamma) = m$. If we find $\rho, \sigma \in \mathcal{L} \setminus \{0\}$ with

$$\alpha' = \sigma^{-1}\beta\rho \sim \alpha \text{ and } \gamma' = \rho^{-1}\gamma\sigma \in \mathcal{L},$$

then

$$\Re(\gamma\beta) = \Re(\rho^{-1}\gamma\beta\rho) = \Re(\gamma'\alpha'),$$

$$N(\sigma) = N(\rho), \ N(\rho^{-1}\gamma\sigma) = N(\gamma) = m$$

(since $N(\alpha) = N(\beta) = 35$) and hence we obtain a solution to (1-3-5).

An auxiliary theorem

Using the above idea, A, Machiavelo and N. Tsopanidis obtained the following result.

Theorem. Let $m, n \in \mathbb{N}$ with $35m - n^4 \in \mathbb{N} \setminus E$.

(i) If $3 \mid m$ and $\gcd(n, 15) = 1$, then the system (1-3-5) has integer solutions.

(ii) If $m \equiv 1 \pmod 3$, $3 \mid n$ but $5 \nmid n$, then the system (1-3-5) has integer solutions.

(iii) If $m \equiv -1 \pmod 3$ and $\gcd(n, 105) = 1$, then the system (1-3-5) has integer solutions.

Integer solutions to (1-3-5)

Theorem (A. Machiavelo and N. Tsopanidis). Any positive integer m can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}$ and $x + 3y + 5z \in \{4^a b^2 : \ a \in \mathbb{N}, \ b \in \{1, 2, 3, 6\}\}$.

This provides an advance on the following conjecture.

Conjecture (Sun [Int. J. Number Theory 15(2019)]). Any positive integer can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ and $|x + 3y - 5z| \in \{4^a : \ a \in \mathbb{N}\}$.

Obtain natural solutions from integer solutions

A. Machiavelo and N. Tsopanidis found a way to obtain natural solutions from integer solutions of (1-3-5). This was further improved and generalized by the speaker.

Theorem (Z.-W. Sun, arXiv:2010.05775). Let a, b, c, d, m be nonnegative real numbers with $a^2+b^2+c^2+d^2 \neq 0$. Suppose that x, y, z, w are real numbers satisfying

$$\begin{cases} x^2+y^2+z^2+w^2=m, \\ ax+by+cz+dw=s, \end{cases}$$

where

$$s \geqslant \sqrt{m(a^2+b^2+c^2+d^2-\min(\{a^2,b^2,c^2,d^2\}\setminus\{0\}))}.$$

Then all the numbers ax, by, cz, dw are nonnegative.

Proof

Let

$$t = ay - bx + cw - dz,\ u = az - bw - cx + dy,\ v = aw + bz - cy - dx.$$

By Euler's four-square identity, we have

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) = s^2 + t^2 + u^2 + v^2.$$

Solving the system of equations

$$\begin{cases} ax + by + cz + dw = s, \\ ay - bx + cw - dz = t, \\ az - bw - cx + dy = u, \\ aw + bz - cy - dx = v, \end{cases}$$

we find that

$$\begin{cases} x = \frac{as - bt - cu - dv}{a^2 + b^2 + c^2 + d^2}, \\ y = \frac{bs + at + du - cv}{a^2 + b^2 + c^2 + d^2}, \\ z = \frac{cs - dt + au + bv}{a^2 + b^2 + c^2 + d^2}, \\ w = \frac{ds + ct - bu + av}{a^2 + b^2 + c^2 + d^2}. \end{cases} \qquad (*)$$

Continue the proof

Suppose that $a > 0$. Then

$$s^2 \geqslant m(a^2 + b^2 + c^2 + d^2 - a^2) = (b^2 + c^2 + d^2)m$$

and hence

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)s^2 \geqslant &(b^2 + c^2 + d^2)(a^2 + b^2 + c^2 + d^2)m \\ = &(b^2 + c^2 + d^2)(s^2 + t^2 + u^2 + v^2).\end{aligned}$$

Thus $a^2 s^2 \geqslant (b^2 + c^2 + d^2)(t^2 + u^2 + v^2)$. By the Cauchy-Schwarz inequality,

$$(bt + cu + dv)^2 \leqslant (b^2 + c^2 + d^2)(t^2 + u^2 + v^2).$$

Therefore $as \geqslant |bt + cu + dv|$ and hence $x > 0$ in view of $(*)$.

Similarly, $y \geqslant 0$ if $b > 0$, and $z \geqslant 0$ if $d > 0$. This ends the proof.

Part IV. Sums of Two Squares and Two Other Terms

Four-square Conjecture and 1-2-3 Conjecture

Four-square Conjecture (Z.-W. Sun, June 21, 2019). Any integer $n > 1$ can be written as $x^2 + y^2 + (2^a 3^b)^2 + (2^c 5^d)^2$ with $x, y, a, b, c, d \in \mathbb{N}$.

Remark. See `http://oeis.org/A308734` for related data. In 2019 G. Resta verified the conjecture for n up to 10^{10}.

Conjecture (1-2-3 Conjecture, Z.-W. Sun, Oct. 10, 2020).

(i) (Weak version) Any positive odd integer can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ and $x + 2y + 3z \in \{2^a : \ a \in \mathbb{Z}^+\}$.

(ii) (Strong version) Any integer $m > 4627$ with $m \not\equiv 0, 2 \pmod 8$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{N}$ and $x + 2y + 3z \in \{4^a : \ a \in \mathbb{Z}^+\}$.

Write $n = a^2 + b^2 + 3^c + 5^d$

Conjecture (Z.-W. Sun, April 28, 2018). Any integer $n > 1$ can be written as $a^2 + b^2 + 3^c + 5^d$ with $a, b, c, d \in \mathbb{N} = \{0, 1, 2, \ldots\}$.

Remark. I have verified this for n up to 2×10^{10}, and I'd like to offer 3500 US dollars as the prize for the first proof of this conjecture. I also conjecture that 5^d in the conjecture can be replaced by 2^d.

Example.

$$2 = 0^2 + 0^2 + 3^0 + 5^0,\ 5 = 0^2 + 1^2 + 3^1 + 5^0,\ 25 = 1^2 + 4^2 + 3^1 + 5^1.$$

Conjecture (Z.-W. Sun, April 2018). Any integer $n > 1$ can be written as the sum of two squares and two central binomial coefficients. Also, any integer $n > 1$ can be written as the sum of two triangular numbers and two powers of five.

Remark. I have verified this for n up to 10^{10}.

References

For the main sources of my above conjectures and related results, you may look at the following papers:

1. Zhi-Wei Sun, *Refining Lagrange's four-square theorem*, J. Number Theory 175(2017), 167–190. `arXiv:1604.06723`
2. Yu-Chen Sun and Zhi-Wei Sun, *Some variants of Lagrange's four squares theorem*, Acta Arith. 183(2018), no.4, 339-356.
3. Zhi-Wei Sun, *Restricted sums of four squares*, Int. J. Number Theory **15** (2019), 1863–1893.
4. Hai-Liang Wu and Zhi-Wei Sun, *On the 1-3-5 conjecture and related topics*, Acta Arith. **193** (2020), 253–268.
5. A. Machiavelo and N. Tsopanidis, *Zhi-Wei Sun's 1-3-5 conjecture and variations*, arXiv:2003.02592 [math.NT], 2020.
6. A. Machiavelo, R. Reis and N. Tsopanidis, *Report on Zhi-Wei Sun's "1-3-5 conjecture" and some of its refinements*, arXiv:2005.13526 [math.NT], 2020.

Thank you!