

# REFINEMENTS OF LAGRANGE'S FOUR-SQUARE THEOREM

LEO GOLDBAKHER AND PAUL POLLACK

**ABSTRACT.** A well-known theorem of Lagrange asserts that every nonnegative integer  $n$  can be written in the form  $a^2 + b^2 + c^2 + d^2$ , where  $a, b, c, d \in \mathbb{Z}$ . We characterize the values assumed by  $a + b + c + d$  as we range over all such representations of  $n$ .

Our point of departure is the following signature result from a first course in number theory.

**Lagrange's four-square theorem.** *Every nonnegative integer can be written as the sum of four integer squares. That is, for every  $n \in \mathbb{N}$ , there are  $a, b, c, d \in \mathbb{Z}$  with*

$$n = a^2 + b^2 + c^2 + d^2. \quad (1)$$

For instance ( $n = 2017$ ), we have

$$2017 = 18^2 + 21^2 + 24^2 + 26^2.$$

Twenty years before Lagrange's proof, Euler had already conjectured a refinement of the four-square theorem for odd numbers  $n$ . The following statement can be found in a letter to Goldbach dated June 9, 1750.

**Conjecture 1.** *Every odd positive integer  $n$  has a representation in the form (1) satisfying the extra constraint  $a + b + c + d = 1$ .*

Picking back up our earlier example, when  $n = 2017$ , Euler's conjecture is satisfied with  $a = -18$ ,  $b = 21$ ,  $c = 24$ , and  $d = -26$ . A proof of Euler's conjecture was posted to MathOverflow by Franz Lemmermeyer in September 2010.<sup>1</sup>

Much more recently, Sun & Sun (apparently unaware of Euler's conjecture) presented a number of related refinements of Lagrange's theorem [3] (cf. [4]). One of their many results is that for every  $n \in \mathbb{N}$ , there is a representation (1) with  $a + b + c + d$  a square, as well as one with  $a + b + c + d$  a cube [3, Theorem 1.1(a)].

We can unify all the above assertions by introducing the *sum spectrum*

$$\mathcal{S}(n) = \{a + b + c + d : a^2 + b^2 + c^2 + d^2 = n\}.$$

Lagrange's theorem is equivalent to  $\mathcal{S}(n) \neq \emptyset$ ; Euler's conjecture asserts that  $1 \in \mathcal{S}(n)$  for all odd  $n \in \mathbb{N}$ ; and Sun & Sun's theorem asserts that  $\mathcal{S}(n)$  contains a perfect square and a perfect cube for every  $n$ . Our goal in this note is to completely describe the set  $\mathcal{S}(n)$ .

We have not found our results stated anywhere in the literature, but we do not claim they are novel. In the introduction to his resolution [1] of Fermat's polygonal number conjecture, Cauchy poses the following problem: *Décomposer un nombre entier donné en*

---

LG is partially supported by an NSA Young Investigator grant. PP is partially supported by NSF award DMS-1402268.

<sup>1</sup>See <https://mathoverflow.net/questions/37278/euler-and-the-four-squares-theorem>.

$n$	exceptional $T$
1	$\emptyset$
2	$\emptyset$
3	$\emptyset$
4	$\emptyset$
5	$\emptyset$
6	$\emptyset$
7	$\emptyset$
8	$\{\pm 2\}$
9	$\emptyset$
10	$\emptyset$
11	$\emptyset$
12	$\emptyset$
13	$\emptyset$
14	$\emptyset$
15	$\emptyset$
16	$\{\pm 2, \pm 6\}$

$n$	exceptional $T$
17	$\emptyset$
18	$\emptyset$
19	$\emptyset$
20	$\emptyset$
21	$\emptyset$
22	$\emptyset$
23	$\emptyset$
24	$\{\pm 2, \pm 6\}$
25	$\emptyset$
26	$\emptyset$
27	$\emptyset$
28	$\{0\}$
29	$\emptyset$
30	$\emptyset$
31	$\emptyset$
32	$\{\pm 2, \pm 4, \pm 6, \pm 10\}$

$n$	exceptional $T$
33	$\emptyset$
34	$\emptyset$
35	$\emptyset$
36	$\emptyset$
37	$\emptyset$
38	$\emptyset$
39	$\emptyset$
40	$\{\pm 2, \pm 6, \pm 10\}$
41	$\emptyset$
42	$\emptyset$
43	$\emptyset$
44	$\{\pm 8\}$
45	$\emptyset$
46	$\emptyset$
47	$\emptyset$
48	$\{\pm 2, \pm 6, \pm 10\}$

TABLE 1. Values of  $T$  satisfying (2) and (3) but not belonging to  $\mathcal{S}(n)$ .

*quatre carrés dont les racines fassent une somme donnée.*<sup>2</sup> For Cauchy, “racines” are nonnegative; hence, he is asking for a description of

$$\mathcal{S}^+(n) := \{a + b + c + d : a, b, c, d \in \mathbb{N} \text{ and } a^2 + b^2 + c^2 + d^2 = n\}.$$

Cauchy goes on to prove a partial characterization of  $\mathcal{S}^+(n)$  (see Remark 1 below for a summary of his results), by essentially the same methods we describe below. Despite being anticipated, we believe an explicit description of  $\mathcal{S}(n)$  is sufficiently interesting (and Cauchy’s work on  $\mathcal{S}^+(n)$  sufficiently underappreciated) to warrant popularization here. Moreover, we will show how our characterization of  $\mathcal{S}(n)$  immediately implies both Sun & Sun’s theorems and a generalization of Euler’s conjecture.

We begin by recording two easy observations. First, since an integer and its square have the same parity, every  $T \in \mathcal{S}(n)$  satisfies

$$T \equiv n \pmod{2}. \quad (2)$$

Second, for any real numbers  $a, b, c, d$ , the Cauchy–Schwarz inequality yields

$$\begin{aligned} (a + b + c + d)^2 &\leq (a^2 + b^2 + c^2 + d^2)(1^2 + 1^2 + 1^2 + 1^2) \\ &= 4(a^2 + b^2 + c^2 + d^2); \end{aligned}$$

it follows that every  $T \in \mathcal{S}(n)$  satisfies

$$T^2 \leq 4n. \quad (3)$$

As shown in Table 1, the necessary conditions (2) and (3) are quite often (but not always) sufficient for membership in  $\mathcal{S}(n)$ . The following theorem, which is our main result, tells the full story.

---

<sup>2</sup>Decompose a given whole number into four squares whose roots make a given sum.

**Theorem 2.** Suppose  $n$  and  $T$  are integers satisfying (2). Then  $T \in \mathcal{S}(n)$  if and only if  $4n - T^2$  is a sum of three integer squares.

Note that (3) is implied by the condition on  $4n - T^2$  and so does not need to be included explicitly as a hypothesis in Theorem 2.

To convince the reader that Theorem 2 qualifies as a complete description of  $\mathcal{S}(n)$ , we recall the following classical result (see the Appendix to Chapter IV of [2] for a proof).

**Legendre–Gauss three-squares theorem.** Let  $n \in \mathbb{N}$ . Then  $n$  can be written as a sum of three squares if and only if  $n \neq 4^k(8\ell + 7)$  for any  $k, \ell \in \mathbb{N}$ .

*Proof of Theorem 2.* We begin by recording the easily-verified identity

$$\begin{aligned} (2(a+b) - T)^2 + (2(a+c) - T)^2 + (2(b+c) - T)^2 + T^2 \\ = 4a^2 + 4b^2 + 4c^2 + 4(T - a - b - c)^2. \end{aligned} \quad (4)$$

Thus if  $T \in \mathcal{S}(n)$ , say with  $a^2 + b^2 + c^2 + d^2 = n$  and  $a + b + c + d = T$ , then

$$(2(a+b) - T)^2 + (2(a+c) - T)^2 + (2(b+c) - T)^2 = 4n - T^2,$$

so that  $4n - T^2$  is a sum of three squares.

Conversely, suppose that  $4n - T^2$  is a sum of three squares, say

$$4n - T^2 = A^2 + B^2 + C^2. \quad (5)$$

In view of (4), it is enough to show that—after possibly swapping the signs of  $A$ ,  $B$ ,  $C$ —there are  $a, b, c \in \mathbb{Z}$  with

$$2a + 2b - T = A, \quad 2a + 2c - T = B, \quad 2b + 2c - T = C. \quad (6)$$

Indeed, in that case setting  $d = T - (a + b + c)$ , we have

$$a + b + c + d = T,$$

and

$$\begin{aligned} 4(a^2 + b^2 + c^2 + d^2) - T^2 \\ = (2a + 2b - T)^2 + (2a + 2c - T)^2 + (2b + 2c - T)^2 \\ = A^2 + B^2 + C^2 = 4n - T^2, \end{aligned}$$

so that

$$a^2 + b^2 + c^2 + d^2 = n.$$

Thus, we focus our attention on (6).

Solving for  $a, b, c$  in terms of  $A, B, C$  gives

$$a = \frac{1}{4}(A + B - C + T), \quad b = \frac{1}{4}(A - B + C + T), \quad c = \frac{1}{4}(-A + B + C + T).$$

We claim that  $A, B, C$ , and  $T$  must all have the same parity. To see this, note that (5) gives  $A^2 + B^2 + C^2 \equiv -T^2 \pmod{4}$ . If  $T$  is odd then  $A^2 + B^2 + C^2 \equiv 3 \pmod{4}$ , and a moment's thought shows that all of  $A, B$ , and  $C$  must be odd. Similarly, if  $T$  is even, then  $A^2 + B^2 + C^2 \equiv 0 \pmod{4}$ , and this forces  $A, B$ , and  $C$  to all be even. In either case, the difference between any pair of  $A, B$ , and  $C$  is even, so the difference between

any pair of  $a$ ,  $b$ , and  $c$  is an integer. It follows that if any of  $a, b, c \in \mathbb{Z}$ , then all three are in  $\mathbb{Z}$ . Moreover,

$$A + B - C + T \equiv A + B + C + T \equiv A^2 + B^2 + C^2 + T^2 \equiv 4n \equiv 0 \pmod{2},$$

and so the only way we can fail to have  $a \in \mathbb{Z}$  (and hence all of  $a, b, c \in \mathbb{Z}$ ) is if

$$A + B - C + T \equiv 2 \pmod{4}. \quad (7)$$

If  $T$  is odd, then  $A$  is odd, and so if necessary we can replace  $A$  with  $-A$  to avoid (7). If  $T$  is even, we will show that (7) cannot occur. Indeed, (7) implies that  $8 \nmid (A + B - C + T)^2$ . But

$$\begin{aligned} (A + B - C + T)^2 &= A^2 + B^2 + C^2 + T^2 + 2(AB - AC + AT - BC + BT - CT) \\ &= 4n + 2(AB - AC + AT - BC + BT - CT) \\ &\equiv 0 \pmod{8}; \end{aligned}$$

here we used that  $n \equiv T \equiv 0 \pmod{2}$  and that all of  $A, B, C$ , and  $T$  are even.  $\square$

Let us see how Theorem 2 makes quick work of both the conjecture of Euler and the theorems of Sun & Sun. We begin with the latter. If  $4n$  itself is a sum of three squares, then Theorem 2 shows that  $T = 0 \in \mathcal{S}(n)$ , and 0 is both a square and a cube. Otherwise, by the Legendre–Gauss theorem,  $4n = 4^{k+1}(8\ell + 7)$ , where  $k$  and  $\ell$  are nonnegative integers. Then

$$\begin{aligned} 4n - (2^k)^2 &= 4^k(32\ell + 27), \quad 4n - (2^{k+1})^2 = 4^{k+1}(8\ell + 6), \\ &\text{and} \quad 4n - (2^{k+2})^2 = 4^{k+1}(8\ell + 3); \end{aligned}$$

invoking the Legendre–Gauss theorem once more, we see that all three of these numbers are sums of three squares. By Theorem 2, all of  $2^k, 2^{k+1}, 2^{k+2}$  must belong to  $\mathcal{S}(n)$ . Clearly, the set  $\{2^k, 2^{k+1}, 2^{k+2}\}$  contains both a square and a cube.

As for Euler’s conjecture, we prove the following generalization (which, for most  $n$ , gives a very simple description of  $\mathcal{S}(n)$ ):

**Proposition 3.** *Suppose  $n \in \mathbb{N}$  is not a multiple of 4. Then*

$$\mathcal{S}(n) = \{T \equiv n \pmod{2} : |T| \leq 2\sqrt{n}\}.$$

**Remark 1.** Cauchy proves that if  $T \in \mathcal{S}^+(n)$ , then  $4n - T^2$  is a sum of three squares, and that when  $4 \nmid n$ ,

$$\mathcal{S}^+(n) \supseteq \{T \equiv n \pmod{2} : \sqrt{3n-2} - 1 \leq T \leq 2\sqrt{n}\}.$$

See [1, Corollary I of Theorem I, Theorem IV, and Corollary II of Theorem III].

*Proof of Proposition 3.* In view of Theorem 2, our task is to show that  $4n - T^2$  is a sum of three squares whenever  $4 \nmid n$ . Suppose first that  $n$  is odd, so that  $T$  is also odd. Then  $4n \equiv 4 \pmod{8}$  and  $T^2 \equiv 1 \pmod{8}$ , whence  $4n - T^2 \equiv 3 \pmod{8}$ . By the Legendre–Gauss theorem,  $4n - T^2$  is a sum of three squares, and we’re done. Now suppose instead that  $n$  is twice an odd integer. Then  $T$  is even, say  $T = 2t$ , so that  $4n - T^2 = 4(n - t^2)$ . It will suffice to show that  $n - t^2$  is a sum of three squares, for then  $4(n - t^2)$  is as well. Since  $n \equiv 2 \pmod{4}$  and  $t^2 \equiv 0$  or  $1 \pmod{4}$ , we have  $n - t^2 \equiv 1$  or  $2 \pmod{4}$ . In

particular,  $n - t^2$  is not of the form  $4^k(8\ell + 7)$ , and so the desired conclusion follows from the Legendre–Gauss theorem. This completes the proof.  $\square$

We conclude this note with a few remarks about the structure of  $\mathcal{S}(n)$  for general  $n$ . When  $8 \mid n$ , it is easy to see that any integer solution to

$$a^2 + b^2 + c^2 + d^2 = n$$

has all of  $a, b, c, d$  even. Thus, there is a bijection  $(a, b, c, d) \leftrightarrow (a/2, b/2, c/2, d/2)$  between representations of  $n$  as a sum of four squares and representations of  $n/4$ . Consequently,

$$\mathcal{S}(n) = 2\mathcal{S}(n/4),$$

where the notation on the right-hand side means dilation by a factor of 2. Iterating, if  $k$  is the largest nonnegative integer for which  $2^{2k+3} \mid n$ , we find that

$$\mathcal{S}(n) = 2^{k+1}\mathcal{S}(n/4^{k+1}).$$

We have from our choice of  $k$  that  $2 \mid n/4^{k+1}$  while  $8 \nmid n/4^{k+1}$ .

The observations of the last paragraph show that to describe  $\mathcal{S}(n)$ , it is enough to consider those cases where  $8 \nmid n$ . When  $4 \nmid n$ , Proposition 3 tells us the answer. However, when  $4 \mid n$ , it does not seem that there is much to be said beyond what follows immediately from Theorem 2 and the Legendre–Gauss theorem.

The situation becomes both clearer and a bit cleaner if one is willing to shift perspective. Rather than first picking  $n$  and asking for a description of the elements of  $\mathcal{S}(n)$ , we may pick  $T$  and ask for which  $n$  we have  $T \in \mathcal{S}(n)$ .

**Proposition 4.** *Let  $T \in \mathbb{Z}$ . Assume that  $n \geq T^2/4$  and  $n \equiv T \pmod{2}$ .*

- (1) *If  $T$  is odd, then  $T \in \mathcal{S}(n)$ .*
- (2) *If  $T$  is twice an odd integer, then  $T \in \mathcal{S}(n)$  if and only if  $n \not\equiv 0 \pmod{8}$ .*
- (3) *Suppose that  $4 \mid T$ . Then  $T \in \mathcal{S}(n)$  if and only if*

$$n \notin \bigcup_{k \geq 1} \{T^2 - 4^k \pmod{2^{2k+3}}\}.$$

*Here the right-hand side is an infinite union of disjoint residue classes modulo  $2^{2k+3}$ , over positive integers  $k$ .*

We leave the (routine) proof of this proposition to the interested reader.

## REFERENCES

- [1] A. L. Cauchy, Démonstration du théorème général de Fermat sur les nombres polygones, *Mém. Sci. Math. Phys. Inst. France* **14** (1813-15), 177–220.
- [2] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, Vol. 7, Springer-Verlag, New York-Heidelberg, 1973.
- [3] Y.-C. Sun and Z.-W. Sun, Some refinements of Lagrange’s four-square theorem (2017), <http://arxiv.org/abs/1605.03074>.
- [4] Z.-W. Sun, Refining Lagrange’s four-square theorem, *J. Number Theory* **175** (2017) 167–190.

DEPT OF MATHEMATICS & STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA, USA  
*E-mail address:* leo.goldmakher@williams.edu

DEPT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA, USA  
*E-mail address:* pollack@uga.edu