Available online at http://scik.org
Algebra Letters, 2015, 2015:2
ISSN: 2051-5502

HOPF'S QUADRATIC MAP AND PERMUTATION INVARIANT PROPERTIES OF PRIMITIVE CUBOIDS

WERNER HÜRLIMANN

Swiss Mathematical Society, Feldstrasse, 8004 Zürich, Switzerland

Abstract: A primitive cuboid is a rectangular parallelepiped with natural edges and inner diagonal that have no common factor and can be identified as a primitive solution of the four squares Diophantine equation $x^2+y^2+z^2=t^2$. The classical quadratic Hopf map associated to Lebesgue's identity is used to study the set of primitive cuboids with odd diagonal. Consider the restriction of the image of the induced integer Hopf map to non-negative solutions of the four squares equation, which may include zeros, and are primitive or not, as well as the corresponding relevant subset of its fibre. As a main result, we show that permutations in this subset that belong to a given partition type generate the same number of distinct solutions to the four squares equation. In the special case of a prime diagonal this subset is complete in the sense that it coincides with its fibre. It implies that each partition type in the fibre generate the same number of distinct primitive cuboids. As an application, we use Jacobi's four squares theorem to derive Shanks' theorem stating that there are exactly n primitive cuboids with odd prime diagonal p of the form $p=8n\pm 1$ or $p=8n\pm 5$. Though more complicated than the original proof, it is remarkable that the Hopf map approach does not use Gauss's formula on the number of primitive three squares representations. Moreover, the alternate proof has the advantage to be constructive and yields an algorithm to generate all primitive cuboids with prime diagonal.

Keywords: sums of squares; Lebesgue's identity; quadratic Hopf map; partition into squares; primitive cuboid; number theoretical algorithm

2010 AMS Subject Classification: 11D09, 11D45, 11Y50

Received March 31, 2015

1. Introduction

Unlike the representation of integers by sums of two and four squares the representation of numbers by sums of three squares has been identified as a much more difficult question (e.g. Davenport [7], Section V.5). It is long known that a number n is a sum of three squares if, and only if $n \neq 4^a(8b+7), a \geq 0, b \geq 0$, a result due to Legendre [24] and Gauss [11] (see Dickson [8], Chap. VII, pp. 261-262). The proof by Legendre assumed that any arithmetic progression contains infinitely many primes, a condition proved much later by Dirichlet in 1837 (see Landau [22], vol. 1, pp.114-121). The first complete but different proof was given by Gauss [11], art. 291. Accounts of this fundamental result are found in many textbooks of number theory like Krätzel [21], Satz 6.14, Grosswald [12], Chap. 4, Sierpinski [36], Section XI.4 and references therein, Nathanson [31], Theorem 1.4, p.23, etc.

A special case is the *cuboid problem*, which consists to solve the Diophantine equation

$$x^2 + y^2 + z^2 = t^2 \tag{1.1}$$

in non-zero natural numbers x, y, z, t. The numbers x, y, z are interpreted as the edges of a cuboid (=rectangular parallelepiped) and t is its inner diagonal. General solutions to (1.1), which may include zeros and non-primitive solutions, however, have been discussed by several authors including Lebesgue [23] (see Dickson [8], Chap. VII, p. 265, Nagell [30], p.194), Ayoub [4], Carmichael [5], Section II.11, Dickson [8], Chap. VII, Sierpinski [35], [36], Section II.10, Mordell [29], Chap. 3, Andreescu et al. [1], Section I.4.1. The more intricate *primitive cuboid problem* of finding natural numbers x, y, z, t with no common factor has been studied by Dickson [9], Skolem [37], Miksa [27], Steiger [40], Spira [39], and more recently by the author [16], [17].

Our new contribution shows how the study of primitive cuboids can be reduced to the study of the classical quadratic Hopf map between the real Euclidean spaces of dimensions 4 and 3 that is associated to the following identity of Lebesgue

$$x = p^2 + q^2 - r^2 - s^2,\ y = 2(pr + qs),\ z = 2(ps - qr),\ t = p^2 + q^2 + r^2 + s^2. \quad (1.2)$$

This technique goes back at least to Ono (1994), Section 7, and is thoroughly described in Section 2. The analysis is based on an invariant map from the set of ordered primitive partitions into four squares to a specific set of permutations that remain invariant for certain partition types or sub-types as described in Table 2.2. The obtained results are applied in Section 3 to determine the number of primitive cuboids with prime diagonal and generate them exhaustively using a specific algorithm. For this, we use Jacobi's four squares theorem to derive Shanks' theorem stating that there are exactly n primitive cuboids with odd prime diagonal p of the form $p = 8n \pm 1$ or $p = 8n \pm 5$. Thanks the Hopf map permutation properties the given new proof is constructive and yields an algorithm to generate all primitive cuboids with prime diagonal. Table 3.2 provides a complete list of all primitive cuboids with prime diagonal for the 25 first odd primes. Finally, Section 4 provides a brief correction note to a previous result by the author.

2. Permutation invariant properties of ordered square partitions

It is well-known that all solutions of the three squares equation (1.1) with g.c.d. $(x, y, z) = 1$ are obtained from Lebesgue's identity (e.g. Carmichael [5], Section II.11, Mordell [29], Chap. 3, Sierpinski [36], end of Section II.10, Andreescu et al. [1], Section I.4.1, Example 7):

$$x = p^2 + q^2 - r^2 - s^2,\ y = 2(pr + qs),\ z = 2(ps - qr),\ t = p^2 + q^2 + r^2 + s^2. \quad (2.1)$$

In particular, if t is an odd prime, all solutions of the primitive cuboid problem with g.c.d. $(x, y, z, t) = 1$ and $0 < x \le y \le z$ are of the form (2.1). At least in this special case, there exist presumably a one-to-one correspondence between the distinct solutions of (1.1) and solutions of the four squares equation $t = p^2 + q^2 + r^2 + s^2$ in Lebesgue's identity (2.1). The

main goal of the present Section it to make explicit a general map that is valid for arbitrary odd t.

Let $h: R^4 \to R^3$ be the classical Hopf map (see Hopf [15], Ono [32], Section 7) between the real Euclidean spaces of dimensions 4 and 3 defined by $v = (v_1, v_2, v_3) = h(u) = (u_1^2 + u_2^2 - u_3^2 - u_4^2, 2(u_1u_3 + u_2u_4), 2(u_1u_4 - u_2u_3))$. For a positive integer t, consider the real sets

$$S^3(t) = \{u \in R^4 : u_1^2 + u_2^2 + u_3^2 + u_4^2 = t\}, \qquad S^2(t) = \{v \in R^3 : v_1^2 + v_2^2 + v_3^2 = t^2\}.$$

Then h induces a map $h_t : S^3(t) \to S^2(t)$. Its restriction to the integers Z induces a map $h_{Z,t} : S^3(t)_Z \to S^2(t)_Z$, where $S^3(t)_Z = S^3(t) \cap Z^4$, $S^2(t)_Z = \{v \in S^2(t) \cap Z^3 : v_2, v_3 \ even\}$. Switching from now on to notation (2.1) one sees that the restricted integer valued Hopf map sends (p,q,r,s) to (x,y,z) such that $h_{Z,t}(p,q,r,s) = (x,y,z)$. In the context of primitive cuboids, one is only interested in distinct positive triples $(x,y,z) \in N_+$ such that $(x,y,z,t) = 1$, where the g.c.d. condition is automatically fulfilled in the special case of odd primes t. It is natural to restrict the set $S^3(t)_Z$ further to the subset of non-negative integers $S^3(t)_N = S^3(t) \cap N^4$. However, the image of the induced Hopf map $h_{N,t} : S^3(t)_N \to S^2(t)_Z$ is larger than the desired set of primitive cuboids in (2.1) with positive coordinates, say $S^2(t)_{N_+}^{pc}$. In fact, the desired solutions of (2.1) in terms of the coordinates (p,q,r,s) are described by the restriction of $h_{N,t}$ to the Hopf fibre denoted by $H^3(t)_N^{pc} = h_{N,t}^{-1}(S^2(t)_{N_+}^{pc})$. Given an ordered primitive quadruple $0 \le p \le q \le r \le s$ only specific permutations $(\bar{p}, \bar{q}, \bar{r}, \bar{s})$ of (p,q,r,s) will belong to the fibre $H^3(t)_N^{pc}$. The

analysis of examples suggests that the feasible permutations depend upon the partition type of a number into squares, a notion introduced by Lehmer [26]. According to Table 2.1 below, there are in general 11 partition types giving rise each to different numbers of representations that take into account permutations and sign changes. In the following, the integer t runs through the set of all odd numbers $t \geq 3$. Then, only six of them are relevant to our mapping, namely the partition types I, II, III, V, VI and VIII.

Table 2.1: Lehmer's 11 partition types into four squares and their numbers of representations

type	partition	# representations
I	$p^2+q^2+r^2+s^2$	384
II	$0^2+p^2+q^2+r^2$	192
III	$p^2+p^2+q^2+r^2$	192
IV	$p^2+p^2+q^2+q^2$	96
V	$0^2+p^2+p^2+q^2$	96
VI	$p^2+p^2+p^2+q^2$	64
VII	$0^2+0^2+p^2+q^2$	48
VIII	$0^2+p^2+p^2+p^2$	32
IX	$0^2+0^2+p^2+p^2$	24
X	$p^2+p^2+p^2+p^2$	26
XI	$0^2+0^2+0^2+p^2$	8

When restricted to the fibre $H^3(t)_N^{pc}$, different permutations of (p,q,r,s) can lead to the same triple (2.1) with $x,y,z>0$. However, in the special case of an odd prime $t \geq 7$, it is remarkable that the feasible permutations associated to a partition type lead always to the same specific number of distinct triples in $S^2(t)_{N_+}^{pc}$, as will be shown later in Theorem 3.1.

For a clear distinction, it is useful to consider also the set denoted by $S^2(t)_N^c = S^2(t)_Z \cap N^3$, which contains all non-negative solutions to (1.1), which may include zeros, and are primitive or not. Its fibre is denoted by $H^3(t)_N^c = h_{N,t}^{-1}(S^2(t)_N^c)$. The following observation is useful. Given $0 \leq p \leq q \leq r \leq s$ a permutation $(\bar{p},\bar{q},\bar{r},\bar{s})$ of (p,q,r,s) will belong to the fibre $H^3(t)_N^c$ provided the following necessary conditions are fulfilled:

(C1) $\bar{p},\bar{s} \geq 1, \quad \bar{q},\bar{r} \geq 0, \quad \bar{q}+\bar{r} \geq 1$

(C2) $\bar{p}\bar{s}-\bar{q}\bar{r}>0, \qquad \bar{p}^2+\bar{q}^2-\bar{r}^2-\bar{s}^2>0$

(C3) $\bar{p}+\bar{q}+\bar{r}+\bar{s} \equiv 1 \pmod 2$

The first two conditions ensure that triples (x,y,z) have positive coordinates, and (C3) is required so that $t \geq 3$ is odd. To analyse the dependence upon the ordered partition types, it is easier to work with a set of simpler structure, denoted by $S^3(t)_N^{pc}$. It contains all permutations $(\bar{p},\bar{q},\bar{r},\bar{s}) \in H^3(t)_N^c$ of an ordered primitive quadruple $0 \leq p \leq q \leq r \leq s$ satisfying (C1), (C2), (C3), where $0 \leq p \leq q \leq r \leq s$ runs through all ordered partition types in Table 2.2 below that satisfy the inequality conditions

(C) $ps-qr \neq 0, \quad p^2+q^2-r^2-s^2 \neq 0.$

Theorem 2.1 (One-to-one mapping between partition types and distinct triples in $S^2(t)^c_{N_+}$). *Let* $t \geq 3$ *run through the set of odd numbers. The permutations in* $S^3(t)^{pc}_N$ *that belong to a given partition type generate the same number of distinct triples in* $S^2(t)^c_{N_+}$ *as described in Table 2.2.*

Table 2.2: Partition types $0 \leq p \leq q \leq r \leq s$ and distinct triples in $S^2(t)^c_{N_+}$

type	partition	# squares in $S^3(t)^{pc}_N$	# zeros in $S^3(t)^{pc}_N$	# triples in $S^2(t)^c_{N_+}$
1	$0 < p < q < r < s$	4	0	6
2	$p = 0 < q < r < s$	4	1	3
(3.1)	$0 < p = q < r < s$	3	0	3
(3.2)	$0 < p < q = r < s$	3	0	3
(3.3)	$0 < p < q < r = s$	3	0	3
(4.1)	$p = 0 < q = r < s$	3	1	2
(4.2)	$p = 0 < q < r = s$	3	1	2
(5.1)	$0 < p = q = r < s$	2	0	1
(5.2)	$0 < p < q = r = s$	2	0	1
6	$p = 0 < q = r = s$	2	1	1

Proof. We proceed step by step following the order of the partition types.

Partition type 1: $0 < p < q < r < s$

When (p,q,r,s) run through the 24 different permutations of the form $(\bar{p},\bar{q},\bar{r},\bar{s})$, the pairs $(|x|,|z|)$ with $xz \neq 0$ take 6 distinct values in 4 packages of (x,z) with possible signs $(+,+)$, $(+,-)$, $(-,+)$ and $(-,-)$. Three cases are possible.

Case (a): $ps - qr > 0$

The required 6 permutations with $x > 0, z > 0$ are given by

$$(s,p,q,r), \quad (s,p,r,q), \quad (s,q,p,r), \quad (s,q,r,p), \quad (s,r,p,q), \quad (s,r,q,p).$$

For all of them the inequality $z = 2(\bar{p}\bar{s} - \bar{q}\bar{r}) > 0$ follows either from $0 < p < q < r < s$ or the assumption $ps - qr > 0$. Checking that $x = \bar{p}^2 + \bar{q}^2 - \bar{r}^2 - \bar{s}^2 > 0$ follows similarly. This is non-trivial for the first two permutations and follows from the calculation

$$x = p^2 + s^2 - q^2 - r^2 = (s - p + r - q)(s - r + q - p) + 2(ps - qr) > 0.$$

These 6 permutations generate at most 6 solutions (x,y,z), namely

$$(p^2 + s^2 - q^2 - r^2, 2(pr + qs), 2(rs - pq)), \quad (p^2 + s^2 - q^2 - r^2, 2(pq + rs), 2(qs - pr)),$$

$$(q^2 + s^2 - p^2 - r^2, 2(ps + qr), 2(rs - pq)), \quad (q^2 + s^2 - p^2 - r^2, 2(pq + rs), 2(ps - qr)),$$

$$(r^2 + s^2 - p^2 - q^2, 2(ps + qr), 2(qs - pr)), \quad (r^2 + s^2 - p^2 - q^2, 2(qs + pr), 2(ps - qr)).$$

If $s = p + q + r$ only 3 of them are distinct, but the components x, y, z are then all even, which implies that t cannot be odd. Therefore, there are exactly 6 distinct triples.

Case (b): $ps-qr<0$, $p^2+s^2>q^2+r^2$

In this situation, the 6 permutations with $x>0, z>0$ read (q,s,p,r), (r,s,p,q), (s,p,q,r), (s,p,r,q), (s,q,p,r), (s,r,p,q). For all of them the conditions $x=\bar{p}^2+\bar{q}^2-\bar{r}^2-\bar{s}^2>0$ and $z=2(\bar{p}\bar{s}-\bar{q}\bar{r})>0$ follow either from $0<p<q<r<s$ or the made assumptions. They generate at most 6 solutions except when $s=p+q+r$. In this situation 3 of them are distinct, but with even t, a contradiction.

Case (c): $ps-qr<0$, $p^2+s^2<q^2+r^2$

The 6 permutations with $x>0, z>0$ are (q,r,p,s), (q,s,p,r), (r,q,p,s), (r,s,p,q), (s,q,p,r), (s,r,p,q). They generate 6 solutions. They are all distinct except when simultaneously $r=p+q+s$ and $s=p+q+r$, which implies that $p+q=0$, hence $p=q=0$, a contradiction.

Partition type 2: $p=0<q<r<s$

In the proof for partition type 1 set $p=0$ to see that $ps-qr=-qr<0$, hence either Case (b) or Case (c) must hold.

Case (b): $s^2>q^2+r^2$

The following pairs generate at most 3 solutions (x,y,z) with $x>0, z>0$, namely

$(s,0,q,r)$ and $(s,0,r,q)$ generate the solution $(s^2-q^2-r^2, 2rs, 2qs)$,

$(q,s,0,r)$ and $(s,q,0,r)$ generate the solution $(q^2+s^2-r^2,2rs,2qr)$,

$(r,s,0,q)$ and $(s,r,0,q)$ generate the solution $(r^2+s^2-q^2,2qs,2qr)$.

They are distinct except when $s=q+r$. In this case t is even and cannot occur.

Case (c): $s^2<q^2+r^2$

The maximum of 3 solutions are generated as follows:

$(q,r,0,s)$ and $(r,q,0,s)$ generate the solution $(q^2+r^2-s^2,2rs,2qs)$

$(q,s,0,r)$ and $(s,q,0,r)$ generate the solution $(q^2+s^2-r^2,2rs,2qr)$

$(r,s,0,q)$ and $(s,r,0,q)$ generate the solution $(r^2+s^2-q^2,2qs,2qr)$

The exceptional case with $r=q+s$ and $s=q+r$ is impossible.

Partition type 3:

Three sub-partition types are distinguished.

(3.1) $0<p=q<r<s$

In the proof for partition type 1 set $q=p$ to see that $ps-qr=p(s-r)>0$, which is Case (a). The permutations (s,p,p,r), (s,p,r,p) and (s,r,p,p) generate 3 solutions except when $s=2p+r$ with one solution and even t, which is excluded.

(3.2) $0<p<q=r<s$

With $r=q$ one has $ps-qr=ps-q^2$ and three cases must be distinguished.

Case (a): $ps > q^2$

The permutations (s,p,q,q), (s,q,p,q) and (s,q,q,p) generate 3 solutions except when $s = p+2q$, which is excluded because t is even.

Case (b): $ps < q^2$, $p^2 + s^2 > 2q^2$

The 3 permutations (q,s,p,q), (s,p,q,q) and (s,q,p,q) generate 3 solutions except when $s = p+2q$, which is excluded because t is even.

Case (c): $ps < q^2$, $p^2 + s^2 < 2q^2$

The 3 permutations (q,q,p,s), (q,s,p,q) and (s,q,p,q) generate 3 solutions except when $p+s=0$ and $s = p+2q$, which is impossible.

(3.3) $0 < p < q < r = s$

One has $ps - qr = r(p-q) < 0$ and $p^2 + s^2 - q^2 - r^2 = p^2 - q^2 < 0$, hence only Case (c) in the proof of partition type 1 can occur. In this situation, the 3 permutations (q,r,p,r), (r,q,p,r) and (r,r,p,q) generate 3 solutions except when $p+q=0$, which is impossible.

Partition type 4:

Two sub-partition types may occur.

(4.1) $p = 0 < q = r < s$

From the proof of partition type 2 one sees that either Case (b) or Case (c) must hold.

Case (b): $s^2 > 2q^2$

The permutation $(s,0,q,q)$ generates the solution $(s^2-2q^2,2qs,2qs)$ while the permutations $(q,s,0,q)$ and $(s,q,0,q)$ generate the solution $(s^2,2qs,2q^2)$. Both are distinct except when $s=2q$, which leads to t even, a contradiction.

Case (c): $s^2 < 2q^2$

The permutation $(q,q,0,s)$ generates the solution $(2q^2-s^2,2qs,2qs)$ while the permutations $(q,s,0,q)$ and $(s,q,0,q)$ generate the solution $(s^2,2qs,2q^2)$. Both are distinct except when $s=2q=0$, which is impossible.

(4.2) $p=0<q<r=s$

Since $ps-qr=-qr<0$ and $p^2+s^2-q^2-r^2=-q^2<0$, only Case (c) in the proof for partition type 2 is possible. The permutations $(q,r,0,r)$ and $(r,q,0,r)$ generate the solution $(q^2,2r^2,2qr)$ while $(r,r,0,q)$ generates the solution $(2r^2-q^2,2qr,2qr)$. Both are distinct except when $q=0$, which is impossible.

Partition type 5:

One distinguishes between two sub-partition types.

(5.1) $0<p=q=r<s$

Since $ps-qr=p(s-p)>0$ one relies on Case (a) in the proof for the sub-partition (3.1). The 3 distinct solutions degenerate to a single solution, namely $(s^2-p^2,2p(p+s),2p(s-p))$. It is generated by the permutation (s,p,p,p).

(5.2) $0<p<q=r=s$

Since $ps-qr=q(p-q)<0$ and $p^2+s^2-q^2-r^2=p^2-q^2<0$ the proof for sub-partition type (3.3) applies. There is exactly one solution $(q^2-p^2,2p(p+q),2q(q-p))$, which is generated by the permutation (q,q,p,q).

Partition type 6: $p=0<q=r=s$

Since $ps-qr=-q^2<0$ and $p^2+s^2-q^2-r^2=-q^2<0$ the proof for sub-partition type (4.2) applies. The permutation $(q,q,0,q)$ generates the single possible solution $(q^2,2q^2,2q^2)$.

Theorem 2.1 is shown. ◊

An important special case is the restriction of Theorem 2.1 to prime numbers $t\geq 7$. In this situation, the set $S^3(t)_N^{pc}$ is *complete* in the sense that it coincides with the fibre $H^3(t)_N^{pc}$. We need the following result on primitive cuboids, originally due to Steiger [40] and Spira [39].

Theorem 2.2 (Unique representation of primitive cuboids). *A primitive cuboid with odd diagonal* $t\geq 3$ *has the unique representation (2.1) if, and only if, there is a permutation* $(\overline{p},\overline{q},\overline{r},\overline{s})$ *of some* $0\leq p\leq q\leq r\leq s$*, which satisfies the Steiger-Spira conditions:*

(C1) $\bar{p},\bar{s} \geq 1, \quad \bar{q},\bar{r} \geq 0, \quad \bar{q}+\bar{r} \geq 1$

(C2) $\bar{p}\bar{s}-\bar{q}\bar{r} > 0, \qquad \bar{p}^2+\bar{q}^2-\bar{r}^2-\bar{s}^2 > 0$

(C3) $\bar{p}+\bar{q}+\bar{r}+\bar{s} \equiv 1 \pmod 2$

(C4) $\gcd(\bar{p}^2+\bar{q}^2, \bar{r}^2+\bar{s}^2, \bar{p}\bar{r}+\bar{q}\bar{s}) = 1$

(C5) $\bar{r} = 0 \Rightarrow \bar{p} \leq \bar{q}, \quad \bar{q} = 0 \Rightarrow \bar{s} \leq \bar{r}$

Proof. See Steiger [40], proof of Theorem 2. ◊

Theorem 2.3 (Completeness of $S^3(t)_N^{pc}$)). *One has* $H^3(t)_N^{pc} = S^3(t)_N^{pc}$ *for all primes* $t \geq 7$.

Proof. As a by-product, one sees that the condition (C4) is always fulfilled for primes. Indeed, suppose that $\gcd(\bar{p}^2+\bar{q}^2, \bar{r}^2+\bar{s}^2) = m \geq 1$. Let a,b be integers such that $\bar{p}^2+\bar{q}^2 = ma$, $\bar{r}^2+\bar{s}^2 = mb$, and $t = \bar{p}^2+\bar{q}^2+\bar{r}^2+\bar{s}^2 = m(a+b)$. If $t \geq 3$ is a prime, then necessarily $m = 1$ and (C4) is fulfilled. Moreover, since $S^2(t)_{N_+}^{pc} = S^2(t)_{N_+}^{c}$ for prime t, one has $H^3(t)_N^{pc} = H^3(t)_N^{c}$. Now, it is clear by definition that $S^3(t)_N^{pc} \subseteq H^3(t)_N^{pc}$. It remains to show that $H^3(t)_N^{pc} \subseteq S^3(t)_N^{c}$. Let $(\bar{p},\bar{q},\bar{r},\bar{s}) \in H^3(t)_N^{pc}$. By (C1) of Theorem 2.2, this primitive quadruple must be permutation of some ordered partition type $0 \leq p \leq q \leq r \leq s$ in Table 2.1. The remaining conditions $p^2+q^2-r^2-s^2 \neq 0$ and $ps-qr \neq 0$ in (C) that define $S^3(t)_N^{pc}$ are shown as follows. Let us distinguish between the first five partition types of Table 2.1. First, it is trivial that $p^2+q^2-r^2-s^2 \neq 0$ because $p^2+q^2 < r^2+s^2$ for all partition types. It remains to show that $ps-qr \neq 0$. From the proof of Theorem 2.1 one sees that

$ps-qr=0$ is only possible for the partition types 1 and (3.2).

Partition type 1: $0<p<q<r<s$

If $ps=qr$ then there exist integers $a,b\geq 1$ such that $p=ab$, $a\,|\,q$, $b\,|\,r$. Write $q=\alpha a, r=\beta b$, for some integers $\alpha,\beta\geq 1$. Then, one has necessarily $s=\alpha\beta$. It follows that $t=p^2+q^2+r^2+s^2=(a^2+\beta^2)(b^2+\alpha^2)$ cannot be a prime number.

Partition type (3.2): $0<p<q=r<s$

If $ps=q^2$ then there exist an integer $a>1$ such that $q=pa$, hence $s=pa^2$, and therefore $t=p^2+2q^2+s^2=p^2(a^2+1)^2$ cannot be a prime. ◊

For composite odd $t\geq 3$, the situation is more complex.

Examples 2.1: non-primitive cuboids generated by $S^3(t)_N^{pc}$

For $t=15$ there are 3 permutations in $S^3(15)_N^{pc}$ of the ordered partition (1,1,2,3) of type 3.1, namely (3.1,1,2), (3,1,2,1) and (3,2,1,1). While the last two generate two primitive cuboids, the first one generates the non-primitive cuboid $(x,y,z,t)=5\cdot(1,2,2,3)$. Similarly, for $t=39$ there are 6 permutations in $S^3(39)_N^{c}$ of the ordered partition (1,2,3,5) of type 1, but only five of them generate primitive cuboids.

Examples 2.2: exceptional permutations $(\bar{p},\bar{q},\bar{r},\bar{s})\in H^3(t)_N^{pc}$ but not in $S^3(t)_N^{pc}$

These examples are related to the exceptional partitions of type 1 and (3.2) in the proof of Theorem 4.3 such that $ps=qr$. For $t=25$ the permutations (4,2,1,2) and (4,1,2,2) of the

ordered partition (1,2,2,4) of type (3.2) are not in $S^3(25)_N^{pc}$ but generate the two primitive cuboids (15,6,12,25) and (9,20,12,25). Similarly, for $t = 65$ the permutations (6,2,3,4), (6,3,2,4) and (6,4,2,3) of the ordered partition (2,3,4,6) of type 1 are not in $S^3(85)_N^{pc}$ but generate the three primitive cuboids (15,52,36,65), (25,48,36,65) and (39,48,20,65).

3. Counting and generating primitive cuboids with prime diagonal

The usefulness of the obtained results is illustrated for the special case of primitive cuboids with prime diagonal. Theorem 2.3 implies that each partition type in the fibre generate the same number of distinct primitive cuboids as follows.

Theorem 3.1 (One-to-one mapping between partition types in $H^3(t)_N^{pc}$ and primitive cuboids). *Let $t \geq 7$ run through the set of odd primes. Each partition type in $H^3(t)_N^{pc}$ generates the same number of distinct triples in $S^2(t)_{N_+}^{pc}$ as described in Table 3.1.*

Table 3.1: Partition types in $H^3(t)_N^{pc}$ and distinct triples in $S^2(t)_{N_+}^{pc}$

type	partition	# squares in $H^3(t)_N^{pc}$	# zeros in $H^3(t)_N^{pc}$	# triples in $S^2(t)_{N_+}^{pc}$
1	$p^2+q^2+r^2+s^2$	4	0	6
2	$0^2+p^2+q^2+r^2$	4	1	3
3	$p^2+p^2+q^2+r^2$	3	0	3
4	$0^2+p^2+p^2+q^2$	3	1	2
5	$p^2+p^2+p^2+q^2$	2	0	1

As an application, a new constructive proof of Shanks' theorem on the number of primitive cuboids with prime diagonal is obtained. It uses Jacobi's four squares theorem, which counts the number of representations of a positive integer into four squares including permutations and sign changes. This result is formulated in terms of the arithmetic function $\sigma(m)$, which for each positive integer m yields the sum of all its positive divisors. As usual, the total number of representations of m as a sum of $k \geq 2$ squares such that $x_1^2 + x_2^2 + ... + x_k^2 = m$, is denoted by $r_k(m)$ while the number of primitive representations with g.c.d. $(x_1, x_2, ..., x_k) = 1$ is denoted by $R_k(m)$ (e.g. Grosswald [12], Section 1.1).

Theorem 3.2 (Jacobi's four squares theorem). *Consider the unique representation of a positive integer* m *as* $m = 2^{a(m)} b(m)$, *where* $a(m)$ *is a non-negative and* $b(m)$ *is odd. Then, one has*

$$r_4(2m-1) = 8\sigma(2m-1), \quad r_4(2m) = 24\sigma(b(2m)). \tag{3.1}$$

Proof. Besides the original articles by Jacobi [18]-[20] a lot of proofs are known (e.g. Venkov [41], Chap. 5, Ewell [10], Sierpinski [36], Section XIII.7, Hirschhorn [13], [14], Andrews et al. [2], Spearman and Williams [38] and references therein). ◊

For an odd prime $t \geq 7$ Jacobi's formula tells us that the number of primitive representations is

$$R_4(t) = 8(t+1). \tag{3.2}$$

We are ready for the following new derivation of Theorem 86 in Shanks (1993).

Theorem 3.3 (Primitive cuboids with prime diagonal from Jacobi's four squares theorem). *Let*

$t \geq 7$ be an odd prime number of the form $t = 8n \pm 1$ or $t = 8n \pm 5$. Then, there are exactly n distinct primitive cuboids with prime diagonal.

Proof. In case $t \geq 7$ is an odd prime, the four squares representations from the partition types in Table 3.1 with at most one zero are relevant. Additionally, two squares representations of the type VII in Table 2.1 are counted in Jacobi's four squares formula. Their number of distinct representations is non-zero and counted 48 times if, and only if, one has $t \equiv 1 \pmod 4$ (Girard-Euler's theorem). Denote by $p_4^{(i)}(m)$ the number of distinct primitive representations of the natural number m by sums of four squares of partition type $i = 1,2,...,5$. Recall the fact that $p_4^{(4)}(t) = 0$ if $t \equiv 5, 7 \pmod 8$ and $p_4^{(4)}(t) = 1$ if $t \equiv 1, 3 \pmod 8$ (e.g. Andreescu et al. [1], Theorem 4.4.2). One distinguishes between two main cases.

Case 1: $t \equiv 1 \pmod 4$

With Table 2.1 one obtains from (3.2) the equality in numbers of primitive representations

$$384 \cdot p_4^{(1)}(t) + 192 \cdot \{p_4^{(2)}(t) + p_4^{(3)}(t)\} + 96 \cdot p_4^{(4)}(t) + 64 \cdot p_4^{(5)}(t) + 48 = 8(t+1). \quad (3.3)$$

Two sub-cases can occur. If $t = 8n + 5$ then divide (3.3) by 64 and use that $p_4^{(4)}(t) = 0$ to see that it is equivalent with the equation

$$6 \cdot p_4^{(1)}(t) + 3 \cdot \{p_4^{(2)}(t) + p_4^{(3)}(t)\} + 2 \cdot p_4^{(4)}(t) + p_4^{(5)}(t) = n. \quad (3.4)$$

With the last column of Table 3.1 this equation tells us that the number of distinct primitive cuboids with prime diagonal t is exactly n. Similarly, if $t = 8n + 1$ then use that

$p_4^{(4)}(t)=1$ to establish the equivalence between (3.3) and (3.4).

Case 2: $t \equiv 3 \pmod 4$

Jacobi's four squares formula (3.2) reads here

$$384 \cdot p_4^{(1)}(t) + 192 \cdot \{p_4^{(2)}(t) + p_4^{(3)}(t)\} + 96 \cdot p_4^{(4)}(t) + 64 \cdot p_4^{(5)}(t) = 8(t+1). \qquad (3.5)$$

Two sub-cases must be considered. If $t = 8n-1$ then (3.5) is equivalent with (3.4) because $p_4^{(4)}(t)=0$. If $t = 8n-5$ the same holds because $p_4^{(4)}(t)=1$. The proof is complete. ◊

The Hopf map approach does not use Gauss's formula on the number of primitive three squares representations (as in the original proof by Shanks [33]). It avoids herewith a result that is not viewed as elementary and simple by some authors, e.g. Davenport [7], p.114 (see however Ankeny [3], Mordell [28], Wójcik [42], Cooper and Hirschhorn [6]). Though more complex than the original proof by Shanks, the alternative proof has the advantage to be constructive. Indeed, it leads to the following algorithm to compute the n distinct solutions in Shanks' theorem. To illustrate, Table 3.2 contains a list of all distinct solutions for the first 25 odd primes.

Theorem 3.4 (Primitive cuboids with prime diagonal: quantitative algorithmic form). *Let* $t \geq 7$ *be an odd prime number of the form* $t = 8n \pm 1$ *or* $t = 8n \pm 5$. *Given the finite list* $s_0^2 = 0 < s_1^2 = 1 < s_2^2 = 4 < \ldots < s_r^2 < t$ *of all squares below* t, *determine all the distinct non-negative primitive solutions of the four squares equation* $p^2 + q^2 + r^2 + s^2 = t$ *for each of the five partition types in Table 3.1. Based on Lebesgue's identity (2.1) determine the permutations of* (p,q,r,s) *that yield the distinct primitive solutions of the equation* $x^2 + y^2 + z^2 = t^2, 0 < x \leq y \leq z$. *The generated list contains exactly* n *primitive cuboids with*

prime diagonal.

Table 3.2: Primitive cuboids with prime diagonal: four squares generators and partition types

p	p mod 8	n	p	q	r	s	partition type	p	p mod 8	n	p	q	r	s	partition type
3	-5	1	0	1	1	1	6	67	-5	9	0	3	3	7	4.1
5	5	0					n.a.				1	1	1	8	5.1
7	-1	1	1	1	1	2	5.1				1	1	4	7	3.1
11	-5	2	0	1	1	3	4.1				1	4	5	5	3.3
13	5	1	1	2	2	2	5.2	71	-1	9	1	3	5	6	1
17	1	2	0	2	2	3	4.1				2	3	3	7	3.2
19	-5	3	0	1	3	3	4.2	73	1	9	0	1	6	6	4.2
			1	1	1	4	5.1				1	2	2	8	3.2
23	-1	3	1	2	3	3	3.3				2	2	4	7	3.1
29	5	3	0	2	3	4	2				4	4	4	5	5.1
31	-1	4	1	1	2	5	3.1	79	-1	10	1	2	5	7	1
			2	3	3	3	5.2				2	5	5	5	5.2
37	5	4	1	2	4	4	3.3				3	3	5	6	3.1
			2	2	2	5	5.1	83	-5	11	0	1	1	9	4.1
41	1	5	0	1	2	6	2				0	3	5	7	2
			0	3	4	4	4.2				1	3	3	8	3.2
43	-5	6	0	3	3	5	4.1				3	3	4	7	3.1
			1	1	4	5	3.1	89	1	11	0	2	2	9	4.1
			3	3	3	4	5.1				0	2	6	7	2
47	-1	6	1	1	3	6	3.1				0	3	4	8	2
			2	3	3	5	3.2				1	4	6	6	3.3
53	5	6	0	1	4	6	2	97	1	12	0	5	6	6	4.2
			2	2	3	6	3.1				1	4	4	8	3.2
59	-5	8	0	1	3	7	2				2	2	5	8	3.1
			0	3	5	5	4.2				3	4	6	6	3.3
			3	3	4	5	3.1				4	4	4	7	5.1
61	5	7	0	3	4	6	2	101	5	12	0	1	6	8	2
			2	2	2	7	5.1				0	2	4	9	2
			2	4	4	5	3.2				0	4	6	7	2
											2	5	6	6	3.3

Remark 3.1. The steps required to generate all distinct fours squares permutations can be reduced to a minimum (constructive version of Table 3.1 as found in the proof of Theorem 2.1).

4. Correction note on primitive cuboids with odd diagonal

We clarify some points from the author [16]. Theorem 3 there claims that any primitive cuboid with odd diagonal is generated by (2.1) such that $(p,q,r,s)=(fP,fQ,dR,dS)$ for some positive integers d,f,P,Q,R,S, which satisfy some conditions, in particular

$$(d, f) = 1, \quad (P,Q) = 1, \quad (R,S) = 1, \tag{4.1}$$

$$\begin{aligned} &ps - qr = df(PS - QR) > 0, \\ &p^2 + s^2 - q^2 - r^2 = f^2(P^2 + Q^2) - d^2(R^2 + S^2) > 0, \end{aligned} \tag{4.2}$$

$$(d, P^2 + Q^2) = 1, \quad (f, R^2 + S^2) = 1, \quad (PR + QS, PS - QR) = 1. \tag{4.3}$$

The stated result includes the case $R = 0$ but omits that $Q = 0$ is possible by the proof of Theorem 2.1, partition types 2 and 4. In fact, under the convention that any integer is divisible by zero, these cases are part of (4.1). On the other hand, the inequality $PR + QS \geq PS - QR$ in (3.9) of [16] is incorrect and superfluous. A counterexample is the solution for $t = 31$ generated by $(d, f) = (1,1), (P,Q) = (5,1), (R,S) = (1,2)$, for which $PR + QS = 7 < PS - QR = 9$ (use Table 3.2 above, partition type (3.1)). To summarize, any primitive cuboid with odd diagonal is generated by Lebesgue's identity with $(p,q,r,s) = (fP, fQ, dR, dS)$ for some positive integers d, f, P, S, and non-negative integers Q, R, not both equal to zero, which satisfy the conditions (4.1), (4.2) and (4.3). It is interesting to relate this characterization with the somewhat different Steiger-Spira conditions of Theorem 2.2. Uniqueness of the representation is achieved if condition (C5) is added, that is $R = 0 \Rightarrow P \leq Q, Q = 0 \Rightarrow S \leq R$.

Conflict of Interests

The author declares that there is no conflict of interests.

REFERENCES

[1] T. Andreescu, D. Andrica, I. Cucurezeanu, An Introduction to Diophantine Equations, Birkhäuser, Springer Science+Business Media, New York, 2010.

[2] G.E. Andrews, S.B. Ekhad, D. Zeilberger, A short proof of Jacobi's formula for the number of representations of an integer as a sum of four squares, Am. Math. Mon. 100, (1993), 273-276.

[3] N.C. Ankeny, Sums of three squares, Proc. Amer. Math. Soc. 8, (1957), 316-319.

[4] B. Ayoub, Integral solutions to the equation $x^2 + y^2 + z^2 = u^2$: a geometrical approach, Math. Mag. 57(4), (1984), 222-223.

[5] R.D. Carmichael, Diophantine Analysis, J. Wiley & Sons, New York, 1915.

[6] S. Cooper, M.D. Hirschhorn, On the number of primitive representations of integers as sum of squares. Ramanujan J. 13, (2007), 7-25.

[7] H. Davenport, The Higher Arithmetic (8^{th} ed.). Cambridge University Press, Cambridge, 2008.

[8] L.E. Dickson, History of the Theory of Numbers, vol. II, Carnegie Institute of Washington, Washington, 1920. Reprint: Chelsea, New York, 1966.

[9] L.E. Dickson, Some relationships between the theory of numbers and other branches of mathematics, In: Proc. Int. Congress Math., Strasbourg, (1920), 41-56.

[10] J.A.Ewell, A simple derivation of Jacobi's four-square formula, Proc. Amer. Math. Soc. 85(3), (1982), 323-326.

[11] C.F. Gauss, Disquitiones Arithmeticae, Fleischer, Leipzig, 1801. German translation: Untersuchungen über höhere Arithmetik, Springer, 1889. Reprint: Chelsea, 1965. English translation: Yale, 1966, Springer, 1986.

[12] E. Grosswald, Representations of Integers as Sums of Squares, Springer, New York, 1985.

[13] M.D. Hirschhorn, A simple proof of Jacobi's four-square theorem, Proc. Amer. Math. Soc. 101(3), (1987), 436-438.

[14] M.D. Hirschhorn, Partial fractions and four classical theorems of number theory, Am. Math. Mon. 107, (2000), 260-264.

[15] H. Hopf, Über die Abbildungen der dreidimensionalen Sphäre auf die Kugelfläche, Math. Annalen 104, (1931), 637-665. In: Selecta: Heinz Hopf, p.52. Springer, New York, Heidelberg, Berlin.

[16] W. Hürlimann, The primitive cuboids with natural edges and diagonals according to Catalan and Sierpinski, Far East Journal of Mathematical Sciences 12(3), (2004), 277-290.

[17] W. Hürlimann, Exact and asymptotic evaluation of the number of distinct primitive cuboids, Journal of Integer Sequences 18(2), (2015), Article 15.2.5.

[18] C.G.J. Jacobi, Note sur la décomposition d'un nombre donné en quatre carrés, J. Reine Angew. Math. 3, (1828), 191 (Werke 1, p.247).

[19] C.G.J. Jacobi, Fundamenta nova theoriae functionum ellipticarum, 1829. Werke 1, 49-239.

[20] C.G.J. Jacobi, De compositione numerorum e quator quadratis, J. Reine Angew. Math. 12, (1834), 167-172. Werke 6, 245-251.

[21] E. Krätzel, Zahlentheorie, Mathematik für Lehrer, Band 19, VEB Deutscher Verlag für Wissenschaften, Berlin, 1981.

[22] E. Landau, Vorlesungen über Zahlentheorie (3 vol.), Hirzel, Leipzig, 1927. Reprint: Chelsea, New York, 1969.

[23] V.A. Lebesgue, Sur une identité qui conduit à toutes les solutions de l'équation $t^2 = x^2 + y^2 + z^2$, Comptes Rendus de l'Académie des Sciences de Paris 66, (1868), 396-398.

[24] A.-M. Legendre, Essai sur la théorie des nombres, Paris, 1798. (2nd ed.) Courcier, Paris, 1808.

[25] A.-M. Legendre, Théorie des Nombres, Didot, Paris, 1830. Reprints: Hermann, Paris, 1900, Blanchard, Paris, 1955.

[26] D.H. Lehmer, On the partition of numbers into squares, Am. Math. Mon. 55, (1948), 476-481.

[27] F. Miksa, A table of integral solutions of $a^2 + b^2 + c^2 = r^2$, Math. Teacher, (1955), 251-255.

[28] L.J. Mordell, On the representation of a number as a sum of three squares, Rev. Math. Pures Appl. 3, (1958), 25-27.

[29] L.J. Mordell, Diophantine Equations, Pure and Applied Mathematics, Vol. 30, Academic Press, London, New York, 1969.

[30] T. Nagell, Introduction to Number Theory, J. Wiley, New York, 1951.

[31] M.B. Nathanson, Additive Number Theory, The Classical Bases, Graduate Texts in Mathematics 164, Springer, New York, 1996.

[32] T. Ono, Variations on a theme of Euler, Quadratic forms, elliptic curves, and Hopf maps, Plenum Press. New York and London, 1994.

[33] D. Shanks, Review of Alan Forbes and Mohan Lal Tables, Math. Comp. 25, (1971), 630.

[34] D. Shanks, Solved and unsolved problems in number theory, Chelsea Publishing Company, New York (4th ed.), 1993.

[35] W. Sierpinski, Pythagorean Triangles, The Scripta Mathematica Studies 9, Yeshiva University, New York, 1962.

[36] W. Sierpinski, Elementary Theory of Numbers, North-Holland Mathematical Library, Vol. 31, North-Holland, Amsterdam, 1988.

[37] Th. Skolem, Om ortogonalt beliggende gitterpunkter pã kuleflater. Norsk Mat. Tidsskr. 23, (1941), 54-61.

[38] B.K. Spearman, K.S. Williams, The simplest arithmetic proof of Jacobi's four squares theorem, Far East J. Math. Sci. (FJMS) 2(3), (2000), 433-439.

[39] R. Spira, The Diophantine equation $x^2 + y^2 + z^2 = m^2$, Am. Math. Mon. 69(5), (1962), 360-365.

[40] F. Steiger, Über die Grundlösungen der Gleichung $a^2 + b^2 + c^2 = d^2$, Elemente der Mathematik 11(5), (1956), 105-108.

[41] B.A. Venkov, Elementary Number Theory, Wolters-Noordhoff Publishing, Groningen, 1970.

[42] J. Wójcik, On sums of three squares, Colloq. Math. 24, (1971), 117-119.