#A3 INTEGERS 17 (2017)

A NEW CONSTRAINT ON PERFECT CUBOIDS

Thomas A. Plick
tomplick@gmail.com

Received: 10/5/14, Revised: 9/17/16, Accepted: 1/23/17, Published: 2/13/17

Abstract

We show that out of the seven segment lengths (three edges, three face diagonals, and space diagonal) of a perfect cuboid, one length must be divisible by 25, and out of the other six lengths, one must be divisible by 25 or two must be divisible by 5.

1. The Result

A *perfect cuboid* is a rectangular prism whose edges, face diagonals, and space diagonals are all of integer length. Suppose we have a prism with dimensions $a \times b \times c$. We denote by d, e, f the lengths of the diagonals of the $a \times b$, $a \times c$, and $b \times c$ faces respectively. Finally, we denote by g the length of the space diagonals of the prism (the line segments connecting opposite corners). We call the seven quantities a, b, c, d, e, f, g the *segment lengths* of the prism. We can see that any perfect cuboid results in a solution to the system of Diophantine equations

$$\begin{aligned} a^2 + b^2 &= d^2 \\ a^2 + c^2 &= e^2 \\ b^2 + c^2 &= f^2 \\ a^2 + b^2 + c^2 &= g^2 \end{aligned}$$

where all the variables are positive.

No perfect cuboid is known to exist; the existence or nonexistence of a perfect cuboid is one of the most famed outstanding problems in number theory (mentioned by [2] and many, many others). A closely related problem is that of finding a rectangular prism in which all but one of the segment lengths are integers. This problem has also received great attention; it is known that any six of the segment lengths can be made integers, if we are willing to let the remaining length be irrational (see [2]). Leech [4] finds generators of almost-perfect cuboids by relating the Diophantine system to cubic surfaces, and Bremner [1] considers a quartic surface defined by the equations. A thorough overview of the literature on perfect cuboids is given by van Luijk [6].

Any perfect cuboid must obey a long list of constraints on its seven segment lengths:

- One of its edges must be divisible by 9, and another must be divisible by 3.
- One of its edges must be divisible by 16, and another must be divisible by 4.
- One of its diagonals must be divisible by 13.
- For each $d \in \{5, 7, 11, 19\}$, it must have an edge divisible by d (possibly different lengths for different divisors).
- For each $d \in \{17, 29, 37\}$, it must have an edge, face diagonal, or space diagonal divisible by d (possibly different lengths for different divisors).

Some of these are found in [3] and [5]. They may also be verified computationally.

Several of these conditions arise from simple considerations of modular arithmetic, by relaxing the equalities of the systems to congruence modulo some integer. For example, to show that one edge must be divisible by 3, consider the system modulo 3: it suffices to show that any triple (a, b, c) for which $a^2 + b^2$, $a^2 + c^2$, $b^2 + c^2$, and $a^2 + b^2 + c^2$ are all quadratic residues modulo 3 (that is, 0 or 1) must have an element congruent to 0. Indeed, if no edge is divisible by 3, then we have $a^2 \equiv b^2 \equiv c^2 \equiv 1 \pmod 3$, but $a^2 + b^2 \equiv 2 \pmod 3$ is not a quadratic residue modulo 3. Roberts [5] demonstrates this for the moduli 7 and 19, where the arithmetic becomes more complicated but the principle remains the same. Our argument uses a similar construction with the modulus 125 to demonstrate divisibility by 5 and 25.

The following theorem adds a new requirement to the list.

Theorem 1. *In any perfect cuboid, one of the seven segment lengths must be divisible by 25. Additionally, either (a) another of its segment lengths must be divisible by 25, or (b) two of its other segment lengths must both be divisible by 5.*

As a result, we have

Corollary 1. *The product of the three edges, three face diagonals, and space diagonal of a perfect cuboid is divisible by* 5^4.

Combining all known conditions on the segment lengths of perfect cuboids, Guy [2] reports that the product of the seven segment lengths must be divisible by

$$2^8 \cdot 3^4 \cdot 5^3 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 37.$$

Our result therefore improves this quantity by a factor of 5.

The rest of this paper is devoted to proving the theorem. Our argument begins with the following lemma.

Lemma 1. *If $x^2 + y^2 \equiv z^2 \pmod{125}$, then x^2, y^2, or z^2 must be congruent to 0, 25, or 100 modulo 125.*

Proof. The hypothesis implies $x^2 + y^2 \equiv z^2 \pmod{5}$. Since 0, 1, and 4 are the only quadratic residues mod 5, when $x^2 \not\equiv 0 \pmod{5}$ and $y^2 \not\equiv 0 \pmod{5}$ we must have $z^2 \equiv 0 \pmod{5}$. Thus one of x^2, y^2, z^2 is divisible by 5, and therefore also by 25. Every multiple of 25 is congruent to one of 0, 25, 50, 75, 100 modulo 125; of these, only 0, 25, and 100 are quadratic residues modulo 125. □

We proceed to the proof of the theorem. Let us consider the Diophantine system again. The first equation is $a^2 + b^2 = d^2$; from the Lemma, we know that one of these terms — d^2 or, without loss of generality, a^2 — must be congruent to 0, 25, or 100. We therefore have six cases to consider. In each case, we show that two lengths must be divisible by 25 or that one must be divisible by 25 and two others must be divisible by 5.

`Case 1:` $a^2 \equiv 0 \pmod{125}$. In this case, we have $25 \mid a$, and the equations simplify to

$$\begin{aligned} b^2 &\equiv d^2 \pmod{125}, \\ c^2 &\equiv e^2 \pmod{125}, \\ b^2 + c^2 &\equiv f^2 \pmod{125}, \\ b^2 + c^2 &\equiv g^2 \pmod{125}. \end{aligned}$$

Applying the Lemma to the third equation, we see that one of b^2, c^2, f^2 must be congruent to 0, 25, or 100 (mod 125). But $b^2 \equiv d^2 \pmod{125}$, $c^2 \equiv e^2 \pmod{125}$, and $f^2 \equiv g^2 \pmod{125}$. Therefore, two of $b^2, c^2, d^2, e^2, f^2, g^2$ are divisible by 5.

`Case 2:` $a^2 \equiv 25 \pmod{125}$. In this case, the Diophantine system becomes

$$\begin{aligned} 25 + b^2 &\equiv d^2 \pmod{125}, \\ 25 + c^2 &\equiv e^2 \pmod{125}, \\ b^2 + c^2 &\equiv f^2 \pmod{125}, \\ 25 + b^2 + c^2 &\equiv g^2 \pmod{125}. \end{aligned}$$

Applying the Lemma to the third equation, we see that one of b^2, c^2, f^2 must be congruent to 0, 25, or 100 (mod 125). Suppose it is b^2. We cannot have $b^2 \equiv 25 \pmod{125}$, since this implies $50 \equiv d^2 \pmod{125}$, and 50 is not a quadratic residue modulo 125. Therefore either $b^2 \equiv 0 \pmod{125}$, in which case $25 \mid b$ and $5 \mid d$, or $b^2 \equiv 100 \pmod{125}$, in which case $5 \mid b$ and $25 \mid d$.

If, instead, c^2 is congruent to 0, 25, or 100, a similar argument follows. Finally, if f^2 is congruent to 0, 25, or 100, we have the same argument again when we combine the third and fourth equations to obtain

$$25 + f^2 \equiv g^2 \pmod{125}.$$

`Case 3:` $a^2 \equiv 100 \pmod{125}$. This case is analogous to Case 2.

`Case 4:` $d^2 \equiv 0 \pmod{125}$. We have $25 \mid d$, and the system becomes

$$\begin{aligned} a^2 + b^2 &\equiv 0 \pmod{125}, \\ a^2 + c^2 &\equiv e^2 \pmod{125}, \\ b^2 + c^2 &\equiv f^2 \pmod{125}, \\ c^2 &\equiv g^2 \pmod{125}. \end{aligned}$$

If c^2 is congruent to 0, 25, or 100, we have $5 \mid c$ and $5 \mid g$. Otherwise, by the Lemma, one of a^2, e^2 must be divisible by 5, and one of b^2, f^2 must be divisible by 5.

`Case 5:` $d^2 \equiv 25 \pmod{125}$. The system becomes

$$\begin{aligned} a^2 + b^2 &\equiv 25 \pmod{125}, \\ a^2 + c^2 &\equiv e^2 \pmod{125}, \\ b^2 + c^2 &\equiv f^2 \pmod{125}, \\ 25 + c^2 &\equiv g^2 \pmod{125}. \end{aligned}$$

By the Lemma, one of a^2, c^2, e^2 must be congruent to 0, 25, or 100. Suppose it is c^2. We cannot have $c^2 \equiv 25 \pmod{125}$, since 50 is not a quadratic residue. Therefore $c^2 \equiv 0$ or $100 \pmod{125}$. If $c^2 \equiv 100 \pmod{125}$, then $g^2 \equiv 0 \pmod{125}$, and we have $5 \mid c$ and $25 \mid g$. Otherwise, $c^2 \equiv 0 \pmod{125}$, and we have $25 \mid c$ and $5 \mid g$.

If c^2 is not congruent to 0, 25, or 100, then we must have that one of a^2, e^2 is congruent to 0, 25, or 100, and one of b^2, f^2 is congruent to 0, 25, or 100. If $a^2 \equiv 0$, 25, or $100 \pmod{125}$, then either $a^2 \equiv 0 \pmod{125}$ (forcing $b^2 \equiv 25 \pmod{125}$) or $a^2 \equiv 25 \pmod{125}$ (forcing $b^2 \equiv 0 \pmod{125}$); $a^2 \equiv 100 \pmod{125}$ requires $b^2 \equiv 50 \pmod{125}$, which is impossible. If, instead, $b^2 \equiv 0$, 25, or $100 \pmod{125}$, the same argument applies.

If neither a^2 nor b^2 is congruent to 0, 25, or 100, we will have $e^2 \equiv 0$, 25, or $100 \pmod{125}$ and $f^2 \equiv 0$, 25, or $100 \pmod{125}$. If $e^2 \equiv 0 \pmod{125}$ then $25 \mid e$, and if $f^2 \equiv 0$ then $25 \mid f$. Otherwise, if $e^2 \equiv f^2 \not\equiv 0 \pmod{125}$, we have $a^2 \equiv b^2 \pmod{125}$ as well; the congruence $a^2 + b^2 \equiv 25 \pmod{125}$ then forces a^2 and b^2 both congruent to 0, a contradiction. The only remaining possibility is that e^2 and f^2 are nonzero and non-congruent, say $e^2 \equiv 25 \pmod{125}$ and $f^2 \equiv 100 \pmod{125}$. But this is actually impossible: it forces $b^2 \equiv c^2 \pmod{125}$, contradicting $b^2 + c^2 \equiv 100 \pmod{125}$.

Therefore, we always have one length divisible by 25 and two others each divisible by 5.

`Case 6:` $d^2 \equiv 100 \pmod{125}$. This case is analogous to Case 5.

The theorem is proved.

It is tempting to conjecture that a perfect cuboid must have two lengths divisible by 25, but our argument cannot prove this: a counterexample occurs with $a^2 \equiv 25$

(mod 125), $b^2 \equiv 100 \pmod{125}, c^2 \equiv 1 \pmod{125}$, where d (the diagonal of the $a \times b$ face) is the only length divisible by 25.

In closing, we remark that the result of this paper may give someone who is doubtful about the existence of perfect cuboids even more reason to doubt. We believe that perfect cuboids likely do not exist, but we still would not be shocked if one were discovered.

Acknowledgement The author thanks the anonymous referee for their helpful suggestions.

References

[1] A. Bremner, The rational cuboid and a quartic surface, *Rocky Mountain J. Math.* **18** (1988), 105-121.

[2] R. K. Guy, *Unsolved Problems in Number Theory* (3rd ed.), Springer, New York, 2004.

[3] M. Kraitchik, On certain rational cuboids, *Scripta Math.* **11** (1946), 317-326.

[4] J. Leech, The rational cuboid revisited, *Amer. Math. Monthly* **84** (1977), 518-533.

[5] T. Roberts, Some constraints on the existence of a perfect cuboid, *Austral. Math. Soc. Gaz.* **37** (2010), 29-31.

[6] R. van Luijk, *On Perfect Cuboids*, undergraduate thesis, Leiden University, 2000.