GLASNIK MATEMATIČKI
Vol. 50(70)(2015), 269 – 277

ON TWO OF JOHN LEECH'S UNSOLVED PROBLEMS CONCERNING RATIONAL CUBOIDS

Allan MacLeod
University of the West of Scotland, Scotland, UK

Abstract. Let $\{X, Y, Z, A, B, C\} \in \mathbb{Q}^+$ be such that $X^2 + Y^2 = A^2$, $X^2 + Z^2 = B^2$ and $Y^2 + Z^2 = C^2$. We consider the problem of finding $T \in \mathbb{Q}^+$ such that either

1. $T^2 - X^2 = \square$, $T^2 - Y^2 = \square$, $T^2 - Z^2 = \square$

or

2. $T^2 - A^2 = \square$, $T^2 - B^2 = \square$, $T^2 - C^2 = \square$.

We show that problem 2 always has a solution and we provide a formula for T. Extensive computation has been unable to find a single solution of problem 1.

1. Introduction

The perfect Rational cuboid problem is still unsolved despite the inherent simplicity of the question. We look for a cuboid with strictly positive integer edges X, Y, Z, such that all the face diagonals and the space diagonal are also integers.

Thus we want $A, B, C, D \in \mathbb{Z}$ with

$$X^2 + Y^2 = A^2, \qquad X^2 + Z^2 = B^2, \qquad Y^2 + Z^2 = C^2 \tag{1.1}$$

and

$$X^2 + Y^2 + Z^2 = D^2 \tag{1.2}$$

In [3], the late John Leech provides an extensive overview of this problem. This survey, in fact, is the basis for the discussion of the perfect cuboid

2010 *Mathematics Subject Classification.* 11D09, 11Y50.
Key words and phrases. Rational cuboid, elliptic curve.

problem in Richard Guy's classic book "Unsolved Problems in Number Theory" ([2]). Leech calls a cuboid satisfying (1.1) only a *classical rational cuboid*. If a perfect cuboid did exist, then

$$D^2 - X^2 = C^2, \qquad D^2 - Y^2 = B^2, \qquad D^2 - Z^2 = A^2$$

and

$$D^2 - A^2 = Z^2, \qquad D^2 - B^2 = Y^2, \qquad D^2 - C^2 = X^2.$$

At the end of [3], Leech asks for solutions of the following related problems, where we assume $(X, Y, Z, A, B, C) \in \mathbb{Z}$ satisfy (1.1)

PROBLEM 1.1. *Find $T \in \mathbb{Z}$ such that*

$$T^2 - X^2 = E^2, \qquad T^2 - Y^2 = F^2, \qquad T^2 - Z^2 = G^2, \tag{1.3}$$

with E, F, G all integers.

PROBLEM 1.2. *Find $T \in \mathbb{Z}$ such that*

$$T^2 - X^2 - Y^2 = E^2, \qquad T^2 - X^2 - Z^2 = F^2, \qquad T^2 - Y^2 - Z^2 = G^2, \tag{1.4}$$

with E, F, G all integers.

Note that this can be written

$$T^2 - A^2 = E^2, \qquad T^2 - B^2 = F^2, \qquad T^2 - C^2 = G^2.$$

Since a solution of the perfect cuboid problem would provide a solution to both problems, if either of these problems has no solution, then there cannot be a perfect cuboid. Note that the converse is not true. If either Problem 1.1 or Problem 1.2 has a solution, we would still need $X^2 + Y^2 + Z^2 = \square$.

2. Generating classical rational cuboids

We first discuss generating solutions to (1.1). Using the classic parametrization of Pythagorean triangles, we have that

$$\frac{Y}{X} = \frac{e^2 - 1}{2e}, \qquad \frac{Z}{X} = \frac{f^2 - 1}{2f}, \qquad \frac{Z}{Y} = \frac{g^2 - 1}{2g}, \tag{2.1}$$

where $e, f, g \in \mathbb{Q}$. Thus

$$\frac{(e^2 - 1)(g^2 - 1)}{4eg} = \frac{f^2 - 1}{2f}, \tag{2.2}$$

which gives the quadratic in g

$$g^2 + \frac{2e(1 - f^2)}{f(e^2 - 1)} g - 1 = 0. \tag{2.3}$$

For this to have rational solutions the discriminant must be a rational square, so there must exist $d \in \mathbb{Q}$ such that

$$d^2 = e^2 f^4 + (e^4 - 4e^2 + 1) f^2 + e^2. \tag{2.4}$$

Considered as a quartic in f, this has a rational point $f = 0, d = e$, and so is birationally equivalent to an elliptic curve. Using the method described in Mordell ([5]), we can show that this elliptic curve is of the form

$$v^2 = u^3 + (e^2+1)^2u^2 + 4e^2(e^2-1)^2u = u(u+4e^2)(u+(e^2-1)^2), \tag{2.5}$$

with the reverse transformation

$$f = \frac{v}{2e(u+(e^2-1)^2)}. \tag{2.6}$$

The properties of elliptic curves are very well described in Silverman and Tate ([6]). The use of elliptic curves in rational cuboid research is exemplified by Bremner ([1]) and the undergraduate thesis of van Luijk ([4]).

We, first, investigate the torsion points, which are the points of finite order. It is clear from (2.5) that there are 3 finite points of order 2 at $(0,0)$,$(-4e^2,0)$ and $(-(e^2-1)^2,0)$. The fact that the coefficient of u is a square suggests that we might have points of order 4, and, in fact, we find 4 points of order 4 at

$$(2e(e^2-1),\ \pm 2e(e^2-1)(e^2+2e-1)\,), \quad (-2e(e^2-1),\ \pm 2e(e^2-1)(e^2-2e-1)\,).$$

Thus, the torsion subgroup must be isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. For the latter to occur, we would require

$$2e(e^2-1) = \square \qquad \text{or} \qquad -2e(e^2-1) = \square, \tag{2.7}$$

both of which can be transformed into looking for points of infinite order on $y^2 = x^3 - 4x$. This is just asking whether 2 is a congruent number and it is a classical result that this is not the case. Thus the torsion subgroup will be isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

We find that the 7 finite torsion points give f undefined, $f = 0$ or $f = \pm 1$, none of which give a non-trivial cuboid. We thus need curves with points of infinite order.

Setting $e = m/n$ with $m, n \in \mathbb{Z}$ and $\gcd(m,n) = 1$, and $u = h/n^4, v = g/n^6$ we have the curve with integer coefficients

$$g^2 = h^3 + (m^2+n^2)^2h^2 + 4m^2n^2(m^2-n^2)^2h. \tag{2.8}$$

Numerical experiments show that this elliptic curve has rank 0 often. The simplest choice to give rank 1 is $m = 5$, $n = 2$, with $(-405, 270)$ being of infinite order. This gives $f = 3/8$ and hence $g = 7/18$. Since we can ignore signs, we finally have $X = 240$, $Y = 252$ and $Z = 275$.

3. Second stage

Given a rational cuboid with sides (X, Y, Z) and face diagonals (A, B, C), both problems have essentially the same second stage. Given a trio of integers (I, J, K), find T such that

$$T^2 - I^2 = \square, \qquad T^2 - J^2 = \square, \qquad T^2 - K^2 = \square. \tag{3.1}$$

Thus there must exist $p, q \in \mathbb{Q}$ such that

$$\frac{T}{I} = \frac{p^2+1}{2p}, \qquad \frac{T}{J} = \frac{q^2+1}{2q}, \tag{3.2}$$

so that

$$q^2 - \frac{I(p^2+1)}{Jp}q + 1 = 0. \tag{3.3}$$

As before, the discriminant must be a rational square, so we consider the quartic in p

$$d^2 = I^2p^4 + (2I^2 - 4J^2)p^2 + I^2 \tag{3.4}$$

The obvious rational point means that the quartic is also birationally equivalent to an elliptic curve, which is

$$w^2 = z^3 - (I^2+J^2)z^2 + I^2J^2z = z(z-I^2)(z-J^2), \tag{3.5}$$

with

$$p = \frac{w}{I(z-J^2)}. \tag{3.6}$$

This curve has 3 points of order 2 at $(0,0)$, $(I^2,0)$ and $(J^2,0)$. Order 4 points will exist if

$$\frac{(z^2-I^2J^2)^2}{4(z^3-(I^2+J^2)z^2+I^2J^2z)} = 0 \text{ or } I^2 \text{ or } J^2 \tag{3.7}$$

has a rational solution, which requires

$$|I^2 - J^2| = \square, \tag{3.8}$$

so will be rare amongst the cuboids we consider.

In general, we need to have an elliptic curve with rank at least 1.

Suppose we take $I = 240$ and $J = 252$ from the previous section. The elliptic curve is

$$w^2 = z^3 - 121104z^2 + 3657830400z,$$

with Denis Simon's ellrank software ([7]) giving the rank as 2 with generators $G_1 = (70560, 2540160)$ and $G_2 = (56448, 677376)$.

The point G_1 gives $p = 3/2$ and then $q = 9/7$ and $T = 260$. We have $T^2 - I^2 = 100^2$ and $T^2 - J^2 = 64^2$. Unfortunately, $T^2 - K^2 = 260^2 - 275^2$ which is certainly not a square.

4. Computational experiments

We vary $e = m/n$ and generate rational cuboids with sides (X, Y, Z) and face diagonals (A, B, C). For each combination of two lengths from a particular triad we try to determine points on the corresponding elliptic curve. From each point, we generate T and test if it satisfies the three square requirements.

The time-consuming aspect of the calculation is the attempt to determine the rank of (2.5) and (3.5). There is no guaranteed method for doing this. As all calculations were done using the Pari-gp package, we could use ellrank, which is written in Pari. This, however, can be very lengthy, especially for large values of I and J.

As an alternative, we can try to find points by simple searching. This should be done using the minimal elliptic curve as points tend to be smaller in the number of digits.

There is also the possibility of using some simple algebra to derive a method which seems to work well in practice. Both the elliptic curves are very similar in structure, so we just describe the process for (3.5).

For curves of the form of (3.5), we have that $z = dU^2/V^2$ and $w = dUW/V^3$, where $d, U, V, W \in \mathbb{Z}$ and d is squarefree, with $\gcd(U, V) = 1$ and $\gcd(d, V) = 1$. Substituting gives

$$d\,W^2 = d^2U^4 - (I^2 + J^2)d\,U^2V^2 + I^2J^2V^4. \tag{4.1}$$

Thus, $d|(IJ)$, so we can work out possible values of d easily. Now

$$\begin{aligned} 4d\,W^2 &= 4d^2U^4 - 4(I^2 + J^2)d\,U^2V^2 + 4I^2J^2V^4, \\ &= (2d\,U^2 - (I^2 + J^2)V^2)^2 - (I^2 + J^2)^2V^4 + 4I^2J^2V^4, \\ &= (2d\,U^2 - (I^2 + J^2)V^2)^2 - (I^2 - J^2)^2V^4. \end{aligned}$$

Define

$$\alpha = 2d\,U^2 - (I^2 + J^2)V^2, \qquad \beta = (I^2 - J^2)V^2, \qquad \gamma = 2W,$$

so that

$$\alpha^2 = \beta^2 + d\,\gamma^2. \tag{4.2}$$

This can be parameterised by

$$\alpha = p^2 + d\,q^2, \qquad \beta = p^2 - d\,q^2, \qquad \gamma = 2pq.$$

Some elementary algebra gives

$$\frac{d\,U^2}{V^2} = \frac{p^2I^2 - d\,q^2J^2}{p^2 - d\,q^2}. \tag{4.3}$$

We loop over (p, q) in some specified range, compute the right-hand-side expression for possible d, and see if it gives a point on the curve. These ideas give a code which is significantly faster than using ellrank.

Having found R generator points $G_1, \ldots, G_R$ on the curves, we compute points on the curve from

$$P = n_1G_1 + \ldots + n_RG_R + \mathrm{Tor}, \tag{4.4}$$

where the n_i are integers up to some limit and Tor is a torsion point.

5. Numerical results

Using all the ideas of the previous sections, codes for both problems were constructed in Pari-gp. The numerical results are totally different for the two problems.

Initial runs produced no solutions for Problem 1.1 but several solutions to Problem 1.2. Deeper investigation with Problem 1.2 suggested that all classical rational cuboids satisfy Problem 1.2, and, eventually, we managed to prove

Theorem 5.1. *All classical rational cuboids where* $X^2+Y^2=\square$, $X^2+Z^2=\square$, *and* $Y^2+Z^2=\square$, *also satisfy* $T^2-(X^2+Y^2)=\square$, $T^2-(X^2+Z^2)=\square$ *and* $T^2-(Y^2+Z^2)=\square$ *for some* $T\in\mathbb{Q}$.

Proof. The proof is basically just chasing various formulae, together with two crucial observations from the numerical output.

By using the formulae in section 3, we have

$$T=\frac{z^2-I^2J^2}{2w}, \tag{5.1}$$

as long as $w\neq 0$. It is easy to check that T^2-I^2 and T^2-J^2 are always squares.

In the specific case of Problem 1.2, $I=A$ and $J=B$ from section 2. We assume e is a free parameter and use (2.6) to give f, with (u,v) a non-torsion point on (2.5). The elliptic curve (3.5) can thus be expressed in terms of e and u.

The first observation from the data is that this elliptic curve always has a rational point with $z=e\,f\,A\,B$ which can be written

$$z=\frac{(e^2+1)(4e^6-8e^4+4e^2(2u+1)+u^2)}{16e^2(u+(e^2-1)^2)}, \tag{5.2}$$

with

$$w=\pm\, z\frac{u^2+4(e^2-1)u-4(e^2-1)^2}{4v}. \tag{5.3}$$

The second observation from the data is that this point does not usually give a solution to Problem 1.2, but double this point does.

Doubling the point and simplifying gives a point with

$$z=\frac{(e^2+1)^2(4e^6-8e^4+4e^2(2u+1)+u^2)^2}{64e^4v^2} \tag{5.4}$$

and

$$w=\pm\, z\,\frac{(e^2-1)(2e^3-2e+u)(2e^3-2e-u)}{8e^2v}. \tag{5.5}$$

All these formulae give a formula for T as

$$\frac{(u^2+4e^2(e^2-1)^2)((e^2+1)^2u^2+16e^2(e^2-1)^2u+4e^2(e^4-1)^2)X}{16e^2(e^2-1)(2e^3-2e+u)(2e^3-2e-u)v}. \tag{5.6}$$

Using this value of T it is possible to check that $T^2-Y^2-Z^2$ is a square. □

As an example, consider the parametric solution of Euler

$$X=8k(k^4-1), \qquad Y=(k^2-1)(k^4-14k^2+1), \qquad Z=2k(3k^4-10k^2+3),$$

which has

$$A=(k^2-1)(k^4+18k^2+1), \qquad B=2k(5k^4-6k^2+5), \qquad C=(k^2+1)^3.$$

We have

$$e=\frac{k^2+1}{4k}, \qquad f=\frac{2(k^2-1)}{k^2+1}, \qquad g=\frac{(k-1)(k^2+4k+1)}{(k+1)(k^2-4k+1)}.$$

From this we find a point (u,v) on (2.5) with

$$u=\frac{(k-1)^2(k^2+4k+1)^2}{16k^3},$$

$$v=\frac{(k^2-1)(k^2+4k+1)^2(k^4+8k^3-14k^2+8k+1)}{256k^5},$$

which finally gives

$$T=\frac{T_1T_2}{8(k^2+1)(k^2+4k+1)(k^2-4k+1)(3k^4-10k^2+3)}, \tag{5.7}$$

where

$$T_1=5k^8+8k^7-12k^6-104k^5+222k^4-104k^3-12k^2+8k+5$$

and

$$T_2=5k^8-8k^7-12k^6+104k^5+222k^4+104k^3-12k^2-8k+5.$$

If we choose $k=3$, we have $X=1920$, $Y=352$ and $Z=936$, with $A=1952$, $B=2136$ and $C=1000$. The value of T is 6434041/2145.

6. an alternative approach to Problem 1.1

For Problem 1.1, the situation is totally opposite. Extensive computation has failed to find a single solution. We also attempted to solve the problem from a different angle.

If T exists, then

$$T^2=X^2+J^2=Y^2+K^2=Z^2+L^2,$$

for $J,K,L\in\mathbb{Q}$.

Thus, there exists angles θ and μ such that

$$\begin{pmatrix} Y \\ K \end{pmatrix}=\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} X \\ J \end{pmatrix} \tag{6.1}$$

and

$$\begin{pmatrix} Z \\ L \end{pmatrix} = \begin{pmatrix} \cos\mu & \sin\mu \\ -\sin\mu & \cos\mu \end{pmatrix} \begin{pmatrix} X \\ J \end{pmatrix}. \tag{6.2}$$

Thus

$$J = \frac{Y - X\,\cos\theta}{\sin\theta}, \qquad K = \frac{Y\,\cos\theta - X}{\sin\theta},$$
$$J = \frac{Z - X\,\cos\mu}{\sin\mu}, \qquad L = \frac{Z\,\cos\mu - X}{\sin\mu}.$$

It is also clear that $\cos\theta$, $\sin\theta$, $\cos\mu$ and $\sin\mu$ are rational, so we can assume

$$\cos\theta = \frac{1-p^2}{1+p^2}, \qquad \sin\theta = \frac{2p}{1+p^2}, \qquad \cos\mu = \frac{1-q^2}{1+q^2}, \qquad \sin\mu = \frac{2q}{1+q^2},$$

where $p, q \in \mathbb{Q}$.

Equating the two expressions for J gives the equation

$$-p(X+Z)q^2 + (p^2(X+Y) - X + Y)q + p(X-Z) = 0 \tag{6.3}$$

and, if this is to give rational q, the discriminant must be a rational square. Some standard algebra leads to the quartic

$$g^2 = h^4 + (2X^2 + 2Y^2 - 4Z^2)h^2 + X^4 - 2X^2Y^2 + Y^4,$$

where $h = p(X+Y)$.

This quartic has a rational solution at $h = 0, g = \pm(X^2 - Y^2)$, so is birationally equivalent to an elliptic curve, which we can show has the form

$$s^2 = t(t - X^2 + Z^2)(t - Y^2 + Z^2), \tag{6.4}$$

with $p = s/(t(X+Y))$.

The curve has, in general, a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and none of the torsion points give a non-trivial solution to the problem. We must, therefore, test whether the curve has strictly positive rank.

We can easily adapt the codes from earlier to this case. But, again, extensive testing has failed to find a non-zero rational solution for T. We used hundreds of hours of computer time with Pari on a variety of lap-top computers. We tried different values of the parameters, different search depths, different powers of generators, all to no avail. These failures, of course, do not prove a solution does not exist.

These failures have led the author to conjecture that a solution to Problem 1.1 does not exist, with the implication that a perfect cuboid does not exist!

In support of the non-existence of a perfect cuboid is the fact that restrictions on possible values for the integer edges and diagonals of such an object have been produced by several authors, such as Korec and Kraitchik. In the section of the perfect cuboid in Guy's book it is quoted that the product of all the edges and diagonals would have to be divisible by

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

Acknowledgement.

The author expresses sincere thanks to the referee for several very helpful comments on the original submission of this work.

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-Verlag, New York, 2004.
[3] J. Leech, *The rational cuboid revisited*, Amer. Math. Monthly **84**, (1977), 518–533.
[4] R. van Luijk, On perfect cuboids, Undergraduate Thesis, Leiden University, 2000.
[5] L. J. Mordell, Diophantine equations, Academic Press, London, 1969.
[6] J. H. Silverman and J. Tate, Rational points on elliptic curves, Springer-Verlag, New York, 1992.
[7] D. Simon, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math. **5** (2002), 7–17.

A. MacLeod
Statistics, O.R. and Mathematics Group
University of the West of Scotland
High St., Paisley,
Scotland. PA1 2BE
E-mail: allan.macleod@uws.ac.uk

Received: 1.10.2014.
Revised: 9.6.2015.