GLASNIK MATEMATIČKI
Vol. 48(68)(2013), 23 – 29

COMPUTATION OF PERFECT "ALMOST-CUBOIDS"

Allan J. MacLeod
University of the West of Scotland, Scotland, U.K.

Abstract. We discuss generating parallelepipeds, with 4 rectangular faces, which have rational lengths and all face and space diagonals also rational.

1. Introduction

The Perfect Cuboid is a notorious unsolved problem in Diophantine equations, see section $D18$ of Guy [2], the papers of Bremner [1] and Leech [3], and the thesis of van Luijk [4] for some of the vast amount written on this subject. It is a problem understandable by a school-pupil, but with no known solution and without a proof that solutions either do or do not exist. We look for a cuboid with all the sides, face diagonals and space diagonals being integers. The vertices of such a cuboid will be at

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = n_1 \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix} + n_2 \begin{pmatrix} 0 \\ b \\ 0 \end{pmatrix} + n_3 \begin{pmatrix} 0 \\ 0 \\ c \end{pmatrix} \tag{1.1}$$

where $n_1, n_2, n_3 \in \{0, 1\}$.

In the absence of a resolution of this problem, researchers have looked for other regular hexahedral shapes which are perfect in the sense of having integer edges, face diagonals and space diagonals. In 2009, Sawyer and Reiter announced that they had found perfect parallelepipeds by search methods, with the results described in [7].

2010 *Mathematics Subject Classification.* 11D25, 11Y50.
Key words and phrases. Perfect cuboids, parallelipipeds, elliptic curves, descent.

One of their parallelepipeds is an example of the simplest extension of (1.1), where the vertices are at

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = n_1 \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix} + n_2 \begin{pmatrix} 0 \\ b \\ 0 \end{pmatrix} + n_3 \begin{pmatrix} d \\ 0 \\ c \end{pmatrix} \tag{1.2}$$

so four faces are rectangular (not two as stated by Sawyer and Reiter). This is why we denote such shapes as "almost-cuboids".

In the following note, we apply slightly more advanced analysis to finding such shapes.

2. Elliptic Curve Approach

Given the vertices we describe in equation (1.2), a perfect almost-cuboid exists if we can find a, b, c, d, with clearly $a, b \in \mathbb{Q}$, such that

$$a^2 + b^2 = p^2, \qquad d^2 + c^2 = q^2, \qquad b^2 + d^2 + c^2 = r^2 \tag{2.1}$$

$$(a+d)^2 + c^2 = s^2, \qquad (a-d)^2 + c^2 = t^2 \tag{2.2}$$

$$(a+d)^2 + b^2 + c^2 = u^2, \qquad (a-d)^2 + b^2 + c^2 = v^2 \tag{2.3}$$

and $p, q, r, s, t, u, v \in \mathbb{Q}$.

Now, equation (2.2) immediately gives $4ad = s^2 - t^2$, so that $d \in \mathbb{Q}$. For c, however, we only require $c^2 \in \mathbb{Q}$, so c can be a quadratic irrational - as in the example given by Sawyer and Reiter.

From (2.1), $b^2 + a^2 = p^2$ and $b^2 + q^2 = r^2$. Suppose a, q are integers with $\gcd(a, q) = 1$, and we assume, without loss of generality, that a, q are strictly positive. Then there exists an integer k such that ka, kb, kq are all integers. Using the standard parametrization of Pythagorean triples, see chapter 15 of Rosen [6], we have $e, f \in \mathbb{Q}$ with

$$\frac{b}{a} = \frac{e^2 - 1}{2e}, \qquad \frac{b}{q} = \frac{f^2 - 1}{2f} \tag{2.4}$$

so that

$$eqf^2 - a(e^2 - 1)f - eq = 0.$$

For this to have rational roots, we must have the discriminant being a rational square, so we look for rational (e, D) satisfying

$$D^2 = a^2 e^4 + (4q^2 - 2a^2)e^2 + a^2. \tag{2.5}$$

If we define $Y = aD$ and $X = ae$, we derive the quartic

$$Y^2 = X^4 + (4q^2 - 2a^2)X^2 + a^4 \tag{2.6}$$

which has the rational point $(0, a^2)$. Thus, the quartic is birationally equivalent to an elliptic curve. Using the method described by Mordell ([5]), we find the elliptic curve to be

$$V^2 = U(U + a^2)(U + q^2) \tag{2.7}$$

with the reverse transformation $e = V/(a(U + q^2))$ which gives

$$b = \frac{U^2 - a^2q^2}{2V}. \tag{2.8}$$

The properties of elliptic curves are very well described in Silverman and Tate ([8]). The rational points form an Abelian group. The points of finite order are called torsion points. For the curve here, there are 3 finite torsion points of order 2, $(0, 0)$, $(-a^2, 0)$ and $(-q^2, 0)$. There are 4 torsion points of order 4, $(aq, \pm aq(a + q))$ and $(-aq, \pm aq(a - q))$. From (2.8), none of these torsion points lead to a non-zero value of b.

For $a = 4w^2$ and $q = (w^2 - 1)^2$, $w \in \mathbb{Q}$, the elliptic curve also has 8 finite torsion points of order 8. These are at

1. $U = -4w(w + 1)^2(w^2 - 1)$,
2. $U = 4w^3(w + 1)^2(w^2 - 1)$,
3. $U = 4w(w - 1)^2(w^2 - 1)$,
4. $U = -4w^3(w - 1)^2(w^2 - 1)$.

and they all give $b = \pm 2w(w^2 - 1)$. We will return to this special case later.

In general, therefore, the torsion points of the elliptic curve do not lead to a suitable b. We, thus, must find curves with rank greater than 0.

3. Finding c, d

Having found input values a, q which give non-zero b, we use (2.2) to find s, t. We have

$$s^2 + t^2 = 2(a^2 + q^2)$$

so, considered as vectors,

$$\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \sqrt{2}a \\ \sqrt{2}q \end{pmatrix} = \begin{pmatrix} \sqrt{2}\cos\theta & \sqrt{2}\sin\theta \\ -\sqrt{2}\sin\theta & \sqrt{2}\cos\theta \end{pmatrix} \begin{pmatrix} a \\ q \end{pmatrix} \tag{3.1}$$

which we can write as

$$\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} a & q \\ q & -a \end{pmatrix} \begin{pmatrix} \sqrt{2}\cos\theta \\ \sqrt{2}\sin\theta \end{pmatrix}.$$

Since s, t, a, q are rational, we must have $x = \sqrt{2}\cos\theta$ and $y = \sqrt{2}\sin\theta$ rational. We can find a simple rational parametrization of $x^2 + y^2 = 2$ by noting that there is an obvious solution at $x = y = 1$, so the line $y = 1 + k(x - 1)$ will meet the circle at a second point which leads to

$$s = \frac{k^2 - 2k - 1}{k^2 + 1}\, a + \frac{k^2 + 2k - 1}{k^2 + 1}\, q,$$

$$t = -\frac{k^2+2k-1}{k^2+1}\,a + \frac{k^2-2k-1}{k^2+1}\,q$$

for $k \in \mathbb{Q}$.

Since $d = (s^2 - t^2)/4a$, we have

$$d = \frac{(a(k^2-1)+2kq)(q(k^2-1)-2ka)}{a(k^2+1)^2} \tag{3.2}$$

and

$$c^2 = \frac{4k(k^2-1)P_4(k,a,q)}{a^2(k^2+1)^4} \tag{3.3}$$

where

$$P_4 = (ka+q)(a(k+1)-q(k-1))(a(k-1)+q(k+1))(kq-a) \tag{3.4}$$

and we can thus easily find acceptable intervals for k which ensure the right hand side of (3.3) is strictly positive giving a real non-zero value for c.

We thus have formulae for a, b, c, d, but we still need to satisfy the equations in (2.3). The first requires that the following quartic in k gives a rational square

$$\begin{aligned}&(b^2+(a+q)^2)k^4 + 4(q^2-a^2)k^3 + (2a^2-12aq+2q^2+2b^2)k^2\\ &+4(a^2-q^2)k + b^2 + (a+q)^2,\end{aligned} \tag{3.5}$$

whilst the second needs the following quartic to be a rational square

$$\begin{aligned}&(b^2+(a-q)^2)k^4 + 4(a^2-q^2)k^3 + (2a^2+12aq+2q^2+2b^2)k^2\\ &+4(q^2-a^2)k + b^2 + (a-q)^2.\end{aligned} \tag{3.6}$$

Unfortunately, neither the coefficient of k^4 nor the constant are guaranteed to be square in either quartic, so the quartic often has no obvious rational solutions and sometimes none at all. We are thus forced to resort to a computational search.

4. Computational Methods

The algorithm used is essentially

1. Select $a, q \in \mathbb{Z}$ with $\gcd(a, q) = 1$,
2. Try to find generators of infinite order on $V^2 = U(U + a^2)(U + q^2)$,
3. From these, determine values of b,
4. Find the rational values of k giving $c^2 > 0$,
5. Determine d,
6. Test if equations (2.3) hold.

For finding generators of the elliptic curve, we have the problem that it is a non-trivial process to determine the rank. We thus reduce the problem to finding simple points of infinite order, which are easy to find but might not give a complete set of generators. We could use a search method, but we found it was more effective to use a simple descent approach.

Suppose $U = du^2/v^2$ and $V = duw/v^3$ (d, u, v mean different things here than in section 2), with $d, u, v, w \in \mathbb{Z}$, and $\gcd(u, v) = \gcd(d, v) = 1$ with d squarefree. Then substituting in (2.7) gives

$$dw^2 = d^2u^4 + d(a^2 + q^2)u^2v^2 + a^2q^2v^4 \tag{4.1}$$

so that $d|(aq)$, meaning possible values of d are easy to calculate.

We can proceed in two possible ways. Firstly, we have

$$4dw^2 = 4d^2u^4 + 4d(a^2 + q^2)u^2v^2 + 4a^2q^2v^4$$

so

$$d(2w)^2 = (2du^2 + (a^2 + q^2)v^2)^2 - (a^2 - q^2)^2v^4$$

and, if we define $H = 2w$, $F = 2du^2 + (a^2 + q^2)v^2$ and $G = (a^2 - q^2)v^2$, we have

$$F^2 = G^2 + dH^2 \tag{4.2}$$

which can be parameterized by $G = m^2 - dn^2$, $H = 2mn$ and $F = m^2 + dn^2$.

We can invert the definitions to give

$$\frac{u^2}{v^2} = \frac{a^2(F - G) - q^2(F + G)}{2dG} = \frac{da^2n^2 - q^2m^2}{d(m^2 - dn^2)}. \tag{4.3}$$

We just loop over values of m, n up to some limit, with $\gcd(m, n) = 1$, and test if the ratios give rational squares.

An alternative descent is provided by writing

$$dw^2 = (du^2 + aqv^2)^2 + d(a - q)^2u^2v^2. \tag{4.4}$$

As we stated before $d|(aq)$ so $aq = de$ with $e \in \mathbb{Z}$, giving

$$w^2 = d(u^2 + ev^2)^2 + (a - q)^2u^2v^2 \tag{4.5}$$

which again gives $F^2 = G^2 + dH^2$ if we define $G = (a - q)uv$, $H = u^2 + ev^2$ and $F = w$.

We do not have such a nice ratio test for a rational point. We use the fact that u^2 must satisfy

$$(a - q)^2x^2 - H(a - q)^2x + eG^2 = 0 \tag{4.6}$$

so we first test for the discriminant of the quadratic being a rational square. Then we test for the roots being rational squares. Combining these descents finds several non-integer points of infinite order.

Having found b values, we could test whether the quartics (3.5) and (3.6) are everywhere locally soluble, but for rational b with large numerators and denominators this can take longer than just generating s, t, d, c and testing (2.3).

Applying all the above ideas, a Pari program found the following ten solutions fairly easily.

Table 1. Perfect ”almost-cuboids”

a	b	d	c
72	65	42036/1225	$48\sqrt{429351}/1225$
60	91	252216/3125	$288\sqrt{429351}/3125$
20	21	17284/9375	$32\sqrt{14362806}/9375$
28	45	51852/8575	$96\sqrt{14362806}/8575$
16199	9240	32786/167	$15132\sqrt{770}/167$
1261	4620	1261/2	$291\sqrt{770}$
60	11	101109420/2393209	$5760\sqrt{292620845}/2393209$
7020	1309	11234380/2197	$640\sqrt{292620845}/2197$
120	119	442815/5408	$9\sqrt{455301391}/5408$
3	4	8856300/2393209	$180\sqrt{455301391}/2393209$

From the results, it is fairly clear that solutions occur in pairs. To see how, suppose a solution comes from $(a,q)=(M,N)$, a point (U,V) on the elliptic curve (2.7) and a certain value of $k=K$. But, the symmetry of the elliptic curve equation gives that (U,V) is also a point on the curve when $(a,q)=(N,M)$, and it also gives the same value of b.

Equation (3.2) does give a different value for d, and we have a different formula also for c^2. The denominator is still a positive square, but the numerator could be negative. It is, however, easy to check that if we change $k=K$ to $k=-K$ the numerator will be the same as in the original solution. Also, negating k just gives the same values for the quartics (3.5) and (3.6), which are thus rational squares.

Thus $(a,q)=(N,M), k=-K$ will also give a perfect ”almost-cuboid”.

The results in the table lead to the following conjecture:

Conjecture 4.1. *There are an infinite number of perfect ”almost-cuboids” with* $a,b\in\mathbb{Z}$ *and* $\gcd(a,b)=1$.

Finally, we return to the special torsion solution at the end of section 2, where $a=4w^2$, $q=(w^2-1)^2$ and $b=2w(w^2-1)$. We can use the formulae above to easily find values of d and c^2 which are both positive. The quartics (3.5) and (3.6) give the following forms, which would need rational solutions,

$$\begin{aligned} j^2 = {} & (w^8+8w^6-2w^4+8w^2+1)k^4+4(w^8-4w^6-10w^4-4w^2+1)k^3 \\ & +2(w^8-24w^6+62w^4-24w^2+1)k^2 \\ & -4(w^8-4w^6-10w^4-4w^2+1)k+w^8+8w^6-2w^4+8w^2+1 \end{aligned}$$

and

$$\begin{aligned}j^2 = {} & (w^8 - 8w^6 + 30w^4 - 8w^2 + 1)k^4 - 4(w^8 - 4w^6 - 10w^4 - 4w^2 + 1)k^3 \\ & + 2(w^8 + 24w^6 - 34w^4 + 24w^2 + 1)k^2 \\ & + 4(w^8 - 4w^6 - 10w^4 - 4w^2 + 1)k + w^8 - 8w^6 + 30w^4 - 8w^2 + 1.\end{aligned}$$

Extensive numerical testing has been unable to locate a rational w which gives a non-trivial solution of even one of these, though this is, of course, not a proof of anything. For specific values of w, we find that the quartics in k are often not even everywhere locally soluble, and this is always true for both curves in the pair. This leads to a second

Conjecture 4.2. *Neither of the above quartics in k have a rational solution if $w \neq 0, \pm 1$.*

Acknowledgements.

The author would like to thank two anonymous referees for their extremely detailed and helpful comments on the original submission.

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, 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, University of Utrecht, 2000.

[5] L. J. Mordell, Diophantine equations, Academic Press, New York, 1969.

[6] K. H. Rosen, Elementary number theory and its applications, Pearson Addison-Wesley, New York, 2000.

[7] J. F. Sawyer and C. A. Reiter, *Perfect parallelepipeds exist*, Math. Comp. **80** (2011), 1037–1040.

[8] J. H. Silverman and J. Tate, Rational points on elliptic curves, Springer, New York, 1992.

A. J. 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: 11.1.2012.
Revised: 4.10.2012.