A NOTE ON THE FIRST CUBOID CONJECTURE.

Ruslan Sharipov

Abstract. Recently the problem of constructing a perfect Euler cuboid was related with three conjectures asserting the irreducibility of some certain three polynomials depending on integer parameters. In this paper a partial result toward proving the first cuboid conjecture is obtained. The polynomial which, according to this conjecture, should be irreducible over integers is proved to have no integer roots.

1. Introduction.

An Euler cuboid is a rectangular parallelepiped whose edges and face diagonals all are of integer lengths. A perfect cuboid is an Euler cuboid whose space diagonal is also of an integer length. Cuboids with integer edges and face diagonals are known since 1719 (see [1–35]), however, no perfect cuboid is known by now. The problem of constructing perfect cuboids or proving their non-existence is an open mathematical problem.

In [36] the problem of constructing perfect cuboids was reduced to the polynomial Diophantine equation $P_{abu}(t) = 0$, where $P_{abu}(t)$ is given by the formula

$$
\begin{aligned}
P_{abu}(t) = t^{12} &+ (6\,u^2 - 2\,a^2 - 2\,b^2)\,t^{10} + (u^4 + b^4 + a^4 + 4\,a^2\,u^2 + \\
&+ 4\,b^2\,u^2 - 12\,b^2\,a^2)\,t^8 + (6\,a^4\,u^2 + 6\,u^2\,b^4 - 8\,a^2\,b^2\,u^2 - \\
&- 2\,u^4\,a^2 - 2\,u^4\,b^2 - 2\,a^4\,b^2 - 2\,b^4\,a^2)\,t^6 + (4\,u^2\,b^4\,a^2 + \\
&+ 4\,a^4\,u^2\,b^2 - 12\,u^4\,a^2\,b^2 + u^4\,a^4 + u^4\,b^4 + a^4\,b^4)\,t^4 + \\
&+ (6\,a^4\,u^2\,b^4 - 2\,u^4\,a^4\,b^2 - 2\,u^4\,a^2\,b^4)\,t^2 + u^4\,a^4\,b^4.
\end{aligned}
\tag{1.1}
$$

The main result of [36] is formulated in the following theorem.

Theorem 1.1. *A perfect Euler cuboid does exist if and only if the Diophantine equation $P_{abu}(t) = 0$ has a solution such that a, b, u, and t are positive integer numbers obeying the inequalities $t > a$, $t > b$, $t > u$, and $(a + t)\,(b + t) > 2\,t^2$.*

Note that $P_{abu}(t)$ is a polynomial of four variables a, b, u and t. However, in the formula (1.1) it is presented as a univariate polynomial depending on three integer parameters a, b, and u. Relying on this presentation, in [37] the theorem 1.1 was reformulated as follows.

Theorem 1.2. *A perfect Euler cuboid does exist if and only if for some positive coprime integer numbers a, b, and u the polynomial equation $P_{abu}(t) = 0$ has a rational solution t obeying the inequalities $t > a$, $t > b$, $t > u$, and $(a+t)\,(b+t) > 2\,t^2$.*

If the equation $P_{abu}(t) = 0$ has a rational solution, then the polynomial (1.1) with integer coefficients is reducible over the field of rational numbers. Note that the leading coefficient of this polynomial is equal to unity. Hence due to the rational root theorem (see [38], [39], or [40]) each rational root of the polynomial $P_{abu}(t)$, if any, is necessarily integer and $P_{abu}(t)$ is reducible over the ring of integers.

In [37] the polynomial (1.1) was studied for reducibility and the following special cases were discovered where $P_{abu}(t)$ is reducible:

$$
\begin{array}{lll}
1) \ \ a = b; & 3) \ \ b\,u = a^2; & 5) \ \ a = u; \\[2mm]
2) \ \ a = b = u; & 4) \ \ a\,u = b^2; & 6) \ \ b = u.
\end{array}
\qquad (1.2)
$$

Being reducible in the cases (1.2), the polynomial (1.1) gives rise to the polynomials

$$
\begin{aligned}
P_{au}(t) = t^8 &+ 6\,(u^2 - a^2)\,t^6 + (a^4 - 4\,a^2\,u^2 + u^4)\,t^4 - \\
&- 6\,a^2\,u^2\,(u^2 - a^2)\,t^2 + u^4\,a^4,
\end{aligned}
\qquad (1.3)
$$

$$
\begin{aligned}
Q_{pq}(t) = t^{10} &+ (2\,q^2 + p^2)\,(3\,q^2 - 2\,p^2)\,t^8 + (q^8 + 10\,p^2\,q^6 + \\
&+ 4\,p^4\,q^4 - 14\,p^6\,q^2 + p^8)\,t^6 - p^2\,q^2\,(q^8 - 14\,p^2\,q^6 + 4\,p^4\,q^4 + \\
&+ 10\,p^6\,q^2 + p^8)\,t^4 - p^6\,q^6\,(q^2 + 2\,p^2)\,(-2\,q^2 + 3\,p^2)\,t^2 - q^{10}\,p^{10}
\end{aligned}
\qquad (1.4)
$$

depending on the integer parameters a, u and p, q. In [37] the reducibility of the polynomials (1.3), (1.4) and the reducibility of the initial polynomial (1.1) were studied numerically and three conjectures were formulated.

Conjecture 1.1. *For any positive coprime integers $a \neq u$ the polynomial $P_{au}(t)$ in (1.3) is irreducible in the ring $\mathbb{Z}[t]$.*

Conjecture 1.2. *For any positive coprime integers $p \neq q$ the polynomial $Q_{pq}(t)$ in (1.4) is irreducible in the ring $\mathbb{Z}[t]$.*

Conjecture 1.3. *For any three positive coprime integer numbers a, b, and u such that none of the conditions (1.2) is satisfied the polynomial $P_{abu}(t)$ in (1.1) is irreducible in the ring $\mathbb{Z}[t]$.*

The main goal of this paper is to prove the following partial result associated with the first cuboid conjecture 1.1.

Theorem 1.3. *For any positive coprime integers $a \neq u$ the polynomial $P_{au}(t)$ in (1.3) has no integer roots.*

2. The inversion symmetry and parity.

The polynomial $P_{au}(t)$ in (1.3) possesses some special property. It is expressed by the following formula which can be verified by direct calculations:

$$
P_{au}(t) = \frac{P_{au}(i\,a\,u/t)\,t^8}{a^4\,u^4}.
\qquad (2.1)
$$

Here $i = \sqrt{-1}$. The formula (2.1) contains the inversion of t in $P_{au}(t)$. For this

reason I call it the inversion symmetry. Apart from (2.1), we have

$$P_{au}(t) = P_{au}(-t). \tag{2.2}$$

The formula (2.2) means that the polynomial $P_{au}(t)$ is even.

3. Breaking the proof of irreducibility into special cases.

The irreducibility of polynomials is usually proved by contradiction. If the conjecture 1.1 is not valid, this would mean that the polynomial (1.3) is reducible, i. e. it is presented as a product of two non-constant polynomials

$$P_{au}(t) = A(t)\,B(t). \tag{3.1}$$

Since $\deg P_{au}(t) = 8$, the equality (3.1) assumes four special cases:

$$
\begin{array}{ll}
1)\;\; P_{au}(t) = A_1(t)\,B_7(t), & 2)\;\; P_{au}(t) = A_2(t)\,B_6(t), \\
3)\;\; P_{au}(t) = A_3(t)\,B_5(t), & 4)\;\; P_{au}(t) = A_4(t)\,B_4(t).
\end{array} \tag{3.2}
$$

Other three cases $P_{au}(t) = A_5(t)\,B_3(t)$, $P_{au}(t) = A_6(t)\,B_2(t)$, $P_{au}(t) = A_7(t)\,B_1(t)$ are equivalent to the cases 1, 2, and 3 up to the transposition of factors.

4. The case of a linear factor.

This case is number one in (3.2). In this case $P_{au}(t) = A_1(t)\,B_7(t)$, where $A_1(t)$ is a linear factor and $B_7(t)$ is its complementary seventh order factor:

$$A_1(t) = t - A_0. \tag{4.1}$$

The formula (3.1) means that $t = A_0$ is a real integer root of the polynomial $P_{au}(t)$. Since $a \neq 0$ and $b \neq 0$, we have $A_0 \neq 0$. Due to (2.1) and (2.2), along with $t = A_0$, the polynomial $P_{au}(t)$ has the following real and imaginary roots:

$$
t = \frac{i\,a\,b}{A_0}, \qquad\qquad t = -A_0, \qquad\qquad t = -\frac{i\,a\,b}{A_0}. \tag{4.2}
$$

The formulas (4.1) and (4.2) mean that

$$P_{au}(t) = (t^2 - A_0^2)\left(t^2 + \frac{a^2\,u^2}{A_0^2}\right)B_4(t). \tag{4.3}$$

Applying the Gauss's lemma (see [38], [39], and [41]), we conclude that the fraction $a^2\,u^2/A_0^2$ in (4.3) simplifies to an integer number. Let's denote

$$C_0 = \frac{a\,u}{A_0}. \tag{4.4}$$

Then the formula (4.3) is written as follows:

$$P_{au}(t) = \left(t^4 + (C_0^2 - A_0^2)\,t^2 - a^2\,u^2\right)B_4(t), \quad \text{where} \;\; A_0\,C_0 = a\,u. \tag{4.5}$$

Now let's apply the formulas (2.1) and (2.2) to (4.5). As a result we get the following symmetries for the polynomial $B_4(t)$ in (4.3) and (4.5):

$$B_4(t) = -\frac{B_4(i\,a\,u/t)\,t^4}{a^2\,u^2}, \qquad\qquad B_4(-t) = B_4(t). \qquad (4.6)$$

The symmetries (4.6) mean that the polynomial $B_4(t)$ is given by the formula

$$B_4(t) = t^4 + B_2\,t^2 - a^2\,u^2. \qquad (4.7)$$

Substituting (4.7) into the formula (4.5), we derive

$$P_{au}(t) = t^8 + (B_2 + C_0^2 - A_0^2)\,t^6 + \big((C_0^2 - A_0^2)\,B_2 - 2\,a^2\,u^2\big)\,t^4 - \\ - a^2\,u^2\,(B_2 + C_0^2 - A_0^2)\,t^2 + u^4\,a^4. \qquad (4.8)$$

Comparing (4.8) with the initial formula (1.3), we find that

$$B_2 + C_0^2 - A_0^2 = 6\,(u^2 - a^2), \\ (C_0^2 - A_0^2)\,B_2 = (u^2 - a^2)^2. \qquad (4.9)$$

The equations (4.9) should be complemented with the equation

$$A_0\,C_0 = a\,u. \qquad (4.10)$$

The equation (4.10) is taken from (4.5). It is equivalent to (4.4). The results of the above calculations are summarized in the following lemma.

Lemma 4.1. *For $a \neq 0$ and $u \neq 0$ the polynomial $P_{au}(t)$ in (1.3) has a linear factor of the form (4.1) in the ring of polynomials $\mathbb{Z}[t]$ if and only if the system of Diophantine equations (4.9) and (4.10) is solvable with respect to the integer variables A_0, B_2, and C_0.*

The Diophantine equations (4.9) and (4.10) are easily solvable for $u = \pm a$. Indeed, in this case we have the following solution for them:

$$A_0 = \pm\,a, \qquad\qquad C_0 = \pm\,a, \qquad\qquad B_2 = 0.$$

Lemma 4.2. *For $u \neq \pm a$ the system of Diophantine equations (4.9) and (4.10) is not solvable with respect to the integer variables A_0, B_2, and C_0.*

Proof. Let's square the first equation (4.9) and let's multiply by 36 the second equation (4.9). As a result we get the equations

$$B_2^2 + 2\,(C_0^2 - A_0^2)\,B_2 + (C_0^2 - A_0^2)^2 = 36\,(u^2 - a^2)^2, \\ 36\,(C_0^2 - A_0^2)\,B_2 = 36\,(u^2 - a^2)^2. \qquad (4.11)$$

Subtracting the second equation (4.11) from the first one, we derive

$$B_2^2 - 34\,(C_0^2 - A_0^2)\,B_2 + (C_0^2 - A_0^2)^2 = 0. \qquad (4.12)$$

The left hand side of the equation (4.12) is factored into the product of two linear terms with respect to B_2. As a result this equation is written as

$$(B_2 - (17 + 12\sqrt{2})(C_0^2 - A_0^2))(B_2 - (17 - 12\sqrt{2})(C_0^2 - A_0^2)) = 0. \qquad (4.13)$$

The equation (4.13) breaks into two separate equations, i.e. it means that A_0, B_2, and C_0 should obey one of the following two equations:

$$\begin{aligned} B_2 &= (17 + 12\sqrt{2})(C_0^2 - A_0^2), \\ B_2 &= (17 - 12\sqrt{2})(C_0^2 - A_0^2). \end{aligned} \qquad (4.14)$$

None of the equations (4.14) can be satisfied by integer numbers A_0, B_2, and C_0 unless $C_0^2 = A_0^2$. But if $C_0^2 = A_0^2$, from the second equation (4.9) we easily derive $u^2 = a^2$ and $u = \pm\, a$. The proof of the lemma 4.2 is over. $\square$

Combining the lemmas 4.1 and 4.2 one easily proves the following theorem.

Theorem 4.1. *For any two positive integers $a \neq u$ the polynomial $P_{au}(t)$ in (1.3) has no linear factors of the form (4.1) in the ring $\mathbb{Z}[t]$.*

The theorem 4.1 implies the theorem 1.3 declared in the introduction. The theorem 1.3 is weaker than the conjecture 1.1. However, if similar results for the other two conjectures 1.2 and 1.3 will be obtained, this would be sufficient to prove the non-existence of perfect cuboids.

References

1. Halcke P., *Deliciae mathematicae oder mathematisches Sinnen-Confect*, N. Sauer, Hamburg, Germany, 1719.
2. Saunderson N., *Elements of algebra,* Vol. 2, Cambridge Univ. Press, Cambridge, 1740.
3. Euler L., *Vollständige Anleitung zur Algebra*, Kayserliche Akademie der Wissenschaften, St. Petersburg, 1771.
4. Dickson L. E, *History of the theory of numbers,* Vol. 2*: Diophantine analysis*, Dover, New York, 2005.
5. Kraitchik M., *On certain rational cuboids*, Scripta Math. **11** (1945), 317–326.
6. Kraitchik M., *Théorie des Nombres,* Tome 3*, Analyse Diophantine et application aux cuboides rationelles*, Gauthier-Villars, Paris, 1947.
7. Kraitchik M., *Sur les cuboides rationelles*, Proc. Int. Congr. Math. **2** (1954), Amsterdam, 33–34.
8. Bromhead T. B., *On square sums of squares*, Math. Gazette **44** (1960), no. 349, 219–220.
9. Lal M., Blundon W. J., *Solutions of the Diophantine equations $x^2 + y^2 2 = l^2$, $y^2 + z^2 = m^2$, $z^2 + x^2 = n^2$*, Math. Comp. **20** (1966), 144–147.
10. Spohn W. G., *On the integral cuboid*, Amer. Math. Monthly **79** (1972), no. 1, 57-59.
11. Spohn W. G., *On the derived cuboid*, Canad. Math. Bull. **17** (1974), no. 4, 575-577.
12. Chein E. Z., *On the derived cuboid of an Eulerian triple*, Canad. Math. Bull. **20** (1977), no. 4, 509–510.
13. Leech J., *The rational cuboid revisited*, Amer. Math. Monthly **84** (1977), no. 7, 518–533; see also Erratum, Amer. Math. Monthly **85** (1978), 472.
14. Leech J., *Five tables relating to rational cuboids*, Math. Comp. **32** (1978), 657–659.
15. Spohn W. G., *Table of integral cuboids and their generators*, Math. Comp. **33** (1979), 428–429.
16. Lagrange J., *Sur le dérivé du cuboide Eulérien*, Canad. Math. Bull. **22** (1979), no. 2, 239–241.
17. Leech J., *A remark on rational cuboids*, Canad. Math. Bull. **24** (1981), no. 3, 377–378.
18. Korec I., *Nonexistence of small perfect rational cuboid*, Acta Math. Univ. Comen. **42/43** (1983), 73–86.
19. Korec I., *Nonexistence of small perfect rational cuboid II*, Acta Math. Univ. Comen. **44/45** (1984), 39–48.

20. Wells D. G., *The Penguin dictionary of curious and interesting numbers*, Penguin publishers, London, 1986.
21. Bremner A., Guy R. K., *A dozen difficult Diophantine dilemmas*, Amer. Math. Monthly **95** (1988), no. 1, 31–36.
22. Bremner A., *The rational cuboid and a quartic surface*, Rocky Mountain J. Math. **18** (1988), no. 1, 105–121.
23. Colman W. J. A., *On certain semiperfect cuboids*, Fibonacci Quart. **26** (1988), no. 1, 54–57; see also *Some observations on the classical cuboid and its parametric solutions*, Fibonacci Quart. **26** (1988), no. 4, 338–343.
24. Korec I., *Lower bounds for perfect rational cuboids,*, Math. Slovaca **42** (1992), no. 5, 565–582.
25. Guy R. K., *Is there a perfect cuboid? Four squares whose sums in pairs are square. Four squares whose differences are square*, Unsolved Problems in Number Theory, 2nd ed., Springer-Verlag, New York, 1994, pp. 173–181.
26. Rathbun R. L., Granlund T., *The integer cuboid table with body, edge, and face type of solutions*, Math. Comp. **62** (1994), 441–442.
27. Van Luijk R., *On perfect cuboids,* Doctoraalscriptie, Mathematisch Instituut, Universiteit Utrecht, Utrecht, 2000.
28. Rathbun R. L., Granlund T., *The classical rational cuboid table of Maurice Kraitchik*, Math. Comp. **62** (1994), 442–443.
29. Peterson B. E., Jordan J. H., *Integer hexahedra equivalent to perfect boxes*, Amer. Math. Monthly **102** (1995), no. 1, 41–45.
30. Rathbun R. L., *The rational cuboid table of Maurice Kraitchik*, e-print math.HO/0111229 in Electronic Archive http://arXiv.org.
31. Hartshorne R., Van Luijk R., *Non-Euclidean Pythagorean triples, a problem of Euler, and rational points on K3 surfaces*, e-print math.NT/0606700 in Electronic Archive http://arXiv.org.
32. Waldschmidt M., *Open diophantine problems*, e-print math.NT/0312440 in Electronic Archive http://arXiv.org.
33. Ionascu E. J., Luca F., Stanica P., *Heron triangles with two fixed sides*, e-print math.NT/0608 185 in Electronic Archive http://arXiv.org.
34. Sloan N. J. A, *Sequences A031173, A031174, and A031175*, On-line encyclopedia of integer sequences, OEIS Foundation Inc., Portland, USA.
35. Stoll M., Testa D., *The surface parametrizing cuboids*, e-print arXiv:1009.0388 in Electronic Archive http://arXiv.org.
36. Sharipov R. A., *A note on a perfect Euler cuboid*, e-print arXiv:1104.1716 in Electronic Archive http://arXiv.org.
37. Sharipov R. A., *Perfect cuboids and irreducible polynomials*, e-print arXiv:1108.5348 in Electronic Archive http://arXiv.org.
38. Artin M., *Algebra*, Prentice Hall, New Jersey, 1991.
39. Kostrikin A. I., *Algebra*, Nauka publishers, Moscow, 1977.
40. *Rational root theorem*, Wikipedia, the Free Encyclopedia, Wikimedia Foundation Inc., San Francisco, USA.
41. *Gauss's lemma (polynomial)*, Wikipedia, the Free Encyclopedia, Wikimedia Foundation Inc., San Francisco, USA.

Bashkir State University, 32 Zaki Validi street, 450074 Ufa, Russia
E-mail address: r-sharipov@mail.ru