PERFECT CUBOIDS AND IRREDUCIBLE POLYNOMIALS.

RUSLAN SHARIPOV

Abstract. The problem of constructing a perfect cuboid is related to a certain class of univariate polynomials with three integer parameters \(a, b,\) and \(u\). Their irreducibility over the ring of integers under certain restrictions for \(a, b,\) and \(u\) would mean the non-existence of perfect cuboids. This irreducibility is conjectured and then verified numerically for approximately 10,000 instances of \(a, b,\) and \(u\).

1. Introduction.

An Euler cuboid is a rectangular parallelepiped whose edges and face diagonals all have integer lengths. A perfect cuboid is an Euler cuboid whose space diagonal is also of an integer length. Cuboids with integer sides and face diagonals were known before Euler (see [1] and [2]). However, they became famous due to Leonhard Euler (see [3]) and were named after him.

As for perfect cuboids, none of them is known by now. The problem of finding perfect cuboids or proving their non-existence is an open mathematical problem. The search for perfect cuboids has the long history. It is reflected in [4–34].

In [35] the problem of finding a perfect cuboid was reduced to the following Diophantine equation of the order 12 with four variables \(a, b, c,\) and \(u\):

\[
\begin{align*}
&u^4 a^4 b^4 + 6 a^4 u^2 b^4 c^2 - 2 u^4 a^4 b^2 c^2 - 2 u^4 a^2 b^4 c^2 + 4 u^2 b^4 a^2 c^4 + \\
&+ 4 a^4 u^2 b^2 c^4 - 12 u^4 a^2 b^2 c^4 + u^4 a^4 c^4 + u^4 b^4 c^4 + a^4 b^4 c^4 + \\
&+ 6 a^4 u^2 c^6 + 6 u^2 b^4 c^6 - 8 a^2 b^2 u^2 c^6 - 2 u^4 a^2 c^6 - 2 u^4 b^2 c^6 - \\
&- 2 a^4 b^2 c^6 - 2 b^4 a^2 c^6 + u^4 c^8 + b^4 c^8 + a^4 c^8 + 4 a^2 u^2 c^8 + \\
&+ 4 b^2 u^2 c^8 - 12 b^2 a^2 c^8 + 6 u^2 c^{10} - 2 a^2 c^{10} - 2 b^2 c^{10} + c^{12} = 0.
\end{align*}
\]

The exact result of the paper [35] is formulated as follows.

Theorem 1.1. A perfect Euler cuboid does exist if and only if the Diophantine equation (1.1) has a solution such that \(a, b, c,\) and \(u\) are positive integer numbers obeying the inequalities and \(a < c, b < c, u < c,\) and \((a + c)(b + c) > 2 c^2.\)

A more simple equation associated with perfect cuboids was derived in [18] (see also [27]). However, our goal in this paper is to study the equation (1.1) (because it is new) and derive the results declared in the abstract.

2000 Mathematics Subject Classification. 11D41, 11D72, 11Y50, 12E05.
2. Rational cuboids.

A rational cuboid is a rectangular parallelepiped the lengths of whose edges are rational numbers. If the lengths of face diagonals are also rational numbers, it is called a rational Euler cuboid. Finally, if the length of the space diagonal is a rational number too, we have a perfect rational cuboid. It is easy to see that each rational Euler cuboid can be transformed to an Euler cuboid with integer sides and diagonals. In the case of perfect cuboids (either integer or rational) each such cuboid can be transformed to a perfect rational cuboid whose space diagonal is equal to unity (see [35]). Conversely each perfect rational cuboid with unit space diagonal yields some perfect cuboid with integer sides and diagonals. Therefore, saying a perfect rational cuboid, we assume its space diagonal to be equal to unity.

3. Expressions for the sides and face diagonals.

Note that the equation (1.1) is homogeneous with respect to its variables \(a, b, c,\) and \(u\). Since \(c > 0\) in the theorem 1.1, we can introduce the fractions

\[
\alpha = \frac{a}{c}, \quad \beta = \frac{b}{c}, \quad \upsilon = \frac{u}{c}.
\]

(3.1)

In terms of the rational variables (3.1) the equation (1.1) is written as

\[
v^4 \alpha^4 \beta^4 + (6 \alpha^4 \upsilon^2 \beta^4 - 2 \upsilon^4 \alpha^4 \beta^2 - 2 \upsilon^4 \alpha^2 \beta^4) + (4 \upsilon^2 \beta^4 \alpha^2 + 4 \alpha^4 \upsilon^4 \beta^2 - 12 \upsilon^4 \alpha^2 \beta^2 + v^4 \alpha^4 + v^4 \beta^4 + \alpha^4 \beta^4) + (6 \alpha^4 \upsilon^2 + 6 \upsilon^2 \beta^4 - 8 \alpha^2 \beta^2 \upsilon^2 - 2 \upsilon^4 \alpha^2 - 2 \upsilon^4 \beta^2 - 2 \beta^4 \alpha^2) + (\upsilon^4 + \beta^4 + \alpha^4 + 4 \alpha^2 \upsilon^2 + 4 \beta^2 \upsilon^2 - 12 \beta^2 \alpha^2) + (6 \upsilon^2 - 2 \alpha^2 - 2 \beta^2) + 1 = 0.
\]

(3.2)

Note that the variables \(a, b, c,\) and \(u\) in (1.1) are neither edges nor diagonals of a perfect cuboid, they are just parameters. They yield the rational parameters \(\alpha, \beta,\) and \(\upsilon\) in (3.2) according to the formulas (3.1). The edges and face diagonals of a perfect rational cuboid are expressed through \(\alpha, \beta,\) and \(\upsilon\). Let’s denote through \(x_1, x_2,\) and \(x_3\) the edges of such a cuboid and through \(d_1, d_2,\) and \(d_3\) its side diagonals:

\[
(x_1)^2 + (x_2)^2 = (d_3)^2, \quad (x_2)^2 + (x_3)^2 = (d_1)^2, \quad (x_3)^2 + (x_1)^2 = (d_2)^2.
\]

(3.3)

Then \(x_1\) and \(d_1\) are expressed through the parameter \(\upsilon:\)

\[
x_1 = \frac{2 \upsilon}{1 + \upsilon^2}, \quad d_1 = \frac{1 - \upsilon^2}{1 + \upsilon^2}.
\]

(3.4)

Let’s denote through \(z\) the following auxiliary parameter:

\[
z = \frac{(1 + \upsilon^2) (1 - \beta^2) (1 + \alpha^2)}{2 (1 + \beta^2) (1 - \alpha^2 \upsilon^2)}.
\]

(3.5)

Then the edges \(x_2\) and \(x_3\) are expressed by the formulas

\[
x_2 = \frac{2 z (1 - \upsilon^2)}{(1 + \upsilon^2) (1 + z^2)}, \quad x_3 = \frac{(1 - \upsilon^2) (1 - z^2)}{(1 + \upsilon^2) (1 + z^2)}.
\]

(3.6)
The side diagonals $d_2$ and $d_3$ are given by the following formulas:

\[ d_2 = \frac{(1 + v^2)(1 + z^2) + 2z(1 - v^2)}{(1 + v^2)(1 + z^2)} \beta, \]
\[ d_3 = \frac{2(v^2 z^2 + 1)}{(1 + v^2)(1 + z^2)} \alpha. \]  

(3.7)

The formulas (3.4), (3.5), (3.6) and (3.7) are taken from [35]. They can be verified by means of direct calculations. Indeed, the second equality (3.3) turns to an identity due to the formulas (3.6). Apart from the equalities (3.3), a perfect rational cuboid is characterized by the equalities

\[ (x_1)^2 + (d_1)^2 = 1, \quad (x_2)^2 + (d_2)^2 = 1, \quad (x_3)^2 + (d_3)^2 = 1. \]  

(3.8)

They mean that the space diagonal of such a cuboid is equal to unity. The first equality (3.8) turns to an identity due to the formulas (3.4).

Thus, the second equality (3.3) and the first equality (3.8) turn to identities. Other four equalities in (3.3) and (3.8) also turn to identities due to (3.4), (3.5), (3.6) and (3.7) modulo the equation (3.2).

4. Back to integer numbers.

The equation (1.1) is homogeneous with respect to its variables. Therefore due to (3.1) and due to the theorem 1.1 the parameters $a$, $b$, $c$, and $u$ in the equation (1.1) can be treated as a quadruple of positive coprime integer numbers, i.e. their greatest common divisor is equal to unity:

\[ \gcd(a, b, c, u) = 1. \]  

(4.1)

Let’s denote through $m$ the greatest common divisor of $a$, $b$, and $u$:

\[ \gcd(a, b, u) = m. \]  

(4.2)

Then from (4.1) and (4.2) we derive the equality

\[ \gcd(m, c) = 1, \]  

(4.3)

i.e. $m$ and $c$ are coprime. Due to (4.2) and (4.3) the fractions $a/m$, $b/m$, and $u/m$ reduce to integer numbers, while $c/m$ is an irreducible fraction if $m \neq 1$. The formula (3.1) can be written in terms of these fractions:

\[ \alpha = \frac{a/m}{c/m}, \quad \beta = \frac{b/m}{c/m}, \quad v = \frac{u/m}{c/m}. \]  

(4.4)

Relying on (4.4), we can change variables as follows:

\[ \frac{a}{m} \rightarrow a, \quad \frac{b}{m} \rightarrow b, \quad \frac{u}{m} \rightarrow u, \quad \frac{c}{m} \rightarrow t. \]  

(4.5)
In terms of the new variable \( t = c/m \) and in terms of the renewed variables \( a, b, \) and \( u \) in (4.5) the formulas (4.4) are written as

\[
\alpha = \frac{a}{t}, \quad \beta = \frac{b}{t}, \quad v = \frac{u}{t}, \quad (4.6)
\]

while the equation (1.1) turns to the following equation:

\[
t^{12} + (6 u^2 - 2 a^2 - 2 b^2) t^{10} + (u^4 + b^4 + a^4 + 4 a^2 u^2 + \\
+ 4 b^2 u^2 - 12 b^2 a^2) t^8 + (6 a^4 u^2 + 6 u^2 b^4 - 8 a^2 b^2 u^2 - \\
- 2 u^4 a^2 - 2 u^4 b^2 - 2 a^4 b^2 - 2 b^4 a^2) t^6 + (4 a^2 b^4 a^2 + \\
+ 4 a^4 u^2 b^2 - 12 u^4 a^2 b^2 + u^4 a^4 + u^4 b^4 + a^4 b^4) t^4 + \\
+ (6 a^4 u^2 b^4 - 2 u^4 a^4 b^2 - 2 u^4 a^2 b^4) t^2 + u^4 a^4 b^4 = 0.
\]

As for the formula (4.2), for the renewed variables \( a, b, \) and \( u \) in (4.5) it yields

\[
\gcd(a, b, u) = 1. \quad (4.8)
\]

The formula (4.8) means that \( a, b, \) and \( u \) in (4.6) and (4.7) are coprime.

Note that the equation (4.7) is the same as the initial equation (1.1), but \( c \) is replaced by \( t \) and the terms are reordered like in a univariate polynomial of the variable \( t \). The theorem 1.1 now is reformulated as follows.

**Theorem 4.1.** A perfect Euler cuboid does exist if and only if for some positive coprime integer numbers \( a, b, \) and \( u \) the polynomial equation (4.7) has a rational solution \( t \) obeying the inequalities \( t > a, t > b, t > u, \) and \((a + t) (b + t) > 2 t^2 \).

5. **Factoring the polynomial equation.**

Let’s denote through \( P_{abu}(t) \) the polynomial in the left hand side of the equation (4.7). Denoting it in this way, we shall treat it as a univariate polynomial of \( t \), while the variables \( a, b, \) and \( u \) are treated as parameters:

\[
P_{abu}(t) = t^{12} + (6 u^2 - 2 a^2 - 2 b^2) t^{10} + (u^4 + b^4 + a^4 + 4 a^2 u^2 + \\
+ 4 b^2 u^2 - 12 b^2 a^2) t^8 + (6 a^4 u^2 + 6 u^2 b^4 - 8 a^2 b^2 u^2 - \\
- 2 u^4 a^2 - 2 u^4 b^2 - 2 a^4 b^2 - 2 b^4 a^2) t^6 + (4 a^2 b^4 a^2 + \\
+ 4 a^4 u^2 b^2 - 12 u^4 a^2 b^2 + u^4 a^4 + u^4 b^4 + a^4 b^4) t^4 + \\
+ (6 a^4 u^2 b^4 - 2 u^4 a^4 b^2 - 2 u^4 a^2 b^4) t^2 + u^4 a^4 b^4.
\]

The polynomial (5.1) is symmetric with respect to the parameters \( a \) and \( b \), i.e.

\[
P_{abu}(t) = P_{bua}(t). \quad (5.2)
\]

In order to study the polynomial \( P_{abu}(t) \) we consider some special cases:

\[
1) \ a = b; \quad 3) \ b u = a^2; \quad 5) \ a = u; \\
2) \ a = b = u; \quad 4) \ a u = b^2; \quad 6) \ b = u. \quad (5.3)
\]
**The special case** \( a = b \). In this special case the polynomial \( P_{abu}(t) = P_{aau}(t) \) is given by the following formula:

\[
P_{aau}(t) = t^{12} + (6u^2 - 4a^2)t^{10} + (8a^2u^2 - 10a^4 + u^4)t^8 + \]
\[
+ (4a^4u^2 - 4a^6 - 4u^4a^2)t^6 + (8a^6u^2 + a^8 - 10u^4a^4)t^4 + \]
\[
+ (6a^8u^2 - 4u^4a^6)t^2 + u^4a^8. \tag{5.4}
\]

The polynomial (5.4) is reducible. It is factored as

\[
P_{aau}(t) = (t^2 + a^2)^2 P_{au}(t), \tag{5.5}
\]

where the polynomial \( P_{au}(t) \) is given by the formula

\[
P_{au}(t) = t^8 + 6(a^2 - u^2)t^6 + (a^4 - 4a^2u^2 + u^4)t^4 - \]
\[
- 6a^2u^2(a^2 - u^2)t^2 + u^4a^4. \tag{5.6}
\]

The formulas (5.5) and (5.6) are easily proved by direct calculations.

**The special case** \( a = b = u \). This case corresponds to \( a = u \) in (5.6). If \( a = u \), the polynomial \( P_{au}(t) = P_{aa}(t) \) is reducible:

\[
P_{aa}(t) = (t - a)^2(t + a)^2(t^2 + a^2)^2. \tag{5.7}
\]

Due to the coprimality (4.8) the special case \( a = b = u \) can fit the theorem 4.1 only for \( a = b = u = 1 \). Then, due to (5.5) and (5.7), the equation (4.7) looks like

\[
(t - 1)^2(t + 1)^2(t^2 + 1)^4 = 0. \tag{5.8}
\]

The equation (5.8) has two real rational solutions \( t = -1 \) and \( t = 1 \). Both of them do not fit the theorem 4.1. Indeed, both of them do not satisfy the inequality \( t > a \), where \( a = 1 \).

Thus, the subcase \( a = b = u \) of the special case \( a = b \) do not provide any perfect cuboid. Other subcases of the case \( a = b \) are described by the following conjecture.

**Conjecture 5.1.** For any positive coprime integers \( a \neq u \) the polynomial \( P_{au}(t) \) in (5.6) is irreducible in the ring \( \mathbb{Z}[t] \).

**The special case** \( bu = a^2 \). Combining \( bu = a^2 \) with (4.8) one can easily derive the following presentation for the integer numbers \( a, b, \) and \( u \):

\[
a = pq, \quad b = p^2, \quad u = q^2. \tag{5.9}
\]

Here \( p \) and \( q \) are two positive integers, satisfying the coprimality condition

\[
gcd(p, q) = 1. \tag{5.10}
\]
Substituting \((5.9)\) into \((5.1)\), we get the polynomial
\[
P_{ppq^2}(t) = t^{12} + (6q^4 - 2p^2q^2 - 2p^4)t^{10} + (q^8 + 4p^2q^6 + \\
+ 5p^4q^4 - 12p^6q^2 + p^8)t^8 - 2p^2q^2(q^8 - 2p^2q^6 + 4p^4q^4 - \\
- 2p^6q^2 + p^8)t^6 + p^4q^4(q^8 - 12p^2q^6 + 5p^4q^4 + 4p^6q^2 + p^8)t^4 + \\
+ q^8p^8(-2q^4 - 2p^2q^2 + 6p^4)t^2 + q^{12}p^{12}. \tag{5.11}
\]
The polynomial \(P_{ppq^2}(t)\) in \((5.11)\) is reducible. Indeed, we have
\[
P_{ppq^2}(t) = (t - a)(t + a)Q_{pq}(t), \tag{5.12}
\]
where \(Q_{pq}(t)\) is the following polynomial:
\[
Q_{pq}(t) = t^{10} + (2q^2 + p^2)(3q^2 - 2p^2)t^8 + (q^8 + 10p^2q^6 + \\
+ 4p^4q^4 - 14p^6q^2 + p^8)t^6 - p^2q^2(q^8 - 14p^2q^6 + 4p^4q^4 + \\
+ 10p^6q^2 + p^8)t^4 - p^6q^2(q^8 + 2p^2)(-2q^4 + 3p^2)t^2 - q^{10}p^{10}. \tag{5.13}
\]
Due to \((5.12)\) the polynomial \((5.11)\) has two rational roots \(t = a\) and \(t = -a\). Both of them do not fit the theorem 4.1 since they do not satisfy the inequality \(t > a\).

Other roots of the polynomial \((5.11)\) coincide with the roots of the polynomial \(Q_{pq}(t)\) in \((5.13)\). The polynomial \((5.13)\) is reducible if \(q = p\). In this case we have
\[
Q_{pq}(t) = (t - a)(t + a)(t^2 + a^2)^4. \tag{5.14}
\]
The formula \((5.14)\) is not surprising. For \(q = p\) from \((5.9)\) we derive \(a = b = u\). This case was already considered (see \((5.7)\) and \((5.8)\)). From \(q = p\) and \((5.10)\) we derive \(p = q = 1\) and \(a = b = u = 1\).

In the case \(p \neq q\) the polynomial \((5.13)\) is described by the following conjecture.

**Conjecture 5.2.** For any positive coprime integers \(p \neq q\) the polynomial \(Q_{pq}(t)\) in \((5.13)\) is irreducible in the ring \(\mathbb{Z}[t]\).

**The special case** \(au = b^2\). This special case reduces to the previous one. Indeed, from \(au = b^2\) and \((4.8)\) we derive
\[
a = p^2, \quad b = pq, \quad u = q^2, \tag{5.15}
\]
where \(p\) and \(q\) are two positive integer numbers obeying the coprimality condition \((5.10)\). When substituted into \((5.1)\), the formulas \((5.15)\) are equivalent to \((5.9)\) due to the symmetry \((5.2)\). They lead to the polynomial \(P_{pppq^2}(t)\) coinciding with the polynomial \((5.11)\) and then lead to the polynomial \((5.13)\), which was already considered.

**The special case** \(a = u\). This special case is rather trivial. In this case the polynomial \(P_{abu}(t) = P_{abu}(t)\) in \((5.1)\) is reducible and we have the formula
\[
P_{abu}(t) = (t^2 + u^2)^4(t - b)^2(t + b)^2. \tag{5.16}
\]
The polynomial \((5.16)\) has two real rational roots \(t = b\) and \(t = -b\). Both of them do not fit the theorem 4.1 since they do not satisfy the inequality \(t > b\).
PERFECT CUBOIDS AND IRREDUCIBLE POLYNOMIALS.

The special case \( b = u \). This case is equivalent to the previous one due to the symmetry (5.2).

The general case not covered by the special cases listed in (5.3) is described by the following conjecture.

**Conjecture 5.3.** For any three positive coprime integer numbers \( a, b, \) and \( u \) such that none of the conditions (5.3) is satisfied the polynomial (5.1) is irreducible in the ring \( \mathbb{Z}[t] \).


There are no proofs for the conjectures 5.1, 5.2, and 5.3 at present time. Therefore I explored them numerically. For this purpose I used the Maxima package version 5.21.1 with the graphic interface wxMaxima 0.85 on the platform of Ubuntu 10.10 with Linux 2.5.35-24.

The conjecture 5.1 was verified and confirmed for \( 1 \leq a \leq 100 \) and \( 1 \leq u \leq 100 \). The conjecture 5.2 was confirmed for \( 1 \leq p \leq 100 \) and \( 1 \leq q \leq 100 \). And the third conjecture 5.3 was confirmed for \( 1 \leq a \leq 22, 1 \leq b \leq 22, \) and \( 1 \leq u \leq 22 \). The number 22 was chosen intentionally since

\[
22^2 = 10648 \approx 10000 = 100^2.
\]

This equality means that each conjecture was tested and confirmed for approximately 10,000 instances of the numeric parameters in it. The overall result obtained can be formulated as follows: the equation (4.7) has no solutions providing perfect cuboids for \( a, b, \) and \( u \) less than or equal to 22.

7. Conclusions.

The conjectures 5.1, 5.2, and 5.3 are not equivalent to the non-existence of perfect cuboids. However, if they are valid, this would be sufficient to prove that perfect cuboids do not exist. The results of the numeric computations reported in the previous section support these conjectures.

References

3. Euler L., *Vollk"{a}ndige Anleitung zur Algebra*, K"{a}yserliche Akademie der Wissenschaften, St. Petersburg, 1771.


