Ivan Korec

Lower bounds for perfect rational cuboids

Mathematica Slovaca, Vol. 42 (1992), No. 5, 565--582

Persistent URL: http://dml.cz/dmlcz/132903

Math. Slovaca, **42** (1992), No. 5, 565–582

Mathematica Slovaca

LOWER BOUNDS FOR PERFECT RATIONAL CUBOIDS

IVAN KOREC[1)]

ABSTRACT. Some lower bounds for a perfect rational cuboid are derived with the help of a computer. For example, its greatest edge must be at least $4 \cdot 10^9$ and its body diagonal z must be at least $11 \cdot 10^6 \cdot q$, where q is the greatest prime divisor of z. Further, z can be neither a prime power nor a product of two primes.

1. Introduction and the main result

A perfect rational cuboid is a cuboid in which (the lengths of) all three edges x_1, x_2, x_3, all three face diagonals y_1, y_2, y_3 and the body diagonal z are integers. It is not known whether any such cuboid exists. In the present paper we prove (using computer computations) that if a perfect rational cuboid exists, then it must be rather large. More precisely, the following result will be proved:

THEOREM 1. *Let z be the body diagonal of a perfect rational cuboid and x be its maximal edge. Then:*

(i) *If q is a prime divisor of z and $z = nq$, then $n > 11 \cdot 10^6$,*
(ii) $z > 8 \cdot 10^9$,
(iii) $x > 4 \cdot 10^9$.

The statements (i) and (ii) are proved by computer computations. The statement (i) substantially diminishes the number of z which must be considered in the computation for (ii); one needs to consider only those z which are not excluded by (i). However, (i) seems to be also of independent interest, therefore the bound for n was computed as high as possible in reasonable time. The statement (iii) is an easy consequence of (ii) and the inequality $z < x \cdot \sqrt{3}$.

The present paper deals more with number-theoretical results necessary for the computations mentioned above than with the details of computer programs.

AMS Subject Classification (1991): Primary 11D09, 11Y50. Secondary 11D72.
Key words: Perfect rational cuboid, Diophantine equations.
[1)] Research supported by Slovak Academy of Sciences Grant 363.

However, these results are presented in the form and order suitable for understanding the programs.

2. Notation and general conditions

Every variable will denote an integer unless something else is explicitly stated; i will denote the imaginary unit. GCD will denote the greatest common divisor, $|$ divisibility relation, **Re**, **Im** the real and the imaginary part of a complex number. $\mathbf{ex}_p(x)$ will denote the exponent of the prime p in the standard factorization of $x \neq 0$. The notation $x = \square$ will mean that x is a square (of an integer), $x \equiv \square \pmod{m}$ ($x \not\equiv \square \pmod{m}$) will mean that x is a quadratic residue (nonresidue, respectively) modulo m.

We shall look for positive integers x_1, x_2, x_3, y_1, y_2, y_3, z which satisfy the equations

$$\begin{gathered} x_1^2 + x_2^2 = y_3^2, \qquad x_1^2 + x_3^2 = y_2^2, \qquad x_2^2 + x_3^2 = y_1^2, \\ x_1^2 + x_2^2 + x_3^2 = z^2. \end{gathered} \tag{2.1}$$

They can be interpreted as the lengths of edges and diagonals of a perfect rational cuboid, as it has been mentioned in the introduction. It is not known whether such integers exist; we shall show that they must be rather large if they exist at all. Without loss of generality we may consider only *primitive* perfect rational cuboids, i. e. we may assume that x_1, x_2, x_3 are relatively prime. Hence (at least) one edge is odd, let it be x_3. Then by easy considerations modulo 8 we can see that x_1, x_2, y_3 are even (and also multiples of 4). The integers y_1, y_2, z are odd. The notation (2.1) (as well as the terminology of this paragraph) is used throughout the whole paper.

Now we shall present three auxiliary results.

LEMMA 2.1. *If z is the body diagonal of a primitive perfect rational cuboid and p is a prime divisor of z, then $p \equiv 1 \pmod{4}$.*

P r o o f. We already know that z is odd, hence we must only prove that z has no prime divisor $p \equiv 3 \pmod{4}$. If p is such a divisor, then $x_1^2 + y_1^2 = z^2$ implies $x_1^2 + y_1^2 \equiv 0 \pmod{p}$, and then $p \mid x$, $p \mid y$. (Otherwise we would have $(x_1^{-1} y_1)^2 \equiv -1 \pmod{p}$, but -1 is a quadratic non-residue modulo p.) Analogously we obtain $p \mid x_2$, $p \mid x_3$, which contradicts $\mathrm{GCD}(x_1, x_2, x_3) = 1$.

LEMMA 2.2. *Let n, q, x be odd positive integers, y be a nonnegative integer and*

$$n^2 q^2 = x^2 + y^2. \tag{2.2.1}$$

Then there are integers a, b, u, v *such that*

$$n^2 = a^2 + (4b)^2, \qquad q^2 = u^2 + (4v)^2 \tag{2.2.2}$$

and

$$x = |au - 16bv|, \qquad y = 4 \cdot |av + bu|. \tag{2.2.3}$$

Further, a, u *are odd and* a, b, u *can be chosen nonnegative.*

P r o o f. If n or q has a prime divisor $p = 4k+3$, then x, y are multiples of p, and we can cancel (2.2.1) by p^2; therefore we may assume that all prime divisors of nq have the form $4k+1$. Let

$$x + y\,\mathrm{i} = \mathrm{i}^e \cdot (r_1 + s_1\,\mathrm{i}) \cdot \ldots \cdot (r_t + s_t\,\mathrm{i}), \tag{2.2.4}$$

$0 \le e \le 3$, be the factorization of $x + y\,\mathrm{i}$ in the ring of Gaussian integers. We may assume that $r_1, \ldots, r_t$ are odd; then $s_1, \ldots, s_t$ are even, and $\mathrm{i}^e = \pm 1$. Obviously

$$n^2 q^2 = x^2 + y^2 = (r_1^2 + s_1^2) \cdot \ldots \cdot (r_t^2 + s_t^2),$$

where the right-hand side is a product of primes. They can be partitioned into two groups, one with the product n and the other with the product q. Let us partition the right side of (2.2.4) in the same way, and denote the products of the obtained groups by $a + b\,\mathrm{i}$ and $u + w\,\mathrm{i}$, respectively. Then a, u are odd and

$$n^2 = a^2 + d^2, \qquad q^2 = u^2 + w^2, \qquad x + y\,\mathrm{i} = (a + d\,\mathrm{i}) \cdot (u + w\,\mathrm{i}).$$

From $x > 0$, $y \ge 0$ and the latest equality we obtain

$$x = |au - dw|, \qquad y = |aw + du|. \tag{2.2.5}$$

Now we can change the signs of a, d, u, w so that a, d, u will be nonnegative (and (2.2.5) remains true). Further, since n, a are odd we have $d^2 \equiv 1 - 1 \equiv 0 \pmod 8$ and hence $d = 4b$ for some integer b. Analogously $w = 4v$, and after substitution we obtain the formulae (2.2.2), (2.2.3).

By Lemma 2.2 we can find all x, y satisfying $x^2 + y^2 = z^2$ provided that z is factorized and we can solve this equation when z is a prime power. The last question is answered by:

LEMMA 2.3. *If* $q \equiv 1 \pmod 4$ *is a prime,* e, r, s *are positive integers and* $q = r^2 + (2s)^2$, *then all nonnegative integer solutions* (x, y), x *odd, of the equation*

$$x^2 + y^2 = q^{2e}$$

are given by the formulae

$$x = q^{e-f} \cdot |\mathbf{Re}((r + 2s\,\mathrm{i})^{2f})|\,, \qquad y = q^{e-f} \cdot |\mathbf{Im}((r + 2s\,\mathrm{i})^{2f})|\,, \tag{2.3.1}$$

where $0 \le f \le e$.

P r o o f. We can use the factorization over the ring of Gaussian integers

$$q^{2e} = (r + 2s\,\mathrm{i})^{2e} \cdot (r - 2s\,\mathrm{i})^{2e}$$

and take arbitrary $2e$ factors from the right side. Since the result is not new in essential and considerations are similar as above the details will be omitted. Notice that for every prime $q \equiv 1 \pmod 4$ positive integers r, s which satisfy $r^2 + (2s)^2 = q$ exist and are uniquely determined.

We shall also need the following theorem:

THEOREM 2.4. *The diophantine equation*

$$x^4 + 18x^2y^2 + y^4 = z^2 \tag{2.4.1}$$

has no integer solution with $xy \ne 0$.

It is a result of H . C . P o c k l i n g t o n ; in [4, page 116] he writes:

"Collecting results, we have $x^4 + nx^2y^2 + y^4 = z^2$ impossible if n is 0, 1, 3, 4, 5, 6, 7 (unless $x = y$), 9, 10, 11, 14 (unless $x = y$), 15, 18, 19, 20, 21, 22, 25, 28, 29, 35, 45, 51, 59, 65, 69, 74, 81, 91, and if $-n$ is 1 (unless $x = y$), 3, 5, 6, 7, 8, 10, 12, 14, 17, 18, 19, 20, 21, 22, 23, 24, 27, 29, 31, 45, 54, 55, 60, 61, 69, 75. If n lies between -30 and 30, the equation can be solved except in the cases just given."

However, the list contains an error; for $-n = 27$ the equation (2.4.1) has the solution $(21, 4, 65)$. Since this error would make Theorem 2.4 suspicious we briefly show how to reduce it to the equation $x^4 - 3x^2y^2 + y^4 = z^2$, which has no integer solution with $xy \ne 0$ by M o r d e l l [3, page 22] (and also by the P o c k l i n g t o n 's list above). Assume that (x, y, z), $xy \ne 0$ is a solution of (2.4.1). Then $z = x^2 + 4axy + y^2$ for a rational number $a = \frac{u}{v} \ne 0$. By substitution into (2.4.1) and an easy computation we obtain a quadratic equation for $\frac{x}{y}$:

$$a \cdot \left(\frac{x}{y}\right)^2 + (2a^2 - 2) \cdot \frac{x}{y} + a = 0\,.$$

Its discriminant $4a^4 - 12a^2 + 4$ must be a square of a rational number. Therefore $u^4 - 3u^2v^2 + v^4 = \square$, and $uv \ne 0$, which is a contradiction.

3. Number-theoretical background for the computation of the lower bound of n

We assume here (2.1) and all conditions on the variables contained in (2.1) from the previous section (particularly, x_3 is odd). Further we assume $z = nq$, where q is a prime. By Lemma 2.1 we know that $q \equiv 1 \pmod 4$. Hence by Lemma 2.3 the integer q^2 can be written as the sum of squares of an odd positive integer and an even integer in three ways:

$$q^2 = q^2 + 0^2, \qquad q^2 = u^2 + (-4v)^2, \qquad q^2 = u^2 + (4v)^2, \tag{3.1}$$

where

$$u = |r^2 - 4s^2|, \qquad |v| = |rs| \neq 0, \qquad r^2 + (2s)^2 = q. \tag{3.2}$$

A parameter k (usually with a subscript) will be used to refer three cases in (3.1); the corresponding values of k will be 0, 1, 2, respectively. (It is not suitable to assume $v > 0$ here, and to write v instead of $|v|$ in (3.2), because we want to use the transformation $v \mapsto -v$ in Lemma 3.4 below.)

THEOREM 3.1. *Let there be a primitive perfect rational cuboid with the body diagonal $z = nq$, q a prime and let $u > 0$, v satisfy $u^2 + (4v)^2 = q^2$. Then there are odd positive integers a_1, a_2, a_3, even nonnegative integers b_1, b_2, b_3 and $k_1, k_2, k_3 \in \{0, 1, 2\}$ such that*

$$a_1^2 + (4b_1)^2 = n^2, \quad a_2^2 + (4b_2)^2 = n^2, \quad a_3^2 + (4b_3)^2 = n^2 \tag{3.1.1}$$

and

$$\left.\begin{aligned} \tfrac14 x_1 &= b_1 q, & y_1 &= a_1 q & &\text{if } k_1 = 0,\\ \tfrac14 x_1 &= |b_1 u - a_1 v|, & y_1 &= |a_1 u + 16 b_1 v| & &\text{if } k_1 = 1,\\ \tfrac14 x_1 &= |b_1 u + a_1 v|, & y_1 &= |a_1 u - 16 b_1 v| & &\text{if } k_1 = 2, \end{aligned}\right\} \tag{3.1.2}$$

$$\left.\begin{aligned} \tfrac14 x_2 &= b_2 q, & y_2 &= a_2 q & &\text{if } k_2 = 0,\\ \tfrac14 x_2 &= |b_2 u - a_2 v|, & y_2 &= |a_2 u + 16 b_2 v| & &\text{if } k_2 = 1,\\ \tfrac14 x_2 &= |b_2 u + a_2 v|, & y_2 &= |a_2 u - 16 b_2 v| & &\text{if } k_2 = 2, \end{aligned}\right\} \tag{3.1.3}$$

$$\left.\begin{aligned} \tfrac14 y_3 &= b_3 q, & x_3 &= a_3 q & &\text{if } k_3 = 0,\\ \tfrac14 y_3 &= |b_3 u - a_3 v|, & x_3 &= |a_3 u + 16 b_3 v| & &\text{if } k_3 = 1,\\ \tfrac14 y_3 &= |b_3 u + a_3 v|, & x_3 &= |a_3 u - 16 b_3 v| & &\text{if } k_3 = 2. \end{aligned}\right\} \tag{3.1.4}$$

Proof. We shall use Lemma 2.2. Since $x_1^2 + y_1^2 = n^2q^2$ and y_1 is odd, there are $a_1 > 0$, $b_1 \geq 0$, $U > 0$ and V such that

$$a_1^2 + (4b_1)^2 = n^2, \qquad U^2 + (4V)^2 = q^2$$

and x_1, y_1 satisfy the formulae analogous to (2.2.3). Since q is a prime we have for (U, V) three possibilities: $(q, 0)$, (u, v) and $(u, -v)$. They correspond to the three lines of (3.1.2).

The formulae (3.1.3) and (3.1.4) can be proved quite similarly. (Notice that for every $i \in \{1, 2, 3\}$ the even member of the pair (x_i, y_i) is written in the first place.)

THEOREM 3.2. *Let the parameters*

$$a_1, a_2, a_3, b_1, b_2, b_3, k_1, k_2, k_3, u, v \tag{3.2.1}$$

correspond to a primitive perfect rational cuboid in the sense of Theorem 3.1. *Denote for* $i = 1, 2, 3$

$$\left.\begin{array}{llll} \alpha_i = b_i^2, & \beta_i = 0, & \gamma_i = 16b_i^2 & \text{if } k_i = 0, \\ \alpha_i = b_i^2, & \beta_i = -a_ib_i, & \gamma_i = a_i^2 & \text{if } k_i = 1, \\ \alpha_i = b_i^2, & \beta_i = a_ib_i, & \gamma_i = a_i^2 & \text{if } k_i = 2 \end{array}\right\} \tag{3.2.2}$$

and

$$\alpha = \alpha_1 + \alpha_2 - \alpha_3, \quad \beta = \beta_1 + \beta_2 - \beta_3, \quad \gamma = \gamma_1 + \gamma_2 - \gamma_3. \tag{3.2.3}$$

Then there holds

$$\alpha \cdot u^2 + 2\beta \cdot uv + \gamma \cdot v^2 = 0. \tag{3.2.4}$$

Proof. We have

$$\left(\frac{1}{4}x_1\right)^2 + \left(\frac{1}{4}x_2\right)^2 - \left(\frac{1}{4}y_3\right)^2 = 0. \tag{3.2.5}$$

Then (3.2.4) can be obtained by a straightforward substitution from the formulae of Theorem 3.1.

The parameters α, β, γ can be rather large (approximately up to n^2, and β^2, $\alpha\gamma$ up to n^4) and therefore it is preferable to work only with their residues modulo suitable integers m. So we do also in the next theorem.

THEOREM 3.3. *Let the assumptions of Theorem 3.1 and Theorem 3.2 be fulfilled and let m be a positive integer. Then:*

(i) $\beta^2 - \alpha\gamma \equiv \square \pmod{m}$,

(ii) *if m is a power of an odd prime, $\beta^2 - \alpha\gamma \equiv \delta^2 \pmod{m}$ and* $\mathrm{GCD}(m, \delta) = 1$, *then*

$$(4\alpha)^2 + (\beta - \delta)^2 \equiv \square \pmod{m} \quad \text{or} \quad (4\alpha)^2 + (\beta + \delta)^2 \equiv \square \pmod{m},$$

(iii) *if $\alpha = 0$, then* $64\beta^2 + \gamma^2 \equiv \square \pmod{m}$,

(iv) *if $\gamma = 0$, then* $4\alpha^2 + \beta^2 \equiv \square \pmod{m}$,

(v) $\mathbf{ex}_2(\alpha) \geq \min(\mathbf{ex}_2(\beta) + 1, \mathbf{ex}_2(\gamma))$,

(vi) *if there are two zeros among α, β, γ, then the third integer is also zero.*

Proof. We may assume $\alpha \not\equiv 0 \pmod{m}$ and $\gamma \not\equiv 0 \pmod{m}$ in the statements (i) and (ii), $\gamma \not\equiv 0 \pmod{m}$ in (iii) and $\alpha \not\equiv 0 \pmod{m}$ in (iv). Otherwise these statements are obviously valid (and useless).

The equation (3.2.4) ought to have an integer solution (U, V) with both components distinct from 0. One such solution is an integer multiple of (u, v), $u^2 + 16v^2$ is a square, and therefore $U^2 + 16V^2$ is also a square. This suffices to obtain (iii) and (iv).

Further let $\alpha \neq 0$ and $\gamma \neq 0$. Then $v \mid \alpha$, and hence we may assume $V = \alpha$. So we obtain the quadratic equation

$$U^2 + 2\beta \cdot U + \alpha\gamma = 0 \tag{3.3.1}$$

for U from (3.2.4). Its discriminant $\beta^2 - \alpha\gamma$ must be a square, which implies (i). Now let the assumptions of (ii) are fulfilled. Then we have $U = -\beta \pm \delta$, and for at least one of these possibilities $U^2 + 16V^2$ must be a square, which gives the conclusion of (ii). (If m, δ are not relatively prime or m is not an odd prime power, then there could be more than two possibilities for $U \pmod{m}$.)

(v) If the inequality does not hold, let the equation (3.2.4) be cancelled by the maximal possible power of 2, and then considered modulo 2. Since u is odd we obtain a contradiction. (Notice that this condition is suitable when m is a power of 2 and $\alpha \not\equiv 0 \pmod{m}$.)

(vi) This is an easy consequence of (3.2.4) and $uv \neq 0$.

For a fixed n, any (primitive) perfect rational cuboid with the diagonal z, where $\frac{z}{n}$ is a prime, can be uniquely determined by the parameters

$$b_1, b_2, b_3, k_1, k_2, k_3, u, v \tag{3.4}$$

(the parameters a_1, a_2, a_3 can be computed). If only the first six parameters in (3.4) are given and we want to find the corresponding perfect rational cuboid, then we can solve the equation (3.2.4) to obtain u, v. However, to do this is unnecessary for some values of these six parameters. It can have two reasons:

a) The same cuboid corresponds also to another combination of values (for which (3.2.4) is solved); these cases are considered in Lemma 3.4.

b) It can be proved (without computing α, β, γ) that no (primitive) perfect rational cuboid corresponds to the given combination of values. These cases are considered in Lemma 3.5.

Maybe, much stronger such statements can be proved. In (iv) of Lemma 3.4 the symbol $\prec$ can be either the usual $<$ or any other linear ordering of the set $\{b \geq 0 \mid n^2 - (4b)^2 = \square\}$.

LEMMA 3.4. *Without loss of generality we may assume that the parameters* (3.4) *satisfy the conditions:*

(i) $k_3 \neq 2$,

(ii) *if* $b_3.k_3 = 0$, *then* $k_1 \neq 2$,

(iii) *if* $b_3 \cdot k_3 = 0$ *and* $b_1 \cdot k_1 = 0$, *then* $k_2 \neq 2$,

(iv) $b_1 \prec b_2$ *or* ($b_1 = b_2$ *and* $k_1 < k_2$).

Proof. If v in (3.4) is replaced by $-v$ and simultaneously every non-zero k_i, $i \in 1,2,3$ is replaced by $3 - k_i$, then the corresponding cuboid remains unchanged. (This is the reason why we did not assume $v > 0$.) If $b_i = 0$, then $k_i = 2$ and $k_i = 1$ gives the same x_i, y_i, hence $k_i = 1$ may be assumed. From these two observations we obtain (i), (ii) and (iii). If (iv) does not hold then we interchange b_1, k_1 with b_2, k_2; then the edges x_1, x_2 will be interchanged, which is not substantial. So we obtain (iv) with $\leq$ instead of $<$; however, the equality is impossible by Lemma 3.5, (v).

LEMMA 3.5. *If there is a primitive perfect rational cuboid with the body diagonal* $z = nq$, q *a prime, then the corresponding parameters* (3.4) *satisfy the following conditions:*

(i) *The integers* $\mathrm{GCD}(n, b_1)$, $\mathrm{GCD}(n, b_2)$, $\mathrm{GCD}(n, b_3)$ *are pairwise relatively prime,*

(ii) $b_1 + k_1 > 0$, $b_2 + k_2 > 0$, $b_3 + k_3 > 0$,

(iii) *there is at most one zero among* b_1, b_2, b_3 *and at most one zero among* k_1, k_2, k_3,

(iv) *if* $k_1 k_2 k_3 \neq 0$, *then* $2 \mid (b_3 + b_1)$ *or* $2 \mid (b_3 + b_2)$; *if* $k_1 k_2 k_3 = 0$, *then* $2 \mid (b_1 + b_2 + b_3)$,

(v) *the pairs* (k_1, b_1), (k_2, b_2), (k_3, b_3) *are pairwise distinct,*

(vi) $b_3 \neq 0$ *or* $b_1 \neq b_2$,

(vii) $b_2 \neq b_3$ *or* $b_1 \neq 0$.

(viii) $b_1 \neq b_2$ *or* $b_1 \neq b_3$ *or* $b_2 \neq b_3$,

(ix) n *is not prime and* $n \neq 1$.

Proof. (i) If $p \mid n$ and $p \mid b_i$ for a prime p, then also $p \mid a_i$ and then $p \mid x_i$. Hence if p divides n and two of b_1, b_2, b_3, then p divides two of the edges x_1, x_2, x_3. However, since $p \mid z$ the prime p divides also the third edge, which is a contradiction.

(ii) If $b_i = k_i = 0$, then $x_i = 0$ (for $i = 1,2$) or $y_3 = 0$ (for $i = 3$), which is a contradiction.

(iii) If $k_i = 0$, then $q \mid x_i$; further, $q \mid z$. If there are two zeros among k_1, k_2, k_3, then q divides z and two edges, and we can continue as in (i).

(iv) The equation (3.2.5) implies that $\frac{1}{4}x_1 + \frac{1}{4}x_2 + \frac{1}{4}y_3$ is even and at least one of $\frac{1}{4}x_1 + \frac{1}{4}y_3$, $\frac{1}{4}x_2 + \frac{1}{4}y_3$ is even. If $k_1k_2k_3 \neq 0$, we have

$$\frac{1}{4}x_1 \equiv b_2 + v \pmod 2, \qquad \frac{1}{4}x_2 \equiv b_2 + v \pmod 2,$$
$$\frac{1}{4}y_3 \equiv b_3 + v \pmod 2$$

and hence

$$b_1 + b_3 \equiv \frac{1}{4}x_1 + \frac{1}{4}y_3 \pmod 2, \qquad b_2 + b_3 \equiv \frac{1}{4}x_2 + \frac{1}{4}y_3 \pmod 2.$$

If, for example, $k_1 = 0$, then $k_2k_3 \neq 0$ and

$$\frac{1}{4}x_1 \equiv b_1 \pmod 2, \quad \frac{1}{4}x_2 \equiv b_2 + v \pmod 2, \quad \frac{1}{4}y_3 \equiv b_3 + v \pmod 2,$$
$$b_1 + b_2 + b_3 \equiv \frac{1}{4}x_1 + \frac{1}{4}x_2 - v + \frac{1}{4}y_3 - v \equiv 0 \pmod 2.$$

The cases $k_2 = 0$, $k_3 = 0$ can be considered in the same way.

(v) Otherwise we have $x_1 = x_2$ or $x_1 = y_3$ or $x_2 = y_3$ and then $y_3 = x_1\sqrt{2}$ or $x_2 = 0$ or $x_1 = 0$, respectively, which is a contradiction.

(vi) If $b_3 = 0$ and $b_1 = b_2$, then $a_3 = n = a^2 + 16b^2$, $a_1 = a_2 = a$, $b_1 = b_2 = b$ for some a, b. Then

$$\alpha = \alpha_1 + \alpha_2 - \alpha_3 = b^2 + b^2 - 0^2 = 2b^2.$$

Further, by Lemma 3.5 we may assume $k_1 < k_2$, and for $k_1 = 0$ we may assume $k_2 \neq 2$. Therefore two cases remain.

1. If $k_1 = 0$, $k_2 = 1$, we have

$$\beta = \beta_1 + \beta_2 - \beta_3 = 0 - ab - 0 = -ab,$$
$$\gamma = \gamma_1 + \gamma_2 - \gamma_3 = 16b^2 + a^2 - n^2 = 0.$$

The equation (3.2.4) gives $2b^2u^2 - 2abuv = 0$, and hence $bu - av = 0$. Then $x_2 = 0$, which is a contradiction.

2. If $k_1 = 1$, $k_2 = 2$, we have

$$\beta = \beta_1 + \beta_2 - \beta_3 = -ab + ab - 0 = 0,$$
$$\gamma = \gamma_1 + \gamma_2 - \gamma_3 = a^2 + a^2 - n^2 = a^2 - 16b^2.$$

Then (3.2.4) gives $2b^2u^2 = (16b^2 - a^2).v^2$, hence $2 \mid (16b^2 - a^2)$, which is a contradiction.

(vii) Let, conversely, $b_2 = b_3 = b$ and $b_1 = 0$. Then $a_1 = n$ and $a_2 = a_3 = a$, where $a^2 + 16b^2 = n^2$. We have

$$\alpha = \alpha_1 + \alpha_2 - \alpha_3 = 0 + b^2 - b^2 = 0.$$

By (ii) we have $k_1 \neq 0$ and by (v) $k_2 \neq k_3$. If we also pay attention to Lemma 3.4, then three cases remain.

1. If $k_3 = 0$, then $k_3 = 1$ may be assumed and we have

$$\beta = \beta_1 + \beta_2 - \beta_3 = 0 - ab - 0 = -ab,$$
$$\gamma = \gamma_1 + \gamma_2 - \gamma_3 = a^2 + n^2 - 16b^2 = 2a^2.$$

Then by (3.2.4) we have $-abuv + a^2v^2 = 0$, hence $bu = av$, and then $x_2 = 0$, which is a contradiction.

2. If $k_3 = 1$, $k_2 = 0$, then

$$\beta = \beta_1 + \beta_2 - \beta_3 = 0 + 0 - (-ab) = ab,$$
$$\gamma = \gamma_1 + \gamma_2 - \gamma_3 = n^2 + 16b^2 - a^2 = 32b^2.$$

Then by (3.2.4) we have $2abuv + 32b^2v^2 = 0$, hence $au + 16bv = 0$, which is a contradiction because a, u are odd.

3. If $k_3 = 1$, $k_2 = 2$, then

$$\beta = \beta_1 + \beta_2 - \beta_3 = 0 + ab - (-ab) = 2ab,$$
$$\gamma = \gamma_1 + \gamma_2 - \gamma_3 = a^2 + n^2 - a^2 = n^2 = a^2 + 16b^2.$$

Then by (3.2.4) we have $4abu + (a^2 + 16b^2)v = 0$, and hence $tu = a^2 + 16b^2$, $tv = -4ab$ for some integer t. Therefore

$$\begin{aligned}(tq)^2 &= t^2u^2 + 16t^2v^2 = (a^2 + 16b^2)^2 + 256a^2b^2 \\ &= a^4 + 288a^2b^2 + 256b^4 = a^4 + 18a^2.(4b)^2 + (4b)^4,\end{aligned}$$

which contradicts Theorem 2.4.

(viii) Let $b_1 = b_2 = b_3 = b$ and $a_1 = a_2 = a_3 = a$. Then

$$\alpha = \alpha_1 + \alpha_2 - \alpha_3 = b^2 + b^2 - b^2 = b^2.$$

By (v) the integers k_1, k_2, k_3 must be pairwise distinct and by Lemma 3.4 we may assume $k_3 \in \{0, 1\}$, $k_1 < k_2$. So two cases remain.

1. If $k_1 = 0$, $k_3 = 1$, then

$$\beta = \beta_1 + \beta_2 - \beta_3 = 0 + ab - (-ab) = 2ab,$$
$$\gamma = \gamma_1 + \gamma_2 - \gamma_3 = 16b^2 + a^2 - a^2 = n^2 = 16b^2.$$

Then by Theorem 3.3, (i) we have

$$\beta^2 - \alpha\gamma = 4a^2b^2 - b^2 \cdot 16b^2 = 4b^2 \cdot (a^2 - 4b^2) = \square.$$

Hence $a^2 - 4b^2 = \square$. Denote $t = \mathrm{GCD}(a, b)$. Then by a well-known expression of sides of Pythagorean triangles we have $\frac{a}{t} = r^2 + s^2$, $\frac{2b}{t} = 2rs$ for some nonzero integers r, s. Then we have

$$\left(\frac{n}{t}\right)^2 = \left(\frac{a}{t}\right)^2 + \left(\frac{4b}{t}\right)^2 = \left(r^2 + s^2\right)^2 + (4rs)^2 = r^4 + 18r^2s^2 + s^4,$$

which contradicts Theorem 2.4.

2. If $k_1 = 1$ and $k_3 = 0$, then

$$\beta = \beta_1 + \beta_2 - \beta_3 = -ab + ab - 0 = 0,$$
$$\gamma = \gamma_1 + \gamma_2 - \gamma_3 = a^2 + a^2 - 16b^2 = 2a^2 - 16b^2.$$

Then we have

$$\beta^2 - \alpha\gamma = 0 - b^2 \cdot (2a^2 - 16b^2) = 2b^2 \cdot (8b^2 - a^2) \neq \square$$

because $8b^2 - a^2$ is odd and $b \neq 0$. This is a contradiction with Theorem 3.3, (i).

(ix) If n is a prime, then the equation $n^2 = a^2 + 16b^2$ has only one solution in positive integers (and if $n = 1$ it has no such solution). However, by (vi) - (viii) at least two such solutions are necessary that the mentioned perfect rational cuboid could exist.

4. Remarks to the first computation

The program was written in the language TURBO PASCAL v. 5.5 and run on PC AT. In every run, all integers n from an interval $[n_1, n_2]$ are considered and at the end input data for the next run are prepared.

After the start, several tables are computed. They later help in fast distinguishing quadratic residues and non-residues, in computing square roots modulo several integers, etc. The computation time of this stage is very short.

Whenever necessary, a portion of suitable n is prepared by a sieve method. It starts with all $n \equiv 1 \pmod 4$ from a suitable subinterval $[a, b]$ of the interval $[n_1, n_2]$. Then for every prime $p \equiv 3 \pmod 4$, $p \le \sqrt{b}$, all multiples of p are excluded. This is done also for some composite p because it is faster than testing primality. Then only n whose prime divisors are all $\equiv 1 \pmod 4$ remain, and they are considered in the further computation in the usual order.

Now let a suitable n be fixed. At first it is factorized, by the classical method, but only primes $\equiv 1 \pmod 4$ are treated. If n is prime, it is immediately excluded. Otherwise the list

$$(A_0, B_0), (A_1, B_1), \dots, (A_t, B_t), \tag{4.1}$$

$(A_0, B_0) = (n, 0)$, of all nonnegative integer solutions (a, b) of the equation $a^2 + (4b)^2 = n^2$ is computed by a method based on Lemma 2.2 and Lemma 2.3.

Then the main (and the most time consuming) part starts, which consists of three nested loops. The outer loop is controlled by (b_3, k_3), the middle loop by (b_1, k_1) and the inner loop by (b_2, k_2). However, b_3, b_1, b_2 are not immediately used as control variables. Instead, three integer variables j_3, j_1, j_2 are used so that $(a_i, b_i) = (A_{j_i}, B_{j_i})$. Notice that $b_i = 0$ if and only if $j_i = 0$.

Whenever possible, pre-computations are made outside the loops. For example, the condition (i) of Lemma 3.4 is used as follows. To every B_j the set $P(j)$ of all prime divisors of $\mathrm{GCD}(n, B_j)$ is prepared, as a subset of the set of all prime divisors of n (technically, $P(j)$ is an integer). In the middle loop the condition $P(j_3) \cap P(j_1) = \emptyset$ is tested; only when it is fulfilled the inner loop is performed. In these cases $Q = P(j_3) \cup P(j_1)$ is pre-computed, and $Q \cap P(j_2) = \emptyset$ is tested in the inner loop.

The main idea of the program is to consider all possible values of the parameters a_i, b_i, k_i, $i = 1, 2, 3$ for a given n, and for every of them prove that no suitable u, v exist. This is done by a sequence of conditions which must be fulfilled by the parameters. They are continually checked, and whenever one of them is not satisfied, the considered combination is excluded (and further conditions are not tested for it). Of course, groups of several combinations are excluded together in one step when possible. (It would be a surprise if some values pass all tests. It can mean either that a perfect rational cuboid is found or, more probably, that the tests are not sufficient. However, this case did not happen.) The program computes some statistics of tests used; the statistics obtained in program testing were used to optimalize the order of the tests.

The conditions of Lemma 3.4 and Lemma 3.5 are not very strong. However, they exclude together more than 70% of the possible cases and make the computation substantially faster, because they are used in the first place, or even in the loop control. So the stronger (but computationally harder) conditions of Theorem 3.3 are applied to a substantially smaller number of cases.

The main tool are the tests based on the conditions (i), (ii) of Theorem 3.3. The condition (i) is used for $m = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 15015$ and $m = 2^{14} = 16384$. When the combination of parameters is not excluded, (i) and (ii) are used for some pairs (m_1, m_2) of prime powers; twenty pairs are prepared but usually only cca 10 is used. These tests seem to be independent and every of them excludes more than 50% of its inputs.

It seems that the conditions (iii) and (iv) can be applied only very rarely (maybe, never, but it is not proved). They were included because they consider the cases when (i), (ii) do not work. Notice that $\alpha \equiv 0 \pmod{m}$ does not imply $\alpha = 0$. Therefore in these cases we must check the condition $\alpha \equiv 0 \pmod{m}$ also for several further moduli m; if they are pairwise relatively prime we need that their product exceeds a bound for $|\alpha|$. In some special cases $\alpha = 0$ or $\gamma = 0$ can be verified immediately.

The computation time for $n_2 - n_1 = 50000$ varied between 10–50 minutes; in the average, it increased with n but not monotonically. By the computation at the Mathematical Institute SAV Bratislava, the bound $16 \cdot 10^5$ was reached. The bound 11.10^6 was reached during the author's stay at The university of Turku in May–June 1991; the computation time was approximately 88 hours; here much larger portions of n were considered in one computation. A summary of one of them is given in Figure 1. In the computation values of n between 1 and 3085925 were considered. For $nCount = 260896$ of them the list (4.1) was computed. Figure 1 also shows the moduli used in the computation, the number of calls of various tests, and the numbers of cases which were excluded by them. The exact meaning of all these numbers cannot be explained without a more detailed description of the computer program. However, even without these details the strength of the tests can be seen from the speed how these numbers decrease.

```
=======================================================================
 25.5.1991, outname='A_1A.BBB',  Time: 16h50m34.8s -- 10h21m 4.5s,
 INPUT:  nStX=1  nIntX=100000000  MultBy=1
         compNumber=5  writeperc=20  wrDetail=-90 wrDFrom=-1 wrDInt=-30
 nStart=1, nFinish=100000001, actBoundPr<=10000
-----------------------------------------------------------------------
 n  from 1 .. 100000001;     * * INTERRUPTED  after  n=3085925
 nCount=260896  All n excluded in  63029.7s.
  cnty3x1excl=24529051  cnty3x1cont=37964021  allx2cases=728963303
  cntCommPr=123813800+71467911  cntkbexcl=154132734+48994785+8661297

modulus= | use:  Uall    UmxxF | quest:  QA         QB      Qa0    Qg0
mdl1*mdl2|     remain          | excl:   EA         EB      Ea0    Eg0
--------------------------------------------------------------------
 15015   | 321892776 1240721 |  319823302          0        0      0
         |  99319067         |  222573709          0        0      0
         |                   |
 16384   |  99319067 1240721 |   95292451   22984760        0      0
         |  48301772         |   47130175    3887120        0      0
         |                   |
 26071 = |  48301772 1207285 |   48269178   25592223        0      0
 841* 31 |   7299199         |   31895756    9106817        0      0
         |                   |
 28037 = |   7299199 1114321 |    7293783    3228203        0      0
 529* 53 |   1035728         |    5183880    1079591        0      0
         |                   |
 29963 = |   1035728  786310 |    1034985     575412        0      0
 361* 83 |    212483         |     702088     121157        0      0
.....................................................................
 29767 = |    212483  370902 |     212336      91982        0      0
 289*103 |     28909         |     151924      31650        0      0
         |                   |
 29237 = |     28909   77746 |      28885      13219        0      0
 169*173 |      4516         |      20642       3751        0      0
         |                   |
 29893 = |      4516   13153 |       4515       2096        0      0
 179*167 |       676         |       3310        530        0      0
         |                   |
 29503 = |       676    2003 |        676        321        0      0
 181*163 |       105         |        491         80        0      0
         |                   |
 29987 = |       105     312 |        104         59        0      0
 191*157 |        26         |         72          7        0      0
         |                   |
 29143 = |        26      78 |         26          8        0      0
 193*151 |         2         |         21          3        0      0
         |                   |
 29353 = |         2       6 |          2          2        0      0
 197*149 |         0         |          1          1        0      0
         |                   |
=======================================================================
```

Figure 1.

5. The second computation.

This computation was simpler (and faster) than the first one, and its theoretical background is also simpler. Besides the results and notation of Section 2, the program was based on the first part of the next theorem.

THEOREM 5.1. *The body diagonal of any perfect rational cuboid is neither a prime power nor a product of two primes.*

P r o o f . We may consider a primitive perfect rational cuboid. If z is a power of a prime p, then there is at most one x not divisible by p such that $z^2 - 16x^2$ is a square. Therefore at least two edges are multiples of p; since $p \mid z$ the third edge is also divisible by p, which is a contradiction. The second statement is an immediate consequence of Lemma 3.5, (ix).

In every run of the program several tables are precomputed. (This part is so fast that it is unnecessary to read tables from a disc file.) One of them concerns primes $\equiv 1 \pmod 4$ and their representations as sums of squares. Another depends on two moduli M, m, which are given in the input data. The modulus M is chosen so that there are many quadratic residues modulo M (usually a prime near to 10000), and only an array of zeros is prepared for it. The modulus m is a product of several primes of the form $4k+3$, hence it is relatively prime with any z which will be considered, and $z^{-1} \pmod m$ exists. For this m, tables concerning the sets

$$Q_m = \{r \mid 0 \le r < m \text{ and } r \equiv \square \pmod m \text{ and } 1 - 16r \equiv \square \pmod m\},$$
$$T_m = \{(i_1, j_1, k_1) \in Q_m \times Q_m \times Q_m \mid i_1 \equiv j_1 + k_1 \pmod m\};$$

are computed; the elements of T_m are sorted with respect to the first component. The role of M, m, Q_m and T_m is explained below.
Then all z from an interval $[z_1, z_2]$ are considered; for some technical reasons, $z_2 < 13z_1$ is assumed. A recursive procedure **P** is used which produces all suitable z from the above mentioned interval; "suitable" means that all prime divisors of z are of the form $4k+1$ and are so small that z is not excluded by the first computation. Roughly speaking, at each depth of calls a new prime divisor of z (with a positive exponent) is joined. This fact also determines the order in which z arise. The depth of recursion, at which an integer z is given, is equal to the number of distinct prime divisors of z. Similarly as n in the first computation, the values of z are continually excluded, i. e. it is proved that they cannot be the body diagonals of any perfect rational cuboid.
For every suitable z, the list

$$b_1, b_2, \ldots, b_s \tag{5.1}$$

of all positive integers x satisfying $z^2 - 16x^2 = \square$ is constructed. The method is similar as in the first computation, but it is not necessary to factorize z for this purpose; the procedure **P** computes an analogous list for some factors of z. (**P** could easily give also the factorization of z, but it is unnecessary.) Further for every b_i from (5.1) $R_i = b_i^2 \text{ MOD } M$ is computed. The integers (5.1) are candidates for the quarters of the even edges and even face diagonals. Let us imagine

$$\frac{1}{4}y_3 = b_i, \qquad \frac{1}{4}x_1 = b_j, \qquad \frac{1}{4}x_2 = b_k.$$

If we prove that there are no $i, j, k \in \{1, 2, \ldots, s\}$ such that

$$b_j^2 + b_k^2 = b_i^2, \tag{5.2}$$

then z will be excluded. A straightforward algorithm would check (5.2) for $\frac{1}{2}s(s-1)(s-2)$ triples (i, j, k). To diminish this number, we continue as follows. Let for every $r \in Q_m$ the set

$$E(r) = \big\{ i \in \{1, \ldots, s\} \mid (b_i z^{-1})^2 \equiv r \pmod{m} \big\}.$$

be computed. The nonempty sets among $E(r)$, $r \in Q_m$, form a partition of the set $\{1, \ldots, s\}$. Now assume $i \in E(i_1)$, $j \in E(j_1)$ and $k \in E(k_1)$. Then (5.2) is possible only if $i \in E(i_1)$, where $i_1 = (j_1 + k_1) \text{ MOD } m$, i.e. $(i_1, j_1, k_1) \in T_m$; otherwise (i, j, k) need not be considered.
The modulus M and the rests R_i are used as follows. For every integer R, $0 \le R < 2M$ define the set

$$D(i_1, R) = \big\{ i \in E(i_1) \mid R_i \equiv R \pmod{M} \big\}$$

(of course, $D(i_1, R) = D(i_1, R - M)$ for every $R \ge M$, but this approach simplifies the condition which will be verified). Now assume $(i_1, j_1, k_1) \in T_m$ and $j \in E(j_1)$, $k \in E(k_1)$. Then (5.2) can hold only if $i \in D(i_1, R_j + R_k)$. However, the sets $D(i_1, R)$ are very often empty, and therefore for most pairs (j, k) (more than 99%) no i remains. For the remaining i, (5.2) is checked modulo 20000 and several consecutive integers; practically, all i were excluded after 20002. (After 10 moduli, an information about a non-excluded case would be printed. This never happened.)
The number of considered pairs (j, k) could be also diminished by the observation that (5.2) implies $|ex_2(b_j) - ex_2(b_k)| \ge 2$. Since we can interchange j, k, we may assume $ex_2(b_k) \ge ex_2(b_j) + 2$, and this condition was used in the program.

```
==========================================================================
 15.11.1991, outname='D:C_5000E6.C',  Time:  9h56m18.5s --  9h58m 3.5s,
 INPUT:  zMinX=5000000  zIntX=2000000  nBndX=11000  MultBy=1000
         comp_number=2  writeperc=20  mdlDg=-9997  mdlPt=33
 zMin=5000000000, zMax=7000000000, nBound=11000000, actBoundPr<=637
--------------------------------------------------------------------------
 mDiag=9973 mPart=33.  All z excluded in  105.0s.
zCount=1575  cntNotExcl=0  cntErrors=0
cntEdges=202500  cntMainCond=2793333  cntSetipntr=84829  cntLastCh=17745+43
==========================================================================
 15.11.1991, outname='D:C_7000E6.C',  Time: 10h 1m54.0s -- 10h 3m21.7s,
 INPUT:  zMinX=7000000  zIntX=1589900  nBndX=11000  MultBy=1000
         comp_number=2  writeperc=20  mdlDg=-9997  mdlPt=33
 zMin=7000000000, zMax=8589900000, nBound=11000000, actBoundPr<=782
--------------------------------------------------------------------------
 mDiag=9973 mPart=33.  All z excluded in  87.7s.
zCount=1292  cntNotExcl=0  cntErrors=0
cntEdges=163830  cntMainCond=2361263  cntSetipntr=68651  cntLastCh=16079+84
==========================================================================
 15.11.1991, outname='D:C_1000E6.C',  Time: 10h 7m47.0s -- 10h 9m22.3s,
 INPUT:  zMinX=1000000  zIntX=2000000  nBndX=11000  MultBy=1000
         comp_number=2  writeperc=20  mdlDg=-9997  mdlPt=33
 zMin=1000000000, zMax=3000000000, nBound=11000000, actBoundPr<=274
--------------------------------------------------------------------------
 mDiag=9973 mPart=33.  All z excluded in  95.3s.
zCount=1491  cntNotExcl=0  cntErrors=0
cntEdges=194254  cntMainCond=2340352  cntSetipntr=81456  cntLastCh=12865+27
==========================================================================
 15.11.1991, outname='D:C_1000E6.C',  Time: 10h23m 9.8s -- 10h30m29.3s,
 INPUT:  zMinX=1000000  zIntX=2000000  nBndX=1600  MultBy=1000
         comp_number=2  writeperc=20  mdlDg=-9997  mdlPt=33
 zMin=1000000000, zMax=3000000000, nBound=1600000, actBoundPr<=1876
--------------------------------------------------------------------------
 mDiag=9973 mPart=33.  All z excluded in  439.5s.
zCount=10696  cntNotExcl=0  cntErrors=0
cntEdges=752013  cntMainCond=6375666  cntSetipntr=310862  cntLastCh=26814+46
==========================================================================
 15.11.1991, outname='D:C_100E6.CC',  Time: 10h32m29.6s -- 10h32m58.1s,
 INPUT:  zMinX=100000  zIntX=900000  nBndX=11000  MultBy=1000
         comp_number=2  writeperc=20  mdlDg=-9997  mdlPt=33
 zMin=100000000, zMax=1000000000, nBound=11000000, actBoundPr<=92
--------------------------------------------------------------------------
 mDiag=9973 mPart=33.  All z excluded in  28.5s.
zCount=537  cntNotExcl=0  cntErrors=0
cntEdges=57377  cntMainCond=453403  cntSetipntr=23982  cntLastCh=1676+7
==========================================================================
 15.11.1991, outname='D:C_100E6.CC',  Time: 10h34m 8.2s -- 10h37m18.4s,
 INPUT:  zMinX=100000  zIntX=900000  nBndX=1600  MultBy=1000
         comp_number=2  writeperc=20  mdlDg=-9997  mdlPt=33
 zMin=100000000, zMax=1000000000, nBound=1600000, actBoundPr<=626
--------------------------------------------------------------------------
 mDiag=9973 mPart=33.  All z excluded in  190.2s.
zCount=4534  cntNotExcl=0  cntErrors=0
cntEdges=351470  cntMainCond=2365950  cntSetipntr=146352  cntLastCh=7586+16
==========================================================================
```

Figure 2.

Notice that for representing the sets $E(r)$, sorting these sets with respect to cx_2 and other purposes, some integers were used as "pointers". The sets $D(i_1, R)$ were initialized in the pre-computation as empty sets, and for every z, i_1 only nonempty of them are prepared (and after using, made empty again). This approach seems to be advantageous because usually $s << M$.

It is little surprising, that the limiting factor was not the time of computation but the size of long integers in TURBO PASCAL. Originally, the computation approximately up to 10^8 was planned, but the bound 10^9 was reached in less than 15 minutes of computation. Therefore the original program was slightly modified so that it works till $\frac{z}{4}$ does not exceed the bound for long integers. (A much more substantial modification would be necessary to obtain still higher lower bounds. The values contained in (ii), (iii) of Theorem 1 are diminished to the integer multiples of 10^9.)

Figure 2 contains a summary of some computations by the modified program. The intervals of z are sometimes overlapping, and two different lower bounds for n are used ($nBound = 16 \cdot 10^5$ and $nBound = 11 \cdot 10^6$). The numbers of considered cases ($zCount$ is the number of considered z and $cntEdges$ the total number of considered potential even edges), as well as the numbers of test calls are substantially smaller than those in Figure 1, which explains why the second computation was much faster than the first one.

REFERENCES

[1] KOREC, I.: *Nonexistence of a small perfect rational cuboid II*, Acta Math. Univ. Comen. **XLIV–XLV** (1984), 39-48.

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

[3] MORDELL, L. J.: *Diophantine equations*, Academic Press, London and New York, 1969.

[4] POCKLINGTON, H. C.: *Some Diophantine impossibilities*, Proc. Cambridge Philosophical Society **17** (1914), 108-121.

Received December 16, 1991

Matematický ústav SAV
Štefánikova 49
814 73 Bratislava
Czecho-Slovakia