Werk

Label: Article

Jahr: 1984

PURL: https://resolver.sub.uni-goettingen.de/purl?312901348_44-45|log10

UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
XLIV—XLV—1984

NONEXISTENCE OF A SMALL PERFECT RATIONAL CUBOID, II.

IVAN KOREC, Bratislava

1. Introduction

There several attempts have been to find a perfect rational cuboid, i. e. a rectangular parallelepiped of which the legths of the edges, the face diagonals and the body diagonal are integers. These attemps are discussed in [3]. Up to now, none of these attemps was succesful; related positive results can be found in [3], a bit also in [2]. It was proved in [2] that there is no perfect rational cuboid with the least edge less than 10000. This bound is enlarged to one million here. In both cases computer computations were used, and the result of the present paper substantially depends on that of [2]. Analogously as in [2], we shall not give details of the computer program. We shall more concentrate on the number-theoretical background of the program, and we give also some results which are not immediately used in it.

2. Notation and previous results

Most of our general notation is commonly used, and it is the same as in [2]. We only notice that $\mathrm{ex}(p, n)$ denotes the greatest integer k such that $p^k \mid n$. Special notation also coincides with that of [2], and it will be repeated below together with some results of [2].

In what follows let x, y, z always denote (the lengths of) the edges of a primitive perfect rational cuboid, i. e. positive integers such that

$$\sqrt{(x^2+y^2)},\ \sqrt{(x^2+z^2)},\ \sqrt{(y^2+z^2)},\ \sqrt{(x^2+y^2+z^2)} \tag{2.1}$$

are also integers, and

$$D(x, y, z)=1. \tag{2.2}$$

We shall also assume that $y<z$, and denote $t=\sqrt{(y^2+z^2)}$ so that

$$y<z<t. \tag{2.3}$$

There are positive integers a, b, c such that

$$y=\frac{1}{2}\left(\frac{x^2}{a}-a\right), \quad z=\frac{1}{2}\left(\frac{x^2}{b}-b\right), \quad t=\frac{1}{2}\left(\frac{x^2}{c}-c\right). \tag{2.4}$$

The integers a, b, c satisfy

$$a\,|\,x^2, \quad b\,|\,x^2, \quad c\,|\,x^2 \tag{2.5}$$

and

$$x>a>b>c. \tag{2.6}$$

Substituting (2.4) into the equality $y^2+z^2=t^2$ we can obtain the equation

$$(a^2c^2+b^2c^2-a^2b^2)x^4-2a^2b^2c^2x^2+a^2b^2c^2(a^2+b^2-c^2)=0. \tag{2.7}$$

If we solve this equation (with respect to x^2 and then to x), we prove that there are positive integers d, v such that

$$d^2=(a^2+b^2)(a^2-c^2)(b^2-c^2) \tag{2.8}$$

$$v^2=abc(abc-d)(a^2+b^2-c^2). \tag{2.9}$$

Further, we can obtain the inequality

$$a^2c^2+b^2c^2>a^2b^2. \tag{2.10}$$

The inequalities (2.6) and (2.10) imply

$$a<\frac{bc}{\sqrt{(b^2-c^2)}}, \quad b<c\sqrt{2}, \quad a^2<c^3. \tag{2.11}$$

If we also assume that x is the least edge, it holds also

$$x>(\sqrt{2}+\sqrt{3})\cdot c. \tag{2.12}$$

Notice that we must not assume $D(a, b, c)=1$; it was possible in [2] because only conditions not containing x were considered. The result of the computer computation referred in [2] can be given in the form

$$c\geqq 3200\cdot \mathrm{D}(a, b, c). \tag{2.13}$$

Together with (2.12) the estimation $x\geqq 10000$ was obtained.

3. Conditions on x, a, b, c

In the theorems of this part we shall implicitely use everything from Part 2 except (2.12) and (2.13). The last two conditions will be mentioned explicitely if they are necessary. Most of theorems proved here were used in the computer computation.

3.1. Theorem. a) For every odd prime p, the integers $\mathrm{ex}(p, a)$, $\mathrm{ex}(p, b)$, $\mathrm{ex}(p, c)$ belong to the interval $[0, 2 \cdot \mathrm{ex}(p, x)]$, and at most one of them belongs to the interval $[1, 2 \cdot \mathrm{ex}(p, x) - 1]$.

b) If x is even then $\mathrm{ex}(2, x) \geqq 2$. Further, the integers ex(2, a), ex(2, b), ex(2, c) belong to the interval $[1, 2 \cdot \mathrm{ex}(2, x) - 1]$, and at most one of them belongs to the interval $[2, 2 \cdot \mathrm{ex}(2, x) - 2]$.

Proof. Consider odd prime p at first. If $\mathrm{ex}(p, x) = 0$ then (2.5) obviously implies $\mathrm{ex}(p, a) = \mathrm{ex}(p, b) = \mathrm{ex}(p, c) = 0$. Otherwise (2.5) implies $\mathrm{ex}(p, a) \leqq 2 \cdot \mathrm{ex}(p, x)$, and analogously for b, c. If $\mathrm{ex}(p, a)$, $\mathrm{ex}(p, b)$ or $\mathrm{ex}(p, c)$ belongs to $[1, 2 \cdot \mathrm{ex}(p, x) - 1]$ then y, z, or t is divisible by p, respectively. However, if two of these numbers are multiplies of p then so is the third. Hence $p \mid \mathrm{D}(x, y, z)$, which contradicts (2.2).

Now let x be even. Since y is an integer (2.4) implies $1 \leqq \mathrm{ex}(2, a) \leqq 2 \cdot \mathrm{ex}(2, x) - 1$, and analogously for b, c. If ex(2, a), ex(2, b), or ex(2, c) belongs to $[2, 2 \cdot \mathrm{ex}(2, \mathrm{x}) - 2]$ then y, z, or t is even, respectively. However, if two of y, z, t are even then so is the third. Therefore $\mathrm{D}(x, y, z)$ is even, which contradicts (2.2). The inequality $\mathrm{ex}(2, x) \geqq 2$, i.e. $4 \mid x$, follows from the fact that x^2 is the difference of two odd squares, $x^2 + t^2$ and t^2.

3.2. Theorem. a) If $p \equiv 3 \pmod 4$ is a prime then

$$\mathrm{ex}(p, c) = 0 \text{ or } \mathrm{ex}(p, c) = 2 \cdot \mathrm{ex}(p, x).$$

b) If x is even then

$$\mathrm{ex}(2, c) = 1 \text{ or } \mathrm{ex}(2, \mathrm{c}) = 2 \cdot \mathrm{ex}(2, x) - 1.$$

Proof. For an odd prime p theorem 3.1 implies $\mathrm{ex}(p, c) \leqq 2 \cdot \mathrm{ex}(p, x)$. Now if $0 < \mathrm{ex}(p, c) < 2 \cdot \mathrm{ex}(p, x)$ then (2.4) implies $p \mid (y^2 + z^2)$. Since $p \equiv 3 \pmod 4$ we obtain $p \mid y$, $p \mid z$, and hence $p \mid \mathrm{D}(x, y, z)$, which contradicts (2.2).

Analogously, for x even theorem 3.1 implies $1 \leqq \mathrm{ex}(2, c) \leqq 2 \cdot \mathrm{ex}(2, x) - 1$. If $1 < \mathrm{ex}(2, c) < 2 \cdot \mathrm{ex}(2, x) - 1$ then (2.3) implies $2 \mid (y^2 + z^2)$. Since $y^2 + z^2$ is a square the numbers y, z must be even, which contradicts $\mathrm{D}(x, y, z) = 1$.

3.3. Theorem. Let $x = p^m \cdot q^n$ for some odd primes p, q and nonnegative integers m, n. Then $p \neq q$, $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, $m \geqq 2$, $n \geqq 2$ and $m + n \geqq 5$.

Proof. If $p = q$ (or $m = 0$ or $n = 0$) then x is a prime power, and the inequality (2.11) cannot be fulfilled by any (pairwise different) powers of a prime. Hence $p \neq$

(and $m \neq 0$ and $n \neq 0$). We may assume $p^m < q^n$. Since the set $A = \{a, b, c\}$ consists of some divisors of x^2 greater than 1 and smaller than x, we have

$$A \subseteq \{p^u;\ 1 \leqq u \leqq 2m-1\} \cup \{p^{2m}\} \cup \{q^v;\ 1 \leqq v \leqq 2n-1\} \cup$$

$$\cup \{p^u q^v;\ 1 \leqq u \leqq 2m-1,\ 1 \leqq v \leqq 2n-1\} \cup \{p^{2m} q^v;\ 1 \leqq v \leqq 2n-1\}.$$

Further in this proof we always assume $1 \leqq u \leqq 2m-1$, $1 \leqq v \leqq 2n-1$.

If A contains an element of the form $p^u q^v$ then by theorem 3.1 the set A cannot contain any element q^v, p^u or $p^{2m} q^v$. It may contain p^{2m} but the third suitable element does not exist. Therefore A does not contain any element $p^u q^v$.

If A contains an element of the form $p^{2m} q^v$ then by theorem 3.1 it cannot contain any q^v. Hence it must contain p^{2m} and some p^u, and therefore $c = p^u$, $b = p^{2m}$, which contradicts (2.11). Therefore

$$A = \{q^v, p^u, p^{2m}\}$$

for suitable u, v.

If $q^v > p^{2m}$ then $a = q^v$, $b = p^{2m}$, $c = p^u$, and the inequality (2.11) does not hold. Therefore p^{2m} is the greatest element of A, i. e., $a = p^{2m}$, $\{b, c\} = \{p^u, q^v\}$. By theorem 3.2 a $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$; otherwise c can be neither p^u nor q^v.

If $m \geqq u$ then $a = p^{2m} \geqq p^{2u} \geqq c^2$, which contradicts (2.11). Therefore $m < u$, hence $u \geqq 2$. Since $2m - 1 \geqq u$ we obtain $m \geqq 2$ and $u \geqq 3$.

If $n = 1$ then $v = 1$, $\{b, c\} = \{q, p^u\}$, and hence

$$2y = q^2 - p^{2m},\ \{2z, 2t\} = \{p^{2m} q - q,\ p^{2m-u} q^2 - p^u\}.$$

Since $4y^2 = |4z^2 - 4t^2|$ we have

$$(q^2 - p^{2m})^2 = |(p^{2m} q - q)^2 - (p^{2m-u} q^2 - p^u)^2|.$$

From the last equality we can obtain the congruences

$$p^{4m} \equiv \pm p^{2u} \pmod{q^2}$$

$$q^4 \equiv \pm q^2 \pmod{p^{4m-2u}}.$$

(Notice that $p^{2m-u} \mid p^u$ because $u > m$.) The first congruence implies $q^2 \mid p_{4m-2u} \pm 1$, and hence $2q^2 \leqq p^{4m-2u} + 1$; the other implies $p^{4m-2u} \mid q^2 \pm 1$, and hence $2p^{4m-2u} \leqq q^2 + 1$. The sum of the inequalities gives a contradiction. Therefore $n \geqq 2$.

It remains to exclude the case $m = 2$, $n = 2$; assume that it takes place. Since $u > m$ we have $u = 3$. Hence $a = p^4$, $\{b, c\} = \{p^3, q^v\}$, and then

$$2y = q^4 - p^4,\ \{2z, 2t\} = \{pq^4 - p^3,\ p^4 q^{4-v} - q^v\}.$$

Since $4y^2 = |4z^2 - 4t^2|$ we have

$$(q^4-p^4)^2=|(pq^4-p^3)^3-(p^4q^{4-v}-q^v)^2|.$$

From this equality we obtain

$$p^8\equiv\pm p^6 \pmod{q^2}.$$

Therefore $q^2\mid p^2\pm 1$, and hence $q^2\leqq p^2+1$, which contradicts $p^2<q^2$.

3.4. Theorem. Let $x=2^mq^n$ for some prime q and nonnegative integers m, n. Then $q\equiv 1 \pmod 4$, $m\geqq 4$ and $n\geqq 2$.

Proof. Analogously as above we can see $q>2$, $m\geqq 1$, $n\geqq 1$, and by theorem 3.1. b $m\geqq 2$. Denote $A=\{a, b, c\}$. The set A contains only some divisors of x^2 less than x; they must fulfil also the conditions of theorem 3.1. Therefore

$$A\subseteq\{2^u;\ 2\leqq u\leqq 2m-2\}\cup\{2^{2m-1}\}\cup\{2q^v;\ 1\leqq v\leqq 2n-1\}\cup$$
$$\cup\{2q^{2n}\}\cup\{2^uq^v;\ 2\leqq u\leqq 2m-2,\ 1\leqq v\leqq 2n-1\}\cup$$
$$\cup\{2^uq^{2n};\ 2\leqq u\leqq 2m-2\}\cup\{2^{2m-1}q^v;\ 1\leqq v\leqq 2n-1\}.$$

Further in the proof we always assume

$$2\leqq u\leqq 2m-2,\quad 1\leqq v\leqq 2n-1.$$

Theorem 3.1 implies that A contains at most one element of the forms

$$2q^v,\ 2^uq^v,\ 2^{2m-1}q^v,$$

and at most one element of the forms

$$2^u,\ 2^uq^v,\ 2^uq^{2n}.$$

As a consequence we can see that A contains at least one of the elements 2^{2m-1}, $2q^{2n}$. However, it cannot contain both of them because only one of them is less than x. Now we can easily see that A does not contain any element of the form 2^uq^v.

If $2^{2m-1}\in A$ then $2q^{2n}$, 2^uq^{2n} are greater than x, and hence

$$A=\{2q^v,\ 2^u,\ 2^{2m-1}\}\ \text{ or }\ A=\{2^u,\ 2^{2m-1},\ 2^{2m-1}q^v\}$$

for some u, v. However, the second case contradicts (2.11). Analogously, if $2q^{2n}\in A$ then 2^{2m-1}, $2^{2m-1}q^v$ are greater than x, and hence

$$A=\{2^u,\ 2q^{2n},\ 2q^v\}\ \text{ or }\ A=\{2^uq^{2n},\ 2q^{2n},\ 2q^v\}.$$

The second case again contradicts (2.11). In both remaining cases we have $\{b, c\}=\{2^u, 2q^v\}$ and $a\in\{2^{2m-1}, 2q^{2n}\}$. (Notice that y^2 will be determined uniquely, independently on the choice of a.) However, theorem 3.2 implies $\mathrm{ex}(2, c)\neq u$, and hence $c=2q^v$, $b=2^u$.

Now the formulas (2.4) imply

$$y = |2^{2m-2} - q^{2n}|,\ z = 2^{2m-1-u}q^{2n} - 2^{u-1},\ t = 2^{2m-2}q^{2n-v} - q^v,$$

and therefore

$$(2^{2m-2} - q^{2n})^2 + (2^{2m-1u}q^{2n} - 2^{u-1})^2 = (2^{2m-2}q^{2n-v} - q^v)^2.$$

The latest equality implies

$$2^{4m-4} + 2^{2u-2} \equiv 0 \pmod{q^2}$$
$$2^{4m-2-2u} + 1 \equiv 0 \pmod{q^2}.$$

Since $4m-2-2u>0$ all divisors of the left side are of the form $4k+1$, and hence $q \equiv 1 \pmod 4$. (The left side is odd, and it is a sum of two relatively prime squares.) Since the numbers $2^{2k}+1$ are square-free for $k=1, 2, 3, 4$ we have $4m-2-2u \geqq 10$, $4m \geqq 12+2u \geqq 16$, and hence $m \geqq 4$. Notice also $q^2 \leqq 2^{4m-2-2u}+1$.

It remains to exclude the case $n=1$. If $n=1$ then $v=1$, $c=2q$, $b=2^u$, $a \in \{2^{2m-1}, 2q^2\}$ and

$$(2^{2m-2} - q^2)^2 + (2^{2m-1-u}q^2 - 2^{u-1})^2 = (2^{2m-2}q - q)^2$$

We shall reduce the last equality modulo $2^{4m-2-2u}$. To do that conveniently we have to estimate u at first.

We can easily see that $a = 2q^2$ contradicts the last inequality of (2.11), and hence $a = 2^{2m-1}$. Using (2.11) once more we obtain $(2^{2m-1})^2 < c^3 < (2^u)^3$, and hence $4m-2 \leqq 3u-1$, $3u \geqq 3m+(m-1)$, what implies $u \geqq m+1$. (We have proved $m>1$.) Therefore $u-1 \geqq 2m-1-u$ and $2m-1 \geqq 4m-2-2u$. Now we can obtain

$$q^4 \equiv q^2 \pmod{2^{4m-2-2u}},\ 2^{4m-2-2u} \mid q^4 - q^2 = q^2 \cdot (q+1) \cdot (q-1).$$

Since $q \equiv 1 \pmod 4$ we obtain

$$2^{4m-2-2u} \leqq 2 \cdot (q-1).$$

On the other hand, we know that $q^2 \leqq 2^{4m-2-2u}+1$. Together we obtain $q^2 \leqq 2 \cdot (q-1)+1 = 2q+1$, which is a contradiction.

3.5. Theorem. If x is the least edge then

$$a < x \cdot (\sqrt{2}-1) \text{ and } c < x \cdot (\sqrt{3}-\sqrt{2}).$$

Proof. Since $y>x$ we have

$$\frac{1}{2}\left(\frac{x^2}{a} - a\right) > x.$$

If we multiply the latest inequality by $\frac{2}{a}$ and denote $r = \frac{x}{a}$ we obtain $r^2 - 1 > 2r$,

$(r-1)^2>2$. However, $r>1$, and hence $r-1>\sqrt{2}$, $r>1+\sqrt{2}$. Therefore $x>$ $\cdot(1+\sqrt{2})$, $a<x\cdot(\sqrt{2}-1)$. The second inequality immediately follows from (2.12).

3.6. Theorem. Denote

$$E=(x^4-b^2c^2)(b^2-c^2),\quad F=2b^2c^2x^4,\quad D=E(E+2F).$$

Then D is a square and

$$a=\sqrt{\frac{x^2\cdot F}{E+F+\sqrt{D}}}.$$

Proof. The equation (2.7) can be rewritten into the form

$$(b^2c^2)\cdot a^4-(E+F)\cdot 2a^2+b^2c^2x^4=0.$$

Let us solve it as a quadratic equation for $A=a^2$. Its discriminant is

$$(E+F)^2-4\cdot b^2c^2\cdot b^2c^2x^4=(E+F)^2-F^2=E(E+2F)=D,$$

and its roots are

$$A_{1,2}=\sqrt{\frac{E+F\pm\sqrt{D}}{2b^2c^2}}.$$

Since $A_1\cdot A_2=x^4$ and $a^2<x^2$ we have $a^2=A_2$, and hence

$$a=\sqrt{A_2}=\frac{x^2}{\sqrt{A_1}}=\sqrt{\frac{2b^2c^2x^4}{E+F+\sqrt{D}}}=\sqrt{\frac{x^2\cdot F}{E+F+\sqrt{D}}}.$$

The next result was not used in computer computation, and does not depend on it.

3.7. Theorem. If x, y, z are the edges of a perfect rational cuboid then $2^6\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 19\,|\,xyz$.

Proof. We may obviously assume (2.2). If $\mathrm{ex}(3, r)=\mathrm{ex}(3, s)$ then r^2+s^2 is not a square because

$$(r^2+s^2)/3^{2\cdot \mathrm{ex}(3,r)}\equiv 2 \pmod 3.$$

Therefore $\mathrm{ex}(3, x)$, $\mathrm{ex}(3, y)$, $\mathrm{ex}(3, z)$ are pairwise different, and hence $\mathrm{ex}(3, xyz)\geqq 0+1+2=3$. Arguing similarly (with the modul 8) we can see that the difference of any two integers from $\mathrm{ex}(2, x)$, $\mathrm{ex}(2, y)$, $\mathrm{ex}(2, z)$ is at least 2. Hence $\mathrm{ex}(2, xyz)\geqq 0+2+4=6$. It remains to prove $5\cdot 7\cdot 11\cdot 19\,|\,xyz$.

Consider a prime p which does not divide xyz; reduce all integers modulo p. Denote $\mathrm{K}(p)$ the set of all quadratic residues modulo p and

$$L(p) = \{u \in K(p);\ u \neq 0 \text{ and } u+1 \in K(p)\}.$$

Let $y^2 \equiv x^2 \cdot u \pmod{p}$ and $z^2 \equiv x^2 \cdot v \pmod{p}$. The numbers

$$y^2,\ y^2+x^2,\ z^2,\ z^2+x^2,\ t^2,\ t^2+x^2,$$

i. e.

$$x^2 \cdot u,\ x^2 \cdot (u+1),\ x^2 \cdot v,\ x^2 \cdot (v+1),\ x^2 \cdot (u+v),\ x^2 \cdot (1+u+v)$$

are quadratic residues modulo p, hence so are

$$u,\ u+1,\ v,\ v+1,\ u+v,\ u+v+1.$$

Therefore $u,\ v,\ u+v \in L(p)$, i. e., the set $L(p)$ contains the sum of its two elements (not necessarily different) modulo p.

For $p=19$ we have

$$K(19) = \{0, 1, 4, 5, 6, 7, 9, 11, 16, 17\},\ L(19) = \{4, 5, 6, 16\}.$$

The set L(19) does not contain any sum of its two elements; e. g., $16+16 \equiv 13 \notin L(19)$. Therefore $19 \mid xyz$. For $p = 11, 7, 5$ we have

$$\begin{aligned} K(11) &= \{0, 1, 3, 4, 5, 9\}, & L(11) &= \{3, 4, 5\}, \\ K(7) &= \{0, 1, 2, 4\}, & L(7) &= \{1\}, \\ K(5) &= \{0, 1, 4\}, & L(5) &= \{4\}. \end{aligned}$$

The sets L(11), L(7), L(5) do not contain any sum of their elements, hence $11 \mid xyz$, $7 \mid xyz$, $5 \mid xyz$, which completes the proof.

4. The computation

The program was written in the language Pascal B and run on the computer CDC 3300; a portion of 5000 values of x was processed in about 2 minutes. Some auxiliary computation (e. g., the table of primes) was done before the main cycle. However, the essential part was the cycle where the values of x were considered in the successive order, and gradually excluded (i. e., it was proved that there is no primitive perfect rational cuboid with the least edge x). For every x the following steps 1.—9. were performed (if a value of x was excluded then all further steps for it were omitted):

1. If $x \equiv 2 \pmod{4}$ then exclude x. (See theorem 3.1. b.)
2. Find the standard form of x.
3. Try to excude x by theorems 3.3 or 3.4.
4. Generate all candidates for c, i. e. all divisors of x^2 which satisfy the inequality $c \geqq 3200$ or $c \geqq 6400$ if x is odd or even, respectively (see (2.13) nd theorem 3.1), and the conditions from theorems 3.1, 3.2, 3.5. Denote by $c_{\min}$, $c_{\max}$ the minimal and the maximal candidate, respectively.

5. If no candidates for c was found then exclude x.

6. Generate all candidates for b, i. e. all divisors of x^2 which satify the inequality

$$c_{\min}+2 \leqq b \leqq \min\,(c_{\max}\cdot\sqrt{2},\ x\cdot(\sqrt{2}-1))$$

and the conditions from theorems 3.1, 3.2, 3.5.

7. If no candidate for b was found then exclude x.

8. For every pair of candidates (c, b), $c<b$, do the following:

8.1. Solve the equation (2.7) with respect to the unknown a by theorem 3.6, and denote the solution by a_1. (Even if x, c, b correspond to a perfect rational cuboid a_1 need not be an integer because of rounding errors. Notice that the formula for a avoids any substraction of reals.)

8.2. Let a be the integer nearest to a_1. If $a \leqq b$ or $|a-a_1| \geqq 0.002$ then exclude the pair (c, b) just considered.

8.3. Verify (2.7) modulo 2003; if (2.7) does not hold then exclude the pair (c, b) just considered.

8.4. Find out whether a divides x^2; if not then exclude the actual pair (c, b).

8.5. Print the pair (c, b), and x, a, too, if it has not been excluded.

9. Print x if it has not been excluded (i. e., if at least one pair (c, b) was printed in 8.5).

Notice that the step 2 need not be always finished; e. g., it can be interrupted (and x can be excluded) if it is clear that x has no prime divisor less than the cubic root of x (see theorems 3.3 and 3.4). In the steps 4. and 6. the standard form of x is used to generate divisors of x^2 (in 4. only suitable ones, see theorem 3.2); only then the inequalities for them are tested. It is much faster than a test of divisibility for all integers from the suitable interval. The constant 0.002 in 8.2 could be rather diminished but more safe computation was preferred; nevertheless, the relative error of a_1 was checked. The prime $p=2003$ in 8.3 was chosen so that $2p^2$ can be immediately represented as an integer, and $p \equiv 3 \pmod 4$; however, 2003 can be replaced by any smaller integer. The tests in 8.2 and 8.3 are so strong that by testing 8.4, 8.5 and 9. the constants 0.002 and 2003 had to be replaced by 0.3 and 11; otherwise those steps were too rare in the computation. That was also the reason why the test like 8.3. was not repeated with another prime.

Gradually all x up to one million were excluded, and hence it was proved:

The result. There is no perfect rational cuboid with the least edge less than 1000000.

REFERENCES

[1] Korec, I.: Diophantine equations $x^2 \pm xy - y^2 = z^2$ and $x^4 \pm x^2y^2 - y^4 = z^2$. Acta Math. Univ. Comenianae 38 (1981) 119—127.

[2] Korec, I.: Nonexistence of a small perfect rational cuboid. Acta Math. Univ. Comenianae 42—43, (1983), 73—86.

[4] Leech, J.: The rational cuboid revisited. Amer. Math. Monthly 84 (1977), 518—533.

[4] Mordell, L. J.: Diophantine equations. Academic Press, London and New York, 1969.

[5] Sierpinski, W.: Teoria liczb. Warszawa—Wroclaw, 1950.

[6] Spohn, W. G.: On the integral cuboid. Amer. Math. Monthly 79 (1972), 57—59.

[7] Spohn, W. G.: On the derived cuboid. Canad. Math. Bull. 17 (1974), 575—577.

Author's address: Received: 5. 10. 1982

Ivan Korec
Katedra algebry a teórie čísel MFF UK
Matematický pavilón
Mlynská dolina
842 15 Bratislava

SÚHRN

NEEXISTENCIA MALÉHO PYTAGOREJSKÉHO KVÁDRA, II.

I. Korec, Bratislava

V práci sa s použitím samočinného počítača dokazuje, že neexistuje pytagorejský kváder (t. j. kváder, v ktorom dĺžky všetkých hrán i uhlopriečok sú celé čísla) s dĺžkou najkratšej hrany menšou než 1000000. Okrem toho sa dokazuje, že ak pytagorejský kváder existuje, tak jeho objem je deliteľný číslom $64 \cdot 27 \cdot 5 \cdot 7 \cdot 11 \cdot 19$.

РЕЗЮМЕ

МАЛЫЙ СОВЕРШЕННЫЙ РАЦИОНАЛЬНЫЙ КУБОИД НЕ СУЩЕСТВУЕТ, II.

И. Корец, Братислава

Прямоугольный параллелэпипед называется совершенным рациональным кубоидом, если длины его ребер, его диагонали и диагоналей всех его граней являются целыми числами. Доказывается, что длина каждого ребра совершенного рационального кубоида (если такой вообще существует) больше или равна 1000000, и что его объем делится на $64 \cdot 27 \cdot 5 \cdot 7 \cdot 11 \cdot 19$.