Werk

Titel: Der Neudruck des Canon missae und der Sandguß

Autor: Hupp, Otto

Ort: Mainz

PURL: https://resolver.sub.uni-goettingen.de/purl?366382810_1942-43|log13

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
XLII—XLIII—1983

NONEXISTENCE OF A SMALL PERFECT RATIONAL CUBOID

IVAN KOREC, Bratislava

1. Introduction

There were several attempts to find perfect rational cuboid, i.e. a rectangular parallelepiped of which the length of the edges, the face diagonals and the body diagonal are integers. (For the sahe of brevity, below we shall say "the edge" instead of "the length of the edge", and analogously for the diagonals.) These attempts are discussed in [2]. Up to now, no of these attempts was succesful. However, there are cuboids for which six of the seven length mentioned above are integers. For example (see [2]):

a) if the edges are 44, 240, 117 then all face diagonals are integers;

b) if the edges are 117, 520, 756 then two face diagonals and the body diagonal are integers;

c) if the edges are 124, 957, $\sqrt{13\,852\,800}$ then all the four diagonals are integers.

In many attempts (e. g. [5], [6]) to find a perfect rational cuboid the authors choose a necessary condition for cuboid to be a perfect rational one. Then they choose a suitable subclass of the class of all cuboid satisfying the necessary condition and tried to find the perfect rational cuboid in the chosen subclass. Sometimes they also proved that in the considered subclass no perfect rational cuboid exists. Of course, such results do not mean that there is no perfect rational cuboid in general. Maybe, there is even a relatively small perfect rational cuboid lost by forming the subclass.

2. The aim of the present paper

In our attempt we consider the class of all perfect rational cuboids. Using a computer program, we shall look for a perfect rational cuboid which is small in some sense (roughly speaking, one with a small edge). Of course, this bound depends on the computation time used, on the computer, etc. However, the present paper does not deal with the details of the computer program. It mainly deals with

a number-theoretical results on which the program is based. We tried to give the results in the form suitable for programming.

In *Section 3* parameters a, b, c, d, v are introduced; a, b, c are independent each from others (at least when they are introduced), d, v are functions of a, b, c in essential. Then some inequalities and other conditions for a, b, c, d, v are derived (provided that the parameters correspond to a perfect rational cuboid).

In *Section 4* modul conditions and strong modul conditions are defined. Then some further conditions for the parameters a, b, c (corresponding to a perfect rational cuboid) are derived. These conditions are formulated as strong modul conditions for a when b, c are fixed. They form our main tool for excluding a when b, c are fixed. Other conditions, which are given in *Section 5*, are used only when the condition from *Section 4* are not sufficient to exclude all values of a. *Section 6* contains a rough description of the computer program and the obtained numerical results. The least edge of any perfect rational cuboid must be at least 10 000.

3. Parameters a, b, c, d, v and inequalities for them

Let x, y, z be the edges of a perfect rational cuboid, i.e. positive integers such that

$$\sqrt{(x^2+y^2)},\quad \sqrt{(x^2+z^2)},\quad \sqrt{(x^2+y^2+z^2)},\quad \sqrt{(y^2+z^2)} \tag{3.1}$$

are also integers. Since $\sqrt{(x^2+y^2)}$ is an integer greater than y there is a positive integer a such that

$$x^2+y^2=(y+a)^2$$

what easily implies

$$y=\frac{1}{2}\left(\frac{x^2}{a}-a\right) \tag{3.2}$$

Analogously we can find positive integers b, c satisfying

$$z=\frac{1}{2}\left(\frac{x^2}{b}-b\right) \tag{3.3}$$

$$\sqrt{(y^2+z^2)}=\frac{1}{2}\left(\frac{x^2}{c}-c\right) \tag{3.4}$$

Since the function

$$f(t)=\frac{1}{2}\left(\frac{x^2}{t}-t\right)$$

is decreasing on the interval $(0, \infty)$ and $f(x)=0$, the formulas (3.2)—(3.4) imply $a<x$, $b<x$ and

$$c<a, \quad c<b, \tag{3.5}$$

For many considerations below, y and z can be interchanged. In these cases we shall assume $y<z$ (the equality is obviously impossible), what implies

$$b<a \tag{3.6}$$

Sometimes we shall also assume that x is the least edge of the cuboid; if this assumption or (3.6) are used, they will be explicitely mentioned. From (3.2)—(3.4) we can obtain

$$\left(\frac{x^2}{a}-a\right)^2+\left(\frac{x^2}{b}-b\right)^2=\left(\frac{x^2}{c}-c\right)^2$$

what after an easy computation gives

$$(a^2c^2+b^2c^2-a^2b^2)x^4-2a^2b^2c^2x^2+a^2b^2c^2(a^2+b^2-c^2)= \tag{3.7}$$

Consider (3.7) as a quadratic equation for $X=x^2$. Its discriminant

$$\begin{gathered}(2a^2b^2c^2)^2-4(a^2c^2+b^2c^2-a^2b^2)a^2b^2c^2(a^2+b^2-c^2)= \\ =4a^2b^2c^2(a^2b^2c^2-((a^2+b^2)c^2-a^2b^2)((a^2+b^2)-c^2))= \\ =4a^2b^2c^2(a^2b^2c^2-(a^2+b^2)^2c^2+(a^2+b^2)c^2+a^2b^2(a^2+b^2)-a^2b^2c^2)= \\ =4a^2b^2c^2(a^2+b^2)(a^2-c^2)(b^2-c^2)\end{gathered}$$

must be a square. Hence there is an integer d such that

$$d^2=(a^2+b^2)(a^2-c^2)(b^2-c^2) \tag{3.8}$$

It can be easily checked that

$$(abc+d)(abc-d)=(a^2+b^2-c^2)(a^2c^2+b^2c^2-a^2b^2) \tag{3.9}$$

If we choose the sign of d conveniently (later we shall see that d must be chosen positive) we obtain

$$x^2=\frac{abc(abc+d)}{a^2c^2+b^2c^2-a^2b^2} \tag{3.10}$$

However, using (3.9) we can replace (3.10) by

$$x^2=\frac{abc(a^2+b^2-c^2)}{abc-d} \tag{3.11}$$

Therefore there is a positive integer v such that

$$v^2=abc(abc-d)(a^2+b^2-c^2) \tag{3.12}$$

Let k be a positive integer. The numbers a, b, c, d, v satisfy the conditions (3.8), (3.12) if and only if the numbers

$$a_1 = ka, \quad b_1 = kb, \quad c_1 = kc, \quad d_1 = k^3 d, \quad v_1 = k^4 v \tag{3.13}$$

also satisfy them. (The same holds for some conditions below, e.g. for the inequalities (3.15), (3.17.) Therefore by looking for a, b, c, d, v we may assume

$$D(a, b, c) = 1 \tag{3.14}$$

Notice that we cannot prove (3.14) from the assumption $D(x, y, z) = 1$.

Now, consider the function

$$F(t) = (a^2c^2 + b^2c^2 - a^2b^2)t^4 - 2a^2b^2c^2t^2 + a^2b^2c^2(a^2 + b^2 - c^2)$$

of the real variable t and assume (3.6). We have

$$\begin{aligned} F(c) &= a^2c^6 + b^2c^6 - a^2b^2c^4 - 2a^2b^2c^4 + a^4b^2c^2 + a^2b^4c^2 - a^2b^2c^4 = \\ &= (a^4b^2c^2 - 2a^2b^2c^4 + b^2c^6) + (a^2b^4c^2 - 2a^2b^2c^4 + a^2c^6) = \\ &= b^2c^2(a^2 - c^2)^2 + a^2c^2(b^2 - c^2)^2 > 0 \end{aligned}$$

$$\begin{aligned} F(a) &= a^6c^2 + a^4b^2c^2 - a^6b^2 - 2a^4b^2c^2 + a^4b^2c^2 + a^2b^4c^2 - a^2b^2c^4 = \\ &= a^6(c^2 - b^2) + a^2b^2c^2(b^2 - c^2) = (a^6 - a^2b^2c^2)(c^2 - b^2) < 0 \end{aligned}$$

$$F(x) = 0$$

Hence $F(t)$ has two positive roots, x and a number from the interval (c, a). Since $F(t)$ is an even polynomial of degree (at most) four, $F(t)$ cannot have any further positive roots (and x its simple root). Since x is the greater positive root of $F(t)$, the number d in (3.10) and (3.11) must be positive. Further, we have $F(t) > 0$ for all $t > x$, and hence

$$a^2c^2 + b^2c^2 - a^2b^2 > 0$$

This inequality can be rewritten into then form

$$\frac{1}{a^2} + \frac{1}{b^2} > \frac{1}{c^2} \tag{3.15}$$

and also into the form

$$a < \frac{bc}{\sqrt{b^2 - c^2}} \tag{3.16}$$

Further, (3.6) implies $\frac{1}{a^2} < \frac{1}{b^2}$, and hence by (3.15) we have

$$b < c\sqrt{2} \tag{3.17}$$

Note that (3.6) was substantialy used only in (3.17); the inequalities (3.15), (3.16)

hold also without this assumption because (3.15) is symmetric in a, b and (3.16) is a corollary of (3.15).

Now, we shall assume

$$x<y<z \tag{3.18}$$

Then $x\sqrt{2}<\sqrt{(y^2+z^2)}$ and hence (3.4) implies

$$x\sqrt{2}<\frac{1}{2}\left(\frac{x^2}{c}-c\right)$$

Therefore for $r=\frac{x}{c}$ we obtain

$$r\sqrt{2}<\frac{1}{2}(r^2-1)$$

what together with $r>1$ gives $r>\sqrt{2}+\sqrt{3}$, *i.e.*

$$x>(\sqrt{2}+\sqrt{3})c\,. \tag{3.19}$$

The above consideration can be summarized as follows

3.1. Theorem. Let there be no positive integers a, b, c, d, v which satisfy (3.5), (3.6), (3.8), (3.12), (3.14), (3.15), (3.17) and

$$c\leqq C_0 \tag{3.1.1}$$

where C_0 is a constant. Then there is no integral cuboid with the least edge x satisfying

$$x\leqq C_0.(\sqrt{2}+\sqrt{3}). \tag{3.1.2}$$

The assumption of Theorem 3.1 will be verified by a computer computation. However, neither condition (3.18) nor its consequences will be immediately used in the computer program. Later the author wants to use the computer results also in another way, in which (3.18) is not suitable.

4. Strong modul conditions

In this section we shall prove some consequences of the conditions

$$(3.8),\quad (3.12),\quad (3.14) \tag{4.1}$$

(Note that (3.6) and (3.15) are not contained in (4.1). Further, (4.1) is symmetric in a, b, hence we may interchange a, b in the consequences of (4.1).)
We shall look for the consequences useful in the computer computation for

Theorem 3.1. The consequences will be formulated as modul conditions

$$a \equiv r_1, \ldots, r_k \pmod{p^n} \tag{4.2}$$

for fixed b, c and for a fixed prime p. The meaning of (4.2) is: a is congruent with one of numbers $r_1, \ldots, r_k$ modulo p^n. The less k is (and the greater p^n is) the stronger (4.2) seems to be. The conditions given here are called strong because k does not exceed 5 in any of them.

For any prime p and for any nonzero integer m we denote by $ex(p, m)$ the exponent of the prime p in the standard form of m, i.e. the greatest integer e such that p^e divides m. We shall very often use the following properties of $ex(p, m)$:

$$ex(p, m.n) = ex(p, m) + ex(p, n) \tag{4.3}$$

$$ex(p, m) \neq ex(p, n) \rightarrow ex(p, m+n) = min(ex(p, m), ex(p, n)) \tag{4.4}$$

When p is fixed we shall write $ex(m)$ instead of $ex(p, m)$.

The next theorem allows us to exclude some pairs b, c from further considerations. Formally, Theorem 4.1 gives modul conditions (4.2) with $k = 0$ for these b, c.

4.1. Theorem. Let the numbers a, b, c, d, v satisfy (4.1) and let p be a prime. Then no of the following conditions take place

$$2 \nmid ex(c),\ 2 \nmid ex(b),\ ex(b^2 - c^2) = 2 \tag{4.1.1}$$

$$ex(c) > 0,\ ex(b) > 0,\ 2 \nmid ex(b^2 - c^2) \tag{4.1.2}$$

$$2 \nmid ex(c),\ ex(b) > 0,\ ex(c) > ex(b) \tag{4.1.3}$$

$$ex(c) > 0,\ 2 \nmid ex(b),\ ex(b) > ex(c) \tag{4.1.4}$$

$$2 \mid ex(c),\ ex(c) > 0,\ 2 \mid ex(b),\ ex(b) > 0,\ ex(b^2 - c^2) = 6 \tag{4.1.5}$$

$$ex(b) = ex(c),\ ex(b^2 - c^2) < 4ex(c),\ 4 \nmid ex(b^2 - c^2) \tag{4.1.6}$$

Proof. In all cases we have $p \mid b$, $p \mid c$, and hence by (3.14) $p \nmid a$, i.e. $ex(a) = 0$. Therefore

$$2ex(d) = ex(d^2) = ex(b^2 - c^2)$$

what immediately excludes the case (4.1.2), and partially also the case (4.1.6). In all remainder cases we have

$$ex(d) < ex(abc)$$

and therefore

$$2ex(v) = ex(v^2) = ex(abc) + ex(abc - d) + ex(a^2 + b^2 - c^2)$$
$$= ex(b) + ex(c) + ex(d)$$

In the cases (4.1.3) and (4.1.4) $ex(b) \neq ex(c)$ and hence

$$2ex(d) = ex(b^2 - c^2) = \min\,(ex(b^2),\ ex(c^2)) = 2\,\min\,(ex(b),\ ex(c))$$
$$2ex(v) = 2\,\min\,(ex(b) + ex(c)) + \max\,(ex(b),\ ex(c))$$

The right-hand side is odd, what is a contradiction. In the cases (4.1.1), (4.1.5) and the rest of (4.1.6) the number $ex(d)$ is odd, $ex(b) + ex(c)$ is even, hence $2ex(v)$ is odd again, what is a contradiction.

For the next theorem we shall need the following well known lemma. (The proof can be found e.g. in [4].)

4.2. Lemma. Let p be an odd prime. Then the congruence

$$s^2 + 1 \equiv 0 \pmod{p^2} \tag{4.2.1}$$

has exactly two solutions (modulo p^2) if $p \equiv 1 \pmod 4$ and has no solution if $p \equiv 3 \pmod 4$.

4.3. Theorem. Let integers a, b, c, d, v satisfy (4.1), let $p \equiv 1 \pmod 4$ be a prime and let s satisfy (4.2.1). Then the condition

$$ex(c) = 0,\ ex(b) = 0,\ 2 \nmid ex(b^2 - c^2) \tag{4.3.1}$$

implies

$$a \equiv \pm c,\ \pm bs \pmod p \tag{4.3.2}$$

Further, every of the conditions

$$2 \nmid ex(c),\ ex(b) = 0 \tag{4.3.3}$$

$$ex(c) = 0,\ 2 \nmid ex(b) \tag{4.3.4}$$

implies

$$a \equiv 0,\ \pm c,\ \pm bs \pmod{p^2}. \tag{4.3.5}$$

Proof. If (4.3.1) holds then

$$2ex(d) = ex((a^2 + b^2)(a^2 - c^2)) + ex(b^2 - c^2)$$

implies that $ex((a^2 + b^2)(b^2 - c^2))$ is odd, hence positive.

Therefore

$$(a^2 + b^2)(a^2 - c^2) \equiv 0 \pmod p$$

and the solutions of this congruence are given in (4.3.2).

Now let (4.3.3) hold. If $ex(a) \geqq 2$ then $a \equiv 0 \pmod{p^2}$, hence it suffices to consider $ex(a) = 0$ and $ex(a) = 1$ in what follows. Let $ex(a) = 0$ at first. If $ex(a^2 + b^2) = 0$ then $ex(d) = 0$, hence

$$2ex(v) = ex(c) + ex(abc - d) + ex(a^2 + b^2 - c^2) = ex(c) + 0 + 0 = ex(c)$$

is odd, what is a contradiction. Therefore $ex(a^2+b^2)$ is positive and since $ex(a^2+b^2)=2ex(d)$ we have $ex(a^2+b^2)\geqq 2$, i.e.

$$a^2+b^2\equiv 0 \pmod{p^2}$$

what implies $a\equiv \pm bs \pmod{p^2}$.

Now let $ex(a)=1$. Since

$$2\mathrm{ex(v)}=1+\mathrm{ex(c)}+\mathrm{ex(abc-d)}$$

the number $ex(abc-d)$ is even. Since $ex(abc)\geqq 2$ and $ex(d)>0$ we have $ex(d)\geqq 2$, i.e. $ex(d^2)=ex(a^2-c^2)\geqq 4$, and thus

$$\mathrm{a^2-c^2}\equiv 0 \pmod{p^4} \tag{4.3.7}$$

Since $ex(a)=1$ we have $ex(a+c)\leqq 1$ or $ex(a-c)\leqq 1$. Then $ex(a-c)\geqq 3$ or $ex(a+c)\geqq 3$, respectively. Therefore

$$a\equiv \pm c \pmod{p^3}$$

what is contained in (4.3.5).

Now assume (4.3.4). Analogously as above we may assume $ex(a)=0$ or $ex(a)=1$. Let $ex(a)=0$ at first. If $ex(a^2-c^2)=0$ then $ex(d)=0$, hence $2ex(v)=ex(b)+ex(abc-d)+ex(a^2+b^2-c^2)=ex(b)+0+0=ex(b)$ is odd, what is a contradiction. Therefore $ex(a^2-c^2)$ is positive. Since $ex(a^2-c^2)=2ex(d)$ we have $ex(a^2-c^2)\geqq 2$, i.e.

$$a^2-c^2\equiv 0 \pmod{p^2}$$

what implies $a\equiv \pm c \pmod{p^2}$.

Now let $ex(a)=1$. Then

$$2ex(v)=1ex(b)+ex(abc-d)$$

hence the number $ex(abc-d)$ is even. Analogously as in the previous case we obtain $ex(d^2)=ex(a^2+b^2)\geqq 4$. Therefore for $a_1=\frac{a}{p}$, $b_1=\frac{b}{p}$ we have $ex(a_1)=0$ and

$$a_1^2+b_1^2\equiv 0 \pmod{p^2}$$

what implies $a_1\equiv \pm b_1 s \pmod{p^2}$. Hence $a\equiv \pm bs \pmod{p^3}$, what is contained in (4.3.5).

4.4. Theorem. Let integers a, b, c, d, v satisfy the condition (4.1) and let $p\equiv 3 \pmod 4$ be a prime. Then (4.3.1) implies

$$a\equiv \pm c \pmod{p} \tag{4.4.1}$$

and (4.3.4) implies

$$a \equiv 0, \pm c \pmod{p^2} \tag{4.4.2}$$

Further, (4.3.3) implies

$$a \equiv \pm c \pmod{p^3} \tag{4.4.3}$$

Proof. The proof of (4.4.1) and (4.4.2) is very similar to that of (4.3.2), (4.3.5) in Theorem 4.3. Therefore we shall only prove (4.4.3); let (4.3.3) hold.

If $ex(a)=0$ then

$$2ex(v)=ex(c)+ex(abc-d)$$

what implies $ex(d)\neq 0$. However $2ex(d)=ex(a^2+b^2)$, i.e. $a^2+b^2\equiv 0 \pmod{p}$, what contradicts $p\equiv 3 \pmod 4$. If $ex(a)=1$ we obtain (4.3.7) and then (4.4.3) in the same way as in the proof of Theorem 4.3.

It remains to exclude $ex(a)=2$. In this case by (4.1.3) of Theorem 4.1 we have $ex(c)=1$. Denote $d_1=\frac{d}{p}$, $c_1=\frac{c}{p}$. We have

$$\begin{aligned} d_1^2 &= (a^2+b^2)(a_1^2-c_1^2)(b^2-c^2) \\ d_1^2 &\equiv b^2.(-c_1^2).b^2 \pmod{p} \\ d_1^2+(b^2c_1)^2 &\equiv 0 \pmod{p} \end{aligned}$$

what contradicts $p\equiv 3 \pmod 4$ and $ex(b^2c_1)=0$.

4.5. Theorem. Let a, b, c, d, v satisfy (4.1) and let $p=2$. Then (4.3.1) implies

$$a \equiv \pm c \pmod 8 \tag{4.5.1}$$

Proof. If a is even then $2ex(d)=ex(b^2-c^2)$, what is a contradiction. Therefore a is odd. Then

$$2ex(d)=1+ex(a^2-c^2)+ex(b^2-c^2)$$

Hence $ex(a^2-c^2)$ is even and since $ex(a^2-c^2)\geqq 3$ we have

$$a^2-c^2\equiv 0 \pmod{16}$$

If $4\mid a+c$ and $4\mid a-c$ then $4\mid 2a$, i.e. a is even, what is a contradiction. Therefore $8\mid a-c$ or $8\mid a+c$, i.e. $a\equiv \pm c \pmod 8$, q.e.d.

4.6. Theorem. Let a, b, c, d, v satisfy (4.1) and the inequalities $c<a$, $c<b$ and (3.15), let $p\equiv 3 \pmod 4$ be a prime and let $2\nmid ex(c)$. Then $p^2<c$.

Proof. Assume, conversely, $p\geqq c$. Since $ex(c)$ is odd and $ex(c)\leqq 2$ we have $ex(c)=1$. We may assume (3.6) without loss of generality.

If $ex(b)=1$ then Theorem 4.1 implies $2\mid ex(b^2-c^2)$, $ex(b^2-c^2)>2$ and hence $p^4\mid b^2-c^2$. Therefore $p^4\leqq b^2-c^2<c^2$ what is a contradiction.

If $ex(b)>1$ then $ex(a)=0$. Denote $c_1=\frac{c}{p}$, $b_1=\frac{b}{p}$, $d_1=\frac{d}{p}$. Since

$$d_1^2=(a^2+b^2)(a^2-c^2)(b_1^2-c_1^2)$$

and $p\mid b_1$ we have

$$d_1^2\equiv -a^4c_1^2 \pmod p$$

$$d_1^2+(a^2c_1)^2\equiv 0 \pmod p$$

what contradicts $p\equiv 3 \pmod 4$ and $p\nmid a^2c_1$.

If $ex(b)=0$ then by Theorem 4.4 we have (4.4.3), and since $a>c$ we obtain $a\geqq p^3-c$. Then (3.15) implies

$$\frac{1}{(p^3-c)^2}+\frac{1}{(c+1)^2}>\frac{1}{c^2} \tag{4.6.1}$$

Since $p^2>c$, $p\mid c$ we have $c\leqq p(p-1)$ and hence

$$(p^3-c)^2\geqq(p^3-p(p-1))^2=(p^3-p^2+p)^2=p^2(p^2-p+1)^2\geqq p^2(c+1)^2$$
$$\geqq c(c+1)^2$$

Therefore (4.6.1) implies

$$\frac{1}{c(c+1)^2}+\frac{1}{(c+1)^2}>\frac{1}{c^2}$$

and hence

$$c+c^2>(c+1)^2$$

what is a contradiction.

5. Other conditions

The main tool for excluding the triples (a, b, c) i.e., for proving that there are no positive integers d, v such that a, b, c, d, v satisfy (3.5), (3.8), (3.12), (3.14) and (3.15)) were given in the previous section. Here we give some additional conditions. The condition (5.1.1) excludes a twoparametrical set of solutions of (3.8) and the conditions from Theorem 5.2 will be used only if no previous conditions are sufficient.

5.1. Theorem. If positive integers a, b, c, d, v satisfy (3.5) and (4.1) then

$$b^2\neq ac \tag{5.1.1}$$

Proof. Let, conversely, $b^2 = ac$. Since $D(a, b, c) = 1$ we have $D(a, c) = 1$. Hence there are integers r, s such that

$$a = r^2, \quad b = rs, \quad c = s^2, \quad D(r, s) = 1$$

Further,

$$d^2 = (a^2 + ac)(a^2 - c^2)(ac - c^2) = ac(a + c)(a^2 - c^2)(a - c) = b^2(a^2 - c^2)^2$$

and hence $d = b(a^2 - c^2)$. Therefore

$$v^2 = abc(abc - b)(a^2 - c^2))(a^2 + b^2 - c^2) = b^4(c^2 + ac - a^2)(a^2 + ac - c^2)$$

Thus the number

$$(c^2 + ac - a^2)(a^2 + ac - c^2) = (s^4 + r^2s^2 - r^4)(r^4 + r^2s^2 - s^4)$$

must be a square. However,

$$D(r^2s^2 + r^4 - s^4, r^2s^2 + s^4 - r^4) = D(2r^2s^2, r^2s^2 + r^4 - s^4) = 1$$

Therefore there are positive integers t, u such that

$$r^4 + r^2s^2 - s^4 = t^2, \quad s^4 + r^2s^2 - r^4 = u^2$$

However, by [1] these diophantine equations have no nontrivial solution (e.g. any solution with $r > s > 0$), what is a contradiction.

5.2. Theorem. Let a, b, c, d, v satisfy the conditions (4.1) and let p be a prime. Then

a) the number

$$(a^2 + b^2)(a^2 - c^2)b^2 - c^2)$$

is a quadratic residue modulo p;

b) if

$$(a^2 + b^2)(a^2 - c^2)(b^2 - c^2) \equiv d_1^2 \pmod{p}$$

then at least one of the numbers

$$abc(abc + d_1)(a^2 + b^2 - c^2), \quad abc(abc - d_1)(a^2 + b^2 - c^2)$$

is a quadratic residue modulo p.

The proof is trivial, and will be omitted. By this theorem we can sometimes replace too big numbers d, v by their residues modulo p.

6. Structure of the program and obtained result

A rough flowchart of the program is given in the picture. The input consists of two positive integers $c_{\min} \leqq c_{\max}$ which are interpreted as the bounds for c (and of some parameters for outputs). The values of c are considered in the successive order. For c fixed, the bound of b are given by (3.5) and (3.17); the values of b are considered in successive order, too. For c, b fixed, the program considers all a satisfying (3.6) and (3.15); however, they are not considered individually.

Denote by W the set of all ordered tripples satisfying (3.5), (3.6), (3.14), (3.15) and corresponding to perfect rational cuboids (we do not know whether $W = \emptyset$ or not). The actual c is declared to be excluded if the program finds out that there are no b, a satisfying $(c, b, a) \in W$. Analogously, for fixed c, b is excluded if the program finds out that there is no a satisfying $(c, b, a) \in W$. For fixed c, b, the value a is excluded if the program finds out $(c, b, a) \notin W$.

The tool for excluding c, b, or a are strong modul conditions and other conditions given in the previous section. Some values of b, or even of c, can be excluded directly. However, usually the values of a must be gradually excluded for fixed b, c. In this case the program generates necessary modul conditions (and other conditions) on a for $(c, b, a) \in W$. It gradually forms the conjunction of all these conditions (in the form of modul condition, too). As soon as all a are excluded (i.e. the formed conjunction represents the empty set) the actual b is exluded. In fact, the test whether all a are excluded is more often than in the rough block diagram. If some values of a are not excluded then they are printed (together with the actual c, b) for further consideration. They may correspond to a perfect rational cuboid. (In fact, this case never occured.)

A most important subprogram of our program is the subprogram for generating a conjuction of two modul conditions. Modul conditions are considered in the form (4.2); however, their moduls need not be powers of primes. The modul of the conjunction is usually the least common multiple of the moduls of the original modul conditions. However, the subprogram consideres also the bounds for a. As soon as every rest represents at most one number, the resulting modul becomes zero. Congruence modulo 0 is understood as equality.

The condition (3.14) and Theorem 5.1 could be applied in our main program only after the modul of the formed conjunction becomes zero. Besides, they are applied only after all strong modul conditions.

The really performed computations on the computer CDC 3300 excluded (in 3 hours) all $c \leqq 3200$. Since

$$3200.(\sqrt{2}+\sqrt{3}) > 10\,000$$

Theorem 3.1 implies:

Result. There is no perfect rational cuboid with the least edge smaller or equal 10 000.

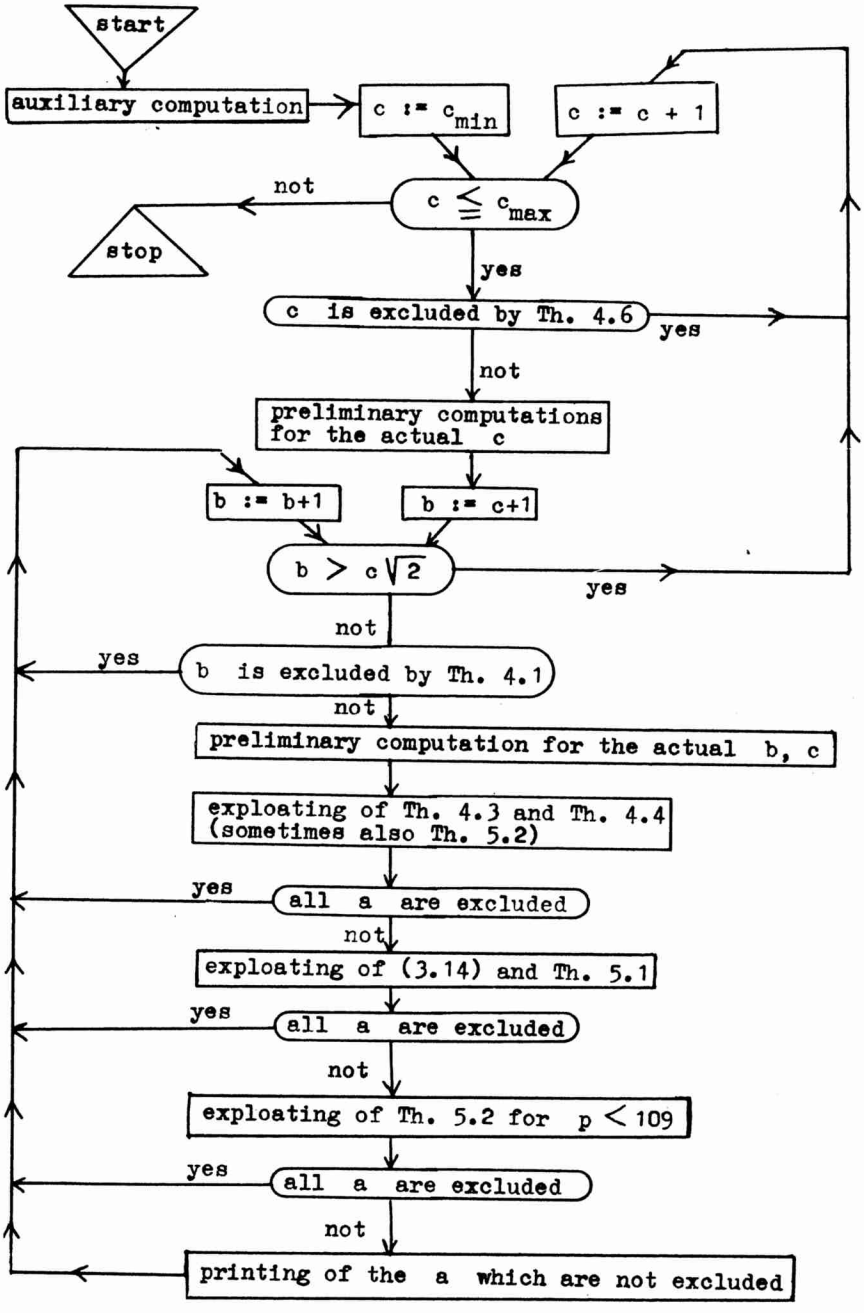
start
auxiliary computation
c := c_{min}
c := c + 1
not
$c \leqq c_{max}$
stop
yes
c is excluded by Th. 4.6
yes
not
preliminary computations for the actual c
b := b+1
b := c+1
$b > c\sqrt{2}$
yes
not
yes
b is excluded by Th. 4.1
not
preliminary computation for the actual b, c
exploating of Th. 4.3 and Th. 4.4 (sometimes also Th. 5.2)
yes
all a are excluded
not
exploating of (3.14) and Th. 5.1
yes
all a are excluded
not
exploating of Th. 5.2 for $p < 109$
yes
all a are excluded
not
printing of the a which are not excluded

Figure 1

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. Comen., 38 (1981), 119—127.
[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] Sierpinski, W.: Teoria liczb, Warszawa—Wroclaw, 1950.
[5] Spohn, W. G.: On the integral cuboid, Amer. Math. Monthly 79 (1972), 57—59.
[6] Spohn, W. G.: On the derived cuboid, Canad. Math. Bull. 17 (1974), 575—577.

Author's address:

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

Received: 29. 5. 1980

РЕЗЮМЕ

МАЛЫЙ СОВЕРШЕННЫЙ РАЦИОНАЛЬНЫЙ КУБОИД НЕ СУЩЕСТВУЕТ

Иван Корец, Братислава

Прямоугольный параллелепипед называется совершенным рациональным кубоидом, если длины всех его ребер, его диягонали и диагоналей всех его граней являются целыми числами. Совершенный рациональный кубоид существует тогда и только тогда когда существуют положительные целые числа a, b, c, d, v для которых имеет место (3.5), (3.8), (3.12), (3.14) и (3.15). Доказываются некоторые следствия этих условий. Например, если p простой делитель числа c и $p \equiv 3 \pmod 4$, $p^2 \nmid c$, то $a \equiv \pm c \pmod{p^3}$. С помощью этих следствий и с использованием ЭВМ доказывается, что условия (3.5)—(3.15) не вышолняются для $c \leqq 3200$. Как следствие получается, что длина каждого ребра совершенного рационального кубоида (если такой вообхе сухествует) больше или равна 10 000.

SÚHRN

NEEXISTENCIA MALÉHO PYTAGOREJSKÉHO KVÁDRA

Ivan Korec, Bratislava

S použitím samočinného počítača sa dokazuje, že neexistuje pytagorejský kváder (t. j. kváder, v ktorom dĺžky všetkých hrán i uhlopriečok sú celé čísla) s dĺžkou najkratšej hrany menšou alebo rovnou 10 000.