COMPLETE SOLUTION OF A PROBLEM OF DIOPHANTUS AND EULER

ANDREJ DUJELLA[*] AND CLEMENS FUCHS[‡]

Abstract. In this paper, we prove that there does not exist a set of four positive integers with the property that the product of any two of its distinct elements plus their sum is a perfect square. This settles an old problem investigated by Diophantus and Euler.

1. Introduction

Let n be an integer. A set of m positive integers is called a Diophantine m-tuple with the property $D(n)$ or simply $D(n)$-m-tuple, if the product of any two of them increased by n is a perfect square. For the case $n = 1$ this problem was first studied by Diophantus and he found a set of four positive rationals with the above property: $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. The first $D(1)$-quadruple however, the set $\{1, 3, 8, 120\}$, was found by Fermat. Euler was able to add the fifth positive rational, $\frac{777480}{8288641}$, to the Fermat's set (see [4] and [16]). Gibbs [15] found examples of sets of six positive rationals with the property of Diophantus. The folklore conjecture is that there does not exist a $D(1)$-quintuple. In 1969, Baker and Davenport [1] proved that the Fermat's set cannot be extended to a $D(1)$-quintuple. Recently, the first author proved that there does not exist a $D(1)$-sextuple and there are only finitely many $D(1)$-quintuples (see [11]).

In the case $n = -1$, the conjecture is that there does not exist a $D(-1)$-quadruple (see [6]). It is known that some particular $D(-1)$-triples cannot be extended to $D(-1)$-quadruples, namely this was verified for the triples $\{1, 2, 5\}$ (by Brown in [3], see also [23, 19, 22, 20]), $\{1, 5, 10\}$ (by Mohanty and Ramasamy in [21]), $\{1, 2, 145\}$, $\{1, 2, 4901\}$, $\{1, 5, 65\}$, $\{1, 5, 20737\}$, $\{1, 10, 17\}$, $\{1, 26, 37\}$ (by Kedlaya [19]) and $\{17, 26, 85\}$ (again by Brown in [3]). Moreover, Brown proved that the following infinite families of $D(-1)$-triples cannot be extended to quadruples:

$$\begin{array}{lll} \{x^2+1, (x+1)^2+1, (2x+1)^2+4\}, & \text{if} \quad x \not\equiv 0 & \pmod 4, \\ \{2, 2x^2+2x+1, 2x^2+6x+5\}, & \text{if} \quad x \equiv 1 & \pmod 4. \end{array}$$

[*] The first author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 0037110.

[‡] The second author was supported by the Austrian Science Foundation FWF, grant S8307-MAT.

The first author proved the conjecture in [7] for all triples of the form $\{1, 2, c\}$.

Let us mention that from [10, Theorem 4] it follows that there does not exist a $D(-1)$-33-tuple. This is the best known upper bound for this problem at present.

The $n = -1$ case is closely connected with an old problem of Diophantus and Euler. Namely, Diophantus studied the problem of finding numbers such that the product of any two increased by the sum of these two gives a square. He found two triples $\{4, 9, 28\}$ and $\{\frac{3}{10}, \frac{21}{5}, \frac{7}{10}\}$ satisfying this property. Euler found a quadruple $\{\frac{5}{2}, \frac{9}{56}, \frac{9}{224}, \frac{65}{224}\}$ and asked if there is an integer solution of this problem (see [5], [4] and [16]). In [9] an infinite family of rational quintuples with the same property was given. Since

$$xy + x + y = (x + 1)(y + 1) - 1,$$

we see that the problem of finding integer m-tuples with the property that for any two distinct elements the product plus their sum is a perfect square is equivalent to finding $D(-1)$-m-tuples.

A polynomial variant of the above problems was first studied by Jones [17], [18], and it was for the case $n = 1$. Recently, polynomial variants were also studied by the authors. They were able to completely prove the polynomial variants of both conjectures for $n = 1$ (here even a stronger version of the quintuple conjecture was proved since the question of finding polynomial quintuples was answered with the result in [11]) in [13] and also for the case $n = -1$ in [12].

In this paper we completely solve the problem investigated by Diophantus and Euler, namely we prove the following result:

Theorem 1a. *There does not exist a set of four positive integers with the property that the product of any two if its distinct elements plus their sum is a perfect square.*

By the above correspondence this implies the following equivalent result on $D(-1)$-m-tuples.

Theorem 1b. *There does not exist a $D(-1)$-quadruple $\{a, b, c, d\}$ with $2 \leq a < b < c < d$.*

In the proof of the above Theorem we first show that if $\{a, b, c, d\}$ is a $D(-1)$-quadruple with minimal d, then $\{1, a, b, c\}$ is also a $D(-1)$-quadruple. This idea was introduced for polynomials already in [12] when we proved the conjecture for polynomials with integral coefficients.

We have the following corollaries, which immediately follow from the above theorems.

Corollary 1. *There does not exist a $D(-1)$-quintuple.*

Moreover, we can state the following restrictions for $D(-1)$-quadruples:

Corollary 2. *If $\{a, b, c, d\}$ is a $D(-1)$-quadruple with $0 < a < b < c < d$, then $a = 1$ and $b \geq 5$.*

It seems that the case $a = 1$ is more involved and much harder. It can be compared with the strong version of the quintuple conjecture for $n = 1$, which says that every $D(1)$-triple can be extended to a $D(1)$-quadruple in an essentially unique way.

We also want to remark that for general n, it was proven by the first author in [6] that if $n \not\equiv 2 \pmod 4$ and $n \notin S = \{-4, -3, -1, 3, 5, 12, 20\}$, then there exists at least one Diophantine quadruple with the property $D(n)$. The conjecture is that for $n \in S$ there does not exist a Diophantine quadruple with the property $D(n)$. This paper gives support to this conjecture for the case $n = -1$.

The strategy of the paper follows the same line as the proofs of almost all other recent results on non-extendability of $D(n)$-m-tuples (especially we will follow the line of [11]). In Section 1 we reduce the problem of finding d which extends $\{a, b, c\}$ to a $D(-1)$-quadruple to a system of simultaneous Pellian equations, which leads to the consideration of intersections of linear recurring sequences. Afterwards we apply congruence relations to show that these sequences cannot have intersections for small indices (in Section 2 we prove that the indices are easily related and in Section 3 we consider the small cases), which leads to a "gap principles", which say that in such a triple there must be a certain gap between b and c (Section 3). Using this gap principle and a theorem about simultaneous approximations of square roots which are close to 1 due to Bennett, we obtain in Section 4 an upper bound for d. Comparing this upper bound with lower bounds obtained by congruence methods we show that such an extension does not exist, which is done on Section 5.

The new ideas in this paper are the following: we explore the assumption that the quadruple $\{a, b, c, d\}$ is minimal and we consider the associated quadruple $\{1, a, b, c\}$ first (observe that we assume that $a \geq 2$), which exists as mentioned above (and this idea comes from the much easier polynomial case handled in our paper [12]). Here we show that we have an excellent "gap principle", namely $c > 40000b^9$. Now this gap is good enough to apply Bennett's theorem and it is also good enough to apply the congruence method introduced in [14]. Here we need to have control on the fundamental solutions of the Pellian equations under consideration. We get upper bounds for them, which are better than in general, again from the fact that $\{1, a, b, c\}$ is also a $D(-1)$-quadruple.

2. Reduction to intersections of recursive sequences

Let $\{a, b, c\}$, where $2 \le a < b < c$, be a $D(-1)$-triple and let r, s, t be positive integers defined by

$$ab - 1 = r^2,\ ac - 1 = s^2,\ bc - 1 = t^2.$$

In this paper, the symbols r, s, t will always have this meaning. Assume that there exists a positive integer $d > c$ such that $\{a, b, c, d\}$ is a $D(-1)$-quadruple. We have

$$ad - 1 = x^2,\ bd - 1 = y^2,\ cd - 1 = z^2, \tag{1}$$

with integers x, y, z. Eliminating d from (1) we obtain the following system of Pellian equations

$$az^2 - cx^2 = c - a, \tag{2}$$

$$bz^2 - cy^2 = c - b. \tag{3}$$

We will describe the sets of solutions of equations (2) and (3) in the following lemma.

Lemma 1. *If (z, x) and (z, y), with positive integers x, y, z, are solutions of (2) and (3) respectively, then there exist integers z_0, x_0 and z_1, y_1 with*

(i) *(z_0, x_0) and (z_1, y_1) are solutions of (2) and (3) respectively,*

(ii) *the following inequalities are satisfied:*

$$0 \le |x_0| < s, \tag{4}$$

$$0 < z_0 < c, \tag{5}$$

$$0 \le |y_1| < t, \tag{6}$$

$$0 < z_1 < c, \tag{7}$$

and there exist integers $m, n \ge 0$ such that

$$z\sqrt{a} + x\sqrt{c} = (z_0\sqrt{a} + x_0\sqrt{c})(s + \sqrt{ac})^{2m}, \tag{8}$$

$$z\sqrt{b} + y\sqrt{c} = (z_1\sqrt{b} + y_1\sqrt{c})(t + \sqrt{bc})^{2n}. \tag{9}$$

Proof. The proof runs along the same line as the proof of [8, Lemma 1]. A polynomial version of this lemma was proved in [12, Lemma 1]. □

The solutions z arising, for given (z_0, x_0), from formula (8) for varying $m \ge 0$ form a binary recurrent sequence $(v_m)_{m\ge0}$ whose initial terms are found by solving equation (8) for z when $m = 0$ and 1, and whose characteristic equation has the roots $(s + \sqrt{ab})^2$ and $(s - \sqrt{ab})^2$. Therefore, we conclude that $z = v_m$ for some (z_0, x_0) with the above properties and integer $m \geq 0$, where

$$v_0 = z_0, \; v_1 = (2ac-1)z_0 + 2scx_0, \; v_{m+2} = (4ac-2)v_{m+1} - v_m. \tag{10}$$

In the same manner, from (9), we conclude that $z = w_n$ for some (z_1, y_1) with the above properties and integer $n \geq 0$, where

$$w_0 = z_1, \; w_1 = (2bc-1)z_1 + 2tcy_1, \; w_{m+2} = (4bc-2)w_{n+1} - w_n. \tag{11}$$

Now the following congruence relations follow easily from (10) and (11) by induction:

$$v_m \equiv (-1)^m z_0 \pmod{2c}, \quad w_n \equiv (-1)^n z_1 \pmod{2c}.$$

From this relations it follows immediately (since $z_0 + z_1 < 2c$) that if the equation $v_m = w_n$ has a solution, then we must also have

$$z_0 = z_1.$$

Moreover, we can also conclude that m and n have the same parity, i.e.

$$m \equiv n \pmod{2}. \tag{12}$$

Furthermore, important relations are obtained by considering the sequences (v_m) and (w_n) modulo c^2. This method was first introduced by Pethő and the first author in [14].

Lemma 2. *We have*

$$\begin{aligned} v_m &\equiv (-1)^m (z_0 - 2acm^2 z_0 - 2csmx_0) \pmod{8c^2}, \\ w_n &\equiv (-1)^n (z_1 - 2bcn^2 z_1 - 2ctny_1) \pmod{8c^2}. \end{aligned}$$

Proof. The proof follows immediately by induction from (10) and (11), respectively. □

From this lemma we can at once conclude that, if $v_m = w_n$ then

$$am^2 z_0 + smx_0 \equiv bn^2 z_1 + tny_1 \pmod{4c}. \tag{13}$$

The next important step is to show that to a $D(-1)$-quadruple $\{a, b, c, d\}$ with $2 \leq a < b < c < d$ another $D(-1)$-quadruple can be associated. By assuming that $\{a, b, c, d\}$ has minimal d under all such $D(-1)$-quadruples, we will conclude that $\{1, a, b, c\}$ is also a $D(-1)$-quadruple.

First we need the following lemma, which is now easy to prove and which will play a key role in the rest of the proof. A polynomial version of this lemma was obtained in [12].

Lemma 3. *Let $\{a, b, c, d\}$ with $0 < a < b < c < d$ be a $D(-1)$-quadruple. Then there exists a positive integer d_0 with $d_0 < c$ such that $ad_0 - 1$, $bd_0 - 1$, $cd_0 - 1$ are perfect squares.*

Proof. We look for a positive integer d such that $z^2 = v_m^2 = w_n^2 = cd - 1$. Therefore, $v_m^2 \equiv -1 \pmod{c}$. Hence, $z_0^2 \equiv -1 \pmod{c}$. Now, we define

$$d_0 = \frac{z_0^2 + 1}{c}.$$

It is easy to check that $d_0 < c$ and that $ad_0 - 1 = y_1^2, bd_0 - 1 = x_0^2$, which implies that $ad_0 - 1, bd_0 - 1, cd_0 - 1$ are perfect squares. □

Assume now that $\{a, b, c, d\}$ with $2 \leq a < b < c < d$ is a $D(-1)$-quadruple with minimal d among all such quadruples. We may use Lemma 4 to construct d_0. From the minimality of d, it follows that $d_0 = 1$ must hold and therefore $\{1, a, b, c\}$ is also a $D(-1)$-quadruple.

This has another important implication on the size of the fundamental solutions of (10) and (11) described in Lemma 1.

Lemma 4. *Let the integers z_0, z_1, x_0, y_1 be as in Lemma 1. Then we have*

$$z_0 = z_1 = \sqrt{c-1}, \quad |x_0| = \sqrt{a-1}, \quad |y_1| = \sqrt{b-1}.$$

Proof. Since we have

$$1 = d_0 = \frac{z_0^2 + 1}{c},$$

we immediately can conclude that

$$z_0 = z_1 = \sqrt{c-1}.$$

Also, by $x_0^2 = ad_0 - 1, y_1^2 = ad_0 - 1$, we get $|x_0| = \sqrt{a-1}, |y_1| = \sqrt{b-1}$, as claimed in the lemma. □

From the fact that $\{1, a, b, c\}$ is again a $D(-1)$-quadruple we can conclude that

$$a = \alpha^2 + 1, \quad b = \beta^2 + 1, \quad c = \gamma^2 + 1.$$

Moreover, to the $D(-1)$-triple $\{1, a, b\}$ we can again associate a pair of Pellian equations as above, which give all extensions to quadruple, as for example c. Moreover, we can associate two linear recursive sequences $(\tilde{v}_m)$ and $(\tilde{w}_n)$ to the triple, such that every solution $\tilde{v}_m = \tilde{w}_n$ gives us an extension of $\{1, a, b\}$ to a $D(-1)$-quadruple. We have

$$\tilde{v}_0 = \tilde{z}_0, \ \tilde{v}_1 = (2b-1)\tilde{z}_0 + 2\beta b\tilde{x}_0, \ \tilde{v}_{m+2} = (4b-2)\tilde{v}_{m+1} - \tilde{v}_m. \tag{14}$$

and

$$\tilde{w}_0 = \tilde{z}_1, \ \tilde{w}_1 = (2ab-1)\tilde{z}_1 + 2rb\tilde{y}_1, \ \tilde{w}_{m+2} = (4ab-2)\tilde{w}_{n+1} - \tilde{w}_n, \tag{15}$$

with

$$0 < \tilde{z}_0 = \tilde{z}_1 < b, \quad |\tilde{x}_0| < \beta, \quad |\tilde{y}_1| < r.$$

We also know that we have $\gamma = \tilde{v}_m = \tilde{w}_n$ for certain values of m and n.

3. Relationships between m and n

In this section we will prove an unconditional relationship between m and n, which will be used several times later on.

Lemma 5. *If $v_m = w_n$, then $n \le m \le 2n$.*

Proof. We have the following estimates for v_1:

$$\begin{aligned} v_1 &= (2ac-1)z_0 + 2scx_0 \ge (2ac-1)z_0 - 2sc|x_0| \\ &= \frac{(4a^2c^2-4ac+1)z_0^2 - 4c^2(ac-1)x_0^2}{(2ac-1)z_0+2sc|x_0|} \ge \frac{4c(ac-1)(az_0^2-cx_0^2)+z_0^2}{(2ac-1)z_0+2sc|x_0|} \\ &> \frac{4c(ac-1)(c-a)+z_0^2}{2(2ac-1)z_0} > \frac{4c(ac-1)(c-a)}{4ac(c-1)} > c-a, \end{aligned}$$

where we have used (2). On the other side we trivially have

$$v_1 \le 4ac^2.$$

Hence,

$$(c-a)(4ac-3)^{m-1} < v_m < 4ac^2(4ac-2)^{m-1}, \quad \text{for } m \ge 1. \tag{16}$$

In the same manner, we obtain

$$(c-b)(4bc-3)^{n-1} < w_n < 4bc^2(4bc-2)^{n-1}, \quad \text{for } n \ge 1. \tag{17}$$

Now, by comparing the lower bound for v_m with the upper bound of w_n and vice versa we will obtain the bounds.

We have

$$(4ac-2)^{n-1} < (c-b)(4bc-3)^{n-1} < 4ac^2(4ac-2)^{m-1} < (4ac-2)^{m+1}$$

and therefore

$$m+1 > n-1,$$

which implies $m > n-2$ or $m \ge n-1$. Since m, n have the same parity (see (12)), we conclude $m \ge n$.

Moreover, we have

$$(c-a)(4s^2)^{m-1} = (c-a)(4ac-4)^{m-1} < (c-a)(4ac-3)^{m-1} < 4bc^2(4bc-2)^{n-1}.$$

It is easy to see that we have

$$4bc-2 < 4s^4$$

and

$$\frac{4bc^2}{c-a} < 8s^4,$$

which is true because we have

$$4bc^2 \le 4(c-2)c^2 < 8(c-1)^3 \le 8(c-a)(ac-1)^2 = 8(c-a)s^4.$$

We have used here, that the function $f(x) = (c-x)(cx-1)^2$ for integers $1 \le x \le c-1$ takes it minimum at $x = 1$. Thus, we have

$$(4s^2)^{m-1} < 8s^4(4s^4)^{n-1},$$

which implies

$$2(m-1) < 4 + 4(n-1).$$

Observe that for the exponent of 4, we have $m - 1 < \frac{3}{2} + n - 1$, which is always satisfied with the above inequality. Therefore, we conclude $m < 2n + 1$ or $m \leq 2n$ and therefore we get what we have claimed. □

The result from above is also true for $D(-1)$-triples $\{a, b, c\}$ with $0 < a < b < c$, where possibly $a = 1$.

Lemma 6. *If $\tilde{v}_m = \tilde{w}_n$, then $n \leq m \leq 2n$.*

Proof. The proof of Lemma 5 does not use the fact that $a \geq 2$ and therefore the same is true for the sequences $\tilde{v}_m$ and $\tilde{w}_n$ which come from the triple $\{1, a, b\}$. □

4. Gap principles

In this section we will prove that for our $D(-1)$-triple $\{a, b, c\}$, we have a large gap between b and c of the form $c > b^9$. This will be essential for the proof of the theorems. We get this result by studying the associated $D(-1)$-quadruple given by $\{1, a, b, c\}$.

Before we do this, we need the following useful gap principle for the elements of an arbitrary $D(-1)$-triple $\{a_1, a_2, a_3\}$.

Lemma 7. *If $\{a_1, a_2, a_3\}$ is a $D(-1)$-triple and $0 < a_1 < a_2 < a_3$, then $a_3 = a_1 + a_2 + 2\sqrt{a_1 a_2 - 1}$ or $a_3 > 3a_1 a_2 \geq 3a_2$.*

Proof. It follows from [10, Lemma 3] that there exist integers e, f, g such that we have

$$a_3 = a_1 + a_2 - e + 2(a_1 a_2 e + \sqrt{a_1 a_2 - 1} fg), \tag{18}$$

with $a_1 e + 1 = f^2, a_2 e + 1 = g^2$. Moreover, since we may take (see [10, Lemma 3])

$$\begin{aligned} f &= a_1 \sqrt{a_1 a_3 - 1} - \sqrt{a_1 a_2 - 1}\sqrt{a_2 a_3 - 1} \quad \text{and} \\ g &= a_2 \sqrt{a_2 a_3 - 1} - \sqrt{a_1 a_2 - 1}\sqrt{a_2 a_3 - 1}, \end{aligned}$$

it is easy to check that f, g are positive.

We have two cases: if $e = 0$, then the above equation gives

$$a_3 = a_1 + a_2 + 2\sqrt{a_1 a_2 - 1},$$

which is the first part of our assertion. Otherwise, we have $e \geq 1$. If $a_1 = 1$ we get $e \geq 3$ and therefore (18) implies $a_3 \geq 7a_1 a_2$. In the case $a_1 = 2$, we have $e \geq 4$ and therefore $a_3 \geq 8a_1 a_2$. Now, if $a_1 \geq 3$, again by (18), we can estimate a_3 by

$$\begin{aligned} a_3 &\geq 2a_1 a_2 + 2\sqrt{a_1 a_2 - 1}\sqrt{a_1 a_2 - a_1 - a_2 + 1} \\ &> 2a_1 a_2 + 2(a_1 a_2 - a_1 - a_2 + 1) > 3a_1 a_2, \end{aligned}$$

where the last inequality is true because of $a_1a_2 > 2a_1 + 2a_2 - 2$ or $(a_1 - 2)(a_2 - 2) \geq 2$.

Altogether, we have

$$a_3 > 3a_1a_2 \geq 3a_2,$$

which was the statement of the lemma. □

We are intended to prove that the equation

$$\tilde{v}_m = \tilde{w}_n \tag{19}$$

does not have a solution for small m, n (besides the trivial solution $\tilde{v}_0 = \tilde{w}_0$ which leads to some extension $d_0 < b$). We will show that if (19) has a solution, then

$$m > 4 \text{ or } n > 4$$

holds. By the relation between m and n proved in the last section (Lemma 6), we have to consider the following cases:

$$\begin{aligned} n &= 1, \quad m = 1, \\ n &= 2, \quad m = 2 \text{ or } 4, \\ n &= 3, \quad m = 3, \\ n &= 4, \quad m = 4. \end{aligned}$$

We will show this separately in the lemmas below.

Lemma 8. *We have* $\tilde{v}_1 \neq \tilde{w}_1$.

Proof. From the definition of the sequences it follows that we have

$$(2b - 1)\tilde{z}_0 + 2\beta b\tilde{x}_0 = (2ab - 1)\tilde{z}_1 + 2rb\tilde{y}_1.$$

We have $\tilde{z}_0 = \tilde{z}_1$. Therefore, by dividing by $2b$ we get

$$(a - 1)\tilde{z}_0 = \beta\tilde{x}_0 - r\tilde{y}_1. \tag{20}$$

We remark that the system of Pellian equations associated to the triple $\{1, a, b\}$ was given by

$$\begin{aligned} \tilde{z}_0^2 - b\tilde{x}_0^2 &= b - 1, \\ a\tilde{z}_0^2 - b\tilde{y}_1^2 &= b - a \end{aligned}$$

which implies

$$(a - 1)\tilde{z}_0^2 - b(\tilde{y}_1^2 - \tilde{x}_0^2) = 1 - a.$$

Squaring (20) and using the last relation, we get

$$(a - 1)b(\tilde{y}_1^2 - \tilde{x}_0^2) - (a - 1)^2 = (b - 1)\tilde{x}_0^2 + (ab - 1)\tilde{y}_1^2 - 2\beta r\tilde{x}_0\tilde{y}_1.$$

Hence,

$$(\tilde{x}_0 r - \tilde{y}_1\beta)^2 = \tilde{x}_0^2 r^2 + \tilde{y}_1^2\beta^2 - 2\beta r\tilde{x}_0\tilde{y}_1 = -(a - 1)^2,$$

which is a contradiction, since the left side is positive and the right hand side of this equation is negative. Therefore, the lemma follows. □

Up to now we have shown that $n, m \geq 2$. Our strategy is now the following: we use Lemma 4 to prove that there exists a certain gap between a and b.

Using this gap principle and the congruence relations from Lemma 2, we obtain larger lower bounds for m, n. We will repeat this until we end up with $n > 4$ or $m > 4$. First, we have the following lemma:

Lemma 9. *If* $\{1, a_2, a_3, a_4\}$ *is a* $D(-1)$*-quadruple and* $1 < a_2 < a_3 < a_4$, *then*

$$a_4 > 4a_2^{1.5}a_3^{2.5}.$$

Proof. As in Section 2, we can associate to the triple $\{1, a_2, a_3\}$ two sequences (v_m) and (w_n) with the above properties such that a_4 comes from some solution $z = v_m = w_n$ for certain indices $n, m \geq 1$ by the formula $a_3a_4 = z^2 + 1$. For every possible solution $z = w_n = v_m$, we can now conclude by Lemma 7 that

$$z \geq w_2 \geq \begin{cases} \frac{a_3}{2} \cdot 3a_2a_3 \geq \frac{3}{2}a_2a_3^2 & \text{if } a_3 > 2a_2 \\ \sqrt{a_3} \cdot 3a_2a_3 \geq 3a_2a_3\sqrt{a_3} & \text{if } a_3 < 2a_2 \end{cases}$$

Because of the relation $a_3a_4 - 1 = z^2$, we have

$$a_4 \geq \begin{cases} \frac{9}{4}a_2^2a_3^3 & \text{if } a_3 > 2a_2, \\ 9a_2^2a_3^2 \geq \frac{9}{2}a_2^{1.5}a_3^{2.5} & \text{if } a_3 < 2a_2. \end{cases}$$

This implies that

$$a_4 > 4a_2^{1.5}a_3^{2.5}.$$

From this the conclusion follows. □

Using this improved gap principle, we now can prove the next step, which is in fact the hardest one.

Lemma 10. *We have* $\tilde{v}_2 \neq \tilde{w}_2$.

Proof. First we can apply Lemma 4 to the triple $\{1, a, b\}$ and we conclude that there exists $d_0 < b$ such that $d_0 - 1, ad_0 - 1$ and $bd_0 - 1$ are all perfect squares. We have two cases depending on whether $d_0 = 1$ or not.

Case $d_0 = 1$: We have

$$\tilde{z}_0 = \beta, \quad \tilde{x}_0 = 0, \quad \tilde{y}_1 = \pm\alpha.$$

It follows that we have just three sequences to consider, namely $(\tilde{v}_m)$ corresponding to $\tilde{x}_0 = 0$ and two sequences $(\tilde{w}_n)$ and $(\tilde{w}'_n)$ corresponding to the case $\tilde{y}_1 = \alpha$ and $-\alpha$, respectively.

We pause for a moment to show some properties of the sequences $(\tilde{v}_m)$ and $(\tilde{w}_n), (\tilde{w}'_n)$. By the proof of Lemma 1 in [8] it follows that $\tilde{v}_0 \leq \tilde{v}_1$. By induction using (10) we immediately conclude that $\tilde{v}_0 \leq \tilde{v}_1 \leq \tilde{v}_2 \leq \ldots$. The same is true for $(\tilde{w}_n)$, so $\tilde{w}_0 \leq \tilde{w}_1 \leq \tilde{w}_2 \leq \ldots$ and $(\tilde{w}'_n)$, hence, $\tilde{w}'_0 \leq \tilde{w}'_1 \leq \tilde{w}'_n \leq \ldots$. Furthermore, we trivially have $\tilde{w}'_n \leq \tilde{w}_n$ for all $n \geq 0$. Moreover, for $\tilde{y}_1 = +\alpha$, we have

$$\tilde{v}_m < \tilde{w}_m, \quad \text{for all } m \geq 1, \tag{21}$$

which follows again by induction.

From this discussion it follows that for $\tilde{y}_1 = \alpha$ we have $\tilde{v}_2 \neq \tilde{w}_2$, and therefore we just have to consider $\tilde{y}_1 = -\alpha$ and therefore only the sequence $(\tilde{w}'_n)$.

Next, we calculate an upper bound for $(\tilde{v}_m)$. We have

$$\tilde{v}_m < (4b)^{m-1} 2b\sqrt{b}, \quad m \geq 1, \tag{22}$$

which can be easily seen by induction. Moreover, we need a lower bound for $(\tilde{w}'_n)$. We have $\tilde{w}_1 \leq 4ab\sqrt{b}$. Moreover,

$$\begin{aligned} \tilde{w}_1 \tilde{w}'_1 &= -4a^2b^2 + 4ab + b - 1 + 4ab^3 - 4b^2 \\ &> 4ab^3 - 4a^2b^2 - 4b^2 + 4ab \geq \frac{7}{3}ab^3. \end{aligned}$$

For the last inequality we have used that

$$4a^2b^2 + 4b^2 - 4ab \leq \frac{5}{3}ab^3,$$

which is true under the assumption that $b > 3a$, which we will assume for the moment. Combining the upper bound for $\tilde{w}_1$ with the lower bound for $\tilde{w}_1\tilde{w}'_1$ we get

$$\tilde{w}'_1 > \frac{7}{12} b\sqrt{b}.$$

Proceeding with induction we end up with

$$\tilde{w}'_n > (3ab)^{n-1} \frac{7}{12} b\sqrt{b}, \quad n \geq 1. \tag{23}$$

Now by comparing the upper bound from (22) with the lower bound from (23) with $(n, m) = (2, 2)$, we get

$$(3ab)\frac{7}{12} b\sqrt{b} > (4b)2b\sqrt{b},$$

which is true for all $a \geq 5$. We remark that in [7] it was proven that the pair $\{1, 2\}$ cannot be extended to a $D(-1)$-quadruple, therefore we may assume that $a \geq 5$ holds. In the same way we can prove that

$$\tilde{v}_m < \tilde{w}'_m \quad \text{for all } m \geq 1, \tag{24}$$

since we have

$$(3ab)^{m-1} \frac{7}{12} b\sqrt{b} > (4b)^{m-1} 2b\sqrt{b},$$

which implies

$$a > \frac{4}{3} \left(\frac{24}{7}\right)^{\frac{1}{m-1}},$$

which is again true since $a \geq 5$.

It remains to consider $b \leq 3a$. In this case we can conclude by the gap principle (Lemma 7) applied to the triple $\{1, a, b\}$ that we have

$$\begin{aligned} b &= a + 2\sqrt{a-1} + 1, \\ a &= b - 2\sqrt{b-1} + 1, \\ \beta &= \sqrt{b-1}, \\ r &= b - \beta = b - \sqrt{b-1}. \end{aligned}$$

Now, if we assume that $\tilde{v}_2 = \tilde{w}_2$, then by (13) we get

$$4\beta \equiv 4(b - 2\beta + 1)\beta - 2(b - \beta)\alpha \pmod{4b}.$$

Therefore,

$$4\beta \equiv -8\beta^2 + 4\beta - 2\beta\alpha \equiv 8 + 4\beta - 2\beta\alpha \pmod{4b}.$$

Hence, we may conclude

$$2\alpha\beta \equiv 8 \pmod{4b},$$

which by $2\alpha\beta = 2\sqrt{a-1}\sqrt{b-1} < 2b$ implies that in fact equality must hold, implying that $2\alpha\beta = 8$ or $\alpha\beta = 4$, which is trivially a contradiction.

Altogether, the proof of the first case is finishes.

Case $d_0 \neq 1$: Now, we look back to our quadruple $\{1, a, d_0, b\}$. Since $d_0 \neq 1$, we can apply our improved gap principle from Lemma 9 and we get

$$b > 4a^{2.5}d_0^{1.5}.$$

From this it follows that

$$b^{2.5} > 4a^{2.5}(bd_0)^{1.5} > 4a^{2.5}\tilde{z}_0^3,$$

or

$$a\tilde{z}_0 < \frac{b}{4^{\frac{2}{5}}\tilde{z}_0^{\frac{1}{5}}} < \frac{3}{5}b.$$

Now, we use again (13) and conclude that

$$4\tilde{z}_0 + 2\beta\tilde{x}_0 \equiv 4a\tilde{z}_0 + 2r\tilde{y}_1 \pmod{4b}.$$

Since $4a\tilde{z}_0$ is the largest term both sides can be bounded by $6a\tilde{z}_0 < 4b$, which follows by the above inequality, and therefore this inequality implies that we have in fact equality here. Thus,

$$2\tilde{z}_0 + \beta\tilde{x}_0 = 2a\tilde{z}_0 - r|\tilde{y}_1|,$$

because for $\tilde{y}_1 > 0$ we would trivially have a contradiction. This can be reformulated as

$$2(a-1)\tilde{z}_0 + \beta\tilde{x}_0 = -r|\tilde{y}_1|.$$

Now, since $\beta\tilde{x}_0 < (a-2)\tilde{z}_0$, which can be seen by squaring and using (14), we receive a contradiction again.

This finally finishes the proof of the lemma. □

Lemma 11. *We have $\tilde{v}_4 \neq \tilde{w}_2$.*

Proof. Again we use Lemma 4 to find a d_0 such that $\{1, a, d_0, b\}$ is a $D(-1)$-quadruple. As before we consider the two cases depending on whether $d_0 = 1$ or not.

Assuming $d_0 = 1$, we are intended to show that we have

$$\tilde{v}_4 > \tilde{w}_2 \geq \tilde{w}_2',$$

where the last inequality is trivially true. We have the following lower bound for $\tilde{v}_4$, which follows from (14), namely

$$\tilde{v}_4 \geq (3ab)^3 b\sqrt{b} \geq 27a^3b^4,$$

where we have used that $\tilde{v}_1 = (2b-1)\beta \geq b\sqrt{b}$. On the other side we have by (15)

$$\tilde{w}_2 \leq (4ab-2)\tilde{w}_1 \leq 16a^2b^3,$$

since we have $\tilde{w}_1 = (2ab-1)\beta + 2r^3b = 2ab\sqrt{b} + 2ab^2 \leq 4ab^2$. Comparing these bounds we trivially get what we want.

Now, we assume that $d_0 \neq 1$. By using (13) and the same estimate as above, we derive

$$16\tilde{z}_0 + 4\beta\tilde{x}_0 = 4a\tilde{z}_0 + 2r\tilde{y}_1 > 2a\tilde{z}_0.$$

Hence,

$$2\beta\tilde{x}_0 > (a-8)\tilde{z}_0,$$

which is trivially true if $a \leq 8$, which means $a = 5$. We will handle this case separately. Otherwise, we can square the above inequality and get

$$4\beta^2\tilde{x}_0^2 > (a-8)^2\tilde{z}_0^2 > (a-8)^2b\tilde{x}_0^2,$$

where we used for the last inequality the Pellian equation lying behind (14), which is $\tilde{z}_0^2 - b\tilde{x}_0^2 = b-1$. Dividing through $\tilde{x}_0^2$ we derive

$$4b - 4 > (a-8)^2b,$$

which is trivially a contradiction unless $5 < a < 10$. But in this range there are no numbers of the form $\alpha^2+1 = a$. Thus, we are left with the case $a = 5$. In this special case we have

$$16\tilde{z}_0 + 4\beta\tilde{x}_0 = 20\tilde{z}_0 + 2r\tilde{y}_1,$$

or

$$2(\tilde{z}_0 - \beta\tilde{x}_0) = -r\tilde{y}_1.$$

This equation implies, since $(\beta\tilde{x}_0)^2 = b\tilde{x}_0^2 - \tilde{x}_0^2 < \tilde{z}_0^2$, that $\tilde{y}_1 < 0$. Thus, we have

$$2\beta\tilde{x}_0 - r\tilde{y}_1 > 3\beta\tilde{x}_0 > 2\tilde{z}_0,$$

which is a contradiction. The last inequality follows from

$$(3\beta\tilde{x}_0)^2 = 9b\tilde{x}_0^2 - 9\tilde{x}_0^2 > 5b\tilde{x}_0^2 > 4b\tilde{x}_0^2 + 4b > 4\tilde{z}_0^2,$$

where we used once again $\tilde{z}_0^2 - b\tilde{x}_0^2 = b - 1$. Therefore, the claim of the lemma is proved. □

Now, we do the remaining two cases, namely $(m,n) = (3,3)$ or $(4,4)$ in the following lemma.

Lemma 12. *We have $\tilde{v}_3 \neq \tilde{w}_3$ and $\tilde{v}_4 \neq \tilde{w}_4$.*

Proof. We start as in the proof of the last lemma and consider the triple $\{1, a, d_0, b\}$. Again we have to consider the two cases $d_0 = 1$ and $d_0 \neq 1$.

Let us assume $d_0 = 1$ first. In Lemma 10 we have already proved that $\tilde{v}_3 < \tilde{w}_3' \leq \tilde{w}_3$ and $\tilde{v}_4 < \tilde{w}_4' \leq \tilde{w}_4$ unless $b \leq 3a$. In the latter case we have $b = a + 2\sqrt{a-1} + 1$. But now from (13) we get for the case $(m,n) = (3,3)$ that

$$9\beta \equiv 9\beta(-2\beta + 1) - 3\alpha(b - \beta) \pmod{4b},$$

which implies

$$0 \equiv 18 + 3\beta(\beta - 1) \pmod{b},$$

where we used that $\alpha = \beta - 1$ which is easy to verify. Since $\beta^2 \equiv -1 \pmod{b}$, we get

$$3\beta \equiv 15 \pmod{b},$$

and therefore $\beta = 5$. This implies $b = 26$ and $a = 26 - 2 \cdot 5 + 1 = 17$, thus we have the triple $\{1, 17, 26\}$. In this case we have $\tilde{z}_0 = 5, \tilde{y}_1 = -4, \tilde{x}_0 = 0$ and it is easy to check directly that for the completely concrete sequences $(\tilde{v}_m)$ and $(\tilde{w}_n')$, we have $\tilde{v}_3 < \tilde{w}_3' \leq \tilde{w}_3$.
In the same way we can handle the case $(m,n) = (4,4)$. We start with

$$16\beta \equiv 16a\beta - 4\alpha r$$

and conclude that $\beta = 7$ must hold. This gives $b = 50$ and $a = 50 - 2 \cdot 7 + 1 = 37$, and therefore the triple $\{1, 37, 50\}$. Here we have $\tilde{z}_0 = 7, \tilde{y}_1 = -6, \tilde{x}_0 = 0$, and we trivially get $\tilde{v}_4 < \tilde{w}_4' \leq \tilde{w}_4$. Therefore, the proof of the first case is finished.

Next, we assume that $d_0 \neq 1$. As in the proof of Lemma 10 we conclude by the improved gap principle (Lemma 9) that we have

$$b > 4a^{2.5}d_0^{1.5} > 8a^{2.5}.$$

From this we get by $bd_0 \geq \tilde{z}_0^2$ that $b^3 > 4a^{2.5}b^{0.5}\tilde{z}_0^3$ or

$$\tilde{z}_0 < \frac{2b}{3a^{\frac{5}{6}}b^{\frac{1}{6}}} = \frac{2b^{\frac{5}{6}}}{3a^{\frac{5}{6}}}.$$

First, we get for the case $(m,n) = (3,3)$ by (13) that

$$9\tilde{z}_0 + 3\beta\tilde{x}_0 \equiv 9a\tilde{z}_0 + 3r\tilde{y}_1 \pmod{4b}.$$

Both sides of this equation can be bounded by $12a\tilde{z}_0$. We want to show that this is $< 4b$. But this follows easily from

$$3a\tilde{z}_0 < 2a^{\frac{1}{6}}b^{\frac{5}{6}} < b,$$

since $b > 8a^{2.5} \geq 8 \cdot 5^{1.5}a > 89a > 2^6a$. From this it follows that we have equality in the above congruence relation. But the left hand side is bounded from above by $12a\tilde{z}_0$ and the right side is bounded from below by $6b\tilde{z}_0$, which show that

$$9\tilde{z}_0 + 3\beta\tilde{x}_0 < 12a\tilde{z}_0 < 6b\tilde{z}_0 < 9a\tilde{z}_0 + 3r\tilde{y}_1$$

and therefore this equation cannot hold.
We now turn to the case $(m,n) = (4,4)$. Here (13) reads

$$16\tilde{z}_0 + 4\beta\tilde{x}_0 \equiv 16a\tilde{z}_0 + 4r\tilde{y}_1 \pmod{4b}.$$

This time both sides are bounded by $20a\tilde{z}_0$ and we want to show that this is $< 4b$. This follows from

$$5a\tilde{z}_0 < \frac{10}{3}a^{\frac{1}{6}}b^{\frac{5}{6}} < b,$$

where we used as before

$$b > 4a^{2.5}d_0^{1.5} = 4a^{1.5}d_0^{1.5}a > 4 \cdot 5^{1.5} \cdot 10^{1.5}a > 1414a > \left(\frac{10}{3}\right)^6 a.$$

Observe that we have used that one of a, d_0 is ≥ 5 and the other one ≥ 10 since there is no number in between which is a perfect square plus one. As before, we conclude that we have equality in the above congruence equation, which leads to a contradiction since the left side is bounded from above by $20a\tilde{z}_0$ and the ride side is bounded from below by $12b\tilde{z}_0$. This concludes the proof of the lemma. □

As stated at the beginning of this section, we are now able to prove a much improved gap principle in the triple $\{a,b,c\}$ with which we started at the beginning.

Lemma 13. *Let $\{a,b,c,d\}$ be a $D(-1)$-quadruple with $2 \leq a < b < c < d$ and with minimal d under all such quadruples, then we have*

$$c > 40000b^9.$$

Proof. We know that in fact $\{1,a,b,c\}$ is a $D(-1)$-quadruple. From this it follows that $bc - 1 = z^2$ for an integer z with $z = \tilde{v}_m = \tilde{w}_n$ for certain integers m, n and by the lemmas in this section we can conclude that $m > 4$ or $n > 4$.

If we assume that $m > 4$, then we have

$$z \geq \tilde{v}_5 > (b-1)(4b-3)^4 > 200b^5,$$

and therefore

$$c = \frac{z^2+1}{b} \geq \frac{\tilde{v}_5 + 1}{b} > 40000b^9.$$

If we assume that $n > 4$, then we have:

$$z \geq \tilde{w}_5 > (b-a)(4ab-3)^4 > \frac{b}{2}(3ab)^4 > 40a^4b^5,$$

where we assumed that $b > 2a$ which gives $b - a > \frac{b}{2}$. It follows that

$$c = \frac{z^2+1}{b} \geq \frac{\tilde{w}_5^2+1}{b} > 1600a^8b^9 > 10^5b^9,$$

since $a \geq 2$.
Otherwise, we have $b - a = 2\sqrt{b-1} - 1 > \sqrt{b}$ by Lemma 7. In this case we get

$$z \geq \tilde{w}_5 > \sqrt{b} \cdot 81a^4b^4$$

and we conclude

$$c > 6400a^8b^8 > 32000a^7b^9 > 10^5b^9,$$

again since $a \geq 2$.

Putting these results together, we have proven that

$$c > 40000b^9,$$

which was the claim of our lemma. □

5. Lower bounds for m, n

The intention in this section is to prove that the gap principle from the last section implies that we can estimate m, n in terms of c from below. The idea is that if $v_m = w_n$, then we can study this equation modulo $8c^2$, which leads to equation (13). But if a, b, m, n are small compared with c, then these congruences are equations, which are in contradiction to the equation $v_m = w_n$. This will imply the lower bounds for m, n. We have the following lemma:

Lemma 14. *If $v_m = w_n$, then $m \geq n > c^{0.064}$.*

Proof. We start with the congruence (13) which is

$$am^2z_0 + smx_0 \equiv bn^2z_0 + tny_1 \pmod{4c}.$$

Let us assume that $n \leq c^{0.064}$. By Lemma 5 we have $m \leq 2c^{0.064} < c^{0.309}$ since $c \geq 17$. All terms in the above congruence are bounded by bm^2z_0. By our assumption, Lemma 4 and the gap principle $c > 40000b^9$ from Lemma 13, we get that

$$bm^2z_0 < \frac{4}{40000^{\frac{1}{9}}} c^{\frac{1}{9}+2\cdot 0.061+\frac{1}{2}} < c.$$

Hence,

$$am^2z_0 + smx_0 = bn^2z_0 + tny_1$$

or

$$z_0(am^2 - bn^2) = tny_1 - smx_0.$$

Squaring leads to

$$-(am^2 - bn^2)^2 \equiv -n^2y_1^2 - m^2x_0^2 - 2stmnx_0y_1 \pmod{c}$$

or

$$[(am^2 - bn^2)^2 - n^2y_1^2 - m^2x_0^2]^2 \equiv 4m^2n^2x_0^2y_1^2 \pmod{c}.$$

The left side is bounded by

$$[(bm^2)^2]^2 = b^4m^8 < 256b^4n^8 < 256b^4c^{0.064} < c$$

since we have $c > 40000b^9$, which implies that the above inequality is satisfied for $256b^4 < 176b^{4.392} < c^{0.488}$ which is true for $b > 2.6$. Also the right side is by Lemma 4 bounded by

$$4m^2n^2ab < 16n^4b^2 < 16b^2c^{0.256} < c.$$

Thus, we may conclude

$$(am^2 - bn^2)^2 = (ny_1 \pm mx_0)^2,$$

which gives

$$am^2 - bn^2 = \pm ny_1 \pm mx_0 \quad \text{or} \quad am^2 - bn^2 = \pm ny_1 \mp mx_0.$$

Therefore, we have

$$\begin{aligned} am^2z_0 - bn^2z_0 &= tny_1 - smx_0 = \pm ny_1z_0 \pm mx_0z_0, \quad \text{or} \\ am^2z_0 - bn^2z_0 &= tny_1 - smx_0 = \pm ny_1z_0 \mp mx_0z_0, \end{aligned}$$

which implies

$$mx_0(s \pm z_0) = ny_1(t \mp z_0) \quad \text{or} \quad mx_0(s \pm z_0) = ny_1(t \pm z_0).$$

Let us first consider the first equation. Squaring once again leads to

$$n^2y_1^2(bc - 1 \mp 2tz_0 + z_0^2) = m^2x_0^2(ac - 1 \pm 2sz_0 + z_0^2).$$

Taking this equation modulo c and multiplying by z_0 gives

$$n^2y_1^2(-2z_0 \pm 2t) \equiv m^2x_0^2(-2z_0 \mp 2s) \pmod{c}.$$

Both sides are bounded by

$$4m^2b^2\sqrt{bc} < 32c^{2\cdot 0.064+\frac{2}{9}+\frac{1}{2}+\frac{1}{18}} < c.$$

Thus, we have equality, which means

$$m^2x_0^2(z_0 \pm s) = n^2y_1^2(z_0 \mp t).$$

But by squaring the starting equation, we also have

$$m^2x_0^2(s \pm z_0)^2 = n^2y_1^2(t \mp z_0)^2,$$

and therefore by dividing this equation by the previous one we conclude that either $s + z_0 = z_0 - t$ or $z_0 - s = z_0 + t$, which gives a contradiction in both cases.

The second equation can be handled exactly in the same way as the first one, leading to

$$\begin{aligned} m^2x_0^2(z_0 \pm s) &= n^2y_1^2(z_0 \pm t), \\ m^2x_0^2(z_0 \pm s)^2 &= n^2y_1^2(z_0 \pm t)^2 \end{aligned}$$

and by dividing one equation through the other we get $z_0 \pm s = z_0 \pm t$, which is again a contradiction.

Therefore, the proof of the lemma is finished. □

6. Application of a theorem of Bennett

Now we are ready to calculate an upper bound for d in the $D(-1)$-quadruple $\{a,b,c,d\}$. For this we apply the following important and very useful result of Bennett [2].

Lemma 15. *If a_i, p_i, q and N are integers for $0 \leq i \leq 2$, with $a_0 < a_1 < a_2, a_j = 0$ for some $0 \leq j \leq 2$, q nonzero and $N > M^9$, where*

$$M = \max_{0 \leq i \leq 2}\{|a_i|\},$$

then we have

$$\max_{0 \leq i \leq 2}\left\{\left|\sqrt{1+\frac{a_i}{N}} - \frac{p_i}{q}\right|\right\} > (130N\gamma)^{-1}q^{-\lambda}$$

where

$$\lambda = 1 + \frac{\log(33N\gamma)}{\log\left(1.7N^2\prod_{0\leq i<j\leq 2}(a_i-a_j)^{-2}\right)}$$

and

$$\gamma = \begin{cases} \frac{(a-2-a_0)^2(a_2-a_1)^2}{2a_2-a_0-a_1} & \textit{if } a_2-a_1 \geq a_1-a_0, \\ \frac{(a_2-a_0)^2(a_1-a_0)^2}{a_1+a_2-2a_0} & \textit{if } a_2-a_1 < a_1-a_0. \end{cases}$$

We apply Lemma 15 to the numbers

$$\theta_1 = \frac{s}{a}\sqrt{\frac{a}{c}} = \sqrt{1-\frac{b}{abc}} \quad \text{and} \quad \theta_2 = \frac{t}{b}\sqrt{\frac{b}{c}} = \sqrt{1-\frac{a}{abc}}.$$

So θ_1 and θ_2 are square roots of rationals which are close to 1. First, we show that every solution of our problem induce good approximations of these numbers.

Lemma 16. *All positive integer solutions x, y, z of (2) and (3) satisfy*

$$\max\left\{\left|\theta_1 - \frac{sbx}{abz}\right|, \left|\theta_2 - \frac{tay}{abz}\right|\right\} < \frac{c}{a}z^{-2}.$$

Proof. This is a special case of Lemma 1 in [10]. □

By combining this lemma with the lower bound from the theorem of Bennett we obtain an upper bound for d.

Lemma 17. *Let $\{a,b,c,d\}$ be a $D(-1)$-quadruple with $2 \leq a < b < c < d$ and with minimal d, then*

$$d < c^{51.06}.$$

Proof. We apply Lemma 15 with $a_0 = -b, a_1 = -a, a_2 = 0, N = abc, M = b, q = abz, p_1 = sbx, p_2 = tay$. Since $abc > b^9$ by our gap principle (Lemma

13), the condition $N > M^9$ is satisfied. Considering γ from Lemma 15 as a function of a we easily get

$$\frac{b^3}{6} \leq \gamma < \frac{b^3}{2}.$$

Lemma 15 and Lemma 16 imply

$$\frac{c}{az^2} > (130abc\gamma)^{-1}(abz)^{\lambda_1 - 2},$$

where

$$\lambda_1 = \frac{\log(33abc\gamma)}{\log\left(1.7c^2(b-a)^2\right)}.$$

This gives

$$z^{\lambda_1} < 65a^2b^6c^2$$

and

$$\log z < \frac{\log(65a^2b^6c^2)\log(1.7c^2(b-a)^{-2})}{\log\left(\frac{1.7c}{33ab(b-a)^2\gamma}\right)}.$$

We have

$$\begin{aligned}
&65a^2b^6c^2 < 65b^8c^2 < \frac{65}{40000^{\frac{8}{9}}}c^{2+\frac{8}{9}} < c^{2.889},\\
&1.7c^2(b-a)^{-2} < c^2,\\
&\frac{1.7c}{33ab(b-a)^2\gamma} > \frac{1.7c}{33abb^2\frac{b^3}{2}} > 0.103cb^{-7} > 391c^{1-\frac{7}{9}} > c^{0.222}.
\end{aligned}$$

Therefore, we get

$$\log z < \frac{2.889\log c \cdot 2\log c}{0.222\log c} < 26.028\log c.$$

Hence,

$$z < c^{26.028} \tag{25}$$

and

$$d = \frac{z^2+1}{c} < c^{51.06},$$

which was the claim of the lemma. □

In the special case that a and b are very close, we can prove a better upper bound.

Lemma 18. *Let $\{a, b, c, d\}$ be a $D(-1)$-quadruple with $2 \leq a < b < c < d$ and with minimal d. If $b < 2a$, then*

$$d < c^{33.72}.$$

Proof. The proof runs the same line as the proof of the last lemma. By the assumption that $b < 2a$, we conclude by Lemma 7 applied to the $D(-1)$-triple $\{1, a, b\}$ that

$$a = b - 2\sqrt{b-1} + 1.$$

In this case we can get a better lower bound for

$$\frac{1.7c}{33ab(b-a)^2\gamma} > \frac{1.7c}{33b^2(2\sqrt{b})^2\frac{b^3}{2}} > 0.0257cb^{-6} > 30c^{1-\frac{6}{9}} > c^{0.333},$$

where we have used that $b-a = 2\sqrt{b-1}-1 \le 2\sqrt{b}$. Now, we get

$$\log z < \frac{2.889\log c \cdot 2\log c}{0.333\log c} < 17.352\log c,$$

and therefore, $z < c^{17.352}$ and

$$d < \frac{z^2+1}{c} < c^{33.72}.$$

That was the claim we wanted to prove. □

7. Proof of the theorems

Now, we put everything together to prove our theorems.

Proof of Theorems 1a and 1b.

Let $\{a,b,c,d\}$ be a $D(-1)$-quadruple with $2 \le a < b < c < d$ and with minimal d. We use the lower bound, which is given by (17), to get

$$c^{n-1} < w_n = z < c^{26.028},$$

where we have used (25) from the proof of Lemma 17. It follows that $n < 27.028$ and thus $n \le 27$. But now we can use Lemma 14 to get

$$c^{0.064} < n \le 27,$$

which implies the following upper bound for c, namely

$$c < 27^{\frac{1}{0.064}} < 27^{15.63} < 2.36 \cdot 10^{22}.$$

By our improved gap principle (Lemma 13), which was $c > 40000b^9$, we therefore derive

$$b \le 94.$$

It is easy to give a list of all $D(-1)$-triples $\{1,a,b\}$ with $b \le 94$. They are

$$\{1,2,5\},\{1,5,10\},\{1,10,17\},\{1,17,26\},\{1,26,37\},$$
$$\{1,37,50\},\{1,50,65\},\{1,65,82\},\{1,5,65\}.$$

The first eight of these triples are $\{1, i^2+1, (i+1)^2+1\}$ for $i = 1,\dots,9$. The only one in the above list, which is not of this form, is the last one, namely $\{1,5,65\}$. As remarked in the introduction it was proved already earlier that $\{1,2,5\},\{1,5,10\},\{1,5,65\},\{1,10,17\}$ and $\{1,26,37\}$ cannot be extended to $D(-1)$-quadruples. So, we are left with the cases

$$\{1, i^2+1, (i+1)^2+1\} \quad \text{for} \quad i = 4,6,7,8,9.$$

In all these cases a and b are very close (in fact they are closest possible) to each other. Therefore, by using Lemma 18 in the same way as above, we get

$$c^{n-1} < w_n = z < c^{17.36},$$

which implies $n \leq 18$. Using the lower bound for n, we get

$$c < 18^{15.63} < 4.17 \cdot 10^{19}.$$

This implies $b \leq 46$. Hence, the only remaining case is

$$\{1, 17, 26\}.$$

In this case we have to consider c's with $17c - 1 = s^2, 26c - 1 = t^2$ and where $c - 1$ is also a square. Therefore, we look at the Pell equation given by

$$17t^2 - 26s^2 = 9,$$

where the fundamental solutions are bounded by $0 < t_0 < 26, |s_0| < \sqrt{17 \cdot 26 - 1} = 21$ and therefore are $s_0 = \pm 4, t_0 = 5$. All the solutions t satisfy the following linear recurrences

$$t_0 = 5, \quad t_1 = 47 \text{ or } 8783, \quad t_{n+2} = 1766 t_{n+1} - t_n.$$

We are interested in those $t = t_n$ for which $t^2 = 27c - 1 \leq 26 \cdot 4.17 \cdot 10^{19}$, this gives $t < 4 \cdot 10^{10}$, and which have the additional property that

$$c - 1 = \frac{t^2 + 1}{26} - 1$$

is a square. It is checked easily that such a t does not exist, showing that $\{1, 17, 26\}$ cannot be extended to a quadruple $\{1, 17, 26, c\}$ with $c < 4.17 \cdot 10^{19}$.

Finally we get that there is no $D(-1)$-quadruple $\{a, b, c, d\}$ with $2 \leq a < b < c < d$. This completes the proof of our main result. □

8. Acknowledgements

This paper was written during a visit of the second author at the University of Zagreb in the frame of a joint Austrian-Croatian project granted by the Croatian Ministry of Science, Education and Sports and the Austrian Exchange Service (Nr. 20/2004). Both authors are most grateful for this support. The second author wants to thank Andrej Dujella for his kind hospitality.

References

[1] A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford Ser.* (2) **20** (1969), 129-137.

[2] M. A. Bennett, On the number of solutions of simultaneous Pell equations, *J. Reine Angew. Math.* **498** (1998), 173-199.

[3] E. Brown, Sets in which $xy + k$ is always a square, *Math. Comp.* **45** (1985), 613-620.

[4] L. E. Dickson, "History of the Theory of Numbers" Vol. 2, Chelsea, New York, 1966, 518-519.

[5] Diophantus of Alexandria, Arithmetics and the Book of Polygonal Numbers, (I. G. Bashmakova, Ed.) (Nauka, 1974) (in Russian), 85-86, 215-217.

[6] A. Dujella, On the exceptional set in the problem of Diophantus and Davenport, *Application of Fibonacci Numbers* Vol. 7, (G. E. Bergum, A. N. Philippou, A. F. Horadam, eds.), Kluwer, Dordrecht, 1998, 69-76.

[7] A. Dujella, Complete solution of a family of simultaneous Pellian equations, *Acta Math. Inform. Univ. Ostraviensis* **6** (1998), 59-67.

[8] A. Dujella, An absolute upper bound for the size of Diophantine m-tuples, *J. Number Theory* **89** (2001), 126-150.

[9] A. Dujella, An extension of an old problem of Diophantus and Euler II, *Fibonacci Quart.* **40** (2002), 118-123.

[10] A. Dujella, On the size of Diophantine m-tuples, *Math. Proc. Cambridge Philos. Soc.* **132** (2002), 23-33.

[11] A. Dujella, There are only finitely many Diophantine quintuples, *J. Reine Angew. Math.* **566** (2004), 183-214.

[12] A. Dujella and C. Fuchs, A polynomial variant of a problem of Diophantus and Euler, *Rocky Mount. J. Math.* **33** (2003), 797-811.

[13] A. Dujella and C. Fuchs, Complete solution of a polynomial version of a problem of Diophantus, *J. Number Theory*, to appear (Preprint: http://www.math.hr/~duje/polquad4.dvi).

[14] A. Dujella and A. Pethö, Generalization of a theorem of Baker and Davenport, *Quart. J. Math. Oxford Ser. (2)* **49** (1998), 291-306.

[15] P. Gibbs, Some rational Diophantine sextuples, preprint, math.NT/9902081.

[16] T. L. Heath, "Diophantus of Alexandria: A study in the history of Greek Algebra". With a supplement containing an account of Fermat's theorems and problems connected with Diophantine analysis and some solutions of Diophantine problems by Euler (Cambridge, England, 1910), Powell's Bookstore, Chicago; Martino Publishing, Mansfield Center, 2003, 162-164, 344-347.

[17] B. W. Jones, A variation of a problem of Davenport and Diophantus, *Quart. J. Math. Oxford* Ser.(2) **27** (1976), 349-353.

[18] B. W. Jones, A second variation of a problem of Davenport and Diophantus, *Fibonacci Quart.* **15** (1977), 323-330.

[19] K. S. Kedlaya, Solving constrained Pell equations, *Math. Comp.* **67** (1998), 833-842.

[20] O. Kihel, On the extendibility of the set $\{1, 2, 5\}$, *Fibonacci Quart.* **38** (2000), 464–466.

[21] S. P. Mohanty and A. M. S. Ramasamy, The simultaneous Diophantine equations $5y^2 - 20 = x^2$ and $2y^2 + 1 = z^2$, *J. Number Theory* **18** (1984), 356-359.

[22] P. G. Walsh, On two classes of simultaneous Pell equations with no solutions, *Math. Comp.* **68** (1999), 385-388.

[23] D. X. Zheng, On the systems of Diophantine equations $y^2 - 2x^2 = 1, z^2 - 5x^2 = 4$ and $y^2 - 5x^2 = 4, z^2 - 10x^2 = 9$, *Sichuan Daxue Xuebao* **24** (1987), 25-29.

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30, 10000 Zagreb, Croatia
e-mail: duje@math.hr

Clemens Fuchs
Institut für Mathematik
TU Graz
Steyrergasse 30, 8010 Graz, Austria
e-mail: clemens.fuchs@tugraz.at