Effective Solution of the $D(-1)$-quadruple Conjecture

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

Alan Filipin
Faculty of Civil Engineering, University of Zagreb
Fra Andrije Kačića-Miošića 26, 10000 Zagreb, Croatia
E-mail: filipin@grad.hr

and

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

Abstract

The $D(-1)$-quadruple conjecture states that there does not exist a set of four positive integers such that the product of any two distinct elements is one greater than a perfect square. An effective proof is given by showing that if $\{a, b, c, d\}$ is such a set then $\max\{a, b, c, d\} < 10^{10^{23}}$, leaving open a completely determined (but currently computationally infeasible large) set of exceptions to check.

1 Introduction and results

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.

*Corresponding author.

A lot of work has been done on $D(n)$-m-tuples in the last decade, but in fact the problem is much older. It was first studied by Diophantus in the case $n = 1$. 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. Later Euler was able to add the fifth positive rational, $\frac{777480}{8288641}$, to the Fermat's set (see [6], [7, pp. 103-104, 232], [8, pp. 141-145] and [27, pp. 177-181]). Recently, Gibbs [25] 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 [2] 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 [15], this refined previous results [22, 12]). The last result is effective, namely if $\{a, b, c, d, e\}$ is a $D(1)$-quintuple, then $d < 10^{2171}$ and $e < 10^{10^{26}}$ (cf. [15, Corollary 4, p. 210]). This proves the $D(1)$-quintuple conjecture in an effective way, leaving open a completely determined finite set to check.

For general n, it is easy to see, by considering congruences modulo 4, that if $n \equiv 2 \pmod 4$ then there does not exist a $D(n)$-quadruple (see [5, 26, 34]), while the first author proved in [9] 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 $D(n)$.

The best known upper bounds for the size of sets with the property $D(n)$ are logarithmic in $|n|$ (see [14, 16]). Moreover, for n prime it was shown recently that the size is bounded by the absolute constant 2^{170} (cf. [21]).

Therefore, in the case $n = -1$ the conjecture is that there does not exist a $D(-1)$-quadruple. In analogy to above this is known as the $D(-1)$-quadruple conjecture and it appeared explicitly in [10] for the first time. 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 [5], see also [39, 30, 38, 31]), $\{1, 5, 10\}$ (by Mohanty and Ramasamy in [33]), $\{1, 2, 145\}$, $\{1, 2, 4901\}$, $\{1, 5, 65\}$, $\{1, 5, 20737\}$, $\{1, 10, 17\}$, $\{1, 26, 37\}$ (by Kedlaya [30]) and $\{17, 26, 85\}$ (again by Brown in [5]). Moreover, Brown proved that the infinite families $\{x^2+1, (x+1)^2+1, (2x+1)^2+4\}$, if $x \not\equiv 0 \pmod 4$, $\{2, 2x^2+2x+1, 2x^2+6x+5\}$, if $x \equiv 1 \pmod 4$ of $D(-1)$-triples cannot be extended to quadruples. The first author proved the conjecture in [11] for all triples of the form $\{1, 2, c\}$.

Very recently, important progress was made by Dujella and Fuchs in [20]. They proved that there does not exist a $D(-1)$-quintuple. More precisely, it is proved that there does not exist a $D(-1)$-quadruple $\{a, b, c, d\}$ with $2 \leq a < b < c < d$. This implies that we are left by considering the case $a = 1$, i.e. $D(-1)$-quadruples of the form $\{1, b, c, d\}$. In [20] it was remarked that the case $a = 1$ seems more involved and much harder and that 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.

In the meantime the non-extendibility of $\{1, b, c\}$ was confirmed for $b = 5$ (in [1]), for $b = 10$ (by the second author [23]), and for $b = 17, 26, 37, 50$ (by Fujita in [24]).

We mention that a polynomial variant of the above problems was first studied by Jones [28], [29], and it was for the case $n = 1$. Recently, polynomial variants were also studied by Dujella and Fuchs. 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 [15]) in [19] and also for the case $n = -1$ in [18].

The aim of the present paper is to go further and to prove that in fact there are at most finitely many $D(-1)$-quadruples $\{1, b, c, d\}$. We will prove the following result:

Theorem 1. *Let $\{1, b, c\}$ be a $D(-1)$-triple. Then:*

(i) If $c > b^9$, then there does not exist an extension to a $D(-1)$-quadruple $\{1, b, c, d\}$ such that $d > c$.

(ii) If $11b^6 \leq c \leq b^9$, then there does not exist an extension to a $D(-1)$-quadruple.

Assume that $\{1, b, c, d\}$ with $1 < b < c < d$ is an extension to a $D(-1)$-quadruple.

(iii) If $b^3 < c < 11b^6$, then $c < 10^{238}, d < 10^{10^{20}}$,

(iv) if $b^{1.1} < c \leq b^3$, then $c < 10^{492}, d < 10^{10^{23}}$,

(v) if $3b < c \leq b^{1.1}$, then $c < 10^{95}, d < 10^{10^{21}}$,

(vi) if $c = 1 + b + 2\sqrt{b-1}$, then $c < 10^{76}, d < 10^{10^{21}}$.

Note that, by [20, Lemma 7], if $c > b$ and $c \neq 1 + b + 2\sqrt{b-1}$ then it holds $c > 3b$. Hence, the theorem covers all possible $D(-1)$-triples $\{1, b, c\}$ such that $1 < b < c$.

To sum up, we get the following effective solution of the $D(-1)$-quadruple conjecture:

Theorem 2. *There are only finitely many $D(-1)$-quadruples. Moreover, if $\{a, b, c, d\}$ is a $D(-1)$-quadruple, then* $\max\{a, b, c, d\} < 10^{10^{23}}$.

As in the case for the $D(1)$-quintuple conjecture, this proves the $D(-1)$-quadruple conjecture in an effective way. Unfortunately, the remaining set is to large to be checked by the means of a computer programm at the moment.

This is also the first nontrivial result (for integers $\not\equiv 2 \pmod 4$) related to the following conjecture

Conjecture 1. *If n is not a perfect square, then there exist only finitely many $D(n)$-quadruples.*

Since, by [9, Remark 3], all elements of a $D(-4)$-quadruple are even, Theorem 2 implies that Conjecture 1 is valid for $n = -1$ and $n = -4$.

Recently, for the case $n = 1$, it was shown by the first author in [17] that the number of $D(1)$-quintuples can be bounded by 10^{1930}. By using similar arguments together with Theorem 1, we can also derive an upper bound for the number of $D(-1)$-quadruples.

Theorem 3. *The number of $D(-1)$-quadruples is bounded by* 10^{903}.

The case $n = -1$ deserves special attention because this case is closely connected with another old problem investigated by 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 [6], [7, pp. 85-86, 215-217], [8, pp. 101-104] and [27, pp. 162-164, 344-347]). In [13] an infinite family of rational quintuples with the same property was given. Since

$$xy + x + y = (x + 1)(y + 1) - 1, \tag{1}$$

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. In fact the main result in [20] completely solved this problem, namely it was shown that there does not exist a set of four positive integers such that the product of any two distinct elements plus there sum is a perfect square.

By the equivalence (1), we get the following corollaries to the above theorems, which extend the problem solved in [20].

Corollary 1. *There are at most finitely many sets* $\{a^2, b^2, c^2\}, 0 < a < b < c$ *of three positive perfect squares such that the product of any two of its distinct elements plus their sum is a perfect square.*

This can be reformulated as (the case of positive elements cannot occur at all by [20, Theorem 1a]):

Corollary 2. *There are at most finitely many sets of four integers with the property that the product of any two of its distinct elements plus their sum is a perfect square.*

Of course, both corollaries are effective and therefore settle the problem up to a finite amount of computations.

In the next section we will start by collecting important information about this problem (especially from [20]). The strategy of proof follows the same lines as the proofs of almost all other recent results on non-extendability of $D(n)$-m-tuples. First we reduce the problem of finding d which extends $\{1, b, c\}$ to a $D(-1)$-quadruple to a system of simultaneous Pellian equations, which leads to the consideration of intersections of linear recurring sequences. We know that the indices of these sequences have the same parity and they are very simply connected. Moreover, we have a very important congruence relation. E.g. this relation implies that the sequences cannot have intersections for small indices. Moreover, by the gap principle, which was the main improvement in the proof in [20], we get precise information on the initial terms of the recurring sequences.

If $c \geq 11b^6$, in Section 3 we obtain (Proposition 1) by Bennett's theorem on simultaneous approximations of square roots which are close to 1 (in a slightly refined version for our context by Fujita [24]) parts (i) and (ii) (the case of *very large solutions*) of our main theorem (Theorem 1).

In Section 4 we will compute some general upper bound for the indices of the recurring sequences in terms of c by using Baker's theory of linear forms in logarithms of algebraic numbers (in fact we will use Matveev's result [32]).

In Section 5 we will give the proof of part (iii)-(v) (*large*, *medium size*, and *small solutions*, respectively) of the theorem (see Propositions 2, 3, 4), where we have to get lower bounds for n in terms of some power of c. For *medium size* (part (iv) of the theorem, i.e. $b^{1.1} < c < b^4$) and *small* (part (v) of the theorem, i.e. $3b < c < b^{1.1}$) *solutions* we first have to refine the congruence relations. In fact this is the most important new part of the proof.

Finally, we will give the proof of the case of *very small solutions* ($c \leq 3b$), namely part (vi) of the theorem, in Section 6 (Proposition 5).

The proof of the quantitative result in Theorem 3 will be given in the final Section 7.

2 Preliminaries

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

$$b - 1 = r^2,\ c - 1 = s^2,\ bc - 1 = t^2.$$

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

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

with integers x, y, z. Eliminating d from (2) we obtain the following system of Pellian equations

$$z^2 - cx^2 = c - a, \tag{3}$$

$$bz^2 - cy^2 = c - b. \tag{4}$$

By combining these two equations we additionally have $y^2 - bx^2 = b - 1$. We will describe the sets of solutions of equations (3) and (4) in the following lemma.

Lemma 1. *If (z, x) and (z, y), with positive integers x, y, z, are solutions of (3) and (4) 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 (3) and (4) respectively,

(ii) the following inequalities are satisfied:

$$0 \leq |x_0| < s, \qquad 0 < z_0 < c, \tag{5}$$

$$0 \leq |y_1| < t, \qquad 0 < z_1 < c, \tag{6}$$

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

$$z\sqrt{a}+x\sqrt{c}=(z_0\sqrt{a}+x_0\sqrt{c})(s+\sqrt{ac})^{2m}, \tag{7}$$
$$z\sqrt{b}+y\sqrt{c}=(z_1\sqrt{b}+y_1\sqrt{c})(t+\sqrt{bc})^{2n}. \tag{8}$$

Proof. This is [20, Lemma 1] $\square$

From (7) we conclude that $z = v_m$, for some (z_0, x_0) with the above properties and integer $m \geq 0$, where

$$v_0 = z_0,\ v_1 = (2c-1)z_0 + 2scx_0,\ v_{m+2} = (4c-2)v_{m+1} - v_m. \tag{9}$$

Hence for varying $m \geq 0$ the solutions z form a binary recurrent sequence $(v_m)_{m\geq 0}$ whose initial terms are found by solving equation (7) for z when $m = 0$ and 1, and whose characteristic equation has the roots $(s+\sqrt{c})^2$ and $(s-\sqrt{c})^2$. In the same manner, from (8), we conclude that $z = w_n$ for some (z_1, y_1) with the above properties and integer $n \geq 0$, where

$$w_0 = z_1,\ w_1 = (2bc-1)z_1 + 2tcy_1,\ w_{m+2} = (4bc-2)w_{n+1} - w_n. \tag{10}$$

Our system of equation (3) and (4) is thus transformed to finitely many equations of the form $z = v_m = w_n$.

From (9) and (10) we get by induction

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

(see [20, Lemma 2]). So if the equation $v_m = w_n$ has a solution, then we have $z_0 = z_1$. Moreover, we have the following properties:

Lemma 2. *If $v_m = w_n, n \neq 0$, then*

(i) $m \equiv n \pmod 2$*,*

(ii) $n \leq m \leq 2n$*,*

(iii) $m^2 z_0 + smx_0 \equiv bn^2 z_1 + tny_1 \pmod{4c}$*.*

Proof. Part (i) and (iii) follow at once from what we just said. Statement (ii) is [20, Lemma 5]. Observe that we remarked there that this statement holds for arbitrary $D(-1)$-quadruples and not only in the special situation considered there. $\square$

Moreover, we have the following bounds for v_m, w_n, respectively.

Lemma 3. *We have*

$$(c-1)(4c-3)^{m-1} < v_m < 4c^2(4c-2)^{m-1}, \quad \text{for } m \geq 1,$$
$$(c-b)(4bc-3)^{n-1} < w_n < 4bc^2(4bc-2)^{n-1}, \quad \text{for } n \geq 1.$$

Proof. This is part of the proof of [20, Lemma 5] (cf. (3.1) in [20] and the equation just before that). □

We collect some useful gap principles for the elements of $D(-1)$-triples and quadruples.

Lemma 4. *Let $\{a, b, c\}$ be a $D(-1)$-triple and $0 < a < b < c$, then $c = a + b + 2r$ or $c > 3ab \geq 3b$.*
Let $\{1, b, c, d\}$ be a $D(-1)$-quadruple and $1 < b < c < d$, then we have $d > c^9$.

Proof. The first part of the Lemma is [20, Lemma 7]. The second part is a consequence of [20, Lemma 13]. Observe that in fact there it is proved for the $D(-1)$-quadruple $\{1, a, b, c\}$ with $1 < a < b < c$. The assumption that $\{a, b, c, d\}$ with $2 \leq a < b < c < d$ and d minimal under all such quadruples was only needed to ensure that $\{1, a, b, c\}$ is really a $D(-1)$-quadruple again (by the use of the key lemma [20, Lemma 3]). □

This has the following important implication on the fundamental solutions of (9) and (10) described in Lemma 1.

Lemma 5. *Let the integers z_0, z_1, x_0, y_1 be as in Lemma 1. If $c \leq b^9$, then*

$$z_0 = z_1 = s, x_0 = 0, y_1 = \pm\sqrt{b-1} = \pm r.$$

Proof. Let us define d_0 by

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

It follows easily that

$$d_0 - 1 = x_0^2, bd_0 - 1 = y_1^2, cd_0 - 1 = z_0^2$$

and $d_0 < c$ (this construction was the key lemma in [20], in fact it was [20, Lemma 3]). If $d_0 > 1$, then $\{1, b, d_0, c\}$ is again a $D(-1)$-quadruple and by the second part of Lemma 4 it follows that $c > b^9$, a contradiction. Hence, $d_0 = 1$, which implies our assertion (cf. also [20, Lemma 4] for this final conclusion). □

It is easy to show that the equation $v_m = w_n$ cannot have solutions with small indices.

Lemma 6. *We have $v_1 \neq w_1$, $v_2 \neq w_2$, $v_4 \neq w_2$.*

Proof. See [20, Lemma 8, Lemma 10 and Lemma 11]. Observe again that the conclusion there is independent of the existence of a minimal extension which was assumed there. □

Now we have collected all information we need to prove our main theorem which will be done in the following sections, respectively.

3 Very large solutions

The proof will follow from a lower bound for m, n in terms of some power of c, together with an logarithmic upper bound obtained from Bennett's theorem. The idea for obtaining the lower bound is that if $v_m = w_n$, then we can study the congruence equation from Lemma 2(iii). We will show that if b, m, n are small compared with c, these congruences are equations, which are in contradiction to the equation $v_m = w_n$.

Lemma 7. *If $v_m = w_n, n \neq 0, 1$ and $c \geq 11b^6$, then $n > c^{\frac{1}{6}}$.*

Proof. From Lemma 2(iii) we have $m^2 z_0 + smx_0 \equiv bn^2 z_0 + tny_1 \pmod{4c}$. Assume now that $n \leq c^{\frac{1}{6}}$. It is easy to see that $\max\{|m^2 z_0|, |smx_0|, |tny_1|\} < |bn^2 z_0|$. We first consider the case $c > b^9$. Let d_0 be such that $cd_0 - 1 = z_0^2$. If $d_0 > 1$ then $\{1, b, d_0, c\}$ is a $D(-1)$-quadruple and we get by the second part of Lemma 4 that $c > (\max\{b, d_0\})^9 > b^6 d_0^3$. Then we have

$$\left|bn^2 z_0\right| < b \cdot c^{\frac{1}{3}} \cdot (cd_0)^{\frac{1}{2}} < c^{\frac{1}{3}} \cdot c^{\frac{1}{2}} \cdot \left(b^6 d_0^3\right)^{\frac{1}{6}} < c.$$

If $d_0 = 1$ then we get as in the proof of Lemma 5 that $z_0 = s$. Thus we immediately get

$$\left|bn^2 z_0\right| < c^{\frac{1}{3}} \cdot c^{\frac{1}{2}} \cdot c^{\frac{1}{2}} < c.$$

Now we consider the case $11b^6 \leq c \leq b^9$. Here we can use Lemma 5 to get

$$\left|bn^2 z_0\right| < c^{\frac{1}{6}} \cdot c^{\frac{1}{3}} \cdot c^{\frac{1}{2}} = c.$$

Therefore we can conclude that $m^2 z_0 + smx_0 = bn^2 z_0 + tny_1$. We have

$$m^2 z_0 + smx_0 < m^2\sqrt{cd_0} + m\sqrt{cd_0} < m(m+1)\sqrt{\frac{c}{b}}\sqrt{|y_1|^2+1}$$

and

$$bn^2 z_0 - tn|y_1| > \sqrt{bc}|y_1|n^2 - tn|y_1| > \sqrt{bc}|y_1|n^2 - \sqrt{bc}|y_1|n = \sqrt{bc}|y_1|n(n-1).$$

This implies

$$m(m+1)\sqrt{|y_1|^2+1} > b|y_1|n(n-1)$$

and by the relation $m \leq 2n$ and $b \geq 65$ we get

$$5 \geq \frac{2n+1}{n-1} > \frac{65|y_1|}{2\sqrt{|y_1|^2+1}} > \frac{65}{2\sqrt{2}}$$

and therefore we get a contradiction that proves the statement. $\square$

Next we need an upper bound for n in terms of c. To obtain it we use the following slightly modified version of a special case of Bennett's theorem [4] (it is also a modified version of Rickert's theorem [35]), which was proved in [24].

Lemma 8. *Let b and N be integers with $b \geq 5$ and $N \geq 2.39b^7$. Then the numbers*

$$\theta_1 = \sqrt{1+\frac{1-b}{N}} \text{ and } \theta_2 = \sqrt{1+\frac{1}{N}}$$

satisfy

$$\max\left\{\left|\theta_1 - \frac{p_1}{q}\right|, \left|\theta_2 - \frac{p_2}{q}\right|\right\} > \left[32.1\frac{b^2(b-1)^2}{2b-1}N\right]^{-1} q^{-1-\lambda}$$

for all integers p_1, p_2, q with $q > 0$, where

$$\lambda = \frac{\log \dfrac{16.1b^2(b-1)^2N}{2b-1}}{\log \dfrac{3.37N^2}{b^2(b-1)^2}} < 1.$$

Proof. This is Theorem 3.5 in [24]. $\square$

We apply this theorem with the numbers $N = t^2 = bc - 1 \geq 11b^7 - 1 > 2.39b^7, p_1 = bsx, p_2bz, q = ty$, i.e. to

$$\theta_1 = \frac{s\sqrt{b}}{t}, \quad \theta_2 = \frac{\sqrt{bc}}{t}.$$

First we show that the solutions of our problem induce good approximations to the roots θ_1, θ_2.

Lemma 9. *All positive integers solutions x, y, z of (3) and (4) satisfy*

$$\max\left\{\left|\theta_1 - \frac{bsx}{ty}\right|, \left|\theta_2 - \frac{bz}{ty}\right|\right\} < \frac{b-1}{y^2}.$$

Proof. Since $f(x) = b(x-1)/(bx-1)$ is an increasing function we get

$$\left|\theta_1 - \frac{bsx}{ty}\right| = \frac{s\sqrt{b}}{t}\left|1 - \frac{x\sqrt{b}}{y}\right| = \frac{s\sqrt{b}}{t}\left|\frac{1-bx^2}{y^2}\right|\left|1 + \frac{x\sqrt{b}}{y}\right|^{-1} < \frac{b-1}{y^2}.$$

Moreover, since $by/y > \sqrt{bc}$ we have

$$\begin{aligned}\left|\theta_2 - \frac{bz}{ty}\right| &= \frac{1}{t}\left|\sqrt{bc} - \frac{bz}{y}\right| = \frac{b}{t}\left|c - \frac{bz^2}{y^2}\right|\left|\sqrt{bc} + \frac{bz}{y}\right|^{-1} \\ &< \frac{b}{t}\frac{c-b}{y^2}\frac{1}{2\sqrt{bc}} < \frac{1}{2y^2}\frac{bc-1}{\sqrt{bc(bc-1)}} < \frac{b-1}{y^2}.\end{aligned}$$

This proves the lemma. $\square$

Now we are ready to prove the first two parts of Theorem 1. Namely, we show the following proposition.

Proposition 1. *Let $\{1, b, c\}$ with $1 < b < c$ be a $D(-1)$-triple. If $c \geq 11b^6$, then there does not exist an integer $d > c$ such that $\{1, b, c, d\}$ is a $D(-1)$-quadruple. If $11b^6 \leq c \leq b^9$, then the triple $\{1, b, c\}$ cannot be extended to a $D(-1)$-quadruple.*

Proof. Combining the upper bound of Lemma 9 with the lower bound from Lemma 8 we get

$$\left[32.1\frac{b^2(b-1)^2}{2b-1}t^2\right]^{-1}(ty)^{-1-\lambda} < \frac{b-1}{y^2},$$

which implies

$$y^{1-\lambda} < 32.1\frac{b^2(b-1)^3}{2b-1}t^{3+\lambda} < \frac{32.1b^2(b-1)^3(bc-1)^2}{2b-1}.$$

We have

$$\frac{1}{1-\lambda} = \frac{\log\dfrac{3.37(bc-1)^2}{b^2(b-1)^2}}{\log\dfrac{3.37(2b-1)(bc-1)}{16.1b^4(b-1)^4}},$$

which leads to

$$\log y < \frac{\log\dfrac{3.37(bc-1)^2}{b^2(b-1)^2}\log\dfrac{32.1b^2(b-1)^3(bc-1)^2}{2b-1}}{\log\dfrac{3.37(2b-1)(bc-1)}{16.1b^4(b-1)^4}}.$$

We have (observe that $c \geq 11b^6$ and $b \geq 65, c \geq 82$)

$$\log \frac{3.37(bc-1)^2}{b^2(b-1)^2} < \log \frac{3.37b^2c^2}{b^2(b-1)^2} < 2\log \frac{1.9c}{b-1} < 2\log 0.03c,$$
$$\log \frac{32.1b^2(b-1)^3(bc-1)^2}{2b-1} < \log\left(16.18b^6c^2\right) < 3\log 1.14c,$$
$$\log \frac{3.36(2b-1)(bc-1)}{16.1b^4(b-1)^4} > \log \frac{2.29(2b^2c-bc-2b+1)}{b^2c} > 1.51.$$

Consequently,

$$\log y < 3.98 \log 0.03c \log 1.14c.$$

Moreover, from (4) and the first part of Lemma 3 we get

$$y > \sqrt{\frac{b}{c}}z = \sqrt{\frac{b}{c}}v_m > \sqrt{\frac{b}{c}}(c-1)(4c-3)^{m-1} > (4c-3)^{m-1}.$$

Assume that $n \neq 0, 1$. Then by Lemma 2 and Lemma 7 we have $m \geq n > c^{\frac{1}{6}}$, which implies

$$\left(c^{\frac{1}{6}}-1\right)\log(4c-3) < 3.98\log 0.03c \log 1.14c. \tag{11}$$

If we define the function

$$f(c) = 3.98\log 0.03c\log 1.14c - \left(c^{\frac{1}{6}}-1\right)\log(4c-3),$$

then it is easy to check that this function is degreasing for $c > 0.55 \cdot 10^{12}$. Since $c \geq 11b^6 \geq 11 \cdot 65^6 > 0.82 \cdot 10^{12}$, inequality (11) cannot by fulfilled. Hence, we conclude that $n = 0$ or $n = 1$. Now, by Lemma 6, we have that $z = v_0 = w_0$. But then $d = (z^2+1)/c < c$. Moreover, if $11b^6 \leq c \leq b^9$, then Lemma 5 implies that $z = s$ and $d = 1$. This proves the proposition. □

4 Diophantine approximation result

All other parts of Theorem 1 will be obtained by applying the theory of linear form of logarithms of algebraic numbers instead of Bennett's approximation result. In this way it will not be possible to exclude any solution, but we will get effective upper bounds. In this section we will prepare the approximation tool that will be used in the proofs in case of solutions that are not very large.

In fact we will use a result by Matveev [32], which we quote in a suitable simplified version.

Lemma 10. *Let Λ be a linear form in logarithm of l multiplicatively independent totally real algebraic numbers $\alpha_1, \ldots, \alpha_l$ with rational integer coefficients $b_1, \ldots, b_l$ $(b_l \neq 0)$. Let $h(\alpha_j)$ denote the absolute logarithmic height of $\alpha_j, 1 \leq j \leq l$. Define the number $D, A_j, 1 \leq j \leq l$, and B by $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_l) : \mathbb{Q}], A_j = \max\{Dh(\alpha_j), |\log \alpha_j|\}$,*

$$B = \max\left\{1, \max\left\{\frac{|b_j|A_j}{A_l} \ : \ 1 \leq j \leq l\right\}\right\}.$$

Then

$$\log \Lambda > -C(l)C_0W_0D^2\Omega, \tag{12}$$

where

$$C(l) = \frac{8}{(l-1)!}(l+2)(2l+3)(4e(l+1))^{l+1}, \quad W_0 = \log\left(1.5eBD\log(eD)\right),$$
$$C_0 = \log\left(e^{4.4l+7}l^{5.5}D^2\log(eD)\right), \qquad \Omega = A_1 \cdots A_l.$$

Proof. See [32, Theorem 2.1]. □

Solving the recurrences (3) and (4) we get

$$v_m = \frac{s}{2}\left[(s+\sqrt{c})^{2m} + (s-\sqrt{c})^{2m}\right],$$
$$w_n = \frac{s\sqrt{b} \pm r\sqrt{c}}{2\sqrt{b}}\left[(t+\sqrt{bc})^{2n} + (t-\sqrt{bc})^{2n})\right].$$

We now turn the equation $v_m = w_n$ into an inequality for a linear form in three logarithms to which Lemma 10 will be applied.

Lemma 11. *If $v_m = w_n, n \neq 0$, then*

$$0 < 2n\log(t+\sqrt{bc}) - 2m\log(s+\sqrt{c}) + \log\frac{s\sqrt{b} \pm r\sqrt{c}}{2\sqrt{b}} < (3.96bc)^{-n+1}.$$

Proof. Let

$$P = s(s+\sqrt{c})^{2m}, \quad Q = \frac{s\sqrt{b} \pm r\sqrt{c}}{\sqrt{b}}(t+\sqrt{bc})^{2n}.$$

Then $v_m = w_n$ implies $P + (c-1)P^{-1} = Q + \frac{c-b}{b}Q^{-1}$. Furthermore, we have

$$P > 4s(c-1) = 4\sqrt{c-1}(c-1) > c-1,$$
$$Q > \frac{s\sqrt{b} - r\sqrt{c}}{\sqrt{b}}(2bc - 1 + 2\sqrt{bc}) \geq 2c \geq 2.$$

We get

$$\begin{aligned} P - Q &= \frac{c-b}{b} Q^{-1} - (c-1)P^{-1} < (c-1)Q^{-1} - (c-1)P^{-1} \\ &= (c-1)(P-Q)P^{-1}Q^{-1}, \end{aligned}$$

and therefore we have $Q > P$. Moreover, $P > Q - (c-1)P^{-1} > Q - 1$, which implies that $\frac{Q-P}{Q} < Q^{-1} \leq \frac{1}{2}$. Hence,

$$0 < \log \frac{Q}{P} = -\log \frac{P}{Q} = -\log\left(1 - \frac{Q-P}{Q}\right) < \frac{Q-P}{Q} + \left(\frac{Q-P}{Q}\right)^2.$$

From this we conclude

$$\begin{aligned} 0 < \log \frac{Q}{P} &< \frac{1}{Q} + \frac{1}{Q^2} < \frac{2}{Q} = \frac{2\sqrt{b}}{s\sqrt{b} \pm \sqrt{c}r}(t + \sqrt{bc})^{-2n} \\ &< \frac{2\sqrt{b}}{s\sqrt{b} - r\sqrt{c}}(3.96bc)^{-n} = \frac{2\sqrt{b}(s\sqrt{b} + r\sqrt{c})}{c-b}(3.96bc)^{-n} \\ &< \frac{4b\sqrt{c}}{c-b}(3.96bc)^{-n} < (3.96bc)^{-n+1}. \end{aligned}$$

This proves the lemma. □

We use this result to prove a principle to obtain an upper bound for n in all remaining cases.

Lemma 12. *If $v_m = w_n$, then*

$$\frac{n-1}{\log\left(\dfrac{160.36n\log(2.02bc)}{\log c}\right)} < 0.33 \cdot 10^{12} \cdot \log c \cdot \log(bc).$$

Proof. We have $l = 3, D = 4$ and therefore $C(3) \leq 0.65 \cdot 10^9$ and $C_0 \leq 29.89$. Moreover, we have $\alpha_1 = s + \sqrt{c}, \alpha_2 = t + \sqrt{bc}$, and

$$\alpha_3 = \frac{s\sqrt{b} \pm r\sqrt{c}}{s\sqrt{b}}.$$

The minimal polynomials of $\alpha_1, \alpha_2, \alpha_3$ are $\alpha_1^2 + (4c-2)\alpha_1 + 1 = 0, \alpha_2^2 + (4bc-2)\alpha_2 + 1 = 0$, and $b(c-1)\alpha_3^2 - 2b(c-1)\alpha_3 + c - b = 0$. Therefore, $A_1 = 2\log(s + \sqrt{c}) < 2\log(2\sqrt{c}) < 1.08\log c, A_2 = 2\log(t + \sqrt{bc}) < \log(\sqrt{2}bc) < 1.05\log(bc)$, and

$$A_3 \leq 2\log bc\frac{s\sqrt{b} + r\sqrt{c}}{s\sqrt{b}} < 2\log(2.02bc) < 2\log(3.96bc).$$

We also have

$$A_3 \geq \log b(c-1) \geq \log(64.2c) > 1.95 \log c.$$

Thus,

$$B \leq \frac{4m \log(2.02bc)}{1.95 \log c} \leq \frac{2.06m \log(2.02bc)}{\log c}.$$

By Lemma 11 and Lemma 10 we therefore get

$$n - 1 < 0.33 \cdot 10^{12} \cdot \log\left(\frac{80.18m \log(2.02bc)}{\log c}\right) \log c \log(bc).$$

Finally, we have

$$\frac{n-1}{\log\left(\frac{160.36n \log(2.02bc)}{\log c}\right)} < 0.33 \cdot 10^{12} \cdot \log c \cdot \log(bc),$$

which is the statement. □

Our remaining goal is to calculate lower bound for n in terms of small powers of c as above. Together with our gap conditions between b and c, the lemma above will enable us to get effective upper bounds for c in every case. This will be done in the next sections.

5 Large, medium and small solutions

We now start with the remaining cases in Theorem 1. Observe that we always have $c \leq 11b^6$ and therefore by Lemma 5 we have $z_0 = z_1 = s, x_0 = 0, y_1 = \pm r$.

We start with the case of large solutions, i.e. with $b^3 \leq c < 11b^6$. We have the following lower bound for n.

Lemma 13. *If $v_m = w_n, n \neq 0, 1$ and $b^3 \leq c < 11b^6$, then $n > c^{\frac{1}{12}}$.*

Proof. We again start with the relation in Lemma 2(iii), which reads here as $m^2 s \equiv bn^2 s \pm tnr \pmod{4c}$. Assume that $n \leq c^{\frac{1}{12}}$. Since $\max\{m^2 s, tnr\} < bn^2 s$, and

$$bn^2 s < c^{\frac{1}{3}} \cdot c^{\frac{1}{6}} \cdot c^{\frac{1}{2}} = c,$$

we have equality in the congruence above, thus $m^2 s = bn^2 s \pm tnr$. This implies $4n^2 s > n(bsn - tr)$ and therefore

$$\frac{b\sqrt{c}}{2} n < (b-4)sn < tr < b\sqrt{c},$$

which gives a contradiction. $\square$

Combining the previous lemma with the result from Baker's theory from Lemma 12, we get part (iii) of Theorem 1.

Proposition 2. *Let $\{1, b, c, d\}$ with $1 < b < c < d$ be a $D(-1)$-quadruple. If $b^3 \leq c \leq 11b^6$, then $c < 0.55 \cdot 10^{237}$ and $d < 10^{10^{20}}$.*

Proof. Since $b^3 \leq c$, we get $\log(2.02bc) < 1.50 \log c$ and therefore it follows by Lemma 12 that

$$\frac{n-1}{\log(240.54n)} < 0.29 \cdot 10^{13} \cdot \frac{4}{3}(\log c)^2 < 0.56 \cdot 10^{15}(\log n)^2,$$

where we have used Lemma 13. Hence, $n < 0.20 \cdot 10^{17}$ and therefore $c < 0.55 \cdot 10^{237}$.

From Lemma 3 we get $z = v_m < 4c^2(4c-2)^{m-1} \leq 4^m c^{m+1}$. Consequently,

$$d \leq \frac{z^2+1}{c} \leq \frac{4^{2m}c^{2m+2}}{c} = 16^m c^{2m+1}.$$

Thus, $\log_{10} d \leq m \log_{10} 16 + (2m+1)\log_{10} c \leq 0.19 \cdot 10^{20}$ and therefore $d \leq 10^{10^{20}}$. $\square$

Next we handle the case of medium size solutions, i.e. with $b^{1.1} \leq c < b^3$, and therefore prove part (iv) of Theorem 1.

Lemma 14. *Let $v_m = w_n, n \neq 0, 1$, and $b^{1.1} \leq c < b^3$. If we moreover assume that $c > 10^{100}$, then $n \geq c^{0.04}$.*

Proof. We will consider the congruence of Lemma 2(iii). As in the lemmata above, we have

$$s(m^2 - bn^2) \equiv \pm rtn \pmod{4c}. \tag{13}$$

Let us define integers A and B by

$$A = 2bc - 2rst - c,$$
$$B = 2bc + 2rst - c.$$

We have $AB = c^2 + 4b^2c - 4b - 4c + 4$. Clearly, $B < 4bc$ and $A > \frac{4b^2c}{4bc} = b$. On the other hand, $A < \frac{c^2+4b^2c}{2bc} < c$. This implies that $2rst > 2bc - 2c$, $B > 4bc - 3c$ and

$$A < \frac{c^2 + 4b^2c}{4bc - 3c} < \frac{c}{3b} + \frac{4}{3}b < 0.334c^{0.75} + 1.334c^{0.91} < c^{0.92},$$

which shows that A is small compared with c. Observe that here we use that $c > 10^{100}$.

Multiplying both sides of (13) by $2s$, we get

$$2(m^2 - bn^2) \equiv \mp An \pmod{c}.$$

Assume now that $n \neq 0$ and $n < c^{0.04}$. Then $An < c$ and $|2(m^2 - bn^2)| \leq 2bn^2 < 2c^{0.91+0.08} < c$. Hence, we have an equality:

$$2bn^2 - 2m^2 = An. \tag{14}$$

The relation (14) and the inequalities $n \leq m \leq 2n$ (cf. Lemma 2(ii)) imply

$$2(b-4)n \leq A \leq 2(b-1)n. \tag{15}$$

Let us define β by

$$c = 4b^2(2n-1) + \beta.$$

We claim that $|\beta| < c^{0.56}$.

Let us first estimate the quantity γ defined by $\gamma = 4bA - c - 4b^2$. From $AB = c^2 + 4b^2c - 4b - 4c + 4$ and $4bc - 3c < B < 4bc$, we obtain

$$\gamma > \frac{1}{4bc}(-16b^2 - 16bc + 16b) > -8,$$
$$\gamma < \frac{3c + 12b^2}{3b} = \frac{c}{b} + 4b.$$

Therefore, $|\gamma| < c^{0.92}$. Furthermore, from (15) we have $4bA = 8b^2n + \delta$, where $|\delta| \leq 32bn < c^{0.966}$. Since $\beta = \delta - \gamma$, we get by putting these estimates together that

$$|\beta| < c^{0.966} + c^{0.92} < 2c^{0.966} < c^{0.97}.$$

Hence,

$$c = 4b^2(2n-1) + \beta, \quad |\beta| < c^{0.97}. \tag{16}$$

Analyzing (16) we will improve this estimate for $|\beta|$. Namely, (16) clearly implies $4b^2 < c < 16nb^2$. It follows that $|\gamma| < \frac{c}{b} + 4b < 20bn < 10n\sqrt{c} < c^{0.55}$, and also $|\delta| < 32bn < c^{0.553}$. Hence, $|\beta| < c^{0.56}$, as we claimed.

Now we are ready to finish our argument. By squaring (14), we get

$$4(bn^2 - m^2)^2 \equiv 4(b-1)n^2 \pmod{c},$$

which implies

$$-n^4\beta \equiv (2n-1)(4(b-1)n^2 - 4m^4 + 8bm^2n^2) \pmod{c}. \tag{17}$$

But the absolute values of both sides of (17) are less that $c^{0.72}$. Hence, we have the equality in (17), and this implies (assuming that $n \neq 0$)

$$n^2 c = (2n-1)(A^2 - 4(b-1)).$$

Since $A^2 \equiv 4(b-1) \pmod{c}$, we find that $(2n-1)|n^2$, which is possible only if $n = 0$ or $n = 1$. We obtained a contradiction, and hence we proved that $n \geq c^{0.04}$ $\square$

Combining this lower bound with the upper bound which follows from Lemma 12, we will again obtain that c is bounded by an absolute constant.

Proposition 3. *Let $\{1, b, c, d\}$ with $1 < b < c < d$ be a $D(-1)$-quadruple. If $b^{1.1} \leq c < b^3$, then $c < 0.30 \cdot 10^{491}$ and $d < 10^{10^{23}}$.*

Proof. Since $b \leq c^{0.91}$, we get $\log(2.02bc) \leq 1.93 \log c$ and $\log(bc) \leq 1.91 \log c$. Now, by Lemma 14 and Lemma 12 we get

$$\frac{n-1}{\log(309.50n)} < 0.40 \cdot 10^{15} \left(\log n\right)^2.$$

Hence, $n < 0.42 \cdot 10^{20}$ and thus $c < 0.30 \cdot 10^{491}$.

As in the proof of Proposition 2, we get by Lemma 3 that $\log_{10} d \leq 2n \log_{10} 16 + (4n+1) \log_{10} c \leq 0.82 \cdot 10^{23}$ and therefore $d \leq 10^{10^{23}}$. $\square$

Finally, we turn to part (v) of Theorem 1. This is the case of small solutions, i.e. with $3b < c < b^{1.1}$.

To get the lower bounds for m, n in terms of some small power of c in the case of small solutions, we will use the following very useful construction, which in fact is the essence of the gap principle in Lemma 4.

Lemma 15. *Let $\{a, b, c\}$ be a $D(-1)$-triple. Define*

$$e = -(a+b+c) + 2abc - 2rst.$$

Then there exist integers u, v, w such that

$$ae + 1 = u^2, be + 1 = v^2, ce + 1 = w^2$$

and

$$c = a + b - e + 2(abe + ruv).$$

Proof. This lemma is a special case of Lemma 3 in [14]. $\square$

Using this lemma we now prove:

Lemma 16. *If $v_m = w_n, n \neq 0, 1, 2$ and $3b < c < b^{1.1}$, then $n \geq 0.25 \cdot c^{0.2}$.*

Proof. With the same notation as in Lemma 14, again we have the congruence

$$2(m^2 - bn^2) \equiv \mp An \pmod{c}. \tag{18}$$

In this case we get

$$A < \frac{c^2 + 4b^2c}{4bc - 3c} = b + \frac{c + 3b}{4b - 3} < b + \frac{2c}{3b}.$$

Hence, $A = b + \alpha$, where $0 < \alpha < c^{0.1}$.

By Lemma 15, there exist integers e, u, v, w such that

$$e + 1 = u^2, \quad be + 1 = v^2, \quad ce + 1 = w^2,$$

and

$$b = 1 + c - e + 2ce - 2suw.$$

Hence, $(b + e - 1)^2 \equiv 4(c - 1)(e + 1)(ce + 1) \equiv -4(e + 1) \pmod{c}$, and

$$b^2 + 2b(e - 1) + e^2 + 2e + 5 \equiv 0 \pmod{c}. \tag{19}$$

Moreover, e is small compared with c. Indeed, from $c = 1 + b - e + 2be + 2ruv > 2be$, we find that $e < \frac{c}{2b} < c^{0.1}$.

Now (18) implies

$$2m^2 \pm \alpha n \equiv b(2n^2 \mp n) \pmod{c}. \tag{20}$$

From (20), we also get

$$(2m^2 \pm \alpha n)^2 \equiv b^2(2n^2 \mp n)^2 \pmod{c} \tag{21}$$

and

$$2(e - 1)(2n^2 \mp n)(2m^2 \pm \alpha n) \equiv 2(e - 1)b(2n^2 \mp n)^2 \pmod{c}. \tag{22}$$

By summing (21) and (22), and taking into account (19), we obtain

$$\begin{aligned}(2n^2 \mp n)^2(e^2 + 2e + 5) + (2m^2 \pm \alpha n)^2 \\ +2(e - 1)(2n^2 \mp n)(2m^2 \pm \alpha n) \equiv 0 \pmod{c}.\end{aligned} \tag{23}$$

Assume now that $n < 0.25 \cdot n^{0.2}$.

Since $n \geq 3$, $e \geq 3$, $m \leq 2n$ and $c \geq 82$, we have the following estimates:

$$\left|(2n^2 \mp n)^2(e^2+2e+5)\right| \leq 6n^4 \cdot 3e^2 \cdot \frac{18c^{0.8}}{256} \cdot \frac{c^2}{4b^2} < 0.02c,$$
$$(2m^2 \pm \alpha n)^2 \leq 8m^4 + \alpha^2 n^2 \leq \frac{c^{0.8}}{2} + \frac{c^{0.6}}{8} < 0.23c,$$

and

$$\left|2(e-1)(2n^2 \mp n)(2m^2 \pm \alpha n)\right| \leq 6en^2(2m^2+\alpha n) \leq \frac{3c^{0.5}}{8}\frac{c^{0.4}}{2} < 0.13c.$$

Therefore, we have the equality in (23), i.e.

$$(e^2+2e+5)X^2 + 2(e-1)(e-1)XY + Y^2 = 0, \tag{24}$$

where $X = (2n^2 \mp n)$, $Y = 2m^2 \pm \alpha n$. Since the discriminant of (24) is negative (it is equal to $-16u^2$), we conclude that by multiplying (24) with $4(e^2+2e+5)$ we get

$$\big(2(e^2+2e+5)X + 2(e-1)^2 Y\big)^2 + 16u^2Y^2 = 0.$$

This implies $X = Y = 0$, which in turn gives $n = 0$, a contradiction. Hence, we proved that $n \geq 0.25 \cdot c^{0.2}$. $\square$

Again by using Lemma 12 we will obtain that c is bounded by an absolute constant.

Proposition 4. *Let $\{1, b, c, d\}$ with $1 < b < c < d$ be a $D(-1)$-quadruple. If $3b < c < b^{1.1}$, then $c < 0.66 \cdot 10^{94}$ and $d < 10^{10^{21}}$.*

Proof. Since $b < \frac{c}{3}$, we have $\log(2.02bc) \leq 2\log(0.83c) < 2\log c$ and $\log(bc) \leq 2\log\frac{c}{9}$. By $c \leq 1024n^5$ (cf. Lemma 16) and Lemma 12 it follows that

$$\frac{n-1}{\log(320.72n)} < 0.66 \cdot 10^{12} \cdot \log(1024n^5)\log(113.78n^5).$$

Hence, $n \leq 0.15 \cdot 10^{19}$ and $c \leq 0.66 \cdot 10^{94}$.

By Lemma 3 we get $\log_{10} d \leq 2n\log_{10} 16 + (4n+1)\log_{10} c \leq 0.55 \cdot 10^{21}$ and therefore $d \leq 10^{10^{21}}$. $\square$

It remains to prove the smallest possible case, i.e. when we have $c < 3b$. This will be done in the following section.

6 Very small solutions

Now we consider the case $c = 1 + b + 2\sqrt{b-1}$ of very small solution (part (vi) in Theorem 1). Observe that we are left to consider $c \leq 3b$. By the gap principle (Lemma 4), this implies that we have indeed $c = 1 + b + 2r$. We can write everything parametrized in r. To avoid confusions we set $k = r$ in this section. Then we have to consider the $D(-1)$-triple

$$\{1, k^2 + 1, (k+1)^2 + 1\}.$$

Moreover, we have

$$s = k + 1, t = k^2 + k + 1, z_0 = z_1 = k + 1, x_0 = 0, y_1 = \pm k,$$

and $k \geq 8$.

If $v_m = w_n, n \neq 0, 1$ then the congruence from Lemma 2(iii) has the form

$$\begin{aligned} m^2(k+1) &\equiv n^2(k^2+1)(k+1) \pm n(k^2+k+1)k \\ &\equiv n^2(k+3) \mp n(k+1) \qquad (\mathrm{mod}\ (k^2+2k+2)). \end{aligned} \tag{25}$$

We start by proving an upper bound for k in terms of n.

Lemma 17. *In this case, if $v_m = w_n, n \neq 0, 1$, then $k < 16n^2$.*

Proof. Assume that $n^2 \leq \frac{1}{16}k$. We have the following estimates

$$\begin{aligned} &m^2(k+1) \leq 4n^2(k+1) < k(k+1) < k^2 + 2k + 2, \\ &\left|n^2(k+3) \pm n(k+2)\right| < \frac{1}{4}k(k+3) + \frac{1}{2}\sqrt{k}(k+1) < k^2 + 2k + 2. \end{aligned}$$

Therefore we have an equality in (25), which gives

$$m^2(k+1) = n^2(k+3) \mp n(k+1).$$

This implies $m^2 \equiv 3n^2 \mp n \pmod{k}$. Since $m^2 \leq 4n^2 < k$ and $|3n^2 \mp n| < \frac{3}{4}k + \frac{1}{4}\sqrt{k} < k$, we have again an equality. This implies $m^2 = 3n^2 \mp n$. Moreover, we now also have the equation $m^2 = n^2 \mp n$. Combining these two facts, we get $2n^2 = \pm n$ and therefore $n = 0$, a contradiction. This proves the lemma. $\square$

We conclude the proof by combining Lemma 17 with Lemma 12 as in all cases above, to get an effective upper bound for k and therefore for c and d.

Proposition 5. *Let $\{1, k^2+1, (k+1)^2+1, d\}$ be a $D(-1)$-quadruple. Then $k < 0.14 \cdot 10^{38}$ and therefore $c = (k+1)^2 + 1 < 0.19 \cdot 10^{75}$ and $d < 10^{10^{21}}$.*

Proof. We have $\log(2.02bc) = \log(2.02(k^2+1)(k^2+2k+1)) \leq 4.46 \log k$ and $\log(k^2 + 2k + 2) > \log k$. By combining Lemma 17 and Lemma 12 we get

$$\frac{n-1}{\log(715.21n)} < 0.33 \cdot 10^{12} \log\left((16n^2+1)^2+1\right) \cdot \log\left(((16n^2)+1)((16n^2+1)^2+1)\right).$$

This implies $n < 0.93 \cdot 10^{18}$ and therefore $k < 0.14 \cdot 10^{38}$.

Moreover, we get $c = (k+1)^2 + 1 < 0.19 \cdot 10^{75}$ and by Lemma 3 we have $\log_{10} d \leq 2n \log_{10} 16 + (4n+1) \log_{10} c \leq 0.21 \cdot 10^{21}$ and finally this gives $d < 10^{10^{21}}$. □

Altogether, by combining Propositions 1, 2, 3, 4 and 5 above, we get Theorem 1. Theorem 2, as well as Corollary 1 and 2 are immediate consequences.

7 Quantitative result

We start by collecting two lemmata which will be needed for the proof of Theorem 3. In the following, $\omega(c)$ will denote, as usual, the number of different prime divisors of an integer c.

Lemma 18. *Let $c \in \mathbb{N}$. The number of solutions $x \in \mathbb{Z}$ of the quadratic congruence*

$$x^2 \equiv -1 \pmod{c}$$

is bounded by $2^{\omega(c)}$.

Proof. This statement can be found in [37, p. 94]. □

We remark that the congruence has no solution if 3 or 4 divides c. Moreover, if c is even, then the number of solutions is bounded by $2^{\omega(c)-1}$.

Lemma 19. *Let $c \in \mathbb{N}$. Then $\log(c) > \frac{1}{2}\omega(c) \log \omega(c)$.*

Proof. This can be found in [17]. The proof follows from results in [36]. □

Now we are ready to prove the quantitative result.

Proof of Theorem 3.

Let $\{1, b, c, d\}$ be a $D(-1)$-quadruple. By Theorem 1 it follows that

$c < 10^{492}$ and $d < 10^{10^{23}}$. Let us first consider the triple $\{1, b, c\}$ with $b < c < 10^{492}$. We have $b - 1 = r^2, c - 1 = s^2$ and therefore $r < s < 10^{246}$. It is clear that the number of such triples is bounded by 10^{492}.

Let us now assume that $\{1, b, c\}$ is fixed. Then, by Lemma 1, the number d is an element of the union of finitely many binary recurrent sequences (arising from (9) for some z_0 with $z_0^2 = cd-1$ and $0 < z_0 < c$). The number of such sequences is less than or equal to the number of solutions of the congruence $z_0^2 \equiv -1 \pmod{c}$. Consequently, this number is bounded by $2^{\omega(c)}$ by Lemma 18.

Let us assume that $2^{\omega(c)} \geq c^{0.787}$. By Lemma 19 we have $c > \omega(c)^{\frac{\omega(c)}{2}}$ and therefore

$$2^{\omega(c)} \geq c^{0.787} > \omega(c)^{0.3935\omega(c)}.$$

This implies $\omega(c) \leq 5$. Hence, $c \leq 81.76$ and therefore a contradiction, since $c \geq 82$. This gives

$$2^{\omega(c)} < c^{0.787}$$

and it follows that the number of recurrences mentioned above is bounded by

$$2^{\omega(c)} < c^{0.787} \leq 10^{388},$$

because of the upper bound for c.

On the other side, the sequences grow exponentially, namely by Lemma 3 we have

$$(c-1)(4c-3)^{m-1} < v_m = z = \sqrt{cd-1} < 10^{10^{23}}.$$

Since $b \geq 82$ we conclude that

$$81(4 \cdot 82 - 3)^{m-1} < 10^{10^{23}}$$

and therefore $m < 10^{23}$. Therefore the number of d's which extend the set $\{1, b, c\}$ to a $D(-1)$-quadruple is at most 10^{411}.

Altogether, the number of $D(-1)$-quadruples is bounded by

$$10^{492} \cdot 10^{411} = 10^{903}$$

and therefore we have proved Theorem 3. □

8 Acknowledgements

This paper was partly written 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); the authors would like to thank them for this support. Moreover, the first author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 0037110 and the third author was supported by the Austrian Science Foundation FWF, grant J2407-N12.

References

[1] Abu Muriefah F. S. and Al-Rashed A. On the extendibility of the Diophantine triples $\{1, 5, c\}$, *Int. J. Math. Math. Sci.* **33** (2004), 1737-1746.

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

[3] Baker A. and Wüstholz G. Logarithmic forms and group varities, *J. Reine Angew. Math.* **442** (1993), 19-62.

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

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

[6] Dickson L. E. History of the Theory of Numbers, Vol. 2, Chelsea, New York, 1966, 513-520.

[7] Diophantus of Alexandria Arithmetics and the Book of Polygonal Numbers, (I. G. Bashmakova, Ed.), Nauka, Moscow, 1974 (in Russian).

[8] Diophantus von Alexandria, Die Arithmetik und die Schrift ber Polygonalzahlen, (G. Wertheim, Ed.), Teubner, Leipzig, 1890.

[9] Dujella A. Generalization of a problem of Diophantus, *Acta Arith.* **65** (1993), 15-27.

[10] Dujella A. 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.

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

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

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

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

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

[16] Dujella A. Bounds for the size of sets with the property $D(n)$, *Glas. Mat. Ser. III* **39** (2004), 199-205.

[17] Dujella A. On the number of Diophantine m-tuples, *Ramanujan J.*, to appear (Preprint: http://www.math.hr/~duje/dvi/number.dvi).

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

[19] Dujella A. and Fuchs C. Complete solution of a polynomial version of a problem of Diophantus, *J. Number Theory* **106** (2004), 326-344.

[20] Dujella A. and Fuchs C. Complete solution of a problem of Diophantus and Euler, *J. London Math. Soc. (2)* **71** (2005), 33-52.

[21] Dujella A. and Luca F. Diophantine m-tuples for primes, *Intern. Math. Research Notices* **47** (2005), 2913-2940.

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

[23] Filipin A. Non-extendibility of $D(-1)$-triples of the form $\{1, 10, c\}$, *Int. J. Math. Math. Sci.* **35** (2005) 2217-2226.

[24] Fujita Y. The extendibility of $D(-1)$-triples $\{1, b, c\}$, *Publ. Math. Debrecen*, to appear.

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

[26] Gupta H. and Singh K. On k-triad sequences, *Internat. J. Math. Math. Sci.* **5** (1985), 799-804.

[27] Heath T. L. 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.

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

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

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

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

[32] Matveev E. M. An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic number. II (Russian), *Izv. Ross. Akad. Nauk. Ser. Math.* **64** (2000), no. 6, 125-180.

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

[34] Mohanty S. P. and Ramasamy A. M. S. On $P_{r,k}$ sequences, *Fibonacci Quart.* **23** (1985), 36-44.

[35] Rickert J. H. Simultaneous rational approximation and related Diophantine equations, *Math. Proc. Cambridge Philos. Soc.* **113** (1993), 461-472.

[36] Rosser J. B. and Schoenfeld L. Approximation formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64-94.

[37] Vinogradov I. M. *Elements of Number Theory*, Dover, New York, 1954.

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

[39] Zheng D. X. 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.