ON $D(-1)$-QUADRUPLES

Nicolae Ciprian Bonciocat, Mihai Cipu,
and Maurice Mignotte

Abstract: Quadruples (a, b, c, d) of positive integers $a < b < c < d$ with the property that the product of any two of them is one more than a perfect square are studied. Improved lower and upper bounds for the entries b and c are established. As an application of these results, a bound for the number of such quadruples is obtained.

2010 Mathematics Subject Classification: 11D09, 11D45, 11B37, 11J68.

Key words: Diophantine m-tuples, Pell equations, linear forms in logarithms.

1. Introduction

A set of positive integers is called $D(-1)$-set if the product of any two distinct elements of it is one more than a perfect square. Dujella and Fuchs [**7**] proved that there exists no $D(-1)$-set with more than four elements. It is also known [**6**] that there are finitely many $D(-1)$-quadruples. This is the best available result towards the conjecture [**4**] that there exists none.

As far as we know, the best result in this direction is due to Filipin and Fujita [**10**], who prove that there exist at most 10^{356} $D(-1)$-quadruples. One of the results obtained in the present paper is the following absolute bound for the number of $D(-1)$-quadruples.

Theorem 1.1. *The number of $D(-1)$-quadruples is less than $4 \cdot 10^{70}$.*

The proof idea already appeared in [**5**]: consider an initial subsequence of a $D(-1)$-quadruple and estimate the number of possibilities to extend it without loosing the defining property. The novelty here is the systematic use of the fact that, with the exception of the first entry, all entries have only odd prime divisors congruent to 1 mod 4. All

integers of the form $x^2 + 1$ have in common this property, along with another useful property —they are either odd or twice an odd number.

In the course of the proof there are needed estimates for the entries of a $D(-1)$-triple (a, b, c) supposedly extendable to a $D(-1)$-quadruple. According to the best published ones, one has $a = 1$, $101 \leq b < c < \min\{11\,b^6, 10^{491}\}$. Moreover, the absolute upper bound for the third entry can be substantially smaller if c is between smaller powers of b (see [6, Theorem 1]). We improve on this result by examining a finer stratification of the search space for c.

Theorem 1.2. *Let $(1, b, c, d)$ with $1 < b < c < d$ be a $D(-1)$-quadruple. Then $b > 1.024 \cdot 10^{13}$ and $\max\{10^{14}b, b^{1.16}\} < c < \min\{2.5\,b^6, 10^{148}\}$. More precisely:*

i) *If $b^5 \leq c < 2.5\,b^6$ then $c < 10^{100}$.*

ii) *If $b^4 \leq c < b^5$ then $c < 10^{82}$.*

iii) *If $b^{3.5} \leq c < b^4$ then $c < 10^{66}$.*

iv) *If $b^3 \leq c < b^{3.5}$ then $c < 10^{57}$.*

v) *If $b^2 \leq c < b^3$ then $c < 10^{111}$.*

vi) *If $b^{1.5} \leq c < b^2$ then $c < 10^{109}$.*

vii) *If $b^{1.4} \leq c < b^{1.5}$ then $c < 10^{128}$.*

viii) *If $b^{1.3} \leq c < b^{1.4}$ then $c < 10^{148}$.*

ix) *If $b^{1.2} \leq c < b^{1.3}$ then $c < 10^{133}$.*

x) *If $b^{1.16} \leq c < b^{1.2}$ then $c < 10^{107}$.*

The statement is an illustration of one of our guiding paradigms, smoothification. At first sight, this means cutting the search domain in many fine slices. More important aspects of the idea will be discussed in Section 3, when all the relevant definitions and notation will be available.

The proof of Theorem 1.2 is based on a study of the system of three generalized Pell equations attached to a hypothetical $D(-1)$-quadruple $(1, b, c, d)$ (see equations (3) to (5) in Section 2). The positive solutions of each individual equation are expressed in terms of the fundamental ones in the usual way. This gives rise, on the one hand, to linear forms in the logarithms of three algebraic numbers and, on the other hand, to linear recurrent sequences. Each of these objects provide useful information on the quadruple under scrutiny. In order to deal with sequences of the type encountered below in equations (8) and (9), Dujella and Pethő introduced the congruence method in [8]. The idea is to consider the recurrent relations modulo c^2 and prove that, under suitable hypotheses,

such congruences turn into equalities. We adopt a different standpoint and use a variant of this idea. Details are found also in Section 3.

A third source of improvements in comparison to published results is the heavy use of computer-aided calculations. The goal is to eliminate small values of various parameters attached to a hypothetical $D(-1)$-quadruple.

The outcome of some large-scale computations is reported in Section 2, where a variety of necessary conditions that must be satisfied by a $D(-1)$-quadruple are tightened by either rising the lower bounds or lowering the upper bounds. Section 3 contains the proof of a variant of Theorem 1.2. Here we use the linear form in logarithms corresponding to the pair of generalized Pell equations involving the third component of a putative $D(-1)$-quadruple. The proof of Theorem 1.2 is completed in Section 4 with the help of an other linear form in three logarithms generated from the system of generalized Pell equations attached to the $D(-1)$-quadruple under study. Theorem 1.2 is applied in the proof of Theorem 1.1, which is given in the final section of the paper.

2. Preparations for the proofs of the main results

The aim of this section is to slightly improve published results on hypothetical $D(-1)$-quadruples. Our strategy consists in strengthening of necessary conditions that must be satisfied by such a quadruple. The combined use of several tools results in higher lower bounds for several parameters naturally attached to the object of study and in more precise information on them.

Below (a, b, c, d) is a $D(-1)$-quadruple with $a < b < c < d$. Then $a = 1$ (see [7]) and $b > 100$ by results proved in [1], [3], [11], and [16]. Moreover, one also knows that $c < 11\, b^6$ (see [6]). Combining a very recent result of He and Togbé [12] with Lemma 7 in [7] one obtains that $c > 3b$. Our first contribution is a slight improvement of the gap between the second and third entries of a hypothetic $D(-1)$-quadruple.

The setting is as follows. To a putative $D(-1)$-quadruple $(1, b, c, d)$ with $1 < b < c < d$ and $c < 11\, b^6$ one associates positive integers r, s, t, x, y, z defined by

$$(1) \qquad b - 1 = r^2, \quad c - 1 = s^2, \quad bc - 1 = t^2,$$

$$(2) \qquad d - 1 = x^2, \quad bd - 1 = y^2, \quad cd - 1 = z^2.$$

Eliminating d in equation (2), one obtains a system of three generalized Pell equations

$$(3) \qquad\qquad z^2 - cx^2 = c - 1,$$

$$(4) \qquad\qquad bz^2 - cy^2 = c - b,$$

$$(5) \qquad\qquad y^2 - bx^2 = b - 1.$$

The positive integer solutions of each of these equations are respectively given by

$$z + x\sqrt{c} = (z_0 + x_0\sqrt{c})(s + \sqrt{c})^{2m}, \qquad m \geq 0,$$

$$z\sqrt{b} + y\sqrt{c} = (z_1\sqrt{b} + y_1\sqrt{c})(t + \sqrt{bc})^{2n}, \quad n \geq 0,$$

$$y + x\sqrt{b} = (y_2 + x_2\sqrt{b})(r + \sqrt{b})^{2l}, \qquad l \geq 0,$$

for suitable integers $0 < z_0 < c$, $|x_0| < s$, $0 < z_1 < bc$, $|y_1| < t$, $0 < y_2 < b$, $|x_2| < r$. In [6] it is shown that for $c < b^9$ one has $x_0 = 0$, $z_0 = z_1 = s$, $y_1 = \rho r$ for a fixed $\rho \in \{-1, 1\}$. Therefore, the solutions (x, y, z) satisfy

$$(6) \qquad\qquad z = v_m = w_n,$$

where m, n are positive integers such that

$$(7) \qquad\qquad m \equiv n \pmod 2, \quad n \leq m \leq 2n,$$

and the integer sequences $(v_p)_{p\geq 0}$, $(w_p)_{p\geq 0}$ are given by explicit formulæ

$$(8) \qquad\qquad v_p = \frac{s}{2}\left((s + \sqrt{c})^{2p} + (s - \sqrt{c})^{2p}\right)$$

and respectively

$$(9) \qquad w_p = \frac{s\sqrt{b} + \rho r\sqrt{c}}{2\sqrt{b}}(t + \sqrt{bc})^{2p} + \frac{s\sqrt{b} - \rho r\sqrt{c}}{2\sqrt{b}}(t - \sqrt{bc})^{2p}.$$

All these assertions are established in [6].

Equation (6) gives rise to a linear form in the logarithms of three algebraic numbers

$$(10) \qquad \Lambda = 2n\log(t + \sqrt{bc}) - 2m\log(s + \sqrt{c}) + \log\frac{s\sqrt{b} + \rho r\sqrt{c}}{s\sqrt{b}},$$

which plays an important role all over the paper.

2.1. Gap principle. Our work uses the next improved gap principle.

Lemma 2.1. *Let $(1, b, c, d)$ be a $D(-1)$-quadruple with $1 < b < c < d$. Then $c > (7 + 3\sqrt{5})b > 13.7\,b$.*

Proof: Put $f = t - rs$, $g = bs - rt$, $h = st - cr$, and $e = 2bc - 2rst - c - b - 1$. Then it is routine to verify that f, g, h are positive, e is nonnegative, and

$$e + 1 = f^2, \quad be + 1 = g^2, \quad ce + 1 = h^2,$$

$$c = 1 + b + (2b - 1)e + 2rfg.$$

Therefore, if $e = 0$ then $f = g = 1$ and $c = 1 + b + 2r$. Having in view equation (1), it results $s = r + 1$. However, He and Togbé have just proved [**12**] that there is no $D(-1)$-quadruple with $s = r + 1$. Hence, $f \geq 2$, whence $e \geq 3$ and

$$c \geq 1 + b + 3(2b - 1) + 4\sqrt{(b - 1)(3b + 1)} > (7 + 3\sqrt{5})b > 13.7\,b. \qquad \square$$

2.2. Improved relative upper bound on c. A close look at Fujita's paper [**11**] suffices to squeeze a little bit the numerical coefficient in the inequality $c < 11b^6$. This has already been noticed by Tamura [**16**]. Since this work is not published yet, we prefer to sketch the argument.

Lemma 2.2. *Let b and N be integers with $b \geq 101$ and $N \geq 2.39b^7$. Then the numbers*

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

satisfy

$$\max\left\{\left|\theta_1 - \frac{p_1}{q}\right|, \left|\theta_2 - \frac{p_2}{q}\right|\right\} > \left\{32.001\,\frac{b^2(b - 1)^2}{2b - 1}N\right\}^{-1}q^{-1-\lambda}$$

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

$$\lambda = \frac{\log \frac{16.0005\,b^2(b-1)^2 N}{2b-1}}{\log \frac{3.3749\,N^2}{b^2(b-1)^2}}.$$

Proof: In the notation introduced in the proof of Lemma 3.6 of [**11**], one has

$$DP = 2b^2(b - 1)^2\frac{8}{2b - 1}\left(1 + \frac{3}{2N}\right) < \frac{16.0005\,b^2(b - 1)^2 N}{2b - 1}$$

and

$$2pDP < \frac{32.001\, b^2(b-1)^2 N}{2b-1}, \quad \frac{L}{D} = \frac{27}{4} \cdot \frac{\left(1-\frac{b-1}{N}\right)^2 N^2}{2b^2(b-1)^2 N} \geq \frac{3.3749\, N^2}{b^2(b-1)^2}.$$

The rest of the proof goes as in *loc.cit.*   □

It is easy to prove the following estimate (see [**11**, Lemma 3.7]): Let $N = t^2$ and θ_1, θ_2 as above, then all the solutions (x, y, z) of the simultaneous Pell-Fermat equations

$$\begin{cases} z^2 - cx^2 = c - 1, \\ bz^2 - cy^2 = c - b \end{cases}$$

satisfy

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

These inequalities are employed as in the proof of Theorem 3.5 from [**11**] to conclude an upper bound on y.

Proposition 2.1. *If* $b \geq 101$ *and* $c \geq 2.4b^6$ *then*

$$\log y < \frac{2 \log \frac{1.8371\, c}{b-1} \cdot \log(16.001\, b^6 c^2)}{\log \frac{0.4135\, c}{b^6}}.$$

Proof: On noting that $c \geq 2.4\, b^6$ implies $N = t^2 = bc - 1 > 2.39\, b^7$, from the above study applied for $p_1 = bsx$, $b_2 = bz$, and $q = ty$ we get

$$\left\{ 32.001 \frac{b^2(b-1)^2}{2b-1} t^2 \right\}^{-1} (ty)^{-1-\lambda} < \frac{b-1}{y^2}.$$

Since $\lambda < 1$, this implies

$$y^{1-\lambda} < 32.001 \frac{b^2(b-1)^3}{2b-1} t^{3+\lambda} < 32.001 \frac{b^2(b-1)^3(bc-1)^2}{2b-1}.$$

Hence,

$$\log y < \frac{\log \frac{3.3749\,(bc-1)^2}{b^2(b-1)^2} \cdot \log \frac{32.001\, b^2(b-1)^3(bc-1)^2}{2b-1}}{\log \frac{3.3749\,(2b-1)(bc-1)}{16.0005\, b^4(b-1)^4}}.$$

Notice that

$$\log \frac{3.3749\,(bc-1)^2}{b^2(b-1)^2} < 2 \log \frac{1.8371\, c}{b-1},$$

$$\log \frac{32.001\, b^2(b-1)^3(bc-1)^2}{2b-1} < \log(16.001\, b^6 c^2),$$

and

$$\log \frac{3.3749\,(2b-1)(bc-1)}{16.0005\,b^4(b-1)^4} > \log \frac{0.4135\,c}{b^4(b-1)^2} > \log \frac{0.4135\,c}{b^6}. \qquad \square$$

From Lemma 2.3 below we get a lower bound on $\log y$

$$m\log(4c-3) < \log y$$

we shall compare with the upper bound just obtained.

Suppose $c = \mu b^6$, with $\mu \geq 2.4$. Then, using the inequality $n > \sqrt{3}(\sqrt{\mu}c)^{1/6}$ we shall shortly prove, we get

$$\sqrt{3}(\sqrt{\mu}c\,)^{1/6}\log(4c-3) < \frac{2\log \frac{1.8371\,c}{b-1} \cdot \log(16.001\,b^6c^2)}{\log \frac{0.4135\,c}{b^6}}.$$

After some tiny simplifications, this is

$$f(c) := \frac{2\log 0.0184\,c \cdot \log(16.001\,c^3/\mu)}{\log(0.4135\,\mu)} - \sqrt{3}\mu^{1/6}c^{1/6}\log(4c-3) > 0.$$

Then a computer verification shows that the previous inequality does not hold for $c \geq 101^6$ and $\mu = 2.5$.

Thus we have proved the following result.

Theorem 2.1. *If $(1,b,c,d)$ is a $D(-1)$-quadruple with $100 < b < c < d$ then*

$$c < 2.5\,b^6.$$

Lemma 2.3. *Keep the notation introduced in the proof of Proposition 2.1. Then $m\log(4c-3) < \log y$.*

Proof: There is nothing to prove for $m = 0$, so assume m is positive. From

$$x = \frac{s}{2\sqrt{c}}\big((s+\sqrt{c})^{2m} - (s-\sqrt{c})^{2m}\big)$$

and $y^2 - bx^2 = r^2$ it results

$$y > x\sqrt{b} = \frac{s\sqrt{b}}{2\sqrt{c}}\big((s+\sqrt{c})^{2m} - (s-\sqrt{c})^{2m}\big)$$

$$> \frac{10s}{2\sqrt{c}}\big((s+\sqrt{c})^{2m} - (s-\sqrt{c})^{2m}\big)$$

$$> \frac{9s(s+\sqrt{c})^{2m}}{2\sqrt{c}} > (s+\sqrt{c})^{2m} > (4c-3)^m. \qquad \square$$

Lemma 2.4. *If $c \geq \max\{\mu b^6, 3\sqrt{3}\mu^{1/4}b^3\}$ then $n > \sqrt{3}\mu^{1/12}c^{1/6}$.*

Proof: We reason by reduction to absurd. From [**7**, Lemma 2 iii)] we have

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

Assuming $n \leq \sqrt{3}\mu^{1/12}c^{1/6}$, we get

$$|s(bn^2 - m^2)| \leq s(b-1)n^2 < 3sb\mu^{1/6}c^{1/3} < 3c^{1/2+1/6+1/3} = 3c,$$

$$rtn < b^{1/2} \cdot (bc)^{1/2} \cdot \sqrt{3}\mu^{1/12}c^{1/6} = \sqrt{3}\,\mu^{1/12}\,b\,c^{2/3} \leq c.$$

It results $s(bn^2 - m^2) = rtn$, whence $(b-1)(bc-1)n^2 = (c-1)(bn^2 - m^2)^2 \geq (c-1)(b-4)^2n^4$. Since $n \geq 3$ by [**7**, Lemma 6], this readily leads to the contradiction $b < 9$. $\qquad\square$

2.3. Inequalities for m and n. Next we consider the inequalities relating m and n. It is known that $n \leq m \leq 2n$. Our study is based on manipulations of the linear form

$$\Lambda = 2d \log(s + \sqrt{c}) - 2n \log \frac{(s + \sqrt{c})^2}{t + \sqrt{bc}} + \log \theta, \quad d := 2n - m.$$

We first examine the consequences of the equality $m = 2n$. It is proved in [**7**] that m and n are of the same parity and that $v_4 \neq w_2$, thus we suppose $n \geq 4$ and even. Then the linear form becomes

$$\Lambda = \log \theta - 2n \log \frac{(s + \sqrt{c})^2}{t + \sqrt{bc}}.$$

Since $(s + \sqrt{c})^2 > 7(t + \sqrt{bc})$ and Λ is positive (see Lemma 2.6 below), one arrives at the conclusion that $n < 1$, a contradiction that shows that one has $m < 2n$. This inequality can be strengthened as follows.

Lemma 2.5. *The indices m and n satisfy*

$$\frac{2m-1}{2n} < \frac{\log(t + \sqrt{bc})}{\log(s + \sqrt{c})} < \frac{\log(4bc)}{\log(3.996c)}.$$

Proof: From Λ positive we deduce

$$2n \log(t + \sqrt{bc}) - (2m-1)\log(s + \sqrt{c}) > \Lambda + \log(s + \sqrt{c}) - \log \theta$$

$$> \log \frac{s\sqrt{b}(s + \sqrt{c})}{s\sqrt{b} + r\sqrt{c}} > \log s > 0. \quad \square$$

The next result provides not only the information (positivity of Λ) already used in the above proof, but also a tight upper bound for the linear form in logarithms associated to a hypothetic $D(-1)$-quadruple.

Lemma 2.6. $0 < \Lambda < 0.04\,(t + \sqrt{bc})^{-2n}$.

Proof: First of all rewrite the equality $v_m = w_n$ in the equivalent form $P + (c-1)P^{-1} = Q + \frac{c-b}{b}Q^{-1}$, with

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

From

$$P \geq s(2c - 1 + 2s\sqrt{c}) > 4s(c - 1)$$

and

$$Q \geq \frac{s\sqrt{b} - r\sqrt{c}}{\sqrt{b}}(2bc - 1 + 2t\sqrt{bc}) \geq 2c,$$

we get

$$Q - P = (c-1)P^{-1} - \frac{c-b}{b}Q^{-1} > (c-1)(P^{-1} - Q^{-1})$$

$$= (c-1)(Q-P)P^{-1}Q^{-1}.$$

Therefore,

$$0 < Q - P < (c-1)P^{-1} < \frac{1}{4s}.$$

We use the elementary inequality $-\log(1 - x) < 1.01x$ valid for $0 < x < 1/101$ to conclude

$$0 < \Lambda = \log\frac{Q}{P} < 1.01\left(\frac{Q-P}{Q}\right) < \frac{1.01}{4sQ}$$

$$\leq \frac{1.01\sqrt{b}}{4s} \cdot \frac{(t + \sqrt{bc})^{-2n}}{s\sqrt{b} - r\sqrt{c}}$$

$$< \frac{1.01\sqrt{b}}{4s} \cdot \frac{(t + \sqrt{bc})^{-2n}}{c - b} \cdot 2s\sqrt{b} < 0.04\,(t + \sqrt{bc})^{-2n}.$$

In the last inequality in this chain we have invoked the gap principle given in Lemma 2.1. $\qquad\square$

We now focus on the inequality $m \geq n$. It can be refined as follows.

Lemma 2.7. *The indices m and n satisfy*

$$\frac{m}{n} > \frac{\log(bc - 1)}{\log(4c)}.$$

Proof: The claim is obtained by noticing that

$$\frac{m}{n} = \frac{1}{\log(s+\sqrt{c})}\left(\log(t+\sqrt{bc}) - \frac{\Lambda}{2n} + \frac{1}{2n}\log\left(1 + \frac{\rho r\sqrt{c}}{s\sqrt{b}}\right)\right)$$

$$> \frac{\log\sqrt{bc-1}}{\log(2\sqrt{c})} = \frac{\log(bc-1)}{\log(4c)}. \qquad \square$$

Since $c < 2.5\,b^6$ and $b \geq 101$, this implies the following result.

Lemma 2.8. *The indices m and n satisfy*

$$\frac{m}{n} > \frac{\log(2.49\,b^7)}{\log(10\,b^6)} > 1.1075.$$

2.4. Small values of n. In [**7**] it is proved that there is no solution of $w_n = v_m$ for $n = 1$ and $n = 2$. We want to extend this result up to $n = 6$. Indeed, we verify the following.

Proposition 2.2. *There is no solution of $w_n = v_m$ for $1 \leq n \leq 6$.*

Proof: We know that $n > \frac{2}{3}c^{1/12}$ for $c > b^3$ (this is essentially proved in [**6**, Lemma 12], where the coefficient is not correct). Similar inequalities relate n and certain powers of c with small positive exponent for $b^{1.1} < c < b^3$ and $c < b^{1.1}$. (We shall prove stronger results of this kind in Section 3.) We also know that $c < 2.5\,b^6$, so assuming $n \leq 6$ we get relatively small absolute upper bounds on c, and an elementary numerical study of the linear form Λ gives much tighter estimates for b and c. It follows that we only have to consider the range $10 \leq r \leq 20000$ (since $b \geq 101$). The verification took around 20 minutes on a personal computer. $\qquad \square$

2.5. A lower bound on b. It is known that there is no $D(-1)$-quadruple $(1, b, c, d)$ with $1 < b < c < d$ for $b < 100$. Here we extend this result up to $r \leq 32 \cdot 10^5$.

Proposition 2.3. *There is no $D(-1)$-quadruple $(1, b, c, d)$ with $1 < b < c < d$ and $b < 1.024 \cdot 10^{13}$.*

The result up to $b < 100$ was proved by several authors. We follow their strategy, using the previous lower bound $n > 6$, consequence of the relation $w_n = v_m$. The method is to apply the Baker-Davenport lemma [**2**] (or a variant of it, like the one from [**8**]) to the linear form Λ. For each fixed r such that $b = r^2 + 1$ we search all the values s which are solutions of the Pell-Fermat equation

$$t^2 - bs^2 = r^2$$

and satisfy $c = s^2 + 1 < 3b^6$. To find all the solutions (u, v) of the equation

$$(11) \qquad\qquad u^2 - bv^2 = r^2$$

we follow a method due to Nagell, also presented in Mollin's book [**14**]. A solution for which $\gcd(u, v) = 1$ is called *primitive*. Two solutions (u, v) and (u', v') are said to be *in the same class* if there exist x and y such that $x^2 - by^2 = 1$ and $u' + v'\sqrt{b} = (x + y\sqrt{b})(u + v\sqrt{b})$. Moreover, the primitive solution (u, v) such that u is non-negative and least possible in its class is called *fundamental*. Fundamental solutions sit in a domain described by the following well-known result. We denote indifferently a solution as (u, v) or $u + v\sqrt{b}$.

Lemma 2.9. *Let D be a positive integer which is not a square and N a positive integer. Suppose that $\beta_0 = u_0 + v_0\sqrt{D}$ is the fundamental solution of the equation $u^2 - Dv^2 = 1$ and $\alpha_0 = x_0 + y_0\sqrt{D}$ is the fundamental solution in its class of the equation $x^2 - Dy^2 = N$. Then*

$$0 < |x_0| \le \sqrt{(u_0 + 1)N/2} \quad and \quad 0 \le |y_0| \le \frac{v_0\sqrt{N}}{\sqrt{2(u_0 + 1)}}.$$

When $x^2 - Dy^2 = N$ with $\gcd(x, y) = \delta > 1$ then δ^2 divides N and if we put $x' = x/\delta$, $y' = y/\delta$, and $N' = N/\delta^2$ then (x', y') is a primitive solution of the equation $x^2 - Dy^2 = N'$, to which the previous lemma applies. We see that any solution of an equation $x^2 - Dy^2 = N$, where N is positive, is of the form $\beta_0^m(x_0 + y_0\sqrt{D})$ for some integers x_0 and y_0 such that

$$0 < |x_0| \le \sqrt{(u_0 + 1)N/2} \quad and \quad 0 \le |y_0| \le \frac{v_0\sqrt{N}}{\sqrt{2(u_0 + 1)}}.$$

From this result it follows that, up to a power of the fundamental unit $2b - 1 + 2r\sqrt{b}$, there is a solution (u, v) to equation (11) which satisfies

$$0 \le |v| < r.$$

Then we find all the possible values of $c = s^2 + 1$ in the range $13.7b < c < 3b^6$, and for each pair (r, s) we apply Baker-Davenport lemma to the linear form Λ. The computer verification for $b < 10^{10}$ took about 24 hours on a personal computer (the code employed for this verification is available at `http://mat.uab.cat/pubmat`). To finish the computations we had to employ a network of 6 computers for roughly three months. All computations were performed by using the package PARI/GP [**15**].

3. Bounds for the size of $D(-1)$-quadruples

In this section we prove a weaker version of Theorem 1.2. We refine the strategy which proved successful in previous work, particularly [**7**], from which we borrow several results and arguments. The reader is referred to this paper for further details and precise references.

As mentioned in the introduction, the proof is based on the following congruences.

Lemma 3.1. *For $n \geq 2$ one has*

$$(12) \quad v_n \equiv (-1)^n \left(\frac{2}{3}(n^4 - n^2)c^2 s - 2n^2 cs + s \right) \qquad (\mathrm{mod}\ 32c^3),$$

$$(13) \quad w_n \equiv (-1)^n \left(\frac{2}{3}(n^4 - n^2)b^2 s + \frac{4}{3}(n^3 - n)b\rho t r \right) c^2$$

$$- (-1)^n (2n^2 bs + 2\rho t r n)c + (-1)^n s \qquad (\mathrm{mod}\ 32c^3).$$

In particular,

$$(14) \qquad v_n \equiv (-1)^n(-2n^2 cs + s) \qquad\qquad (\mathrm{mod}\ 8c^2),$$

$$(15) \qquad w_n \equiv -(-1)^n(2n^2 bs + 2\rho t r n)c + (-1)^n s \quad (\mathrm{mod}\ 8c^2).$$

Another tool intensively utilized in this section is the linear form Λ introduced in equation (10). A lower bound for Λ is obtained by the next particular case of [**13**, Theorem 2.1].

Lemma 3.2. *Let Λ be a linear form in logarithms 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 $\mathrm{h}(\alpha_j)$ denote the absolute logarithmic height of α_j, $1 \leq j \leq l$. Choose numbers B, D, A_j, $1 \leq j \leq l$, such that $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_l) : \mathbb{Q}]$,*

$$A_j \geq \max\{D\,\mathrm{h}(\alpha_j), |\log \alpha_j|\},$$

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

Then

$$\log |\Lambda| > -C(l) C_0 W_0 D^2 A_1 \cdots A_l,$$

where

$$C(l) = \frac{8}{(l-1)!}(l+2)(2l+3)\left(4e(l+1)\right)^{l+1},$$

$$C_0 = \log\left(e^{4.4l+7} l^{5.5} D^2 \log(eD)\right), \quad W_0 = \log\left(1.5eBD\log(eD)\right).$$

In our case we have $l=3$, $\alpha_1=s+\sqrt{c}$, $\alpha_2=t+\sqrt{bc}$, $\alpha_3=\frac{s\sqrt{b}+\rho r\sqrt{c}}{s\sqrt{b}}$, $D=4$,
$\mathrm{h}(\alpha_1)=\frac{1}{2}\log\alpha_1$, $\mathrm{h}(\alpha_2)=\frac{1}{2}\log\alpha_2$, $\mathrm{h}(\alpha_3)=\frac{1}{2}\left(\log b(c-1)+\log\frac{s\sqrt{b}+r\sqrt{c}}{s\sqrt{b}}\right)$.
We therefore may take

$$A_1 = 2\log\alpha_1, \quad A_2 = 2\log\alpha_2, \quad A_3 = 2\log\left(s\sqrt{b}(s\sqrt{b}+r\sqrt{c})\right),$$

(16)
$$B = \frac{2mA_2}{A_3}.$$

Combining Lemma 2.6 and Matveev's theorem, we obtain an upper bound for n in terms of b and c.

Lemma 3.3. *In the above notation one has*
$$n < 6.16 \cdot 10^{11}\log\left(77.84\frac{n\log(4c)}{\log(1.99bc)}\right)\log(4c)\log(2bc).$$

Proof: Compare the expressions bounding Λ and take into account that $m < 2n$ to get
$$n < 3.08 \cdot 10^{11}\log(39.92\,B)\,A_1\,A_3.$$

We obtain the announced bound by noticing that $A_1 < \log(4c)$, $A_2 < \log(4bc)$, $A_3 < 2\log(2bc)$ and
$$A_3 > 2\log\left(b(c-1)+(b-1)(c-1)\right) > 2\log(1.99bc)$$

because $b > 10^{13}$, so we may put instead of B from equation (16) the bigger quantity
$$\frac{2n\log(4c)}{\log(1.99bc)}. \qquad \square$$

The proof of Theorem 1.2 proceeds by comparison of n and c, which results in an absolute bound for c. The basic idea of [7] is to show that the congruence

(17)
$$s(m^2 - bn^2) \equiv \rho trn \pmod{4c},$$

which is derived from Lemma 3.1 with the help of equations (14) and (15), turns into an equality. Following the proof of [6, Lemma 14], we consider the integers

(18)
$$A = 2bc - 2rst - c, \quad B = 2bc + 2rst - c.$$

This choice is motivated by the fact that multiplying both sides of (17) by $2s$ results in

(19)
$$2(bn^2 - m^2) \equiv -\rho An \pmod{c},$$

and the goal is to show that this congruence, in fact, implies the equality $2(bn^2 - m^2) = An$.

A key ingredient of our work is provided by the next result.

Lemma 3.4. *The positive integer A introduced in equation* (18) *satisfies*

$$b + \frac{1}{4.002}\left(\frac{b-1}{c-1} + \frac{c-1}{b-1}\right) + \frac{1}{2.001} < A < b + \frac{1}{4}\left(\frac{b-1}{c-1} + \frac{c-1}{b-1}\right) + \frac{1}{2}.$$

In particular,

$$\max\left\{\frac{c-5}{4b} + b, b + \frac{1}{4.002}\left(\frac{b}{c} + \frac{c}{b}\right) + \frac{1}{2.001}\right\} < A < \frac{1}{3.999}\left(\frac{c}{b} + 4b\right).$$

Moreover, for $c < b^{2.75}$ one also has

$$A < \left(\frac{c}{4b} + b\right)\left(1 + \frac{1}{b}\right).$$

Proof: The term A is given by the formulæ

$$A = 2bc - 2rst - c = 2(r^2+1)(s^2+1) - 2rst - s^2 - 1 = 2r^2s^2 + 2r^2 + s^2 + 1 - 2rst.$$

For $0 < u < 10^{-4}$, we use the estimates

$$1 + \frac{1}{2}u - \frac{1}{8}u^2 < (1+u)^{1/2} < 1 + \frac{1}{2}u - \frac{1}{8.001}u^2.$$

The term t satisfies

$$t^2 + 1 = bc = (r^2+1)(s^2+1),$$

hence

$$t = rs(1+u)^{1/2}, \quad \text{where } u = r^{-2} + s^{-2} < 10^{-4}.$$

Combining the above information, after some easy simplification we obtain

$$r^2 + 1 + \frac{1}{4.002}\left(\frac{r^2}{s^2} + \frac{s^2}{r^2}\right) + \frac{1}{2.001} < A < r^2 + 1 + \frac{1}{4}\left(\frac{r^2}{s^2} + \frac{s^2}{r^2}\right) + \frac{1}{2}.$$

In terms of b and c, this is

$$b + \frac{1}{4.002}\left(\frac{b-1}{c-1} + \frac{c-1}{b-1}\right) + \frac{1}{2.001} < A < b + \frac{1}{4}\left(\frac{b-1}{c-1} + \frac{c-1}{b-1}\right) + \frac{1}{2},$$

which readily implies

$$b + \frac{1}{4.002}\left(\frac{b}{c} + \frac{c}{b}\right) + \frac{1}{2.001} < A < \frac{1}{3.999}\left(\frac{c}{b} + 4b\right).$$

To prove the other lower bound for A, notice that $B = (2b-1)c + 2rst$ satisfies $AB = c^2 + 4b^2c - 4c - 4b + 4$ and $B < 4bc$. Therefore,

$$A > \frac{c^2 + 4b^2c - 4c - 4b}{4bc} > b + \frac{c-5}{4b} > \frac{c}{4b}.$$

The last upper bound for A is consequence of the inequality

$$\frac{b-1}{4(c-1)} + \frac{c-1}{4(b-1)} < \frac{c}{4b} + \frac{c}{4b^2} + \frac{b}{2},$$

or equivalently $c^2 - (2b^3 - b^2 + 1)c + b^4 < 0$. When $b^2 \leq c$ this follows from $2c^2 - (2b^3 - b^2 + 1)c < 0$, which is true because $c < b^{2.75}$. In case $b^2 > c$ it suffices to note that our gap principle implies $2b^4 - (2b^3 - b^2 + 1)c < 0$. $\square$

The next lemmas point out applications of the inequalities just proved.

Lemma 3.5. *For a putative $D(-1)$-quadruple $(1, b, c, d)$ with $1 < b < c < d$ put $b - 1 = r^2$, $c - 1 = s^2$, $bc - 1 = t^2$, and $f = t - rs$, where r, s, t are positive. Then one has $c > 4 f^2(b-1) - 2.1\, b$ and $s > 2\, fr - 2r/f$. In particular, $c > 3.999 f^2 b > 3.999 \cdot 10^{14} b$.*

Proof: Notice that $A = e + b + 1 = f^2 + b$, with e and f the integers introduced in the proof of the gap principle Lemma 2.1. The first two of the above estimates easily follow from the previous lemma, while the last one is an experimental result —explicit computations provided no $D(-1)$-quadruple for which $f \leq 10^7$. $\square$

We are now in a position to bound from below n by powers of c with much larger exponents than those available in the literature. Such a result allows one to get an absolute upper bound for c via Lemma 2.6. Introducing subsequently this upper bound in Matveev's theorem, n is also bounded from above by a huge constant. This kind of result is obtained by an approach described in the introduction as smoothification. The basic idea is to bound from below n by an expression depending continuously on parameters naturally present in the solution to our problem, and to use such inequalities in conjunction with a stratification with many layers of the search space.

Lemma 3.6. *Suppose $v_m = w_n$, where $n \geq 7$. Then for $c \geq 0.0576\, b^3$ one has*

$$n > \min\{3.99\, b, 0.03\, \sqrt{c/b}\}.$$

In particular,

   a) *if $b^5 \leq c < 2.5\, b^6$ then $n > 3.42\, c^{1/6}$,*

   b) *if $b^4 \leq c < b^5$ then $n > 3.99\, c^{1/5}$,*

   c) *if $b^{3.5} \leq c < b^4$ then $n > 3.99\, c^{1/4}$,*

   d) *if $133^2 b^3 \leq c < b^{3.5}$ then $n > 3.99\, c^{2/7}$.*

Proof: We argue by reduction to absurd. Assuming $n \leq \min\{3.99b, 0.03\sqrt{c/b}\}$, from $c \geq 0.0576\,b^3 > 15992\,b^2$ one obtains the two inequalities

$$0 < An < \frac{1}{3.999}\left(\frac{c}{b} + 4b\right) n < \frac{1}{3.998}\frac{cn}{b} < 0.998c$$

and

$$0 < 2(bn^2 - m^2) < 2bn^2 < 0.002b(c/b) = 0.002c.$$

From congruence (19) one concludes that $2(bn^2 - m^2) = An$. Hence,

$$A < 2bn \leq 0.06\sqrt{bc}.$$

Lemma 3.4 yields

$$A > \frac{c}{4b}$$

which contradicts the previous inequality.

We treat the case a). Since $0.03\sqrt{c/b} > 3.99\,b$ for $c > 133^2\,b^3$, one has

$$n > 3.99\,b > 3.99\,(c/2.5)^{1/6} > 3.42\,c^{1/6}.$$

Thus part a) holds.

The others parts are obtained similarly.   □

We now provide a proof for all parts of a weaker version of Theorem 1.2 referring to large $D(-1)$-quadruples. While in [6] it is obtained that in this range one has $c < 10^{238}$, we succeed to lower the bound to less than 10^{107}. In the proofs we use a simple observation: for any positive constant C, a function of the type $x \mapsto x/(\log x + C)$ is increasing for $x > 3$.

Proposition 3.1. *Let $(1, b, c, d)$ be a $D(-1)$-quadruple with $10^{13} < b < c < d$.*

a) *If $b^5 \leq c < 2.5\,b^6$ then $c < 1.66 \cdot 10^{106}$.*

b) *If $b^4 \leq c < b^5$ then $c < 5.41 \cdot 10^{87}$.*

c) *If $b^{3.5} \leq c < b^4$ then $c < 2.71 \cdot 10^{69}$.*

d) *If $b^3 \leq c < b^{3.5}$ then $c < 2.32 \cdot 10^{60}$.*

Proof: Each interval $b^M \leq c < b^N$ has been divided into subintervals $b^{m_j} \leq c < b^{n_j}$, with $m_j = M + (j-1)\Delta$, $n_j = m_j + \Delta$ for $j = 1, 2, \ldots, (N - M)/\Delta$, where $\Delta = 0.05$ or 0.1. On each subinterval, Lemma 3.3 and the previous lemma yield an upper bound on c. The proof is obtained by computing the maximum in each interval.   □

The most difficult part of the proof covers the range $b^{1.1} \leq c < b^3$. The absolute bound for such c obtained in [**6**] is 10^{491}. We succeed to improve on this estimate by considering a stratification with seven layers of the range of variation for c.

In order to obtain relative lower bounds on n for the medium size $D(-1)$-quadruples we study the relation

(20) $$2(bn^2 - m^2) + \rho An = jc.$$

The congruence method essentially consists of an attempt to find hypotheses under which one can conclude that one has $j = 0$. We adopt a different point of view. Our idea is to study what happens for nonzero values of j. As a result of such a study, inequalities of the type $n > f(b, c, j)$ will emerge.

We start with a result whose proof is easy.

Lemma 3.7. *If* $15992\, b^2 \leq c < b^3$ *then* $n > 0.125\, c/b^2$.

Proof: Assuming $n \leq 0.125\, c/b^2$, one gets

$$An < \frac{1}{3.999}\left(\frac{c}{b} + 4b\right)n < \frac{1}{3.998}\frac{cn}{b} < 0.032c^2/b^3,$$

$$2bn^2 < 0.032c^2/b^3,$$

so that $An = 2bn^2 - 2m^2$. Hence,

$$\frac{c}{4b} < A < 2bn \leq \frac{c}{4b},$$

a blatant contradiction.   □

For other $D(-1)$-quadruples of medium size, a relative lower bound on n is provided by the following analogue of Lemma 3.6.

Lemma 3.8. *Suppose* $v_m = w_n$, *with* $n \geq 7$ *and* $c < b^{2.75}$.
  a) *If* $\rho = 1$ *then* $n > 0.5\sqrt{jc/b} \geq 0.5\sqrt{c/b}$.
  b) *Let* $\rho = -1$. *Then* j *is nonnegative. If* j *is positive then* $n > 0.5\sqrt{2jc/b} \geq 0.5\sqrt{2c/b}$. *If* $j = 0$ *then* $c > 51.99b^2$ *and*

$$n > \begin{cases} c^{2/11} & \text{for } c \geq \max\{b^{2.5}, 10^{50}\}, \\ 0.214(c/b)^{1/3} & \text{for } c < b^{2.5}. \end{cases}$$

Proof: a) Notice that the integer j is positive when $\rho = 1$, so that $\max\{2bn^2, An\} \geq jc/2$. If the maximum is $2bn^2$, the desired conclusion is obvious. In the opposite case one has $2An \geq c$, and Lemma 3.4 yields

$$n \geq \frac{2b^2c}{(b+1)(c+4b^2)} = \frac{2(b-1)c}{c+4b^2} + \frac{2c}{(b+1)(c+4b^2)}.$$

The right hand side is greater than $b - 1$ when $c \geq 4b^2$, and greater than $0.249c/b$ when $c < 4b^2$. We use this information in relations $0.251(4b + c/b) > A > 2bn$ and arrive to either $0.251c > b^2n \geq b^3$ or $4 \times 0.251b > bn$, both of which being impossible under the hypotheses in force.

b) Now there are three cases to examine.

If $j < 0$, Lemma 3.4 entails

$$2(bn^2 - m^2) + c \leq An < \left(\frac{c}{4b} + b\right)\left(1 + \frac{1}{b}\right)n.$$

For $c \geq 4b^2$ this readily implies $n > 1.998b$, whence

$$\frac{1.001c}{2b} > A > 1.999\,bn > 3.994\,b^2,$$

so that $c > b^3$, contradiction. For $c < 4b^2$ one gets $4n > 0.499c/b$, which in turn implies

$$2.002\,b > A > 1.999\,bn,$$

another contradiction. Thus, equation (20) can not hold for j negative.

If $j > 0$ then $2(bn^2 - m^2) \geq jc + An$, whence $2bn^2 > jc$.

It remains to consider the case $j = 0$, that is, $A = 2bn - k$, where $k := 2m^2/n$. From $n \geq 7$, $b > 10^{13}$, $2n < k < 8n$, and Lemma 3.4 it follows

$$13.999\,b < 2(b - 4)n < A < 1.0001\left(\frac{c}{4b} + b\right),$$

so that $c > 51.99\,b^2$.

Assume $c \geq 10^{50}$ and $b^{2.5} \leq c < b^{2.75}$. If $n \leq c^{2/11}$ then

$$\frac{c}{4b} < A < 2bn \implies c < 8\,b^2n < 8\,c^{4/5 + 2/11},$$

so that $c^{1/55} < 8$, in contradiction with $c \geq 10^{50}$.

For $c < b^{2.5}$, denote $D := 4b^2(2n - 1) - c$, $E := 4bA - c - 4b^2$. From

$$4(b - 1) \equiv A^2 = 4b^2n^2 - 4bkn + k^2 \pmod{c}$$

one gets

(21) $Dn^2 \equiv 4(2n - 1)b^2n^2 \equiv (2n - 1)[4(b - 1) + 4bnk - k^2] \pmod{c}$.

On noticing that $D = E + 4bk > 8bn - 5 > 0$, $k < 8n$, $D < c/b + 4b + 32bn$, one concludes

$$0 < Dn^2 + (2n - 1)[4(b - 1) + 4bnk - k^2] < Dn^2 + 8bn(nk + 1)$$

$$< 32bn^3 + \left(\frac{c}{b} + 4b\right)n^2 + 8bn(8n^2 + 1).$$

For $n \leq 0.214(c/b)^{1/3}$ this is less than c, so that congruence (21) is actually an equality that can be written

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

However, as remarked by Dujella, Filipin, and Fuchs in [**6**], this leads to a contradiction: since $A^2 - 4(b-1)$ is divisible by c, it follows that $2n-1$ divides n^2, and this is impossible for $n \geq 2$. The contradiction is due to the assumption $n \leq 0.214(c/b)^{1/3}$. □

For the remaining class of medium $D(-1)$-quadruples we follow the reasoning employed in the proof of Lemma 16 from [**6**]. Although the strategy is the same, the details are much more intricate because the estimates are tighter.

Lemma 3.9. *Suppose $v_m = w_n$ for some $c < b^{1.3}$, then*

$$n > (3b^2/c)^{1/4}.$$

Proof: For ease of reference, we put $\Delta := e + 1$, so that $A = b + \Delta$. Lemma 3.4 yields $e < \Delta < 0.251\, c/b$.

A simple computation shows that one has

$$b + e - 1 = (2e+1)c - 2sfh,$$

where f, h are the positive integers introduced in the proof of Lemma 2.1. Squaring this equality, one obtains

$$(22) \qquad b^2 + 2(e-1)b + e^2 + 2e + 5 \equiv 0 \pmod{c}.$$

From congruence (19), rewritten in the form

$$b(2n^2 + \rho n) \equiv 2m^2 - \rho \Delta n \pmod{c},$$

one gets, on the one hand,

$$b^2(2n^2 + \rho n)^2 \equiv (2m^2 - \rho \Delta n)^2 \pmod{c},$$

and, on the other hand,

$$2(e-1)b(2n^2 + \rho n)^2 \equiv 2(e-1)(2n^2 + \rho n)(2m^2 - \rho \Delta n) \pmod{c}.$$

Having in view (22), the sum of the last two congruences becomes

$$(23) \quad -(e^2 + 2e + 5)(2n^2 + \rho n)^2 \equiv (2m^2 - \rho \Delta n)^2$$
$$+ 2(e-1)(2n^2 + \rho n)(2m^2 - \rho \Delta n) \pmod{c}.$$

Assume $n \leq (3b^2/c)^{1/4}$. By computation we know that $e > 10^{14}$, we also know that $7 \leq n < m < 2n$, thus we have the following estimates:

$$0 < |2m^2 - \rho\Delta|n < 8n^2 + \Delta n < \left(8n + 0.251\,\frac{c}{b}\right)n,$$

$$0 < (2m^2 - \rho\Delta n)^2 < \left(8n + 0.251\,\frac{c}{b}\right)^2 n^2,$$

$$0 < 2(e-1)(2n^2 + \rho n)|2m^2 - \rho\Delta n| < \frac{0.502c}{b} \times \left(2 + \frac{1}{7}\right)n^2 \times (8n^2 + \Delta n),$$

$$0 < (e^2 + 2e + 5)(2n^2 + \rho n)^2 < 0.252^2 \cdot \frac{c^2}{b^2} \cdot \frac{15^2}{7^2} \cdot n^4 = 0.8748\,c.$$

As one can verify that, under the hypotheses on c and n, the sum of the right sides is less than c, one concludes that congruence (23) is actually an equality of the form

$$(e^2 + 2e + 5)X^2 + 2(e-1)XY + Y^2 = 0,$$

with $X := 2n^2 + \rho n$, $Y := 2m^2 - \rho\Delta n$. As the discriminant is negative, it results $X = Y = 0$, which is possible only for $n = 0$. The contradiction implies the asserted result. □

Now we can complete the proof of a weaker analog of Theorem 1.2. Besides the first nine cases enumerated in the statement of Theorem 1.2, we shall also consider b and c satisfying either

  x') $b^{1.1} \leq c < b^{1.2}$

or

  xi) $c < b^{1.1}$.

The resulting bounds for b and c are as follows.

Proposition 3.2. *Let* $(1, b, c, d)$ *be a* $D(-1)$-*quadruple with* $10^{13} \leq b < c < d$.

  a) *If* $b^2 \leq c < b^3$ *then* $c < 7.21 \cdot 10^{114}$.
  b) *If* $b^{1.5} \leq c < b^2$ *then* $c < 7.62 \cdot 10^{112}$.
  c) *If* $b^{1.4} \leq c < b^{1.5}$ *then* $c < 5 \cdot 10^{132}$.
  d) *If* $b^{1.3} \leq c < b^{1.4}$ *then* $c < 1.32 \cdot 10^{166}$.
  e) *If* $b^{1.2} \leq c < b^{1.3}$ *then* $c < 2.11 \cdot 10^{138}$.
  f) *If* $b^{1.1} \leq c < b^{1.2}$ *then* $c < 4.47 \cdot 10^{110}$.
  g) *If* $c < b^{1.1}$ *then* $c < 5.03 \cdot 10^{88}$.
  h) *There is no* $D(-1)$-*quadruple with* $b^{8/7} \geq c$.

Proof: All but the last part are proved in the manner seen above. For the proof of part h) we use Lemma 3.5, according to which one has $c > 3.999 f^2 b > 3.999 \cdot 10^{14} b$. Therefore, supposing that $c \leq b^{8/7}$, one gets

$$3.999 \cdot 10^{14} b < c \leq b^{8/7},$$

whence

$$1.6 \cdot 10^{102} < b,$$

in contradiction with f) and g). □

4. Proof of Theorem 1.2

In this section we improve the previously obtained results with the help of the linear form

$$\Lambda_1 = 2m \log(s + \sqrt{c}) - 2l \log(r + \sqrt{b}) + \log \frac{s\sqrt{b}}{r\sqrt{c}},$$

attached to positive solutions to the system of Diophantine equations consisting of (3) and (5).

From [**12**] it is known that if one has a solution with $x = v_m = u_l$, where m is positive, then

$$0 < \Lambda_1 < \frac{b}{b-1} \cdot (r + \sqrt{b})^{-4l}.$$

An application of Matveev's theorem results in an upper bound for the index l. Comparison of l with a certain power of b as in the previous section is very cumbersome, so we take an indirect approach. Since $m \log(s + \sqrt{c}) < l \log(r + \sqrt{b})$ (cf., for instance, Lemma 3.3 from [**12**], in whose proof the additional hypothesis $s = r + 1$ is not used), one gets an upper bound for m of the kind

$$(24) \qquad m < 3.08 \cdot 10^{11} \log \left(\frac{38.92\, m \log(4c)}{\log(0.999 bc)} \right) \log(4b) \log(bc).$$

All is needed in order to employ Lemmas 3.6 to 3.9 is a lower bound for the quotient m/n. Our next lemma provides this information.

Lemma 4.1. *For $c > c_0$ one has $m > \mu\, n$, with c_0 and μ given in table below.*

Case	i)	ii)	iii)	iv)	v)	vi)	vii)	viii)	ix)	x')	xi)
c_0	10^{98}	10^{80}	10^{64}	10^{54}	10^{68}	10^{106}	10^{120}	10^{144}	10^{130}	10^{105}	10^{84}
μ	1.155	1.191	1.238	1.271	1.321	1.491	1.658	1.707	1.761	1.822	1.895

TABLE 1

Proof: For $b^5 \le c < 2.5b^6$ and $c > 10^{98}$, from Lemma 2.7 one gets

$$\frac{m}{n} > \frac{\log(0.3999c^{7/6})}{\log(4c)} > 1.155. \qquad \square$$

Having in view Proposition 3.2, it is apparent that decreasing the upper bound on c requires a careful study of the range $b^{1.2} \le c < b^{1.4}$. A successful idea leads to the next result.

Lemma 4.2. *If $v_m = w_n$ for some c satisfying $b^{5/4} \le c < b^{4/3}$ then*

$$n > \left(\frac{10b^2}{3c}\right)^{1/4}.$$

Proof: We reason by reduction to absurd. The only differences in comparison with the proof of Lemma 3.9 appear when estimating the terms in equation (23).

Notice that Lemmas 3.8 and 3.9 together with Proposition 3.2 entail

$$n > \min\left\{0.5\sqrt{b^{1/4}}, \left(3b^{2-4/3}\right)^{1/4}\right\} > \min\{0.5{\cdot}10^{13/8}, 3^{1/4}{\cdot}10^{13/6}\} > 21.$$

Therefore, in the notation introduced in the proof of Lemma 3.9, under the present hypotheses one obtains with the help of Lemma 3.4

$$|2m^2 - \rho\Delta n| < \left(8n + 0.251\,\frac{c}{b}\right)n < \left(\frac{5}{3} + 0.251\right)\frac{nc}{b} < 1.918\frac{nc}{b},$$

$$(2m^2 - \rho\Delta n)^2 < 1.918^2\sqrt{\frac{10}{3}}\frac{c^{3/2}}{b} < 6.717\,c^{3/4},$$

$$2(e-1)(2n^2+\rho n)|2m^2-\rho\Delta n| < \frac{0.502c}{b}\times\left(2+\frac{1}{22}\right)n^2\times1.918\frac{nc}{b} < 4.859\,c^{7/8},$$

$$(e^2 + 2e + 5)(2n^2 + \rho n)^2 < 0.252^2\cdot\frac{c^2}{b^2}\cdot\frac{45^2}{22^2}\cdot n^4 < 0.886\,c.$$

Since the sum of the right hand sides of the inequalities in the last three lines is less than c, one arrives at a contradiction. $\qquad \square$

Combining all these ingredients in the same manner as in the previous section, one obtains the following absolute bounds for b and c.

Proposition 4.1. *Let $(1, b, c, d)$ with $1 < b < c < d$ be a $D(-1)$-quadruple with $b > 1.024 \cdot 10^{13}$. Then:*

  i) *If $b^5 \le c < 2.5\,b^6$ then $b < 3.03 \cdot 10^{16}$ and $c < 1.86 \cdot 10^{99}$.*

  ii) *If $b^4 \le c < b^5$ then $b < 2.47 \cdot 10^{16}$ and $c < 9.42 \cdot 10^{81}$.*

  iii) *If $b^{3.5} \le c < b^4$ then $b < 1.96 \cdot 10^{16}$ and $c < 1.46 \cdot 10^{65}$.*

iv) *If $b^3 \leq c < b^{3.5}$ then $b < 1.69 \cdot 10^{16}$ and $c < 6.37 \cdot 10^{56}$.*

  v) *If $b^2 \leq c < b^3$ then $b < 8.79 \cdot 10^{43}$ and $c < 1.87 \cdot 10^{110}$.*

 vi) *If $b^{1.5} \leq c < b^2$ then $b < 1.47 \cdot 10^{72}$ and $c < 4.67 \cdot 10^{108}$.*

vii) *If $b^{1.4} \leq c < b^{1.5}$ then $b < 3.70 \cdot 10^{90}$ and $c < 6.68 \cdot 10^{127}$.*

viii) *If $b^{1.3} \leq c < b^{1.4}$ then $b < 2.69 \cdot 10^{110}$ and $c < 2.65 \cdot 10^{147}$.*

 ix) *If $b^{1.2} \leq c < b^{1.3}$ then $b < 1.38 \cdot 10^{102}$ and $c < 6 \cdot 10^{132}$.*

  x) *If $b^{8/7} \leq c < b^{1.2}$ then $b < 4.24 \cdot 10^{88}$ and $c < 2.25 \cdot 10^{106}$.*

The proof will be complete as soon as we show the next result.

Proposition 4.2. *There is no $D(-1)$-quadruple $(1, b, c, d)$ with $10^{13} < b < c < d$ and $c \leq b^{1.16}$.*

Proof: Suppose there exists at least one $D(-1)$-quadruple such that $c \leq b^{1.16}$. Then, by Lemma 3.5,

$$3.999 \cdot 10^{14} b < c \leq b^{1.16},$$

whence

$$b > \left(3.999 \cdot 10^{14}\right)^{6.25} > 10^{91},$$

in contradiction with part x) of Proposition 4.1. $\qquad\square$

Having in view Lemma 3.3 and Theorem 1.2, we get the following absolute bounds for n and b. The fact that $m < 2n < 10^{20}$ has been used by some of our programs.

Proposition 4.3. *Suppose $(1, b, c, d)$ is a $D(-1)$-quadruple with $10^{13} < b < c < d$. Then the values of n and b satisfy the inequalities given in Table 2.*

Case	i)	ii)	iii)	iv)	v)	vi)	vii)	viii)	ix)	x)
$b <$	10^{17}	10^{17}	10^{17}	10^{19}	10^{35}	10^{73}	10^{91}	10^{110}	10^{103}	10^{89}
$n <$	10^{18}	10^{17}	10^{17}	10^{17}	10^{18}	10^{18}	10^{18}	10^{19}	10^{19}	10^{18}
$n >$	10^{13}	10^{13}	10^{13}	10^{11}	10^4	894	200	73	247	523

TABLE 2. *Absolute bounds for b and n.*

5. A bound for the number of $D(-1)$-quadruples

Below $(1, b, c, d)$ is a $D(-1)$-quadruple with $10^{13} < b < c < d$. Since $\sqrt{b-1}$ is an integer, b is either an odd integer whose prime divisors are

all congruent to 1 mod 4 or twice such an odd integer. Besides this fact, our argument uses the paradigm "compute rather than estimate".

As already mentioned in the introduction, the proof idea is to see how many possibilities are there to prolongate an initial subsequence to a $D(-1)$-set with one more element.

In order to estimate the number of $D(-1)$-couples $(1, b)$, we shall use the information provided by Theorem 1.2. On account of this, we have

$$b \leq B := 2.69 \cdot 10^{110}, \quad c \leq C := 2.65 \cdot 10^{147}.$$

Therefore, the number of $D(-1)$-pairs $(1, b)$ is less than

$$N := B^{1/2} < 1.641 \cdot 10^{55}.$$

By [6, Lemma 1], each such a pair can be extended to a $D(-1)$-triple $(1, b, c)$ only if c belongs to the union of finitely many binary recurrent sequences. It is known (see *loc.cit.*) that the number of sequences does not exceed the number of solutions of the congruence $t^2 \equiv -1 \pmod{b}$ with $0 < t < b$. According to [17, g, §4, ch. V], there are at most $2^{\omega(b)}$ such solutions, where $\omega(b)$ denotes the number of distinct prime divisors of b. With some computer assistance, we find that the product of the first 49 primes congruent to 1 mod 4 is greater than $B/2$. Allowing for even b, we conclude that the number of sequences is at most

$$S := 2^{49}.$$

Thus, the third component of a $D(-1)$-triple $(1, b, c)$ can be selected out of S sequences by requiring that $bc - 1 = t^2$ for a suitable positive integer t. Any solution t to this equation appears in one of the recurrent sequences, say, at index m. It is well-known that the terms of recurrent sequences have an exponential growth. In our case we readily find $t_m > (b-1)(4b-3)^{m-1}$. From $b > 10^{13}$ and $t \leq T := \sqrt{B \cdot C - 1}$ it results $m \leq M := 9$. Therefore, a fixed $D(-1)$-couple $(1, b)$ can be extended to a $D(-1)$-triple in at most $M \cdot S$ ways.

Fix a $D(-1)$-triple $(1, b, c)$ with $10^{13} < b < c$. According to [10, Theorem 1.1], each $D(-1)$-triple $(1, b, c)$ can be embedded in at most two $D(-1)$-quadruples $(1, b, c, d)$. Hence, the number Q of $D(-1)$-quadruples is bounded from above by

$$Q < 2 \cdot N \cdot M \cdot S < 1.7 \cdot 10^{71}.$$

Dividing the set of solutions into two pieces: the first with $c < b^2$ and the second with $c \geq b^2$, with obvious notation we get the following upper bound for the number Q of $D(-1)$-quadruples:

$$Q \leq 2 \cdot N_1 \cdot M_1 \cdot S_1 + 2 \cdot N_2 \cdot M_2 \cdot S_2,$$

where

$$N_1 = B^{1/2}, \quad N_2 = \left(10^{36}\right)^{1/2}, \quad M_1 = 2, \quad M_2 = 6, \quad S_1 = 2^{49}, \quad S_2 = 2^{36}.$$

Then we get the result announced in Theorem 1.1:

$$Q \le 4 \cdot 10^{70}.$$

References

[1] F. S. Abu Muriefah and A. Al-Rashed, On the extendibility of the Diophantine triple $\{1, 5, c\}$, *Int. J. Math. Math. Sci.* **33–36** (2004), 1737–1746. DOI: 10.1155/S0161171204305181.

[2] 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.

[3] A. Dujella, Complete solution of a family of simultaneous Pellian equations, Proceedings of the 13th Czech and Slovak International Conference on Number Theory (Ostravice, 1997), *Acta Math. Inform. Univ. Ostraviensis* **6(1)** (1998), 59–67.

[4] A. Dujella, On the exceptional set in the problem of Diophantus and Davenport, in: *"Applications of Fibonacci numbers"*, Vol. 7 (Graz, 1996), Kluwer Acad. Publ., Dordrecht, 1998, pp. 69–76.

[5] A. Dujella, On the number of Diophantine m-tuples, *Ramanujan J.* **15(1)** (2008), 37–46. DOI: 10.1007/s11139-007-9066-0.

[6] A. Dujella, A. Filipin, and C. Fuchs, Effective solution of the $D(-1)$-quadruple conjecture, *Acta Arith.* **128(4)** (2007), 319–338. DOI: 10.4064/aa128-4-2.

[7] A. Dujella and C. Fuchs, Complete solution of a problem of Diophantus and Euler, *J. London Math. Soc. (2)* **71(1)** (2005), 33–52. DOI: 10.1112/S002461070400609X.

[8] A. Dujella and A. Pethő, A generalization of a theorem of Baker and Davenport, *Quart. J. Math. Oxford Ser. (2)* **49(195)** (1998), 291–306. DOI: 10.1093/qmathj/49.3.291.

[9] A. Filipin, Nonextendibility of $D(-1)$-triples of the form $\{1, 10, c\}$, *Int. J. Math. Math. Sci.* **14** (2005), 2217–2226. DOI: 10.1155/IJMMS.2005.2217.

[10] A. Filipin and Y. Fujita, The number of $D(-1)$-quadruples, *Math. Commun.* **15(2)** (2010), 387–391.

[11] Y. Fujita, The extensibility of $D(-1)$-triples $\{1, b, c\}$, *Publ. Math. Debrecen* **70(1–2)** (2007), 103–117.

[12] B. He and A. Togbé, On the $D(-1)$-triple $\{1, k^2 + 1, k^2 + 2k + 2\}$ and its unique $D(1)$-extension, *J. Number Theory* **131(1)** (2011), 120–137. DOI: 10.1016/j.jnt.2010.07.006.

[13] E. M. Matveev, An explicit lower bound for a homogeneous
     rational linear form in logarithms of algebraic numbers. II, (Rus-
     sian), *Izv. Ross. Akad. Nauk Ser. Mat.* **64(6)** (2000), 125–180;
     translation in: *Izv. Math.* **64(6)** (2000), 1217–1269. DOI: 10.1070/
     IM2000v064n06ABEH000314.

[14] R. A. Mollin, *"Fundamental Number Theory with Applications"*,
     CRC Press, Boca Raton, FL, 1998.

[15] The PARI Group, PARI/GP, version 2.3.4, Bordeaux (2008),
     available at: http://pari.math.u-bordeaux.fr/.

[16] R. Tamura, Non-extendibility of $D(-1)$-triples $\{1, b, c\}$, Preprint.

[17] I. M. Vinogradov, *"Elements of number theory"*, Translated by
     S. Kravetz. Dover Publications, Inc., New York, 1954.

Nicolae Ciprian Bonciocat and Mihai Cipu:
Simion Stoilow Institute of Mathematics
of the Romanian Academy
Research Unit nr. 5
P. O. Box 1-764
RO-014700 Bucharest
Romania
E-mail address: Nicolae.Bonciocat@imar.ro
E-mail address: Mihai.Cipu@imar.ro

Maurice Mignotte:
Université de Strasbourg
U. F. R. de Mathématiques
67084 Strasbourg
France
E-mail address: Maurice.Mignotte@math.unistra.fr