TOKYO J. MATH.
VOL. 41, NO. 2, 2018
DOI: 10.3836/tjm/1502179250

On the Polynomial Quadruples with the Property $D(-1; 1)$

Marija BLIZNAC TREBJEŠANIN, Alan FILIPIN and Ana JURASIĆ

University of Split, University of Zagreb and University of Rijeka

(Communicated by T. Komatsu)

Abstract. In this paper we prove, under some assumptions, that every polynomial $D(-1)$-triple in $\mathbf{Z}[X]$ can only be extended to a polynomial $D(-1; 1)$-quadruple in $\mathbf{Z}[X]$ by polynomials $d^{\pm}$. More precisely, if $\{a, b, c; d\}$ is a polynomial $D(-1; 1)$-quadruple, then

$$d = d^{\pm} = -(a + b + c) + 2(abc \pm rst),$$

where r, s and t are polynomials from $\mathbf{Z}[X]$ with positive leading coefficients that satisfy $ab - 1 = r^2$, $ac - 1 = s^2$ and $bc - 1 = t^2$.

1. Introduction

DEFINITION 1. Let $n \neq 0$ be an integer. We call a set of m distinct positive integers a $D(n)$-m-tuple, if the product of any two of its distinct elements increased by n is a perfect square.

One of the most interesting questions concerning such sets is how large those sets can be. The most well-known and studied case is in $n = 1$, but the cases $n = -1$ and $n = 4$ have also been intensively studied in recent years. All the details, together with the history of the problem, all generalizations and the most recent results with references can be found on webpage [2].

In the case $n = 1$, we have the following conjecture:

CONJECTURE 1. *If $\{a, b, c, d\}$ is a $D(1)$-quadruple such that $a < b < c < d$, then*

$$d = d_+ = a + b + c + 2\left(abc + \sqrt{(ab + 1)(ac + 1)(bc + 1)}\right).$$

It is obvious that this conjecture implies that there does not exist a $D(1)$-quintuple. Dujella [1] proved an important result, that there does not exist a $D(1)$-sextuple and that there are only finitely many $D(1)$-quintuples. There have been some improvements of his results recently (the reader can again consult [2]), but the proof of the conjecture is still far away. However, very recently He, Togbé and Ziegler reported that they proved that there does not

Received October 31, 2016; revised March 28, 2017
2010 *Mathematics Subject Classification*: 11D09, 11D45
Key words and phrases: Diophantine m-tuples, polynomials

exist a $D(1)$-quintuple.

In the case $n = -1$, there is a conjecture that there does not exist a $D(-1)$-quadruple. Similarly as in the case $n = 1$, Dujella et al. [3] proved that there exist only finitely many $D(-1)$-quadruples. Even though a $D(-1)$-triple $\{a, b, c\}$ such that $a < b < c$ conjecturally cannot be extended to a $D(-1)$-quadruple, there always exist a positive integer d such that each of $ad + 1$, $bd + 1$ and $cd + 1$ is a perfect square. Moreover, $d = d^+$ has such property, where

$$d^+ = -(a + b + c) + 2\big(abc + \sqrt{(ab - 1)(ac - 1)(bc - 1)}\big).$$

This leads us to the following definition:

DEFINITION 2. A set $\{a, b, c; d\}$ of four distinct positive integers is said to have a property $D(-1; 1)$, or that it is $D(-1; 1)$-quadruple, if $\{a, b, c\}$ is a $D(-1)$-triple and each of $ad + 1$, $bd + 1$ and $cd + 1$ is a perfect square.

There are not a lot of works done on the existence of such sets, but we have a reason to believe that the following conjecture is true:

CONJECTURE 2. *If $\{a, b, c; d\}$ has the property $D(-1; 1)$, then*

$$d = d^{\pm} = -(a + b + c) + 2\big(abc \pm \sqrt{(ab - 1)(ac - 1)(bc - 1)}\big).$$

It is possible that $d^- = 0$, and in that case we do not have extension of $D(-1)$-triple to $D(-1; 1)$-quadruple. Fujita [10, 11] proved Conjecture 2 for $D(-1)$-triples of the form $\{1, 2, c\}$ and for parametric family of $D(-1)$-triples of the form $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$ where $k \geq 1$ is an integer. The second author [9] proved the same if $a = k^{12} + 1$, $b = k^{12} + 2k^6 + 2$ and $c = 4k^{12}+4k^6+5$ where $k \geq 1$ is an integer. He and Togbé [12] proved that $D(-1)$-triples of the form $\{1, k^2 + 1, (k + 1)^2 + 1\}$, where k is a positive integer, have a unique extension to a $D(-1; 1)$-quadruple. Their result and its proof is important, because the authors in [12] have used the linear forms in two logarithms for the first time in solving such problems. All mentioned results support Conjecture 2.

There are various generalizations of $D(n)$-m-tuples which can also be found at [2]. However, in this paper we study the polynomial variant of the problem so we need the following definitions:

DEFINITION 3. Let $n \neq 0$ be a polynomial with integral coefficients. We call the set of m distinct non-zero polynomials from $\mathbf{Z}[X]$ a polynomial $D(n)$-m-tuple, if the product of any two of its distinct elements increased by n is a square of some polynomial with integer coefficients.

DEFINITION 4. A set $\{a, b, c; d\}$ of four non-zero distinct polynomials from $\mathbf{Z}[X]$ is said to have a property $D(-1; 1)$, or that it is polynomial $D(-1; 1)$-quadruple, if $\{a, b, c\}$ is

a polynomial $D(-1)$-triple and each of $ad+1$, $bd+1$ and $cd+1$ is a square of polynomial from $\mathbf{Z}[X]$.

In this paper we consider a polynomial variant of the $D(-1;1)$ problem. We can assume that at least one polynomial in polynomial $D(-1)$-triple is not constant, because otherwise we are in the integer case. Let $\mathbf{Z}^+[X]$ denote the set of all polynomials with integer coefficients and with a positive leading coefficient. For $a, b \in \mathbf{Z}[X]$, we define $a < b$ if $b - a \in \mathbf{Z}^+[X]$. We also define $|a|$ for a polynomial $a \in \mathbf{Z}[X]$ such that $|a| = a$ for $a \geq 0$ and $|a| = -a$ for $a < 0$. The main result of the paper is the following theorem:

THEOREM 1. *Let $\{a, b, c\}$ be a polynomial $D(-1)$-triple such that $0 < a < b < c$. If any of the following two conditions*:

1. $\deg(c) < (3\deg(a) + 5\deg(b))/2$,
2. *there does not exist the extension of $\{a, b, c\}$ to a $D(-1;1)$-quadruple with $0 < d < c$ and $d \neq d^-$,*

is satisfied, then such a triple can be extended to a polynomial $D(-1;1)$-quadruple only by polynomials $d^{\pm}$. More precisely, if $r, s, t \in \mathbf{Z}[X]$ are polynomials with positive leading coefficients which satisfy $ab - 1 = r^2$, $ac - 1 = s^2$ and $bc - 1 = t^2$, and if $\{a, b, c; d\}$ is a polynomial $D(-1;1)$-quadruple, then

$$d = d^{\pm} = -(a + b + c) + 2(abc \pm rst)\,.$$

REMARK 1. The first assumption is satisfied for example for $a = 1$, $b = x^2 + 1$, $c = 4x^4 + 1$ or $a = 1$, $b = 4x^2 + 1$, $c = 16x^6 - 8x^4 + x^2 + 1$. An example when the first condition on degrees is not satisfied is $a = 1$, $b = x^2 + 1$, $c = 64x^8 + 64x^6 + 16x^4 + 1$. The first assumption implies the second one, as will be explained in details in Section 3. Unfortunately, when the condition on degrees is not satisfied, the second assumption was of importance to give us the initial values of sequences introduced in Section 2. We believe that the second assumption, and with it, a polynomial variant of Conjecture 2, is always true for $D(-1;1)$-quadruples.

This problem is not solved for the integer case, except for some families mentioned above. The idea of considering polynomial variant is that Conjecture 1 and non-existence of $D(-1)$-quadruple were proved by Dujella and Fuchs in [4] and [5] in polynomial case, while in integer case there is still a lot of work towards proving those conjectures. The polynomial variant was solved in an easier way, since in its solving there appeared contradictions in comparing degrees of polynomials, which was not possible in an integer case.

In order to prove Theorem 1, we mostly use methods and strategy from [4] and [5]. However, not everything works in the same way, so some new ideas were needed which make this result interesting. Unfortunately, the minimality assumption does not hold here, at least not in the same or some obvious way, so we added the conditions mentioned in Theorem 1

that give us the important information on initial values of binary recurrence sequences whose intersection we want to find. It is therefore important that we work in $\mathbf{Z}[X]$ where we have ordered elements.

The organization of the paper is the following. Firstly, we transform our problem of the extension of $D(-1)$-triple to solving the system of simultaneous Pellian equations. Furthermore, it is transformed to finding intersection of binary recurrent sequences. We solve this using congruence relations and gap principle.

Let us also mention that solving this problem we have found one mistake made in [9]. There is also necessary to consider the case of m and n not having the same parity. However, the same way as here, this case is easier to solve.

2. System of Pellian Equations

From now on we assume that $\{a, b, c\}$ is a polynomial $D(-1)$-triple such that $a < b < c$, and without loss of generality we can assume that all polynomials are from $\mathbf{Z}^+[X]$. Moreover, we assume that at least one of the polynomials a, b and c is non-constant since otherwise we are in the integer case because it is not possible to extend triple $\{a, b, c\}$ of constant polynomials with non-constant polynomial d, which is easy to see by comparing leading coefficients in equations (2). Therefore, $\deg(c) > 0$. Then there exist $r, s, t \in \mathbf{Z}^+[X]$ such that

$$ab - 1 = r^2, \quad ac - 1 = s^2, \quad bc - 1 = t^2\,. \tag{1}$$

Letters r, s and t will always have this meaning in this paper. Let $a_0, b_0, c_0, r_0, s_0, t_0$ be the leading coefficients of the polynomials a, b, c, r, s, t, respectively. Then, from (1), we have $a_0c_0 = s_0^2$ and $b_0c_0 = t_0^2$. Hence, a_0, b_0, c_0 must have the same sign, so there is no loss of generality in assuming that $a, b, c \in \mathbf{Z}^+[X]$. Also, a_0b_0 is obviously a perfect square. We can furthermore conclude that a and b cannot both be constants, because then $a_0b_0 - 1$ would also be a perfect square and this is possible only for $a = b = 1$, and we do not allow equal elements in the triple.

Assume that we can extend polynomial $D(-1)$-triple $\{a, b, c\}$ to a $D(-1; 1)$-quadruple with $d \in \mathbf{Z}^+[X]$. Then, there also exist $x, y, z \in \mathbf{Z}^+[X]$ such that

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

Notice that we can always construct the polynomials $d^{\pm}$ with the property that $ad^{\pm} + 1$, $bd^{\pm} + 1$ and $cd^{\pm} + 1$ are perfect squares. We give the construction in the following lemma which was proved in [7].

LEMMA 1. *Let $\{a,b,c\}$ be a polynomial $D(-1)$-triple and let* (1) *holds. Then, there exist polynomials $d^{\pm}, u^{\pm}, v^{\pm}, w^{\pm} \in \mathbf{Z}[X]$ such that*

$$ad^{\pm}+1=(u^{\pm})^2,\ \ bd^{\pm}+1=(v^{\pm})^2,\ \ cd^{\pm}+1=(w^{\pm})^2\,. \tag{3}$$

More precisely,

$$d^{\pm}=-(a+b+c)+2abc\pm 2rst\,, \tag{4}$$

$$u^{\pm}=at\pm rs,\ \ v^{\pm}=bs\pm rt,\ \ w^{\pm}=cr\pm st\,. \tag{5}$$

An easy computation gives us

$$d^{+}\cdot d^{-}=(c-a-b-2r)(c-a-b+2r)\,. \tag{6}$$

Furthermore, we have

$$c=a+b-d^{\pm}+2abd^{\pm}\mp 2ru^{\pm}v^{\pm}\,.$$

Let us for the rest of the paper denote

$$\deg(a)=\alpha,\ \ \deg(b)=\beta\ \text{ and }\ \deg(c)=\gamma\,.$$

We have that $\alpha\geq 0$ and $\beta>0$.

We first prove a gap principle, which is well known in the classical case and was also used in considering polynomial variants of the problem of Diophantus (see e.g. [5, Lemma 4]).

LEMMA 2. *Let $\{a,b,c\}$ be a polynomial $D(-1)$-triple for which* (1) *holds and $a<b<c$. Then $c=a+b+2r$ or $\gamma\geq\deg(d^{-})+\alpha+\beta$, where d^{-} is defined by* (4).

PROOF. From (4), we conclude that $\deg(d^{+})=\alpha+\beta+\gamma$. Let $\deg(d^{-})\geq 0$. From (6) and from the fact that $a<b<c$ we get

$$\deg(d^{+})+\deg(d^{-})=\deg((c-a-b)^2-(2r)^2)\leq 2\gamma$$

so $\deg(d^{-})\leq\gamma-\alpha-\beta$. Since we have at most one constant in the polynomial $D(-1)$-triple $\{a,b,c\}$, we conclude that $\deg(d^{-})<\gamma$.

Now we have two possibilities.

1) If $d^{-}=0$, then from (6) we get $c=a+b\pm 2r$. However, we cannot have $c=a+b-2r$, because $a<b<c$. Therefore, $c=a+b+2r$.

2) If $d^{-}\neq 0$, then $\gamma\geq\deg(d^{-})+\alpha+\beta$. □

Notice that from Lemma 2 we either have that

$$\gamma\geq\alpha+\beta$$

or $c = a + b + 2r$.

Eliminating d from (2), we obtain the following system of simultaneous Pellian equations:

$$az^2 - cx^2 = a - c\,, \tag{7}$$

$$bz^2 - cy^2 = b - c\,. \tag{8}$$

We will now describe the sets of solutions of equations (7) and (8). In the proof we follow the strategy used in [4, Lemma 1], but also in numerous similar results on the solutions of Pellian equations.

LEMMA 3. *Let (z, x) and (z, y) be solutions, with x, y, z in $\mathbf{Z}^+[X]$, of (7) and (8) respectively. Then there exist solutions (z_0, x_0) and (z_1, y_1), with z_0, x_0, z_1, y_1 in $\mathbf{Z}[X]$, of (7) and (8), respectively such that*

(i) *the following inequalities are satisfied*:

$$0 < x_0,\ x_0^2 \le a(c-a),\ z_0^2 < c(c-a)\,, \tag{9}$$

$$0 < y_1,\ y_1^2 \le b(c-b),\ z_1^2 < c(c-b)\,, \tag{10}$$

(ii) *and there exist integers $m, n \ge 0$ such that*

$$z\sqrt{a} + x\sqrt{c} = (z_0\sqrt{a} + x_0\sqrt{c})(2ac - 1 + 2s\sqrt{ac})^m\,, \tag{11}$$

$$z\sqrt{b} + y\sqrt{c} = (z_1\sqrt{b} + y_1\sqrt{c})(2bc - 1 + 2t\sqrt{bc})^n\,. \tag{12}$$

PROOF. First observe that

$$(s + \sqrt{ac})^{2m} = (s^2 + ac + 2s\sqrt{ac})^m = (2ac - 1 + 2s\sqrt{ac})^m\,.$$

Multiplying that with the conjugate $(s - \sqrt{ac})^{2m}$ we obtain that

$$(s + \sqrt{ac})^{2m}(s - \sqrt{ac})^{2m} = (s^2 - ac)^{2m} = (-1)^{2m} = 1\,. \tag{13}$$

Let us consider all pairs (z^*, x^*) of polynomials of the form

$$z^*\sqrt{a} + x^*\sqrt{c} = (z\sqrt{a} + x\sqrt{c})(2ac - 1 + 2s\sqrt{ac})^m\,,$$

where $m \in \mathbf{Z}$ and (z, x) is a solution of (7) in polynomials from $\mathbf{Z}^+[X]$. By (13) it is clear that (z^*, x^*) satisfies (7) .

Let $(2ac - 1 + 2s\sqrt{ac})^m = p + q\sqrt{ac}$, where $p, q \in \mathbf{Z}[X]$. We have

$$z^*\sqrt{a} + x^*\sqrt{c} = (zp + cxq)\sqrt{a} + (px + azq)\sqrt{c}\,.$$

Hence, $x^* = px + azq$. We want to show that $x^* > 0$. If $m \ge 0$, then $p, q > 0$ so $x^* > 0$. If $m < 0$, then $p > 0$ and $q < 0$. If we assume that $x^* \le 0$, then $px \le -azq$. Both sides

in the previous inequality are positive so squaring we obtain $p^2x^2 \leq a^2z^2q^2$. From (13) we conclude that $p^2 - acq^2 = 1$ and we further obtain $x^2 + x^2q^2ac \leq q^2a^2z^2$. Therefore,

$$x^2 \leq q^2a(az^2 - cx^2) = q^2a(a-c) < 0\,,$$

which is a contradiction. So, we conclude that $x^* > 0$.

Among all pairs (z^*, x^*), we choose a pair with the property that x^* is minimal, and we denote that pair by (z_0, x_0). We define polynomials z' and x' by

$$z'\sqrt{a} + x'\sqrt{c} = (z_0\sqrt{a} + x_0\sqrt{c})(2ac - 1 - 2s\varepsilon\sqrt{ac})\,,$$

where $\varepsilon = 1$ if $z_0 > 0$ and $\varepsilon = -1$ if $z_0 < 0$. From the minimality of x_0 we conclude that

$$x' = x_0(2ac-1) - 2asz_0\varepsilon \geq x_0\,.$$

This leads to $x_0(ac-1) \geq as|z_0|$. Squaring this inequality, we get

$$x_0^2(ac-1)^2 \geq a^2s^2z_0^2 = a(ac-1)(a-c+cx_0^2)\,.$$

Finally, we can conclude that $0 < x_0$ and $x_0^2 \leq a(c-a)$. The bound for $|z_0|$ follows from (7).

We proved that there is a solution (z_0, x_0) of (7), which satisfies (9), and an integer $m \in \mathbf{Z}$ such that (11) holds. It remains to prove that $m \geq 0$. Assume that $m < 0$. Then, as above, we obtain $z = z_0p + x_0cq$ (notice that in this case $q < 0$). Thus, from the condition $z > 0$, we obtain $z_0p > -x_0cq$ where both sides of inequality are positive. By squaring that inequality and using the equation $p^2 - acq^2 = 1$, we obtain

$$z_0^2 > x_0^2c^2q^2 - acq^2z_0^2 = cq^2(c-a) \geq c(c-a)\,.$$

This is in contradiction with (9), so we conclude that $m \geq 0$.

The proof of the statement for the equation (8) is analogous. □

By Lemma 3, there exist a non-negative integer m and a solution (z_0, x_0) of (7) such that (9) and (11) hold. Also, there exist a non-negative integer n and a solution (z_1, y_1) of (8) such that (10) and (12) hold. Hence, $z = v_m = w_n$, where the binary recurrent sequences $(v_m)_{m\geq 0}$ and $(w_n)_{n\geq 0}$ are defined by

$$v_0 = z_0,\quad v_1 = (2ac-1)z_0 + 2scx_0,\quad v_{m+2} = (4ac-2)v_{m+1} - v_m\,, \tag{14}$$

$$w_0 = z_1,\quad w_1 = (2bc-1)z_1 + 2tcy_1,\quad w_{n+2} = (4bc-2)w_{n+1} - w_n\,. \tag{15}$$

3. Congruence Relations

From (14) and (15), by induction, we can easily prove the following lemma:

LEMMA 4. *Let the sequences (v_m) and (w_n) be given by* (14) *and* (15). *Then, we have*

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

Also, by induction on m and n, respectively, from (14) *and* (15) *we obtain the following information on the degrees of the elements of the above sequences.*

LEMMA 5. *Let* (v_m) *and* (w_n) *be the sequences defined by* (14) *and* (15). *Then, for* $m, n \geq 1$ *we have*

$$\deg(v_m) = (m-1)(\alpha+\gamma) + \deg(v_1)\,,$$
$$\deg(w_n) = (n-1)(\beta+\gamma) + \deg(w_1)\,.$$

The following lemma follows from Lemma 4 and estimates for initial values z_0 and z_1.

LEMMA 6. *If the equation* $v_m = w_n$ *has a solution, then* $(-1)^m z_0 = (-1)^n z_1$.

Furthermore, it can easily be proved by induction, that the same congruence as in [6, Lemma 2] are obtained by considering the sequences (v_m) and (w_n) modulo $8c^2$:

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

From the congruences and Lemma 6, it follows that if $v_m = w_n$ and $m \equiv n \pmod 2$, then

$$am^2 z_0 + smx_0 \equiv bn^2 z_1 + tny_1 \pmod{4c}\,, \tag{16}$$

while if m and n do not have the same parity, then

$$am^2 z_0 + smx_0 \equiv -bn^2 z_1 - tny_1 \pmod{4c}\,. \tag{17}$$

In order to prove Theorem 1, we will now compute the initial values of our sequences.

We are interested in sequences (v_m) and (w_n) such that $z^2 = v_m^2 = w_n^2 = cd+1$, where $d \in \mathbf{Z}^+[X]$. This implies that $v_m^2 \equiv 1 \pmod c$ and $w_n^2 \equiv 1 \pmod c$. From Lemma 4 it follows that

$$z_0^2 \equiv 1 \pmod c\,.$$

Then, there exists

$$d_0 = \frac{z_0^2 - 1}{c} \in \mathbf{Z}^+[X] \cup \{0\}\,.$$

From (7) and (8) we have

$$x_0^2 = ad_0 + 1 \ \text{ and } \ y_1^2 = bd_0 + 1\,. \tag{18}$$

Furthermore, from (9), we have $cd_0 = z_0^2 - 1 < c^2$, so

$$d_0 < c\,.$$

Therefore, we can construct a polynomial $d_0 < c$ such that either $d_0 = 0$ or $\{a, b, c; d_0\}$ is a polynomial $D(-1;1)$-quadruple. If the second condition of Theorem 1 is satisfied, then it is easy to conclude that $d_0 = 0$ or $d_0 = d^-$. Furthermore, if the first condition is satisfied, then we get the same from [8, Lemma 5]. We only have to notice that $\{ia, ib, -id_0, ic\}$ is a polynomial $D(1)$-quadruple in $\mathbf{Z}[i][X] \subset \mathbf{C}[X]$. Then, from [8, Lemma 5] we get that

$\{ia, ib, -id_0, ic\}$ cannot be irregular $D(1)$-quadruple. That implies that it is a regular quadruple or that $id_0 = 0$ or that some elements in quadruple are same. If it is a regular quadruple, we have

$$-id_0 = ia + ib + ic + 2ia \cdot ib \cdot ic - 2ir \cdot is \cdot it$$

and

$$d_0 = -(a + b + c) + 2abc - 2rst = d^- .$$

If $id_0 = 0$, then it is obvious that $d_0 = 0$. Finally, because the quadruple is from $\mathbf{Z}[i][X]$ (where in general the squares cannot differ by 1), the only possibility to have the same elements is when $a = 1$ and $d_0 = -1$. But, then $\{a, b, c; d_0\}$ is obviously not a $D(-1;1)$-quadruple in $\mathbf{Z}[X]$. Thus, we conclude that $d_0 \in \{0, d^-\}$.

From $cd_0 + 1 = z_0^2$, we have the first possibility that $d_0 = 0$ and then

1.) $z_0 = \pm 1$.

The second possibility is that $d_0 = d^-$. Then, using (3), we obtain

2.) $z_0 = \pm(cr - st)$.

4. Proof of Theorem 1

In this section we will finish the proof of the main theorem.

Let us consider the case **1.)** first. Using (9), (10) and (18), for $d_0 = 0$ we obtain that $x_0 = 1$ and $y_1 = 1$. Let $a = A^2DX^\alpha + \cdots$, $b = B^2DX^\beta + \cdots$ and $c = C^2DX^\gamma + \cdots$, where A, B, C, D are positive integers. We will consider several subcases depending on degrees of the polynomials a, b and c.

1. a) Let $\beta < \gamma$. From (16), for $m \equiv n \pmod 2$, we have

$$\pm am^2 + sm \equiv \pm bn^2 + tn \pmod{4c} .$$

In this case we obtain that $\pm am^2 + sm = \pm bn^2 + tn$, so we conclude that $\alpha = \beta$. Similarly, from (17) we have the same result for $m \not\equiv n \pmod 2$. Then, by Lemma 5, we get that $m = n$. Hence, $\pm m(a - b) = t - s$. Multiplying that with $t + s$, we obtain $\mp m(b - a)(t + s) = t^2 - s^2 = c(b - a)$. Finally, we have

$$\mp m(t + s) = c ,$$

which contradicts $\beta < \gamma$.

1. b) Assume that $\alpha < \beta = \gamma$. By Lemma 2 we have that if $c \neq a + b + 2r$, then $\gamma \geq \deg(d^-) + \alpha + \beta$ and $d^- \neq 0$. In this case a and d^- are both constant polynomials. Also, $d^- = \mu^2 D$ for some positive integer μ, because the leading coefficient of $bd^- + 1$ is

a perfect square. Then we have that $ad^- + 1$ and ad^- are both perfect squares, which is not possible. Therefore $c = a + b + 2r$. This yields $s = a + r$ and $t = b + r$. Then, if $m \equiv n \pmod 2$, from (16) we have

$$\pm am^2 + am + rm \equiv \pm bn^2 + bn + rn \pmod{4c}.$$

From $b \equiv -a - 2r \pmod c$, we have

$$a(\pm m^2 \pm n^2 + n + m) = r(\mp 2n^2 - n - m).$$

Since $\alpha < \beta$, both sides of this equation are equal to 0. Therefore, $m = n = 0$, which yields $d = 0$, or $m = n = 1$ which implies $z_0 = z_1 = -1$. Then, $z = v_1 = w_1 = 1 + 2rc$. From that we obtain

$$d = 4r(a + r)(b + r) = -(a + b + c) + 2abc + 2rst = d^+.$$

In case $m \not\equiv n \pmod 2$, from (17) we get $m = \mp 2n^2 + n$ which contradicts the assumption about parities of m and n.

1. c) Assume now that $\alpha = \beta = \gamma$. By Lemma 2 we have that $c = a + b + 2r$. From (14), (15) and Lemma 5 we conclude that $m = n$. From (16), we obtain

$$(\pm m^2 + m)(a - b) \equiv 0 \pmod{4c}. \tag{19}$$

If $\pm m^2 + m \neq 0$, then $k(b - a) = l(a + b + 2r)$, where $k, l \in \mathbf{Z}$, $k \neq l$ and $k \neq 0$. From that, it follows $(k - l)b - (k + l)a = 2lr$. Squaring this, using (1), we further get $(k - l)^2b^2 - 2(k^2 + l^2)ab + (k + l)^2a^2 = -4l^2$. We finally have

$$((k - l)^2b - (k + l)^2a)(b - a) = -4l^2.$$

By comparing the leading coefficients of the polynomials on both hand sides of the previous equation, we obtain $4kl = 0$, which is not possible.

Let us now consider the case **2.)** Using (9), (10) and (18), for $d_0 = d^-$ we obtain that $x_0 = at - rs$ and $y_1 = bs - rt$. If $\beta = \gamma$, then $c = a + b + 2r$, as we already concluded using Lemma 2. In that case $st - cr = 1$, so $z_0 = \pm 1$ which was already solved. Therefore, we may assume that $\beta < \gamma$.

2. a) Let us first assume that $\alpha = \beta < \gamma$. From (14), (15) and Lemma 5 we conclude that $m = n$. It is obvious if $m \equiv n \pmod 2$. However, if $m \not\equiv n \pmod 2$, we have $\deg(v_1) = 2\gamma$ and $\deg(w_1) = \alpha + \gamma$ or vice versa. In both cases, Lemma 5 implies that $m = n \pm 1$ and $\alpha = 0$ which is not possible because it would imply that $\beta = \alpha = 0$. Now, from (16), using (1), we have

$$\mp astm^2 + astm + rm \equiv \mp bstn^2 + bstn + rn \pmod c.$$

Multiplying that with $2st$, we obtain

$$\mp 2(am(m\mp 1)-bn(n\mp 1))\equiv 2rst(n-m) \pmod{c}\,. \tag{20}$$

Since $m=n$,

$$\mp 2m(m\mp 1)(a-b)=0\,. \tag{21}$$

This can only hold for $m=n=0$, which leads to $d=d^-$, or $m=n=1$, where from (21) we first conclude that $z_0=cr-st$ and then, $z=v_1=w_1=cr+st$, and finally $d=d^+$.

2. b) Suppose that $\alpha<\beta<\gamma$. First, from (4) we see that it holds

$$-2rst\equiv d^-+a+b \pmod{c}\,. \tag{22}$$

From Lemma 2 we have that $\deg(d^-)+\alpha+\beta\le\gamma$. Then, since $\alpha+\beta>0$, it follows that $\deg(d^-)<\gamma$. Let us now separate the cases depending on the degree of d^-.

Assume first that $\deg(d^-)<\beta$ and $m\equiv n \pmod 2$. In this case, from (20), using (22), and by comparing the leading coefficients, we obtain that $\pm 2n(n\mp 1)=m-n$. Hence,

$$m=n\pm 2n(n\mp 1)=\begin{cases}-2n^2-n\,,\\ 2n^2-n\,,\end{cases} \tag{23}$$

where the first possibility holds for $z_0=cr-st<0$ and the second for $z_0=-cr+st>0$. Both cases can hold for $m=n=0$. This leads to $d=d^-$. The first case can only hold in this situation, since otherwise we obtain $m<0$ which is not possible. For the second case, from (14) and (15) we obtain that

$$\deg(v_1)=2\gamma+\frac{\alpha-\beta}{2}\,,$$
$$\deg(w_1)=2\gamma+\frac{\beta-\alpha}{2}\,.$$

From that and Lemma 5, we furthermore obtain

$$\deg(v_m)=2\gamma+\frac{\alpha-\beta}{2}+(m-1)(\alpha+\gamma)\,,$$
$$\deg(w_n)=2\gamma+\frac{\beta-\alpha}{2}+(n-1)(\beta+\gamma)\,.$$

Therefore, for $v_m=w_n$, it follows that

$$m(\alpha+\gamma)=n(\beta+\gamma)\,. \tag{24}$$

From that, for $n\ge m\ge 1$, we obtain a contradiction. So $n<m$ or $m=n=0$. Moreover, we have $m=2n^2-n$, so $(2n-1)(\alpha+\gamma)=(\beta+\gamma)$ and $(2n-2)(\gamma+\alpha)=\beta-\alpha$. This can only hold for $n=1$, but then, from (23), we obtain $m=1$ which is not possible. In case

that $m \not\equiv n \pmod 2$, from

$$\mp 2(am(m \mp 1) - bn(n \pm 1)) \equiv -2rst(m+n) \pmod c\,, \tag{25}$$

using (22) and by comparing the leading coefficients, we obtain that $\pm 2n(n \pm 1) = m + n$ which is in contradiction with the assumption about parities of m and n.

If $\deg(d^-) > \beta$ and if $m \not\equiv n \pmod 2$ from (25), by using (22), and by comparing the leading coefficients, we have $m + n = 0$ which leads to contradiction. On the other hand, if $m \equiv n \pmod 2$, then from (20) and (22) we obtain $0 = m - n$ or $m = n$. In this case, from (20) we get that $\mp 2m(m \mp 1)(a - b) = 0$. This is possible only for $m = 0$ or $m = 1$. For $m = n = 0$ we have $d = d^-$. The case $m = n = 1$ is not possible if $z_0 > 0$, as we have already shown. For $z_0 = cr - st$, we have $z = v_1 = w_1 = cr + st$ and then $d = d^+$.

Suppose finally that $\deg(d^-) = \beta$. Since $s^2t^2 \equiv 1 \pmod c$, there exists $c_1 \in \mathbf{Q}[X] \setminus \{0\}$ such that $\deg(c_1) \geq \frac{\gamma}{2}$, $c_1 | c$ and

$$st \equiv \pm 1 \pmod{c_1}\,. \tag{26}$$

From Lemma 2 we obtain that $\beta \leq \frac{\gamma-\alpha}{2}$. Now we consider congruences (20) and (25) modulo c_1 and we use (26). That way we obtain, in each case, the congruence modulo c_1 with the polynomial of degree equal to $\frac{\alpha+\beta}{2}$ on the right hand side and on the left hand side the polynomial of degree equal to β. If $\beta < \frac{\gamma}{2}$, we have a contradiction, except for $\pm 2n(n \mp 1) = 0$, in the first case, and $\pm 2n(n \pm 1) = 0$ in the other, which leads to the conclusion that $n = 0$ or $n = 1$ in both cases. For $n = 0$, we conclude from (20) and (26), and similarly from (25), that $m = 0$, which for the same parity case leads to the conclusion that $d = d^-$, and in the other case to an obvious contradiction. Analogously, for $n = 1$ it follows that $m = 1$, in the same parity case, which leads to $d = d^+$, and in the case $m \not\equiv n \pmod 2$ we get $m = -1$ $(m+n = 0)$, which is not possible. We are now left with the possibility that $\beta = \frac{\gamma}{2}$ i.e. $\alpha = 0$.

To a polynomial $D(-1)$-pair $\{a, b\}$ we can again associate a Pellian equation

$$at^2 - bs^2 = b - a\,, \tag{27}$$

which gives all extensions of the pair $\{a, b\}$ to the polynomial $D(-1)$-triple $\{a, b, c\}$. Moreover, if we denote with (t_0, s_0) the fundamental solution of the equation (27), we can associate a linear recurrent sequence to the pair $\{a, b\}$. We have $t = \widetilde{t}_v$, where the binary recurrence sequence $(\widetilde{t}_v)_{v\geq 0}$ is defined by

$$\widetilde{t}_0 = t_0,\ \ \widetilde{t}_1 = (2ab-1)t_0 + 2rbs_0,\ \ \widetilde{t}_{v+2} = (4ab-2)\widetilde{t}_{v+1} - \widetilde{t}_v\,.$$

Also, similarly as in the proof of Lemma 3, we obtain that $|t_0| < b$. Since in this case $\alpha = 0$ and $\beta = \frac{\gamma}{2}$, we must have $\deg(t) = \frac{3\beta}{2}$. It is easy to prove that $\widetilde{t}_v \equiv (-1)^v t_0 (\mathrm{mod}\, b)$. On the other hand, from $bc - 1 = t^2$ and using the previous congruence we have $t_0^2 \equiv -1 (\mathrm{mod}\, b)$ so we conclude $\frac{\beta}{2} \leq \deg(t_0) \leq \beta$. We can prove by induction that $\deg(\widetilde{t}_v) = (v-1)(\alpha+\beta) +$

$\deg(\widetilde{t}_1)$ for $v \geq 1$ which leads to the conclusion that the only possibility is $\deg(t_0) = \frac{\beta}{2}$. It actually follows from the fact that $\beta \leq \deg(\widetilde{t}_1) \leq 2\beta$ which yields $\deg(\widetilde{t}_2) \geq 2\beta > \frac{3\beta}{2}$, so the only possibility for t is $t = t_1$. Then, $\deg(\widetilde{t}_1) = \frac{3\beta}{2}$ and $\deg(t_0) = \frac{\beta}{2}$ (we have to notice that $((2ab-1)^2 t_0^2 - 4r^2 b^2 s_0^2)$ is of degree 3β in this case). Now from (27) we get that $\deg(s_0) = 0$ and $ac_0 = s_0^2 + 1$ is a constant. In that case ac_0 must also be a square since $\{a, b, c_0\}$ is also a polynomial $D(-1)$-triple. This is possible only for $a = c_0 = 1$. Therefore, we have $s_0 = 0$ and $t_0 = \sqrt{b-1} = r$. Then, all the solutions t of (27) satisfy the following linear recurrences

$$\widetilde{t}_0 = r, \;\; \widetilde{t}_1 = (2ab-1)r, \;\; \widetilde{t}_{v+2} = (4ab-2)\widetilde{t}_{v+1} - \widetilde{t}_v$$

and we are interested in those $t = \widetilde{t}_v$ for which $\deg(t) = \frac{3\beta}{2}$. We conclude that $t = \widetilde{t}_1$ and then we get $c = 4b^2 - 8b + 5$. Using (3) and (5), we finally obtain that $d^- = b - 2$. Now, from (20) and (25), using (22), and by comparing the leading coefficients, we obtain that $\pm 2n(n \mp 1) = 2(m-n)$ in the case $m \equiv n \pmod 2$, and $\pm 2n(n \pm 1) = 2(m+n)$ if $m \not\equiv n \pmod 2$. In the second case, we get $m = \pm n^2$ which is contradiction with the assumption about parity. On the other hand, in the first case we have

$$m = n \pm n(n \mp 1) = \begin{cases} -n^2\,, \\ n^2\,, \end{cases} \tag{28}$$

where the first possibility holds for $z_0 = cr - st < 0$ and the second for $z_0 = -cr + st > 0$. Both cases hold for $m = n = 0$. This leads to $d = d^-$. The first case can only hold in this situation, since otherwise we obtain $m < 0$, which is not possible. For the second case, for $v_m = w_n$, from (24), it follows that

$$2n^2\beta = 3n\beta\,.$$

It is obviously not possible for positive integer n. It finishes the proof of Theorem 1.

ACKNOWLEDGMENT. The authors were supported by Croatian Science Foundation under the project no. 6422. The third author was also supported by the University of Rijeka research grant no. 13.14.1.2.02. We also thank the referee for careful reading and valuable suggestions.

References

[1] A. DUJELLA, There are only finitely many Diophantine quintuples, J. Reine Angew. Math. **566** (2004), 183–214.

[2] A. DUJELLA, Diophantine m-tuples, http://web.math.pmf.unizg.hr/~duje/dtuples.html.

[3] A. DUJELLA, A. FILIPIN and C. FUCHS, Effective solution of the $D(-1)$-quadruple conjecture, Acta Arith. **128.4** (2007), 319–338.

[4] A. DUJELLA and C. FUCHS, A polynomial variant of a problem of Diophantus and Euler, Rocky Mountain J. Math. **33** (2003), 797–811.

[5] A. DUJELLA and C. FUCHS, Complete solution of the polynomial version of a problem of Diophantus, J. Number Theory **106** (2004), 326–344.

[6] A. DUJELLA and C. FUCHS, Complete solution of a problem of Diophantus and Euler, J. London Math. Soc. **71** (2005), 35–52.

[7] A. DUJELLA, C. FUCHS and R. F. TICHY, Diophantine m-tuples for linear polynomials, Period. Math. Hungar. **45** (2002), 21–33.

[8] A. DUJELLA and A. JURASIC, On the size of sets in a polynomial variant of a problem of Diophantus, Int. J. Number Theory **6** (2010), 1449–1471.

[9] A. FILIPIN, On the polynomial parametric family of the sets with the property $D(-1;1)$, Bol. Soc. Mat. Mexicana **16** (2010), 1–8.

[10] Y. FUJITA, The $D(1)$-extensions of $D(-1)$-triples $\{1,2,c\}$ and integer points on the attached elliptic curves, Acta Arith. **128** (2007), 349–375.

[11] Y. FUJITA, The Hoggatt-Bergum conjecture on $D(-1)$-triples $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$ and integer points on the attached elliptic curves, Rocky Mountain J. Math. **39** (2009), 1907–1932.

[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** (2011), 120–137.

Present Addresses:
MARIJA BLIZNAC TREBJEŠANIN
FACULTY OF SCIENCE,
UNIVERSITY OF SPLIT,
RUĐERA BOŠKOVIĆA 33, 21000 SPLIT, CROATIA.
e-mail: marbli@pmfst.hr

ALAN FILIPIN
FACULTY OF CIVIL ENGINEERING,
UNIVERSITY OF ZAGREB,
FRA ANDRIJE KAČIĆA-MIOŠIĆA 26, 10000 ZAGREB, CROATIA.
e-mail: filipin@grad.hr

ANA JURASIĆ
DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF RIJEKA,
RADMILE MATEJČIĆ 2, 51000 RIJEKA, CROATIA.
e-mail: ajurasic@math.uniri.hr