COMPLETE SOLUTION OF THE POLYNOMIAL VERSION OF A PROBLEM OF DIOPHANTUS

ANDREJ DUJELLA* AND CLEMENS FUCHS‡

ABSTRACT. In this paper, we prove that if $\{a, b, c, d\}$ is a set of four non-zero polynomials with integer coefficients, not all constant, such that the product of any two of its distinct elements plus 1 is a square of a polynomial with integer coefficients, then

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1).$$

This settles the "strong" Diophantine quintuple conjecture for polynomials with integer coefficients.

1. INTRODUCTION

A set of m positive integers is called a Diophantine m-tuple if the product of any two of its distinct elements increased by 1 is a perfect square (cf. [3]). The first Diophantine quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat. In 1969, Baker and Davenport [2] proved that the Fermat's set cannot be extended to a Diophantine quintuple. The "folklore" conjecture is that there does not exist a Diophantine quintuple. Recently, the first author proved that there does not exist a Diophantine sextuple and there are only finitely many Diophantine quintuples (see [5]).

It was known already to Euler that every Diophantine pair $\{a, b\}$ can be extended to a Diophantine quadruple. Namely, if $ab + 1 = r^2$, then

$$\{a, b, a + b + 2r, 4r(a + r)(b + r)\}$$

is a Diophantine quadruple. A Diophantine triple of the form $\{a, b, a+b+2r\}$ is called a regular Diophantine triple. In 1979, Arkin, Hoggatt and Strauss [1] proved that every Diophantine triple can be extended to a Diophantine quadruple. More precisely, let $ab + 1 = r^2, ac + 1 = s^2, bc + 1 = t^2$, where r, s, t are positive integers. Define

$$d_{\pm} = a + b + c + 2abc \pm 2rst.$$

Then

$$\{a, b, c, d_{\pm}\}$$

*The first author was supported by the Ministry of Science and Technology, Republic of Croatia, grant 0037110.

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

are Diophantine quadruples (observe that $d_- < c$). Indeed,

$$(1) \quad ad_\pm + 1 = (at \pm rs)^2, \quad bd_\pm + 1 = (bs \pm rt)^2, \quad cd_\pm + 1 = (cr \pm st)^2.$$

Diophantine quadruples of this form are called regular Diophantine quadruples. Equivalently, $\{a, b, c, d\}$ is regular, if and only if

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1)$$

(see [9]). This is a quadratic equation in d with the roots $d_\pm$.

There is even a stronger version of the "folklore" conjecture from above, namely if we fix a Diophantine triple $\{a, b, c\}$, then there is a unique positive integer d such that $d > \max\{a, b, c\}$ and $\{a, b, c, d\}$ is a Diophantine quadruple. This means that every Diophantine quadruple is regular. In the mentioned result of the nonexistence of Diophantine sextuples, the author proves this stronger conjecture for all triples satisfying some gap conditions.

A polynomial variant of the above problems was first studied by Jones [10, 11].

Definition 1. *A set $\{a_1, a_2, \ldots, a_m\}$ of m non-zero polynomials with integer coefficients, which are not all constant, is called a* polynomial Diophantine m-tuple *if for all $1 \leq i < j \leq m$ the following holds: $a_i \cdot a_j + 1 = b_{ij}^2$, where $b_{ij} \in \mathbb{Z}[X]$.*

Observe that every polynomial pair can be extended to a polynomial triple and that every polynomial triple can be extended to a polynomial quadruple. In fact the relations from above are true after all, because they are obtained by purely algebraic manipulations. Therefore, we define

Definition 2. *A polynomial Diophantine quadruple $\{a, b, c, d\}$ is called* regular *if*

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1),$$

or, equivalently, if $d = d_+$ or d_-, where

$$d_\pm = a + b + c + 2abc \pm 2rst$$

and $r, s, t \in \mathbb{Z}[X]$ are defined by

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

The result obtained by the first author already mentioned above about the existence of only finitely many Diophantine quintuples implies that there does not exist a polynomial Diophantine quintuple. In the present paper, we will prove the "stronger" Diophantine quintuple conjecture for polynomials. Namely, we have

Theorem 1. *All polynomial Diophantine quadruples are regular.*

This theorem has been proved by Jones in [11] in the case that a, b, c are linear polynomials. Moreover, Jones has proved that there is no polynomial Diophantine quadruple with four polynomials all having the same positive degree (cf. [11, Corollary 1]). Other results related to polynomial versions of the above problem of Diophantus can be found in [6, 7, 8].

In the proof of Theorem 1, we follow the strategy from the paper of the first author [5]. Namely, we first transform the problem into solving a system of simultaneous Pellian equation, which reduces to finding intersections of binary recurring sequences of polynomials. We will assume that we have an irregular polynomial Diophantine quadruple $\{a, b, c, d\}$ with minimal d. This will lead, by using congruence relations and a gap principle, to a very precise determination of the initial terms of the recurring sequences. From this we will be able to prove our main result.

2. Reduction to intersections of recursive sequences

Let $\mathbb{Z}^+[X]$ denote the set of all polynomials with integer coefficients with positive leading coefficient. For $a, b \in \mathbb{Z}[X]$, $a < b$ means that $b - a \in \mathbb{Z}^+[X]$. The usual fundamental properties of inequality hold for this order. For $a \in \mathbb{Z}[X]$, we define $|a| = a$ if $a \geq 0$, and $|a| = -a$ if $a < 0$.

If $\{a, b, c, d\}$, $a < b < c < d$ is a Diophantine quadruple, then d is non-constant. Assume now that a and b are constant polynomials. Considering leading coefficients of $ad + 1$ and $bd + 1$ we conclude that ab is a perfect square, contradicting the assertion that $ab + 1$ is also a perfect square. Therefore, we proved that in a polynomial Diophantine quadruple there is at most one constant polynomial. It is also clear that all leading coefficients of the polynomials in a Diophantine m-tuple have the same sign. This implies that there is no loss of generality in assuming that they are all positive, i.e. that all polynomials are in $\mathbb{Z}^+[X]$.

Assume that $\{a, b, c, d\}$, where $0 < a < b < c < d$, is an irregular polynomial Diophantine quadruple with minimal d among all irregular polynomial Diophantine quadruples. Under this assumption we will end up with a contradiction, which implies that such a quadruple cannot exist.

Let $r, s, t \in \mathbb{Z}^+[X]$ be defined by

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

In this paper, the symbols r, s, t will always have this meaning. Moreover, let

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

with $x, y, z \in \mathbb{Z}^+[X]$. Eliminating d from (2) we obtain the system

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

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

We will now describe the sets of solutions of equation (3) and (4). The following lemma is an analogue of the result proved in [4] for the classical case of Pellian equations in integers (cf. [4]). A similar lemma for polynomials was also proved in [6].

Let

$$\deg a = A, \quad \deg b = B \quad \text{and} \quad \deg c = C.$$

The letters A, B, C will have this meaning for the rest of the paper.

Lemma 1. *If (z, x) and (z, y), with $x, y, z \in \mathbb{Z}^+[X]$, are polynomial solutions of (3) and (4) respectively, then there exist $z_0, x_0 \in \mathbb{Z}[X]$ and $z_1, y_1 \in \mathbb{Z}[X]$ with*

(i) *(z_0, x_0) and (z_1, y_1) are solutions of (3) and (4) respectively,*
(ii) *the following inequalities are satisfied:*

$$\deg x_0 \le \frac{A+C}{4} < \deg s, \quad \deg z_0 \le \frac{3C-A}{4} < C, \tag{5}$$

$$\deg y_1 \le \frac{B+C}{4} < \deg t, \quad \deg z_1 \le \frac{3C-B}{4} < C, \tag{6}$$

and

$$x_0, |z_0|, y_1, |z_1| > 0, \tag{7}$$

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

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

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

where this means that the coefficients of $\sqrt{a}, \sqrt{b}$ and $\sqrt{c}$ respectively on both sides are equal.

Proof. The proof of the statements follow from [8, Lemma 4]. □

In that way, our problem reduces to solving equations of the form

$$v_m = w_n,$$

where v_m and w_n are binary recursive sequences defined by

$$v_0 = z_0, \quad v_1 = sz_0 + cx_0, \quad v_{m+2} = 2sv_{m+1} - v_m, \tag{10}$$

for some solution (z_0, x_0) of (3) with (5), and

$$w_0 = z_1, \quad w_1 = tz_1 + cy_1, \quad w_{n+2} = 2tw_{n+1} - w_n, \tag{11}$$

for some initial values (z_1, y_1) as above.

We will need information on the degrees of these sequences and we collect these in the lemma below.

Lemma 2. *Let $(v_m), (u_n)$ be the sequences from above. Then*

$$\deg v_m = \deg v_1 + (m-1)\frac{A+C}{2},$$
$$\deg w_n = \deg w_1 + (n-1)\frac{B+C}{2}.$$

Proof. The proof runs by induction on m, n respectively and follows easily from (10) and (11). □

3. Gap principle and congruence relations

As we have seen, the polynomials $d_0 = d_+$ and d_- have the property that $ad_0 + 1, bd_0 + 1, cd_0 + 1$ are perfect squares. We repeat this construction in the following lemma which was proved e.g. in [7].

Lemma 3. *Let $\{a, b, c\}$ be a polynomial Diophantine triple and let $ab+1 = r^2, ac+1 = s^2, bc+1 = t^2$. Then for*

$$d_\pm = a + b + c + 2abc \pm 2rst,$$

we have

$$ad_\pm + 1 = u^2, \quad bd_\pm + 1 = v^2, \quad cd_\pm + 1 = w^2$$

with $u = at \pm rs, v = bs \pm rt, w = cr \pm st$. Furthermore, it holds

$$c = a + b + d_\pm + 2(abd_\pm \mp ruv).$$

Let us remark that an easy computation shows that

$$d_+ \cdot d_- = (c - a - b - 2r)(c - a - b + 2r).$$

The trivial observation that if $d_- \neq 0$, then $d_- \geq 1$ leads to the very useful gap principle, which was already proved by Jones in [11].

Lemma 4. *If $\{a, b, c\}$ is a polynomial Diophantine triple and $a < b < c$, then $c = a + b + 2r$ or $c \geq 2abd_- + 1$, where d_- is defined as above and $d_- \neq 0$.*

Proof. This was shown for example in the proof of Lemma 3 in [7] and follows easily from Lemma 3. □

Observe that from the gap principle it follows that we either have

$$C \geq A + B,$$

i.e. C is larger than A, B, since $A \geq 0$ and $B > 0$, or $c = a + b + 2r$ holds. We will use this fact several times later on.

Let us consider the sequences (v_m) and (w_n) modulo $2c$. From (10) and (11) it is easily seen (by induction) that

$$v_{2m} \equiv z_0 \pmod{2c}, \quad v_{2m+1} \equiv sz_0 + cx_0 \pmod{2c}, \tag{12}$$

$$w_{2n} \equiv z_1 \pmod{2c}, \quad w_{2n+1} \equiv tz_1 + cy_1 \pmod{2c}. \tag{13}$$

We will deduce later very precise information on the initial terms z_0 and z_1.

As a consequence of Lemma 1 and the relations (12) and (13), we obtain the following lemma.

Lemma 5. *We have:*

1) *If the equation $v_{2m} = w_{2n}$ has a solution, then $z_0 = z_1$.*

2) *If the equation $v_{2m+1} = w_{2n}$ has a solution, then $cx_0 - s|z_0| = |z_1|$.*

3) *If the equation $v_{2m} = w_{2n+1}$ has a solution, then $cy_1 - t|z_1| = |z_0|$.*

4) *If the equation $v_{2m+1} = w_{2n+1}$ has a solution, then $cx_0 - x|z_0| = cy_1 - t|z_1|$.*

Proof. We split the proof according to the statements of the lemma.

1) From Lemma 1 and equation (12) we have $|z_0 - z_1| < 2c$ and $z_0 \equiv z_1 \pmod{2c}$, which implies $z_0 = z_1$.

2) Observe that

$$(c+s)(cx_0 - s|z_0|) \le (cx_0 + s|z_0|)(cx_0 - s|z_0|) = \\ = c^2x_0^2 - s^2z_0^2 = c^2 - ac - z_0^2 \le c^2 - s^2,$$

thus $cx_0 - s|z_0| < c$. On the other hand we have

$$c^2 - ac - z_0^2 \ge c^2 - ac - \frac{c(c-a)}{4} = \frac{3c(c-a)}{4} > 0,$$

since $\deg z_0 \le \frac{3C}{2}$ which follows from (5) of Lemma 1 and $\deg c(c-a) = 2C$. This last equation follows trivially if $C > A$ and otherwise we have (by the gap principle) that $c = a+b+2r$ and therefore $\deg c - a = \deg b = C$. Hence,

$$0 < cx_0 - s|z_0| < c.$$

By (12) we have $sz_0 + cx_0 \equiv z_1 \pmod{2c}$. Thus we conclude that if $z_0 > 0$ then $z_1 = sz_0 - cx_0$, and if $z_0 < 0$, then $z_1 = sz_0 + cx_0$.

3) As in **2)**, we find that

$$0 < cy_1 - t|z_1| < c,$$

which implies that if $z_1 > 0$, then $z_0 = tz_1 - cy_1$, and if $z_1 < 0$, then $z_0 = tz_1 + cy_1$.

4) We have already proved that

$$0 < cx_0 - s|z_0| < c, \quad 0 < cy_1 - t|z_1| < c.$$

Hence, we have two possibilities: if $z_0 > 0$ then also $z_1 > 0$ and $sz_0 - cx_0 = tz_1 - cy_1$, and if $z_0 < 0$ then $z_1 < 0$ and $sz_0 + cx_0 = tz_1 + cy_1$. □

In the following lemma we will consider the sequences (v_m) and (w_n) modulo $4c^2$.

Lemma 6. *We have:*

1) $v_{2m} \equiv z_0 + 2c(az_0m^2 + sx_0m) \pmod{8c^2}$

2) $v_{2m+1} \equiv sz_0 + c\,[2asz_0m(m+1) + x_0(2m+1)] \pmod{4c^2}$

3) $w_{2n} \equiv z_1 + 2c(bz_1n^2 + ty_1n) \pmod{8c^2}$

4) $w_{2n+1} \equiv tz_1 + c\,[2btz_1n(n+1) + y_1(2n+1)] \pmod{4c^2}$

Proof. The proof runs by induction and can be done totally in the same way as in [4, Lemma 4]. □

4. Precise determination of initial terms

From the estimates of initial terms and congruence condition modulo $2c$, it follows that if the equation $v_m = w_n$ has a solution, then there exists a solution with $m = 0$ or 1 (see Lemma 5). But, that small solution induces $d_0 < c$ such that $ad_0 + 1$, $bd_0 + 1$ and $cd_0 + 1$ are perfect squares. From our minimality assumption it follows that $d_0 = 0$ or $d_0 = d_-$. This conclusion leads to very precise determination of initial terms:

Lemma 7. *We have:*

1) *If $v_{2m} = w_{2n}$ has a solution, then either*

1.1) $z_0 = z_1 = \pm 1$, *or*

1.2) $z_0 = z_1 = \pm(cr - st)$.

2) *If $v_{2m+1} = w_{2n}$ has a solution, then $z_0 = \pm t$ and $z_1 = \pm(st - cr)$.*

3) *If $v_{2m} = w_{2n+1}$ has a solution, then $z_0 = \pm(cr - st)$ and $z_1 = \mp s$.*

4) *If $v_{2m+1} = w_{2n+1}$ has a solution, then $z_0 = \pm t$ and $z_1 = \pm s$.*

Proof. **1)** From Lemma 5 we have $z_0 = z_1$. Define $d_0 = (z_0^2 - 1)/c \in \mathbb{Z}^+[X]$. Then we have

$$cd_0 + 1 = z_0^2.$$

We have already seen that $d_0 = 0$ or d_-. If $d_0 = 0$ then $z_0 = \pm 1$. If $d_0 = d_-$ then

$$z_0^2 = cd_- + 1 = (cr - st)^2,$$

(see equation (1)) and $z_0 = \pm(cr - st)$.

2) By Lemma 5, if $z_1 > 0$ then $z_0 < 0$ and we define $z' = z_1 = cx_0 + sz_0$, and if $z_1 < 0$ then $z_0 > 0$ and we define $z' = -z_1 = cx_0 - sz_0$. Thus $z' > 0$. Define $d_0 = (z'^2 - 1)/c \in \mathbb{Z}^+[X]$. We have again

$$cd_0 + 1 = z'^2.$$

Now we show that $d_0 = 0$ is impossible. This is clearly true if $z' > 1$. In the case that $z' = 1$, it follows that

$$c(c - a) - z_0^2 = c^2 - ac - z_0^2 = (cx_0 + s|z_0|)z'$$

and therefore

$$2C = \deg\left((cx_0 + s|z_0|)z'\right) \leq \frac{3C}{2},$$

which is a contradiction. Here we have again used that $\deg c(c-a) = 2C$; this is clearly true if $C > A$ and otherwise we have $c - a = b + 2r$, i.e. $\deg(c-a) = \deg b = C$.

This means that $d_0 = d_-$ and as above $z' = \pm(cr - st)$. Thus $z_1 = \pm(cr - st)$ and

$$|z_1| = cr - st = cx_0 - s|z_0|.$$

Observe that we have $cr - st > 0$ since $c^2r^2 = abc^2 + c^2 > abc^2 + ac + bc + 1 = (ac+1)(bc+1) = s^2t^2$. The fact that $c^2 > bc + ac + 1$ follows easily from the gap principle (Lemma 4). The last equation can be rewritten as $c(x_0 - r) = s(|z_0| - t)$. From $\gcd(c, s) = 1$ (which is a consequence of $ac + 1 = s^2$) it follows that $|z_0| \equiv t \pmod{c}$, and since $|z_0| < c, t < c$ (which follows from Lemma 1 and $bc+1 = t^2$), we conclude that $|z_0| = t$ and $x_0 = r$.
3) In analogy to above, let $z' = z_0 = cy_1 + tz_1$ if $z_0 > 0$, and $z' = -z_0 = cy_1 - tz_1$ if $z_0 < 0$, and define $d_0 = (z'^2 - 1)/c$. Then

$$cd_0 + 1 = z'^2$$

and $0 < d_0 < c$. Thus $d = d_-$, which implies $|z'| = cr - st$. Hence, $|z_0| = cr - st$ and $c(y_1 - r) = t(|z_1| - s)$. Since $\gcd(t, c) = 1$ we have $|z_1| \equiv s \pmod{c}$, which implies $|z_1| = s$.
4) Let $z' = cx_0 - s|z_0| = cy_1 - t|z_1|$ and $d_0 = (z'^2 - 1)/c$. We have $d_0 = d_-$ and therefore $|z'| = cr - st$. We have already shown that this fact implies $|z_0| = t$ and $|z_1| = s$. □

Let $a = \alpha^2\delta X^A + \cdots$, $b = \beta^2\delta X^B + \cdots$, $c = \gamma^2\delta X^C + \cdots$.
We will consider several subcases:

$$B < C, \quad A < B = C, \quad A = B = C.$$

These cases correspond to the different types of standard Diophantine triples (see Definition 1 in [5]). Note that if $B = C$, then $c = a + b + 2r$. Indeed, by our gap principle (Lemma 4) we have that if $c \neq a + b + 2r$, then $c \geq 2abd_-$, where d_- is defined in Definition 1 and $d_- \neq 0$. Assume that $B = C$. Then a and d_- are both constant polynomials. From this it follows that $B = C > 0$ (because there can be at most one constant polynomial in the Diophantine triple) and $d_- = \mu^2\delta$ because the leading coefficient of $bd_- + 1$ is a perfect square. But then we have that $ad_- + 1$ and ad_- are both perfect squares, a contradiction.

In the next section we will turn our discussion to the remaining cases. Before we do this, we collect some technical information in the following lemmata.

Lemma 8. *Assume that $B < C$. Then, we have*

$$\deg(cr - st) = C - \frac{A+B}{2}.$$

Moreover, if $z_0 = cr - st$ *then*

$$\deg(cx_0 - sz_0) = \frac{B+C}{2},$$

and if $z_1 = cr - st$ *then*

$$\deg(cy_1 - tz_1) = \frac{A+C}{2}.$$

Proof. First, we conclude from

$$(cr - st)(cr + st) = c^2r^2 - s^2t^2 = c^2 - ac - bc - 1$$

that

$$\deg(cr - st) + C + \frac{A+B}{2} = 2C$$

and therefore the first part of the lemma follows. Now, observe

$$cx_0^2 = a(cr - st)^2 + c - a \Longrightarrow \deg x_0 = \frac{C-B}{2},$$
$$cy_1^2 = b(cr - st)^2 + c - b \Longrightarrow \deg y_1 = \frac{C-A}{2}.$$

Thus, we have

$$\deg sz_0 = \deg cx_0 = \frac{3C-B}{2}.$$

By using the equation

$$(cx_0 - sz_0)(cx_0 + sz_0) = c^2x_0^2 - s^2z_0^2 =$$
$$= ca(cr - st)^2 + c^2 - ac - s^2(cr - st)^2 = c^2 - ac - (cr - st)^2,$$

and by observing that $C > A$, we get

$$\deg(cx_0 - sz_0) = \frac{B+C}{2}.$$

The last part can be obtained analogously. □

Lemma 9. *Let* $e = 2rst - 2cr^2 + c$. *Then, we have*

(i) $\deg e = C - A - B < C$, *if* $C > A + 2B$,
(ii) $\deg e \leq B = C - A - B < C$, *if* $C = A + 2B$, *and*
(iii) $\deg e = B$, *if* $C < A + 2B$.

Proof. Let $U = e(st + cr)$. We have $U = 2acr + 2bcr + 2r + cst - c^2r$ and since $\deg(st - cr) = C - \frac{A+B}{2}$ by the previous lemma, $\deg U \leq 2C - \frac{A+B}{2}$ (observe that for $C = A + 2B$ the polynomials $2bcr$ and $cst - c^2r < 0$ have the same degree). Hence, $\deg e \leq C - A - B < C$.

For $C > A + 2B$ we get $\deg e = C - A - B$.

If we assume $C < A + 2B$, then the dominant summand in U is $2bcr$ and therefore $\deg U = B + C + \frac{A+B}{2}$, which in turn implies $\deg e = B$. □

Lemma 10. *Let $\{a, b, c\}$ with $a < b < c$ be a polynomial Diophantine triple and assume that $B < C = A + 2B$. Then*

$$\{a, b, d_-, c\} = \{a, b, a + b \pm 2r, 4r(r \pm a)(b \pm r)\}.$$

Moreover, in this case we have $e = \mp 2r$.

Proof. First, by using the equation

$$d_+ \cdot d_- = (c - a - b - 2r)(c - a - b + 2r),$$

which yields $\deg c = \deg(abd_-)$, we get $\deg d_- = B$. Since $B < C$ we have three possibilities, namely $0 < a < b < d_- < c, 0 < a < d_- < b < c$ or $0 < d_- < a < b < c$. Observe that $d_- \neq 0$, since $d_- = 0$ implies $c = a+b\pm 2r$ and thus $B = C$, a contradiction. Moreover, $d_- \neq a, b$, since this would lead to $a^2 + 1 = r^2$, $b^2 + 1 = s^2$ respectively, which is also a contradiction.

Now, since $A \leq B = \deg d_-$, we apply Lemma 3 to the triple $\{a, b, d_-\}$. We have that $e_+ = c$. But now, by the equation

$$e_+ \cdot e_- = c \cdot e_- = (d_- - a - b - 2r)(d_- - a - b + 2r),$$

we get, since $C = A + 2B \geq 2B$, that $\deg e_- \leq 0$. Assume that $e_- \neq 0$. By observing that $ae_- + 1, be_- + 1$ are squares, we conclude by comparing coefficients that $e_- = \psi^2\delta$. Moreover, we have $A = 0$ and therefore $a = \alpha^2\delta$, which yields a contradiction. Therefore we conclude $e_- = 0$ and thus that the triple $\{a, b, d_-\}$ is regular, i.e. $d_- = a + b \pm 2r$. Now, we use once more that c can be recalculated by a, b and d_-. We have (cf. Lemma 3)

$$c = a + b + d_- + 2(abd_- + ruv),$$

where $u^2 = ad_- + 1$ and $v^2 = bd_- + 1$. From above it follows that $u = r \pm a, v = b \pm r$ and

$$\begin{aligned} c &= a + b + a + b \pm 2r + 2ab(a + b \pm 2r) + 2ruv = \\ &= 2(a + b)r^2 \pm 2r(2ab + 1) + 2ruv = 2r(ar + ab \pm ab \pm r^2) + 2ruv = \\ &= 2r(r \pm a)(b \pm r) + 2ruv = 4ruv. \end{aligned}$$

It implies that

$$c = 4r(r \pm a)(b \pm r).$$

In this case we have

$$\begin{aligned} s &= 2r^2 \pm 2ar - 1, \\ t &= 2br \pm (2r^2 - 1). \end{aligned}$$

Now, let $e = 2rst - 2cr^2 + c$. Direct computation shows that $e = \mp 2r$. □

5. Proof of the Theorem

We conclude the proof of our theorem by showing our conjecture for all solutions, which come from intersections of the recurring sequences obtained with the initial values described in Lemma 7.

Case **1.1)** $v_{2m} = w_{2n}, z_0 = z_1, |z_0| = 1$.

Observe that we get by equation (3) and (4), $x_0^2 = y_0^2 = 1$ and as they are positive by Lemma 1 we conclude $x_0 = y_0 = 1$. Therefore, by Lemma 2

$$\deg v_m = C + (m-1)\frac{A+C}{2},$$
$$\deg w_n = C + (n-1)\frac{B+C}{2},$$

if $B < C$ or $z_0 = 1$ and

$$\deg v_m = C + (m-1)\frac{A+C}{2},$$
$$\deg w_n = \frac{A+B}{2} + (n-1)\frac{B+C}{2},$$

if $B = C$ and $z_0 = -1$. The only fact one has to be aware of is that by

$$(c-s)(c+s) = c^2 - s^2 = c^2 - ac - 1$$

we can conclude that $\deg(c-s) = C$ and analogously we get $\deg(c-t) = C$ if $A \leq B < C$, while $\deg(c-s) = B$ and $\deg(c-t) = \frac{A+B}{2}$ if $B = C$, since in this case we have $c = a + b + 2r$.

As in [5, formula (29)], we get from Lemma 6

$$\pm am^2 + sm \equiv \pm bn^2 + tn \pmod{4c}. \tag{14}$$

Assume that $m, n \neq 0$ (because $m = n = 0$ leads to the trivial solution $d = 0$).

a) Let $B < C$. Then (14) implies that $\pm am^2 + sm = \pm bn^2 + tn$. This further implies $\frac{A+C}{2} = \frac{B+C}{2}$ and $A = B$. But this means that $m = n$ (by comparing degrees in $v_{2m} = w_{2n}$), $\pm m(a-b) = t - s$ and by the equation

$$m^2(a-b)(t+s) = \pm m(t-s)(t+s) = \pm mc(b-a)$$

we get $\pm m(t+s) = c$. The comparison of the degrees gives $\frac{B+C}{2} = C$, a contradiction.

b) Let $A < B = C$. Then $c = a + b + 2r$, which yields $s = a + r$ and $t = b + r$. Therefore (14) implies

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

Since a and r have different degrees, both sides of this equation are equal to 0. This implies $(m, n) = (0, 0)$, which yields $d = 0$, or $(m, n) = (1, 1)$, which yields $d = 4r(a+r)(b+r) = a + b + c + 2abc + 2rst = d_+$ since $z_0 = -1, x_0 = 1$, thus $v_1 = c - s = b + r$ and finally

$$z = v_2 = w_2 = 2sv_1 - v_0 = 2(a+r)(b+r) + 1,$$

leading to the d as claimed above.

c) Let $A = B = C$. Then $m = n$ and $c = a + b + 2r$. Therefore (14) becomes

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

This implies (for $\pm m^2 + m \neq 0$, otherwise we would have $d = 0$ or $d = d_+$, namely for $m = 0$ or $m = 1$, respectively, with the same arguments as above) that there exist integers k, p, q $(k \neq 0)$ such that

$$pb - qa = 2kr.$$

We may assume that $p \neq 0$, since otherwise from $q^2a^2 = 4k^2(ab+1)$ we would obtain that a and b are constant polynomials, a contradiction. With $v = pq + 2k^2$, we obtain

$$p^2b^2 - 2vab + a^2q^2 = 4k^2. \tag{15}$$

We have $v^2 - p^2q^2 = (2k(m^2 \pm m))^2$. Since the discriminant of the quadratic polynomial $f(x) = p^2x^2 - 2vx + a^2$ is a perfect square, we can factorize the left hand side of (15). With $l = 2k(m^2 \pm m)$ we have

$$(p^2b - va - la)(p^2b - va + la) = 4k^2p^2. \tag{16}$$

We conclude that both factors on the left hand side of (16) are constant. Since $l \neq 0$, we obtain that a is constant. But then (16) implies that b is also a constant, and we obtained a contradiction as before.

This finishes the proof in the case **1.1)**.

In all other cases we may assume that $B < C$. Indeed, if $B = C$, then $c = a + b + 2r < 4b$ and it implies $cr - st = 1$. But the case $z_0 = z_1 = \pm 1$ was already handled in case **1.1)**. In all remaining cases we obtain a contradiction. If $z_0 = \pm t$, then $\deg t = \deg(b+r) = C > \deg z_0$, contradicting Lemma 1. If $z_1 = \pm s$, then from $z_1^2 = ac + 1$ and $\deg z_1 \leq \frac{C}{2}$ we conclude that $A = 0$. We also have $y_1 = r$. Consider now the relation

$$2(t-1)y_1^2 \leq b(c-b)$$

(see the proof of Lemma 1 from [4]). Since $\deg(2(t-1)r^2) = 2B$ and $\deg(b(c-b)) = \deg(b(a+2r)) = \frac{3B}{2}$, we obtain a contradiction again.

Now, we can consider the remaining cases.

Case **1.2)** $v_{2m} = w_{2n}, z_0 = z_1 = \pm(cr - st)$.

First let us assume that we have $A = B$. From Lemmas 2 and 8 we get that

$$\deg v_m = \left\{ \begin{array}{c} \frac{3C-B}{2} \\ \frac{B+C}{2} \end{array} \right\} + (m-1)\frac{A+C}{2},$$

$$\deg w_n = \left\{ \begin{array}{c} \frac{3C-A}{2} \\ \frac{A+C}{2} \end{array} \right\} + (n-1)\frac{B+C}{2},$$

where the first case in each of these formulae correspond to the first possible sign, i.e. to $z_0 = z_1 = cr - st$ and the second case to the minus sign, i.e. to $z_0 = z_1 = -(cr - st)$. We will carry on using this notation below.

Now comparing degrees, which means to consider $\deg v_n = \deg w_n$, implies $m = n$. Moreover, from Lemma 6 we get by observing that $x_0 = rs - at$ and $y_1 = rt - bs$ (cf. [7, p. 28]) that

$$\mp astm(m \pm 1) + rm \equiv \mp bstn(n \pm 1) + rn \pmod{c}$$

and by multiplying with $2st$ we obtain

$$\mp 2\left[am(m \pm 1) - bn(n \pm 1)\right] \equiv 2rst(n - m) \pmod{c}. \tag{17}$$

Since $m = n$ we conclude

$$\mp 2m(m \pm 1)(a - b) = 0,$$

which can only hold for $(m, n) = (0, 0)$, which leads to $d = d_- < c$, or $(m, n) = (1, 1)$. The last case leads to the only solutions which is allowed, namely $d = d_+ = a + b + c + 2abc + 2rst$, since $z = v_2 = w_2 = 2sv_1 - v_0 = cr + st$.

Thus, we may assume that $A < B < C$. From Lemmas 1 and 8 we conclude that $C \leq 2A + B$. Using the equation

$$d_+ \cdot d_- = (c - a - b - 2r)(c - a - b + 2r),$$

which yields $\deg c = \deg(abd_-)$, we therefore get $\deg d_- \leq A$.

Now we are intended to show that the leading coefficients of b and e are equal. We have

$$e = 2rst - 2cr^2 + c \quad \text{and} \quad d_- = a + b + c + 2abc - 2rst.$$

From this it follows

$$d_- = a + b + c + 2abc - (e + 2cr^2 - c) = a + b - e$$

and thus the conclusion follows since $\deg d_- \leq A < B = \deg e$.

Now from (17) we conclude

$$\mp 2[am(m \pm 1) - bn(n \pm 1)] = e(n - m)$$

and by comparing the leading coefficients we get

$$\pm 2n(n \pm 1) = n - m$$

or

$$m = n \mp 2n(n \pm 1) = \begin{cases} -n(2n + 1) \\ n(2n - 1) \end{cases}$$

Both cases can hold with $m = n = 0$, leading to $d = d_-$. The first case can only hold in this situation. From $\deg v_{2n} = \deg w_{2n}$ we conclude

$$m = n\frac{B + C}{A + C},$$

and therefore we get in the second case that

$$2n - 1 = \frac{B + C}{A + C} < \frac{2C}{C} = 2. \tag{18}$$

Therefore, we have $n < 2$ and the only remaining possibilities are $(m, n) = (0, 0)$ and $(m, n) = (1, 1)$, which lead to $d = d_-$ and $d = d_+$.

This finishes the proof in the case **1.2)**.

Case **2)** $v_{2m+1} = w_{2n}, z_0 = \pm t, z_1 = \pm(st - cr)$.

We apply Lemma 1 and Lemma 8 and conclude

$$\deg(\pm t) = \frac{B+C}{2} \leq \frac{3C-A}{4} \implies C \geq A + 2B,$$
$$\deg(\pm(st-cr)) = C - \frac{A+B}{2} \leq \frac{3C-B}{4} \implies C \leq 2A + B.$$

But $A + 2B \leq C \leq 2A + B$, implies that $A = B$ and $C = A + 2B = 3A$.

We get from (3) that $x_0 = r$. Therefore, for the degrees of v_m and w_n we have by Lemma 2 and Lemma 8:

$$\deg v_m = C \pm \frac{A+B}{2} + (m-1)\frac{A+C}{2},$$
$$\deg w_n = \left\{ \begin{array}{c} \frac{A+C}{2} \\ \frac{3C-A}{2} \end{array} \right\} + (n-1)\frac{B+C}{2}.$$

By comparing degrees in $v_m = w_n$ we get

$$4A + 2A(m-1) = 2A + 2A(n-1) \implies n = m+1, \text{ or}$$
$$2A + 2A(m-1) = 4A + 2A(n-1) \implies m = n+1.$$

Now we use Lemma 6 and get

$$sz_0 + c[2asz_0m(m+1) + x_0(2m+1)] \equiv z_1 + 2c(bz_1n^2 + ty_1n) \pmod{4c^2}.$$

Observe again that $y_1 = rt - bs > 0$ and that $x_0 = r$. By diving through c and multiplying with $2st$ we conclude

$$\mp[2am(m+1) - 2bn(n \mp 1)] \equiv 2rst(m - n + \delta) \pmod{4c}, \tag{19}$$

where $\delta = 1$ or 0. Applying Lemma 10, we see that $2rst \equiv e = \mp 2r \pmod{c}$. Observe that $A = B = \deg r$. Thus, we get

$$2am(m+1) - 2bn(n \mp 1) = 2r(m - n + \delta)$$

or

$$2m(m+1)(a-b) = 0 \quad \text{or}$$
$$2(n+1)(n+2)a - 2n(n+1)b = 2r.$$

The first case implies either $a = b$, a contradiction, or $m = 0$ leading to $d = 0$. In the second case we define the integers

$$p = 2(n+1)(n+2), \ q = 2n(n+1)$$

and receive the same contradiction as in the case **1.1)**.

This finishes the proof in the case **2)**.

Case **3)** $v_{2m} = w_{2n+1}, z_0 = \pm(cr - st), z_1 = \mp s$.

We start again by applying Lemma 1 and Lemma 8 and we conclude $2A + B \leq C \leq A + 2B$.

As above (compare also with equation (48) in [5]) we conclude from Lemma 6

$$\mp 2[am(m \pm 1) - bn(n+1)] = e(n - m + \delta), \tag{20}$$

where $\delta = 0$ or 1.

First, let us assume that $C = A + 2B$. Hence, by Lemma 10 we get $e = \mp 2r$. By comparing degrees in (20), we conclude that either $m = n = 0$, which leads to a contradiction, or $A = B$. We get from (4) that $y_1 = r$. Therefore, for the degrees of v_m and w_n we have by Lemma 2 and Lemma 8:

$$\deg v_m = \left\{ \begin{array}{c} \frac{3C-B}{2} \\ \frac{B+C}{2} \end{array} \right\} + (m-1)\frac{A+C}{2},$$

$$\deg w_n = C \mp \frac{A+B}{2} + (n-1)\frac{B+C}{2}.$$

By comparing the coefficients in $v_m = w_n$ we get similarly as before

$$n = m + 1, \text{ or } m = n + 1.$$

As in case **2)** we derive by inserting this relation in (20) that

$$0 > am(m+1) - b(m+1)(m+2) = r > 0,$$

which is a contradiction, or

$$2[a(n+1)n - bn(n+1)] = 0,$$

which implies $n = 0$ or $a = b$ and thus also a contradiction.

We are left with the case $C < A + 2B$. Since we have $C \geq 2A + B$, we conclude that $A < B$ must hold. Moreover, we derive from the equation

$$d_+ \cdot d_- = (c - a - b - 2r)(c - a - b + 2r)$$

that $\deg d_- < B$. Since by Lemma 9 we have $\deg e = B$ we get as in case **1.2)** that b and e have the same leading coefficients. By comparing the leading coefficients in (20) we get

$$\pm 2n(n+1) = n - m + \delta$$

or

$$m = n \mp 2n(n+1) + \delta = \left\{ \begin{array}{r} -n(2n+1) \\ (2n+1)(n+1) \end{array} \right.$$

As in case **1.2)** the first case is only possible for $(m, n) = (0, 0)$ leading to $d = d_-$. By comparing the degrees of v_{2m} and w_{2n+1} we get in the second case that $m(A + C) = n(B + C)$ and thus

$$2n + 1 = \frac{m}{n+1} < \frac{m}{n} = \frac{B+C}{A+C} < \frac{2C}{C} = 2,$$

a contradiction.

Therefore the proof in case **3)** is also finished.

Case **4)** $v_{2m+1} = w_{2n+1}, |z_0| = t, |z_1| = s$.

Our starting point is the following relation (compare with equation (38) in [5]), which is a consequence of Lemma 6:

$$\pm 2astm(m+1)+r(2m+1)\equiv \pm 2bstn(n+1)+r(2n+1) \pmod{4c}, \tag{21}$$

where we again have divided through c.

First, we again get from (3) and (4) that $x_0=y_1=r$. Therefore, for the degrees of v_m and w_n we have:

$$\deg v_m = C \pm \frac{A+B}{2} + (m-1)\frac{A+C}{2},$$
$$\deg w_n = C \pm \frac{A+B}{2} + (n-1)\frac{B+C}{2}.$$

From the comparison of degrees we have $(A+C)(m-1)=(B+C)(n-1)$. If $A=B$, then $m=n$ and (21) becomes $m(m+1)(a-b)\equiv 0 \pmod{2c}$, a contradiction. Thus $A<B$.

We compare the degree of $|z_0|=t$ with the estimate for $\deg z_0$ in Lemma 1. Therefore, we can conclude that $C\geq A+2B$.

As in [5], (21) can be rearranged in the following form

$$\pm 2[am(m+1)-bn(n+1)]\equiv 2rst(n-m) \pmod{2c}. \tag{22}$$

Let $e=2rst-2cr^2+c$. We have $2rst\equiv e \pmod{c}$ and $\deg e<C$ by Lemma 9. Thus (22) implies

$$\pm 2[am(m+1)-bn(n+1)]=e(n-m). \tag{23}$$

If $C>A+2B$, then $\deg e=C-A-B$ (by Lemma 9) and the comparison of degrees in (23) gives $C=A+2B$, a contradiction.

Hence, we have $C=A+2B$. But, by Lemma 10 we conclude that $e=\mp 2r$. Hence, $\deg e=\frac{A+B}{2}<B$, which is a contradiction to equation (23).

This finishes the proof in the case **4)**.

Altogether the statement of Theorem 1 follows. □

References

[1] J. Arkin, V. E. Hoggatt and E. G. Strauss, On Euler's solution of a problem of Diophantus, *Fibonacci Quart.* **17** (1979), 333-339.

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

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

[5] A. Dujella, There are only finitely many Diophantine quintuples, *J. Reine Angew. Math.*, to appear.

[6] A. Dujella and C. Fuchs, A polynomial variant of a problem of Diophantus and Euler, *Rocky Mount. J. Math.*, to appear.

[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 F. Luca, On a problem of Diophantus with polynomials, preprint.

[9] P. Gibbs, A generalised Stern-Brocot tree from regular Diophantine quadruples, preprint, math.NT/9903035.
[10] B. W. Jones, A variation of a problem of Davenport and Diophantus, *Quart. J. Math. Oxford* Ser.(2) **27** (1976), 349-353.
[11] B. W. Jones, A second variation of a problem of Davenport and Diophantus, *Fibonacci Quart.* **15** (1977), 323-330.

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

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