A POLYNOMIAL VARIANT OF A PROBLEM OF DIOPHANTUS AND EULER

ANDREJ DUJELLA AND CLEMENS FUCHS*

Abstract. In this paper, we prove that there does not exist a set of four polynomials with integer coefficients, which are not all constant, such that the product of any two of them is one greater than a square of a polynomial with integer coefficients.

1. Introduction

Let n be an integer. A set of m positive integers is called a Diophantine m-tuple with the property $D(n)$ or simply $D(n)$-m-tuple, if the product of any two of them increased by n is a perfect square. The first $D(1)$-quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat. The folklore conjecture is that there does not exist a $D(1)$-quintuple. In 1969, Baker and Davenport [1] proved that the Fermat's set cannot be extended to a $D(1)$-quintuple. Recently, the first author proved that there does not exist a $D(1)$-sextuple and there are only finitely many $D(1)$-quintuples (see [10]).

In the case $n = -1$, the conjecture is that there does not exist a $D(-1)$-quadruple (see [5]). It is known that some particular $D(-1)$-triples cannot be extended to $D(-1)$-quadruples (see [2], [6], [13], [14]). Let us mention that from [9, Theorem 4] it follows that there does not exist a $D(-1)$-33-tuple.

This $n = -1$ case is closely connected with an old problem of Diophantus and Euler. Namely, Diophantus studied the problem of finding numbers such that the product of any two increased by the sum of these two gives a square. He found two triples $\{4, 9, 28\}$ and $\{\frac{3}{10}, \frac{21}{5}, \frac{7}{10}\}$ satisfying this property. Euler found a quadruple $\{\frac{5}{2}, \frac{9}{56}, \frac{9}{224}, \frac{65}{224}\}$ (see [4], [3]). In [8] an infinite family of rational quintuples with the same property was given. Since

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

we see that the problem of finding integer m-tuples with the same property is equivalent to finding $D(-1)$-m-tuples.

*This work was supported by the Austrian Science Foundation FWF, grant S8307-MAT.

A polynomial variant of the above problems was first studied by Jones [11], [12], and it was for the case $n = 1$.

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

A natural question is how large such sets can be. Let us define

$$P_n = \sup\{|S| : S \text{ is a polynomial } D(n)\text{-tuple}\}.$$

¿From [9, Theorem 1] it follows that $P_n \leq 22$ for all $n \in \mathbb{Z}$. The above mentioned result about the existence of only finitely many $D(1)$-quintuples implies that $P_1 = 4$.

In the present paper, we will prove that $P_{-1} = 3$. First of all, $P_{-1} \geq 3$. More precisely, if $a \cdot b - 1 = r^2$, then

$$\{a, b, a + b + 2r\}$$

is a polynomial $D(-1)$-triple. E.g.

$$\{x^2 + 1, x^2 + 2x + 2, 4x^2 + 4x + 5\}$$

is a polynomial $D(-1)$-triple (see [2]). Therefore, we have to prove that $P_{-1} < 4$, and this is the statement of our main theorem.

Theorem 1. *There does not exist a polynomial $D(-1)$-quadruple.*

The proof of Theorem 1 is divided into several parts. In Section 2, we transform our problem into a system of polynomial Pellian equations, which leads to finding intersections of some binary recursive sequences. We obtain some useful information about initial terms of these sequences.

In Section 3, we show that there is no loss of generality in assuming that one element of our initial triple is equal to 1. This, together with results from Section 2, allow us to completely determine initial terms of corresponding sequences.

In Section 4, we prove Theorem 1 by showing that our sequences cannot have nontrivial common terms. This is done by comparing degrees and leading coefficients of corresponding polynomials.

2. Two sequences of polynomials

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 polynomial $D(-1)$-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 $D(-1)$-quadruple there is at most one constant polynomial. It is also clear that all leading coefficients of the polynomials in a polynomial $D(-1)$-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 $\mathbb{Z}^+[x]$.

Let $\{a,b,c\}$, where $0<a<b<c$, be a polynomial $D(-1)$-triple and let $r,s,t\in\mathbb{Z}^+[x]$ be defined by

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

In this paper, the symbols r,s,t will always have this meaning. Assume that $d\in\mathbb{Z}^+[x], d>c$, is a polynomial such that $\{a,b,c,d\}$ is a polynomial $D(-1)$-quadruple. We have

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

with $u,y,z\in\mathbb{Z}^+[x]$. Eliminating d from (1) we obtain the following system of polynomial Pellian equations

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

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

We will describe the sets of solutions of equations (2) and (3). We will follow the arguments in the classical case of Pellian equations in integers (cf. [7]).

Lemma 1. *If (z,u) and (z,y), with $u,y,z\in\mathbb{Z}^+[x]$, are polynomial solutions of (2) and (3) respectively, then there exist $z_0,u_0\in\mathbb{Z}[x]$ and $z_1,y_1\in\mathbb{Z}[x]$ with*

(i) *(z_0,u_0) and (z_1,y_1) are solutions of (2) and (3) respectively,*
(ii) *the following inequalities are satisfied:*

$$0\le|u_0|<s, \tag{4}$$

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

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

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

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

$$z\sqrt{a}+u\sqrt{c}=(z_0\sqrt{a}+u_0\sqrt{c})(s+\sqrt{ac})^{2m}, \tag{8}$$

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

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

Proof. It is clear that it suffices to prove the statement of the lemma for equation (2). First observe that

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

and by multiplying with the conjugate $(s-\sqrt{ac})^{2m}$ we see that

$$(s+\sqrt{ac})^{2m}(s-\sqrt{ac})^{2m} = (s^2-ac)^{2m} = (-1)^{2m} = 1. \tag{10}$$

Let now (z,u) be a solution of (2) in polynomials from $\mathbb{Z}^+[x]$. Consider all pairs (z^*,u^*) of polynomials of the form

$$z^*\sqrt{a}+u^*\sqrt{c} = (z\sqrt{a}+u\sqrt{c})(s+\sqrt{ac})^{2m},\ m\in\mathbb{Z}.$$

By (10) it is clear that (z^*,u^*) satisfies (2).

We would like to show that $z^*>0$. We write $(s+\sqrt{ac})^{2m} = A+B\sqrt{ac}$, where $A,B\in\mathbb{Z}[x]$ satisfying $A^2-acB^2=1$. Therefore we have

$$z^*\sqrt{a}+u^*\sqrt{c} = (z\sqrt{a}+u\sqrt{c})(A+B\sqrt{ac}) = (Az+cuB)\sqrt{a}+(Au+azB)\sqrt{c},$$

and this yields

$$z^* = Az+cuB.$$

Now, if $m\geq 0$ then we have $A,B>0$ and thus $z^*>0$. On the other hand, if $m<0$ we have $A>0, B<0$. If we assume that $z^*\leq 0$, we have $Az\leq -Bcu$ and both sides are >0. Squaring yields $A^2z^2\leq B^2c^2z^2$. Using the fact that $A^2-acB^2=1$ we obtain $z^2B^2ac+z^2\leq B^2c^2u^2$ and therefore

$$z^2\leq cB^2(cu^2-az^2) = cB^2(a-c)<0,$$

a contradiction.

Among all pairs (z^*,u^*), we can now choose a pair with the property that z^* is minimal, and we denote that pair by (z_0,u_0). Define polynomials z' and u' by

$$z'\sqrt{a}+u'\sqrt{c} = (z_0\sqrt{a}+u_0\sqrt{c})(2ac-1-2s\varepsilon\sqrt{ac}),$$

where $\varepsilon=1$ if $u_0>0$, and $\varepsilon=-1$ if $u_0<0$. From the minimality of z_0 we conclude that $z'=z_0(2ac-1)-2csu_0\varepsilon\geq z_0$ and this leads to $cs|u_0|\leq z_0(ac-1)$ and further to $c|u_0|\leq sz_0$. Squaring this inequality we obtain

$$acz_0^2-c(c-a) = c^2u_0^2\leq acz_0^2-z_0^2$$

and finally

$$z_0^2\leq c(c-a)<c^2,$$

which implies (5). Now we have

$$cu_0^2 = az_0^2-c+a\leq ac^2-a^2c-c+a<ac^2-c=cs^2 \tag{11}$$

and therefore we obtain also (4). Hence, we have proved that there exists a solution (z_0,u_0) of (2), which satisfies (4) and (5), and an integer $m\in\mathbb{Z}$ such that

$$z\sqrt{a}+u\sqrt{c} = (z_0\sqrt{a}+u_0\sqrt{c})(s+\sqrt{ac})^{2m}.$$

It remains to show that $m \geq 0$. Suppose that $m < 0$. Then, as above, we have $(s+\sqrt{ac})^{2m} = A - B\sqrt{ac}$, with $A, B \in \mathbb{Z}^+[x]$ satisfying $A^2 - acB^2 = 1$. We have $u = Au_0 - z_0 Ba$ and from the condition $u > 0$ we obtain $Au_0 > z_0 Ba$ and by squaring $u_0^2 > B^2 a(c-a) \geq ac - a^2$, which by (11) implies

$$ac^2 - a^2c \leq cu_0^2 \leq ac^2 - a^2c - c + a.$$

This implies $-c + a \geq 0$, which is clearly a contradiction. $\square$

The solutions z arising, for given (z_0, u_0), from formula (8) for varying $m \geq 0$ form a binary recurrent sequence $(v_m)_{m\geq 0}$ whose initial terms are found by solving equation (8) for z when $m = 0$ and 1, and whose characteristic equation has the roots $(s+\sqrt{ab})^2$ and $(s-\sqrt{ab})^2$. Therefore, we conclude that $z = v_m$ for some (z_0, u_0) with the above properties and integer $m \geq 0$, where

$$v_0 = z_0,\ v_1 = (2ac-1)z_0 + 2scu_0,\ v_{m+2} = (4ac-2)v_{m+1} - v_m. \tag{12}$$

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

$$w_0 = z_1,\ w_1 = (2bc-1)z_1 + 2tcy_1,\ w_{m+2} = (4bc-2)w_{n+1} - w_n. \tag{13}$$

Now the following congruence relations follow easily from (12) and (13) by induction.

Lemma 2. *Let the sequences (v_m) and (w_n) be given by (12) and (13). Then we have*

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

Proof. It suffices to prove the statement of the lemma for v_m. By looking on (12) we have

$$v_0 = z_0,\ v_1 \equiv -z_0 \pmod{2c}.$$

Proceeding the induction step, we see using (12)

$$v_{m+2} \equiv -2(-1)^{m+1}z_0 - (-1)^m z_0 = (-1)^{m+2} z_0 \pmod{2c},$$

as stated. $\square$

Now we can prove the following lemma, which says that a solution of $v_m = w_n$ implies also a solution at the beginning of the sequences.

Lemma 3. *If the equation $v_m = w_n$ has a solution, then $z_0 = z_1$.*

Proof. Assume that $v_m = w_n$ has a solution. By Lemma 2 we conclude

$$z_0 \equiv \pm z_1 \pmod{2c}.$$

If we assume that $z_0 \equiv z_1 \pmod{2c}$, then we can conclude by using (4) and (7) from Lemma 1, namely

$$0 < z_0 < c, \quad 0 < z_1 < c,$$

that $z_0 = z_1$ holds. If we assume that $z_0 \equiv -z_1 \pmod{2c}$, we have $2c | z_0 + z_1$, which contradicts the fact that $z_0 + z_1 < 2c$. This finishes the proof. □

3. Reduction to the case $a = 1$

In this section, we show that it suffices to prove that polynomial $D(-1)$-triples $\{a, b, c\}$, where $a = 1$, cannot be extended to a polynomial $D(-1)$-quadruple.

Lemma 4. *Let $\{a, b, c, d\}$ with $0 < a < b < c < d$ be a polynomial $D(-1)$-quadruple. Then there exists $d_0 \in \mathbb{Z}^+[x]$ with $d_0 < c$ such that $ad_0 - 1$, $bd_0 - 1$, $cd_0 - 1$ are perfect squares.*

Proof. We are interested in sequences (v_m) (and (w_n)) such that $z^2 = v_m^2 = w_n^2 = cd - 1$, where $d \in \mathbb{Z}^+[x]$. This implies that $v_m^2 \equiv -1 \pmod{c}$. By Lemma 2 this means

$$z_0^2 \equiv -1 \pmod{c}.$$

In this case we define

$$d_0 = \frac{z_0^2 + 1}{c} \in \mathbb{Z}^+[x].$$

For this d_0 we have

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

By Lemma 3 we find

$$bd_0 - 1 = b\frac{z_1^2 + 1}{c} - 1 = \frac{cy_1^2 + c - b + b}{c} - 1 = y_1^2$$

and finally also

$$ad_0 - 1 = a\frac{z_0^2 + 1}{c} - 1 = \frac{1}{c}(az_0^2 + a - c) = \frac{1}{c}cu_0^2 = u_0^2$$

holds. Furthermore, we have

$$cd_0 = z_0^2 + 1 < c^2,$$

which implies

$$d_0 < c.$$

□

Assume now that $\{a, b, c, d\}$ is a polynomial $D(-1)$-quadruple with minimal d. We may use Lemma 4 to construct d_0. From the minimality of d, it follows that $\{a, b, c, d_0\}$ is not a polynomial $D(-1)$-quadruple and this means that $d_0 \in \{a, b\}$. But this implies that $d_0^2 - 1$ is a perfect square, which can only hold in the case when $d_0 = 1$. Since $b > a \geq 1$, we conclude that $a = 1$.

Remark 1. It follows that it suffices to consider polynomial $D(-1)$-quadruples, which contain the constant polynomial 1.

Now let $\{1, b, c\}$ with $1 < b < c$ be a polynomial $D(-1)$-triple. By the previous discussion, we have $d_0 = 1$. This implies that $z_0^2 + 1 = c$ and therefore we have $z_0 = \pm s$. Because of the fact that $z_0 > 0$ we have $z_0 = s$. In the same way, we can conclude that $z_1 = s$. Now we have

$$cu_0^2 = z_0^2 - c + 1 = c - 1 - c + 1 = 0$$

and this yields $u_0 = 0$. Finally we get

$$cy_1^2 = bz_1^2 - c + b = b(c-1) - c + b = bc - c = cr^2$$

and therefore $y_1 = \pm r$. To sum up, it suffices to consider the following three sequences

$$v_0 = s,\ v_1 = (2c-1)s,\ v_{m+2} = (4c-2)v_{m+1} - v_m, \tag{14}$$

and

$$w_0 = s,\ w_1 = (2bc-1)s + 2tcr,\ w_{n+2} = (4bc-2)w_{n+1} - w_n, \tag{15}$$

$$w'_0 = s,\ w'_1 = (2bc-1)s - 2tcr,\ w'_{n+2} = (4bc-2)w'_{n+1} - w'_n. \tag{16}$$

4. Proof of Theorem 1

Let $\{1, b, c\}$ be a polynomial $D(-1)$-triple. Let us repeat the defining equations:

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

In what follows, we need the leading coefficients of b and c. We know that b and c are non-constant, and thus their leading coefficients are perfect squares. Let us give them names:

$$\mathrm{lc}(b) = \beta^2,\ \mathrm{lc}(c) = \gamma^2,$$

where β and γ are positive integers. Let v_m and w_n, w'_n be the remaining sequences from the last section. To finish the proof, we have to show that no nontrivial solution is obtained from these sequences. The trivial solution is always $v_0 = w_0 = s$, which leads to $d = 1$, which does not yield the extension of our triple $\{1, b, c\}$. We divide the proof in three cases. The first one is handled by the following lemma.

Lemma 5. *The equation $v_m = w_n$ has no nontrivial solution.*

Proof. First let us mention that $\deg v_m < \deg v_{m+1}$, $m = 0, 1, 2, \ldots$. To be precise we have

$$\deg v_m = \frac{1}{2}\deg c + m \deg c, \quad m \geq 0. \tag{17}$$

This follows at once by induction using the recurring formula (14). The same is also true for the second sequence w_n with

$$\deg w_n = \frac{1}{2}\deg c + n\left(\deg b + \deg c\right), \quad n \geq 0. \tag{18}$$

Again, by induction, we can now read off the leading coefficient of v_m, which is

$$2^{2m-1}\gamma^{2m+1}, \quad m \geq 1.$$

We have $\mathrm{lc}(v_0) = \gamma$, $\mathrm{lc}(v_1) = 2\gamma^3$ and using the recursive formula (14) we get

$$\mathrm{lc}(v_{m+1}) = 4\gamma^2 \mathrm{lc}(v_m) = 4\gamma^2 2^{2m-1}\gamma^{2m+1} = 2^{2(m+1)-1}\gamma^{2(m+1)+1}.$$

In the same way, we find the leading coefficient of w_n, which is

$$2^{2n}\beta^{2n}\gamma^{2n+1}.$$

First we have $\mathrm{lc}(w_0) = \gamma$, $\mathrm{lc}(w_1) = 2\beta^2\gamma^2\gamma + 2\beta\gamma\gamma^2\beta = 4\beta^2\gamma^3$. By using the recursive formula for w_n, one finds

$$\mathrm{lc}(w_{n+1}) = 4\beta^2\gamma^2 \mathrm{lc}(w_n) = 2^{2n+2}\beta^{2n+2}\gamma^{2n+3}.$$

If the equation $v_m = w_n$ has a solution, we must have equal leading coefficients, which means

$$2^{2m-1}\gamma^{2m+1} = 2^{2n}\beta^{2n}\gamma^{2n+1}.$$

This implies

$$\left(\frac{2^{m-n}\gamma^{m-n}}{\beta^n}\right)^2 = 2,$$

which yields

$$\sqrt{2} = \frac{2^{m-n}\gamma^{m-n}}{\beta^n} \in \mathbb{Q},$$

a contradiction. Thus $v_m = w_n$ cannot hold and the proof is finished. $\square$

To handle the equation $v_m = w'_n$, we have to distinguish whether $\deg b < \deg c$ or $\deg b = \deg c$ holds.

Lemma 6. *Assume that* $\deg b < \deg c$. *Then the equation* $v_m = w'_n$ *has no nontrivial solution.*

Proof. First we calculate

$$\begin{aligned} w'_1 w_1 &= (2bc-1)^2 s^2 - 4t^2c^2r^2 = \\ &= -4b^2c^2 + 4bc + c - 1 + 4bc^3 - 4c^2. \end{aligned}$$

Because of our assumption $\deg b < \deg c$, we obtain that the dominating summand is $4bc^3$. Therefore we get

$$\mathrm{lc}(w'_1 w_1) = 4\beta^2\gamma^6$$

and

$$\deg w'_1 w_1 = 3\deg c + \deg b.$$

On the other hand, we already know that

$$\mathrm{lc}(w_1) = 4\beta^2\gamma^3$$

and

$$\deg w_1 = \deg b + \frac{3}{2}\deg c.$$

Hence, we can conclude that

$$\mathrm{lc}(w_1') = \gamma^3 \quad \text{and} \quad \deg w_1' = \frac{3}{2}\deg c.$$

Now by induction and by the recursion (16) we get that $\deg w_n' < \deg w_{n+1}'$ and that the leading coefficient of w_n' is given by

$$2^{2n-2}\beta^{2n-2}\gamma^{2n+1}, \quad n \geq 1.$$

Namely we have $\mathrm{lc}(w_0') = \gamma, \mathrm{lc}(w_1') = \gamma^3$ and using (16) we obtain

$$\mathrm{lc}(w_{n+1}') = 4\beta^2\gamma^2\mathrm{lc}(w_n') = 2^{2n}\beta^{2n}\gamma^{2n+3}.$$

Again, if $v_m = w_n'$ has a solution, we can conclude by comparing the leading coefficients that

$$2^{2m-1}\gamma^{2m+1} = 2^{2n-2}\beta^{2n-2}\gamma^{2n+1}.$$

As before we get

$$\sqrt{2} = 2^{n-m}\gamma^{n-m}\beta^{n-1} \in \mathbb{Q},$$

which is a contradiction. This yields that in this case no solution can exist. □

Before we can prove the remaining part, we need the following useful gap principle for the elements of a polynomial $D(-1)$-m-tuple. The principle is a direct modification from the integer case (see [9, Lemma 3]). The analogous statement for polynomial $D(1)$-triples was proved by Jones in [12].

Lemma 7. *Let $\{a, b, c\}$ be a polynomial $D(-1)$-triple. Then there exist polynomials $e, u, y, z \in \mathbb{Z}[x]$ such that*

$$ae + 1 = u^2, \; be + 1 = y^2, \; ce + 1 = z^2$$

and

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

Proof. Define

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

Then

$$\begin{aligned}(ae + 1) - (at - rs)^2 &= -a(a + b + c) + 2a^2bc - 2arst + 1 - \\ &\quad -a^2(bc - 1) + 2arst - (ab - 1)(ac - 1) = 0.\end{aligned}$$

Hence, we may take $u = at - rs$, and analogously $y = bs - rt, z = cr - st$. We have

$$\begin{aligned}abe + ruy &= -ab(a + b + c) + 2a^2b^2c - 2abrst + abrst - \\ &\quad -a(ab - 1)(bc - 1) - b(ab - 1)(ac - 1) + rst(ab - 1) = \\ &= abc - (a + b) - rst,\end{aligned}$$

and finally

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

□

Using this lemma we can finish our proof.

Lemma 8. *Assume that* $\deg b = \deg c$. *Then the equation* $v_m = w'_n$ *has no nontrivial solution.*

Proof. First we conclude by Lemma 7 that there exist polynomials e, f, g, h such that

$$e + 1 = f^2, \ be + 1 = g^2, \ ce + 1 = h^2 \tag{19}$$

and

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

By looking at the proof of Lemma 7, we see that we have

$$e = -1 - b - c + 2bc - 2rst.$$

We want to show that $e = 0$. Let us assume $e \neq 0$ and define

$$\bar{e} = -1 - b - c + 2bc + 2rst.$$

Then

$$\deg \bar{e} = \deg b + \deg c = 2 \deg c = \deg c^2. \tag{20}$$

Let us calculate

$$\begin{aligned} e\bar{e} &= (2bc - 1 - b - c)^2 - 4r^2s^2t^2 = \\ &= (2bc - 1 - b - c)^2 - 4(b-1)(c-1)(bc-1) = \\ &= 1 + b^2 + c^2 - 2b - 2bc - 2c + 4. \end{aligned}$$

This yields

$$\deg e + \deg \bar{e} = \deg e\bar{e} \leq \deg c^2.$$

Using (20), we can conclude

$$\deg e \leq 0.$$

But looking at (19) we see that

$$e + 1 = \varphi^2 \quad \text{and} \quad e = \psi^2$$

must hold with $\varphi, \psi \in \mathbb{Z}$. This is only possible if $e = 0$.

This implies now that $f = 1, g = 1$ and $c = 1 + b + 2r$. Next let us express all polynomials in terms of the polynomial r. We have

$$b = r^2 + 1,$$

and therefore

$$c = r^2 + 2r + 2.$$

Next we calculate $s^2 = c - 1 = b + 2r = r^2 + 2r + 1 = (r+1)^2$, thus

$$s = r + 1.$$

In the same way, we get via $t^2 = bc - 1 = (r^2 + 1)(r^2 + 2r + 2) - 1 = r^4 + 2r^3 + 3r^2 + 2r + 1 = (r^2 + r + 1)^2$, that

$$t = r^2 + r + 1.$$

This gives us

$$\begin{aligned} w_1' &= (2bc-1)s-2tcr = \\ &= (2r^4+4r^3+6r^2+4r+3)(r+1)-2(r^3+r^2+r)(r^2+2r+2) = \\ &= 2r^2+3r+3. \end{aligned}$$

¿From this we conclude that

$$\deg w_1' = \deg c$$

and by induction, using the recurring formula (16), we get

$$\deg w_n' = \deg c + 2(n-1)\deg c, \quad n \geq 1.$$

Let us assume that $v_m = w_n'$ has a solution. Then by comparing the degree of v_m, which is given by (17), and the degree of w_n', we get

$$\frac{1}{2}\deg c + m \deg c = \deg c + 2(n-1)\deg c$$

and

$$\frac{1}{2} + m = 2n - 1,$$

a contradiction. Therefore $v_m = w_n'$ cannot have a solution and the proof is finished. □

Now Theorem 1 follows directly from Lemma 5, Lemma 6 and Lemma 8.

References

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

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

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

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

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

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

[7] A. Dujella, An absolute bound for the size of Diophantine m-tuples, *J. Number Theory*, to appear.

[8] A. Dujella, An extension of an old problem of Diophantus and Euler II, *Fibonacci Quart.*, to appear.

[9] A. Dujella, On the size of Diophantine m-tuples, *Math. Proc. Cambridge Philos. Soc.*, to appear.

[10] A. Dujella, There are only finitely many Diophantine quintuples, preprint.

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

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

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

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

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