A POLYNOMIAL VARIANT OF A PROBLEM OF DIOPHANTUS FOR PURE POWERS

ANDREJ DUJELLA*, CLEMENS FUCHS‡ AND FLORIAN LUCA

ABSTRACT. In this paper, we prove that there does not exist a set of 11 polynomials with coefficients in a field of characteristic 0 with the property that the product of any two distinct elements plus 1 is a perfect square. Moreover, we prove that there does not exist a set of 5 polynomials with the property that the product of any two distinct elements plus 1 is a perfect kth power with $k \geq 7$. Combining these results, we get an absolute upper bound for the size of a set with the property that the product of any two elements plus 1 is a pure power.

2000 *Mathematics Subject Classification:* 11D99, 11C08, 05D10.
Keywords: diophantine m-tuples, Mason's inequality, function fields, Ramsey theory.

1. INTRODUCTION

Diophantus of Alexandria [6] was interested in finding sets with the property that the product of any two of its distinct elements increased by one is a perfect square. Such a set consisting of m elements is therefore called a Diophantine m-tuple. He gave the example $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$. The first Diophantine quadruple consisting of positive integers was found by Fermat and it was the set $\{1, 3, 8, 120\}$. The folklore conjecture is that there does not exist a quintuple consisting of positive integers and having the property of Diophantus. In 1969, Baker and Davenport [1] proved that the Fermat's set cannot be extended to a Diophantine quintuple in $\mathbb{Z}$. Recently, the first author proved that there does not exist a Diophantine sextuple, and there are only finitely many Diophantine quintuples over the integers (see [8]).

Many generalizations of this problem were considered since then, for example by adding a fixed integer n instead of 1 (which was first considered

*The first author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 0037110.
‡The second author was supported by the Austrian Science Foundation FWF, grant NFN S9611.
This paper was partly written during a visit of the second author at the Department of Mathematics of the University of Zagreb within a joint Austrian-Croatian project granted by the Croatian Ministry of Science, Education and Sport and the Austrian Exchange Service (No. 23/2006).

in [2], cf. also [7, 9] for bounds for general n and [14] for a recent absolute upper bound for the size of such a set for n prime), kth powers instead of squares (see [3]), or considering the problem over other domains than $\mathbb{Z}$ or $\mathbb{Q}$. So we define:

Definition 1. *Let $m \geq 2, k \geq 2$ and R be a commutative ring with 1. A* kth power Diophantine m-tuple in R *is a set $\{a_1, \ldots, a_m\}$ consisting of m different nonzero elements from R such that $a_i a_j + 1$ is a kth power of an element of R for $1 \leq i < j \leq m$. Moreover, a set $\{a_1, \ldots, a_m\}$ of m different nonzero elements from R is called a* pure power Diophantine m-tuple *if $a_i a_j + 1$ is a kth power of an element of R for some $k \geq 2$ and all $1 \leq i < j \leq m$.*

We have already seen that for $k = 2$ and $R = \mathbb{Z}$ we have $m \leq 5$. For larger values of k and $R = \mathbb{Z}$, Bugeaud and Dujella [3] proved that

$$\begin{aligned} &m \leq 7 \quad \text{for} \quad k = 3, \\ &m \leq 5 \quad \text{for} \quad k = 4, \\ &m \leq 4 \quad \text{for} \quad 5 \leq k \leq 176, \\ &m \leq 3 \quad \text{for} \quad k \geq 177. \end{aligned}$$

Recently, Luca [21] proved that if $\{a_1, \ldots, a_m\} \subseteq \{1, \ldots, N\}$ is a pure power Diophantine m-tuple in $\mathbb{Z}$, then

$$m \leq c \left(\frac{\log N}{\log \log N} \right)^{\frac{3}{2}}$$

for all sufficiently large values of N and an effectively computable constant c. This improves earlier results by several authors (cf. [17, 18, 4]). Moreover, he proved that under the ABC-conjecture the size of a pure power Diophantine m-tuple in $\mathbb{Z}$ is bounded by an absolute constant (see [21, Theorem 1.4, p. 14]). This improves a result from [5].

Besides the cases $R = \mathbb{Q}$ and $R = \mathbb{Z}$, also polynomial variants of the above problem have been considered. The first such variant was studied by Jones [19], [20], and it was for the case $R = \mathbb{Z}[X]$ and $k = 2$. Other results for this case can be found in [11], where the authors proved that for every Diophantine quadruple $\{a, b, c, d\}$ in $\mathbb{Z}[X]$, where not all the polynomials are constant, we have $(a+b-c-d)^2 = 4(ab+1)(cd+1)$. This implies that every Diophantine triple in $\mathbb{Z}[X]$ can be extended to a Diophantine quadruple in an essentially unique way.

In [10], Dujella and Fuchs proved that there does not exist a set of four polynomials in $\mathbb{Z}[X]$ with the property that the product of any two is one greater than a perfect square in $\mathbb{Z}[X]$. Dujella and Fuchs jointly with Tichy [12] and Walsh [13] considered generalizations of the problem to sets where the product of any two plus a linear polynomial $n = aX + b$ is a perfect square. In this case, they proved best possible upper bounds for sets where

all polynomials have the same degree. Moreover, they showed that there does not exist a set with more than 12 polynomials in $\mathbb{Z}[X]$ with the property that the product of any two plus a linear polynomial is a perfect square.

Dujella and Luca considered the case $k \geq 3$ and $R = \mathbb{K}[X]$, where $\mathbb{K}$ is an algebraically closed field of characteristic zero. Let us mention that in this case we have to assume that not all the polynomials in a kth power Diophantine m-tuple $\{a_1, \ldots, a_m\}$ are constant since any m-tuple of constant polynomials is a kth Diophantine m-tuple for any $k \geq 2$. We will also assume this for the rest of the paper.

From this assumption, it follows that at most one of the polynomials a_i for $i = 1, \ldots, m$ is constant (this is Lemma 1 in [15]). We mention that the same conclusion is true (with very little modification of the proof) for pure power Diophantine m-tuples in $\mathbb{K}[X]$.

Now the main result from [15] was: if $\{a_1, \ldots, a_m\}$ is a kth power Diophantine m-tuple in $\mathbb{K}[X]$, then

$$\begin{aligned} m &\leq 5 \quad \text{for} \quad k = 3, \\ m &\leq 4 \quad \text{for} \quad k = 4, \\ m &\leq 3 \quad \text{for} \quad k \geq 5, \\ m &\leq 2 \quad \text{for} \quad k \geq 5 \text{ and } k \text{ even}. \end{aligned}$$

Observe that the result for $k = 2$ is missing. The first aim of this paper is to close that gap by proving an upper bound for the size of a 2nd power Diophantine m-tuple in $\mathbb{K}[X]$. We have the following theorem:

Theorem 1. *There does not exist a 2nd power Diophantine 11-tuple in $\mathbb{K}[X]$, i.e.*

$$m \leq 10 \quad \textit{for} \quad k = 2.$$

We remind the reader that in the case $\mathbb{K} = \mathbb{Z}$, we already know that there does not exist a Diophantine 5-tuple (which is a consequence of the main result from [8]).

This result is derived by considering a gap principle together with an upper bound for the degrees of the elements of such a Diophantine m-tuple, which is obtained by reducing the problem to a system of Pellian equations and by studying the solutions to these Pellian equations which lie in finitely many binary linear recursive sequences. Here, we will use auxiliary results which are contained in the paper by Dujella and Luca [15].

As a second result, we prove an analogue of the conditional result for pure power Diophantine m-tuples which was obtained by Luca in [21] and which was mentioned above. We prove:

Theorem 2. *There does not exist a pure power Diophantine quintuple where all perfect powers which appear are ≥ 7. In more details: there does not exist a set of five polynomials in $\mathbb{K}[X]$, not all of them constant, with the property*

that the product of any two distinct elements plus 1 *is a perfect* k*th power with* $k \geq 7$*.*

As a consequence, we get the following result, which can be obtained as a combination of the previous results for fixed exponent and Ramsey theory [16] (this is the reason why the upper bound explodes compared to the results above). We mention that this strategy was first introduced in this context by Gyarmati, Sárközy and Stewart [18] and was later also used in [4, 5, 21].

Theorem 3. *If* $\{a_1, \ldots, a_m\}$ *is a pure power Diophantine* m*-tuple in* $\mathbb{K}[X]$*, then* $m \leq 2 \cdot 10^9$*.*

In fact, one can choose the Ramsey number $R(11, 6, 4, 5; 2)$ as an upper bound (for a definition of Ramsey numbers we refer to Section 3). The parameters in this Ramsey number come from the cases of $k = 2, 3, 5$ and from Theorem 2. So, improving the above results on kth power Diophantine m-tuples will also reduce this bound. This is the case e.g. for pure power Diophantine m-tuples in $\mathbb{Z}[X]$, as mentioned above, where we get $m \leq R(5, 6, 4, 5; 2) \leq 7362115 \leq 8 \cdot 10^5$. By slightly changing the arguments in the proof of Theorem 2, it is possible to prove that there does not exist a pure power Diophantine quadruple in $\mathbb{K}[X]$ with all powers ≥ 8, but this would lead to $m \leq R(11, 6, 4, 4, 4; 2) \leq 6 \cdot 10^{10}$.

The proofs of the last two theorems essentially run along the same line as the proof given by Luca in [21] (for the proof of Theorem 2 compare also with Lemma 2 and 3 in [15]). It is well known that the polynomial variant of the ABC-conjecture is solved, namely it appears as special case of the fundamental inequality obtained first by Mason (see [22] and also [24]), which is the function field analog of Baker's method for linear forms in logarithms of algebraic numbers.

In Section 2, we will consider the case of $k = 2$ and $R = \mathbb{K}[X]$. There we will give a proof of Theorem 1. In Section 3, we turn to the case of pure power Diophantine m-tuples and give proofs of Theorems 2 and 3.

2. Proof of Theorem 1

We start by proving a gap principle, which is well known in the classical case and which was also used in the results for $\mathbb{Z}[X]$.

We will say polynomial Diophantine m-tuple instead of 2nd power Diophantine m-tuple in $\mathbb{K}[X]$ for brevity.

Lemma 1. *Let* $\{a, b, c\}$ *be a polynomial Diophantine triple and* $ab + 1 = r^2$*. Let* α*,* β*,* γ *be degrees of* a, b, c*, respectively, and assume that* $\alpha \leq \beta \leq \gamma$*. Then* $c = a + b \pm 2r$ *or* $\gamma \geq \alpha + \beta$*.*

Proof. Let $ac+1=s^2$ and $bc+1=t^2$. Consider the polynomials

$$\begin{aligned} d_1 &= a+b+c+2abc+2rst, \\ d_2 &= a+b+c+2abc-2rst. \end{aligned}$$

We have

$$d_1 \cdot d_2 = a^2+b^2+c^2-2ab-2ac-2bc-4.$$

Therefore, $\deg(d_1)+\deg(d_2) \leq 2\gamma$. Since at most one of the elements of a polynomial Diophantine m-tuple is constant, we have that $\deg(d_1) \neq \deg(d_2)$. Let d_- be the polynomial with smaller degree among d_1 and d_2. Then $\deg(d_-) < \gamma$. It holds

$$ad_-+1=(at \pm rs)^2=R^2, \quad bd_-+1=(bs \pm rt)^2=S^2.$$

Denote

$$\begin{aligned} c_1 &= a+b+d_-+2abd_-+2rRS, \\ c_2 &= a+b+d_-+2abd_--2rRS. \end{aligned}$$

Then $ac_1+1=(aS+rR)^2=(abs \pm art+art \pm abs \pm s)^2$ and $ac_2+1=(aS-rR)^2=(abs \pm art-art \mp abs \mp s)^2$. Hence, there exist $i \in \{1,2\}$ such that $ac_i+1=s^2=ac+1$, which implies $c=c_i$. Let $c'=c_j$, where $j \in \{1,2\}$, $j \neq i$. Since $c \cdot c' = c_1c_2 = a^2+b^2+d_-^2-2ab-2ad_--2bd_--4$, we have $\deg(c)+\deg(c') \leq 2\gamma$. Hence, $\deg(c) \geq \deg(c')$.

Now we have two possibilities:

1) If $d_-=0$, then $R=\pm 1$, $S=\pm 1$ and $c=a+b\pm 2r$.

2) If $d_- \neq 0$, then $\gamma \geq \deg(abd_-) \geq \alpha+\beta$. □

As a consequence of Lemma 1, we can prove the following gap principle for a polynomial Diophantine quadruple.

Lemma 2. *If $\{a,b,c,d\}$ is a polynomial Diophantine quadruple with $0<\alpha \leq \beta \leq \gamma \leq \delta$, then $\delta \geq \beta+\gamma$.*

Proof. Assume that $\delta < \beta+\gamma$. Then, by Lemma 1, we have $\delta=\gamma$. Consider the Diophantine triples $\{a,c,d\}$ and $\{b,c,d\}$. Lemma 1 implies that $d=a+c+2s=b+c+2t$. This relation implies $a-b=2(t-s)$. Multiplying by $t+s$ we obtain $t+s=-2c$, which clearly implies $\beta=\gamma$. But now we may apply Lemma 1 to the triple $\{a,b,d\}$ and obtain

$$d=a+b+2r=a+c+2s=b+c+2t.$$

From $2t-2s=a-b$ and $2t+2s=-4c$, it follows $4t=a-b-4c$. Similarly, from $2t-2r=a-c$ and $2t+2r=-4b$, it follows $4t=a-c-4b$. Hence, we obtained $b=c$, a contradiction. □

Before we can prove an upper bound for the degrees of the elements contained in a polynomial Diophantine quadruple, we will recall the method of reducing the problem of extending a Diophantine triple to a quadruple

to the resolution of a system of Pellian equations.

Let $ab+1=r^2$, $ac+1=s^2$, $bc+1=t^2$, $ad+1=x^2$, $bd+1=y^2$, $cd+1=z^2$. Then

$$az^2 - cx^2 = a - c, \tag{1}$$

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

By [15, Lemma 4], there exist a nonnegative integer m_0 and a solution (Z_0, X_0) of (1) such that $\deg(Z_0) \le \frac{3\gamma-\alpha}{4}$, $\deg(X_0) \le \frac{\alpha+\gamma}{4}$ and

$$z\sqrt{a} + x\sqrt{c} = (Z_0\sqrt{a} + X_0\sqrt{c})(s + \sqrt{ac})^{m_0},$$

and there exist a nonnegative integer n_0 and a solution (Z_1, Y_0) of (2) such that $\deg(Z_1) \le \frac{3\gamma-\beta}{4}$, $\deg(Y_1) \le \frac{\beta+\gamma}{4}$ and

$$z\sqrt{b} + y\sqrt{c} = (Z_1\sqrt{b} + Y_1\sqrt{c})(t + \sqrt{bc})^{n_0}.$$

Hence, $z = V_{m_0} = W_{n_0}$, where the sequences $(V_m)_{m\ge 0}$ and $(U_n)_{n\ge 0}$ are defined by

$$V_0 = Z_0, \quad V_1 = sZ_0 + cX_0, \quad V_{m+2} = 2sV_{m+1} - V_m, \tag{3}$$

$$W_0 = Z_1, \quad W_1 = tZ_1 + cY_1, \quad W_{n+2} = 2tW_{n+1} - W_n. \tag{4}$$

The sequences satisfy the following congruence relations.

Lemma 3. *We have*

$$V_{2m} \equiv Z_0 \pmod{c}, \quad V_{2m+1} \equiv sZ_0 \pmod{c},$$
$$W_{2n} \equiv Z_1 \pmod{c}, \quad W_{2n+1} \equiv tZ_1 \pmod{c},$$

and

$$V_{2m} \equiv Z_0 + 2c(aZ_0m^2 + sX_0m) \pmod{c^2},$$
$$V_{2m+1} \equiv sZ_0 + c(2asZ_0m(m+1) + X_0(2m+1)) \pmod{c^2},$$
$$W_{2n} \equiv Z_1 + 2c(bZ_1n^2 + tY_1n) \pmod{c^2},$$
$$W_{2n+1} \equiv tZ_1 + c(2btZ_1n(n+1) + Y_1(2n+1)) \pmod{c^2}.$$

Proof. This follows from (3) and (4) by induction. □

In the next lemma, we give relations between the initial terms Z_0, Z_1, X_0, Y_1.

Lemma 4.

1) *If $V_{2m} = W_{2n}$, then $Z_0 = Z_1$.*
2) *If $V_{2m+1} = W_{2n}$, then $(Z_0, Z_1) = (\pm 1, \pm s)$, or $(Z_0, Z_1) = (\pm s, \pm 1)$, or $Z_1 = sZ_0 + cX_0$ or $Z_1 = sZ_0 - cX_0$.*
3) *If $V_{2m} = W_{2n+1}$, then $(Z_0, Z_1) = (\pm t, \pm 1)$, or $Z_0 = tZ_1 + cY_1$, or $Z_0 = tZ_1 - cY_1$.*
4) *If $V_{2m+1} = W_{2n+1}$, then $sZ_0 + cX_0 = tZ_1 \pm cY_1$, or $sZ_0 - cX_0 = tZ_1 \pm cY_1$.*

Proof.

1) From Lemma 3, we have $Z_0 \equiv Z_1 \pmod{c}$, and since $\deg(Z_0) < \gamma$, $\deg(Z_1) < \gamma$, we conclude that $Z_0 = Z_1$.

2) We have $Z_1 \equiv sZ_0 \pmod{c}$. If $Z_0 = \pm 1$, then $Z_1 = \pm s$. If $Z_0 \neq \pm 1$, then $\deg(Z_0) \geq \frac{\gamma}{2}$, $\deg(X_0) \geq \frac{\alpha}{2}$ [15, Lemma 5]. If $\alpha = 0$ and X_0 is constant, then $(Z_0, Z_1) = (\pm s, \pm 1)$. Indeed, assume that X_0 is constant and put $e = (X_0^2 - 1)/a$. Then $\{a, e, c\}$ is a Diophantine triple, and now [15, Lemma 1] implies $a = e$, $X_0^2 = a^2 + 1$ and $Z_0^2 = s^2$. Furthermore, $Z_1 \equiv sZ_0 \equiv \pm 1 \pmod{c}$. Assume now that X_0 is not constant. Since

$$(cX_0 + sZ_0)(cX_0 - sZ_0) = c^2 - ac - Z_0^2,$$

we conclude that one of the polynomials $cX_0 + sZ_0$, $cX_0 - sZ_0$ has degree less that γ, and they are both congruent to Z_1 modulo c. Hence, one of these polynomials is equal to Z_1.

3) This case in completely analogous to case 2), except that β cannot be equal to zero.

4) We have $sZ_0 \equiv tZ_1 \pmod{c}$. If X_0 and Y_1 are not constant then, as above, we conclude that one of the polynomials $cX_0 + sZ_0$, $cX_0 - sZ_0$ and one of the polynomials $cY_1 + tZ_1$, $cY_1 - tZ_1$ have degrees less than γ, and these two polynomials are congruent modulo c, thus, they have to be equal. If $Z_0 = \pm 1$, then $Z_1 \equiv \pm st \pmod{c}$. Since $(\pm st - cr)(\pm st + cr) = ac + bc + 1 - c^2$, one of the polynomials $\pm st - cr$, $\pm st + cr$ has degree less then γ, and therefore it has to be equal to Z_1. But $\deg(Z_1) \leq \frac{3\gamma - \beta}{4}$, while $\deg(\pm st \pm cr) \geq 2\gamma - (\gamma + \frac{\alpha + \beta}{2})$, a contradiction.

We have shown in 2) that if X_0 is constant and $Z_0 \neq \pm 1$, then $Z_0 = \pm s$. Now from $tZ_1 \equiv \pm 1 \pmod{c}$, it follows $Z_1 = \pm t$ and $Y_1^2 = b^2 + 1$, a contradiction. Finally, if $Z_1 = 1$, then $Z_0 \equiv \pm st \pmod{c}$ and Z_0 has to be equal to $\pm st - cr$ or $\pm st + cr$. But, as above, $\deg(Z_0) < \deg(\pm st \pm cr)$.□

Now we are ready to prove the above mentioned upper bound.

Proposition 1. *Let $\{a, b, c, d\}$ be a polynomial Diophantine quadruple. Denote by α, β, γ, δ degrees of a,b,c,d, respectively. Assume that $\beta > \alpha$ and $\gamma > 4\beta - \alpha$. Then $\delta < 3\gamma$.*

Proof. We will consider three cases, depending on parities of m_0 and n_0.

Case 1. $m_0 = 2m$, $n_0 = 2n$.

From Lemmas 3 and 4, we have

$$aZ_0m^2 + sX_0m \equiv bZ_0n^2 + tY_1n \pmod{c}. \tag{5}$$

Both sides of (5) have degrees $\leq \beta + \frac{3\gamma - \beta}{4} < \gamma$. Therefore, we can replace $\equiv$ by $=$ in (5):

$$aZ_0m^2 + sX_0m = bZ_0n^2 + tY_1n. \tag{6}$$

Since $\alpha < \beta$, we may assume that $Z_0 \neq \pm 1$. Furthermore, (6) implies that

$$\deg(bZ_0n^2 + tY_1n) < \max(\deg(bZ_0), \deg(tY_1)). \tag{7}$$

We have

$$(bZ_0 + tY_1)(bZ_0 - tY_1) = b^2 - bc - Y_1^2,$$

which implies that $\deg(bZ_0) = \deg(tY_1)$ and that one of the polynomials $bZ_0 + tY_1$, $bZ_0 - tY_1$ has degree less than $\deg(bZ_0)$. But now (7) implies that $n = 0$ or $n = 1$.

Case 2. $m_0 = 2m + 1$, $n_0 = 2n$.

By Lemma 4, we have to consider three cases.
a) $(Z_0, Z_1) = (\pm 1, \pm s)$.
Lemma 3 implies

$$\pm 2asm(m + 1) \pm (2m + 1) \equiv \pm 2bsn^2 \pm 2rtn \pmod{c}. \tag{8}$$

Both sides of (8) have degrees $\leq \beta + \frac{\alpha+\gamma}{2} < \gamma$. Hence, we have equality in (8). From $(bs - rt)(bs + rt) = b^2 - ab - bc - 1$, we conclude that one of the polynomials $bs - rt$, $bs + rt$ has degree less that $\deg(bs)$. Since the polynomial $bsn^2 \pm rtn$ also has degree less that $\deg(bs)$, we conclude that $n = 0$ or $n = 1$.
b) $(Z_0, Z_1) = (\pm s, \pm 1)$.
Now Lemma 3 implies

$$\pm a \pm 2am(m + 1) + X_0(2m + 1) \equiv \pm 2bn^2 \pm 2tn \pmod{c}. \tag{9}$$

Since the degree of left-hand side is $\leq \frac{\alpha+\gamma}{4}$, and the degree of right-hand side is $= \frac{\beta+\gamma}{2} < \gamma$, we obtained a contradiction (unless $n = 0$).
c) $Z_1 = sZ_0 \pm cX_0$.
Now Lemma 3 gives

$$2aZ_1m(m + 1) + X_0(2m + 1 \mp 1) \equiv 2bZ_1n^2 + 2tY_1n \pmod{c}. \tag{10}$$

As in 1), we replace $\equiv$ by $=$, and by examining the degree of right-hand side obtain a contradiction (unless $n \leq 1$).

Case 3. $m_0 = 2m$, $n_0 = 2n + 1$.

We have to consider two cases.
a) $(Z_0, Z_1) = (\pm t, \pm 1)$.
We obtain the following congruence

$$\pm 2atm^2 \pm 2rsm \equiv \pm 2btn(n + 1) \pm (2n + 1) \pmod{c}. \tag{11}$$

Since the degree of right-hand side of (11) is greater than the degree of left-hand side and less than γ, we obtain a contradiction as before (unless $n = 0$).
b) $Z_0 = tZ_1 \pm cY_1$.

Now we have the congruence

$$2aZ_0m^2 + 2sX_0m \equiv 2bZ_0n(n+1) + Y_1(2n+1\pm 1) \pmod{c}, \tag{12}$$

and again the degree of right-hand side of (12) is greater than the degree of left-hand side and $\leq \beta + \frac{3\gamma-\alpha}{4} < \gamma$, which yields a contradiction (for $n \neq 0$).

Case 4. $m_0 = 2m+1$, $n_0 = 2n+1$.

Now Lemma 3 gives

$$2asZ_0m(m+1) + X_0(2m+1\pm 1) \equiv 2btZ_1n(n+1) + Y_1(2n+1\mp 1) \pmod{c}. \tag{13}$$

Noticing that $tZ_1 \equiv sZ_0 \pmod{c}$ and multiplying (13) by s, we obtain

$$2aZ_0m(m+1) + sX_0(2m+1\pm 1) \equiv 2bZ_0n(n+1) + sY_1(2n+1\pm 1) \pmod{c}. \tag{14}$$

Among the four polynomials in (14), the largest degree has the polynomial $2bZ_0n(n+1)$, and its degree is less than γ. This leads to a contradiction (unless $n = 0$).

Up to now, we proved that if $n_0 = 2n$, then $n = 0$ or $n = 1$, and if $n_0 = 2n+1$, then $n = 0$. Therefore, we actually proved that

$$n_0 \leq 2.$$

Now, we have

$$cd + 1 = z^2 = W_n^2 \leq W_2^2.$$

From

$$W_2 = Z_1 + 2c(bZ_1 + tY_1),$$

we obtain

$$\deg(W_2) \leq \gamma + \beta + \frac{3\gamma - \beta}{4} = \frac{7\gamma + 3\beta}{4}$$

and

$$\delta \leq \frac{7\gamma + 3\beta}{2} - \gamma = \frac{5\gamma + 3\beta}{2} < 3\gamma.$$

□

Now we are ready to proof our first theorem. This will be done by combining the gap principle with the upper bound from the last proposition.

Proof of Theorem 1.

Assume that $\{a_1, a_2, \ldots, a_{11}\}$ is a polynomial Diophantine 11-tuple. Denote the degree of a_i by α_i, for $i = 1, 2, \ldots, 11$. Let $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_{11}$.

We will show that the triple $\{a_1, a_4, a_8\}$ satisfies conditions on the triple $\{a, b, c\}$ in Proposition 1. By Lemma 2, we have $\alpha_4 > \alpha_1$ and

$$\alpha_8 \geq \alpha_7 + \alpha_6 \geq 2\alpha_6 + \alpha_5 \geq 3\alpha_5 + 2\alpha_4 \geq 5\alpha_4.$$

Therefore, we may apply Proposition 1. We obtain that

$$\alpha_{11} < 3\alpha_8.$$

On the other hand, Lemma 2 implies

$$\alpha_{11} \geq \alpha_{10} + \alpha_9 \geq 2\alpha_9 + \alpha_8 > 3\alpha_8,$$

a contradiction. □

3. Proofs of Theorems 2 and 3

Let us recall the definitions of the discrete valuations on the field $\mathbb{K}(X)$, where X is transcendental over the field $\mathbb{K}$. For $\xi \in \mathbb{K}$ define the valuation ν_ξ such that for $f \in \mathbb{K}(X)$ we have $f(X) = (X-\xi)^{\nu_\xi(Q)} a(X)/b(X)$ where a, b are polynomials with $a(\xi)b(\xi) \neq 0$. Further, for $f = a/b$ with $a, b \in \mathbb{K}[X]$, we put $\deg f := \deg a - \deg b$; thus $\nu_\infty := -\deg$ is a discrete valuation on $\mathbb{K}(X)$. These are all discrete valuations on $\mathbb{K}(X)$.

We need the following generalization of the degree from $\mathbb{K}[X]$ to $\mathbb{K}(X)$. We define the *height* of f by

$$\mathcal{H}(f) = -\sum_{\nu} \min\{0, \nu(f)\}$$

where the sum is taken over all valuations on $\mathbb{K}(X)$; thus the height $\mathcal{H}(f)$ is just the number of poles of f counted according to multiplicity. We note that if f lies in $\mathbb{K}[X]$, then $\mathcal{H}(f) = \deg f$.

Now we state the following theorem on the solutions of two-dimensional unit equations over an algebraic function field, which is usually referred to as Mason's inequality and which can be seen as an analog of Baker's theorem concerning lower bounds for linear forms in logarithms of algebraic numbers. A proof of this theorem can be found in the monograph of Mason (cf. [22, Lemma 2]).

Theorem 4. (R.C. Mason) *Let γ_1, γ_2 and γ_3 be non-zero elements of $\mathbb{K}(X)$ with $\gamma_1 + \gamma_2 + \gamma_3 = 0$, and such that $\nu(\gamma_1) = \nu(\gamma_2) = \nu(\gamma_3)$ for each valuation ν not in the finite set $\mathcal{V}$. Then*

$$\mathcal{H}(\gamma_1/\gamma_2) \leq \max\{0, |\mathcal{V}| - 2\},$$

where $|\mathcal{V}|$ denotes the number of elements of $\mathcal{V}$.

Now we are ready to prove our theorems. We start by obtaining a gap principle which gives an inequality between the degrees of the elements in a pure power Diophantine triple.

Lemma 5. *Assume that $a, b, c \in \mathbb{K}[X]$ satisfy $ac + 1 = u^k$ and $bc + 1 = v^\ell$ with $u, v \in \mathbb{K}[X]$ and $k, \ell \geq k_0 \geq 3$. Let α, β, γ be the degree of a, b, c, respectively, and assume that $\alpha \leq \beta \leq \gamma$. Then*

$$\gamma \leq \frac{k_0 + 2}{k_0 - 2}\beta.$$

Proof. By eliminating c from the equations $ac + 1 = u^k, bc + 1 = v^\ell$ we get

$$bu^k - av^\ell = b - a.$$

Applying Mason's inequality (cf. Theorem 4) to this unit equation we get

$$\mathcal{H}(bu^k/(b-a)) \leq |\mathcal{V}| - 2,$$

where $\mathcal{V} = \{\infty\} \cup \{z \in \mathbb{K} \ : \ u(z) = 0, v(z) = 0, a(z) = 0, b(z) = 0, b(z) - a(z) = 0\}$. Observe that some of the zeros of a, b and $b - a$ may coincide. The cardinality of this set can be bounded by

$$|\mathcal{V}| \leq 1 + \frac{1}{k}\alpha + \frac{1}{k}\gamma + \frac{1}{\ell}\beta + \frac{1}{\ell}\gamma + \beta + \alpha + \sum_{z\in\mathbb{K}} \max\{0, \nu_z(b-a) - \nu_z(bu^k)\},$$

since $k \deg u = \deg ac = \alpha + \gamma$ and $\ell \deg v = \deg bc = \beta + \gamma$. Of course, this upper bound is not sharp in general. On the other hand, calculating the height under consideration, we get

$$\begin{aligned}
&\mathcal{H}(bu^k/(b-a)) \\
&\quad = \quad -\min\{\deg(b-a) - \deg(bu^k), 0\} - \sum_{z\in\mathbb{K}} \min\{0, \nu_z(bu^k) - \nu_z(b-a)\} \\
&\quad = \quad \deg(bu^k) - \deg(b-a) + \sum_{z\in\mathbb{K}} \max\{0, \nu_z(b-a) - \nu_z(bu^k)\} \\
&\quad \geq \quad \gamma + \alpha + \sum_{z\in\mathbb{K}} \max\{0, \nu_z(b-a) - \nu_z(bu^k)\}.
\end{aligned}$$

Observe that $\deg(bu^k) - \deg(b-a) \geq \deg(u^k) = \deg(ac) = \gamma + \alpha \geq 0$. It follows that

$$\gamma \leq \left(\frac{1}{k} + \frac{1}{\ell} + 1\right)\beta + \left(\frac{1}{k} + \frac{1}{\ell}\right)\gamma \leq \left(\frac{2}{k_0} + 1\right)\beta + \frac{2}{k_0}\gamma$$

and therefore the bound in the lemma. □

By using Mason's inequality once again, we prove an upper bound for the degree of the first element in a pure power Diophantine quadruple in terms of the degrees of the other three elements. We have:

Lemma 6. *Assume that $a_1, a_2, a_3, a_4 \in \mathbb{K}[X]$ are four different polynomials that satisfy $a_1a_2+1 = x_1^{p_1}, a_2a_3+1 = x_2^{p_2}, a_3a_4+1 = x_3^{p_3}, a_4a_1+1 = x_4^{p_4}$ with $x_1, x_2, x_3, x_4 \in \mathbb{K}[X]$ and $p_1, p_2, p_3, p_4 \geq k_0 \geq 2$ and let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ denote the degree of a_1, a_2, a_3, a_4, respectively. Assume that $\alpha_1 \leq \alpha_2 \leq \alpha_3 \leq \alpha_4$. Then*

$$\alpha_1 \leq \frac{1}{k_0 - 1}(\alpha_2 + \alpha_3 + \alpha_4).$$

Proof. We have $a_1a_2a_3a_4 = (x_1^{p_1} - 1)(x_3^{p_3} - 1) = (x_2^{p_2} - 1)(x_4^{p_4} - 1)$ and using this identity we get

$$x_1^{p_1}x_3^{p_3} - x_2^{p_2}x_4^{p_4} = x_1^{p_1} + x_3^{p_3} - x_2^{p_2} - x_4^{p_4} = (a_1 - a_3)(a_2 - a_4).$$

Observe that this expression is different from 0 since we assume that the polynomials are different. Now we apply Mason's inequality (cf. Theorem 4)

to the unit equation

$$x_1^{p_1}x_3^{p_3} - x_2^{p_2}x_4^{p_4} = (a_1 - a_3)(a_2 - a_4).$$

Let $\mathcal{V}$ be the set of distinct zeros of $x_1x_2x_3x_4(a_1-a_3)(a_2-a_4)$ in $\mathbb{K}$ together with ∞. Observe that some of the zeros of $x_1x_2x_3x_4$ and $(a_1 - a_3)(a_2 - a_4)$ may coincide. Therefore the cardinality of $\mathcal{V}$ can be estimated by

$$\begin{aligned}|\mathcal{V}| \le 1 + \frac{1}{p_1}(\alpha_1 + \alpha_2) + \frac{1}{p_3}(\alpha_3 + \alpha_4) + \frac{1}{p_2}(\alpha_2 + \alpha_3) + \frac{1}{p_4}(\alpha_1 + \alpha_4)\\ + \sum_{z\in\mathbb{K}} \max\{0, \nu_z((a_1 - a_3)(a_2 - a_4)) - \nu_z(x_1^{p_1}x_3^{p_3})\}.\end{aligned}$$

We mention that the upper bound is not sharp in general, since we counted the roots of $x_1x_2x_3x_4$ by multiplicity and just used a partial correction in the term involving $(a_1 - a_3)(a_2 - a_4)$, but this will be enough to get our desired bound. First we get

$$\mathcal{H}(x_1^{p_1}x_3^{p_3}/((a_1 - a_3)(a_2 - a_4)) \le |\mathcal{V}| - 2,$$

and by calculating the height directly we obtain

$$\begin{aligned}&\mathcal{H}(x_1^{p_1}x_3^{p_3}/((a_1 - a_3)(a_2 - a_4))\\ &\quad = -\min\{0, \deg((a_1 - a_3)(a_2 - a_4)) - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)\}\\ &\qquad\qquad - \sum_{z\in\mathbb{K}} \min\{0, \nu_z(x_1^{p_1}x_3^{p_3}) - \nu_z((a_1 - a_3)(a_2 - a_4))\}\\ &\quad \ge \alpha_1 + \alpha_2 + \sum_{z\in\mathbb{K}} \max\{0, \nu_z((a_1 - a_2)(a_3 - a_4)) - \nu_z(x_1^{p_1}x_3^{p_3})\}.\end{aligned}$$

By comparing upper and lower bound we get

$$\begin{aligned}2\alpha_1 \le \alpha_1 + \alpha_2 &\le \frac{1}{p_1}(\alpha_1 + \alpha_2) + \frac{1}{p_3}(\alpha_3 + \alpha_4) + \frac{1}{p_2}(\alpha_2 + \alpha_3) + \frac{1}{p_4}(\alpha_1 + \alpha_4)\\ &\le \frac{2}{k_0}(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)\end{aligned}$$

and thus

$$\left(1 - \frac{1}{k_0}\right)\alpha_1 \le \frac{1}{k_0}(\alpha_2 + \alpha_3 + \alpha_4).$$

From this, the claim follows. □

Now we are ready the give the proof of Theorem 2, which is obtained by comparing the upper and lower bound from Lemma 5 and 6.

Proof of Theorem 2.

Let $\{a_1, a_2, a_3, a_4, a_5\}$ be a pure power Diophantine quintuple in $\mathbb{K}[X]$ such that the product of any two distinct elements plus 1 is a perfect kth power for some $k \ge k_0 \ge 3$. We denote the degrees by $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$, respectively. Since at most one element in a pure power Diophantine m-tuple is constant, it follows that $\alpha_2 \ge 1$.

By Lemma 6, we get that

$$\alpha_2 \leq \frac{1}{k_0-1}(\alpha_3+\alpha_4+\alpha_5).$$

Now, by using Lemma 5 several times (applied to $\{a_1,a_2,a_3\}$, $\{a_1,a_2,a_4\}$ and $\{a_1,a_2,a_5\}$, respectively), it follows that

$$\alpha_2 \leq \frac{1}{k_0-1}\left[\frac{k_0+2}{k_0-2}+\frac{k_0+2}{k_0-2}+\frac{k_0+2}{k_0-2}\right]\alpha_2 = \frac{3(k_0+2)}{(k_0-1)(k_0-2)}\alpha_2.$$

Observe again that $\alpha_2 \geq 1$. It follows

$$\frac{3(k_0+2)}{(k_0-1)(k_0-2)} \geq 1.$$

This inequality leads to a contradiction if $k_0 \geq 7$ (the left-hand side is a rational function in k_0 which tends to 0 for k_0 to infinity). This proves the theorem. □

Proof of Theorem 3.

We first note that we already know that there is no quintuple such that the product of any two plus one is a kth power with $k \geq 7$ by Theorem 2. It remains to take only the possibilities with smaller exponents into account. Clearly, we can restrict to prime exponents and thus assume that the exponent k belongs to the list $\mathcal{P} = \{2,3,5\}$ of primes below 7.

Now let G be the graph whose vertices are the elements of the pure power Diophantine m-tuple. We color the edge of G with the 4 colors $\mathcal{P} \cup \{\infty\}$ in the following way: if $a_ia_j + 1 = x^k$, then the edge from a_i to a_j is colored with p if p is the smallest prime from $\mathcal{P}$ dividing k and with ∞ if there is no such $p \in \mathcal{P}$.

Now it is clear that $m \leq R(11,6,4,5;2)$. Recall that the Ramsey number $R(n_{s_1}, n_{s_2}, \ldots, n_{s_t}; 2)$ is the smallest positive integer R such that no matter how we color the edges of the complete graph with R vertices with the colors $s_1, s_2, \ldots, s_t$, there exist i and a complete monochromatic subgraph with n_i vertices colored with color i. The numbers n_i in our upper bound follow from our Theorem 1 (namely, $n_2 = 11$), the bounds proved in [15] (namely, $n_3 = 6$ and $n_5 = 4$) and the bound from Theorem 2 (namely, $n_\infty = 5$).

To simplify the upper bound we use the recurrence

$$\begin{aligned} &R(n_{s_1}, n_{s_2}, \ldots, n_{s_t}; 2) \\ &\qquad \leq \quad t-2+\sum_{i=1}^{t} R(n_{s_1}, \ldots, n_{s_{i-1}}, n_{s_i}-1, n_{s_{i+1}}, \ldots, n_{s_t}; 2), \end{aligned}$$

together with the facts that Ramsey numbers are symmetric with respect to the n_i, i.e.

$$R(n_{s_1}, n_{s_2}, \ldots, n_{s_t}; 2) = R(n_{\sigma(s_1)}, n_{\sigma(s_2)}, \ldots, n_{\sigma(s_t)}; 2)$$

for a permutation σ of the set $\{s_1, \ldots, s_t\}$, and that we have

$$R(2, n_{s_1}, n_{s_2}, \ldots, n_{s_{t-1}}; 2) = R(n_{s_1}, n_{s_2}, \ldots, n_{s_{t-1}}; 2),$$
$$R(n; 2) = n.$$

A list of upper bounds for small Ramsey numbers can be found in [23], e.g. we have $R(3, 3; 2) = 6, R(3, 3, 3; 2) = 17$ and $R(3, 3, 3, 3; 2) \leq 62$. For all these results, we refer to the survey paper [23]. By using all the bounds there together with the general recurrence formula from above, it is easy to show that $m \leq 180952390 \leq 2 \cdot 10^9$. This finishes the proof. □

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] Y. Bugeaud and A. Dujella, On a problem of Diophantus for higher powers, *Math. Proc. Cambridge Philos. Soc.* **135** (2003), 1-10.

[4] Y. Bugeaud and K. Gyarmati, On generalizations of a problem of Diophantus, *Illinios J. Math.* **48** (2004), 1105-1115.

[5] R. Dietmann, C. Elsholtz, K. Gyarmati, and M. Simonovits, Shifted products that are coprime pure powers, *J. Comb. Theor. A* **111** (2005), 24-36.

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

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

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

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

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

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

[12] A. Dujella, C. Fuchs, and R. F. Tichy, Diophantine m-tuples for linear polynomials, *Period. Math. Hungar.* **45** (2002), 21-33.

[13] A. Dujella, C. Fuchs, and G. Walsh, Diophantine m-tuples for linear polynomials. II. Equal degrees, *J. Number Theory*, to appear.

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

[15] A. Dujella and F. Luca, On a problem of Diophantus with polynomials, *Rocky Mountain J. Math.*, to appear (Preprint: http://www.math.hr/∼duje/dvi/dluca.dvi).

[16] R. L. Graham, B. L. Rothschild, and J. H. Spencer, *Ramsey Theory*, John Wiley & Sons, 1980.

[17] K. Gyarmati, On a problem of Diophantus, *Acta Arith.* **97** (2001), 53-65.

[18] K. Gyarmati, A. Sárközy, and C. L. Stewart, On shifted products which are powers, *Mathematika* 49 (2002), 227-230.

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

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

[21] F. Luca, On shifted products which are powers, *Glas. Mat. Ser. III* **40(60)** (2005), 13-20.
[22] R. C. Mason, *Diophantine equations over function fields*, London Mathematical Society Lecture Notes Series, vol. 96, Cambridge University Press, Cambridge, 1984.
[23] S. P. Radziszowski, Small Ramsey numbers, *Electronic J. Compu.* Dynamical Survey DS1 (2004), 1-42.
[24] M. Rosen, *Diophantine Equations over Function Fields*, Cambridge Univ. Press, Cambridge, 2002.

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

Clemens Fuchs
Institut für Analysis und Computational Number Theory (Math A)
TU Graz
Steyrergasse 30/II
A-8010 Graz
Austria
E-mail: clemens.fuchs@tugraz.at

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán
México
E-mail: fluca@matmor.unam.mx