On a problem of Diophantus with polynomials

Andrej Dujella *Florian Luca*

Abstract. Let $m \geq 2$ and $k \geq 2$ be integers and let R be a commutative ring with a unit element denoted by 1. A k-th power diophantine m-tuple in R is an m-tuple $(a_1,\ a_2,\ \ldots,\ a_m)$ of non-zero elements of R such that $a_i a_j + 1$ is a k-th power of an element of R for $1 \leq i < j \leq m$. In this paper, we investigate the case when $k \geq 3$ and $R = \mathbf{K}[X]$, the ring of polynomials with coefficients in a field $\mathbf{K}$ of characteristic zero. We prove the following upper bounds on m, the size of diophantine m-tuple: $m \leq 5$ if $k = 3$; $m \leq 4$ if $k = 4$; $m \leq 3$ for $k \geq 5$; $m \leq 2$ for k even and $k \geq 8$.

1. Introduction

Let $m \geq 2,\ k \geq 2$ be positive integers and R be a commutative ring with 1. A kth power diophantine m-tuple in R is an m-tuple $(a_1,\ a_2,\ \ldots,\ a_m)$ of non-zero elements of R such that $a_i a_j + 1$ is a kth power of an element of R for $1 \leq i < j \leq m$. Given R and k, the question of interest is usually finding an upper bound on m, the size of such a kth power diophantine m-tuple. For $k = 2$ and $R = \mathbf{Z}$, or $\mathbf{Q}$, the ring of integers, or the field of rational numbers, this question has received a lot of interest (see [3], pages 513-520). For example, the first diophantine quadruple of rational numbers $\left(\frac{1}{16},\ \frac{33}{16},\ \frac{17}{4},\ \frac{105}{16}\right)$ was found by Diophantus himself, while the first diophantine quadruple of integers $(1,\ 3,\ 8,\ 120)$ was found by Fermat. In 1969, Baker and Davenport (see [1]) showed that Fermat's quadruple cannot be extended to a diophantine quintuple of integers, and in 1998, Dujella and Pethő (see [7]) proved that even the pair (1,3) cannot be extended to a diophantine quintuple. When $R = \mathbf{Z}$ and $k = 2$ it is conjectured that $m \leq 4$, and the best result available to date towards this conjecture is due to the first author who proved (see [4]) that $m \leq 5$, and that $m = 5$ can happen only in finitely many, effectively computable, instances. In the case in which $R = \mathbf{Q}$ and $k = 2$, the first Diophantine quintuple was found by Euler and a few diophantine sextuples were recently found by Gibbs (see [8]). However, no upper bound for the size of such sets is known.

The case $R = \mathbf{Z}[X]$ and $k = 2$ was considered by Jones (see [10,11]). Among other results, he proved that the pair of polynomials $(X,\ X + 2)$ cannot be extended to a diophantine quintuple. Recently, some variants of this case were considered by Dujella and Fuchs (see [5]) and Dujella, Fuchs and Tichy (see [6]). In [5], it was showed that there is no quadruple of polynomials $(a_1,\ a_2,\ a_3,\ a_4)$ with integer coefficients and at least one of them non-constant, such that $a_i a_j - 1$ is a perfect square in $\mathbf{Z}[X]$ for all $1 \leq i < j \leq 4$. In [6], an absolute upper bound was given for the size of sets of polynomials with integer coefficients such that the product of any two of them plus a linear polynomial is a square.

For $R = \mathbf{Z}$ and larger values of k, Bugeaud and Dujella (see [2]) showed that there is no kth power diophantine quadruple provided that $k \geq 177$. They also gave upper bounds on the size of a kth power diophantine m-tuple for the remaining values $3 \leq k \leq 176$.

In this paper, we investigate the above question when $k \geq 3$ and $R = \mathbf{K}[X]$, the ring of polynomials with coefficients in any field $\mathbf{K}$ of characteristic zero. There is no loss of generality in assuming that $\mathbf{K}$ is algebraically closed. Before we state our results, let us make a few remarks. Suppose

Keywords and phrases : Diophantine m-tuples, polynomials.
2000 *Mathematics Subject Classification* : 11C08, 11D41.

that $k \geq 2$ and $(a_1, \ldots, a_m)$ is a kth power diophantine m-tuple. When $R = \mathbf{Z}$, then the fact that $a_i \neq a_j$ holds for all $i \neq j$ follows from the fact that the equation $a^2 + 1 = r^k$ has no integer solutions (a, r, k) with $k \geq 2$ and $a \neq 0$. However, this is not necessarily so over other rings. In particular, if $(a_1, a_2, \ldots, a_m)$ is a kth power diophantine m-tuple over R, and if $a_m^2 + 1$ happens to be an kth power in R, then we may adjoin at the m-tuple $(a_1, \ldots, a_m)$ values of a_m, say t times, where $t \geq 1$ is any positive integer, obtaining in this way a kth power diophantine $(m+t)$-tuple. Since when $\mathbf{K}$ is algebraically closed the equation $a^2 + 1 = r^k$ admits a solution r in $\mathbf{K}$ for any given values of $a \in \mathbf{K}$ and integer $k \geq 2$, it follows that we have to assume that our kth power diophantine m-tuple $(a_1, a_2, \ldots, a_m)$ consisting of non-zero polynomials in $\mathbf{K}[X]$, fulfills $a_i \neq a_j$ for $i \neq j$ whenever a_i is a constant polynomial. Let us also notice that since $\mathbf{K}$ is algebraically closed, any m-tuple of constant polynomials is a kth power diophantine m-tuple for any $k \geq 2$. So, we will assume that at least one of the polynomials is non-constant. From now on, we will work under these assumptions.

Let us also notice that, at least in principle, one may ask for a slightly more general problem, namely given $k \geq 2$, to determine an upper bound for m such that there exist $\lambda \in \mathbf{K}^*$ and an m-tuple of non-zero polynomials $(a_1, a_2, \ldots, a_m)$ with coefficients in $\mathbf{K}$ and at least one of them non-constant, and such that

$$a_i a_j + \lambda = r_{ij}^k \qquad \text{for } 1 \leq i < j \leq m \tag{1}$$

holds, with $r_{ij} \in \mathbf{K}[X]$ for all $1 \leq i < j \leq m$. However, since K is algebraically closed, we may replace a_i by $\lambda^{-1/2} a_i$ and r_{ij} by $\lambda^{-1/k} r_{ij}$ and obtain our original problem.

Our main result is the following.

Theorem.

Assume that $\mathbf{K}$ is an algebraically closed field and that $(a_1, a_2, \ldots, a_m)$ is a kth power diophantine m-tuple consisting of polynomials with coefficients in $\mathbf{K}$ not all of them constant. Assume also that if a_i and a_j are constant polynomials for $i \neq j$, then $a_i \neq a_j$. Then,

i. $m \leq 5$ *if* $k = 3$*;*

ii. $m \leq 4$ *if* $k = 4$*;*

iii. $m \leq 3$ *for* $k \geq 5$*;*

iv. $m \leq 2$ *for* k *even and* $k \geq 8$.

The paper is organized as follows. We first prove a couple of lemmas concerning inequalities between the degrees of polynomials appearing in kth power diophantine triples and, respectively, quadruples. Combining these two results, we get an easy proof of parts i-iii of our Theorem. For the proof of part iv of the above Theorem, we will develop a theory of Pell-like equations in $\mathbf{K}[X]$.

2. Inequalities for the degrees of polynomials

In the proof of our first two lemmas we will use the following theorem of Mason [12] (see also [13]), which is usually referred to as the *abc theorem* for polynomials:

The *abc* Theorem.

Let f, g, h be three non-zero polynomials, not all three constant such that f and g are coprime and $f + g = h$. Then,

$$\max(\deg(f), \deg(g), \deg(h)) \leq N(fgh) - 1,$$

where for a non-constant polynomial λ we denote by $N(\lambda)$ the number of distinct roots of λ.

Lemma 1.

Let $(a_1,\ a_2,\ \dots,\ a_m)$ be a kth power diophantine m-tuple satisfying the conditions from the hypothesis of the Theorem. Then $a_i \neq a_j$ for $i \neq j$ and at most one of the polynomials a_i for $i = 1,\ \dots,\ m$ is constant.

Proof. We already know that the constant polynomials appearing in the m-tuple are distinct. Assume that there exist a non-constant polynomial a such that $a = a_i = a_j$ for some $i \neq j$. We write

$$a^2 + 1 = r^k \tag{2}$$

and notice that a and r have no common root and that

$$\deg(r) = \frac{2\deg(a)}{k}.$$

An applications of Mason's theorem to the equation (2) gives $2\deg(a) \leq \deg(a) + \frac{2\deg(a)}{k} - 1$ or $(k-2)\deg(a) \leq -k$, which is obviously a contradiction.
To prove the second assertion of Lemma 1, assume that $a \neq b$ are two constant polynomials belonging to the m-tuple, and let c be a non-constant polynomial in the m-tuple. We write

$$ac + 1 = r^k \qquad \text{and} \qquad bc + 1 = s^k, \tag{3}$$

where r and s are some non-constant polynomials. Relations (3) imply

$$br^k - as^k = b - a. \tag{4}$$

Applying Mason's theorem to the equation (4), we get $k\deg(r) \leq 2\deg(r) - 1 < 2\deg(r)$, which is a contradiction. $\square$

Lemma 2.

Assume that $a,\ b,\ c$ are distinct polynomials such that at most one of them is constant. Assume moreover that

$$ac + 1 = r^k \qquad \textit{and} \qquad bc + 1 = s^k \tag{5}$$

hold with two polynomials r and s. Let $\alpha = \deg(a),\ \beta = \deg(b),\ \gamma = \deg(c)$ and assume that $\alpha \leq \beta$. Then,

$$(k-2)\gamma \leq (k+1)\beta + \alpha - k. \tag{6}$$

Proof. We may, of course, assume that c is not constant otherwise relation (6) is obviously satisfied. Thus, $\gamma > 0$. From (5), we read $\deg(r) = \dfrac{\alpha+\gamma}{k}$ and $\deg(s) = \dfrac{\beta+\gamma}{k}$. In particular, $\deg(s) \geq \deg(r) > 0$. Eliminating c from the two relations (5) we get

$$br^k - as^k = b - a. \tag{7}$$

Let $g = \gcd(r, s)$ and $h = \gcd(a, b)$. We may write (7) as

$$\frac{b}{h}\left(\frac{r}{g}\right)^k - \frac{a}{h}\left(\frac{s}{g}\right)^k = \frac{b-a}{hg^k}. \tag{8}$$

It is clear that the polynomials appearing in (8) satisfy the conditions of Mason's theorem. We obtain

$$k\Big(\frac{\beta+\gamma}{k}-\deg(g)\Big)+(\alpha-\deg(h))\leq$$

$$\Big(\frac{\alpha+\gamma}{k}-\deg(g)+\beta-\deg(h)\Big)+\Big(\frac{\beta+\gamma}{k}-\deg(g)+\alpha-\deg(h)\Big)+(\beta-\deg(h)-k\deg(g))-1.$$

Thus,

$$\alpha+\beta+\gamma\leq\frac{\alpha+\beta+\gamma}{k}+\alpha+2\beta-1,\tag{9}$$

and it is easy to see that inequality (9) is equivalent to inequality (6). $\square$

Notice that, in particular, Lemma 2 gives us an upper bound on the largest degree of a polynomial appearing in a kth power diophantine triple in terms of the degrees of the other two polynomials.

In what follows, we prove a gap principle for the largest degree of a polynomial appearing in a kth power diophantine quadruple in terms of the degrees of the other three involved polynomials. This principle appears originally in a paper of Gyarmati (see [9], and [2] for some slight improvements of the principle from [9]) for kth power diophantine m-tuples consisting of integers. Our next lemma illustrates the above principle in the polynomial context.

Lemma 3.
Let $\mathcal{A}=\{a,\ b\}$ and $\mathcal{B}=\{c_1,\ c_2\}$ be two sets consisting each of two non-zero distinct polynomials with coefficients in $\mathbf{K}$. Let $\alpha,\ \beta,\ \gamma_1,\ \gamma_2$ be the degrees of $a,\ b,\ c_1,\ c_2$, respectively, and assume that $\alpha\leq\beta$ and $\gamma_1\ \leq\gamma_2$. Assume moreover that $fg+1$ is a kth power of a polynomial with coefficients in $\mathbf{K}$ for all $f\in\mathcal{A}$ and $g\in\mathcal{B}$. Then,

$$\beta+\gamma_2\geq(k-1)(\alpha+\gamma_1).\tag{10}$$

Proof. Write

$$\begin{aligned} ac_1+1&=r_1^k, \\ ac_2+1&=r_2^k, \end{aligned}\qquad\text{and}\qquad \begin{aligned} bc_1+1&=s_1^k, \\ bc_2+1&=s_2^k, \end{aligned}\tag{11}$$

with some polynomials $r_i,\ s_i$ for $i=1,\ 2$. Notice that $\deg(r_i)=\dfrac{\alpha+\gamma_i}{k}$ and $\deg(s_i)=\dfrac{\beta+\gamma_i}{k}$ for $i=1,\ 2$. In particular, $\deg(s_i)\geq\deg(r_i)$ for $i=1,\ 2$, $\deg(s_2)\geq\deg(s_1)$ and $\deg(r_2)\geq\deg(r_1)$. From the first and the last relations (11) we get

$$abc_1c_2=(ac_1)(bc_2)=(r_1^k-1)(s_2^k-1)$$

and from the second and the third relations (11) we get

$$abc_1c_2=(ac_2)(bc_1)=(r_2^k-1)(s_1^k-1).$$

Thus,

$$(r_1^k-1)(s_2^k-1)=(r_2^k-1)(s_1^k-1),$$

or

$$(r_1s_2)^k-(r_2s_1)^k=r_1^k+s_2^k-r_2^k-s_1^k.\tag{12}$$

We first notice that the two polynomials appearing in the two sides of (12) are not zero. Indeed, if $(r_1s_2)^k=(r_2s_1)^k$, we get $(ac_1+1)(bc_2+1)=(ac_2+1)(bc_1+1)$, or $ac_1+bc_2=ac_2+bc_1$, which leads to $(a-b)(c_1-c_2)=0$, contradicting the fact that $a \neq b$ and $c_1 \neq c_2$. To get a gap principle, we compare the degrees of the two polynomials appearing in (12). Let $\zeta_1, \ldots, \zeta_k$ be all the roots of 1 of exponent k in $\mathbf{K}$, i.e. the roots of the polynomial $X^k - 1$. Since $\mathbf{K}$ is of characteristic zero, it follows that all these roots are distinct. Let A be the leading coefficient of $r_1 s_2$ and B be the leading coefficient of $r_2 s_1$. Notice that

$$(r_1 s_2)^k - (r_2 s_1)^k = \prod_{i=1}^{k} (r_1 s_2 - \zeta_i r_2 s_1). \tag{13}$$

The two polynomials $r_1 s_2$ and $r_2 s_1$ have the same degree, namely $\delta := \dfrac{\alpha+\beta+\gamma_1+\gamma_2}{k}$, therefore

$$r_1 s_2 - \zeta_i r_2 s_1 = (A - \zeta_i B) X^{\delta} + \text{terms of smaller degree.} \tag{14}$$

Since ζ_i are distinct for $i = 1, 2, \ldots, k$, at most one of the elements $A - \zeta_i B$ can be zero. This shows that the inequality

$$\deg(r_1 s_2 - \zeta_i r_2 s_1) < \delta$$

can hold for at most one value of the index $i = 1, 2, \ldots, k$, and if it does hold for one index i, then $\deg(r_1 s_2 - \zeta_i r_2 s_1) \geq 0$ because this polynomial cannot be the zero polynomial. This argument shows that

$$\deg((r_1 s_2)^k - (r_2 s_1)^k) \geq (k-1)\delta = \Big(\frac{k-1}{k}\Big)(\alpha+\beta+\gamma_1+\gamma_2). \tag{15}$$

Since obviously

$$\deg(r_1^k + s_2^k - r_2^k - s_1^k) \leq \deg(s_2^k) = \beta + \gamma_2, \tag{16}$$

we get, by (12), (15), and (16), that

$$\frac{k-1}{k}(\alpha+\beta+\gamma_1+\gamma_2) \leq \beta + \gamma_2, \tag{17}$$

and it is easy to see that inequality (17) is equivalent to inequality (10). $\square$

3. The proof of the Theorem: Parts i-iii

We first deal with the case $k \geq 5$. Assume that (a, b, c, d) is a kth power diophantine quadruple of polynomials satisfying the hypothesis of the Theorem. Let $\alpha, \beta, \gamma, \delta$ be the degrees of a, b, c, d, respectively, and assume that $\alpha \leq \beta \leq \gamma \leq \delta$. By Lemma 1, we know that at most one of them can be constant (and if this is so, then the constant polynomial must be a), and that all four of them are distinct. Applying Lemma 2 to the triple (a, b, c, d), we get

$$\delta \leq \frac{(k+1)\beta}{k-2} + \frac{\alpha}{k-2} - \frac{k}{k-2}. \tag{18}$$

Applying Lemma 3 to the pairs of sets $\mathcal{A} = \{a, b\}$ and $\mathcal{B} = \{c, d\}$, we get

$$\delta + \beta \geq (k-1)(\alpha+\gamma) \geq (k-1)(\alpha+\beta). \tag{19}$$

Thus,

$$(k-1)\alpha + (k-2)\beta \leq \delta \leq \frac{(k+1)\beta}{k-2} + \frac{\alpha}{k-2} - \frac{k}{k-2},$$

or

$$0 \leq \Big(\frac{k+1}{k-2} - (k-2)\Big)\beta + \Big(\frac{1}{k-2} - (k-1)\Big)\alpha - \frac{k}{k-2}, \tag{20}$$

which is obviously a contradiction because $\beta > 0$ and $\frac{k+1}{k-2} - (k-2) < 0$ for $k \geq 5$. Thus, there does not exist a kth power diophantine quadruple if $k \geq 5$.
When $k = 4$, inequality (18) for the quadruple $(a,\ b,\ c,\ d)$ shows that

$$\delta \leq \frac{5\beta}{2} + \frac{\alpha}{2} - 2 \tag{21}$$

and inequality (19) for this quadruple implies

$$\delta + \beta \geq 3\alpha + 3\gamma. \tag{22}$$

Assume now that there exist a fourth power diophantine quintuple $(a,\ b,\ c,\ d,\ e)$ and let $\alpha \leq \beta \leq \gamma \leq \delta \leq \epsilon$ be the degrees of $a,\ b,\ c,\ d,\ e$, respectively. Applying inequality (22) for the two quadruples $(b,\ c,\ d,\ e)$ and $(a,\ b,\ c,\ d)$, we get

$$\epsilon + \gamma \geq 3(\delta + \beta) \geq 9(\gamma + \alpha),$$

or

$$\epsilon \geq 8\gamma + 9\alpha. \tag{23}$$

However, inequality (21) for the quadruple $(a,\ b,\ c,\ e)$ shows that

$$\epsilon \leq \frac{5}{2}\beta + \frac{\alpha}{2} - 2, \tag{24}$$

and now (23) and (24) lead to

$$\frac{5}{2}\beta + \frac{\alpha}{2} - 2 \geq 8\gamma + 9\alpha,$$

which is obviously impossible because $\gamma \geq \beta$.
Assume now that $k = 3$ and that $(a,\ b,\ c,\ d,\ e,\ f)$ is a third power diophantine sextuple and assume that $\alpha \leq \beta \leq \gamma \leq \delta \leq \epsilon \leq \phi$ are the degrees of $a,\ b,\ c,\ d,\ e,\ f$, respectively. For the third power diophantine quadruple $(a,\ b,\ c,\ d)$ inequality (18) becomes

$$\delta \leq 4\beta + \alpha - 3, \tag{25}$$

while inequality (19) becomes

$$\delta + \beta \geq 2\alpha + 2\gamma. \tag{26}$$

Thus, using (26) for the diophantine quadruples $(c,\ d,\ e,\ f)$ and $(b,\ c,\ d,\ e)$, we get

$$\phi + \delta \geq 2(\epsilon + \gamma) \geq 4(\delta + \beta),$$

or

$$\phi \geq 3\delta + 4\beta. \tag{27}$$

But using (25) for the diophantine quadruple $(a,\ b,\ c,\ f)$, we also have

$$\phi \leq 4\beta + \alpha - 3, \tag{28}$$

and now (27) and (28) imply

$$4\beta + \alpha - 3 \geq 3\delta + 4\beta,$$

or

$$\alpha - 3 \geq 3\delta,$$

which is impossible because $\delta \geq \alpha$. So, parts i-iii of the Theorem are proved. $\square$

4. A Pell-like equation in polynomials

Assume now that k is even and large enough. Write $k = 2k_0$,

$$ab + 1 = r^k, \qquad ac + 1 = s^k, \qquad bc + 1 = t^k, \tag{29}$$

with $r,\ s,\ t$ in $\mathbf{K}[X]$. Clearly, $\deg(r) = \dfrac{\alpha+\beta}{k}$, $\deg(s) = \dfrac{\alpha+\gamma}{k}$ and $\deg(t) = \dfrac{\beta+\gamma}{k}$, therefore $\deg(t) \geq \deg(s) \geq \deg(r) > 0$. Eliminating c from the second and third formula (29) above, we get

$$a(t^{k_0})^2 - b(s^{k_0})^2 = b - a. \tag{30}$$

Let $R := r^{k_0}$, $S := s^{k_0}$, and $T := t^{k_0}$. Equation (30) above implies that the equation

$$aU^2 - bV^2 = a - b, \tag{31}$$

where

$$ab + 1 = R^2 \tag{32}$$

admits a solution non-trivial solution $(U,\ V)$ (i.e. both U and V are non-constant polynomials) such that both U and V are k_0th powers of some polynomials t and s. In what follows, we take a closer look at all the solutions of equation (31) when a and b satisfy (32).

Lemma 4.

Assume that a and b are non-zero polynomials with at least of them non-constant and assume moreover that

$$ab + 1 = R^2 \tag{33}$$

holds with some polynomial R. Let $\deg(a) = \alpha$ and $\deg(b) = \beta$ and assume that $\alpha \leq \beta$. Assume moreover that $(U,\ V)$ are polynomials such that

$$aU^2 - bV^2 = a - b. \tag{34}$$

Then the following hold:

i. *ab is not the square of a polynomial.*

ii. *$U \neq 0$.*

iii. *If U is constant, then $(U,\ V) = (\pm 1,\ \pm 1)$.*

iv. *There exist $(U_0,\ V_0)$ satisfying equation (34) and such that both $\deg(U_0) \leq \dfrac{3\beta-\alpha}{4}$ and $\deg(V_0) \leq \dfrac{\alpha+\beta}{4}$ hold, and some non-negative integer m, such that up to replacing $(U,\ V)$ by $(\pm U,\ \pm V)$ the formula*

$$U\sqrt{a} + V\sqrt{b} = (U_0\sqrt{a} + V_0\sqrt{b})(R + \sqrt{ab})^m \tag{35}$$

holds.

v. *Assume that* $(U,\ V)$ *is a solution of* (34) *and that formula* (35) *holds. If* $U^2 \equiv 1 \pmod b$*, then* $V^2 \equiv 1 \pmod a$*, and the above congruence relations hold for* $(U,\ V)$ *replaced by* $(U_0,\ V_0)$ *as well. In particular, if* $(U_0,\ V_0) \neq (\pm 1,\ \pm 1)$*, then both* $\deg(U_0) \geq \dfrac{\beta}{2}$ *and* $\deg(V_0) \geq \dfrac{\alpha}{2}$ *hold.*

Proof. Part i has already been done in Lemma 1. To see part ii, notice that $U = 0$ implies $bV^2 = b - a$, which leads to $b \mid a$. Since $\beta \geq \alpha$, we conclude that $b = c_1 a$, where c_1 is some element of $\mathbf{K}$. Since $\mathbf{K}$ is algebraically closed, we get $ab = c_1 a^2 = (\sqrt{c_1} a)^2$ which contradicts i. Part iii follows for part ii as well. Indeed, if U is a constant, then $bV^2 = b - a - aU^2$ and from degree considerations we get that V is constant as well. But now $b(V^2-1) = a(U^2-1)$, and if $U^2 - 1$ is not the zero constant, then $V^2 - 1$ is not the zero constant either, and therefore we get $b = c_1 a$ with $c_1 = \dfrac{U^2-1}{V^2-1} \in \mathbf{K}$, but by part i this is impossible via the argument used to prove part ii.

To prove iv, we use an argument already employed before in a similar context in [5] (see Lemma 1 in [5]). Assume that $(U,\ V)$ is any solution of (34) and for any integer m and signs $\varepsilon_1,\ \varepsilon_2 \in \{\pm 1\}$ define

$$U^*\sqrt{a} + V^*\sqrt{b} = \varepsilon_1(U\sqrt{a} + \varepsilon_2 V\sqrt{b})(R + \sqrt{ab})^m. \tag{36}$$

For $m \geq 0$, the above relation defines, in a formal way, U^* and V^* unambiguously in terms of $U,\ V,\ a,\ b,\ R,\ m$ and the two signs ε_1 and ε_2 (the fact that this is so follows from i, because by i, ab is not a perfect square). For $m < 0$, we use the obvious fact that

$$(R + \sqrt{ab})^m = (R - \sqrt{ab})^{-m}, \tag{37}$$

which is a consequence of the fact that

$$(R + \sqrt{ab})^m \cdot (R - \sqrt{ab})^m = (R^2 - ab)^m = 1, \tag{38}$$

to also express U^* and V^* in terms of $U,\ V,\ a,\ b,\ R,\ m$ and the two signs ε_1 and ε_2. From relation (36) we also conclude that

$$U^*\sqrt{a} - V^*\sqrt{b} = \varepsilon_1(U\sqrt{a} - \varepsilon_2 V\sqrt{b})(R - \sqrt{ab})^m, \tag{39}$$

and therefore, by formula (38), and the fact that $(U,\ V)$ is a solution of (34), we conclude that

$$a(U^*)^2 - b(V^*)^2 = (U^*\sqrt{a} + V^*\sqrt{b})(U^*\sqrt{a} - V^*\sqrt{b}) =$$

$$(U\sqrt{a} + \varepsilon_2 V\sqrt{b})(U\sqrt{a} - \varepsilon_2 V\sqrt{b})(R + \sqrt{ab})^m(R - \sqrt{ab})^m = aU^2 - bV^2 = a - b,$$

therefore the pair $(U^*,\ V^*)$ satisfies equation (34) as well. Notice that by ii, U^* is never zero, and if it is a constant, then it must be ± 1.

Out of all possible pairs of solutions $(U^*,\ V^*)$ obtained by formula (36) from the starting pair $(U,\ V)$ for all possible integers m and signs $\varepsilon_1,\ \varepsilon_2$, we choose one for which $\deg(U^*)$ is minimal and we denote such a solution by $(U_0,\ V_0)$. From formula (36), we notice that

$$U\sqrt{a} + \varepsilon_2 V\sqrt{b} = \varepsilon_1(U_0\sqrt{a} + V_0\sqrt{b})(R + \sqrt{ab})^{m_0} \tag{40}$$

holds with some signs $\varepsilon_1,\ \varepsilon_2$ and some integer m_0. Changing simultaneously the signs of U and V we may assume that $\varepsilon_1 = 1$, and now by changing only the sign of V, if needed, we may assume that $\varepsilon_2 = 1$. If m_0 is negative, then relation (40) implies that

$$U\sqrt{a} - V\sqrt{b} = (U_0\sqrt{a} - V_0\sqrt{b})(R + \sqrt{ab})^{-m_0}$$

holds with $-m_0 \geq 0$. Thus, by replacing V with $-V$ and V_0 with $-V_0$ (notice that this replacement does not change the degree of V_0), we may assume that formula (35) holds with $m \geq 0$ and the pair $(U_0,\ V_0)$ for which the degree of U_0 is minimal. All is left to prove is that $\deg(U_0) \leq \frac{3\beta - \alpha}{4}$.
Let

$$U_1\sqrt{a} + V_1\sqrt{b} = (U_0\sqrt{a} + V_0\sqrt{b})(R + \sqrt{ab})$$

and

$$U_{-1}\sqrt{a} + V_{-1}\sqrt{b} = (U_0\sqrt{a} + V_0\sqrt{b})(R + \sqrt{ab})^{-1} = (U_0\sqrt{a} + V_0\sqrt{b})(R - \sqrt{ab}).$$

Then,

$$U_1 = RU_0 + bV_0 \qquad \text{and} \qquad U_{-1} = RU_0 - bV_0. \tag{41}$$

By the minimality of $\deg(U_0)$, and the fact that U^* is never zero, we get

$$\deg(U_1) \geq \deg(U_0) \qquad \deg(U_{-1}) \geq \deg(U_0), \tag{42}$$

and

$$\max(\deg(U_1),\ \deg(U_{-1})) = \deg(U_0) + \frac{\alpha + \beta}{2}.$$

By multiplying now relations (41), and using (34), and the fact that at least one of the inequalities in (42) is strict, we get

$$\deg(U_0^2) < \deg(U_1U_{-1}) = \deg(U_0^2R^2 - b^2V_0^2) =$$
$$\deg(U_0^2(ab+1) - b^2V_0^2) = \deg(b(aU_0^2 - bV_0^2) + U_0^2) =$$
$$\deg(b(a-b) + U_0^2). \tag{43}$$

But relation (43) clearly implies that $\deg(U_1) + \deg(U_{-1}) \leq \deg(b(a-b)) \leq 2\beta$. Hence,

$$2\deg(U_0) + \frac{\alpha + \beta}{2} \leq 2\beta$$

and $\deg(U_0) \leq \frac{3\beta - \alpha}{4}$.
When $V_0 = 0$, we get even a better inequality because in this case $aU_0^2 = a - b$, therefore $a \mid b$ and $U_0^2 = 1 - \frac{b}{a}$. Thus, $\deg(U_0) = \frac{\beta - \alpha}{2}$ in this case.
If $V_0 \neq 0$ is constant, then $\deg(V_0) = 0 < \frac{\alpha + \beta}{4}$. Finally, if V_0 is not constant, then by looking at the degrees of the polynomials appearing in formula (34) we get that

$$\deg(aU_0^2) = \deg(bV_0^2),$$

therefore

$$\deg(V_0) = \deg(U_0) - \frac{\beta - \alpha}{2} \leq \frac{3\beta - \alpha}{4} - \frac{\beta - \alpha}{2} = \frac{\alpha + \beta}{4},$$

which finishes the proof of iv.
For v, let us notice first that formula (34) can be written as

$$\frac{U^2 - 1}{b} = \frac{V^2 - 1}{a} \tag{44}$$

So, if $b \mid U^2-1$, it follows that the rational function appearing on the left hand side of equation (44) is, in fact, a polynomial, therefore the function appearing on the right hand side of equation (44) must be a polynomial as well. Hence $a \mid V^2-1$ when $b \mid U^2-1$. To prove the similar statement about the pair $(U_0,\ V_0)$, it suffices to show, by induction on $m \geq 0$ from formula (35), that if $b \mid U^2-1$ and

$$U\sqrt{a}+V\sqrt{b}=(U_*\sqrt{a}+V_*\sqrt{b})(R+\sqrt{ab})$$

then $b \mid U_*^2-1$ as well. But obviously,

$$U_*\sqrt{a}+V_*\sqrt{b}=(U\sqrt{a}+V\sqrt{b})(R-\sqrt{ab}),$$

therefore

$$U_*=UR-Vb,$$

and

$$U_*^2=(UR-Vb)^2=U^2R^2-2URVb+b^2V^2=U^2(ab+1)-2URVb+b^2V^2,$$

therefore

$$U_*^2 \equiv U^2 \pmod{b}. \tag{45}$$

Since $U^2 \equiv 1 \pmod{b}$, relation (45) implies that $U_*^2 \equiv 1 \pmod{b}$ as well, and the proof of v follows by induction on m. Hence, if $b \mid U^2-1$, then $b \mid U_0^2-1$. In particular, if U_0 is not constant (i.e., not ± 1), then U_0^2-1 is non-zero and a multiple of b, therefore $2\deg(U_0)=\deg(U_0^2-1) \geq \beta$. The statement about $\deg(V_0)$ being at least $\dfrac{\alpha}{2}$ when $a \mid V_0^2-1$ and V_0 is not ± 1 is obtained in a similar way. Lemma 4 is therefore proved. $\square$

Assume now that (a,b,c) is a kth power diophantine triple. Then $(U,\ V)=(t^{k_0},\ s^{k_0})$ is a solution of equation (34). Let $(U_0,\ V_0)$ be a solution of equation (34) arising from the solution $(U,\ V)$ as explained in the proof of Lemma 4, and with U_0 of minimal possible degree. Then, by Lemma 4, we have $\deg(U_0) \leq \dfrac{3\beta-\alpha}{4}$ and $\deg(V_0) \leq \dfrac{\alpha+\beta}{4}$, and if $V_0=0$, then $\deg(U_0)=\dfrac{\beta-\alpha}{2}$. Let $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$ be the sequences of polynomials given by

$$U_n\sqrt{a}+V_n\sqrt{b}=(U_0\sqrt{a}+V_0\sqrt{b})(R+\sqrt{ab})^n. \tag{46}$$

It is easy to see that both $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$ are binary recurrent sequences satisfying

$$U_1=RU_0+bV_0 \quad \text{and} \quad V_1=U_0a+V_0b, \tag{47}$$

$$U_{n+2}=2RU_{n+1}-U_n \quad \text{and} \quad V_{n+2}=2RV_{n+1}-V_n \quad \text{for all } n \geq 0. \tag{48}$$

In what follows, we will gather some more of the properties of the sequences $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$.

Lemma 5. *Let the sequences (U_n) and (V_n) be defined by (48), and let $m \geq 0$ be an integer such that $(t^{k_0},\ s^{k_0})=(U_m,\ V_m)$. Then:*

i. $U_n^2 \equiv 1 \pmod{b}$ *and* $V_n^2 \equiv 1 \pmod{a}$ *for all $n \geq 0$. In particular, if $(U_0,\ V_0) \neq (\pm 1,\ \pm 1)$, then* $\deg(U_0) \geq \dfrac{\beta}{2}$ *and* $\deg(V_0) \geq \dfrac{\alpha}{2}$.

ii. $m \geq 1$.

iii. $\deg(U_1) \geq \max(\deg(U_0),\ \beta/2)$, $\deg(V_1) \geq \max(\deg(V_0),\ \alpha/2)$.

iv. *The relations*

$$\deg(U_n)=(n-1)\frac{\alpha+\beta}{2}+\deg(U_1), \tag{49}$$

$$\deg(V_n) = (n-1)\frac{\alpha+\beta}{2} + \deg(V_1), \tag{50}$$

hold for all $n \geq 1$ and

$$2\deg(U_n) + \alpha = 2\deg(V_n) + \beta \tag{51}$$

holds for all $n \geq 1$ as well and even for $n = 0$ except for the case in which $(U_0,\ V_0) = (\pm 1,\ \pm 1)$.

Proof. For part i, notice that since $bc + 1 = t^k = U_m^2$, it follows that $b \mid U_m^2 - 1$, and now, by v of Lemma 4, it follows that $b \mid U_0^2 - 1$. One may now use induction of n to show that this divisibility relation holds for all $n \geq 0$. Thus, by v of Lemma 4 again, $b \mid U_n^2 - 1$ and $a \mid V_n^2 - 1$ hold for all $n \geq 0$. The remaining assertions of part i follow from part v of Lemma 4.
For part ii, notice that since $U_m^2 = t^k = bc + 1$, it follows that $2\deg(U_m) = \beta + \gamma \geq 2\beta$, therefore $\deg(U_m) \geq \beta$. Since by iv of Lemma 4, $\deg(U_0) \leq \dfrac{3\beta - \alpha}{4} < \beta$, it follows that $m = 0$ is impossible, therefore $m \geq 1$.
For part iii, notice first of all that the fact that $\deg(U_1) \geq \deg(U_0)$ follows from the fact that U_0 has been chosen to have minimal degree. If $\deg(U_1) = 0$, then both U_1 and U_0 are constants, therefore $U_1 = U_0 = \pm 1$. In particular, $V_1 = V_0 = \pm 1$. But

$$U_1 = RU_0 + bV_0$$

therefore

$$\pm R = \pm 1 \pm b$$

and

$$ab + 1 = R^2 = (\pm 1 \pm b)^2 = b^2 \pm 2b + 1,$$

or

$$a = b \pm 2.$$

By simultaneously changing the signs of all three $(a,\ b,\ c)$, if needed, we may assume that $b = a + 2$, therefore $\alpha = \beta > 0$, and now relation (30) becomes

$$at^k - (a+2)s^k = -2. \tag{52}$$

In particular, t and s have the same degree $\deg(t) = \deg(s) = \dfrac{\alpha+\gamma}{k}$, and no common root. Applying Mason's theorem to the equation (52) we obtain

$$(k-2)(\alpha+\gamma) \leq k\alpha - k.$$

Thus

$$2(k-2)\alpha \leq (k-2)(\alpha+\gamma) \leq k\alpha - k,$$

or

$$(k-4)\alpha \leq -k,$$

which is impossible for $k \geq 4$. Thus, we have shown that $\deg U_1 > 0$, therefore $\deg(U_1) \geq \max(\deg(U_0),\ \beta/2)$. To prove the similar relation for the degree of V_1, notice first that $V_1 \neq \pm 1$. Indeed, for if $V_1 = \pm 1$, then $U_1 = \pm 1$, which is a contradiction. So, $V_1 \neq \pm 1$ and we get that $\deg(V_1) \geq \dfrac{\alpha}{2}$. To prove that $\deg(V_1) \geq \deg(V_0)$, we first show that $V_1 \neq 0$. Indeed, for if $V_1 = 0$, then the relation

$$U_0\sqrt{a} + V_0\sqrt{b} = (U_1\sqrt{a} + V_1\sqrt{b})(R - \sqrt{ab})$$

with $V_1 = 0$ gives $U_0 = U_1 R$, contradicting the fact that $\deg(R) > 0$ and $\deg(U_1) \geq \deg(U_0)$. Finally, assume that $V_1 \neq 0,\ \pm 1$. From the relation

$$a(U_1^2 - 1) = b(V_1^2 - 1)$$

we get

$$2\deg(U_1) + \alpha = 2\deg(V_1) + \beta. \tag{53}$$

If $V_0 = \pm 1$, then obviously $\deg(V_0) = 0 \leq \deg(V_1)$. Finally, if $V_0 \neq \pm 1$, then from the relation

$$a(U_0^2 - 1) = b(V_0^2 - 1), \tag{54}$$

we also get

$$2\deg(U_0) + \alpha = 2\deg(V_0) + \beta. \tag{55}$$

Finally, (53), (55), and the fact that $\deg(U_1) \geq \deg(U_0)$ imply that $\deg(V_1) \geq \deg(V_0)$. This completes the proof of part iii.

For part iv, notice that by recurrence formulae (48), the fact that $\deg(R) = \dfrac{\alpha+\beta}{2}$, and the fact that $\deg(U_1) \geq \deg(U_0)$ and $\deg(V_1) \geq \deg(V_0)$, we get, by induction on n, that $\deg(U_{n+1}) > \deg(U_n)$ and $\deg(V_{n+1}) > \deg(V_n)$ hold for all $n \geq 1$, and that

$$\deg(U_{n+2}) = \deg(R) + \deg(U_{n+1}) \quad \text{and} \quad \deg(V_{n+2}) = \deg(R) + \deg(V_{n+1}) \tag{56}$$

hold for all $n \geq 0$. Obviously, relations (56) imply (49) and (50). Finally, relation (51) follows from identifying degrees in the formula

$$a(U_n^2 - 1) = b(V_n^2 - 1).$$

Lemma 5 is therefore proved. $\square$

We now have sufficient information of the sequences $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$ to be able to complete the proof of our Theorem.

5. The proof of the Theorem: Part iv

Let $m \geq 1$ and recall that $U_m = t^{k_0}$, $V_m = s^{k_0}$, and $R = r^{k_0}$. Here, $m \geq 1$ by Lemma 5. By the same Lemma 5, we have

$$\frac{\beta+\gamma}{2} = k_0\deg(t) = \deg(U_m) = (m-1)\frac{\alpha+\beta}{2} + \deg(U_1)$$

and

$$\frac{\alpha+\gamma}{2} = k_0\deg(s) = \deg(V_m) = (m-1)\frac{\alpha+\beta}{2} + \deg(V_1),$$

therefore

$$\frac{\alpha+2\beta+\gamma}{2k_0} = \deg(ts) = \deg(t) + \deg(s) = \frac{1}{k_0}((m-1)(\alpha+\beta) + \deg(U_1) + \deg(V_1)). \tag{57}$$

However, by Lemma 2, we have

$$(2k_0 - 2)\gamma \leq (2k_0 + 1)\beta + \alpha - 2k_0,$$

and it is easy to see that the above inequality implies

$$\Big(\frac{k_0-1}{2k_0}\Big)(\alpha+2\beta+\gamma) \le (\alpha+3\beta)\Big(\frac{1}{2}-\frac{1}{4k_0}\Big)-\frac{1}{2} < \frac{\alpha+3\beta}{2}. \tag{58}$$

The combination of (57) with (58) gives

$$\Big(\frac{k_0-1}{k_0}\Big)((m-1)(\alpha+\beta)+\deg(U_1)+\deg(V_1)) < \frac{\alpha+3\beta}{2}. \tag{59}$$

Relation (59) obviously implies that $m \le 2$ for $k_0 \ge 3$ (i.e., $k \ge 6$). Indeed, if $k_0 \ge 3$, and $m \ge 3$ then

$$\Big(\frac{k_0-1}{k_0}\Big)((m-1)(\alpha+\beta)+\deg(U_1)+\deg(V_1)) \ge \frac{2}{3}\cdot\Big(2(\alpha+\beta)+\frac{\beta}{2}+\frac{\alpha}{2}\Big) = \frac{5}{3}(\alpha+\beta),$$

therefore inequality (59) would be

$$\frac{5}{3}(\alpha+\beta) < \frac{\alpha+3\beta}{2},$$

therefore

$$10\alpha+10\beta < 3\alpha+9\beta, \tag{60}$$

which is obviously impossible. Thus, $m \le 2$. We now want to eliminate the case $m = 2$. What we do, we show that the case $m = 2$ is possible only when $(U_0,\ V_0) = (\pm 1,\ \pm 1)$. Assume first that $\alpha = \beta$ and $m = 2$. Then, since $\deg(U_1) \ge \beta/2$ and $\deg(V_1) \ge \alpha/2$, we get $\deg(U_1)+\deg(V_1) \ge \beta$. Now inequality (59) with $k_0 \ge 3$ implies

$$2\beta = \frac{2}{3}((\alpha+\beta)+\beta) \le \frac{k_0-1}{k_0}\cdot((m-1)(\alpha+\beta)+\deg(U_1)+\deg(V_1)) < \frac{\alpha+3\beta}{2} = 2\beta,$$

which is a contradiction. So $\alpha < \beta$.
Assume now that $(U_0,\ V_0) \ne (\pm 1,\ \pm 1)$. Since

$$U_1 = RU_0 + bV_0,$$

it follows that either

$$\deg(U_1) = \frac{\alpha+\beta}{2} + \deg(U_0), \tag{61}$$

or

$$\deg(U_1) < \frac{\alpha+\beta}{2} + \deg(U_0). \tag{62}$$

We treat the first instance. In this case,

$$\deg(V_1) = \frac{\alpha+\beta}{2} + \deg(V_0),$$

therefore

$$\deg(U_1)+\deg(V_1) = \alpha+\beta+\deg(U_0)+\deg(V_0).$$

Since $(U_0,\ V_0) \ne (\pm 1,\ \pm 1)$, we get that

$$\deg(U_0)+\deg(V_0) \ge \frac{\alpha+\beta}{2},$$

therefore

$$\deg(U_1) + \deg(V_1) \geq \frac{3(\alpha+\beta)}{2}.$$

Thus, inequality (59) implies that

$$\frac{5}{3}(\alpha+\beta) = \frac{2}{3} \cdot \Big((\alpha+\beta) + \frac{3}{2}(\alpha+\beta)\Big) \leq \frac{k_0-1}{k_0} \cdot ((m-1)(\alpha+\beta) + \deg(U_1) + \deg(V_1)) <$$

$$\frac{\alpha+3\beta}{2},$$

and we get again inequality (60), which is impossible. We now treat the second instance. For this, we will assume that $k_0 \geq 4$ (i.e., that $k \geq 8$). From $\alpha < \beta$,

$$U_1(U_0R - bV_0) = U_0^2R^2 - b^2V_0^2 = (ab+1)U_0^2 - b^2V_0^2 = b(aU_0^2 - bV_0^2) + U_0^2 = b(a-b) + U_0^2,$$

inequality (62), and the fact that $\deg(U_0) < \beta$, we get

$$\deg(U_1) + \frac{\alpha+\beta}{2} + \deg(U_0) = 2\beta,$$

therefore

$$\deg(U_1) = \frac{3\beta-\alpha}{2} - \deg(U_0).$$

Since

$$\deg(V_1) = \deg(U_1) + \frac{\alpha-\beta}{2},$$

we get

$$\deg(U_1) + \deg(V_1) = 2\deg(U_1) + \frac{\alpha-\beta}{2} = 3\beta - \alpha + \frac{\alpha-\beta}{2} - 2\deg(U_0) = \frac{5\beta-\alpha}{2} - 2\deg(U_0).$$

Thus, inequality (59) with $k_0 \geq 4$ tells us that

$$\frac{3}{4} \cdot \Big((\alpha+\beta) + \frac{5\beta-\alpha}{2} - 2\deg(U_0)\Big) < \frac{\alpha+3\beta}{2},$$

or

$$\frac{21\beta+3\alpha}{8} - \frac{\alpha+3\beta}{2} < \frac{3}{2}\deg(U_0),$$

or

$$\deg(U_0) > \frac{9\beta-\alpha}{12}. \tag{63}$$

On the other hand, by Lemma 4 we have $\deg(U_0) \leq \dfrac{3\beta-\alpha}{4}$, which is obviously in contradiction with (62).

The conclusion so far is that either $m = 2$ in which case $(U_0,\ V_0) = (\pm 1,\ \pm 1)$ must hold, or $m = 1$.

The Case $m = 2$. In this case, by simultaneously changing the signs of both U_0 and V_0, we may assume that $U_0 = 1$. Thus, $V_0 = \pm 1$. We write

$$t^{k_0}\sqrt{a} + s^{k_0}\sqrt{b} = U_2 = (\sqrt{a} \pm \sqrt{b})(R + \sqrt{ab})^2 = (2ab + 1 \pm 2Rb)\sqrt{a} + (2ab + 1 \pm 2Ra)\sqrt{b}, \tag{64}$$

therefore

$$\begin{cases} t^{k_0} = 2r^{2k_0} - 1 \pm 2r^{k_0}b, \\ s^{k_0} = 2r^{2k_0} - 1 \pm 2r^{k_0}a, \end{cases} \tag{65}$$

Clearly s and t are coprime, because if not, U_2 and V_2 will have a non-trivial common divisor which, by an argument employed earlier, should also be a common divisor of both U_0 and V_0, which is impossible because $U_0 = V_0 = 1$. From (65), we get

$$2r^{k_0}(b-a) = t^{k_0} - s^{k_0}. \tag{66}$$

With (66) and Mason's theorem, we get

$$\max(\deg((b-a)r^{k_0},\ t^{k_0},\ s^{k_0})) \leq N((b-a)rst) - 1. \tag{67}$$

Identifying degrees, we get that the only relevant inequality from (67) is

$$\deg((b-a)r^{k_0}) = \deg(b-a) + \frac{\alpha+\beta}{2} \leq N((b-a)rst) - 1 \leq \deg(b-a) + \frac{\alpha+\beta+\gamma}{k_0} - 1.$$

If $\alpha < \beta$, then (65) implies $\dfrac{\beta+\gamma}{2} = \dfrac{\alpha+\beta}{2} + \beta$ and $\gamma = 2\beta + \alpha$. On the other hand, Lemma 2 for $k_0 \geq 3$ implies $\gamma < \dfrac{k_0+1}{k_0-1}\,\beta \leq 2\beta$, a contradiction. Therefore, we may assume that $\alpha = \beta$. But now we have

$$\alpha < \frac{2\alpha+\gamma}{k_0},$$

which implies

$$\gamma > (k_0 - 2)\alpha. \tag{68}$$

But for $k_0 \geq 4$, Lemma 2 implies $\gamma < \dfrac{5}{3}\,\alpha$, which clearly contradicts (68).

The Case $m = 1$. In this case, we get $U_1 = t^{k_0},\ V_1 = s^{k_0}$, and since

$$U_1\sqrt{a} + V_1\sqrt{b} = (U_0\sqrt{a} + V_0\sqrt{b})(R + \sqrt{ab}),$$

we also have

$$U_0\sqrt{a} + V_0\sqrt{b} = (U_1\sqrt{a} + V_1\sqrt{b})(R + \sqrt{ab})^{-1} = (U_1\sqrt{a} + V_1\sqrt{b})(R - \sqrt{ab}),$$

and we read

$$U_0 = RU_1 - bV_1 \qquad \text{and} \qquad V_0 = RV_1 - aU_1, \tag{69}$$

or

$$U_0 = (rt)^{k_0} - bs^{k_0} \qquad \text{and} \qquad V_0 = (rs)^{k_0} - at^{k_0} \tag{70}$$

We look at the second relation (69). Notice that since $R^2 = 1 + ab$ and $V_1^2 = 1 + ac$, it follows that RV_1 and a are coprime. So, if RV_1 and aU_1 are not coprime, then their greatest common divisor will be exactly the greatest common divisor of RV_1 and U_1. The greatest common divisor of U_1 and V_1 is the same as the greatest common divisor of U_0 and V_0. Let this divisor be $\Lambda_1 = \lambda_1^{k_0}$.

Finally, let Λ_2 be the greatest common divisor of U_1/Λ_1 and R. In particular, $\Lambda_2 = \lambda_2^{k_0}$ (because both R and $U_1/\Lambda_1 = (t/\lambda_1)^{k_0}$ are k_0th powers). We may thus write the second relation (70) as

$$\frac{V_0}{(\lambda_1\lambda_2)^{k_0}} = \Big(\frac{r}{\lambda_2}\Big)^{k_0} \cdot \Big(\frac{s}{\lambda_1}\Big)^{k_0} - a\Big(\frac{t}{\lambda_1\lambda_2}\Big)^{k_0}. \tag{71}$$

The polynomials appearing in (71) are all coprime. In order to apply Mason's theorem, it suffices to show that they are all non-zero and that they are not all constant. We shall first treat the case in which one of them is zero. In this case, since $U_1 \neq 0$ and $V_1 \neq 0$ (see Lemmas 4 and 5), we get $V_0 = 0$, therefore $RV_1 = aU_1$. But we have just said that both R and V_1 are coprime to a which leaves us with the case in which a is constant. With a constant and $V_0 = 0$, we get

$$a - b = aU_0^2,$$

therefore

$$b = aU_0^2 - a.$$

In particular, we get that $\deg(U_0) = \beta/2$, and that

$$r^k = R^2 = ab + 1 = a(aU_0^2 - a) + 1 = (aU_0)^2 + (1 - a^2),$$

and since the degrees of U_0 and R are positive, the above relation gives, via Lemma 1, $a = \pm 1$. Now we have $R^2 = U_0^2 = V_1^2$ (the last equality here follows from $V_1 = RV_0 + aU_0$, with $a = \pm 1$ and $V_0 = 0$). Hence, $ab + 1 = ac + 1$, therefore $b = c$, a contradiction.

So, we know that all polynomials appearing in formula (71) are non-zero. Let us deal with the case in which they are all constant. In this case, a is a constant and s/λ_1 is a constant. In particular, V_1/Λ_1 is a constant, and since $\Lambda_1 = \gcd(U_1,\ V_1) = \gcd(U_0,\ V_0)$, and $\deg(V_1) \geq \deg(V_0)$ we get that V_0/Λ_1 is constant. Relation (71) now shows that Λ_2 is constant, and since R/Λ_2 is also constant, we now get that R is constant, which contradicts the fact that $\deg(R) > 0$. Since we took care of the degenerate instance, we may apply Mason's theorem to relation (71) to conclude that

$$\deg\Big(a\Big(\frac{t}{\lambda_1\lambda_2}\Big)^{k_0}\Big) = \alpha + \frac{\beta+\gamma}{2} - k_0(\deg(\lambda_1) + \deg(\lambda_2)) <$$

$$\alpha + \deg(V_0) - k_0(\deg(\lambda_1) + \deg(\lambda_2)) + \frac{\alpha+\beta+\gamma}{k_0} - 2(\deg(\lambda_1) + \deg(\lambda_2)),$$

or

$$\frac{\beta+\gamma}{2} < \deg(V_0) + \frac{\alpha+\beta+\gamma}{k_0}. \tag{72}$$

If $V_0 = \pm 1$, we then get

$$(k_0 - 2)(\beta + \gamma) < 2\alpha$$

which is impossible for $k_0 \geq 3$. So, we may assume that $V_0 \neq \pm 1$, therefore $U_0 \neq \pm 1$ and the relation

$$\deg(U_0) - \deg(V_0) = \frac{\beta - \alpha}{2}. \tag{73}$$

holds. Inequality (72) and relation (73) give us

$$\frac{\beta+\gamma}{2} < \deg(U_0) + \frac{\alpha-\beta}{2} + \frac{\alpha+\beta+\gamma}{k_0}. \tag{74}$$

From the formula

$$U_1 = RU_0 + bV_0$$

it follows that

$$\frac{\beta+\gamma}{2} = \deg(U_1) \leq \deg(U_0) + \frac{\alpha+\beta}{2}. \tag{75}$$

If (75) holds with equality, then

$$\frac{\beta+\gamma}{2} = \deg(U_0) + \frac{\alpha+\beta}{2},$$

and with (74) we get

$$\deg(U_0) + \frac{\alpha+\beta}{2} < \deg(U_0) + \frac{\alpha-\beta}{2} + \frac{\alpha+\beta+\gamma}{k_0},$$

therefore

$$\beta < \frac{\alpha+\beta+\gamma}{k_0},$$

or

$$(k_0-1)\beta < \alpha+\gamma \leq \beta+\gamma,$$

or

$$(k_0-2)\beta < \gamma. \tag{76}$$

It is clear that (76) contradicts Lemma 2 for $k_0 \geq 4$.

Assume now that (75) holds with strict inequality. Then, since

$U_1(U_0R - bV_0) = (U_0R + bV_0)(U_0R - bV_0) = (R^2U_0^2 - b^2V_0^2) = ((ab+1)U_0^2 - b^2V_0^2) = b(b-a) + U_0^2$,

we get

$$\deg(U_1) + \frac{\alpha+\beta}{2} + \deg(U_0) = \beta + \deg(b-a) \leq 2\beta,$$

therefore

$$\deg(U_1) \leq \frac{3\beta-\alpha}{2} - \deg(U_0).$$

By Lemma 5, we have

$$\frac{\beta}{2} \leq \deg(U_0) \leq \frac{3\beta-\alpha}{2} - \frac{\beta+\gamma}{2} = \frac{2\beta-\alpha-\gamma}{2},$$

which implies $\alpha+\gamma \leq \beta$, and this is possible only if $\alpha = 0$ and $\beta = \gamma$. But now (72), together with

$$\deg(V_0) \leq \frac{\alpha+\beta}{4} = \frac{\beta}{4},$$

leads to

$$\beta < \frac{\beta}{4} + \frac{2\beta}{k_0},$$

which gives a contradiction for $k_0 \geq 3$.

This finishes the proof of the last assertion of the Theorem. □

Acknowledgement

This paper was written when we both attended the workshop "Effective Methods for Diophantine Equations" in Debrecen, Hungary, October, 2001. We thank the organizers for giving us the opportunity to participate in this workshop. We also thank the referee for valuable suggestions.

References

[1] A. Baker, 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] Y. Bugeaud, A. Dujella, *A problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc., to appear.

[3] L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Chelsea, New York, 1966.

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

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

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

[7] A. Dujella, A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), 291–306.

[8] P. Gibbs, *Some rational sextuples*, preprint, math.NT/9902081.

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

[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 on a problem of Diophantus and Davenport*, Fibonacci Quart. **16** (1978), 155–165.

[12] R. C. Mason, *Equations over function fields*, Lecture Notes in Math. **1068**, Springer, Berlin, 1984, pp. 149–157.

[13] W. W. Stothers, *Polynomial identities and Hauptmoduln*, Quart. J. Math. Oxford Ser. (2) **32** (1981), 349–370.

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

Florian Luca
Mathematical Institute of the UNAM
Campus Morelia
Ap. Postal 61-3 (Xangari)
CP 58 089
Morelia, Michoacán
MEXICO
e-mail: fluca@matmor.unam.mx