Generalization of a theorem of Baker and Davenport

Andrej Dujella (Zagreb) and Attila Pethő*(Debrecen)

1 Introduction

The Greek mathematician Diophantus of Alexandria noted that the rational numbers $\frac{1}{16}$, $\frac{33}{16}$, $\frac{17}{4}$ and $\frac{105}{16}$ have the following property: the product of any two of them increased by 1 is a square of a rational number (see [4]). The first set of four positive integers with the above property was found by Fermat, and it was $\{1, 3, 8, 120\}$. A set of positive integers $\{a_1, a_2, \ldots, a_m\}$ is said to have *the property of Diophantus* if $a_i a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$. Such a set is called *a Diophantine m-tuple* (or P_1-set of size m). In 1969, Baker and Davenport [2] proved that if d is a positive integer such that $\{1, 3, 8, d\}$ is a Diophantine quadruple, then d has to be 120. The same result was proved by Kanagasabapathy and Ponnudurai [9], Sansone [12] and Grinstead [7]. This result implies that the Diophantine triple $\{1, 3, 8\}$ cannot be extended to a Diophantine quintuple.

In the present paper we generalize the result of Baker and Davenport and prove that the Diophantine pair $\{1, 3\}$ can be extended to infinitely many Diophantine quadruples, but it cannot be extended to a Diophantine quintuple.

The first part of this assertion is easy. Of course let $\{1, 3, c\}$ be a Diophantine triple, then from [8, Theorem 8] it follows that there exists $k \geq 1$ such that

$$c = c_k = \frac{1}{6}[(2+\sqrt{3})(7+4\sqrt{3})^k + (2-\sqrt{3})(7-4\sqrt{3})^k - 4]$$

and it is easy to check that $\{1, 3, c_k, c_{k-1}\}$ and $\{1, 3, c_k, c_{k+1}\}$ are Diophantine quadruples provided $k \geq 2$. We have: $c_0 = 0$, $c_1 = 8$, $c_2 = 120$, $c_3 = 1680$, $\ldots$. Now we formulate our main results.

Theorem 1 *Let k be a positive integer. If d is an integer such that there exist integers x, y, z with the property*

$$d + 1 = x^2, \quad 3d + 1 = y^2, \quad c_k d + 1 = z^2, \tag{1}$$

then $d \in \{0, c_{k-1}, c_{k+1}\}$.

[1]Research partially supported by Hungarian National Foundation for Scientific Research Grants No. 16791 and 16975

From Theorem 1 we obtain the following corollaries immediately.

Corollary 1 *The Diophantine pair* $\{1,3\}$ *cannot be extended to a Diophantine quintuple.*

Corollary 2 *Let* $0 < l < k$ *and* z *be integers such that*

$$c_l c_k + 1 = z^2$$

then $l = k - 1$.

Remark 1 The statement of Theorem 1 for $k = 1$ is just Baker-Davenport's result, and the case $k = 2$ is proved recently by Kedlaya [10].

Let k be the minimal positive integer, if such exists, for which the statement of Theorem 1 is not valid. Then $k \geq 3$ and we begin our proof by proving that $k \leq 75$.

Proposition 1 *If Theorem* 1 *is true for* $1 \leq k \leq 75$*, then it holds for all positive integers* k.

The proof of Proposition 1 is divided into several parts. In Section 2 we consider the equations (1) separately and prove for any fixed k that their solutions belong to the union of the set of members of finitely many linear recurrence sequences. In Section 3 we first localize the initial terms of the recurrence sequences defined previously provided that the system of equations (1) is soluble. Here we use congruence conditions modulo $c = c_k$. In the second step we consider the remaining sequences modulo c^2 and rule out all but two equations in terms of linear recurrence sequences. This ends the formal-algebraic part of the paper.

The most essential step toward the proof of Theorem 1 is contained in Section 4. Here we transform the exponential equations into inequalities for linear forms in three logarithms of algebraic numbers, which depend on the parameter k. A smooth application of the theorem of Baker and Wüstholz [3] finishes the proof of Proposition 1.

Finally in Section 5 we prove Theorem 1 for $2 \leq k \leq 75$ by using a version of the reduction procedure due to Baker and Davenport [2].

2 Preliminaries

The system (1) is equivalent to the system of Pell equations:

$$z^2 - c_k x^2 = 1 - c_k\,, \quad (2)$$

$$3z^2 - c_k y^2 = 3 - c_k\,. \quad (3)$$

From the definition of c_k it follows that there exist integers s_k and t_k such that

$$\begin{aligned} c_k + 1 &= s_k^2\,, \\ 3c_k + 1 &= t_k^2\,. \end{aligned}$$

Thus neither c_k nor $3c_k$ is a square and both $\mathbf{Q}(\sqrt{c_k})$ and $\mathbf{Q}(\sqrt{3c_k})$ are real quadratic number fields. Moreover $s_k + \sqrt{c_k}$ and $t_k + \sqrt{3c_k}$ are non-trivial units of norm 1 in the number rings $\mathbf{Z}[\sqrt{c_k}]$ and $\mathbf{Z}[\sqrt{3c_k}]$ respectively. Thus there is a finite set $\{z_0^{(i)} + x_0^{(i)}\sqrt{c_k},\ i = 1, \ldots, i_0\}$ of elements of $\mathbf{Z}[\sqrt{c_k}]$ such that if (z, x) is any solution of (2) in integers then

$$z + x\sqrt{c} = (z_0^{(i)} + x_0^{(i)}\sqrt{c})(s + \sqrt{c})^m$$

for some index i and integer m. In this case, $z = v_m^{(i)}$ for some m, where the sequence $\{v_m^{(i)}\}$ is defined by the recursion

$$v_0^{(i)} = z_0^{(i)}, \quad v_1^{(i)} = sz_0^{(i)} + cx_0^{(i)}, \quad v_{m+2}^{(i)} = 2sv_{m+1}^{(i)} - v_m^{(i)}.$$

For simplicity, we have omitted here the index k and will continue to do so. We call the set $\{z_0^{(i)} + x_0^{(i)}\sqrt{c},\ i = 1, \ldots, i_0\}$ of solutions of $z^2 - cx^2 = 1 - c$ fundamental if we choose representatives so that the $|z_0^{(i)}|$ are minimal.

Similarly, all solutions of (3) are given by

$$z\sqrt{3} + y\sqrt{c} = (z_1^{(j)}\sqrt{3} + y_1^{(j)}\sqrt{c})(t + \sqrt{3c})^n, \quad j = 1, \ldots, j_0,$$

or by $z = w_n^{(j)}$ for some j and n, where the sequence $\{w_n^{(j)}\}$ is defined by the recursion

$$w_0^{(j)} = z_1^{(j)}, \quad w_1^{(j)} = tz_1^{(j)} + cy_1^{(j)}, \quad w_{n+2}^{(j)} = 2tw_{n+1}^{(j)} - w_n^{(j)}.$$

Here the elements $z_1^{(j)}\sqrt{3} + y_1^{(j)}\sqrt{c}$ are fundamental solutions of equation (3). In this way we reformulated the system of equations (1) to finitely many diophantine equations of form

$$v_m^{(i)} = w_n^{(j)}$$

in integers $1 \le i \le i_0, 1 \le j \le j_0, m$ and n.

By [11, Theorem 108a] we have the following estimates for the fundamental solutions of (2) and (3):

$$0 \le |z_0^{(i)}| \le \sqrt{\frac{1}{2}(s-1)(c-1)} < \sqrt{\frac{c\sqrt{c}}{2}} < \frac{c}{4}\,, \tag{4}$$

$$0 < x_0^{(i)} \le \sqrt{\frac{c-1}{2(s-1)}} < \sqrt{\frac{c(s+1)}{2c}} < \sqrt{\frac{\sqrt{c}+2}{2}}\,, \tag{5}$$

$$0 \le |z_1^{(j)}| \le \frac{1}{3}\sqrt{\frac{3}{2}(t-1)(c-3)} < \sqrt{\frac{c\sqrt{c}}{2\sqrt{3}}} < \frac{c}{6}\,, \tag{6}$$

$$0 < y_1^{(j)} \le \sqrt{\frac{3(c-3)}{2(t-1)}} < \sqrt{\frac{c(t+1)}{2c}} < \sqrt{\frac{\sqrt{3c}+2}{2}}\,. \tag{7}$$

3 Application of congruence relations

Let a mod b denote the least non-negative residue of the integer a modulo the integer b and consider the sequences ($v_m^{(i)}$ mod c) and ($w_n^{(j)}$ mod c). We have:

$$v_2^{(i)} \equiv (2s^2-1)z_0^{(i)} = (2c+1)z_0^{(i)} \equiv v_0^{(i)} \pmod{c}, \quad v_3^{(i)} \equiv sz_0^{(i)} \equiv v_1^{(i)} \pmod{c}.$$

Therefore, $v_{2m}^{(i)} \equiv z_0^{(i)} \pmod{c}$ and $v_{2m+1}^{(i)} \equiv sz_0^{(i)} \pmod{c}$, for all $m \ge 0$. Furthermore,

$$w_2^{(j)} \equiv (2t^2-1)z_1^{(j)} = (6c+1)z_1^{(j)} \equiv w_0^{(j)} \pmod{c}, \quad w_3^{(j)} \equiv tz_1^{(j)} \equiv w_1^{(j)} \pmod{c}.$$

Therefore, $w_{2n}^{(j)} \equiv z_1^{(j)} \pmod{c}$ and $w_{2n+1}^{(i)} \equiv tz_1^{(j)} \pmod{c}$, for all $n \ge 0$. In the following lemma we prove that if (1) has a non-trivial solution then the initial terms of the sequences $v^{(i)}$ and $w^{(j)}$ are restricted.

LEMMA 1 *Let $k \ge 2$ be the smallest positive integer for which the assertion of Theorem 1 is not true. Let $1 \le i \le i_0, 1 \le j \le j_0$ and $v^{(i)}, w^{(j)}$ be the sequences defined in Section 2. Then*

1° *If the equation $v_{2m}^{(i)} = w_{2n}^{(j)}$ has a solution, then $v_0^{(i)} = z_0^{(i)} = z_1^{(j)} = w_0^{(j)} = \pm 1$.*

2° *If the equation $v_{2m+1}^{(i)} = w_{2n}^{(j)}$ has a solution, then $z_0^{(i)} = \pm 1$ and $z_1^{(j)} = sz_0^{(i)} = \pm s$.*

3° *If the equation $v_{2m}^{(i)} = w_{2n+1}^{(j)}$ has a solution, then $z_0^{(i)} = \pm t$ and $z_1^{(j)} = z_0^{(i)}/t = \pm 1$.*

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

Proof. **1°** We have $z_0^{(i)} \equiv z_1^{(j)} \pmod{c}$. From (4) and (6) we obtain $z_0^{(i)} = z_1^{(j)}$. Let $d_0 = [(z_1^{(j)})^2 - 1]/c$. Then d_0 satisfies system (1). We compare d_0 with c_{k-1}: certainly $c_{k-1} \ge c_k/15$, and

$$d_0 < \frac{1}{c} \cdot \frac{c\sqrt{c}}{2\sqrt{3}} = \frac{\sqrt{c}}{2\sqrt{3}} < 0.027c\,.$$

Hence, $d_0 < c_{k-1}$, and from the minimality of k it follows that $d_0 = 0$. Thus, $|z_1^{(j)}| = 1$ and we have: $z_0^{(i)} = z_1^{(j)} = 1$ or $z_0^{(i)} = z_1^{(j)} = -1$.

2° We have $sz_0^{(i)} \equiv z_1^{(j)} \pmod{c}$. If $z_0^{(i)} = \pm 1$, then as $c - s > c/2$ inequality (6) implies that $z_1^{(j)} = sz_0^{(i)} = \pm s$. Assume $|z_0^{(i)}| \geq 2$. Then $x_0^{(i)} \geq 2$ and we have $|z_0^{(i)}| \geq t$. Let us consider the number $cx_0^{(i)} - s|z_0^{(i)}|$. We have

$$cx_0^{(i)} - s|z_0^{(i)}| = \frac{c^2(x_0^{(i)})^2 - s^2(z_0^{(i)})^2}{cx_0^{(i)} + s|z_0^{(i)}|} = \frac{c^2 - c(x_0^{(i)})^2 - 1}{cx_0^{(i)} + s|z_0^{(i)}|} < \frac{c^2}{2c + c\sqrt{3}} < \frac{c}{3}\,.$$

Furthermore,

$$\begin{aligned} c^2 - c(x_0^{(i)})^2 - 1 \;&\geq\; c^2 - \frac{c(\sqrt{c}+2)}{2} - 1 > 0.94c^2, \\ cx_0^{(i)} + s|z_0^{(i)}| \;&\leq\; c\sqrt{\frac{\sqrt{c}+2}{2}} + \sqrt{c+1}\sqrt{\frac{c\sqrt{c}}{2}} < 1.48c\sqrt[4]{c}, \end{aligned}$$

and so

$$cx_0^{(i)} - s|z_0^{(i)}| > 0.63\sqrt{c\sqrt{c}} > \sqrt{\frac{c\sqrt{c}}{2\sqrt{3}}}. \tag{8}$$

Notice that in the proof of (8) we did not use the assumption that $|z_0^{(i)}| > 1$.

Let $z_0^{(i)} > 0$. Since $z_1^{(j)} \equiv sz_0^{(i)} \pmod{c}$ and $-c < sz_0^{(i)} - cx_0^{(i)} < 0$, we have $z_1^{(j)} \in \{sz_0^{(i)} - cx_0^{(i)}, sz_0^{(i)} - cx_0^{(i)} + c\}$. But

$$\begin{aligned} sz_0^{(i)} - cx_0^{(i)} \;&<\; -\sqrt{\frac{c\sqrt{c}}{2\sqrt{3}}}, \\ sz_0^{(i)} - cx_0^{(i)} + c \;&>\; \frac{2c}{3}, \end{aligned}$$

which both contradict (6).

If $z_0^{(i)} < 0$, then we have $z_1^{(j)} \in \{sz_0^{(i)} + cx_0^{(i)}, sz_0^{(i)} + cx_0^{(i)} - c\}$, and since

$$\begin{aligned} sz_0^{(i)} + cx_0^{(i)} \;&>\; \sqrt{\frac{c\sqrt{c}}{2\sqrt{3}}}, \\ sz_0^{(i)} + cx_0^{(i)} - c \;&<\; -\frac{2c}{3}, \end{aligned}$$

we obtain contradiction as before.

3° We have $z_0^{(i)} \equiv tz_1^{(j)} \pmod{c}$. If $z_1^{(j)} = \pm 1$, then (4) implies $z_0^{(i)} = tz_1^{(j)} = \pm t$. Assume $|z_1^{(j)}| \geq 2$. Then $y_1^{(j)} \geq 2$ and we have $|z_1^{(j)}| \geq s$. As in **2°** we have

$$cy_1^{(j)} - t|z_1^{(j)}| = \frac{3c^2(y_1^{(j)})^2 - 3t^2(z_1^{(j)})^2}{3(cy_1^{(j)} + t|z_1^{(j)}|)} = \frac{3c^2 - 3(y_1^{(j)})^2 - 8c - 3}{3(cy_1^{(j)} + t|z_1^{(j)}|)} < \frac{3c^2}{3(2c + c\sqrt{3})} < \frac{c}{3},$$

$$\begin{aligned} 3c^2 - 3(y_1^{(j)})^2 - 8c - 3 &\geq 2.9c^2, \\ 3(cy_1^{(j)} + s|z_1^{(j)}|) &\leq 5.74c\sqrt[4]{c}, \end{aligned}$$

and

$$cy_1^{(j)} - t|z_1^{(j)}| \geq \frac{1}{2}\sqrt{c\sqrt{c}}. \tag{9}$$

Thus we have $z_0^{(i)} \in \{tz_1^{(j)} \mp cy_1^{(j)}, tz_1^{(j)} \mp cy_1^{(j)} \pm c\}$. But

$$|tz_1^{(j)} \mp cy_1^{(j)} \pm c| > \frac{2c}{3},$$

and (4) implies that

$$z_0^{(i)} = tz_1^{(j)} \mp cy_1^{(j)}. \tag{10}$$

Let $d_0 = [(z_0^{(i)})^2 - 1]/c$. From (9) and the definition of the sequences $v^{(i)}$ and $w^{(j)}$ we see that d_0 satisfies the system (1). Furthermore,

$$d_0 < \frac{1}{c} \cdot \frac{c\sqrt{c}}{2} < 0.046c < c_{k-1}$$

and from the minimality of k, it follows that $d_0 = 0$. But, now we have $|z_0^{(i)}| = 1$, which is in a contradiction with (9) and (10).

4° We have $sz_0^{(i)} \equiv tz_1^{(j)} \pmod{c}$. The estimates for the numbers $cx_0^{(i)} - s|z_0^{(i)}|$ and $cy_1^{(j)} - t|z_1^{(j)}|$ in the proof of **2°** and **3°** imply the following:

a) If $z_0^{(i)} > 0$ and $z_1^{(j)} > 0$, then $sz_0^{(i)} - cx_0^{(i)} = tz_1^{(j)} - cy_1^{(j)}$.

b) If $z_0^{(i)} > 0$ and $z_1^{(j)} < 0$, then $sz_0^{(i)} - cx_0^{(i)} + c = tz_1^{(j)} + cy_1^{(j)}$. But $sz_0^{(i)} - cx_0^{(i)} + c > \frac{2c}{3}$ and $tz_1^{(j)} + cy_1^{(j)} < \frac{c}{3}$, a contradiction.

c) If $z_0^{(i)} < 0$ and $z_1^{(j)} > 0$, then $sz_0^{(i)} + cx_0^{(i)} = tz_1^{(j)} - cy_1^{(j)} + c$. But $sz_0^{(i)} + cx_0^{(i)} < \frac{c}{3}$ and $tz_1^{(j)} - cy_1^{(j)} + c > \frac{2c}{3}$, a contradiction.

d) If $z_0^{(i)} < 0$ and $z_1^{(j)} < 0$, then $sz_0^{(i)} + cx_0^{(i)} = tz_1^{(j)} + cy_1^{(j)}$.

Hence, we have

$$sz_0^{(i)} \mp cx_0^{(i)} = tz_1^{(j)} \mp cy_1^{(j)}.$$

Consider the number

$$d_0 = \frac{1}{c}[(sz_0^{(i)} \mp cx_0^{(i)})^2 - 1].$$

As in **3°** we see that d_0 satisfies the system (1). Furthermore,

$$d_0 \ < \ \frac{1}{c} \cdot (\frac{c}{3})^2 = \frac{c}{9} < c,$$

and, by (8), $d_0 > 0$. Therefore, from the minimality of k it follows that $d_0 = c_{k-1}$.

We have

$$c \cdot c_{k-1} + 1 = (st - 2c)^2.$$

Hence,

$$cx_0^{(i)} - s|z_0^{(i)}| = 2c - st,$$

and

$$c(x_0^{(i)} - 2) = s(|z_0^{(i)}| - t).$$

Since $\gcd(s, c) = 1$, we have $x_0^{(i)} \equiv 2 \pmod{s}$, and from (5) we conclude that $x_0^{(i)} = 2$ and $|z_0^{(i)}| = t$. In the same manner, from

$$cy_1^{(j)} - t|z_1^{(j)}| = 2c - st$$

we conclude that $y_1^{(j)} = 2$ and $|z_1^{(j)}| = s$. Thus we have $z_0^{(i)} = t$, $z_1^{(j)} = s$ or $z_0^{(i)} = -t$, $z_1^{(j)} = -s$. ■

Now we will consider the sequences ($v^{(i)} \bmod c^2$) and ($w^{(j)} \bmod c^2$) which have the initial terms given in Lemma 1. (We will omit the superscripts (i) and (j).)

Lemma 2 *Assume that the conditions of Lemma* 1 *are satisfied, then*

1° $v_{2m} \equiv z_0 + 2c(m^2 z_0 + msx_0) \pmod{c^2}$

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

3° $w_{2n} \equiv z_1 + 2c(3n^2 z_1 + nty_1) \pmod{c^2}$

4° $w_{2n+1} \equiv tz_1 + c[6n(n+1)tz_1 + (2n+1)y_1] \pmod{c^2}$

Proof. We prove the lemma by induction. We use the fact that the sequences (v_{2m}) and (v_{2m+1}) satisfy the recurrence relation

$$a_{m+2} = 2(2c+1)a_{m+1} - a_m \,,$$

and the sequences (w_{2n}) and (w_{2n+1}) satisfy the recurrence relation

$$b_{n+2} = 2(6c+1)b_{n+1} - b_n \,.$$

1° $v_0 = z_0, \quad v_2 = 2s^2 z_0 + 2scx_0 - z_0 = z_0 + 2c(z_0 + sx_0)$.
Assume that the assertion is valid for $m-1$ and m. Then we have

$$\begin{aligned} v_{2m+2} &= (4c+2)v_{2m} - v_{2m-2} \\ &\equiv 4cz_0 + 2z_0 + 4c(m^2 z_0 + msx_0) - z_0 - 2c[(m-1)^2 z_0 + (m-1)sx_0] \\ &= z_0 + 2c[z_0(2 + 2m^2 - m^2 + 2m - 1) + sx_0(2m - m + 1)] \\ &= z_0 + 2c[(m+1)^2 z_0 + (m+1)sx_0] \pmod{c^2} \,. \end{aligned}$$

2° $v_1 = sz_0 + cx_0, \quad v_{-1} = sz_0 - cx_0.$
Assume that the assertion is valid for $m-1$ and m. Then we have

$$\begin{aligned} v_{2m+3} &= (4c+2)v_{2m+1} - v_{2m-1} \\ &\equiv 4csz_0 + 2sz_0 + 2c[2m(m+1)sz_0 + (2m+1)x_0] \\ &\quad - sz_0 - c[2m(m-1)sz_0 + (2m-1)x_0] \\ &= sz_0 + c[sz_0(4+4m^2+4m-2m^2+2m) + x_0(4m+2-2m+1)] \\ &= sz_0 + c[2(m+1)(m+2)sz_0 + (2m+3)x_0] \pmod{c^2}. \end{aligned}$$

The proof of **3°** and **4°** is completely analogous. ■

COROLLARY 3 *The equations* $v_{2m} = w_{2n+1}$ *and* $v_{2m+1} = w_{2n}$ *have no solutions in integers* n, m.

Proof. If $v_{2m} = w_{2n+1}$, then Lemmas 1 and 2 imply

$$\pm 2m^2 t + 4ms \equiv \pm 6n(n+1)t + (2n+1) \pmod{c}.$$

But this contradicts the obvious fact that c is even.
If $v_{2m+1} = w_{2n}$, then Lemmas 1 and 2 imply

$$\pm 2m(m+1)s + (2m+1) \equiv \pm 6n^2 s + 4nt \pmod{c}$$

and we have again a contradiction with the fact that c is even. ■

4 Linear forms in three logarithms

LEMMA 3 **1°** *If* $v_{2m} = w_{2n}$, *then*

$$0 < 2m\log(s+\sqrt{c}) - 2n\log(t+\sqrt{3c}) + \log\frac{\sqrt{3}(\sqrt{c}\pm 1)}{\sqrt{c}\pm\sqrt{3}} < \frac{3}{2}(s+\sqrt{c})^{-4m}.$$

2° *If* $v_{2m+1} = w_{2n+1}$, *then*

$$0 < (2m+1)\log(s+\sqrt{c}) - (2n+1)\log(t+\sqrt{3c}) + \log\frac{\sqrt{3}(2\sqrt{c}\pm t)}{2\sqrt{c}\pm s\sqrt{3}} < 22(s+\sqrt{c})^{-4m-2}.$$

Proof. **1°** We have by Lemma 1,**1°** that

$$\begin{aligned} v_m &= \frac{1}{2}[(\sqrt{c}\pm 1)(s+\sqrt{c})^m + (-\sqrt{c}\pm 1)(s-\sqrt{c})^m], \\ w_n &= \frac{1}{2\sqrt{3}}[(\sqrt{c}\pm\sqrt{3})(t+\sqrt{3c})^n + (-\sqrt{c}\pm\sqrt{3})(t-\sqrt{3c})^n]. \end{aligned}$$

If we put

$$P=(\sqrt{c}\pm 1)(s+\sqrt{c})^m,\quad Q=\frac{1}{\sqrt{3}}(\sqrt{c}\pm\sqrt{3})(t+\sqrt{3c})^n,$$

then

$$P^{-1}=\frac{\sqrt{c}\mp 1}{c-1}(s-\sqrt{c})^m,\quad Q^{-1}=\frac{\sqrt{3}(\sqrt{c}\mp\sqrt{3})}{c-3}(t-\sqrt{3c})^n.$$

Now the relation $v_m=w_n$ implies $P-(c-1)P^{-1}=Q-\frac{c-3}{3}Q^{-1}$. It is clear that $P>1$ and $Q>1$, and from

$$P-Q=(c-1)P^{-1}-(\frac{c}{3}-1)Q^{-1}>(c-1)(P^{-1}-Q^{-1})=(c-1)(Q-P)P^{-1}Q^{-1}$$

it follows that $P>Q$. Furthermore, we have $P-Q<(c-1)P^{-1}$ and $\frac{P-Q}{P}<(c-1)P^{-2}$. We may assume that $m\geq 1$. Thus, we have $P\geq(\sqrt{c}-1)\cdot 2\sqrt{c}>c$, and so $(c-1)P^{-2}<\frac{1}{8}$. Hence,

$$\begin{aligned}0<\log\frac{P}{Q}&=-\log(1-\frac{P-Q}{P})\\&<(c-1)P^{-2}+(c-1)^2P^{-4}<\frac{9}{8}(c-1)\cdot\frac{1}{(\sqrt{c}-1)^2}(s+\sqrt{c})^{-2m}<\frac{3}{2}(s+\sqrt{c})^{-2m},\end{aligned}$$

which implies the assertion taking into consideration that both n and m are even.

2° We have by Lemma 1,**4°** that

$$\begin{aligned}v_m&=\frac{1}{2}[(2\sqrt{c}\pm t)(s+\sqrt{c})^m+(-2\sqrt{c}\pm t)(s-\sqrt{c})^m],\\w_n&=\frac{1}{2\sqrt{3}}[(2\sqrt{c}\pm s\sqrt{3})(t+\sqrt{3c})^n+(-2\sqrt{c}\pm s\sqrt{3})(t-\sqrt{3c})^n].\end{aligned}$$

Let us put

$$P=(2\sqrt{c}\pm t)(s+\sqrt{c})^m,\quad Q=\frac{1}{\sqrt{3}}(2\sqrt{c}\pm s\sqrt{3})(t+\sqrt{3c})^n.$$

Then we have

$$P^{-1}=\frac{2\sqrt{c}\mp t}{c-1}(s-\sqrt{c})^m,\quad Q^{-1}=\frac{\sqrt{3}(2\sqrt{c}\mp s\sqrt{3})}{c-3}(t-\sqrt{3c})^n,$$

and the relation $v_m=w_n$ implies $P-(c-1)P^{-1}=Q-\frac{c-3}{3}Q^{-1}$. As in **1°**, we obtain $P>Q$ and $P-Q<(c-1)P^{-1}$. As we may assume that $m\geq 1$, we have $P\geq(2\sqrt{c}-t)\cdot 2\sqrt{c}>\frac{c}{2}$ and $(c-1)P^{-2}<\frac{1}{2}$. Hence,

$$0<\log\frac{P}{Q}=-\log(1-\frac{P-Q}{P})$$

$$
\begin{aligned}
&< \frac{3}{2}(c-1)P^{-2} < \frac{3}{2}(c-1)\cdot\frac{1}{(2\sqrt{c}-t)^2}(s+\sqrt{c})^{-2m} \\
&= \frac{3}{2}(c-1)\frac{2\sqrt{c}+t}{(c-1)(2\sqrt{c}-t)}(s+\sqrt{c})^{-2m} = \frac{3}{2}(1+\frac{2}{2\sqrt{\frac{c}{3c+1}}-1})(s+\sqrt{c})^{-2m} \\
&< 22(s+\sqrt{c})^{-2m}.
\end{aligned}
$$

■

Now we use Lemmas 2 and 3 and obtain a lower bound for m and n. We consider two cases:

1° $v_{2m} = w_{2n}, \quad m,n \neq 0$
From Lemma 3 we have

$$2m\log(s+\sqrt{c}) - 2n\log(t+\sqrt{3c}) < 0\,,$$

and so

$$\frac{m}{n} < \frac{\log(t+\sqrt{3c})}{\log(s+\sqrt{c})} = \frac{\log\sqrt{3}}{\log(s+\sqrt{c})} + \frac{\log(\sqrt{c+\frac{1}{3}}+\sqrt{c})}{\log(\sqrt{c+1}+\sqrt{c})} < 1.178\,.$$

On the other hand, Lemma 2 implies

$$\pm 2m^2 + 2ms \equiv \pm 6n^2 + 2nt \pmod{c}\,.$$

Assume that $n < 0.105\sqrt{c}$. Then $m < 0.124\sqrt{c}$. We have

$$
\begin{aligned}
2|\pm m^2 + ms| &\le 2c(0.124^2 + 0.124\cdot 1.005) < \frac{c}{3}\,, \\
2|\pm 3n^2 + nt| &\le 2c(3\cdot 0.105^2 + 0.105\cdot 1.735) < \frac{c}{2}\,.
\end{aligned}
$$

Hence, $\pm m^2 + ms = \pm 3n^2 + nt$. But

$$
\begin{aligned}
0.876ms &\le \pm m^2 + ms \le 1.124ms\,, \\
0.685nt &\le \pm 3n^2 + nt \le 1.315nt\,.
\end{aligned}
$$

Note that $1.727 \le t/s < \sqrt{3}$. Thus, for sign $+$ we obtain:

$$\frac{ms}{nt} \ge 0.889 \quad\Rightarrow\quad \frac{m}{n} \ge 1.535\,,$$

and for sign $-$ we obtain:

$$\frac{ms}{nt} \ge 0.685 \quad\Rightarrow\quad \frac{m}{n} \ge 1.182\,,$$

a contradiction.

2° $v_{2m+1} = w_{2n+1}$
From Lemma 3 we have

$$(2m+1)\log(s+\sqrt{c}) - (2n+1)\log(t+\sqrt{3c}) < 0\,,$$

and so

$$\frac{2m+1}{2n+1} < \frac{\log(t+\sqrt{3c})}{\log(s+\sqrt{c})} < 1.178\,.$$

On the other hand, Lemma 2 implies

$$\pm 2m(m+1)st + 2(2m+1) \equiv \pm 6n(n+1)st + 2(2n+1) \pmod{c}\,. \tag{11}$$

Multiplying congruence (11) by s we obtain

$$\pm 2m(m+1)t + 2(2m+1)s \equiv \pm 6n(n+1)t + 2(2n+1)s \pmod{c}\,.$$

Let $m_1 = m + \frac{1}{2}$, $n_1 = n + \frac{1}{2}$, and let $n_1 < 0.156\sqrt[4]{c}$. Then $m_1 < 0.184\sqrt[4]{c}$. We have

$$\begin{aligned}
2|\pm m(m+1)t + (2m+1)s| &\le 2(0.184^2 \cdot 1.735c + 2 \cdot 0.184 \cdot 1.005\sqrt{c\sqrt{c}}) < \frac{c}{2}\,,\\
2|\pm 3n(n+1)t + (2n+1)s| &\le 2(3 \cdot 0.156^2 \cdot 1.735c + 2 \cdot 0.156 \cdot 0.105\sqrt{c\sqrt{c}}) < \frac{c}{2}\,.
\end{aligned}$$

Hence,

$$m(m+1)t \pm (2m+1)s = 3n(n+1)t \pm (2n+1)s\,. \tag{12}$$

Multiplying congruence (11) by t we obtain

$$\pm 2m(m+1)s + 2(2m+1)t \equiv \pm 6n(n+1)s + 2(2n+1)t \pmod{c}$$

and in the same manner as above we obtain

$$m(m+1)s \pm (2m+1)t = 3n(n+1)s \pm (2n+1)t\,. \tag{13}$$

Since $t \neq \pm s$ we conclude from (12) and (13) that

$$m(m+1) \pm (2m+1) = 3n(n+1) \pm (2n+1)$$

and

$$m(m+1) \mp (2m+1) = 3n(n+1) \mp (2n+1)\,.$$

Hence $2m+1 = 2n+1$ and $m(m+1) = 3n(n+1)$, which implies that $m = n = 0$.
Thus we have proved

Lemma 4 **1°** *If* $v_{2m} = w_{2n}$ *and* $n \neq 0$, *then* $n > 0.105\sqrt{c}$.

2° *If* $v_{2m+1} = w_{2n+1}$ *and* $n \neq 0$, *then* $n > 0.156\sqrt[4]{c}$.

Now we apply the following theorem of Baker and Wüstholz [3]:

THEOREM 2 *For a linear form* $\Lambda \neq 0$ *in logarithms of* l *algebraic numbers* $\alpha_1, \dots, \alpha_l$ *with rational coefficients* $b_1, \dots, b_l$ *we have*

$$\log \Lambda \geq -18(l+1)!\, l^{l+1} (32d)^{l+2} h'(\alpha_1) \cdots h'(\alpha_l) \log(2ld) \log B\,,$$

where $B = \max(|b_1|, \dots, |b_l|)$*, and where* d *is the degree of the number field generated by* $\alpha_1, \dots, \alpha_l$.

Here

$$h'(\alpha) = \frac{1}{d} \max\left(h(\alpha), |\log\, \alpha|, 1\right),$$

and $h(\alpha)$ denotes the standard logarithmic Weil height of α.

1) Let us first consider the equation $v_{2m} = w_{2n}$, with $n \neq 0$. Using Lemma 3,**1**°, we will apply Theorem 2. We have: $l = 3$, $d = 4$, $B = 2m$,

$$\alpha_1 = s + \sqrt{c}, \quad \alpha_2 = t + \sqrt{3c},$$

$$\alpha_3 = \frac{\sqrt{3}(\sqrt{c}+1)}{\sqrt{c}+\sqrt{3}}, \quad \alpha_3' = \frac{\sqrt{3}(\sqrt{c}-1)}{\sqrt{c}-\sqrt{3}},$$

$$h'(\alpha_1) = \frac{1}{2} \log \alpha_1 < 0.33 \log c, \quad h'(\alpha_2) = \frac{1}{2} \log \alpha_2 < 0.38 \log c,$$

$$h'(\alpha_3) = h'(\alpha_3') < \frac{1}{4} \log(12.63c^2) < 0.64 \log c,$$

$$\log \frac{3}{2}(s+\sqrt{c})^{-4m} < \log(s+\sqrt{c})^{-3m} < -\frac{3}{2} m \log c.$$

Hence

$$\frac{3}{2} m \log c < 3.822 \cdot 10^{15} \cdot 0.33 \log c \cdot 0.38 \log c \cdot 0.64 \log c \cdot \log 2m,$$

and

$$\frac{m}{\log 2m} < 2.045 \cdot 10^{14} \log^2 c.$$

But $m > n > 0.105\sqrt{c}$. Thus

$$m < 2.045 \cdot 10^{14} \log 2m \log^2(91m^2),$$

which implies $m < 9 \cdot 10^{19}$ and finally $c < 8 \cdot 10^{41}$. From

$$\frac{1}{6}(2+\sqrt{3})(7+4\sqrt{3})^k < 8 \cdot 10^{41},$$

it follows that $k \leq 36$.

2) Let $v_{2m+1} = w_{2n+1}$, with $n \neq 0$. Now we have: $l = 3$, $d = 4$, $B = 2m + 1$,

$$\alpha_1 = s + \sqrt{c}, \quad \alpha_2 = t + \sqrt{3c},$$

$$\alpha_3 = \frac{\sqrt{3}(2\sqrt{c} + t)}{2\sqrt{c} + s\sqrt{3}}, \quad \alpha_3' = \frac{\sqrt{3}(2\sqrt{c} - t)}{2\sqrt{c} - s\sqrt{3}},$$

$$h'(\alpha_1) < 0.33 \log c, \quad h'(\alpha_2) < 0.38 \log c,$$

$$h'(\alpha_3) = h'(\alpha_3') < \frac{1}{4} \log(75.79c^2) < 0.73 \log c,$$

$$\log 22(s + \sqrt{c})^{-4m-2} < -2m \log c.$$

Hence

$$2m \log c < 3.822 \cdot 10^{15} \cdot 0.33 \log c \cdot 0.38 \log c \cdot 0.73 \log c \cdot \log(2m + 1),$$

and

$$\frac{m}{\log(2m + 1)} < 1.75 \cdot 10^{14} \log^2 c.$$

But $m > n > 0.156 \sqrt[4]{c}$. Thus

$$m < 1.75 \cdot 10^{14} \log(2m + 1) \log^2(1689m^4),$$

which implies $m < 4 \cdot 10^{20}$ and finally $c < 5 \cdot 10^{85}$. It implies $k \leq 75$, which completes the proof of Proposition 1. ■

5 The reduction method

For completing the proof of Theorem 1 for all positive integers k, we must check the following:

1) If $2 \leq k \leq 36$ and

$$v_0 = \pm 1, \quad v_1 = \pm s + c, \quad v_{m+2} = 2sv_{m+1} - v_m, \quad m \geq 0,$$

$$w_0 = \pm 1, \quad w_1 = \pm t + c, \quad w_{n+2} = 2tw_{n+1} - w_n, \quad n \geq 0,$$

then $v_{2m} = w_{2n}$ implies that $m = n = 0$. We know that $n \leq m < 9 \cdot 10^{19}$.

2) If $2 \leq k \leq 75$ and

$$v_0 = t, \quad v_1 = \pm st + 2c, \quad v_{m+2} = 2sv_{m+1} - v_m, \quad m \geq 0,$$

$$w_0 = s, \quad w_1 = \pm st + 2c, \quad w_{n+2} = 2tw_{n+1} - w_n, \quad n \geq 0,$$

then $v_{2m+1} = w_{2n+1}$ implies that $m = n = 0$. We know that $n \leq m < 4 \cdot 10^{20}$.

We use the reduction method based on the Baker-Davenport lemma (see [2]). Let $\kappa = \log(s+\sqrt{c})/\log(t+\sqrt{3c})$, $\gamma_{1,2} = \sqrt{3}(\sqrt{c}\pm 1)/(\sqrt{c}\pm\sqrt{3})$, $\gamma_{3,4} = \sqrt{3}(2\sqrt{c}\pm t)/(2\sqrt{c}\pm s\sqrt{3})$, $\mu_{1,2} = \log\gamma_{1,2}/\log(t+\sqrt{3c})$, $\mu_{3,4} = \log\gamma_{3,4}/\log(t+\sqrt{3c})$, $A_1 = 3/2\log(t+\sqrt{3c})$, $A_2 = 22/\log(t+\sqrt{3c})$, $B = (s+\sqrt{c})^2$.

Let $v_m = w_n$, $m, n \geq 0$. If m and n are even, then Lemma 3,**1**° implies

$$0 < m\kappa - n + \mu_{1,2} < A_1 \cdot B^{-m}, \tag{14}$$

and if m and n are odd, then Lemma 3,**2**° implies

$$0 < m\kappa - n + \mu_{3,4} < A_2 \cdot B^{-m}. \tag{15}$$

LEMMA 5 *Suppose that M is a positive integer. Let p/q be the convergent of the continued fraction expansion of κ such that $q > 6M$ and let $\varepsilon = \|\mu q\| - M \cdot \|\kappa q\|$, where $\|\cdot\|$ denotes the distance from the nearest integer.*

a) *If $\varepsilon > 0$, then there is no solution of the inequality*

$$0 < m\kappa - n + \mu < AB^{-m} \tag{16}$$

in integers m and n with

$$\frac{\log(Aq/\varepsilon)}{\log B} \leq m \leq M\,.$$

b) *Let $r = \lfloor \mu q + \frac{1}{2} \rfloor$. If $p - q + r = 0$, then there is no solution of inequality (16) in integers m and n with*

$$\max(\frac{\log(3Aq)}{\log B}, 1) < m \leq M\,.$$

Proof. **a)** Assume that $0 \leq m \leq M$. We have

$$m(\kappa q - p) + mp - nq + \mu q < qAB^{-m}.$$

Thus

$$qAB^{-m} > |\mu q - (nq - mp)| - m\|\kappa q\| \geq \|\mu q\| - M\|\kappa q\| = \varepsilon\,,$$

which implies

$$m < \frac{\log(Aq/\varepsilon)}{\log B}\,.$$

b) Assume that $0 \leq m \leq M$. We have

$$m(\kappa q - p) + (mp - nq + r) + (\mu q - r) < qAB^{-m}.$$

Thus

$$|mp-nq+r| < qAB^{-m} + |\mu q - r| + m|\kappa q - p| < qAB^{-m} + \|\mu q\| + M\|\kappa q\| < qAB^{-m} + \frac{2}{3}\,.$$

If $qAB^{-m} \leq \frac{1}{3}$, then

$$mp - nq + r = 0\,. \tag{17}$$

Thus $m \equiv m_0 \pmod{q}$, where m_0 is the least nonnegative solution of linear Diophantine equation (17). But $p - q + r = 0$ implies $m_0 = 1$. Now, $0 \leq m \leq M$ and $q > 6M$ implies that $m = 1$.

If $qAB^{-m} > \frac{1}{3}$, then

$$m < \frac{\log(3Aq)}{\log B}\,.$$

■

We apply Lemma 5 to inequality (14), resp. (15), with $M = 2{\cdot}10^{20}$, resp. $M = 8{\cdot}10^{20}$. If the first convergent such that $q > 6M$ does not satisfy the conditions **a)** or **b)** of Lemma 5, then we use the next convergent. We have to consider $2 \cdot 35 + 2 \cdot 74 = 218$ cases, and the use of next convergent is necessary only in 3 cases. In all cases ($2 \leq k \leq 36$ for μ_1 and μ_2, and $2 \leq k \leq 75$ for μ_3 and μ_4) the reduction gives new bound $m \leq M_0$, where $M_0 \leq 9$. The next step of the reduction (the applying of Lemma 5 with $M = M_0$) in all cases gives $m \leq 1$, which completes the proof of Theorem 1.

6 Concluding remarks

Arkin, Hoggatt and Strauss [1] proved that every Diophantine triple $\{a, b, c\}$ can be extended to the Diophantine quadruple $\{a, b, c, d\}$. More precisely, if $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$, then we can take $d = a + b + c + 2abc \pm 2rst$. The conjecture is that d has to be $a + b + c + 2abc \pm 2rst$. Thus, in present paper we verify this conjecture for Diophantine triples of the form $\{1, 3, c\}$. Let us observe that the above conjecture is verified for Diophantine triples of the form $\{k-1, k+1, 4k\}$, $k \geq 2$, (see [6]), and also for the Diophantine triples $\{1, 8, 120\}$, $\{1, 8, 15\}$, $\{1, 15, 24\}$, $\{1, 24, 35\}$ and $\{2, 12, 24\}$ (see [10]).

If we allow that the elements of a Diophantine m-tuples are positive rational numbers, then the statement of Corollary 1 is not longer valid. Namely, the Diophantine pair $\{1, 3\}$ can be extended on infinitely many ways to the rational Diophantine quintuple. For example, if c is an integer such that $\{1, 3, c\}$ is a Diophantine triple, and integers s and t are defined by $c + 1 = s^2$, $3c + 1 = t^2$, then the sets

$$\{1,\ 3,\ c,\ 7c + 4st + 4,\ \frac{8st(2s+t)(3s+2t)(2c+st)}{(21c^2 + 12c - 1 + 12cst)^2}\}$$

and

$$\{1,\ 3,\ c,\ \frac{8(c-4)(c-2)(c+2)}{(c^2-8c+4)^2},$$
$$\frac{(2c-st+t-s-1)(2c-st-t+s-1)(2c-st+3t-5s+1)(2c-st-3t+5s+1)(2s-t-1)(2s-t+1)}{(83c^2+56c-4-48cst)^2}\}$$

have the property that the product of its any two distinct elements increased by 1 is a square of a rational number (see [5, Corollary 2 and Example 5]).

References

REFERENCES

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

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

[3] A. Baker and G. Wüstholz, 'Logarithmic forms and group varieties', *J. Reine Angew. Math.* 442 (1993), 19–62.

[4] Diophanti Alexandrini Arithmeticorum Libri Sex, cum commentariis C. G. Bacheti et observationibus D. P. de Fermat, Toulouse 1670; in particular Lib. IV, q. XXI, page 161.

[5] A. Dujella, 'On Diophantine quintuples', *Acta Arith.* 81 (1997), 69–79.

[6] A. Dujella, 'The problem of the extension of a parametric family of Diophantine triples', *Publ. Math. Debrecen* 51 (1997), 311–322.

[7] C. M. Grinstead, 'On a method of solving a class of Diophantine equations', *Math. Comp.* 32 (1978), 936–940.

[8] B. W. Jones, 'A second variation on a problem of Diophantus and Davenport', *Fibonacci Quart.* 16 (1978), 155–165.

[9] P. Kanagasabapathy and T. Ponnudurai, 'The simultaneous Diophantine equations $y^2-3x^2=-2$ and $z^2-8x^2=-7$', *Quart. J. Math. Oxford Ser. (2)* 26 (1975), 275–278.

[10] K. S. Kedlaya, 'Solving constrained Pell equations', *Math. Comp.*, to appear.

[11] T. Nagell, *Introduction to Number Theory*, Almqvist, Wiley (1951), Stockholm, New York.

[12] G. Sansone, 'Il sistema diofanteo $N+1=x^2$, $3N+1=y^2$, $8N+1=z^2$', *Ann. Mat. Pura Appl. (4)* 111 (1976), 125–151.

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

Institute of Mathematics
and Computer Science
Lajos Kossuth University
H-4010 Debrecen P.O. Box 12
Hungary
E-mail: pethoe@math.klte.hu