BULLETIN OF INTERNATIONAL MATHEMATICAL VIRTUAL INSTITUTE
ISSN 1840-4367
Vol. 3(2013), 59-68
Available online: www.imvibl.org

Former
BULLETIN OF SOCIETY OF MATHEMATICIANS BANJA LUKA
ISSN 0354-5792 (o), ISSN 1986-521X (p)

EXPLICIT VERSION OF WORLEY'S THEOREM IN DIOPHANTINE APPROXIMATIONS

Bernadin Ibrahimpašić

Abstract. In this paper we give several explicit results on rational approximations of the form $|\alpha - a/b| < k/b^2$, in terms of continued fractions.

1. Introduction

There are a number of results on approximations of a real number α by a rational number a/b. We mention two classical results (see [**9**]). One is the classical Legendre's theorem in Diophantine approximations, which states that if a real number α and a rational number $\frac{a}{b}$ (we will always assume that $b \geqslant 1$), satisfy the inequality

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}, \tag{1.1}$$

then $\frac{a}{b}$ is a convergent of the continued fraction expansion of $\alpha = [a_0; a_1, \ldots]$. The second result is from Fatou [**5**], who showed that if

$$|\alpha - \frac{a}{b}| < \frac{1}{b^2},$$

then $\frac{a}{b} = \frac{p_m}{q_m}$ or $\frac{p_{m+1} \pm p_m}{q_{m+1} \pm q_m}$, where $\frac{p_m}{q_m}$ denotes the m-th convergent of α.

Worley [**14**] generalized these results to the inequality $\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}$, where k is an arbitrary positive real number. The results of Worley was slightly improved in [**1**].

Theorem 1.1 (Worley [**14**], Dujella [**1**]). *Let α be a real number and let a and b be coprime nonzero integers, satisfying the inequality*

$$\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}, \tag{1.2}$$

2010 *Mathematics Subject Classification.* 11K60, 11A55.

Key words and phrases. Diophantine approximations, Continued fractions.

where k is a positive real number. Then $(a,b) = (rp_{m+1} \pm sp_m, rq_{m+1} \pm sq_m)$, for some $m \geqslant -1$ and nonnegative integers r and s such that $rs < 2k$.

Theorem 1.2 (Worley [**14**]). *If α is an irrational number, $k \geqslant \frac{1}{2}$ and $\frac{a}{b}$ is a rational approximation to α (in reduced form) for which the inequality (1.2) holds, then either $\frac{a}{b}$ is a convergent $\frac{p_m}{q_m}$ to α or $\frac{a}{b}$ has one of the following forms:*

$$\text{(i)}\quad \frac{a}{b} = \frac{rp_{m+1}+sp_m}{rq_{m+1}+sq_m} \qquad \begin{array}{l} r > s \quad \textit{and} \quad rs < 2k, \quad \textit{or} \\ r \leqslant s \quad \textit{and} \quad rs < k + \frac{r^2}{a_{m+2}}, \end{array}$$

$$\text{(ii)}\quad \frac{a}{b} = \frac{sp_{m+1}-tp_m}{sq_{m+1}-tq_m} \qquad \begin{array}{l} s < t \quad \textit{and} \quad st < 2k, \quad \textit{or} \\ s \geqslant t \quad \textit{and} \quad st\left(1 - \frac{t}{2s}\right) < k, \end{array}$$

where r, s and t are positive integers.

Since the fraction a/b is in reduced form, it is clear that in the statements of Theorems 1.1 and 1.2 we may assume that $\gcd(r,s) = 1$ and $\gcd(s,t) = 1$.

Worley [**14**] gave the explicit version of his result for $k = 2$. He showed, if a real number α and a rational number $\frac{a}{b}$ satisfy the inequality $\left|\alpha - \frac{a}{b}\right| < \frac{2}{b^2}$, then $\dfrac{a}{b} = \dfrac{rp_{m+1} + sp_m}{rq_{m+1} + sq_m}$, where

$$(r,s) \in R_2 = \{(0,1),(1,1),(1,2),(2,1),(3,1)\},$$

or $\dfrac{a}{b} = \dfrac{sp_{m+2} - tp_{m+1}}{sq_{m+2} - tq_{m+1}}$, where

$$(s,t) \in T_2 = \{(1,1),(1,2),(1,3),(2,1)\}$$

(for an integer $m \geqslant -1$).

This result for $k = 2$ has been in [**4**] applied for solving the family of Thue inequalities

$$|x^4 - 4cx^3y + (6c+2)x^2y^2 + 4cxy^2 + y^4| \leqslant 6c + 4.$$

Theorem 1.1 was used in [**1**] for a description of a modification of Verheul and van Tilborg variant of Wiener's attack ([**12**, **13**]) on RSA cryptosystem with small secret exponent.

Dujella and Ibrahimpašić [**2**] extended Worley's work [**14**] and gave explicit and sharp versions of Theorems 1.1 and 1.2 for $k = 3, 4, 5, \ldots, 12$. They gave the pairs (r,s) which appear in the expression of solutions of (1.2) in the form $(a,b) = (rp_{m+1} \pm sp_m, rq_{m+1} \pm sq_m)$.

These results have been applied to cryptanalysis of the KMOV [**7**] and LUC [**8**] cryptosystems with short secret exponent, and in [**3**] applied for solving the family of Thue inequalities

$$|x^4 + 2(1-c^2)x^2y^2 + y^4| \leqslant 2c + 3,$$

where the system and the original Thue equation are not equivalent: each solution of the Thue equation induces a solution of the system, but not vice-versa.

In this paper we will extend Worley's work (and also the work of Dujella and Ibrahimpašić) and give explicit and sharp version of Theorems 1.1 and 1.2 for $k = 13$. We will list the pairs (r,s) which appear in the expression of solutions of (1.2) in the form $(a,b) = (rp_{m+1} \pm sp_m, rq_{m+1} \pm sq_m)$, and we will show by explicit examples that all pairs from the list are indeed necessary. We will prove some patterns in pairs (r,s) and (s,t) which appear in representations $(a,b) = (rp_{m+1} + sp_m,\ rq_{m+1} + sq_m)$ and $(a,b) = (sp_{m+2} - tp_{m+1}, sq_{m+2} - tq_{m+1})$ of solutions of inequality (1.2).

Our main result is the following theorem.

THEOREM 1.3. *Let $k \geqslant 3$ be a integer. There exist a real number α and rational numbers $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ such that*

$$\left|\alpha - \frac{a_1}{b_1}\right| < \frac{k}{b_1^2}$$

and

$$\left|\alpha - \frac{a_2}{b_2}\right| < \frac{k}{b_2^2}$$

where

$$\begin{aligned} (a_1, b_1) &= (rp_{m+1} + 2p_m, rq_{m+1} + 2q_m) \qquad \textit{and} \\ (a_2, b_2) &= (2p_{m+2} - tp_{m+1}, 2q_{m+2} - tq_{m+1}), \end{aligned}$$

for some $m \geqslant -1$ and integers r and t such that $1 \leqslant r, t \leqslant k-1$.

2. Explicit version of Worley's theorem for $k = 13$

Dujella and Ibrahimpašić [**2**] gave the following result.

PROPOSITION 2.1. *Let $k \in \{3,4,5,6,7,8,9,10,11,12\}$. If a real number α and a rational number $\frac{a}{b}$ satisfy the inequality (1.2), then $\dfrac{a}{b} = \dfrac{rp_{m+1} + sp_m}{rq_{m+1} + sq_m}$, where $(r,s) \in R_k = R_{k-1} \cup R'_k$, or $\dfrac{a}{b} = \dfrac{sp_{m+2} - tp_{m+1}}{sq_{m+2} - tq_{m+1}}$, where $(s,t) \in T_k = T_{k-1} \cup T'_k$ (for an integer $m \geqslant -1$), where the sets R'_k and T'_k are given in the following table. Moreover, if any of the elements in sets R_k or T_k is omitted, the statement will no longer be valid.*

k	R'_k	T'_k
3	$\{(1,3),(4,1),(5,1)\}$	$\{(3,1),(1,4),(1,5)\}$
4	$\{(1,4),(3,2),(6,1),(7,1)\}$	$\{(4,1),(2,3),(1,6),(1,7)\}$
5	$\{(1,5),(2,3),(8,1),(9,1)\}$	$\{(5,1),(3,2),(1,8),(1,9)\}$
6	$\{(1,6),(5,2),(10,1),(11,1)\}$	$\{(6,1),(2,5),(1,10),(1,11)\}$
7	$\{(1,7),(2,5),(4,3),(12,1),(13,1)\}$	$\{(7,1),(5,2),(3,4),(1,12),(1,13)\}$
8	$\{(1,8),(3,4),(7,2),(14,1),(15,1)\}$	$\{(8,1),(4,3),(2,7),(1,14),(1,15)\}$
9	$\{(1,9),(5,3),(16,1),(17,1)\}$	$\{(9,1),(3,5),(1,16),(1,17)\}$
10	$\{(1,10),(9,2),(18,1),(19,1)\}$	$\{(10,1),(2,9),(1,18),(1,19)\}$
11	$\{(1,11),(2,7),(3,5),(20,1),(21,1)\}$	$\{(11,1),(7,2),(5,3),(1,20),(1,21)\}$
12	$\{(1,12),(5,4),(7,3),$ $(11,2),(22,1),(23,1)\}$	$\{(12,1),(4,5),(3,7),$ $(2,11),(1,22),(1,23)\}$

If we extend this result, we have:

Proposition 2.2. *If a real number α and a rational number $\frac{a}{b}$ satisfy the inequality*

$$\left|\alpha - \frac{a}{b}\right| < \frac{13}{b^2}, \tag{2.1}$$

then $\frac{a}{b} = \frac{rp_{m+1} + sp_m}{rq_{m+1} + sq_m}$, *where*

$$(r, s) \in R_{13} = R_{12} \cup \{(1, 13), (3, 7), (4, 5), (24, 1), (25, 1)\},$$

or $\frac{a}{b} = \frac{sp_{m+2} - tp_{m+1}}{sq_{m+2} - tq_{m+1}}$, *where*

$$(s, t) \in T_{13} = T_{12} \cup \{(13, 1), (7, 3), (5, 4), (1, 24), (1, 25)\}$$

(for an integer $m \geqslant -1$).

Proof. From the proof of the Theorem 1.1 in [**1**] (see also [**2**]) we have that r, s and t are related with

$$t = sa_{m+2} - r, \tag{2.2}$$

and we have the following inequalities

$$a_{m+2} > \frac{r}{s}, \tag{2.3}$$

$$r^2 - sra_{m+2} + ka_{m+2} > 0, \tag{2.4}$$

$$a_{m+2} > \frac{t}{s}, \tag{2.5}$$

$$t^2 - sta_{m+2} + ka_{m+2} > 0, \tag{2.6}$$

where m is the largest integer satisfying

$$\alpha < \frac{a}{b} \leqslant \frac{p_m}{q_m}.$$

Here we assume that $\alpha < a/b$, since the other case is completely analogous (see [**1**, **2**]).

By Theorem 1.1, we have to consider only pairs of nonnegative integers (r, s) and (s, t) satisfying $rs < 2k$, $st < 2k$, $\gcd(r, s) = 1$ and $\gcd(s, t) = 1$. The inequalities (2.4) and (2.6) for $r = 1$, resp. $t = 1$, imply that the pairs $(r, s) = (1, s)$ and $(s, t) = (s, 1)$ with $s \geqslant k + 1 = 14$ can be excluded. Similarly, for $r = 2$ or 3, resp. $t = 2$ or 3, we can exclude the pairs $(r, s) = (2, s)$ and $(s, t) = (s, 2)$ with $s \geqslant \frac{13}{2} + 2$, and the pairs $(r, s) = (3, s)$ and $(s, t) = (s, 3)$ with $s \geqslant \frac{13}{3} + 3$. In particular, the pairs $(r, s) = (2, 9), (2, 11), (3, 8)$, and the pairs $(s, t) = (9, 2), (11, 2), (8, 3)$ can be excluded.

Now we show that the pairs $(r, s) = (8, 3)$ and $(s, t) = (3, 8)$ can be replaced with other pairs with smaller products rs, resp. st.

For $(r, s) = (8, 3)$ and $k = 13$, from (2.3) and (2.4) we obtain $\frac{8}{3} < a_{m+2} < \frac{64}{11}$, and therefore we have three possibilities: $a_{m+2} = 3, 4$ or 5. If $a_{m+2} = 3$, then from (2.2) we obtain $t = 3 \cdot 3 - 8 = 1$, and we can replace $(r, s) = (8, 3)$ by $(s, t) = (3, 1)$. If $a_{m+2} = 4$, we can replace it by $(s, t) = (3, 4)$ and if $a_{m+2} = 5$, we can replace it by $(s, t) = (3, 7)$.

The proof for pairs $(s,t)=(3,8)$ is completely analogous. We use the inequalities (2.5) and (2.6), instead of (2.3) and (2.4). We obtain $\frac{8}{3} < a_{m+2} < \frac{64}{11}$, and therefore we have, again, three possibilities: $a_{m+2}=3,4$ or 5. If $a_{m+2}=3$, we can replace $(s,t)=(3,8)$ by $(r,s)=(1,3)$, if $a_{m+2}=4$, we can replace it by $(r,s)=(4,3)$ and if $a_{m+2}=5$, we can replace it by $(r,s)=(7,3)$.

Our next aim is to show that if we exclude any of the pairs (r,s) or (s,t) appearing in Proposition 2.2, the statement of the proposition will no longer be valid. More precisely, if we exclude a pair $(r',s') \in R_{13}$, then there exist a real number α and a rational number $\frac{a}{b}$ satisfying (2.1), but such that $\frac{a}{b}$ cannot be represented in the form $\frac{a}{b}=\frac{rp_{m+1}+sp_m}{rq_{m+1}+sq_m}$ nor $\frac{a}{b}=\frac{sp_{m+2}-tp_{m+1}}{sq_{m+2}-tq_{m+1}}$, where $m \geqslant -1$, $(r,s) \in R_{13} \setminus \{(r',s')\}$, $(s,t) \in T_{13}$ (and similarly for an excluded pair $(s',t') \in T_{13}$).

In the next table, we give explicit examples for each pair. There are many such examples of different form, but we give some numbers α of the form $\sqrt{d}$, where d is a non-square positive integer.

α	a	b	m	r	s	t
$\sqrt{5328}$	11533	158	1	**1**	**13**	12
$\sqrt{168}$	1063	82	1	**3**	**7**	4
$\sqrt{56}$	943	126	1	**4**	**5**	6
$\sqrt{626}$	30049	1201	0	**24**	**1**	26
$\sqrt{677}$	33851	1301	0	**25**	**1**	27
$\sqrt{5328}$	127957	1753	1	12	**13**	**1**
$\sqrt{168}$	1387	107	1	4	**7**	**3**
$\sqrt{56}$	1377	184	1	6	**5**	**4**
$\sqrt{626}$	32551	1301	0	26	**1**	**24**
$\sqrt{677}$	36557	1405	0	27	**1**	**25**

Let us consider $\alpha=\sqrt{56}=[7,\overline{2,14}]$. The some convergents of $\sqrt{56}$ are $\frac{7}{1}$, $\frac{15}{2}$, $\frac{217}{29}$, $\frac{449}{60}$, $\frac{6503}{869}$, ... Its rational approximation $\frac{943}{126}$ (the third row of the table) satisfies $\left|\sqrt{56}-\frac{943}{126}\right| \lessapprox 0.0008123 < \frac{13}{126^2}$. We have that the only representation of the fraction $\frac{943}{126}$ in the form $\frac{rp_{m+1}+sp_m}{rq_{m+1}+sq_m}$, $(r,s)\in R_{13}$ or $\frac{sp_{m+2}-tp_{m+1}}{sq_{m+2}-tq_{m+1}}$, $(s,t)\in T_{13}$ is $\frac{943}{126}=\frac{4\cdot 217+5\cdot 15}{4\cdot 29+5\cdot 2}=\frac{4\cdot p_2+5\cdot p_1}{4\cdot q_2+5\cdot q_1}$, which implies that the pair $(4,5)$ cannot be excluded from the set R_{13}.

□

3. Case $s=2$

Dujella and Ibrahimpašić [**2**] prove some patterns in pairs (r,s) and (s,t) which appear in representations $(a,b)=(rp_{m+1}+sp_m, rq_{m+1}+sq_m)$ and $(a,b)=(sp_{m+2}-tp_{m+1}, sq_{m+2}-tq_{m+1})$ of solutions of inequality (1.2), where k is a positive integer. They prove that for each positive integer k there exist a real number α and rational numbers $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ such that $\left|\alpha-\frac{a_1}{b_1}\right| < \frac{k}{b_1^2}$ and $\left|\alpha-\frac{a_2}{b_2}\right| < \frac{k}{b_2^2}$ where

$$(a_1,b_1)=(rp_{m+1}+p_m, rq_{m+1}+q_m)$$

and

$$(a_2, b_2) = (p_{m+2} - tp_{m+1}, q_{m+2} - tq_{m+1})$$

, for some $m \geqslant -1$ and integers r and t such that $1 \leqslant r, t \leqslant 2k-1$.

These results for the pairs $(r,s) = (2k-1, 1)$ and $(s,t) = (1, 2k-1)$ (with $\alpha = \sqrt{4k^2+1}$) immediately imply the following result [**2**] which shows that Theorem 1.1 is sharp.

Proposition 3.1. *For each $\varepsilon > 0$ there exist a positive integer k, a real number α and a rational number $\frac{a}{b}$, such that*

$$\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2},$$

and $\frac{a}{b}$ cannot be represented in the form $\frac{a}{b} = \frac{rp_{m+1} \pm sp_m}{rq_{m+1} \pm sq_m}$, for $m \geqslant -1$ and nonnegative integers r and s such that $rs < (2-\varepsilon)k$.

We will prove some patterns in pairs $(r, 2)$ and $(2, t)$.

Let $\alpha_m = [a_m; a_{m+1}, a_{m+2}, \ldots]$ and $\frac{1}{\beta_m} = \frac{q_{m-1}}{q_{m-2}} = [a_{m-1}, a_{m-2}, \ldots, a_1]$, with the convention that $\beta_1 = 0$. Then for $\frac{a}{b} = \frac{rp_{m+1}+sp_m}{rq_{m+1}+sq_m}$, we have

$$\begin{aligned} b^2\left|\alpha - \tfrac{a}{b}\right| &= b\left|(rq_{m+1} + sq_m)\tfrac{\alpha_{m+2}p_{m+1}+p_m}{\alpha_{m+2}q_{m+1}+q_m} - (rp_{m+1} + sp_m)\right| \\ &= \tfrac{|s\alpha_{m+2}-r|(rq_{m+1}+sq_m)}{\alpha_{m+2}q_{m+1}+q_m} = \tfrac{|s\alpha_{m+2}-r|(r+s\beta_{m+2})}{\alpha_{m+2}+\beta_{m+2}}. \end{aligned} \tag{3.1}$$

The relation (3.1) can be reformulated in terms of s and $t = sa_{m+2} - r$:

$$b^2\left|\alpha - \tfrac{a}{b}\right| = \left(t + \tfrac{s}{\alpha_{m+3}}\right)\left|s - \tfrac{t+\frac{s}{\alpha_{m+3}}}{\alpha_{m+2}+\beta_{m+2}}\right|. \tag{3.2}$$

Let $s = 2$. This implies r is odd, since we assume $\gcd(r,s) = 1$. We claim that for $1 < r \leqslant k-1$ (for $r = 1$ see [**2**]), where $k \geqslant 3$, $\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}$ holds. For $x \geqslant 1$, we consider the number $\alpha = \sqrt{(3x)^2 + 3}$. Its continued fraction expansion has the form

$$\sqrt{(3x)^2+3} = \left[3x; \overline{2x, 6x}\right]$$

(see e.g. [**10**, p.297]). For $m \geqslant 1$ we have $\alpha_{2m-1} = [2x, 6x, 2x, 6x, \ldots]$ and $\alpha_{2m} = [6x, 2x, 6x, 2x, \ldots]$, and obtain

$$\begin{array}{ccccc} 2x + \frac{1}{6x+1} & < & \alpha_{2m-1} & < & 2x + \frac{1}{6x} \\ 6x + \frac{1}{2x+1} & < & \alpha_{2m} & < & 6x + \frac{1}{2x} \\ 6x + \frac{1}{2x+1} & < & \frac{1}{\beta_{2m+1}} & \leqslant & 6x + \frac{1}{2x} \\ \frac{1}{6x+\frac{1}{2x+1}} & > & \beta_{2m+1} & \geqslant & \frac{1}{6x+\frac{1}{2x}} . \end{array}$$

If we take $m = -1$ then we have the rational number

$$\frac{a}{b} = \frac{r \cdot p_0 + 2 \cdot p_{-1}}{r \cdot q_0 + 2 \cdot q_{-1}} = \frac{3rx + 2}{r} .$$

We claim that for $r \leqslant k-1$, $\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}$ holds. By (3.1) this is equivalent to

$$\left(2 - \frac{r}{\alpha_1}\right) r < k.$$

It suffices to check that

$$\left(2-\frac{r}{\alpha_1}\right)r<\left(2-\frac{r}{2x+\frac{1}{6x}}\right)r<k\,.$$

If we take $x=\left\lfloor\frac{k}{2}\right\rfloor$, since k is a positive integer, we have only two possibilities: $x=\frac{k}{2}$ or $x=\frac{k-1}{2}$. Thus, we have

$$\left(2-\frac{r}{2x+\frac{1}{6x}}\right)r\leqslant\left(2-\frac{r}{k+\frac{1}{3(k-1)}}\right)r=\frac{6k^2-6k+2-(3k-3)\,r}{3k^2-3k+1}\cdot r<k$$

which implies

$$(3k-3)\,r^2-\left(6k^2-6k+2\right)r+\left(3k^3-3k^2+k\right)>0\,.$$

This condition is satisfied for $r\leqslant k-1$.

The same result for pairs $(r,s)=(r,2)$ holds also if $m\geqslant 1$ is odd. From (3.1), for $r\leqslant k-1$, we have that is suffices to check that

$$\frac{(2\alpha_{m+2}-r)\,(r+2\beta_{m+2})}{\alpha_{m+2}+\beta_{m+2}}<\frac{\left(2\left(2x+\frac{1}{6x}\right)-r\right)\left(r+2\cdot\frac{1}{6x+\frac{1}{2x+1}}\right)}{2x+\frac{1}{6x+1}+\frac{1}{6x+\frac{1}{2x}}}<k\,. \tag{3.3}$$

We take again $x=\left\lfloor\frac{k}{2}\right\rfloor$. In the case $x=\frac{k}{2}$, the condition (3.3) implies

$$\begin{aligned}&\left(81k^6+108k^5+81k^4+45k^3+18k^2+3k\right)r^2-\\&-\left(162k^7+216k^6+162k^5+90k^4+54k^3+12k^2+6k+2\right)r+\\&+\left(81k^8+108k^7+27k^6-36k^5-54k^4-81k^3-33k^2-16k-4\right)>0,\end{aligned}$$

which is satisfied for $r\leqslant k-1$.

In the case $x=\frac{k-1}{2}$, the condition (3.3) implies

$$\begin{aligned}&\left(81k^6-378k^5+756k^4-819k^3+504k^2-168k+24\right)r^2-\\&-\left(162k^7-918k^6+2268k^5-3150k^4+2664k^3-1392k^2+432k-64\right)r+\\&+\left(81k^8-459k^7+1080k^6-1278k^5+639k^4+126k^3-279k^2+86k\right)>0\end{aligned}$$

which is satisfied for $r\leqslant k-1$, too.

We have t is odd, since we assume $\gcd(s,t)=1$. Let us consider pairs $(2,t)$. We claim that for $1<t\leqslant k-1$ (for $t=1$ see [**2**]), where $k\geqslant 3$, $\left|\alpha-\frac{a}{b}\right|<\frac{k}{b^2}$ holds.

Again, for $x\geqslant 1$ we consider the number $\alpha=\sqrt{(3x)^2+3}$.

Take first $m=-1$. We have the rational number

$$\frac{a}{b}=\frac{2\cdot p_1-t\cdot p_0}{2\cdot q_1-t\cdot q_0}=\frac{12x^2+2-3xt}{4x+t}\,.$$

We claim that for $t \leqslant k-1$, $\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}$ holds. By (3.2) this is equivalent to

$$\left(t + \frac{2}{\alpha_2}\right)\left(2 - \frac{t + \frac{2}{\alpha_2}}{\alpha_1 + \beta_1}\right) < k.$$

It suffices to check that

$$\left(t + \frac{2}{\alpha_2}\right)\left(2 - \frac{t + \frac{2}{\alpha_2}}{\alpha_1 + \beta_1}\right) < \left(t + \frac{2}{6x + \frac{1}{2x+1}}\right)\left(2 - \frac{t + \frac{2}{6x + \frac{1}{2x}}}{2x + \frac{1}{6x}}\right) < k\,.$$

If we take $x = \left\lfloor \frac{k}{2} \right\rfloor$, then for $x = \frac{k}{2}$ we have

$$\begin{aligned}
&\left(27k^5 + 27k^4 + 18k^3 + 9k^2 + 3k\right)t^2 - \\
&-\left(54k^6 + 54k^5 + 18k^4 + 6k^2 + 2\right)t + \\
&+\left(27k^7 + 27k^6 - 9k^5 - 18k^4 - 3k^3 - 9k^2 - 3k - 4\right) > 0
\end{aligned}$$

which is satisfied for $t \leqslant k-1$.

In the case $x = \frac{k-1}{2}$, we have

$$\begin{aligned}
&\left(27k^5 - 108k^4 + 180k^3 - 153k^2 + 66k - 12\right)t^2 - \\
&-\left(54k^6 - 270k^5 + 558k^4 - 612k^3 + 384k^2 - 138k + 26\right)t + \\
&+\left(27k^7 - 135k^6 + 261k^5 - 216k^4 + 24k^3 + 72k^2 - 36k\right) > 0
\end{aligned}$$

which is satisfied for $t \leqslant k-1$, too.

The analogous result for pairs $(s,t) = (2,t)$ holds for all odd $m \geqslant 1$. By (3.2) we have that, for $t \leqslant k-1$, is sufficiently to check

$$\left(t + \frac{2}{6x + \frac{1}{2x+1}}\right)\left(2 - \frac{t + \frac{2}{6x + \frac{1}{2x}}}{2x + \frac{1}{6x} + \frac{1}{6x + \frac{1}{2x+1}}}\right) < k\,.$$

Again, if we take $x = \left\lfloor \frac{k}{2} \right\rfloor$, then in the case $x = \frac{k}{2}$, we obtain

$$\left(81k^7 + 162k^6 + 162k^5 + 108k^4 + 54k^3 + 18k^2 + 3k\right)t^2 -$$

$$\left(162k^8 + 324k^7 + 324k^6 + 216k^5 + 126k^4 + 72k^3 + 36k^2 + 12k + 2\right)t +$$

$$\left(81k^9 + 162k^8 + 108k^7 - 63k^5 - 99k^4 - 75k^3 - 51k^2 - 27k - 4\right) > 0\,,$$

and in the case $x = \frac{k-1}{2}$, we have

$$\left(81k^7 - 405k^6 + 891k^5 - 1107k^4 + 837k^3 - 387k^2 + 102k - 12\right)t^2 -$$

$$\left(162k^8 - 972k^7 + 2592k^6 - 3996k^5 + 3906k^4 - 2484k^3 + 1008k^2 - 240k + 26\right)t +$$

$\left(81k^9 - 486k^8 + 1242k^7 - 1674k^6 + 1125k^5 - 117k^4 - 354k^3 + 216k^2 - 36k\right) > 0.$

Both inequalities are satisfied for $t \leqslant k-1$.

We have proved the Theorem 1.3.

4. A Diophantine application

In [**4**], Dujella and Jadrijević considered the Thue inequality

$$\left|x^4 - 4cx^3y + (6c+2)\,x^2y^2 + 4cxy^3 + y^4\right| \leqslant 6c+4,$$

where $c \geqslant 3$ is an integer. Using the method of Tzanakis [**11**], they showed that, for $c \geqslant 5$, solving the Thue equation $x^4 - 4cx^3y + (6c+2)\,x^2y^2 + 4cxy^3 + y^4 = \mu$, $\mu \in \mathbb{Z} \setminus \{0\}$, reduces to solving the system of Pellian equations

$$(2c+1)\,U^2 - 2cV^2 = \mu \tag{4.1}$$

$$(c-2)\,U^2 - cZ^2 = -2\mu, \tag{4.2}$$

where $U = x^2 + y^2$, $V = x^2 + xy - y^2$ and $Z = -x^2 + 4xy + y^2$. It suffices to find solutions of the system (4.1) and (4.2) which satisfy the condition $\gcd(U,V,Z) = 1$. Then $\gcd(U,V) = 1$, and $\gcd(U,Z) = 1$ or 2, since $4V^2 + Z^2 = 5U^2$.

Using the result of Worley [**14**, Corollary, p. 206], in [**4**, Proposition 2] they proved that if μ is an integer such that $|\mu| \leqslant 6c+4$ and that the equation (4.1) has a solution in relatively prime integers U and V, then

$$\mu \in \{1,\ -2c,\ 2c+1,\ -6c+1,\ 6c+4\}.$$

Analysing the system (4.1) and (4.2), and using the properties of convergents of $\sqrt{\frac{2c+1}{2c}}$, they were able to show that the system has no solutions for $\mu = -2c, 2c+1, -6c+1$.

In [**2**], Dujella and Ibrahimpašić, applying results for $k = 9$ to the equation (4.2), gave a new proof of this result for $c \geqslant 5$, based on the precise information on μ's for which (4.2) has a solution in integers U and Z such that $\gcd(U,Z) \in \{1,2\}$.

But, from [**4**, Lemma 4] we have the inequality given in the following lemma.

LEMMA 4.1. *Let $c \geqslant 3$ be an integer. All positive integer solutions (U,V,Z) of the system of Pellian equations (4.1) and (4.2) satisfy*

$$\left|\sqrt{\frac{c-2}{c}} - \frac{Z}{U}\right| < \frac{6c+4}{U^2\sqrt{c\,(c-2)}} < \frac{13}{U^2}. \tag{4.3}$$

Using the result from Section 2, it is now easy to prove that for $c \geqslant 3$, system (4.1) and (4.2) has solutions only for $\mu \in \{1, 6c+4\}$. Using results for $k = 3, 4, \ldots, 13$, from [**2**] and from Section 2, Ibrahimpašić [**6**] completely solved the family of quartic Thue inequalities

$$\left|x^4 - 2cx^3y + 2x^2y^2 + 2cxy^3 + y^4\right| \leqslant 6c+4,$$

where c is a nonnegative integer.

References

[1] A. Dujella, *Continued fractions and RSA with small secret exponents*, Tatra Mt. Math. Publ. **29** (2004), 101–112.

[2] A. Dujella, B. Ibrahimpašić, *On Worley's theorem in Diophantine approximations*, Ann. Math. Inform. **35** (2008), 61–73.

[3] A. Dujella, B. Ibrahimpašić, B. Jadrijević, *Solving a family of quartic Thue inequalities using continued fractions*, Rocky Mountain J. Math. **41** (2011), 1173–1182.

[4] A. Dujella, B. Jadrijević, *A family of quartic Thue inequalities*, Acta Arithmetica **111** (2004), 61–76.

[5] P. Fatou, *Sur l'approximation des incommensurables et les series trigonometriques*, C. R. Acad. Sci. (Paris) **139** (1904), 1019–1021.

[6] B. Ibrahimpašić, *A parametric family of quartic Thue inequalities*, Bull. Malays. Math. Sci. Soc (2) **34** (2011), 215–230.

[7] B. Ibrahimpašić, *Cryptanalysis of KMOV cryptosystem with short secret exponent*, Proceedings of the 19^{th} Central European Conference on Information and Intelligent Systems, September 24–26, 2008, 407–414.

[8] B. Ibrahimpašić, *Cryptanalysis of LUC cryptosystem with short secret exponent*, Book of the Proceedings of the 8^{th} Central European Conference on Cryptography, July 2–4, 2008, Graz, 30–31.

[9] S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley, Reading, 1966.

[10] W. Sierpiński, *Elementary Theory of Numbers*, PWN, Warszawa; North-Holland, Amsterdam, 1987.

[11] N. Tzanakis, *Explicit solution of a class of quartic Thue equations*, Acta Arithmetica **64** (1993), 271–283.

[12] E. R. Verheul, H. C. A. van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Appl. Algebra Engrg. Comm. Computing **8** (1997), 425–435.

[13] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36** (1990), 553–558.

[14] R. T. Worley, *Estimating* $|\alpha - p/q|$, J. Austral. Math. Soc. Ser. A **31** (1981), 202–206.

Received by editor 04.03.2013; Available online 25.03.2013

Faculty of Education, University of Bihać, Luke Marjanovića bb, 77000 Bihać, Bosnia and Herzegovina

E-mail address: `bernadin@bih.net.ba`