On Worley's theorem in Diophantine approximations

Andrej Dujella and Bernadin Ibrahimpašić

Abstract

In this paper we prove several results on connection between continued fractions and rational approximations of the form $|\alpha - a/b| < k/b^2$, for a positive integer k.

1 Introduction

The classical Legendre's theorem in Diophantine approximations states that if a real number α and a rational number $\frac{a}{b}$ (we will always assume that $b \geq 1$), satisfy the inequality

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

then $\frac{a}{b}$ is a convergent of the continued fraction expansion of $\alpha = [a_0; a_1, \ldots]$. This result has been extended by Fatou [3] (see also [5, p.16]), 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.

In 1981, Worley [12] generalized these results to the inequality $\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}$, where k is an arbitrary positive real number. Worley's result was slightly improved in [1].

[0] *2000 Mathematics Subject Classification* Primary 11A55, 11J70; Secondary 11D09.

The first author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 037-0372781-2821.

Theorem 1.1 (Worley [12], Dujella [1]) *Let α be a real number and let a and b be coprime nonzero integers, satisfying the inequality*

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

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

The original result of Worley [12, Theorem 1] contains three types of solutions to the inequality (2). Two types correspond to two possible choices for signs $+$ and $-$ in $(rp_{m+1} \pm sp_m, rq_{m+1} \pm sq_m)$, while [1, Theorem 1] shows that the third type (corresponding to the case $a_{m+2} = 1$) can be omitted.

In Section 3 we will show that Theorem 1.1 is sharp, in the sense that the condition $rs < 2k$ cannot be replaced by $rs < (2-\varepsilon)k$ for any $\varepsilon > 0$. However, it appears that the coefficients r and s show different behavior. So, improvements of Theorem 1.1 are possible if we allow nonsymmetric conditions on r and s. Indeed, already the paper of Worley [12] contains an important contribution in that direction.

Theorem 1.2 (Worley [12], Theorem 2) *If α is an irrational number, $k \geq \frac{1}{2}$ and $\frac{a}{b}$ is a rational approximation to α (in reduced form) for which the inequality (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:*

(i) $\frac{a}{b} = \frac{rp_{m+1}+sp_m}{rq_{m+1}+sq_m}$ $\quad r > s$ *and* $rs < 2k$, *or* $\quad r \leq s$ *and* $rs < k + \frac{r^2}{a_{m+2}}$,

(ii) $\frac{a}{b} = \frac{sp_{m+1}-tp_m}{sq_{m+1}-tq_m}$ $\quad s < t$ *and* $st < 2k$, *or* $\quad s \geq t$ *and* $st\left(1 - \frac{t}{2s}\right) < k$,

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 [12, Corollary, p.206] also gave the explicit version of his result for $k = 2$: $|\alpha - \frac{a}{b}| < \frac{2}{b^2}$ implies $\frac{a}{b} = \frac{p_m}{q_m}, \frac{p_{m+1} \pm p_m}{q_{m+1} \pm q_m}, \frac{2p_{m+1} \pm p_m}{2q_{m+1} \pm q_m}, \frac{3p_{m+1}+p_m}{3q_{m+1}+q_m}, \frac{p_{m+1} \pm 2p_m}{q_{m+1} \pm 2q_m}$ or $\frac{p_{m+1}-3p_m}{q_{m+1}-3q_m}$. This result for $k = 2$ has been applied for solving some Diophantine equations. In [7], it was applied to the problem of finding positive integers a and b such that $(a^2+b^2)/(ab+1)$ is an integer, and in [2] it was used for solving the family of Thue inequalities

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

On the other hand, Theorem 1.1 has applications in cryptography, too. Namely, in [1], a modification of Verheul and van Tilborg variant of Wiener's attack ([10, 11]) on RSA cryptosystem with small secret exponent has been described, which is based on Theorem 1.1.

We will extend Worley's work and give explicit and sharp versions of Theorems 1.1 and 1.2 for $k = 3, 4, 5, \ldots, 12$. We will list the pairs (r, s) which appear in the expression of solutions of (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 hope that our results will also find applications on Diophantine problems, and in Section 4 we will present such an application. In such applications, it is especially of interest to have smallest possible list of pairs (r, s). It is certainly possible to extend our result for $k > 12$. However, already our results make it possible to reveal certain patterns, and they also suffice for our Diophantine applications.

2 Explicit versions of Worley's theorem

We start by few details from the proof of Theorem 1.1 in [1], which will be useful in our future arguments. In particular, we will explain how the integer m appearing in the statement of Theorem 1.1 can be found. We assume that $\alpha < \frac{a}{b}$, since the other case is completely analogous. Let m be the largest odd integer satisfying

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

If $\frac{a}{b} > \frac{p_1}{q_1}$, we take $m = -1$, following the convention that $p_{-1} = 1$, $q_{-1} = 0$. Since $|p_{m+1}q_m - p_m q_{m+1}| = 1$, the numbers r and s defined by

$$\begin{aligned} a &= rp_{m+1} + sp_m, \\ b &= rq_{m+1} + sq_m \end{aligned}$$

are integers, and since $\frac{p_{m+1}}{q_{m+1}} < \frac{a}{b} \leq \frac{p_m}{q_m}$, we have that $r \geq 0$ and $s > 0$. From the maximality of m, we find that

$$\frac{sa_{m+2} - r}{bq_{m+2}} = \left|\frac{p_{m+2}}{q_{m+2}} - \frac{a}{b}\right| < \left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}. \tag{3}$$

From (3) we immediately have

$$a_{m+2} > \frac{r}{s}, \tag{4}$$

and we can derive the inequality

$$r^2 - sra_{m+2} + ka_{m+2} > 0 \tag{5}$$

(see [1, proof of Theorem 1] for details, and note also that (5) is exactly the inequality from Theorem 1.2(i) - the second case).

Let us define a positive integer t by $t = sa_{m+2} - r$. Then we have

$$\begin{aligned} a &= rp_{m+1} + sp_m = sp_{m+2} - tp_{m+1}, \\ b &= rq_{m+1} + sq_m = sq_{m+2} - tq_{m+1}, \end{aligned}$$

and s and t satisfy analogs of (4) and (5):

$$a_{m+2} > \frac{t}{s}, \tag{6}$$

$$t^2 - sta_{m+2} + ka_{m+2} > 0. \tag{7}$$

If $r > t$, i.e. $rs > st$, then we will represent a and b in terms of s and t (which corresponds to $-$ sign in Theorem 1.1).

Let us consider now the case $k = 3$. Hence, we are considering the inequality

$$|\alpha - \frac{a}{b}| < \frac{3}{b^2}. \tag{8}$$

By Theorem 1.1, we have that $(a, b) = (rp_{m+1} + sp_m, rq_{m+1} + sq_m)$ or $(sp_{m+2} - tp_{m+1}, sq_{m+2} - tq_{m+1})$, where $rs < 6$, $st < 6$, $\gcd(r, s) = 1$ and $\gcd(s, t) = 1$. However, the inequalities (5) and (7) for $r = 1$, resp. $t = 1$, show that the pairs $(r, s) = (1, 4), (1, 5)$ and $(s, t) = (4, 1), (5, 1)$ can be omitted. Therefore, we proved

Proposition 2.1 *If a real number α and a rational number $\frac{a}{b}$ satisfy the inequality (8), then $\frac{a}{b} = \frac{rp_{m+1} + sp_m}{rq_{m+1} + sq_m}$, where*

$$(r, s) \in R_3 = \{(0, 1), (1, 1), (1, 2), (1, 3), (2, 1), (3, 1), (4, 1), (5, 1)\},$$

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

$$(s, t) \in T_3 = \{(1, 1), (2, 1), (3, 1), (1, 2), (1, 3), (1, 4), (1, 5)\}$$

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

Our next aim is to show that Proposition 2.1 is sharp, i.e. that if we omit any of the pairs (r,s) or (s,t) appearing in Proposition 2.1, the statement of the proposition will no longer be valid. More precisely, if we omit a pair $(r',s') \in R_3$, then there exist a real number α and a rational number $\frac{a}{b}$ satisfying (8), 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 $m \geq -1$, $(r,s) \in R_3 \setminus \{(r',s')\}$, $(s,t) \in T_3$ (and similarly for an omitted pair $(s',t') \in T_3$).

We will show that by giving explicit examples for each pair. Although we have found many such examples of different form, in the next table we give numbers α of the form $\sqrt{d}$, where d is a non-square positive integer.

α	a	b	m	r	s	t
$\sqrt{10}$	3	1	0	**0**	**1**	6
$\sqrt{17}$	37	9	0	**1**	**1**	7
$\sqrt{2}$	5	4	0	**1**	**2**	3
$\sqrt{8}$	23	8	1	**1**	**3**	2
$\sqrt{17}$	70	17	0	**2**	**1**	6
$\sqrt{26}$	158	31	0	**3**	**1**	7
$\sqrt{26}$	209	41	0	**4**	**1**	6
$\sqrt{37}$	371	61	0	**5**	**1**	7

α	a	b	m	r	s	t
$\sqrt{17}$	235	57	0	7	**1**	**1**
$\sqrt{2}$	11	8	0	3	**2**	**1**
$\sqrt{8}$	37	13	1	2	**3**	**1**
$\sqrt{17}$	202	49	0	6	**1**	**2**
$\sqrt{26}$	362	71	0	7	**1**	**3**
$\sqrt{26}$	311	61	0	6	**1**	**4**
$\sqrt{37}$	517	85	0	7	**1**	**5**

For example, consider $\alpha = \sqrt{8} = [2, \overline{1,4}]$. Its rational approximation $\frac{23}{8}$ (the forth row of the table) satisfies $\left|\sqrt{8} - \frac{23}{8}\right| \approx 0.046572875 < \frac{3}{8^2}$. The convergents of $\sqrt{8}$ are $\frac{2}{1}, \frac{3}{1}, \frac{14}{5}, \frac{17}{6}, \frac{82}{29}, \frac{99}{35}, \frac{478}{169}, \ldots$. The only representation of the fraction $\frac{23}{8}$ in the form $\frac{rp_{m+1}+sp_m}{rq_{m+1}+sq_m}$, $(r,s) \in R_3$ or $\frac{sp_{m+2}-tp_{m+1}}{sq_{m+2}-tq_{m+1}}$, $(s,t) \in T_3$ is $\frac{23}{8} = \frac{1\cdot 14+3\cdot 3}{1\cdot 5+3\cdot 1} = \frac{1\cdot p_2+3\cdot p_1}{1\cdot q_2+3\cdot q_1}$, which shows that the pair $(1,3)$ cannot be omitted from the set R_3.

Proposition 2.2 *Let $k \in \{4,5,6,7,8,9,10,11,12\}$. If a real number α and a rational number $\frac{a}{b}$ satisfy the inequality (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 $m \geq -1$), 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
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	$\{(1,12),(5,4),(7,3),$ $(11,2),(22,1),(23,1)\}$	$\{(12,1),(4,5),(3,7),$ $(2,11),(1,22),(1,23)\}$

Proof: 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 $\gcd(s,t) = 1$. Furthermore, as in the case $k = 3$, it follows directly from the inequalities (5) and (7) for $r = 1$, resp. $t = 1$, that the pairs $(r,s) = (1,s)$ and $(s,t) = (s,1)$ with $s \geq k+1$ can be omitted. 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 $s \geq \frac{k}{2}+2$, and the pairs $(r,s) = (3,s)$ and $(s,t) = (s,3)$ with $s \geq \frac{k}{3}+3$.

Now we show that all remaining possible pairs which are not listed in the statement of Proposition 2.2 can be replaced with other pairs with smaller products rs, resp. st. We give details only for pairs (r,s), since the proof for pairs (s,t) is completely analogous (using the inequalities (6) and (7), instead of (4) and (5)).

Consider the case $k = 4$ and $(r,s) = (2,3)$. By (5), we obtain $a_{m+2} < 2$. Thus, the pair $(r,s) = (2,3)$ can appear only for $a_{m+2} = 1$. However, in that case we have $t = sa_{m+2} - r = 1$, and therefore the $(r,s) = (2,3)$ can be replaced by the pair $(s,t) = (3,1)$.

Analogously we can show that for $k = 7$ the pair $(r,s) = (3,4)$ can be replaced by $(s,t) = (4,1)$, for $k = 8,9,10$ the pair $(r,s) = (3,5)$ can be replaced by $(s,t) = (5,2)$, while for $k = 11,12$ the pair $(r,s) = (4,5)$ can be replaced by $(s,t) = (5,1)$.

We have only three remaining pairs to consider: the pair $(r,s) = (5,3)$ for $k = 8$ and the pairs $(r,s) = (5,4)$ and $(r,s) = (7,3)$ for $k = 11$. For $(r,s) = (5,3)$ and $k = 8$, from (4) and (5) we obtain $\frac{5}{3} < a_{m+2} < \frac{25}{7}$, and therefore we have two possibilities: $a_{m+2} = 2$ or $a_{m+2} = 3$. If $a_{m+2} = 2$, we can replace $(r,s) = (5,3)$ by $(s,t) = (3,1)$, while if $a_{m+2} = 3$, we can replace it by $(s,t) = (3,4)$. Similar approach works for two pairs with $k = 11$. For $(r,s) = (5,4)$, from (4) and (5) we obtain $\frac{5}{4} < a_{m+2} < \frac{25}{9}$, which implies $a_{m+2} = 2$. Then we have $t = 3$ and the pair $(r,s) = (5,4)$ can be replaced by the pair $(s,t) = (4,3)$. For $(r,s) = (7,3)$ we obtain $\frac{7}{3} < a_{m+2} < \frac{49}{10}$, which yields $a_{m+2} = 3$ or $a_{m+2} = 4$. If $a_{m+2} = 3$, we can replace $(r, s) = (7, 3)$ by $(s, t) = (3, 2)$, while if $a_{m+2} = 4$, we can replace it by $(s, t) = (3, 5)$.

It remains to show that all pairs listed in the statement of the proposition are indeed necessary (they cannot be omitted). This is shown by the examples from the following tables:

$k = 4$						
α	a	b	m	r	s	t
$\sqrt{35}$	89	15	1	**1**	**4**	3
$\sqrt{39}$	968	155	1	**3**	**2**	5
$\sqrt{50}$	601	85	0	**6**	**1**	8
$\sqrt{65}$	911	113	0	**7**	**1**	9
$\sqrt{35}$	219	37	1	3	**4**	**1**
$\sqrt{39}$	1580	253	1	5	**2**	**3**
$\sqrt{50}$	799	113	0	8	**1**	**6**
$\sqrt{65}$	1169	145	0	9	**1**	**7**

$k = 5$						
α	a	b	m	r	s	t
$\sqrt{80}$	197	22	1	**1**	**5**	4
$\sqrt{12}$	111	32	1	**2**	**3**	4
$\sqrt{82}$	1313	145	0	**8**	**1**	10
$\sqrt{101}$	1819	181	0	**9**	**1**	11
$\sqrt{80}$	653	73	1	4	**5**	**1**
$\sqrt{12}$	201	58	1	4	**3**	**2**
$\sqrt{82}$	1639	181	0	10	**1**	**8**
$\sqrt{101}$	2221	221	0	11	**1**	**9**

$k = 6$						
α	a	b	m	r	s	t
$\sqrt{194}$	6421	461	3	**1**	**6**	5
$\sqrt{84}$	5105	557	1	**5**	**2**	7
$\sqrt{122}$	2441	221	0	**10**	**1**	12
$\sqrt{145}$	3191	265	0	**11**	**1**	13
$\sqrt{194}$	989	71	1	5	**6**	**1**
$\sqrt{84}$	7103	775	1	7	**2**	**5**
$\sqrt{122}$	2927	265	0	12	**1**	**10**
$\sqrt{145}$	3769	313	0	13	**1**	**11**

$k = 7$						
α	a	b	m	r	s	t
$\sqrt{360}$	835	44	1	**1**	**7**	6
$\sqrt{48}$	215	31	1	**2**	**5**	3
$\sqrt{87}$	2136	229	1	**4**	**3**	5
$\sqrt{170}$	4081	313	0	**12**	**1**	14
$\sqrt{197}$	5123	365	0	**13**	**1**	15
$\sqrt{360}$	4345	229	1	6	**7**	**1**
$\sqrt{48}$	305	44	1	3	**5**	**2**
$\sqrt{87}$	2649	284	1	5	**3**	**4**
$\sqrt{170}$	4759	365	0	14	**1**	**12**
$\sqrt{197}$	5909	421	0	15	**1**	**13**

$k = 8$						
α	a	b	m	r	s	t
$\sqrt{674}$	39799	1533	3	**1**	**8**	7
$\sqrt{90}$	1129	119	1	**3**	**4**	5
$\sqrt{147}$	16574	1367	1	**7**	**2**	9
$\sqrt{226}$	6329	421	0	**14**	**1**	16
$\sqrt{257}$	7711	481	0	**15**	**1**	17
$\sqrt{674}$	4751	183	1	7	**8**	**1**
$\sqrt{90}$	1831	193	1	5	**4**	**3**
$\sqrt{147}$	21254	1753	1	9	**2**	**7**
$\sqrt{226}$	7231	481	0	16	**1**	**14**
$\sqrt{257}$	8737	545	0	17	**1**	**15**

$k = 9$						
α	a	b	m	r	s	t
$\sqrt{1088}$	2441	74	1	**1**	**9**	8
$\sqrt{105}$	4273	417	1	**5**	**3**	7
$\sqrt{290}$	9281	545	0	**16**	**1**	18
$\sqrt{325}$	11051	613	0	**17**	**1**	19
$\sqrt{1088}$	17449	529	1	8	**9**	**1**
$\sqrt{105}$	5933	579	1	7	**3**	**5**
$\sqrt{290}$	10439	613	0	18	**1**	**16**
$\sqrt{325}$	12349	685	0	19	**1**	**17**

$k = 10$						
α	a	b	m	r	s	t
$\sqrt{1762}$	163917	3905	3	**1**	**10**	9
$\sqrt{228}$	41207	2729	1	**9**	**2**	11
$\sqrt{362}$	13033	685	0	**18**	**1**	20
$\sqrt{401}$	15239	761	0	**19**	**1**	21
$\sqrt{1762}$	15909	379	1	9	**10**	**1**
$\sqrt{228}$	50297	3331	1	11	**2**	**9**
$\sqrt{362}$	14479	761	0	20	**1**	**18**
$\sqrt{401}$	16841	841	0	21	**1**	**19**

$k = 11$						
α	a	b	m	r	s	t
$\sqrt{2600}$	5711	112	1	**1**	**11**	10
$\sqrt{224}$	973	65	1	**2**	**7**	5
$\sqrt{240}$	2990	193	1	**3**	**5**	7
$\sqrt{442}$	17681	841	0	**20**	**1**	22
$\sqrt{485}$	20371	925	0	**21**	**1**	23
$\sqrt{2600}$	52061	1021	1	10	**11**	**1**
$\sqrt{224}$	2275	152	1	5	**7**	**2**
$\sqrt{240}$	6770	437	1	7	**5**	**3**
$\sqrt{442}$	19447	925	0	22	**1**	**20**
$\sqrt{485}$	22309	1013	0	23	**1**	**21**

$k = 12$						
α	a	b	m	r	s	t
$\sqrt{3842}$	518743	8369	3	**1**	**12**	11
$\sqrt{235}$	7159	467	1	**5**	**4**	7
$\sqrt{27}$	1933	372	1	**7**	**3**	8
$\sqrt{327}$	86564	4787	1	**11**	**2**	13
$\sqrt{530}$	23321	1013	0	**22**	**1**	24
$\sqrt{577}$	26543	1105	0	**23**	**1**	25
$\sqrt{3842}$	42335	683	1	11	**12**	**1**
$\sqrt{235}$	9949	649	1	7	**4**	**5**
$\sqrt{27}$	2198	423	1	8	**3**	**7**
$\sqrt{327}$	102224	5653	1	13	**2**	**11**
$\sqrt{530}$	25439	1105	0	24	**1**	**22**
$\sqrt{577}$	28849	1201	0	25	**1**	**23**

■

3 Cases $r = 1$, $s = 1$ and $t = 1$

The results from the previous section suggest that there are 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 (2). In particular, these patterns are easy to recognize for pairs of the form $(r, s) = (r, 1)$ or $(1, s)$, and $(s, t) = (s, 1)$ or $(1, t)$. In this section we will prove that the results on these pairs, already proved for $k \leq 12$, are valid in general. These facts will allow us to show that the inequality $rs < 2k$ in Theorem 1.1 is sharp.

We will assume that k is a positive integer. From Theorem 1.1 it directly follows that among the pairs of the form $(r, 1)$, only pairs where $r \le 2k-1$ can appear. Similarly, for pairs $(1, t)$ we have $t \le 2k-1$. On the other hand, from (5) and (7) it follows that for pairs $(1, s)$ we have $s \le k$, and for pairs $(s, 1)$ we have $s \le k$. These results follow also from Theorem 1.2. We will show that all these pairs that do not contradict Theorem 1.2 can indeed appear.

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

$$\begin{aligned} b^2\left|\alpha - \tfrac{a}{b}\right| &= b\left|(rq_{m+1}+sq_m)\tfrac{\alpha_{m+2}p_{m+1}+p_m}{\alpha_{m+2}q_{m+1}+q_m} - (rp_{m+1}+sp_m)\right| \\ &= \tfrac{|s\alpha_{m+2}-r|(rq_{m+1}+sq_m)}{\alpha_{m+2}q_{m+1}+q_m} = \tfrac{|s\alpha_{m+2}-r|(r+s\beta_{m+2})}{\alpha_{m+2}+\beta_{m+2}}. \end{aligned} \tag{9}$$

We start with the pairs of the form $(r, 1)$. Let us consider the number $\alpha = \sqrt{4k^2+1}$. Its continued fraction expansion has the form

$$\sqrt{4k^2+1} = [2k; \overline{4k}]$$

(see e.g. [8, p.297]). Take first $m = -1$, i.e. consider the rational number $\frac{a}{b}$ defined by

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

Hence, $a = 2rk+1$ and $b = r$. We claim that for $r \le 2k-1$ it holds $\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}$. By (9), this is equivalent to $\left(1 - \frac{r}{\alpha_1}\right) r < k$. For $m \ge 1$ we have $\alpha_m = [4k, 4k, \ldots] < 4k + \frac{1}{4k}$. Thus, it suffices to check that $4kr^2 - (16k^2+1)r + 16k^3 + k > 0$, what is clearly satisfied for $r \le 2k-1$. More precisely, this is satisfied for r less than $\frac{16k^2+1-\sqrt{16k^2+1}}{8k} > 2k - \frac{1}{2}$.

We can proceed similarly for $m \ge 0$. The only difference is that $4k < \frac{1}{\beta_{m+2}} = [4k, \ldots, 4k] < 4k + \frac{1}{4k}$. Hence, by (9), we obtain that it suffices to check that for $r \le 2k-1$ it holds

$$\left(4k + \frac{1}{4k} - r\right) \frac{r + \frac{1}{4k}}{4k + \frac{2}{4k+\frac{1}{4k}}} < k.$$

But this condition is equivalent to $(256k^4 + 16k^2)r^2 - (1024k^5 + 64k^3)r + (1024k^6 - 64k^4 - 32k^2 - 1) > 0$, which holds for r less than $2k - \frac{3}{4}$, so it certainly holds for $r \le 2k-1$.

The same example $\alpha = \sqrt{4k^2+1}$ can be used to handle the pairs $(s,t) = (1,t)$. The relation (9) can be reformulated in terms of s and $t = sa_{m+2} - r$:

$$b^2\left|\alpha - \tfrac{a}{b}\right| = \left(t + \tfrac{s}{\alpha_{m+3}}\right)\left|s - \tfrac{t+\frac{s}{\alpha_{m+3}}}{\alpha_{m+2}+\beta_{m+2}}\right|. \tag{10}$$

Now, for $m = -1$ we are considering the rational number

$$\frac{a}{b} = \frac{s\cdot p_1 - t\cdot p_0}{s\cdot q_1 - t\cdot q_0} = \frac{8k^2+1-2tk}{4k-t} = 2k + \frac{1}{4k-t}.$$

By (10), the condition $\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}$ leads to $16k^2t^2 - 64k^3t + 64k^4 - 12k^2 - 1 > 0$. Similarly, for $m \geq 0$, we obtain the condition $8k^2t^2 - (32k^3+2k)t + 32k^4 - 4k^2 - 1 > 0$. It is easy to see that both conditions are satisfied for $t \leq 2k-1$.

For pairs of the form $(1,s)$ and $(s,1)$ we use α of the form $\alpha = \sqrt{x^2-1}$, where the integer x will be specified later (if necessary). For $x \geq 2$, we have the following continued fraction expansion

$$\sqrt{x^2-1} = [x-1; \overline{1, 2x-2}]$$

(see e.g. [8, p.297]). Let us consider the pairs of the form $(r,s) = (1,s)$. We take $m = -1$ and define the rational number

$$\frac{a}{b} = \frac{1\cdot p_0 + s\cdot p_{-1}}{1\cdot q_0 + s\cdot q_{-1}} = \frac{x-1+s}{1}.$$

Hence, $a = x-1+s$ and $b = 1$, and for $s \leq k$ it holds

$$\left|\alpha - \tfrac{a}{b}\right| < (x-1+s) - (x-1) = s \leq \tfrac{k}{b^2}.$$

The same result for pairs $(r,s) = (1,k)$ holds also if $m \geq 1$ is odd and if x is sufficiently large. Indeed, from (9) we obtain the condition

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

which is satisfied for $x \geq \frac{k^2-2k+5}{2}$.

Finally, consider the pairs of the form $(s,t) = (s,1)$ for $s \leq k$. Take $m = -1$ and define the rational number

$$\frac{a}{b} = \frac{s\cdot p_1 - 1\cdot p_0}{s\cdot q_1 - 1\cdot q_0} = \frac{sx-x+1}{s-1} = x + \frac{1}{s-1}.$$

Hence, $a = sx - x + 1$ and $b = s - 1$. We have $\sqrt{x^2-1} > \frac{p_2}{q_2} = x - \frac{1}{2x-1}$. Thus,

$$\left|\alpha - \tfrac{a}{b}\right| < \tfrac{1}{s-1} + \tfrac{1}{2x-1},$$

and we obtain the condition

$$\frac{1}{s-1} + \frac{1}{2x-1} < \frac{k}{(s-1)^2}. \tag{11}$$

If we choose x to be greater than $\frac{k^2-2k+2}{2}$, then we have $\frac{1}{2x-1} < \frac{1}{(k-1)^2}$, while for $s \le k$ it hold $\frac{k}{(s-1)^2} - \frac{1}{s-1} \ge \frac{k}{(k-1)^2} - \frac{1}{k-1} = \frac{1}{(k-1)^2}$, and we showed that for such x's the condition (11) is fulfilled.

Again, the analogous result for pairs $(s,t) = (k,1)$ holds for all odd $m \ge 1$, but x has to be larger than in the case $m = -1$. Namely, the relation (10) yields the condition

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

which is satisfied for $x \ge \frac{k^2-k+6}{2}$.

Our 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 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 $m \ge -1$ and nonnegative integers r and s such that $rs < (2-\varepsilon)k$.

PROOF: Take $k > \frac{1}{\varepsilon}$, $\alpha = \sqrt{4k^2+1}$ and e.g. $\frac{a}{b} = \frac{2k(2k-1)+1}{2k-1}$. Then $\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2}$. If $m = -1$, then $r = 2k-1$, $s = 1$, $t = 2k+1$, and thus $rs = 2k-1 > 2k - k\varepsilon = (2-\varepsilon)k$, while $st = 2k+1$. If $m \ge 0$, then from $s = -bp_{m+1} + aq_{m+1}$ it follows that $|s| \ge \left|\frac{a}{b} - \frac{p_1}{q_1}\right| bq_1 = 2k+1$, and therefore $|rs| \ge 2k+1$ and $|st| \ge 2k+1$. ■

4 A Diophantine application

In [2], Dujella and Jadrijević considered the Thue inequality

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

where $c \geq 5$ is an integer. In this section we will assume that $c \geq 5$, since the cases $c = 3$ and $c = 4$ require somewhat different details. Using the method of Tzanakis [9], they showed that 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

$$\begin{aligned} (2c+1)\,U^2 - 2cV^2 &= \mu && (12)\\ (c-2)\,U^2 - cZ^2 &= -2\mu, && (13) \end{aligned}$$

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 (12) and (13) which satisfy the condition $\gcd(U, V, Z) = 1$. Then $\gcd(U, V) = 1$, and $\gcd(U, Z) = 1$ or 2, since $4V^2 + Z^2 = 5U^2$. It is clear that the solutions of the system (12) and (13) induce good rational approximations of the corresponding quadratic irrationals. More precisely, from [2, Lemma 4] we have the inequalities given in the following lemma.

Lemma 4.1 *Let $c \geq 5$ be an integer. All positive integer solutions (U, V, Z) of the system of Pellian equations (12) and (13) satisfy*

$$\begin{aligned} \left|\sqrt{\frac{2c+1}{2c}} - \frac{V}{U}\right| &< \frac{2}{U^2} && (14)\\ \left|\sqrt{\frac{c-2}{c}} - \frac{Z}{U}\right| &< \frac{6c+4}{U^2\sqrt{c\,(c-2)}} < \frac{9}{U^2}. && (15) \end{aligned}$$

Using the result of Worley [12, Corollary, p. 206], in [2, Proposition 2] the authors proved that if μ is an integer such that $|\mu| \leq 6c+4$ and that the equation (12) has a solution in relatively prime integers U and V, then

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

Analysing the system (12) and (13), and using the properties of convergents of $\sqrt{\frac{2c+1}{2c}}$, they were able to show that the system has no solutions for $\mu = -2c, 2c+1, -6c+1$. Applying results from the previous sections to the equation (13), we will present here a new proof of that result, based on the precise information on μ's for which (13) has a solution in integers U and Z such that $\gcd(U,Z) \in \{1,2\}$.

The simple continued fraction expansion of a quadratic irrational $\alpha = \frac{e+\sqrt{d}}{f}$ is periodic. This expansion can be obtained using the following algorithm. Multiplying the numerator and the denominator by f, if necessary, we may assume that $f|(d-e^2)$. Let $s_0 = e$, $t_0 = f$ and

$$a_n = \left\lfloor \frac{s_n+\sqrt{d}}{t_n} \right\rfloor, \quad s_{n+1} = a_n t_n - s_n, \quad t_{n+1} = \frac{d-s_{n+1}^2}{t_n} \quad \text{for } n \geq 0 \tag{16}$$

(see [6, Chapter 7.7]). If $(s_j,t_j) = (s_k,t_k)$ for $j < k$, then

$$\alpha = [a_0; \dots, a_{j-1}, \overline{a_j, \dots, a_{k-1}}].$$

Applying this algorithm to $\sqrt{\frac{c-2}{c}} = \frac{\sqrt{c(c-2)}}{c}$, we find that

$$\sqrt{\frac{c-2}{c}} = [0; 1, \overline{c-2, 2}].$$

According to our results (Proposition 2.2 for $k=9$), applied to $\alpha = \sqrt{\frac{c-2}{c}}$, all solutions of (13) have the form $Z/U = (rp_{m+1}+sp_m)/(rq_{m+1}+sq_m)$ an index $m \geq -1$ and integers r and s. For the determination of the corresponding μ's, we use the following result (see [2, Lemma 1]):

Lemma 4.2 *Let $\alpha\beta$ be a positive integer which is not a perfect square, and let p_m/q_m denotes the mth convergent of the continued fraction expansion of $\sqrt{\frac{\alpha}{\beta}}$. Let the sequences (s_m) and (t_m) be defined by (16) for the quadratic irrational $\frac{\sqrt{\alpha\beta}}{\beta}$. Then*

$$\begin{aligned} &\alpha(rq_{m+1}+sq_m)^2 - \beta(rp_{m+1}+sp_m)^2 \\ &= (-1)^m(s^2 t_{m+1} + 2rs s_{m+2} - r^2 t_{m+2}). \end{aligned} \tag{17}$$

Since the period of continued fraction expansion of $\sqrt{\frac{c-2}{c}}$ is equal to 2, according to Lemma 4.2, we have to consider only the fractions $(rp_{m+1} + sp_m)/(rq_{m+1}+sq_m)$ for $m=1$ and $m=2$. By checking all possibilities, we obtain the following result.

Proposition 4.3 *Let μ be an integer such that $|\mu| \leq 6c+4$ and that the equation*

$$(c-2)U^2 - cZ^2 = -2\mu$$

has a solution in integers U and Z such that $\gcd(U,Z) = 1$ or 2.

(i) If $c \geq 15$ *is odd, then*

$$\mu \in M_1 = \{1, 4, 2c, 4c+1, 6c+4, -2c+4, -4c+9, -6c+16\}.$$

Furthermore, if $c = 5, 11, 13$, *then* $\mu \in M_1 \cup \{-8c+25\}$*; if* $c = 9$, *then* $\mu \in M_1 \cup \{-8c+25, -10c+36\}$*; if* $c = 7$, *then* $\mu \in M_1 \cup \{-8c+25, -10c+36, -12c+49\}$.

(ii) Let $M = M_1 \cup M_2$, *where*

$$M_2 = \left\{-\frac{11}{2}c+36, -\frac{9}{2}c+25, -\frac{7}{2}c+16, -\frac{5}{2}c+9, -\frac{3}{2}c+4, -\frac{1}{2}c+1, \frac{1}{2}c, \frac{3}{2}c+1, \frac{5}{2}c+4, \frac{7}{2}c+9\right\}.$$

If $c \geq 108$ *is even, then* $\mu \in M \cup \left\{\frac{9}{2}c+16, \frac{11}{2}c+25\right\}$.

For even c *with* $6 \leq c \leq 106$, *we have* $\mu \in M \cup M^{(c)}$, *where* $M^{(c)}$ *can be given explicitly, as in the case (i). E.g.*

$$M^{(6)} = \left\{-\frac{21}{2}c+25, -10c+36, -8c+25, -\frac{15}{2}c+16\right\}.$$

Comparing the set $\{1, -2c, 2c+1, -6c+1, 6c+4\}$ from [2, Proposition 2] with the sets appearing in Proposition 4.3, we obtain the desired conclusion.

Corollary 4.4 *Let* $c \geq 5$ *be an integer. If the system (12) and (13) has a solution with* $|\mu| \leq 6c+4$ *in relatively prime integers* U, V *and* Z, *then* $\mu = 1$ *or* $\mu = 6c+4$.

References

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

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

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

[4] J. F. Koksma, *On continued fraction*, Simon Stevin **29** (1951/52), 96–102.

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

[6] I. Niven, H. S. Zuckerman and H. L. Montgomery, An Introduction to the Theory of Numbers, John Wiley, New York, 1991.

[7] C. F. Osgood, F. Luca, P. G. Walsh, *Diophantine approximations and a problem from the 1988 IMO*, Rocky Mountain J. Math. **36** (2006), 637–648.

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

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

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

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

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

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

Bernadin Ibrahimpašić
Pedagogical Faculty, University of Bihać
Džanića mahala 36, 77000 Bihać, Bosnia and Herzegovina
E-mail address: `bernadin@bih.net.ba`