# DIOPHANTINE APPROXIMATIONS AND A PROBLEM FROM THE 1988 IMO 

F. LUCA, C.F. OSGOOD AND P.G. WALSH


#### Abstract

Harborth has recently shown how to describe all integer solutions to a Diophantine equation arising from a problem at the 1988 International Mathematical Olympiad. Harborth uses a clever reduction method, although it seems that this method is somewhat ad hoc. The purpose of the present paper is to show how the result of Harborth can be proved, and extended, using the classical theory of continued fractions. More to the point, a shortcoming in this classical theory is circumvented by an extension to Legendre's theorem concerning a sufficient condition for a rational integer to be a convergent to a given irrational number.


1. Introduction. Problem 6 from the 1988 International Mathematical Olympiad asked the participants to prove that if $a$ and $b$ are positive integers for which

$$
\begin{equation*}
k=\frac{a^{2}+b^{2}}{a b+1} \tag{1.1}
\end{equation*}
$$

is an integer, then $k$ must be the square of an integer. Recently, Harborth [3] has taken this problem one step further by providing closed formulas for the complete solution set of triples of integers ( $a, b, k$ ) satisfying (1.1).

A simple rearrangement of (1.1), together with the substitution $x=b k-2 a, y=b$ shows that solutions $(a, b, k)$ of (1.1) are in correspondence with solutions $(x, y, k)$ of the quadratic equation

$$
\begin{equation*}
x^{2}-\left(k^{2}-4\right) y^{2}=4 k \tag{1.2}
\end{equation*}
$$

If $k$ is even, or if $\operatorname{gcd}(x, y)>2$, then it is relatively simple to determine the solutions to (1.2) using the basic theory of continued fractions. To see this, assume first that $k$ is even, $k=2 l$ say, and assume that $k>2$,

[^0]as the case $k=2$ is trivial. It follows that $x$ is even, say $x=2 z$, and that $z^{2}-\left(l^{2}-1\right) y^{2}=2 l$. Considering this equation modulo 8 shows that $z, y$ and $l$ are all even, and furthermore if $z_{1}=z / 2, y_{1}=y / 2$, then $z_{1}^{2}-\left(l^{2}-1\right) y_{1}^{2}=l / 2$. It follows from the theory of diophantine approximations (in particular Legendre's theorem, about which we will say more in a later section), that $z_{1} / y_{1}$ is a convergent to $\sqrt{l^{2}-1}$. From the special form of this particular quadratic discriminant, it follows that $l / 2$ is the square of an integer, and that $\sqrt{l / 2}$ must divide both $z_{1}$ and $y_{1}$, i.e., that $x+y \sqrt{k^{2}-4}$ is an integer multiple of a unit in $\mathbf{Z}\left[\sqrt{l^{2}-1}\right]$. Therefore, $k$ must be the square of an integer, $\sqrt{k}$ divides $x$ and $\sqrt{k} / 2$ divides $y$. In the case that $\operatorname{gcd}(x, y)>2$ and $k=2 l$ is even, then $x /(2 y)$ is a convergent to $\sqrt{l^{2}-1}$, and the same conclusions as in the previous case are determined. In the case that $\operatorname{gcd}(x, y)>2$ and $k$ is odd, then $(2 x+y) /(2 y)$ is a convergent to $\left(1+\sqrt{k^{2}-4}\right) / 2$ and once again the same conclusions are drawn. Finally, if $\operatorname{gcd}(x, y)=2$ and $k$ is odd, it is then easy to check that $\left(x_{1}, y_{1}\right)$ given by $x_{1}=(x / 2) k+(y / 2)\left(k^{2}-4\right)$, $y_{1}=(x / 2)+(y / 2) k$ is a solution to (1.2) satisfying $\operatorname{gcd}\left(x_{1}, y_{1}\right)=1$.

The point of this preamble is to point out that the only potential difficulty in solving (1.2) arises in the case that $k$ is odd and $\operatorname{gcd}(x, y)=$ 1. The method of using continued fractions, as described above, does not provide a means to rule out the possibility of integer solutions to (1.2) in this case. There is relevant work of Hurwitz [4], Fatou [1], Grace [2] and of Khinchin [5] on mediating fractions. Also, Selenius [7] has proved some interesting related results, but we are unable to find explicit statements that will enable the direct resolution of equation (1.2).

The main purpose of the present paper is to expand on the current state of knowledge about continued fractions, in the sense of generalizing a classical theorem of Legendre. In particular, necessary conditions will be described for when a fraction is a good approximation to a real number, but not good enough to be deemed a true convergent. We will then apply these results to quadratic fields, and see that solving certain types of quadratic diophantine equations, such as (1.2), can then be achieved with minimal effort.
2. Harborth's reduction method. Before proceeding to the main part of our work, we describe Harborth's method for the sake of completeness. Furthermore, we provide a somewhat different description
of the solution set of equation (1.1). What seems most interesting is that this method, which is designed to solve (1.1), provides a way to completely solve equation (1.2). We will be terse for the sake of brevity.

Theorem 2.1. All positive integers $(a, b, k)$, with $a \leq b$, for which $k=\left(a^{2}+b^{2}\right) /(a b+1)$ is an integer are given by

1. $k$ odd. $(a, b, k)=\left(l y,\left(l x+l^{3} y\right) / 2, l^{2}\right)$, where $(x, y)$ satisfy $x^{2}-$ $\left(l^{4}-4\right) y^{2}=4$.
2. $k$ even. $(a, b, k)=\left(l y, l x+\left(l^{3} / 2\right) y, l^{2}\right)$, where $(x, y)$ satisfy $x^{2}-\left(4 l^{4}-1\right) y^{2}=1$.

The main idea of the proof of Theorem 2.1 is given in the following result.

Lemma 2.1. Let $a<b$ be positive integers such that $b=m a+r$ with $1 \leq r \leq a-1$, and put $s=a-r$. Then $(a, b, k)$ is a solution to (1.1) if and only if $(a, s, k)$ is a solution to (1.1), and if this occurs, $k=m+1$.

Proof. Putting $b=m a+r$ into (1.1) and solving for $k$, we find that

$$
\begin{equation*}
k=m+\frac{a^{2}+m a r+r^{2}-m}{m a^{2}+r a+1} \tag{2.1}
\end{equation*}
$$

The fraction in (2.1) is strictly between 0 and 3 , and being an integer, must then either be equal to 1 or 2 . We first show that the latter is not possible. If $k \geq 6$, then $m \geq 4$, and it is a simple exercise to check that the fraction in (2.1) cannot be 2. Also, one can verify that (1.1) has no solutions for $k=2,3,5$, and that the only solution for $k=1$ is $(a, b)=(1,1)$. Finally, if $k=4$, then $(a, b)=(2 y, 2 x+4 y)$ where $x^{2}-3 y^{2}=1$. Therefore, $b / a=(x / y)+2>3$, forcing $m=3$, and the fraction in (2.1) to be 1 .
We have shown that $k=m+1$, and that

$$
a^{2}+m a r+r^{2}-m=m a^{2}+r a+1
$$

Substituting $a-s$ for $r$ in this last equation, and some rearranging yields

$$
a^{2}+s^{2}=(m+1)(a s+1)
$$

which proves the only if portion of the theorem. For the converse, if $(a, s, m+1)$ is a solution to (1.1), then putting $b=m a+(a-s)$, one can see that $(a, b, k)$ is also a solution.

Theorem 2.1 is now a simple consequence of this lemma and the remarks in the Introduction. First of all, it is clear that all of the solutions given in the statement of Theorem 2.1 satisfy (1.1). To show that all solutions of (1.1) are of the described form, let $(a, b, k)$ be a solution of $(1.1)$. If $\operatorname{gcd}(a, b)>2$, then one obtains a solution $(x, y)$ to (1.2) with $\operatorname{gcd}(x, y)>2$. The remarks given in the Introduction show how such a solution must be an integer multiple of a unit in either $\mathbf{Z}\left[\sqrt{l^{2}-1}\right]$, where $k=2 l$, or $\mathbf{Z}\left[\left(1+\sqrt{k^{2}-4}\right) / 2\right]$ in the case that $k$ is odd. By considering the two cases of the parity of $k$ separately, one is led to a solution of the form described in the statement of the theorem. If $\operatorname{gcd}(a, b)=2$, then there exists a solution to (1.2) with $\operatorname{gcd}(x, y)=2$. If $k$ is odd, then as described in the previous section, this leads to a solution $(x, y)$ to (1.2) with $\operatorname{gcd}(x, y)=1$, and hence to a solution $(a, b)$ of (1.1) with $\operatorname{gcd}(a, b)=1$, and this will be dealt with henceforth. If $(x, y)$ is a solution to (1.2) with $\operatorname{gcd}(x, y)=2$ and $k=2 l$, then 4 divides $x$. It follows that $(x / 4) /(y / 2)$ is a convergent to $\sqrt{l^{2}-1}$, and the argument proceeds as in the previous cases. Finally, if $(a, b, k)$ is a solution to (1.1) with $\operatorname{gcd}(a, b)=1$ and $b>a$, then in the notation of Lemma 2.1, $(a, s, k)$ is also a solution and satisfies $a>s>0, \operatorname{gcd}(a, s)=1$. Repeating this reduction procedure must eventually lead to a solution $\left(s_{1}, 1, k\right)$, where $s_{1}>1$, contradicting the fact that $(a, b, k)=(1,1,1)$ is the only solution to (1.1) with one of $a$ or $b$ equal to 1 .

We see then that the method of Harborth not only determines all solutions to (1.1), but also provides a clever, but somewhat ad hoc, approach for solving equation (1.2). We state this as a corollary to Theorem 2.1.

Corollary 2.1. If $k>1$ is an odd integer, then the quadratic equation

$$
x^{2}-\left(k^{2}-4\right) y^{2}=4 k
$$

has no solutions in coprime integers $(x, y)$.

As mentioned before, it is very surprising that this result can be proved using the reduction techniques described in the proof of Lemma 2.1 and yet does not follow directly from known results in the theory of diophantine approximation, in particular, from Legendre's necessary condition for an approximation to be a convergent. The next section is an attempt to remedy this situation.
3. Diophantine approximations. Throughout this discussion, $\alpha$ will denote an irrational number. Legendre proved that if a rational number $p / q$ satisfies $|\alpha-p / q|<1 /\left(2 q^{2}\right)$, then $p / q$ is a convergent to $\alpha$. As we have seen above, this result is not strong enough to show that (1.2) is not solvable in coprime integers $x$ and $y$. In this section we describe necessary conditions when a given approximation is not quite good enough to be concluded a convergent.
Throughout the paper we will make reference to the usual notation concerning the continued fraction expansion of an irrational number. In particular, if

$$
\alpha=a_{0}+\frac{1}{a_{1}+\frac{1}{a_{2}+\ldots}}
$$

for an integer $a_{0}$ and positive integers $a_{1}, a_{2}, \ldots$, then this is the continued fraction expansion of $\alpha$, denoted neatly by $\alpha=\left[a_{0} ; a_{1}, a_{2} \ldots\right]$, each $a_{n}$ is a partial quotient, and the convergents to $\alpha$ are given by

$$
\frac{p_{n}}{q_{n}}=\left[a_{0} ; a_{1}, a_{2} \ldots, a_{n}\right],\left(p_{n}, q_{n}\right)=1 .
$$

The numerators and denominators of convergents satisfy the recursion formulae

$$
p_{n+1}=a_{n+1} p_{n}+p_{n-1}, q_{n+1}=a_{n+1} q_{n}+q_{n-1} \quad \text { for } \quad n \geq 1
$$

We will use the fact that, for each $n \geq 0$, the inequality

$$
\begin{equation*}
\left|\alpha-\frac{p_{n}}{q_{n}}\right|<\frac{1}{q_{n} q_{n+1}} \tag{3.1}
\end{equation*}
$$

holds (for example, see Lemma 3E of [6]). For more details on continued fractions, and their properties, the reader is referred to either $[\mathbf{5}]$ or $[\mathbf{6}]$.

Definition. Assume that $\alpha$ has the continued fraction expansion given above. A mediating fraction to $\alpha$ is any rational number $p / q$ of the form

$$
p=m p_{n}+p_{n-1}, q=m q_{n}+q_{n-1}
$$

where $1 \leq m \leq a_{n+1}$.

Notice that a convergent is the special case of a mediating fraction, namely when $m=a_{n+1}$.

Theorem 3.1. Let $\alpha$ denote an irrational number and $r / s$ a rational number in reduced form, with $s \geq \max \left(2, q_{1}\right)$, such that

$$
\begin{equation*}
\left|\alpha-\frac{r}{s}\right|<\frac{2}{s^{2}} . \tag{3.2}
\end{equation*}
$$

Then there exist integers $n \geq 1$ and $1 \leq m<a_{n+1}$, such that one of the following conditions hold.
(i) $(r, s)=\left(p_{n}, q_{n}\right)$.
(ii) $(r, s)=\left(m p_{n}+p_{n-1}, m q_{n}+q_{n-1}\right)$.
(iii) $(r, s)=\left(p_{n}+2 p_{n-1}, q_{n}+2 q_{n-1}\right)$.
(iv) $(r, s)=\left(2 p_{n}-p_{n-1}, 2 q_{n}-q_{n-1}\right)$.

Moreover, if $(r, s)$ satisfies condition (iii), but not (i) or (ii), then

$$
\left|\alpha-\frac{r}{s}\right|>\frac{1}{s^{2}},
$$

and if $(r, s)$ satisfies condition (iv), but not (i), (ii), or (iii), then

$$
\left|\alpha-\frac{r}{s}\right|>\frac{3}{2 s^{2}}
$$

Remark. In the case that $s<\max \left(2, q_{1}\right)$, the theorem does not hold. On the other hand, it is not difficult to prove under these circumstances that either $s=1$ or $r / s=a_{0}+1 /\left(a_{1}-1\right)$. We do not pursue the details here.

Proof. By replacing $\alpha$ by $\alpha-a_{0}$, there is no loss in generality in assuming that $0<\alpha<1$. Given $r / s$, let $n \geq 1$ be defined by $q_{n} \leq s<q_{n+1}$. We will also assume that $r / s>\alpha$, since the alternative case can be treated in a similar manner. We use the fact that

$$
\begin{equation*}
r q_{n}-s p_{n}=s q_{n}\left(\frac{r}{s}-\alpha\right)+s q_{n}\left(\alpha-\frac{p_{n}}{q_{n}}\right) \tag{3.3}
\end{equation*}
$$

If $s=q_{n}$, then (3.1) and (3.2) show that

$$
q_{n}\left|r-p_{n}\right|=\left|r q_{n}-s p_{n}\right|<q_{n}^{2}\left|\alpha-\frac{r}{q_{n}}\right|+q_{n}^{2}\left|\alpha-\frac{p_{n}}{q_{n}}\right|<2+\frac{q_{n}}{q_{n+1}}<3
$$

Therefore, $q_{n}\left|r-p_{n}\right| \leq 2$, and since $q_{n} \geq 2$, it follows that either $r=p_{n}$ or $q_{n}=2$. In the latter case we see that $p_{n}=1$, and hence $\left|r-p_{n}\right|=1$, implying that either $r=0$ or $r=2$. These are not possible since the fractions $0 / 2$ or $2 / 2$ are not in reduced form, showing that $r=p_{n}$.
We shall henceforth assume that $q_{n}<s<q_{n+1}$. The quantity $((r / s)-\alpha)$ appearing in (3.3) is positive. We study the sign of $\left(\alpha-\left(p_{n} / q_{n}\right)\right)$. If this quantity is negative, then

$$
\frac{p_{n}}{q_{n}}>\alpha .
$$

Therefore,

$$
\frac{p_{n-1}}{q_{n-1}}<\alpha<\min \left\{\frac{p_{n}}{q_{n}}, \frac{r}{s}\right\}
$$

It follows that

$$
\begin{align*}
0<\left|r q_{n}-s p_{n}\right| & \leq \max \left\{s q_{n}\left(\frac{r}{s}-\alpha\right), s q_{n}\left(\frac{p_{n}}{q_{n}}-\alpha\right)\right\}  \tag{3.4}\\
& <\max \left\{\frac{2 q_{n}}{s}, \frac{s}{q_{n+1}}\right\}
\end{align*}
$$

Since $q_{n}<s<q_{n+1}$, we deduce various statements from (3.4). For example, since

$$
s q_{n}\left(\alpha-\frac{p_{n}}{q_{n}}\right)
$$

is negative, but of absolute value smaller than $s / q_{n+1}<1$, it follows that $r q_{n}-s p_{n}$ is nonnegative. Moreover, since $2 q_{n} / s<2$, we see that

$$
\begin{equation*}
r q_{n}-s p_{n}=1 \tag{3.5}
\end{equation*}
$$

Therefore $1<2 q_{n} / s$, which also implies that $s<2 q_{n}$. Since $\left(p_{n} / q_{n}\right)>$ $\alpha$, it follows that $\left(p_{n} / q_{n}\right)>\left(p_{n-1} / q_{n-1}\right)$, and hence

$$
\begin{equation*}
p_{n-1} q_{n}-q_{n-1} p_{n}=-1 \tag{3.6}
\end{equation*}
$$

It is well known that, if $a$ and $b$ are coprime and $x_{0}$ and $y_{0}$ is an integer solution of $a x-b y=1$, then all the solutions of $a x-b y=1$ are of the form $x=x_{0}+m b$ and $y=y_{0}+m a$ for some integer $m$. From this remark, together with (3.5) and (3.6), there is an integer $m$ for which $r=-p_{n-1}+m p_{n}$ and $s=-q_{n-1}+m q_{n}$. Since $q_{n}<s<2 q_{n}$, the only possibility is $m=2$. Thus, $(r, s)=\left(2 p_{n}-p_{n-1}, 2 q_{n}-q_{n-1}\right)$, which is condition (iv) of the theorem. We now show that the inequality

$$
\begin{equation*}
\left|\alpha-\frac{r}{s}\right|>\frac{3}{2 s^{2}} \tag{3.7}
\end{equation*}
$$

must hold for this case. Assume that (3.7) does not hold. Then inequality (3.4) holds with the better factor $3 / 2$ instead of the factor 2 , showing that $s<3 q_{n} / 2$. Thus, $2 q_{n}-q_{n-1}<3 q_{n} / 2$, and therefore $q_{n}<2 q_{n-1}$. If $n=1$, we then get $q_{1}<2 q_{0}=2$ implying $q_{1}=1$, and now the inequality $s<3 q_{1} / 2=3 / 2$ implies $s=1$, which is a contradiction. So, $n \geq 2$. Since $q_{n}=a_{n} q_{n-1}+q_{n-2}$, we deduce that $a_{n}=1$, and so $p_{n}=p_{n-1}+p_{n-2}$ and $q_{n}=q_{n-1}+q_{n-2}$. That is, $r=2 p_{n}-p_{n-1}=p_{n-1}+2 p_{n-2}$ and $s=2 q_{n}-q_{n-1}=q_{n-1}+2 q_{n-2}$, and $(r, s)$ satisfies condition (iii).

We will now assume that the quantity $\left(\alpha-\left(p_{n} / q_{n}\right)\right)$, appearing in (3.3), is positive. In this case, we have

$$
\min \left\{\frac{p_{n-1}}{q_{n-1}}, \frac{r}{s}\right\}>\alpha>\frac{p_{n}}{q_{n}}
$$

as well as

$$
\begin{equation*}
0<r q_{n}-s p_{n}<s q_{n}\left(\frac{r}{s}-\alpha\right)+\frac{s}{q_{n+1}} \tag{3.8}
\end{equation*}
$$

If

$$
\begin{equation*}
\left(\frac{r}{s}-\alpha\right)<\frac{1}{s^{2}}, \tag{3.9}
\end{equation*}
$$

then

$$
0<r q_{n}-s p_{n}<\frac{q_{n}}{s}+\frac{s}{q_{n+1}}<2 .
$$

Therefore,

$$
r q_{n}-s p_{n}=1
$$

Note that, in the case being considered,

$$
p_{n-1} q_{n}-p_{n} q_{n-1}=1,
$$

and so $r=p_{n-1}+m p_{n}$ and $s=q_{n-1}+m q_{n}$ for some integer $m$. Since $q_{n}<s<q_{n+1}=a_{n+1} q_{n}+q_{n-1}$, we see $1 \leq m<a_{n+1}$, and hence condition (ii) holds. Finally, let us assume that (3.9) does not hold. By (3.3), we have that

$$
\begin{equation*}
0<r q_{n}-s p_{n}<\frac{2 q_{n}}{s}+\frac{s}{q_{n+1}}<3 . \tag{3.10}
\end{equation*}
$$

The case $r p_{n}-s q_{n}=1$ being already treated, we may assume that $r p_{n}-s q_{n}=2$. Since $s / q_{n+1}<1$, (3.10) can hold only if $s<2 q_{n}$. Subtracting the equation $p_{n-1} q_{n}-p_{n} q_{n-1}=1$ from $r q_{n}-s p_{n}=$ 2 , we get $\left(r-p_{n-1}\right) q_{n}-\left(s-p_{n-1}\right) p_{n}=1$. Since we also have $p_{n-1} q_{n}-q_{n-1} p_{n}=1$, it follows that $r-p_{n-1}=p_{n-1}+m p_{n}$ and $s-q_{n-1}=q_{n-1}+m q_{n}$ for some integer $m$. Thus, $r=m p_{n}+2 p_{n-1}$ and $s=m q_{n}+2 q_{n-1}$ for some integer $m$. If $m<0$, then $s \leq 2 q_{n-1}-q_{n}<$ $q_{n}$, which is impossible, while if $m=0$, we get $r=2 p_{n-1}$ and $s=2 q_{n-1}$ which are not coprime. Thus, $m>0$ and since $s<2 q_{n}$, we see that $m<2$. Therefore, $m=1$ and so condition (iii) holds.
4. The equation $x^{2}-\left(k^{2}-4\right) y^{2}=4 t$. Armed with these new results on diophantine approximations, equations such as (1.2) can be solved. In particular, we prove the following more general result.

Theorem 4.1. Let $k>1$ be an odd integer. If $t$ is a positive integer for which $t<2 \sqrt{k^{2}-4}$ and the equation

$$
\begin{equation*}
x^{2}-y^{2}\left(k^{2}-4\right)=4 t \tag{4.1}
\end{equation*}
$$

has solutions in coprime positive integers $x, y$, then $t=1$ or $t=k+2$.

Proof. Let $\alpha=\left(1+\sqrt{k^{2}-4}\right) / 2$. As $x$ and $y$ are odd, (4.1) can be rewritten as

$$
\left(\frac{(x+y) / 2}{y}-\left(\frac{1+\sqrt{k^{2}-4}}{2}\right)\right)\left(\frac{(x+y) / 2}{y}-\left(\frac{1-\sqrt{k^{2}-4}}{2}\right)\right)=\frac{t}{y^{2}}
$$

If $((x+y) / 2) / y<\left(1+\sqrt{k^{2}-4}\right) / 2$, the product is negative, contradicting the fact that $t$ is positive. Therefore, we must have that $((x+y) / 2) / y>\left(1+\sqrt{k^{2}-4}\right) / 2$. From our assumption on $t$, we have that

$$
\begin{aligned}
\frac{(x+y) / 2}{y}-( & \left.\frac{1+\sqrt{k^{2}-4}}{2}\right) \\
& =\frac{t}{y^{2}\left(((x+y) / 2) /(y)-\left(\left(1-\sqrt{k^{2}-4}\right) / 2\right)\right)} \\
& <\frac{t}{y^{2} \sqrt{k^{2}-4}}<\frac{2}{y^{2}}
\end{aligned}
$$

The results of the previous section imply that $((x+y) / 2) / y$ is either a convergent, a mediating fraction to $\alpha$, or there are two convergents $p_{n-1} / q_{n-1}, p_{n-2} / q_{n-2}$ to $\alpha$ for which either

$$
\frac{(x+y) / 2}{y}=\frac{p_{n-1}+2 p_{n-2}}{q_{n-1}+2 q_{n-2}}
$$

or

$$
\frac{(x+y) / 2}{y}=\frac{2 p_{n-1}-p_{n-2}}{2 q_{n-1}-q_{n-2}}
$$

The partial quotients to $\alpha$ are given by

$$
\alpha=[(k-1) / 2 ; 1, k-2,1, k-2, \ldots,],
$$

and the first few convergents $p_{0} / q_{0}, p_{1} / q_{1}, \ldots$, are $((k-1) / 2) / 1,((k+$ $1) / 2) / 1,\left(\left(k^{2}-3\right) / 2\right) /(k-1), \ldots$. An inductive argument shows that $x$ and $y$, defined by $(x, y)=\left(2 p_{i}-q_{i}, q_{i}\right)$, satisfy

$$
x^{2}-y^{2}\left(k^{2}-4\right)=-4(k+2)
$$

for $i \geq 0$ and even, and

$$
x^{2}-y^{2}\left(k^{2}-4\right)=4
$$

for $i \geq 0$ and odd.
Consider first the case that $((x+y) / 2) / y$ is a mediating fraction. In the 0th step, the mediating fractions are simply $i / 1$ with $1 \leq i \leq$ $(k-1) / 2$. Putting $(x, y)=(2 i-1,1)$, we see that these mediating fractions lead to $x, y$ for which $x^{2}-y^{2}\left(k^{2}-4\right)$ is negative.

For $1 \leq i \leq(k-1) / 2$, put $\delta_{i}=\left((2 i-1)+\sqrt{k^{2}-4}\right) / 2$. Consider now the case that $(x, y)=(2 u-v, v)$ where $u / v$ is a mediating fraction in the $2 n$th iteration of the continued fraction (recall that $a_{2 n-1}=1$ for all $n \geq 1$, and so we need only consider the even-indexed iterations). Define

$$
\varepsilon=\frac{k+\sqrt{k^{2}-4}}{2}
$$

then it can be seen that for some $i=1, \ldots,(k-1) / 2$, and some integer $j$,

$$
\frac{x+y \sqrt{k^{2}-4}}{2}=\delta_{i} \varepsilon^{j}
$$

from which it follows that $x^{2}-y^{2}\left(k^{2}-4\right)$ is negative. Thus, mediating fractions lead only to values $x, y$ for which $x^{2}-y^{2}\left(k^{2}-4\right)$ is negative.

Now consider the case that there are consecutive convergents $p_{n-1} /$ $q_{n-1}, p_{n-2} / q_{n-2}$ to $\alpha$ for which

$$
\begin{equation*}
\frac{(x+y) / 2}{y}=\frac{p_{n-1}+2 p_{n-2}}{q_{n-1}+2 q_{n-2}} \tag{4.2}
\end{equation*}
$$

and $a_{n}=1$. It follows that $n$ must be odd. In the case $n=1$, we see that $((x+y) / 2) / y=((k+3) / 2) / 1$. Therefore, $y=1, x=k+2$ and $x^{2}-y^{2}\left(k^{2}-4\right)=4(k+2)$. Let $\gamma_{1}=\left((k+2)+\sqrt{k^{2}-4}\right) / 2$, and for $n>1$ and $n$ odd, let $\gamma_{n}=\left(x+y \sqrt{k^{2}-4}\right) / 2$, where $x$ and $y$ satisfy (4.2). Then, as in the previous case,

$$
\gamma_{n}=\gamma_{1} \varepsilon^{j}
$$

for some integer $j$, and so $x^{2}-y^{2}\left(k^{2}-4\right)=4(k+2)$.

In the case that there are consecutive convergents $p_{n-1} / q_{n-1}$, $p_{n-2} / q_{n-2}$ to $\alpha$ for which

$$
((x+y) / 2) / y=\left(2 p_{n-1}-p_{n-2}\right) /\left(2 q_{n-1}-q_{n-2}\right)
$$

a similar analysis shows that either $x^{2}-y^{2}\left(k^{2}-4\right)=4(k+2)$ or $x^{2}-y^{2}\left(k^{2}-4\right)=-6 k+13$. This completes the proof of the theorem. -

Note added in proof. Worley [8] has proved results very similar to Theorem 3.1. We thank Andrej Dujella for making us aware of Worley's work.

Acknowledgments. The authors gratefully acknowledge the comments of the anonymous referee. The third author is grateful to the Natural Sciences and Engineering Research Council of Canada for its support.

## REFERENCES

1. P. Fatou, Sur l'approximation des incommensurables et des séries trigonométriques, C.R. Acad. Sci. Paris 139 (1904), 1019-1021.
2. J.H. Grace, The classification of rational approximations, Proc. London Math. Soc. 17 (1918), 247-258.
3. H. Harborth, Positive integers $\left(a^{2}+b^{2}\right) /(a b+1)$ are squares, preprint, 2002.
4. A. Hurwitz, Über die angenäherte Darstellungen der Zahlen durch rationale Brüche, Math. Ann. 44 (1894), 417-436.
5. Y.A. Khinchin, Continued fractions, Univ. of Chicago Press, Chicago, 1964.
6. W.M. Schmidt, Diophantine approximation, Lecture Notes in Math. 785, Springer-Verlag, New York, 1980.
7. C.-O. Selenius, Kriterion für Zahlen quadratischer Zahlkörper mit Normbetrag kleiner als die Quadratwurzel aus der Diskriminante, Acta Acad. Abo. 26, 1966.
8. R.T. Worley, Estimating $|\alpha-p / q|$, J. Austral. Math. Soc. 31 (1981), 202-206.
[^1]
[^0]:    2000 AMS Mathematics Subject Classification. Primary 11J70, 11D09.
    Received by the editors on June 5, 2003, and in revised form on June 25, 2003.

[^1]:    Instituto de Matemáticas UNAM, Campus Morelia Ap. Postal 61-3
    (Xangari)CP 58 089, Morelia, Michoacán, Mexico
    E-mail address: fluca@matmor.unam.mx
    NSA Mathematical Sciences, National Security Agency, Suite 6557, Ft. George G. Meade, MD 20755-6557

    Department of Mathematics, University of Ottawa, 585 King Edward
    St., Ottawa, Ontario, Canada K1N-6N5
    E-mail address: gwalsh@mathstat.uottawa.ca

