JOURNAL OF NUMBER THEORY 16, 19–30 (1983)

The Minima of Indefinite Binary Quadratic Forms

PETER J. NICHOLLS

Department of Mathematics, Northern Illinois University, DeKalb, Illinois 60115

Communicated by P. T. Bateman

Received October 24, 1980; revised April 1, 1981

The study of the minima of indefinite binary quadratic forms has a long history and the classical results concerning the determination of such minima are stated in terms of the continued fraction expansion of the roots. These results are recast in geometric terms. Using this, and well-known geometric properties of the modular group, some necessary and sufficient conditions for a certain class of quadratic forms to have positive unattained minima are obtained.

1. Introduction

We consider a binary quadratic form

$$f(x, y) = ax^2 + bxy + cy^2, \tag{1.1}$$

where a, b, c are real and the discriminant $d = b^2 - 4ac$ is positive. We define

$$M(f) = \inf\{|f(x, y)|; x, y \text{ integers}, (x, y) \neq (0, 0)\}$$

and

$$m(f) = M(f)\, d^{-1/2}.$$

It is this term, $m(f)$, which we consider as the minimum of the form f.

We say that $f(x, y) = ax^2 + bxy + cy^2$ and $f_1(x_1, y_1) = a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2$ are *equivalent* if there is a transformation T

$$T:\quad \begin{aligned} x &= rx_1 + sy_1, \\ y &= tx_1 + uy_1, \end{aligned} \qquad ru - st = 1,$$

where r, s, t, u are integers such that T transforms $f(x, y)$ into $f_1(x_1, y_1)$.

The quadratic equation $f(x, 1) = 0$ has two distinct real roots α, β and we have

$$f(x, y) = a(x - \alpha y)(x - \beta y). \tag{1.2}$$

0022-314X/83/010019-12\$03.00/0

If either root is rational then $m(f)=0$ and so we assume from now on that neither root is rational. Following Dickson [1, p. 100] we say that f is an *Hermite reduced form* if

$$\alpha > 1 \qquad \text{and} \qquad -1 < \beta < 0. \tag{1.3}$$

The study of the minima of binary quadratic forms and its connection with Diophantine approximation has a long history and there is a large literature dating back to the last century. The classical theory, due originally to Lagrange, may be found in Dickson [1, 2]. We summarise what we need of the classical theory.

THEOREM A. (i) *Two equivalent binary quadratic forms have the same minimum.*

(ii) *Every binary quadratic form with irrational roots is equivalent to a reduced form.*

(iii) *Suppose f is of the form* (1.2) *and is reduced. We represent α and β by infinite continued fractions*

$$\alpha = [b_0, b_1, b_2, \ldots],$$
$$-\beta = [0, b_{-1}, b_{-2}, \ldots]$$

and form the sum

$$\mu_i = [b_i, b_{i+1}, \ldots] + [0, b_{i-1}, b_{i-2}, \ldots]$$

for every integer i, then $m(f) = \inf_i (1/\mu_i)$.

This theorem then, solves the problem of the determination of the minimum of a quadratic form—at least in principle. In practice, the algorithm given in part (iii) is difficult to use and the procedure described there seems somewhat difficult to motivate.

Our first aim is to recast this theorem in geometrical terms and to show in particular that the condition given in (iii) has a very elementary interpretation which completely avoids the technicalities of the continued fraction theory. We obtain, as a consequence, a new proof of Theorem A. Our second aim is to use this new formulation to obtain information about binary forms with a positive unattained minimum. Of course, in studying the possible values of $m(f)$, one may restrict attention to forms which attain their minimum—as the minimum of any form must be attained by some form [3, p. 389]. It is, however, of some interest to find forms which do not attain their minima and the first example, due to Schur, was reported in a paper by Remak [6]. Quite recently, examples of such forms were given by Setzer in the case where α, β are quadratic integers [7]. We will be able to give a fairly complete classification of those forms (1.2) which have a positive unattained minimum in the case where α, β are quadratic integers.

We denote by Γ the modular group

$$\Gamma = \left\{ V\colon V(z) = \frac{az+b}{cz+d};\ a, b, c, d \in Z,\ ad - bc = 1 \right\}$$

and state our first result.

THEOREM 1. (i) *If α, β are irrational reals then for some $V \in \Gamma$ we have either*

$$V(\alpha) > 1 \qquad \text{and} \qquad -1 < V(\beta) < 0$$

or

$$V(\beta) > 1 \qquad \text{and} \qquad -1 < V(\alpha) < 0.$$

(ii) *If f is the quadratic form* (1.2) *then*

$$m(f) = \frac{1}{\sup\{|V(\alpha) - V(\beta)|\colon V \in \Gamma\}}.$$

(iii) *There exists $S \in \Gamma$, $S = (az+b)(cz+d)^{-1}$, with $|S(\alpha) - S(\beta)| = \sup\{|V(\alpha) - V(\beta)|\colon V \in \Gamma\}$ if and only if $|f(d, -c)| = M(f)$.*

Thus to minimise a quadratic form one seeks to pull apart the roots as much as possible using elements in the modular group. In fact Theorem 1 contains all the information given in Theorem A. To see this recall that two forms,

$$f = a(x - \alpha y)(x - \beta y),$$
$$g = a_1(x_1 - \alpha_1 y_1)(x_1 - \beta_1 y_1)$$

are equivalent if and only if $|a_1/a| = |(\alpha - \beta)/(\alpha_1 - \beta_1)|$ and, for some $V \in \Gamma$, $V(\alpha) = \alpha_1$, $V(\beta) = \beta_1$ [1, p. 99]. In view of this remark the first two parts of Theorem A follow immediately from Theorem 1.

We now consider part (iii) of Theorem A. If i is positive we set $S_i/T_i = [b_0, b_1, \ldots, b_{i-1}]$ in lowest terms. Now Markoff has shown [4, p. 385] that $\mu_i = \sqrt{D}\,|f(S_i, T_i)|^{-1}$, where D is the discriminant of the form f. Since f is of the form (1.2) we observe that $D = [a(\alpha - \beta)]^2$ and so $\mu_i = |a|\,|\alpha - \beta|\,|f(S_i, T_i)|^{-1}$. Now we find integers a_i, b_i so that $a_i S_i + b_i T_i = 1$ and then $V(z) = (a_i z + b_i)(-T_i z + S_i)^{-1}$ is in Γ. A routine calculation shows that

$$|V_i(\alpha) - V_i(\beta)| = |\alpha - \beta|\,|(-T_k\alpha + S_k)(-T_k\beta + S_k)|^{-1}$$

and we have shown that $\mu_i = |V_i(\alpha) - V_i(\beta)|$. There is a similar result in the case where i is negative and we see that in order to maximise μ_i we should maximise $|V(\alpha) - V(\beta)|$ over the set of transforms V in Γ with the property that $V^{-1}(\infty)$ is a convergent in the continued fraction expansion of α or β. In view of the fact that these convergents are the best rational approximations to α and β it is not difficult to prove that we obtain the same result if we maximise $|V(\alpha) - V(\beta)|$ over all V in Γ.

Theorem 1 will be proved in Section 2. We will now state our results concerning binary quadratic forms with positive unattained minima.

An irrational number α is a *quadratic irrational* if it is a root of a quadratic equation with integer coefficients. We denote the other root by α^*. A quadratic irrational α is a *quadratic integer* if $\alpha\alpha^*$ and $\alpha + \alpha^*$ are integers. This is equivalent to requiring that α be an irrational root of a quadratic equation $x^2 + Bx + C = 0$ and B and C integers.

We will see in Section 2 that α is a quadratic irrational if and only if there exists a hyperbolic transform in Γ fixing α and α^*. This leads rather easily to our next result.

THEOREM 2. *Let α, β be quadratic irrationals with $\alpha \neq \beta$, $\alpha \neq \beta^*$. Then the number η is an accumulation point of the set $\{|V(\alpha) - V(\beta)|: V \in \Gamma\}$ if and only if $\eta = |T(\alpha) - T(\alpha^*)|$ or $\eta = |T(\beta) - T(\beta^*)|$ for some $T \in \Gamma$.*

We remark that this is precisely Theorem 1(a) of Setzer [7].

From now on we restrict our attention to quadratic integers α, β and we wish to determine whether the form (1.2) has an attained minimum. We may as well assume that $|\beta - \beta^*| \geqslant |\alpha - \alpha^*|$ and we have the following result.

THEOREM 3. *Suppose α, β are quadratic integers with $|\beta - \beta^*| \geqslant |\alpha - \alpha^*|$ and that α does not lie in the segment between β and β^*, then* $\sup\{|V(\alpha) - V(\beta)|: V \in \Gamma\}$ *is attained.*

Following Setzer we define, for our quadratic irrationals α, β the forms

$$\begin{aligned} A(x, y) &= (x - \alpha y)(x - \alpha^* y). \\ B(x, y) &= (x - \beta y)(x - \beta^* y). \end{aligned} \tag{1.4}$$

It turns out to be important whether or not the pair β, β^* are interchanged by an elliptic element of order two in Γ. This is equivalent to the equation $B(x, y) = -1$ having a solution in integers—a fact which we prove later.

THEOREM 4. *If α, β are quadratic integers with $|\beta - \beta^*| \geqslant |\alpha - \alpha^*|$ and if $B(x, y) = -1$ has a solution in integers, then* $\sup\{|V(\alpha) - V(\beta)|: V \in \Gamma\}$ *is attained.*

If one considers the possible arrangements of the four numbers α, α^*, β, β^* on the real line there are eight such arrangements with $|\beta-\beta^*| \geqslant |\alpha-\alpha^*|$ and which fail to satisfy the hypothesis of Theorem 3. In two of these the hypothesis of Theorem 4 is necessary and sufficient for the supremum to be attained.

THEOREM 5. *If α, β are quadratic integers and if $B(x, y) = -1$ has no solution in integers then in either of the two cases*

(i) $\beta < \alpha^* < \alpha < \beta^*$, *or*

(ii) $\beta^* < \alpha < \alpha^* < \beta$

$\sup\{|V(\alpha) - V(\beta)|: V \in \Gamma\} = |\beta - \beta^*|$ *and is not attained.*

In the remaining six cases we must impose an extra condition in order to ensure that the supremum is not attained.

THEOREM 6. *If α, β are quadratic integers with $|\beta-\beta^*| \geqslant 2|\alpha-\alpha^*|$ and if $B(x, y) = -1$ has no solution in integers then in any of the following four cases* $\sup\{|V(\alpha) - V(\beta)|: V \in \Gamma\} = |\beta - \beta^*|$ *and is not attained*:

(iii) $\beta < \alpha < \beta^* < \alpha$,

(iv) $\alpha^* < \beta < \alpha < \beta^*$,

(v) $\alpha^* < \beta^* < \alpha < \beta$,

(vi) $\beta^* < \alpha < \beta < \alpha^*$.

THEOREM 7. *If α, β are quadratic integers with $|\beta-\beta^*| \geqslant 2|\alpha-\alpha^*| + 2 \cdot 5^{-1/2}$ and if $B(x, y) = -1$ has no solution in integers then in either of the following two cases* $\sup\{|V(\alpha) - V(\beta)|: V \in \Gamma\} = |\beta - \beta^*|$ *and is not attained*:

(vii) $\beta < \alpha < \alpha^* < \beta^*$,

(viii) $\beta^* < \alpha^* < \alpha < \beta$.

In view of Theorem 1 we can say that if the hypotheses of Theorems 5, 6 or 7 are satisfied then $m(f) = |\beta - \beta^*|^{-1}$ and is not attained. We remark that Setzer's conditions for unattained unfinium are slightly stronger than those required in Theorem 7. If the hypotheses of Theorem 3 or 4 are satisfied then $m(f)$ is attained.

2. Proofs of Theorems 1 and 2

Let α, β be real irrationals. If $V \in \Gamma$, $V(z) = (az+b)(cz+d)^{-1}$ then

$$V(\alpha) - V(\beta) = \frac{\alpha - \beta}{(c\alpha + d)(c\beta + d)}. \tag{2.1}$$

There exist infinitely many co-prime pairs c, d with

$$|\alpha + d/c| \leqslant \frac{1}{\sqrt{5}\,|c|^2} \qquad \text{(Hurwitz' theorem).}$$

For each such pair we may find a transform $V(z) = (az+b)(cz+d)^{-1}$ in Γ and, from (2.1),

$$\begin{aligned} |V(\alpha) - V(\beta)| &= \frac{|\alpha - \beta|}{|c\alpha + d|\,|c\beta + d|} \\ &\geqslant \frac{|\alpha - \beta|\,\sqrt{5}}{|\beta + d/c|} \\ &\geqslant \frac{|\alpha - \beta|\,\sqrt{5}}{|\alpha - \beta| + |\alpha + d/c|}, \end{aligned}$$

which clearly exceeds 2 for some V. So assuming that $|V(\alpha) - V(\beta)| > 2$ we translate the smaller of $V(\alpha)$, $V(\beta)$ into $(-1, 0)$ by a power of the element $P(z) = z + 1$ (in Γ). This proves part (i) of Theorem 1.

We see immediately from (2.1) that

$$|V(\alpha) - V(\beta)| = |f(d, -c)|^{-1}\sqrt{D}, \tag{2.2}$$

where D is the discriminant of f. As before, given d, c, relatively prime we can construct an element V of Γ satisfying (2.2) and the remaining two parts of Theorem 1 follow immediately.

To prove Theorem 2 we start by showing that any quadratic irrational is fixed by some hyperbolic element in Γ. Suppose α is a root of $Ax^2 + Bx + C = 0$, with A, B, C integers and $D = B^2 - 4AC$ positive and non-square. We solve the Pellian equation $t^2 - Du^2 = 4$ in integers t, u $(u \neq 0)$ and set

$$H(z) = \{1/2(t - Bu)\,z - Cu\} \cdot \{Auz + 1/2(t + Bu)\}^{-1},$$

which clearly is a hyperbolic element in Γ and fixes α.

Given the hypotheses of Theorem 2 we let H_1, H_2 be hyperbolic elements in Γ fixing α, α^* and β, β^*, respectively. Choose $T \in \Gamma$ and suppose that $\eta = |T(\alpha) - T(\alpha^*)|$. If α^* is the attractive fix point of H_1 then we see that

$TH_1^n(\alpha) = T(\alpha)$ and $TH_1^n(\beta) \to T(\alpha^*)$ as $n \to +\infty$. Thus η is an accumulation point of $\{|V(\alpha) - V(\beta)|: V \in \Gamma\}$.

Suppose now that η is an accumulation point of $\{|V(\alpha) - V(\beta)|: V \in \Gamma\}$. Since the translation z: $z \to z+1$ belongs to Γ we can find a sequence $\{V_n\} \subset \Gamma$ and two real numbers λ, μ with $|\lambda - \mu| = \eta$ and $V_n(\alpha) \to \lambda$, $V_n(\beta) \to \mu$ as $n \to \infty$. Select ω on the geodesic joining α to β and observe that, on a subsequence if necessary, $\{V_n(\omega)\}$ converges to either λ or μ. Suppose $V_n(\omega) \to \mu$, then we have a geodesic ray joining ω to α whose images approximate the geodesic joining λ to μ. Since α is a hyperbolic fix point it is well known (see [5], for example) that under these circumstances the geodesic joining λ to μ is an image of the axis of H_1. Thus for some $T \in \Gamma$, $\eta = |\lambda - \mu| = |T(\alpha) - T(\alpha^*)|$ and the proof of Theorem 2 is complete.

3. Proofs of Theorems 3 and 4

We start with a lemma.

LEMMA. *Let α be a quadratic integer then*

(a) $|V(\alpha) - V(\alpha^*)| \leqslant |\alpha - \alpha^*|$ *for all* $V \in \Gamma$.

(b) *If* $|V(\alpha) - V(\alpha^*)| \neq |\alpha - \alpha^*|$ *then* $|V(\alpha) - V(\alpha^*)| \leqslant \frac{1}{2}|\alpha - \alpha^*|$.

(c) *If* $V(\alpha) - V(\alpha^*) = \alpha - \alpha^*$ *then for some integers* m, n, $V = P^n H^m$, *where* H *is the hyperbolic transform fixing* α, α^* *and* P *is the translation* $P(z) = z + 1$.

(d) *If* $V(\alpha) - V(\alpha^*) = \alpha^* - \alpha$ *then for some integer* n, $V = P^n E$, *where* E *is an elliptic element of order two interchanging* α *and* α^*.

Proof. From (1.4) and (2.2) we observe that

$$|V(\alpha) - V(\alpha^*)| = |\alpha - \alpha^*| \cdot |A(d, -c)|^{-1},$$

where A is the quadratic form

$$A(x, y) = (x - \alpha y)(x - \alpha^* y)$$

and $V(z) = (az + b)(cz + d)^{-1} \in \Gamma$. Since α is a quadratic integer $A(x, y)$ has integer coefficients, note also that $c^2 + d^2 > 0$ and therefore $|A(d, -c)| \geqslant 1$. This proves part (a). If $|A(d, -c)| \neq 1$ then $|A(d, -c)| \geqslant 2$ and this proves part (b). Now suppose $V(\alpha) - V(\alpha^*) = \alpha - \alpha^*$. From (1.4) and (2.1) we see that $A(d, -c) = 1$. An easy calculation yields

$$V(\alpha) - \alpha = bc(\alpha + \alpha^*) + ac\alpha\alpha^* + bd,$$

which is an integer, say n. Therefore $V(\alpha) = P^n(\alpha)$ and $P^{-n}V$ fixes α. Thus

$P^{-n}V$ is a power of H and part (c) is proved. Suppose finally that $V(\alpha)-V(\alpha^*)=\alpha^*-\alpha$ then we see from (1.4) and (2.1) that $A(d,-c)=-1$. An easy calculation yields

$$V(\alpha)-\alpha^*=-(ac\alpha\alpha^*+ad(\alpha+\alpha^*)+bd),$$

which is an integer, say n. Therefore $V(\alpha)=P^n(\alpha^*)$ and $P^{-n}V(\alpha)=\alpha^*$. Similarly, $P^{-n}V(\alpha^*)=\alpha$. Thus $(P^{-n}V)^2$ fixes α, α^*, since $P^{-n}V$ is clearly not a power of H we must have $(P^{-n}V)^2=I$ and the proof of the lemma is complete.

We now prove Theorem 3. In view of Theorem 2 and the lemma we have only to find $V\in\Gamma$ with $|V(\alpha)-V(\beta)|\geqslant|\beta-\beta^*|$ and the theorem is proved. Let H be the primitive hyperbolic element fixing β, β^* and with β^* as the attractive fixed point. Since all elements of Γ are orientation preserving we see that for all positive integers n, $H^n(\alpha)$ lies outside the segment joining β to β^* and so, for n large enough,

$$\begin{aligned}|H^n(\beta)-H^n(\alpha)|&=|\beta-H^n(\alpha)|\\&>|\beta-\beta^*|,\end{aligned}$$

which completes the proof of Theorem 3.

To prove Theorem 4 we assume $B(x,y)=-1$ has a solution in integers. By (2.1) and part (d) of the lemma we note that there is an elliptic element of order two, $E\in\Gamma$ with $E(\beta)=\beta^*$. We assume that α lies in the segment joining β to β^*, otherwise we can appeal to Theorem 3. Now observe that $E(\alpha)$ lies outside the segment joining β to β^*. With H defined as above we see as before that for large enough positive n

$$\begin{aligned}|H^{-n}E(\beta)-H^{-n}E(\alpha)|&=|\beta^*-H^{-n}E(\alpha)|\\&>|\beta-\beta^*|,\end{aligned}$$

which completes the proof of Theorem 4.

4. Proofs of Theorems 5, 6 and 7

Suppose V, given by $V(z)=(az+b)(cz+d)^{-1}\in\Gamma$ then the isometric circle, $I(V)$, is given by

$$I(V)=\{z\colon |cz+d|=1\}\qquad\text{provided}\quad c\neq 0.$$

We recall that the action of V is an inversion in $I(V)$ followed by a reflection in the perpendicular bisector of the line joining the centers of $I(V)$ and

$I(V^{-1})$. We note that the radius of $I(V)$ is $|c|^{-1}$ and this is at most one. We note further that if γ is a quadratic integer then

$$|\gamma - \gamma^*| \geqslant \sqrt{5}. \tag{4.1}$$

We now prove Theorem 5 and we will consider only case (i)—case (ii) has a similar proof. Suppose the result is false. Then, from Theorem 2, we see that for some $V \in \Gamma$

$$|V(\alpha) - V(\beta)| \geqslant |\beta - \beta^*| > |\alpha - \beta|. \tag{4.2}$$

Using (2.1) we see that $|c\alpha + d| \cdot |c\beta + d| < 1$ if $V(z) = (az + b)(cz + d)^{-1}$ and so either α or β is interior to $I(V)$.

Case 1. Suppose $V(\beta) < V(\alpha)$, since V is orientation preserving we must have either

$$V(\beta^*) < V(\beta) < V(\alpha^*) < V(\alpha) \tag{4.3}$$

or

$$V(\beta) < V(\alpha^*) < V(\alpha) < V(\beta^*). \tag{4.4}$$

However, (4.4) implies that $|V(\beta) - V(\beta^*)| > |V(\alpha) - V(\beta)|$ which, together with (4.2), contradicts the lemma. So we must have (4.3). Now if α is interior to $I(V)$ we see from (4.1) that α^*, β are exterior to $I(V)$ and, from our remarks on the action of V, we deduce that $|V(\alpha^*) - V(\beta)| < |\alpha^* - \beta|$. Thus

$$\begin{aligned} |V(\alpha) - V(\beta)| &\leqslant |V(\alpha) - V(\alpha^*)| + |V(\beta) - V(\alpha^*)| \\ &< |\alpha - \alpha^*| + |\beta - \alpha^*| \\ &= |\alpha - \beta|, \end{aligned}$$

which contradicts (4.2).

On the other hand, if β is interior to $I(V)$ then α, β^* are exterior to $I(V)$ and we see that

$$\begin{aligned} |V(\alpha) - V(\beta)| &< |V(\alpha) - V(\beta^*)| \qquad \text{from (4.3)} \\ &< 2, \end{aligned}$$

and this, with (4.1), contradicts (4.2).

Case 2. Suppose $V(\alpha) < V(\beta)$, since V is orientation preserving we must have either

$$V(\alpha^*) < V(\alpha) < V(\beta^*) < V(\beta) \tag{4.5}$$

or

$$V(\alpha) < V(\beta^*) < V(\beta) < V(\alpha^*). \tag{4.6}$$

However, (4.6) implies that $|V(\alpha) - V(\alpha^*)| > |V(\alpha) - V(\beta)|$, which, with (4.2), contradicts the lemma. So we must have (4.5). Now if α is interior to $I(V)$ then α^*, β are exterior to $I(V)$ and we see that

$$\begin{aligned} |V(\alpha) - V(\beta)| &< |V(\alpha^*) - V(\beta)| \qquad \text{from (4.5)} \\ &< 2, \end{aligned}$$

and this, with (4.1), contradicts (4.2).

On the other hand, if β is interior to $I(V)$ then α, β^* are exterior to $I(V)$ and, from our remarks on the action of V, we observe that

$$\begin{aligned} |V(\alpha) - V(\beta)| &= |V(\alpha) - V(\beta^*)| + |V(\beta^*) - V(\beta)| \\ &< 1 + |V(\beta^*) - V(\beta)|. \end{aligned} \tag{4.7}$$

Now since $B(x, y) = -1$ has no solution in integers we see from the lemma and (4.5) above that $|V(\beta^*) - V(\beta)| \leqslant |\beta - \beta^*|/2$. Thus from (4.2) and (4.7) we see that

$$|\beta - \beta^*| < 1 + \frac{|\beta - \beta^*|}{2},$$

which contradicts (4.1). We have shown that (4.2) cannot be true for any $V \in \Gamma$ and this completes the proof of Theorem 5.

To prove Theorem 6 we consider only case (iii) as the others are similar. We suppose that $B(x, y) = -1$ has no solution in integers, that $|\beta - \beta^*| \geqslant 2|\alpha - \alpha^*|$ and that for some $V \in \Gamma$

$$|V(\alpha) - V(\beta)| \geqslant |\beta - \beta^*| > |\alpha - \beta| \tag{4.8}$$

and we derive a contradiction. Assuming (4.8) we note that $V(\alpha) < V(\beta)$, otherwise either $|V(\beta) - V(\beta^*)| > |V(\alpha) - V(\beta)|$ or $|V(\alpha) - V(\alpha^*)| > |V(\alpha) - V(\beta)|$ both of which, in view of (4.8), contradict the lemma. Thus we have

$$V(\alpha) < V(\beta^*) < V(\alpha^*) < V(\beta) \tag{4.9}$$

and so

$$\begin{aligned} |V(\alpha) - V(\beta)| &< |V(\alpha) - V(\alpha^*)| + |V(\beta) - V(\beta^*)| \\ &\leqslant |\alpha - \alpha^*| + \frac{|\beta - \beta^*|}{2} \end{aligned}$$

in view of the lemma and the fact that $B(x, y) = -1$ has no solution in integers. This inequality and (4.8) imply that $|\beta - \beta^*| < 2|\alpha - \alpha^*|$ and the proof of Theorem 6 is complete.

We now prove Theorem 7 and consider only case (vii). Suppose then that $B(x, y) = -1$ has no solution in integers and, for some $V \in \Gamma$,

$$|V(\alpha) - V(\beta)| \geqslant |\beta - \beta^*| > |\alpha - \beta|. \tag{4.10}$$

If $V(\beta) < V(\alpha)$ then we must have

$$V(\beta^*) < V(\beta) < V(\alpha) < V(\alpha^*) \tag{4.11}$$

otherwise either $|V(\beta) - V(\beta^*)| > |V(\alpha) - V(\beta)|$ or $|V(\alpha) - V(\alpha^*)| > |V(\alpha) - V(\beta)|$ both of which, in view of (4.11), contradict the lemma. Either α or β is interior to $I(V)$ and it follows that α^*, β^* are both exterior to $I(V)$. Considering the action of V we see that $|V(\alpha^*) - V(\beta^*)| < 1$ and from (4.10), (4.11) and (4.1) we derive a contradiction. Thus we must have

$$V(\alpha) < V(\alpha^*) < V(\beta^*) < V(\beta). \tag{4.12}$$

If V composed with a translation does not fix α, α^* then from the lemma we see that $|V(\alpha) - V(\alpha^*)| \leqslant 1/2\,|\alpha - \alpha^*|$ and $|V(\beta^*) - V(\beta)| \leqslant 1/2\,|\beta - \beta^*|$. Since α^*, β^* are both exterior to $I(V)$ we see that $|V(\alpha^*) - V(\beta^*)| < 1$ and from (4.12)

$$|V(\alpha) - V(\beta)| < 1 + 1/2\,|\alpha - \alpha^*| + 1/2\,|\beta - \beta^*|.$$

Using (4.10) we find

$$|\beta - \beta^*| < |\alpha - \alpha^*| + 2. \tag{4.13}$$

Now suppose V fixes α, α^*. Since either α or β is interior to $I(V)$ we see that the center of $I(V)$ is to the left of α. Inverting in $I(V)$ the image of α^* is α and the image of β^* is to the right of the center of $I(V)$. Thus $|V(\alpha^*) - V(\beta^*)|$ does not exceed the distance from the center of $I(V)$ to α.

Call this latter distance x and we have $x(|\alpha - \alpha^*| + x) = |c|^{-2}$, where $V(z) = (az + b)(cz + d)^{-1}$. Thus

$$x < \frac{1}{|\alpha - \alpha^*| \cdot |c|^2} \leqslant \frac{1}{\sqrt{5}}$$

and we have proved that $|V(\alpha^*) - V(\beta^*)| < 5^{-1/2}$. From (4.12) we see that

$$\begin{aligned} |V(\alpha) - V(\beta)| &= |V(\alpha) - V(\alpha^*)| + |V(\alpha^*) - V(\beta^*)| + |V(\beta) - V(\beta^*)| \\ &< |\alpha - \alpha^*| + 5^{-1/2} + \tfrac{1}{2}\,|\beta - \beta^*|. \end{aligned}$$

From (4.10) we find

$$|\beta-\beta^*|<2\,|\alpha-\alpha^*|+2\cdot 5^{-1/2}. \tag{4.14}$$

This completes the proof of Theorem 7.

References

1. L. E. Dickson, "Introduction to the Theory of Numbers," Chicago Univ. Press, Chicago, 1929.
2. L. E. Dickson, "Studies in the Theory of Numbers," Chicago Univ. Press, Chicago, 1930.
3. M. Hall, Jr., The Markoff spectrum, *Acta Arith.* **18** (1971), 387–399.
4. A. Markoff, Sur les Formes binaires indéfinies, *Math. Ann.* **15** (1879), 381–406.
5. P. J. Nicholls, Special limit points for Fuchsian groups and automorphic functions near the limit set, *Indiana Univ. Math. J.* **24** (1974), 143–148.
6. R. Remak, Über die geometrisch Darstellung der in definiten binaren quadratischen Minimalformen, *Jber. Deutsch. Math. Verein.* **33** (1925), 228–245.
7. B. Setzer, The Structure of minima for binary quadratic forms, *Illinois J. Math.* **23** (1979), 352–362.