J. Austral. Math. Soc. (*Series A*) **61** (1996), 360–368

QUADRATIC DIOPHANTINE EQUATIONS AND TWO GENERATOR MÖBIUS GROUPS

ENG-CHYE TAN and SER-PEOW TAN

(Received 22 March 1995; revised 5 November 1995)

Communicated by R. Howlett

Abstract

In this paper, we study the set of rational μ in $(-2, 2)$ for which the group G_μ generated by

$$A = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$

is not free by using quadratic Diophantine equations of the form $ax^2 - by^2 = \pm 1$. We give a new set of accumulation points for rational values of μ in $(-2, 2)$ for which G_μ is not free, thereby extending the results of Beardon where he showed that $1/\sqrt{N}$ are accumulation points, where N is an integer which is not a perfect square. In particular, we exhibit an infinite set of accumulation points for μ between 1 and 2 including the point 1.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 11C, secondary 11D, 30F.

1. Introduction

Let $\mu \in \mathbb{R}$ and G_μ be the subgroup of $SL(2, \mathbb{R})$ generated by

$$A = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}.$$

In this paper, we study the problem of characterizing the set of μ for which G_μ is not free. We use the fact that $SL(2, \mathbb{R})$ acts on the upper half-plane as Möbius maps where A and $-A$ have the same action if $A \in SL(2, \mathbb{R})$; we do not distinguish between matrices and their action as Möbius maps.

Using the theory of discrete groups, it is easy to see that G_μ is free and discrete when $|\mu| \geq 2$; see for example [1]. Furthermore, it is known that G_μ is free whenever

μ is transcendental; see [3] or [5]. This leaves the countable set of algebraic values of μ in $(-2, 2)$ to consider. Without loss of generality, we may assume that μ is positive, and henceforth we shall always do so; so we consider the algebraic values of μ in $(0, 2)$.

Geometrically, one can show that for any $\mu \in (0, 2)$, $A^{-1}B$ is an elliptic transformation in $PSL(2, \mathbb{R})$ with rotation angle θ where

$$2 - \mu^2 = 2\cos\theta.$$

If $\mu = 2\sin \pi p/q$, then $\theta = 2\pi p/q$, so $(A^{-1}B)^q = I$. The set of such values for μ is dense in $(0, 2)$. Of these values, the only value of μ which is rational is 1. Thus, G_μ is not free for a dense set of irrational algebraic values in $(0, 2)$.

This leaves the case of the set of rational μ in $(0, 2)$ to consider. This seems to be a much harder problem: it is not known, for example, if there is a dense set of rational μ in $(0, 2)$ for which G_μ is not free, or even whether G_μ is not free for every rational μ in $(0, 2)$. The best results in this respect have been obtained by Lyndon and Ullman [5], and recently by Beardon [2] which we summarize below:

THEOREM 1 (Lyndon and Ullman [5]). *The group G_μ is not free for the following values of μ:*

$$\mu \in \{3/2, 4/3, 5/3, 5/4\} \tag{1.1}$$

or

$$\mu = \frac{p}{p^2 + 1}, \qquad p = 1, 2, \ldots \tag{1.2}$$

or

$$\mu = \frac{1}{p}, \qquad p = 2, 3, \ldots \tag{1.3}$$

THEOREM 2 (Beardon [2]). *Suppose that for some N, the integers p and q satisfy Pell's equation*

$$q^2 - Np^2 = 1. \tag{1.4}$$

Then G_μ is not free for $\mu = p/q$.

REMARK. In fact, Theorem 2 also holds if p, q satisfy the negative Pell's equation and more generally, if p, q satisfy

$$q^2 - Np^2 = m, \qquad m|N. \tag{1.5}$$

https://doi.org/10.1017/S1446788700000434 Published online by Cambridge University Press

COROLLARY 1 (Beardon [2]). *For each positive integer N that is not a square, there is a sequence of distinct rational values μ_n converging to $1/\sqrt{N}$ for which G_{μ_n} is not free.*

Moreover, Lyndon and Ullman observed that if G_μ is not free, then $G_{\mu/n}$ is also not free for $n = 2, 3, \ldots$; this gives the set of values in (1.3) of Theorem 1. Finally, Beardon [2] also showed that G_μ is not free for $\mu \in \{3/5, 4/5, 5/6, 3/7, 4/9, 5/9, 5/7\}$ by doing a computer search for words of the form $A^r B^s A^t B^u A^v$ which are lower triangular.

Some of the questions which arise from the above results are: firstly, are there other accumulation points for rational values of μ for which G_μ is not free? In particular, is 1 an accumulation point? (The accumulation points which have been obtained so far are all $\leq 1/\sqrt{2}$.) Secondly, Lyndon and Ullman only produced four values of μ in (1.2) for which G_μ is not free (Theorem 1 above) and, in general, the methods of Beardon used for Theorem 2 work only for $\mu \in (0, 1)$. Are there infinitely many rational values of μ in (1.2) for which G_μ is not free, or even infinitely many accumulation points in (1.2) for rational values of μ for which G_μ is not free?

In this paper, we answer the above questions affirmatively by showing a much larger set of accumulation points for rational μ for which G_μ is not free, including an infinite set of accumulation points in (1.2), converging to 1. More specifically, we prove the following:

THEOREM 3. *Let a, k, N be positive integers and $\epsilon_1, \epsilon_2 = \pm 1$. Suppose that $ka + \epsilon_1 \neq 0$ and p, q are non-zero integers satisfying the following quadratic Diophantine equation:*

$$aq^2 - (ka + \epsilon_1)Np^2 = \epsilon_2. \tag{1.6}$$

Then G_μ is not free for $\mu = p/q$.

COROLLARY 2. *Let a, k, N be positive integers and $\epsilon_1, \epsilon_2 = \pm 1$ such that $ka + \epsilon_1 \neq 0$. If the quadratic Diophantine equation*

$$ax^2 - (ka + \epsilon_1)Ny^2 = \epsilon_2 \tag{1.7}$$

admits an integer solution in x and y, then there exists an infinite sequence of distinct rationals μ_n converging to $\sqrt{a/(ka + \epsilon_1)N}$ such that G_{μ_n} is not free.

REMARK. For a given set of values for $a, k, N, \epsilon_1, \epsilon_2$, there is a finite algorithm for determining if the quadratic Diophantine equation (1.7) admits an integer solution; see [4] for example.

The most interesting case where equation (1.7) of Corollary 2 admits integer solutions is when $k = 1$, $N = 1$ giving us the following:

COROLLARY 3. *For each positive integer a and $\epsilon = \pm 1$, $(a + \epsilon \neq 0)$, there is a sequence of distinct rational values μ_n converging to $\sqrt{a/(a+\epsilon)}$ for which G_{μ_n} is not free.*

In particular, we have the accumulation points $\sqrt{1/2}, \sqrt{2/3}, \sqrt{3/4}, \ldots$ when $\epsilon = 1$ and $\sqrt{2}, \sqrt{3/2}, \sqrt{4/3}, \ldots$ when $\epsilon = -1$, the latter set giving infinitely many accumulation points in (1.2). Since these accumulation points themselves accumulate at 1, and following the observation of Lyndon and Ullman, we have the following:

COROLLARY 4. *For each positive integer p there is a sequence of distinct rational values μ_n converging to $1/p$ for which G_{μ_n} is not free.*

REMARK. Note that the accumulation points obtained in Corollary 4 are not covered in Corollary 1.

Putting $a = 2$, $k = 1$ and $\epsilon_1 = -1$ in Theorem 3 and Corollary 2, we have:

COROLLARY 5. *Let N be a positive integer and $\epsilon = \pm 1$. Suppose that p, q are integers satisfying the following quadratic Diophantine equation:*

$$2q^2 - Np^2 = \epsilon. \tag{1.8}$$

Then G_μ is not free for $\mu = p/q$. Furthermore, if p, q exists, then there exists an infinite sequence of distinct rationals μ_n converging to $\sqrt{2/N}$ such that G_{μ_n} is not free.

As remarked earlier, for each given value of N, there is a finite algorithm for determining if equation (1.8) in Corollary 5 admits integer solutions. However, no necessary and sufficient conditions seem to be known for determining the set of values of N for which equation (1.8) admits integer solutions. It is easy to see that a necessary condition for N is that

$$N \equiv 1, 3, \text{ or } 7 \mod 8$$

but this is not sufficient. A computer search gives the following list for the values of N below 100:

$$N \in \{1, 3, 7, 9, 11, 17, 19, 23, 27, 31, 33, 43, 47, 49, 51, 57, 59, 67, 71, 73, 79, 81, 83, 89, 97, 99\}.$$

Similarly, putting $a = 3$, $N = 1$ and letting $M = ka + \epsilon_1$ in Corollary 2, we have:

https://doi.org/10.1017/S1446788700000434 Published online by Cambridge University Press

COROLLARY 6. *Let M be an integer, $M > 1$ and $\epsilon = \pm 1$. Suppose that p, q are integers satisfying the following quadratic Diophantine equation:*

$$3q^2 - Mp^2 = \epsilon. \tag{1.9}$$

Then G_μ is not free for $\mu = p/q$. Furthermore, if p, q exists, then there exists an infinite sequence of distinct rationals μ_n converging to $\sqrt{3/M}$ such that G_{μ_n} is not free.

REMARK. Note that the above theorem does not apply to the case where $M = 1$. In fact, in this case, $p = 2$ and $q = 1$ satisfy equation (1.9) but G_2 is free and discrete. We have not been able to determine if $\sqrt{3}$ is in fact an accumulation point. However, for the next convergent of $\sqrt{3}$, $\mu = 7/4$, $p = 7$, $q = 4$ satisfy equation (1.9) and we have been able to show that G_μ is not free. (Lyndon and Ullman in [5] were unable to determine this using their difference equation.) The details are given in Section 4.

Finally, in the case where $a = 4$, $N = 1$ and letting $M = ka + \epsilon_1$ in Corollary 2, we have the following:

COROLLARY 7. *Let M be an integer, $M > 1$, $\epsilon = \pm 1$. Suppose that p, q are integers satisfying the following quadratic Diophantine equation:*

$$4q^2 - Mp^2 = \epsilon. \tag{1.10}$$

Then G_μ is not free for $\mu = p/q$. Furthermore, if p, q exist, then there exists an infinite sequence of distinct rationals μ_n converging to $2/\sqrt{M}$ such that G_{μ_n} is not free.

REMARK. If equation (1.10) admits integer solutions in p and q, then M must be odd and not a square and since $M > 1$, $k \geq 1$.

The rest of this paper is organized as follows. In Section 2, we give preliminary definitions and results and deal with the Pell's equation case. In Section 3, we give the proofs for Theorem 3 and Corollary 2 and finally in Section 4, we deal with the $\mu = 7/4$ case and give some concluding remarks on possible directions for further study.

2. Preliminaries and the Pell's equation case

We shall use a slightly different normalization of the group G_μ from that used by Beardon in [2]. We conjugate A and B by

$$S = \begin{pmatrix} \mu^{-1/2} & 0 \\ 0 & \mu^{1/2} \end{pmatrix}$$

https://doi.org/10.1017/S1446788700000434 Published online by Cambridge University Press

and work with the group generated by SAS^{-1} and SBS^{-1} instead. For convenience we shall also call these new generators A and B, and the group generated by them G_μ. Clearly, the original group is not free if and only if the normalized group is not free so that the problem is equivalent. We shall also only consider rational μ in the interval $(0, 2)$, where $\mu = p/q$, p, q relatively prime.

We therefore have, as our basic set-up,

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ \mu^2 & 1 \end{pmatrix}, \qquad G_\mu = \langle A, B \rangle \tag{2.1}$$

where $0 < \mu = p/q < 2$.

We use the observation of Lyndon and Ullman [5] that G_μ is not free if there exist non-zero integers $a_1, b_1, \ldots, a_n$ such that

$$W_n = A^{a_n} \cdots B^{b_1} A^{a_1} = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}. \tag{2.2}$$

This follows from the fact that $W_n^{-1} B W_n$ commutes with B ($W_n^{-1} B W_n$ and B are parabolic elements with the same fixed points) thus giving a relation in A and B. This is also the basis of the results in [2].

Using the usual action of $PSL(2, \mathbb{R})$ on the extended upper half-plane (that is, the upper half-plane with its boundary), we observe that $W_n = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$ if and only if W_n fixes zero. We are therefore trying to find a sequence of powers of A and B that eventually moves zero back to itself. We therefore need to know the action of powers of A and B on rationals. An easy computation gives

$$A^n(a/b) = n + a/b, \qquad B^n(a/b) = aq^2/(bq^2 + anp^2). \tag{2.3}$$

We are now ready to deal with the Pell's equation case and the results of [2].

Suppose that s, t are non-zero integers. From (2.3), we have

$$B^s A^t(0) = tq^2/(q^2 + stp^2). \tag{2.4}$$

It follows that there exists an integer r such that $A^r B^s A^t(0) = 0$ if and only if $q^2 + stp^2$ divides tq^2. This is in fact a slightly different but equivalent formulation of Theorem 2 in [2]. Lyndon and Ullman's result (Theorem 1, (1.2) above) and Beardon's result (Theorem 2 above) now follow, choosing $t = -1$, $s = p^2 + 2$ in the former and $t = -1$, $s = N$ in the latter. From equation (2.4), one sees easily that the more general version of Theorem 2 also holds by using $t = N$, $s = -1$. This gives more cases of μ for which G_μ is not free, for example, $q = 2$, $p = 1$ satisfy

$$q^2 - 6p^2 = -2 \tag{2.5}$$

https://doi.org/10.1017/S1446788700000434 Published online by Cambridge University Press

from which it follows (see [4]) that there are infinitely many p's and q's which satisfy equation (2.5) and G_μ is not free for $\mu = p/q$. These values are distinct from the solutions of the equation

$$q^2 - 6p^2 = 1.$$

However, the values also accumulate at $1/\sqrt{6}$ and from the nature of equation (2.4) we see that considering words of the form $A^r B^s A^t$ will not produce any more accumulation points than $1/\sqrt{N}$, where N is non-square.

3. Proof of results

PROOF OF THEOREM 3. We will show the following: Let a, k, N be positive integers and $\epsilon_1, \epsilon_2 = \pm 1$ such that $ka + \epsilon_1 \neq 0$. Suppose p, q are non-zero integers satisfying the quadratic Diophantine equation:

$$aq^2 - (ka + \epsilon_1)Np^2 = \epsilon_2. \tag{1.6}$$

Then there exist non-zero integers r, s, t, u, v such that $A^r B^s A^t B^u A^v(0) = 0$; equivalently,

$$A^r B^s A^t B^u A^v = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}. \tag{3.1}$$

The trick is that, instead of trying to solve for r, s, t, u, v by multiplying out the matrices in equation (3.1), we use the intermediate point ϵ_1/a. Let

$$r = -\epsilon_2(ka + \epsilon_1)q^2, \qquad s = -N, \qquad t = k,$$
$$u = \epsilon_1(ka + \epsilon_1)N, \quad \text{and} \quad v = \epsilon_1\epsilon_2 q^2.$$

The following is immediate from (2.3) and (1.6):

$$A^{-v}B^{-u}\left(\frac{\epsilon_1}{a}\right) = 0, \qquad A^r B^s\left(\frac{ka + \epsilon_1}{a}\right) = 0, \qquad A^t\left(\frac{\epsilon_1}{a}\right) = \frac{ka + \epsilon_1}{a}$$

so that $A^r B^s A^t B^u A^v(0) = 0$. Note that r, s, t, u, v are all non-zero integers.

PROOF OF COROLLARY 2. Let $f(x, y) = ax^2 - (ka + \epsilon_1)Ny^2$. The discriminant of f, $\Delta(f) = 4a(ka + \epsilon_1)N$ is positive. Furthermore, if $f(x, y) = \epsilon_2$ admits an integer solution, then a and $(ka + \epsilon_1)N$ are relatively prime. $\Delta(f)$ cannot be a square since this would imply that a and $(ka + \epsilon_1)N$ are also squares, contradicting the fact that $f(x, y) = \epsilon_2$ admits an integer solution. It now follows by well-known results in number theory (see [4, pp. 104–122]) that $f(x, y) = \epsilon_2$ admits infinitely many integer solutions if it admits a solution. If we write the set of solutions as $\{(x, y) = (q_n, p_n) : n = 1, 2, \ldots, p_1 < p_2 < \cdots\}$, then p_n/q_n converges to $\sqrt{a/(ka + \epsilon_1)N}$ as n approaches infinity.

https://doi.org/10.1017/S1446788700000434 Published online by Cambridge University Press

4. Concluding remarks

In proving our results, we have only used words of the form

$$W = A^r B^s A^t B^u A^v = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}.$$

By considering words of arbitrary length, we should be able to determine more values of μ for which G_μ is not free. In fact, since the converse of Lyndon and Ullman's observation is also true (if G_μ is not free, there exists non-zero integers $a_1, b_1, \ldots, a_n$ such that

$$W_n = A^{a_n} \ldots B^{b_1} A^{a_1} = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \quad),$$

we should in principle be able to determine all rational values of μ for which G_μ is not free using this criterion but there is no clear way to choose the a_i and the b_i so that eventually zero gets mapped to itself.

One seemingly natural choice is the following algorithm:

Algorithm for forming words in A and B to determine if G_μ is not free.

STEP 1: Choose $a_1 = 1$ so $A^{a_1}(0) = 1$.

GENERAL STEP: We have a word W in A and B with $W(0) = \alpha/\beta$. If the left term of W is a power of A, choose a non-zero power b_k of B so that the absolute value of the denominator of $B^{b_k}(\alpha/\beta)$ is minimized and form the new word $B^{b_k}W$. If the left term of W is a power of B, choose a non-zero power a_k of A so that the absolute value of the numerator of $A^{a_k}(\alpha/\beta)$ is minimized and form the new word $A^{a_k}W$. If at some point, the numerator becomes zero, we stop and conclude that G_μ is not free; however, if the process does not terminate, we cannot, in general, make any conclusions about G_μ.

The above algorithm is, in fact, essentially the same as the difference equation method given by Lyndon and Ullman in [5]. Also, for the first step, we can choose a_1 to be any non-zero integer. However, the algorithm does not terminate when $\mu = 7/4$ as observed in [5]. Running our algorithm through a computer, we obtained a word W_1 in A and B such that $W_1(0) = 4/7$ and continuing the process, we found another word W_2 with $W_2(4/7) = 4/7$. This explains why the process does not terminate: the images become periodic after a finite time and 0 is not in the periodic loop. The word we obtain would thus be $\cdots W_2 W_2 W_1$. However, this is actually sufficient to show that G_μ is not free for $\mu = 7/4$ since we have $W_1^{-1} W_2 W_1(0) = 0$. Unfortunately,

https://doi.org/10.1017/S1446788700000434 Published online by Cambridge University Press

the word W_1 is extremely long with length of about 1,000. One can obtain a much shorter word by using the trick in the proof of Theorem 3 and mapping 0 to $1/3$ and then $-2/3$ first. We obtain the following much shorter word:

$$A^{16}B^{-1}A^3B^2A^6B^{-1}A^2BA^{-1}B^{-26}AB^{-1}A^4B^{-1}AB^{-1}AB^{-1}A^{16} = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}.$$

The above algorithm does provide a possible means of attacking the problem, if one could show for example that the numerators α_k of the successive images of 0 under the algorithm return infinitely often to a certain bounded set, say, $|\alpha_k| < N$ for infinitely many k, then the next denominator is bounded by Np^2 so that by the pigeon-hole principle, the successive images of 0 eventually become periodic, giving words W_1, W_2 in A and B with $W_1(0) = \alpha/\beta$, $W_2(\alpha/\beta) = \alpha/\beta$ which would imply that G_μ is not free. There seems to be some interesting ergodic properties related to the algorithm and a probabilistic or ergodic theoretic method may show a dense set of rational μ in some open sub-interval of $(0, 2)$ for which G_μ is not free.

Acknowledgment

The authors would like to thank Seng-Kiat Chua for helpful conversations and in particular for supplying the list of $N < 100$ for which equation (1.8) admits integer solutions.

References

[1] A. Beardon, *The geometry of discrete groups* (Springer, New York, 1983).
[2] ———, 'Pell's equation and two generator free Möbius groups', *Bull. London Math. Soc.* **25** (1993), 527–532.
[3] B. Chang, S.A. Jennings and R. Ree, 'On certain pairs of matrices which generate free groups', *Canad. J. Math.* **10** (1958), 279–284.
[4] D. E. Flath, *Introduction to number theory* (Wiley, New York, 1989).
[5] R. C. Lyndon and J. L. Ullman, 'Groups generated by two linear parabolic transformations', *Canad. J. Math.* **21** (1969), 1388–1403.

Department of Mathematics
Faculty of Science
National University of Singapore
10 Kent Ridge Crescent
Singapore 0511
e-mail: mattanec@nus.sg and mattansp@nus.sg