Applied Mathematics, 2014, 5, 1400-1411
Published Online June 2014 in SciRes. http://www.scirp.org/journal/am
http://dx.doi.org/10.4236/am.2014.510132

Scientific Research

Diophantine Equations and the Freeness of Möbius Groups

Marin Gutan

Laboratoire de Mathématiques, Université Blaise-Pascal, Clermont-Ferrand, France
Email: marin.gutan@math.univ-bpclermont.fr

Received 16 March 2014; revised 16 April 2014; accepted 23 April 2014

Abstract

Let p and q be two fixed non zero integers verifying the condition $gcd(p,q)=1$. We check solutions in non zero integers a_1, b_1, a_2, b_2 and a_3 for the following Diophantine equations: ($B1$) $(a_1+a_2)q^2+a_1b_1a_2p^2=0$ ($B2$) $(a_1+a_2+a_3)q^4+(a_1b_1a_2+a_1b_1a_3+a_1b_2a_3+a_2b_2a_3)q^2p^2+a_1b_1a_2b_2a_3p^4=0$. The equations ($B1$) and ($B2$) were considered by R.C. Lyndon and J.L. Ullman in [1] and A.F. Beardon in [2] in connection with the freeness of the Möbius group G_λ generated by two matrices of $\mathcal{SL}_2(\mathbb{C})$, namely $A=\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix}$ and $B=\begin{pmatrix}1 & 0\\ \lambda & 1\end{pmatrix}$ where $\lambda=\frac{p}{q}$. They proved that if one of the equations ($B1$) or ($B2$) has solutions in non zero integers then the group G_λ is not free. We give algorithms to decide if these equations admit solutions. We obtain an arithmetical criteria on p and q for which ($B1$) admits solutions. We show that for all p and q the equations ($B1$) and ($B2$) have only a finite number of solutions.

Keywords

Diophantine Equation, Möbius Groups, Free Group

1. Introduction

Let k and d be two positive integers with $d\geq 2$ and $A_1,\cdots,A_k$ be matrices of the group $\mathcal{GL}_d(\mathbb{C})$.

How to cite this paper: Gutan, M. (2014) Diophantine Equations and the Freeness of Möbius Groups. *Applied Mathematics*, **5**, 1400-1411. http://dx.doi.org/10.4236/am.2014.510132

Denote $\mathcal{G}p(A_1,\cdots,A_k)$ the group, respectively $\mathcal{S}gp(A_1,\cdots,A_k)$ the semigroup, generated by the matrices $A_1,\cdots,A_k$.

The following problem $\mathfrak{P}$ has been studied in several papers:

- Instance: $A_1,\cdots,A_k \in \mathcal{GL}_d(\mathbb{C})$
- Question: $\mathcal{G}p(A_1,\cdots,A_k)$ or $\mathcal{S}gp(A_1,\cdots,A_k)$ are they free with $A_1,\cdots,A_k$ as generators?

Recall that in 1991 D. Klarner, J.-C. Birget and W. Satterfield in [3] proved that if $d \geq 3$ then the problem $\mathfrak{P}$ is not decidable. Moreover in 1999 J. Cassaigne, T. Harju and J. Karhümaki in [4] proved that the same result is true if we suppose that all the matrices $A_1,\cdots,A_k$ are lower triangular.

The case $d=2$ is open and seems difficult. In [5] and [6] results concerning the freeness of the semigroups and groups generated by two matrices are established. In this paper we are studying this problem restricted to the case of Möbius groups.

Let $\lambda \in \mathbb{C}^*$ and $\tau = \lambda^2$. The Möbius group G_λ is the subgroup of $\mathcal{SL}_2(\mathbb{C})$ generated by $A = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$.

The problem of characterization of the set of complex values of λ or τ for which the group G_λ is free, was studied in several papers. Thus in [1] it is proved that if λ is transcendental or $|\lambda| \geq 2$ then G_λ is free.

R.C. Lyndon and J.L. Ullman in [1] remarked that G_λ is not free if and only if there exists a word $w = a_1 b_1 a_2 b_2 \cdots a_{n-1} b_{n-1} a_n$ whose $2n-1$ letters are non zero integers so that the product of the powers of matrices $M_\lambda(w) = A^{a_1} B^{b_1} A^{a_2} B^{b_2} \cdots A^{a_{n-1}} B^{b_{n-1}} A^{a_n}$ is a lower triangular matrix. The element in the right upper corner of the matrix $M_\lambda(w)$ is of the form $\lambda \mathcal{Q}_\tau(w)$ where $\mathcal{Q}_\tau(w) = \sum_{j=0}^{n-1} c_j \tau^j$ is a polynomial in τ of degree $n-1$ with coefficients c_j. Moreover c_j are polynomials with integers coefficients in the variables $a_1, b_1, a_2, b_2, \cdots, a_n$.

Results concerning the set of algebraic values of λ or τ for which the group G_λ is not free were obtained in [1] [2] [7]-[11].

Deciding if for $\tau \in \mathbb{Q} \cap]0,4[$ the group G_λ is not free seems very difficult. Let us recall some important results in this direction.

The group G_λ is not free if λ belongs to one of the following sets: $A = \left\{ \frac{1}{n} \middle| n \in \mathbb{Z}^* \right\}$,

$B = \left\{ \frac{p}{kp+1} \middle| p, k \in \mathbb{N}^* \right\}$, $C = \left\{ \frac{m+n}{mn} \middle| m, n \in \mathbb{N}^*, m+n > 1 \right\}$ (see [1] [2] [7] [8] [10] [11]).

In this paper we check if for a given $\tau \in \mathbb{Q} \cap]0,4[$ there exists a non trivial word of non zero integers $w = a_1 b_1 a_2 b_2 \cdots a_{n-1} b_{n-1} a_n$ such that $Q_\tau(w) = 0$.

The main results of our paper concern the freeness of Möbius groups:

- We prove that if the length of w is small then the problem is decidable (cases $n=2$ and $n=3$) (see Theorems 1, 2 and 3).
- We give algorithms which solve the problem for $n \in \{2,3\}$ (see Corollary 1 and the proof of Theorem 3). Moreover, we give an arithmetical criteria for this problem when $n=2$ (see 2 of Theorem 1).
- We give a lower bound numerical function l defined from $\mathbb{Q} \cap]2,4[$ to $\mathbb{N}^*$, increasing and unbounded, such that for each $\tau \in \mathbb{Q} \cap]2,4[$, if $M_\tau(w)$ is a lower triangular matrix then the length of w is bigger than $l(\tau)$ (see Theorem 4 and Corollary 3).

As proved by A.F. Beardon ([2]) in these two cases $n \in \{2,3\}$ we have to find solutions for the equations ($B1$) and ($B2$). In fact in our paper we consider and study two more general equations:

($B'1$) $(a_1 + a_2)q + a_1 b_1 a_2 p = 0$

($B'2$) $(a_1 + a_2 + a_3)q^2 + (a_1 b_1 a_2 + a_1 b_1 a_3 + a_1 b_2 a_3 + a_2 b_2 a_3)qp + a_1 b_1 a_2 b_2 a_3 p^2 = 0$.

2. Sequences of Polynomials Associated to Matrices

In this section, we study the properties of some sequences of polynomials in a fixed $\tau = \lambda^2$ associated to matrices of the group G_λ.

We consider $\left(\left(\mathbb{Z}\setminus\{0\}\right)^*,\cdot\right)$ the free monoid of words on non zero integers with the concatenation operation. We denote by ϵ the empty word of the free monoid $\left(\mathbb{Z}\setminus\{0\}\right)^*$ and a non empty word $w\in\left(\mathbb{Z}\setminus\{0\}\right)^*$ by $w=k_1k_2k_3\cdots k_n$, where $k_1,\cdots,k_n$ are non zero integers. Then n is called the length of w and is denoted by $|w|$. The reversal of a word $w=k_1k_2k_3\cdots k_n$ is $w^{\sim}=k_n\cdots k_3k_2k_1$ and the opposite of w is $-w=(-k_1)(-k_2)(-k_3)\cdots(-k_n)$.

For every word $w=a_1b_1a_2b_2\cdots a_{n-1}b_{n-1}a_n$ of $\left(\mathbb{Z}\setminus\{0\}\right)^*$ of length $|w|=2n-1$ we consider the matrix product

$$M_\lambda(w)=A^{a_1}B^{b_1}A^{a_2}B^{b_2}\cdots A^{a_{n-1}}B^{b_{n-1}}A^{a_n}.$$

For instance, for a_1,b_1,a_2 non zero integers we have:

$$M_\lambda(a_1)=\begin{pmatrix}1 & a_1\lambda\\ 0 & 1\end{pmatrix} \text{ and } M_\lambda(a_1b_1a_2)=\begin{pmatrix}1+a_1b_1\tau & \lambda(a_1+a_2+a_1b_1a_2\tau)\\ b_1\lambda & 1+a_2b_1\tau\end{pmatrix}.$$

We use the notation:

$$M_\lambda(w)=\begin{pmatrix}\mathcal{P}_\tau(w) & \lambda\mathcal{Q}_\tau(w)\\ \lambda\mathcal{R}_\tau(w) & \mathcal{S}_\tau(w)\end{pmatrix}.$$

We remark that $\mathcal{P}_\tau(w),\mathcal{Q}_\tau(w),\mathcal{R}_\tau(w)$ and $\mathcal{S}_\tau(w)$ are polynomials in τ with coefficients in $\mathbb{Z}$. We also have $(-\omega)^{\sim}=-(\omega^{\sim})$ and $\left[M_\lambda(\omega)\right]^{-1}=M_\lambda\left((-\omega)^{\sim}\right)$

If $\mathcal{T}\in\{\mathcal{P},\mathcal{S}\}$ then $\mathcal{T}_\tau(-w)=\mathcal{T}_\tau(w)$ and if $\mathcal{T}\in\{\mathcal{Q},\mathcal{R}\}$ then $\mathcal{T}_\tau(-w)=-\mathcal{T}_\tau(w)$. Also $\mathcal{P}(w)=\mathcal{S}(w^{\sim})$ and if $\mathcal{T}\in\{\mathcal{Q},\mathcal{R}\}$ then $\mathcal{T}_\tau(w)=\mathcal{T}_\tau(w^{\sim})$.

We use the notation $M_\lambda(w)=\begin{pmatrix}* & 0\\ * & *\end{pmatrix}$ to indicate that $M_\tau(w)$ is a lower triangular matrix or that $\mathcal{Q}_\tau(w)=0$.

From now on, in order to simplify the notation we write:

$$\begin{pmatrix}P_n & \lambda Q_n\\ \lambda R_n & S_n\end{pmatrix}=\begin{pmatrix}\mathcal{P}_\tau(w) & \lambda\mathcal{Q}_\tau(w)\\ \lambda\mathcal{R}_\tau(w) & \mathcal{S}_\tau(w)\end{pmatrix}.$$

For instance, P_n is an abbreviation for the polynomial in τ with parameters $a_1,b_1,a_2,b_2,\cdots,a_{n-1},b_{n-1},a_n$ defined by:

$$P_n(a_1,b_1,a_2,b_2,\cdots,a_{n-1},b_{n-1},a_n)=\mathcal{P}_\tau(a_1b_1a_2b_2\cdots a_{n-1}b_{n-1}a_n).$$

Using the fact that $A,B\in\mathcal{SL}_2(\mathbb{C})$ we have:

$$P_nS_n-\tau Q_nR_n=1. \tag{1}$$

The sequences of polynomials in τ, $(P_n)_{n\geq1}$, $(Q_n)_{n\geq1}$, $(R_n)_{n\geq1}$ and $(S_n)_{n\geq1}$ verify the following relations:

$$\begin{pmatrix}P_1 & Q_1\\ R_1 & S_1\end{pmatrix}=\begin{pmatrix}1 & a_1\\ 0 & 1\end{pmatrix} \tag{2}$$

$$\begin{pmatrix}P_2 & Q_2\\ R_2 & S_2\end{pmatrix}=\begin{pmatrix}1+a_1b_1\tau & (a_1+a_2)+a_1b_1a_2\tau\\ b_1 & 1+a_2b_1\tau\end{pmatrix} \tag{3}$$

$$\begin{pmatrix}P_{n+1} & Q_{n+1}\\ R_{n+1} & S_{n+1}\end{pmatrix}=\begin{pmatrix}P_n+b_n\tau Q_n & a_{n+1}P_n+(1+a_{n+1}b_n\tau)Q_n\\ R_n+b_nS_n & a_{n+1}\tau R_n+(1+a_{n+1}b_n\tau)S_n\end{pmatrix} \tag{4}$$

$$\begin{pmatrix} P_{n+1} & Q_{n+1} \\ R_{n+1} & S_{n+1} \end{pmatrix} = \begin{pmatrix} P_n + b_n\tau Q_n & a_{n+1}P_{n+1} + Q_n \\ R_n + b_n S_n & a_{n+1}\tau R_{n+1} + S_n \end{pmatrix}. \tag{5}$$

The relations (4) and (5) follow from the equality

$$\begin{pmatrix} P_{n+1} & \lambda Q_{n+1} \\ \lambda R_{n+1} & S_{n+1} \end{pmatrix} = \begin{pmatrix} P_n & \lambda Q_n \\ \lambda R_n & S_n \end{pmatrix} B^{b_n} A^{a_{n+1}}.$$

In the following sections, we also use the following two relations:

$$P_3 = 1 + (a_1b_1 + a_1b_2 + a_2b_2)\tau + a_1b_1a_2b_2\tau^2. \tag{6}$$

$$\begin{aligned} Q_3 &= a_1 + a_2 + a_3 \\ &+ (a_1b_1a_2 + a_1b_1a_3 + a_1b_2a_3 + a_2b_2a_3)\tau + a_1b_1a_2b_2a_3\tau^2 \end{aligned} \tag{7}$$

Using the previous relations we obtain

Proposition 1 *The sequences* $(Q_n)_{n\geq 1}$ *and* $(Q_n)_{n\geq 1}$ *of polynomials in* τ *verify the following identities*:

$$a_nQ_{n+1} - [(a_n + a_{n+1}) + a_nb_na_{n+1}\tau]Q_n + a_{n+1}Q_{n-1} = 0 \tag{8}$$

$$b_nP_{n+1} - [(b_n + b_{n+1}) + b_na_nb_{n+1}\tau]P_n + b_{n+1}P_{n-1} = 0. \tag{9}$$

Proof. From (5) we have

$$P_{n+1} = \frac{1}{a_{n+1}}[Q_{n+1} - Q_n] \text{ and } P_n = \frac{1}{a_n}[Q_n - Q_{n-1}].$$

These identities and the equation $P_{n+1} = P_n + b_n\tau Q_n$ give the equation (8). The equation (9) can be similarly obtained .

Let us suppose that $\tau = \frac{p}{q} = \lambda^2$ where p and q are non zero integers and $gcd(p,q) = 1$.

If $p = 1$ the group G_λ is not free because in this case $Q_2(1,-2q,1)(\tau) = 0$ (see [1]).

In the following we consider that $p > 1$. Then $\mathcal{P}_{\frac{p}{q}}(w) \neq 0$, and $\mathcal{S}_{\frac{p}{q}}(w) \neq 0$. Indeed, if $\mathcal{P}_{\frac{p}{q}}(w)\mathcal{S}_{\frac{p}{q}}(w) = 0$ then using the fact that $\det(\mathcal{M}_\tau(w)) = 1$ we deduce $-\frac{p}{q}\mathcal{Q}_{\frac{p}{q}}(w)\mathcal{R}_{\frac{p}{q}}(w) = 1$ which is in contradiction with the fact that $gcd(p,q) = 1$.

This remark allows us to define a new sequence $(x_n)_{n\geq 1}$ by $x_n = \frac{Q_n}{P_n}$. This sequence satisfies the following relation:

$$x_{n+1} = a_{n+1} + \frac{1}{b_n\tau + \frac{1}{x_n}}. \tag{10}$$

Thus we obtain

$$x_{n+1} = a_{n+1} + \cfrac{1}{b_n\tau + \cfrac{1}{a_n + \cfrac{1}{b_{n-1}\tau + \cfrac{1}{a_{n-1} + \cdots}}}}.$$

These relations are similar with formulas for continued fractions. The properties of these sequences will be used in the next sections of our paper.

Let us also consider the sequence $(y_n)_{n\geq 1}$ defined by:

$$y_n = y_n(a_1, b_1, \cdots, a_n, b_n) = \frac{1}{b_n\tau + \frac{1}{x_n}} = x_{n+1} - a_{n+1}.$$

We remark that $x_{n+1}(a_1, b_1, \cdots, a_n, b_n, a_{n+1}) = 0$ if and only if

$$x_n(a_1, b_1, \cdots, a_n) = y_1(-a_{n+1}, -b_n).$$

The following lemma is the key element of Section 5.

Lemma 1 *Let* $a_1, b_1, \cdots, a_n, b_n, a_{n+1}$ *be* $2n+1$ *non zero integers and suppose that* $\tau > 1$. *If* $x_{n+1}(a_1, b_1, \cdots, a_n, b_n, a_{n+1}) = 0$ *then* $|x_n(a_1, b_1, \cdots, a_n)| \leq \frac{1}{\tau - 1}$.

Proof. If $x_{n+1}(a_1, b_1, \cdots, a_n, b_n, a_{n+1}) = 0$ we have

$$|x_n(a_1, b_1, \cdots, a_n)| = |y_1(-a_{n+1}, -b_n)| = \frac{1}{\left|b_n\tau + \frac{1}{a_{n+1}}\right|} \leq \frac{1}{|b_n|\tau - \frac{1}{|a_{n+1}|}} \leq \frac{1}{\tau - 1}.$$

Let $\tau = \lambda^2$ such that G_λ is not free. We define the following numerical function:

$\kappa(\tau) = \min\left\{n \in \mathbb{N}^* \middle| \exists w \in (\mathbb{Z} \setminus \{0\})^*, |w| = 2n-1 \text{ and } \mathcal{Q}_\tau(w) = 0\right\}$. The *number* $\kappa(\tau)$ will be called the *calibre* of the group G_λ.

Hence $\kappa(\tau) = 2$ if and only if there are non zero integers a_1, b_1, a_2 such that $A^{a_1}B^{b_1}A^{a_2} = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$. Also we have $\kappa(\tau) \leq 3$ if and only if there are non zero integers a_1, b_1, a_2, b_2, a_3 such that $A^{a_1}B^{b_1}A^{a_2}B^{b_2}A^{a_3} = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$.

3. The Diophantine Equation (B1)

In the next three sections, we consider the following problem $\mathfrak{P}(n)$, where $n \in \mathbb{N}$, $n \geq 2$:

- Instance: Two non zero integers p, q with $gcd(p, q) = 1$.
- Question: Is there a word of length $2n-1$ of non zero integers $w = a_1b_1 \cdots a_n$ such that

$$M_\tau(w) = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}, \text{ where } \tau = \frac{p}{q}?$$

So we check solutions in non zero integers $a_1, b_1, \cdots, a_n$ for the diophantine equation

$$Q_n(a_1, b_1, \cdots, a_n)(\tau) = 0. \tag{11}$$

The set of $\tau = \lambda^2$ for which the Möbius group G_λ is not free coincides with the set of τ for which there exists $n \geq 2$ such that the Equation (11) admits solutions.

In this section, we consider the case $n = 2$ and in the next section the case $n = 3$. The relation $Q_2(a_1, b_1, a_2) = 0$ is equivalent to the Equation ($B'1$) and the relation $Q_3(a_1, b_1, a_2) = 0$ is equivalent to the equation ($B'2$). If p and q are perfect squares we obtain the equations ($B1$) and ($B2$).

We will prove that the problem $\mathfrak{P}(2)$ is decidable. The decidability of the problem $\mathfrak{P}(2)$ has already been established by A.F. Beardon (Theorem 2, [2]) for the case when p and q are perfect squares. Our algorithm is simpler and allows us to give an arithmetical criteria for integers p and q for which the problem $\mathfrak{P}(2)$ has solutions (see Theorem 1 below).

First, we prove a result concerning the equation ($B'1$).

Proposition 2 *Let* p *and* q *be two integers with* $gcd(p, q) = 1$ *and* $\alpha \in \mathbb{Z}$. *Denote*

$$L(p, q, \alpha) = \left\{(a_1, b_1, a_2) \in (\mathbb{Z}^*)^3 \middle| q(a_1 + a_2) + pa_1b_1a_2 = \alpha\right\}.$$

Then:

1. If $(a_1,b_1,a_2)\in L(p,q,\alpha)$ and $i\in\{1,2\}$ we have

$$|b_1|\le\frac{1}{|p|}(|\alpha|+2|q|)$$

$$|a_i|\le\frac{1}{|p|}\left(q^2+|q|+|p\alpha|\right).$$

2. The set $L(p,q,\alpha)$ is finite.

Proof.

1) Let $(a_1,b_1,a_2)\in L(p,q,\alpha)$ and for $i\in\{1,2\}$ put $d_i=q+pa_ib_1$. Then $d_1d_2=q^2+pb_1\alpha$, $d_i\equiv q(mod\ p)$ and $d_i\ne q$.

As $b_1=\frac{1}{p}\left[\frac{\alpha}{a_1a_2}-q\left(\frac{1}{a_1}+\frac{1}{a_2}\right)\right]$ we deduce $|b_1|\le\frac{1}{|p|}(|\alpha|+2|q|)$. Because $|d_i|\le q^2+|pb_1\alpha|$ and $a_i=\frac{d_i-q}{pb_1}$ we have

$$|a_i|\le\frac{|d_i|+|q|}{|pb_1|}\le\frac{1}{|p|}\left(q^2+|q|+|p\alpha|\right).$$

2) results from (1).

Using the previous proposition we can obtain the decidability of the problem $\mathfrak{P}(2)$.

Theorem 1 *Let p and q be two integers with $gcd(p,q)=1$. The following sentences are equivalent*:

1. The equation $q(a_1+a_2)+pa_1b_1a_2=0$ has solutions in non zero integers.
2. There exists a divisor d of q^2, $d\ne q$ such that $d\equiv q(mod\ p)$.
3. $\tau=\frac{p}{q}\in\left\{\frac{1}{m}+\frac{1}{n}\middle|(m,n)\in(\mathbb{Z}^*)^2,m+n\ne0\right\}$.

Proof. The equivalence between (1) and (2) results from the Proposition 2. It is enough to consider $\alpha=0$ in that proposition. The equivalence between (1) and (3) is obvious.

Remark 1 *Let $D(n)$ be the set of all divisors of the integer n. If d is like in* (2) *of the previous Theorem* 1 *then a solution (a_1,b_1,a_2) to the equation* (*B*′1) *can be obtained by taking*

- $b_1\in D\left(\frac{d_1-q}{p}\right)\cap D\left(\frac{d_2-q}{p}\right)$ and
- $a_i=\frac{d_i-q}{pb_1}$ for $i\in\{1,2\}$

where $d_1=d$ and $d_2=\frac{q^2}{d}$. Moreover any solution (a_1,b_1,a_2) of the equation (*B*′1) can be obtained by this method. We can write τ as in (3) of the Theorem 1

$$\tau=\frac{p}{q}=\frac{1}{\frac{q-d_1}{p}}+\frac{1}{\frac{q-d_2}{p}}.$$

The results of A.F. Beardon ([2], theorem 2) concerning the problem $\mathfrak{P}(2)$ for the case when p and q are perfect squares (or equivalently when $\lambda\in\mathbb{Q}$) result immediately from the next corollary.

Corollary 1 *Let p and q be two non zero integers with $gcd(p,q)=1$ and $\tau=\frac{p^2}{q^2}=\lambda^2$. The group G_λ is not free with the calibre $k(\tau)=2$ if and only if there exists a divisor d of q^4, $d\ne q^2$ such that $d\equiv q^2\left(mod\ p^2\right)$.*

From the previous theorem it also follows:

1) The equation ($B'1$) has no solution if $\tau=\frac{p}{q}>2$.

2) $k\left(\frac{p}{q}\right)=2$ in the following cases: a) $p=1$; b) $p=2$; c) $p\geq 3$ and $q=kp\pm 1$ with $k\in\mathbb{N}^*$.

Below we present another form of the Theorem 1 in which we use the decomposition of q as a product of prime numbers.

Theorem 2 *Let p and q be two integers with $p>2$ and $gcd(p,q)=1$. Let us suppose that the decomposition of q as a product of powers of distinct prime numbers $\pi_1,\pi_2,\cdots,\pi_m$ is $q=\pi_1^{\alpha_1}\pi_2^{\alpha_2}\cdots\pi_m^{\alpha_m}$. Then $k\left(\frac{p}{q}\right)=2$ if and only if there exist*:

- two disjoint subsets I and J of $\{1,2,\cdots,m\}$ with $I\cup J\neq\emptyset$.
- a set of integers $(\delta_l)_{l\in I\cup J}$ with $1\leq\delta_l\leq\alpha_l$ for every $l\in I\cup J$.
- $\varepsilon\in\{1,-1\}$.

such that $\prod_{i\in I}\pi_i^{\delta_i}\equiv\varepsilon\prod_{j\in J}\pi_j^{\delta_j}\ (mod\ p)$.

Proof. Let $d=\varepsilon\pi_1^{\beta_1}\pi_2^{\beta_2}\cdots\pi_m^{\beta_m}$ be a divisor of $q^2, d\neq\pm q$. We can drop the case $d=-q$ because $p>2$. Hence $(\beta_1,\beta_2,\cdots,\beta_m)\neq(\alpha_1,\alpha_2,\cdots,\alpha_m)$ and $0\leq\beta_k\leq 2\alpha_k$ for every $k\in\{1,2,\cdots,m\}$. We put $I=\left\{i\in\{1,2,\cdots,m\}\middle|\beta_i<\alpha_i\right\}$ and $J=\left\{j\in\{1,2,\cdots,m\}\middle|\beta_j>\alpha_j\right\}$. Then $I\cap J=\emptyset$ and $I\cup J\neq\emptyset$. Let:

$$\delta_\ell=\begin{cases}\alpha_\ell-\beta_\ell & \text{if } \ell\in I\\ \beta_\ell-\alpha_\ell & \text{if } \ell\in J\end{cases}.$$

We have $1\leq\delta_\ell\leq\alpha_\ell$ for every $\ell\in I\cup J$. The condition $d\equiv q\ (mod\ p)$ is equivalent to

$$\prod_{i\in I}\pi_i^{\delta_i}\equiv\varepsilon\prod_{j\in J}\pi_j^{\delta_j}\ (mod\ p).$$

Corollary 2 *Let p and α be two non zero integers and π be a prime number. Suppose that $gcd(p,\pi)=1$. Then $k\left(\frac{p}{\pi^\alpha}\right)=2$ if and only if there exists an integer δ with $1\leq\delta\leq\alpha$ such that $\pi^\delta\equiv\varepsilon(mod\ p)$ where $\varepsilon\in\{1,-1\}$.*

Proof. We take $m=1$ in the previous theorem.

Example: Using the previous results and an example from ([7]) we have $k\left(\frac{12}{127}\right)=3$ and $k\left(\frac{12}{127^2}\right)=2$.

4. The Beardon Diophantine Equation (B2)

Now we consider the problem $\mathfrak{P}(3)$. We mention that the equation $Q_3(a_1,b_1,a_2,b_2,a_3)(\tau)=0$ has been considered in several papers (see [2] [8] [10]) for the case when p and q are perfect squares.

From now on, we suppose that $Q_2(a_1,b_1,a_2)(\tau)\neq 0$ for every $(a_1,b_1,a_2)\in(\mathbb{Z}^*)^3$ *i.e.* following Theorem 1, τ does not belong to $A=\left\{\frac{1}{m}+\frac{1}{n}\middle|(m,n)\in(\mathbb{Z}^*)^2, m+n\neq 0\right\}$. Hence we can define a function $\varphi:]0,4[\cap(\mathbb{Q}\setminus A)\to\mathbb{Q}_+^*$ by $\varphi(\tau)=\inf\{|\tau-\alpha|\,|\,\alpha\in A\}$. We remark that $\varphi(\tau)>0$ and

a) $\varphi(\tau)=\tau-2$ if $\tau\in]2,4[$.

b) $\varphi(\tau)=\min\left\{\tau-1-\frac{1}{k+1},1+\frac{1}{k}-\tau\right\}$ if $\tau\in]1,2[$, where $k=\left[\frac{1}{\tau-1}\right]$.

Using the relations (8) for the sequence of polynomials $(Q_n)_{n\geq 1}$ we prove that the problem $\mathfrak{P}(3)$ is decidable.

Theorem 3 *Let $\tau\in Q\cap]0,4[$ such that τ does not belong to the set $\left\{\frac{1}{m}+\frac{1}{n}\middle|(m,n)\in(\mathbb{Z}^*)^2\right\}$. Then the*

equation

$$Q_3(a_1,b_1,a_2,b_2,a_3)(\tau)=0$$

has a finite number of solutions $(a_1,b_1,a_2,b_2,a_3)\in(\mathbb{Z}^*)^5$.

Proof. Using the relations (8) we deduce that

$$Q_2(a_1,b_1,a_2)Q_2(a_2,b_2,a_3)=a_1a_3.$$

Hence $\left(\tau+\frac{1}{b_1}\left(\frac{1}{a_1}+\frac{1}{a_2}\right)\right)\left(\tau+\frac{1}{b_2}\left(\frac{1}{a_2}+\frac{1}{a_3}\right)\right)=\frac{1}{b_1b_2a_2^2}$. Using the function φ we have:

$$|b_1b_2|a_2^2\le\frac{1}{\left[\varphi(\tau)\right]^2}.$$

We obtain a finite number of possibilities for b_1,b_2 and a_2. So a_1 and a_3 remain to be studied. From the equation

$$Q_3(a_1,b_1,a_2,b_2,a_3)(\tau)=0$$

it follows that

$$P_3(a_1,b_1,a_2,b_2,a_3)S_3(a_1,b_1,a_2,b_2,a_3)=1.$$

Hence there exists $(d_1,d_2)\in\mathbb{Z}^2$ such that

- $d_1d_2=q^4$.
- $q^2+(a_1b_1+a_1b_2+a_2b_2)qp+a_1b_1a_2b_2p^2=d_1$.
- $q^2+(a_2b_2+a_3b_1+a_2b_1)qp+a_3b_2a_2b_1p^2=d_2$.

Thus there exists a finite number of possibilities for a_1 and a_3.

If $Q_3(a_1,b_1,a_2,b_2,a_3)(\tau)=0$ from the inequality $|b_1b_2|a_2^2\le\frac{1}{\left[\varphi(\tau)\right]^2}$ we obtain

a) If $\tau\in\left]3,4\right[$ then $\mathfrak{P}(3)$ has no solution.

b) If $\tau\in\left]2+\frac{1}{\sqrt{2}},3\right[$ then $b_1,b_2,a_2\in\{-1,1\}$.

We also remark that the equation ($B'2$) is equivalent to the following equation

$$\frac{a_1q}{q+a_1b_1p}+\frac{a_3q}{q+a_3b_2p}=-a_2. \tag{12}$$

This enables us to obtain some explicit expressions for the rationals τ such that equation ($B'2$) has solutions in $\mathbf{Z}^*$.

Proposition 3 *Let k,ℓ be two* non *zero integers and k_1,k_2 be two divisors of k. If $\tau=\frac{1}{k}+\frac{1}{\ell}\left(\frac{1}{k_1}+\frac{1}{k_2}\right)$ then the equation* ($B'2$) *has solutions in* $\mathbf{Z}^*$.

Proof. Let $b_1=k_1,b_2=k_2,a_2=-\ell$ and $b_1a_1=b_2a_3=-k$. Then (10) is equivalent to $\tau=\frac{1}{k}+\frac{1}{\ell}\left(\frac{1}{k_1}+\frac{1}{k_2}\right)$.

Note that if in equation ($B'2$) we have $b_1a_1=b_2a_3$ then τ is exactly given by the above expression.

Using once again (10) we obtain

Proposition 4 *Let α and α' be in $\mathbf{Z}^*$ with $|\alpha|\ne|\alpha'|$. If*

$$\tau=\frac{\alpha^2+\alpha'^2}{\alpha\alpha'(\alpha-\alpha')}$$

then the equation ($B'2$) has solutions in $\mathbf{Z}^*$.

Proof. Consider (10) for $b_1=b_2=1, a_1=\alpha$ and $a_3=-\alpha'$. Then $\dfrac{1}{b_1\tau+\dfrac{1}{a_1}}=\alpha-\rho$ and $\dfrac{1}{b_2\tau+\dfrac{1}{a_3}}=-\alpha'+\rho$, where $\rho=\dfrac{\alpha^2+\alpha'^2}{\alpha+\alpha'}$. It follows that if we take $-a_2=\alpha-\alpha'$ then (10) is verified.

In the next proposition we give another method to obtain solutions of Equation (*B*'2). It is similar to those presented in [8] and [10].

Proposition 5 *Let p and q be two integers with $gcd(p,q)=1$. Suppose that there exist a_1, b_2 and a_2 in $\mathbf{Z}^*$ such that $(a_1+a_2)q+a_1b_1a_2p=1$. If $\tau=\dfrac{p}{q}$ then the equation (B'2) has solutions in $\mathbf{Z}^*$.*

Proof. Let $A_1=a_1q, B_1=b_1a_2, A_2=-1, B_2=-b_2a_1$ and $A_3=a_2q$. Then $\dfrac{1}{B_1\tau+\dfrac{1}{A_1}}+\dfrac{1}{B_2\tau+\dfrac{1}{A_2}}=-A_2$. Hence the **equation** (*B*'2) has solutions.

We end this section with the following open questions:

Questions:

1) Find all the solutions of (*B*2).

2) Find arithmetical characterizations (similar to those given in Theorem 1 for the positive integers p and q for which the problem $\mathfrak{P}(3)$ has solutions.

5. Increasing Unbounded Lower Bound Function for κ

In this section, we prove that in order to show that the group G_λ is not free for a rational τ with $\tau=\lambda^2<4$ and τ close to 4, we have to consider longer and longer words in A and B. Similar remarks (without any proof) have been made by A.F. Beardon in [2] and S.P. Farbman in [7].

Everywhere in this section, we consider that τ is a rational number in the open interval $]2,4[$.

From the Lemma 1, Section 2, if $x_{n+1}(a_1,\cdots,a_n,b_n,a_{n+1})(\tau)=0$ then $\left|x_n(a_1,\cdots,a_n)(\tau)\right|\le\dfrac{1}{\tau-1}$. For this reason we consider the sequence $(\alpha_n)_{n\ge1}$ of rational functions in the variable τ, $\alpha_n=\alpha_n(\tau)$, defined by:

$$\begin{cases}\alpha_1=1\\ \alpha_{n+1}=1-\dfrac{1}{\tau-\dfrac{1}{\alpha_n}}\end{cases}$$

For example

$$\alpha_2(\tau)=\frac{\tau-2}{\tau-1}, \alpha_3(\tau)=\frac{\tau^2-4\tau+3}{\tau^2-3\tau+1} \text{ and } \alpha_4(\tau)=\frac{\tau^3-6\tau^2+10\tau-4}{\tau^3-5\tau^2+6\tau-1}.$$

We also define the function $l:]2,4[\to\mathbf{N}\setminus\{0,1\}$ by the formula:

$$l(\tau)=\inf\left\{k\in\mathbf{N}^*\middle|\alpha_k(\tau)\le\frac{1}{\tau-1}\right\}.$$

Thus one has $l(\tau)=2$ if and only if $\tau\in]2,3]$, $l(\tau)=3$ if and only if $\tau\in\left]3,2+\sqrt{2}\right]$ and $l(\tau)=4$ if and only if $\tau\in\left[2+\sqrt{2},\dfrac{5+\sqrt{5}}{2}\right]$.

Now we will calculate $\alpha_n(\tau)$.

Note that $\alpha_n(\tau)=x_n(1,-1,1,-1,\cdots,-1,1)(\tau)$. For this reason we find the matrix

$X_{n+1}=AB^{-1}AB^{-1}\cdots AB^{-1}A=\left(AB^{-1}\right)^n A=C^nA$, where $C=AB^{-1}$. We suppose now that $\lambda=2\sin\left(\frac{\theta}{2}\right)$ with $\theta\in\left]\frac{\pi}{2},\pi\right[$, so $\tau=\lambda^2=2(1-\cos\theta)$. As $\operatorname{trace}(C)=2-\tau=2\cos\theta$ the matrix C verifies the equation:

$$C^2-2\cos\theta C+I_2=O_2.$$

Using this relation we find that

$$C^n=\frac{1}{\sin\theta}\begin{pmatrix}\sin((n+1)\theta)-\sin\theta & 2\sin\left(\frac{\theta}{2}\right)\sin(n\theta)\\ -2\sin\left(\frac{\theta}{2}\right)\sin(n\theta) & \sin(n\theta)-\sin\left((n-1)\frac{\theta}{2}\right)\end{pmatrix}.$$

Hence $\alpha_{n+1}(\tau)=\frac{\sin((n+1)\theta)}{\sin((n+1)\theta)-\sin(n\theta)}=\frac{1}{1-\frac{\sin(n\theta)}{\sin((n+1)\theta)}}$.

Lemma 2 *Let* $(\alpha,\tau,x)\in\mathbb{R}^3$, $\tau>2$ *be such that* $|x|\geq\alpha>\frac{1}{\tau-1}$. *Then for every* $a,b\in\mathbf{Z}^*$ *we have* $\left|a+\frac{1}{b\tau+\frac{1}{x}}\right|\geq 1-\frac{1}{\tau-\frac{1}{\alpha}}>0$.

Proof. Since $\frac{1}{|x|}\leq\tau-1<\tau$ we obtain that $\left|\frac{1}{b\tau+\frac{1}{x}}\right|\leq\frac{1}{\tau-\frac{1}{\alpha}}<1$. Hence $\left|a+\frac{1}{b\tau+\frac{1}{x}}\right|\geq 1-\frac{1}{\tau-\frac{1}{\alpha}}$.

The previous expression for $\alpha_n(\tau)$ and Lemma 2 show that $l(\tau)$ is well defined and $l(\tau)<\kappa(\tau)$, for every τ in the open interval $]2,4[$. So l is a lower bound numerical function for the function κ restricted to $]2,4[$.

Theorem 4 *For any* $n\in\mathbb{N}^*$ *and* $\tau\in]2,4[$ *one has* $l(\tau)=n+1$ *if and only if there exists* $\theta\in\left]\frac{n}{n+1}\pi,\frac{n+1}{n+2}\pi\right]$ such *that* $\tau=2-2\cos\theta$.

Proof. Let $l(\tau)=n+1$, where $n\in\mathbb{N}^*$. From the definition of the function l this previous equality holds if and only if $\alpha_{n+1}(\tau)\leq\frac{1}{\tau-1}$ and $\alpha_k(\tau)>\frac{1}{\tau-1}$, for all $k\in\{1,\cdots,n\}$. But $\alpha_k(\tau)>\frac{1}{\tau-1}$ if and only if $\frac{1}{1-\frac{\sin((k-1)\theta)}{\sin(k\theta)}}>\frac{1}{1-2\cos\theta}$.

Thus we obtain the system of two inequalities $\frac{\sin((k-1)\theta)}{\sin(k\theta)}<1$ and $\frac{\sin((k+1)\theta)}{\sin(k\theta)}<0$.

Finally, $l(\tau)=n+1$ if and only if we have $\frac{\sin((n+1)\theta)}{\sin((n+2)\theta)}\geq 0$ and $\frac{\sin(k\theta)}{\sin((k+1)\theta)}<0$ for all $k\in\{1,\cdots,n\}$.

These inequalities give $\theta\in\left]\frac{n}{n+1}\pi,\frac{n+1}{n+2}\pi\right]$.

Corollary 3 *The function* l *is increasing and unbounded.*

Therefore

$$\lim_{\tau\to 4,\tau<4} l(\tau)=\lim_{\tau\to 4,\tau<4}\kappa(\tau)=\infty.$$

Example: We consider the sequence $\tau_n=4-\frac{1}{2^n}$, for $n\in\mathbf{N}$.

• For $n=0$ we have $\tau_0=3$. So $\alpha_2(\tau_0)=\frac{1}{2}\le\frac{1}{\tau_0-1}$, hence $l(\tau_0)=2$. As $x_3(-1,1,-1,1,-1)(\tau_0)=0$, it follows that $\kappa(\tau_0)=3$.

• For $n=1$ we have $\tau_1=\frac{7}{2}$ and $\alpha_2(\tau_1)=\frac{3}{5}$, $\alpha_3(\tau_1)=\frac{5}{11}$, $\alpha_4(\tau_1)=\frac{3}{13}<\frac{1}{\tau_1-1}=\frac{2}{5}$. Hence $l(\tau_1)=4$ and since

$$x_5(2,-1,1,-1,1,-1,1,-1,2)(\tau_1)=0$$

we have $\kappa(\tau_1)=5$

• For $n=2$ we have $\tau_2=\frac{15}{4}$ and $\alpha_2(\tau_2)=\frac{7}{11}$, $\alpha_3(\tau_2)=\frac{33}{61}$, $\alpha_4(\tau_2)=\frac{119}{251}$, $\alpha_5(\tau_2)=\frac{305}{781}$, $\alpha_6(\tau_2)=\frac{231}{451}<\frac{1}{\tau_2-1}=\frac{4}{11}$. Hence $l(\tau_2)=6$ and $\kappa(\tau_2)\ge 7$. From [7] we have $\kappa(\tau_2)\le 18$.

Questions:

1) Is it true that for every $\tau\in\mathbb{Q}\cap]0,4[$ and $n\in\mathbb{N},n\ge 2$, the problem $\mathfrak{P}(n)$ is decidable?

2) Is it true that for every $\tau\in\mathbb{Q}\cap]0,4[$ there exists $n\in\mathbb{N},n\ge 2$ such that the problem $\mathfrak{P}(n)$ is decidable?

3) Is it true that for every $\tau\in\mathbb{Q}\cap]0,4[$ there exists $n\in\mathbb{N},n\ge 2$, such that the problem $\mathfrak{P}(n)$ has solutions?

4) Find $\kappa(\tau_n)$, for $n\ge 2$.

Acknowledgements

I thank Elias Tahhan (University S. Bolivar, Caracas) and Jerzy Tomasik (Universite d'Auvergne, Clermont-Ferrand) for discussion concerning some logical aspects of my paper.

References

[1] Lyndon, R.C. and Ullman, J.L. (1969) Groups Generated by Two Linear Parabolic Transformations. *Canadian Journal of Mathematics*, **21**, 1388-1403. http://dx.doi.org/10.4153/CJM-1969-153-1

[2] Beardon, A.F. (1993) Pell's Equation and Two Generator Möbius Groups. *Bulletin of the London Mathematical Society*, **25**, 527-532. http://dx.doi.org/10.1112/blms/25.6.527

[3] Klarner, D., Birget, J.-C. and Satterfield, W. (1991) On the Undecidability of the Freeness of Integer Matrix Semigroups. *International Journal of Algebra and Computation*, **1,** 223-226. http://dx.doi.org/10.1142/S0218196791000146

[4] Cassaigne, J., Harju, T. and Karhumaki, J. (1999) On the Undecidability of the Freeness of Matrix Semigroups. *International Journal of Algebra and Computation*, **9**, 295-305. http://dx.doi.org/10.1142/S0218196799000199

[5] Cassaigne, J. and Nicolas, F. (2012) On the Decidability of Semigroup Freeness. *RAIRO—Theoretical Informatics and Applications*, **46**, 355-399. http://dx.doi.org/10.1051/ita/2012010

[6] Gawrychowski, P., Gutan, M. and Kisielewicz, A. (2010) On the Problem of Freness of Multplicative Matrix Semigroups. *Theoretical Computer Science*, **411**, 1115-1120. http://dx.doi.org/10.1016/j.tcs.2009.12.005

[7] Farbman, S.P. (1995) Non-Free Two-Generator Subgroups of $SL_2(Q)$. *Publicacions Mathemàtiques*, **39**, 379-391. http://dx.doi.org/10.5565/PUBLMAT_39295_13

[8] Tan, E.-C. and Tan, S.-P. (1996) Quadratic Diophantine Equations and Two Generators Möbius Groups. *Journal of the Australian Mathematical Society*, **61**, 360-368. http://dx.doi.org/10.1017/S1446788700000434

[9] de la Harpe, P. (2000) Topics in Geometric Group Theory. Chicago Lectures in Mathematics. University of Chicago Press, Chicago.

[10] Grytczuk, A. and Wojtowicz, M. (2000) Beardon's Diophantine Equations and Non-Free Möbius Groups. *Bulletin of the London Mathematical Society*, **32**, 305-310. http://dx.doi.org/10.1017/S1446788700000434

[11] Bamberg, J. (2000) Non-Free Points for Groups Generated by a Pair of 2 × 2 Matrices. *Journal of the London Mathematical Society*, **62**, 795-801. http://dx.doi.org/10.1112/S0024610700001630