On parabolic and elliptic elements of the modular group

BİLAL DEMİR
ÖZDEN KORUOĞLU

Follow this and additional works at: https://journals.tubitak.gov.tr/math

Part of the Mathematics Commons

Recommended Citation
Available at: https://journals.tubitak.gov.tr/math/vol46/iss7/13

This Article is brought to you for free and open access by TÜBİTAK Academic Journals. It has been accepted for inclusion in Turkish Journal of Mathematics by an authorized editor of TÜBİTAK Academic Journals. For more information, please contact academic.publications@tubitak.gov.tr.
On parabolic and elliptic elements of the modular group

Bilal DEMİR®, Özden KORUOĞLU*
Department of Mathematics, Necatibey Faculty of Education, Balıkesir University, Altıeylül, Balıkesir, Turkey

Received: 04.01.2022 • Accepted/Published Online: 03.07.2022 • Final Version: 05.09.2022

Abstract: The modular group $\Gamma = \text{PSL}(2, \mathbb{Z})$ is isomorphic to the free product of two cyclic groups of orders 2 and 3. In this paper, we give a necessary and sufficient condition for the existence of elliptic and parabolic elements in $\Gamma$ with a given cusp point. Then we give an algorithm to obtain such elements in words of generators using continued fractions and paths in the Farey graph.

Key words: Modular group, continued fractions, Farey graph

1. Introduction

The modular group $\Gamma = \text{PSL}(2, \mathbb{Z})$ consists of $2 \times 2$ matrices over the ring of integers with determinant 1. Since this is the quotient of $\text{SL}(2, \mathbb{Z})$ by $\{ \pm I \}$, every element is identified with its negative. The modular group is generated by two elements,

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

By taking $S = TU = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ then the presentation of $\Gamma$ is:

$$\Gamma = < T, S : T^2 = S^3 = I > \cong \mathbb{Z}_2 \ast \mathbb{Z}_3$$

The modular group acts on the upper half plane $\mathbb{H} = \{ x + iy : x, y \in \mathbb{R}, y > 0 \}$ via linear fractional transformations $(a \quad b \\ c \quad d, z) \to \frac{az + b}{cz + d}$. This action is discontinuous and these transformations are orientation preserving isometries of $\mathbb{H}$. There are numerous studies about the modular and extended modular group in the literature, relating many branches of mathematics such as group theory, number theory automorphic functions, etc. The algebraic structures of subgroups of the modular and extended modular group and related topics are studied in [1–12].

The complex number $z$ is called the fixed point of an element $V \in \Gamma$ if

$$V(z) = z$$

Correspondence: ozdenk@balikesir.edu.tr

2010 AMS Mathematics Subject Classification: 20H10, 11B57

This work is licensed under a Creative Commons Attribution 4.0 International License.
where \( V(z) \) is the Möbius transformation corresponding to \( V \). For \( V = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \) the solutions of the equation 1.1 are calculated as

\[
z = \frac{a - d \pm \sqrt{(a + d)^2 - 4}}{2c}
\]  

(1.2)

It can be seen from the equation 1.2 that the number of fixed points of an element \( V \in \Gamma \) is related to the trace of \( V \). Based on this consideration, the elements of \( \Gamma \) are classified as follows:

- \(|\text{tr}V| > 2\), then there are two fixed points in \( \mathbb{R} \cup \{\infty\} \) and \( V \) is called a hyperbolic element.
- \(|\text{tr}V| = 2\), then there is one fixed point in \( \mathbb{R} \cup \{\infty\} \) and \( V \) is called a parabolic element.
- \(|\text{tr}V| < 2\), then there are two conjugate fixed points in \( \mathbb{C} \cup \{\infty\} \) and \( V \) is called an elliptic element.

Since \( \Gamma \) is a discrete subgroup of \( \text{PSL}(2, \mathbb{R}) \), all elements of finite order are elliptic and vice versa. Parabolic and hyperbolic elements are of infinite order. The generator \( U \) is a parabolic element while the other generator \( T \) is elliptic of order 2. Elliptic elements are used in the presentation of \( \Gamma \) for describing the algebraic group structure. For this purpose, we consider the elliptic generator of order 3, \( S \). Hence the modular group is isomorphic to the free product of two cyclic groups of order 2 and 3. Furthermore, every element in \( \Gamma \) can be expressed as a word \( W(T, U) \) or \( W(T, S) \).

In this study, we give a necessary and sufficient condition for the existence of elliptic and parabolic elements in \( \Gamma \) with a given cusp point. A cusp point is the image of infinity under transformation defined by an element of the modular group. We then express these elements as words in generators. For this purpose, we use continued fractions and the Farey graph.

2. Materials and methods

There are impressive relationships between the modular group and continued fractions. In recent years many studies have contributed to the theory of continued fractions by considering the action of some subgroups of Möbius transformations. In [13] integer continued fraction expansions and geodesic expansions are studied from the perspective of graph theory. Short and Walker represented Rosen continued fractions by paths in a class of graphs in hyperbolic geometry[14]. The same authors also studied connections between even integer continued fractions and the Farey graph[15]. Relations between cusp points and Fibonacci numbers are studied in [16] using the Farey graph and continued fractions. Algebraic and combinatorial properties of continued fractions and the modular group related to the Farey graph are given in [17].

In [18], Rosen defined \( \lambda \) continued fractions for \( \lambda \in \mathbb{R} \):

\[
[r_0\lambda; r_1\lambda, ..., r_n\lambda] = r_0\lambda - \frac{1}{r_1\lambda - \frac{1}{r_2\lambda - \cdots - \frac{1}{\cdots - \frac{1}{r_{n-1}\lambda - \frac{1}{r_n\lambda}}}}}
\]

where the coefficients \( r_i \) are integers, which can be positive, negative, or zero. In this expansion, for \( i \leq n \), \( C_i = \frac{p_i}{q_i} = [r_0\lambda; r_1\lambda, ..., r_i\lambda] \) is called \( ith \) convergent of the expansion. And it can be seen by calculation that \( p_iq_{i-1} - q_ip_{i-1} = \pm 1 \). Owing to this viewpoint, Rosen revealed a criterion for the membership problem for
Hecke groups $H(\lambda)$, a general class of the modular group. He proved that an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H(\lambda)$ if and only if $\frac{a \lambda}{c}$ has a finite $\lambda$ continued fraction expansion. For $\lambda = 1$ this expression is called an integer continued fraction and is related to the modular group; the membership problem for the modular group is obvious because $\Gamma = \text{PSL}(2, \mathbb{Z})$. Continued fractions provide an interesting viewpoint for several problems of the modular group.

Consider the transformations $U(z) = z + 1$ and $T(z) = -\frac{1}{z}$ that correspond to the generators $U$ and $T$ of $\Gamma$. Let us observe the corresponding transformation of the element $V = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = U^{r_0}TU^{r_1}TU^{r_2}T...U^{r_n}T \in \Gamma$;

$$V(z) = U^{r_0}TU^{r_1}TU^{r_2}T...U^{r_n}T(z) = U^{r_0}TU^{r_1}TU^{r_2}T...U^{r_n}\left(-\frac{1}{z}\right) = U^{r_0}TU^{r_1}TU^{r_2}T...T(r_n - \frac{1}{z})$$

$$V(z) = r_0 - \frac{1}{r_1 - \frac{1}{...r_n - \frac{1}{z}}}$$

It can be seen that every word in $\Gamma$ is associated to an integer continued fraction expansion. Moreover, the image of infinity under the corresponding Möbius transformation is the integer continued fraction expansion of the cusp point. Conversely, every integer continued fraction expansion of a rational number $p/q$ is associated to a word $V = W(U, T) \in \Gamma$ such that $V(\infty) = \frac{p}{q}$.

A real number is rational if and only if it has a finite integer continued fraction expansion. There are some algorithms in the literature for obtaining integer continued fraction expansions of a real number, one of the best methods is using the Farey graph.

The Farey graph is a graph with vertex set $\hat{Q} = \mathbb{Q} \cup \{\infty\}$ and two reduced fractions $\frac{p}{q}$ and $\frac{r}{s}$ are adjacent if and only if $ps - rq = \pm 1$, i.e. they are Farey neighbours. An edge between two vertices is drawn by a hyperbolic line in $\mathbb{H}$. The edges between $\frac{1}{0}$ and $\frac{1}{1}$ are vertical lines. To construct the graph, first join the vertices $\frac{1}{0}, \frac{0}{1}$ and $\frac{1}{1}$ and obtain a big triangle. If the endpoints of a long edge are $\frac{a}{c}$ and $\frac{b}{d}$, the label of the third vertex of the triangle is $\frac{a}{c} \oplus \frac{b}{d} = \frac{a + b}{c + d}$, see in Figure 2.

A path in a graph consists of consecutive adjacent vertices. So a Farey path $< v_1, v_2, ..., v_n >$ is a path such that $v_i = \frac{p_i}{q_i} \in \frac{1}{0}$ for $i = 1, 2, ..., n$ are reduced rationals and since the consecutive $v_i$’s are adjacent $p_i, q_{i-1} - q_i, p_{i-1} = \pm 1$. We know from [19] that $C_1, C_2, ..., C_n$ are consecutive convergents of an integer continued fraction expansion of a rational $x$ if and only if $< \infty, C_0, C_1, ..., C_n, x >$ is a path in the Farey graph. Moreover, the geodesic path corresponds to the geodesic integer continued fraction expansion. We combine both this result and Rosen’s result to obtain word forms of elliptic and parabolic elements.
3. Results

In this section, we first give necessary and sufficient conditions for the existence of parabolic and elliptic elements in $\Gamma$ with a given cusp point $\frac{p}{q}$. Then we give an algorithm to express these elements in words of generators.

First, we start with elliptic elements. An elliptic element $V \in \Gamma$ has trace $trV = -1, 0, 1$. We investigate all cases.

**Theorem 3.1** Let $\frac{p}{q}$ be a reduced rational. Then there exists an elliptic element of order 2 in $\Gamma$ with cusp point $\frac{p}{q}$ if

$$q|p^2 + 1$$  \hspace{1cm} (3.1)

Furthermore, the aforementioned element is

$$V = \begin{pmatrix} p & -q^2 - 1 \\ q & -p \end{pmatrix}$$

**Proof** Let $V = \begin{pmatrix} p & r \\ q & s \end{pmatrix}$ be an elliptic element in $\Gamma$. Since $V$ is elliptic we have $|trV| = |p + s| < 2$. In addition, as $V$ is of order two we know from [20] that $V$ must be conjugate to $T$. Hence $trV = 0$. We have $p = -s$. Using $ps - qr = 1$ we calculate

$$r = \frac{p(-p) - 1}{q}$$

Here $r$ must be an integer hence the proof is done for the case $p + s = 0$. \hfill $\Box$

The elliptic elements of order 3 in $\Gamma$ have trace $\pm 1$. The proof of the following theorem is similar to that of Theorem 3.1 so we omit it.

**Theorem 3.2** For a given reduced rational $\frac{p}{q}$ there exists an elliptic element of order 3 in $\Gamma$ if,

$$q|\pm p - p^2 - 1$$  \hspace{1cm} (3.2)

2754
Additionally, the matrix representation of this element is
\[ V = \begin{pmatrix} p & \pm p - p^2 - 1 \\ q & \pm 1 - p \end{pmatrix} \]

**Corollary 3.3** Let \( \frac{p}{q} \) be a reduced rational number. Then there exists an elliptic element in \( \Gamma \) with cusp point \( \frac{p}{q} \) if and only if
\[ q \mid p^2 - 1 - trV.p \quad (3.3) \]
Furthermore, if the condition 3.3 holds then the desired element is:
\[ V = \begin{pmatrix} p & trV.p - p^2 - 1 \\ q & trV - p \end{pmatrix} \]

Here \( trV \) is the trace of \( V \) which can be 1, 0, −1 in this case.

Now we examine the parabolic case.

**Theorem 3.4** Let \( \frac{p}{q} \) be a reduced rational number. Then there exists a parabolic element in \( \Gamma \) with cusp point \( \frac{p}{q} \) if and only if
\[ q \mid (p \mp 1)^2 \quad (3.4) \]
Moreover, the aforementioned parabolic element is
\[ V = \begin{pmatrix} p & -(p \mp 1)^2 \\ q & \pm 2 - p \end{pmatrix} \]

**Proof** Suppose \( V = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \) is a parabolic element in \( \Gamma \). Then \( trV = p + s = \pm 2 \). We have \( s = \pm 2 - p \).
Using the equation \( ps - rq = 1 \) one can calculate,
\[ r = \frac{-(p \mp 1)^2}{q} \]
As \( r \) is an integer we have the proof. \( \square \)

So far, we have given necessary and sufficient conditions for the existence of parabolic and elliptic elements in the modular group with given cusp point \( \frac{p}{q} \). Our aim is now to obtain these elements as words in generators. We use the relationships between continued fractions and the Farey graph. Here we give an algorithm for obtaining the word \( W(U, T) \) of the elements mentioned in 3.3 and 3.4. Let the reduced rational \( \frac{p}{q} \) satisfy the condition 3.3 for the elliptic case or 3.4 for the parabolic case.

- Calculate \( \frac{r}{s} \)
- Choose a path from infinity to \( \frac{p}{q} \) in the Farey graph such that the penultimate vertex is \( \frac{r}{s} \)
- Obtain the associated integer continued fraction expansion of \( \frac{p}{q} \).
• Obtain the word \( W(U, T) \).

We explain this process with an example. Consider the rational \( \frac{4}{7} \). One can see that \( \frac{4}{7} \) satisfies the condition 3.3 for trace \(-1\). Hence there exists an elliptic element \( V \) of order 3 in the modular group.

\[
V = \begin{pmatrix} 4 & -3 \\ 7 & -5 \end{pmatrix}
\]

In the first step, we have \( r_{35} = 3 \). In the second step, we need an arbitrary path in the Farey graph from infinity to \( \frac{4}{7} \) such that the penultimate vertex is \( \frac{3}{5} \). It can be seen in Figure 2 that \( \frac{3}{5} \) is the third vertex of the triangle obtained by the Farey sum of \( \frac{1}{2} \) and \( \frac{2}{3} \). The Farey sum of \( \frac{1}{2} \) and \( \frac{3}{5} \) is \( \frac{4}{7} \). Hence we choose the path,

\[
< \infty, 1, \frac{3}{5}, \frac{4}{7} >
\]

Next, we need an integer continued fraction of \( \frac{4}{7} \). We obtain this expansion via the Farey path. The associated integer continued fraction expansion is

\[
\frac{4}{7} = 1 - \frac{1}{3 - \frac{1}{2 - \frac{1}{2}}} = [1, 3, 2, 2]
\]

Finally, we obtain the element \( V \) as a word \( W(U, T) \).

\[
V = \begin{pmatrix} 4 & -3 \\ 7 & -5 \end{pmatrix} = UTU^3TU^2TU^2T
\]

For convenience, throughout this paper, we need to define a function \( \tau_\alpha : \mathbb{Q} \to \mathbb{Q} \) where \( \alpha \) is an integer continued fraction expansion of a fixed rational number \( \frac{a}{b} \). Let \( \alpha = [r_0, r_1, ..., r_n] \), then for all \( x \in \mathbb{Q} \),

\[
\tau_\alpha(x) = \frac{1}{r_n - \frac{1}{r_{n-1} - \frac{1}{... - \frac{1}{r_1 - \frac{1}{r_0 - x}}}}}
\]

It is obvious that if the rationals \( x \) and \( \frac{a}{b} \) are adjacent in the Farey graph then \( \tau_\alpha(x) \) will be an integer. Hence, we can extend every Farey path \( < \infty, ..., \frac{a}{b} > \) to \( < \infty, ..., \frac{a}{b}, x > \). As a result, this process gives us a path from infinity to \( x \) such that the penultimate vertex is \( \frac{a}{b} \). Since every path from infinity to \( \frac{a}{b} \) defines an integer continued fraction expansion of \( \frac{a}{b} \), such an extended path defines an integer continued fraction expansion of \( x \). Here \( \tau_\alpha(x) \) is the last digit of the integer continued fraction expansion of \( x \). We explain this result in the next theorem.

**Theorem 3.5** Let \( \frac{a}{b} \) and \( \frac{c}{d} \) be adjacent rationals and let \( \alpha = [r_0, r_1, ..., r_n] \) be an integer continued fraction expansion of \( \frac{a}{b} \). Then the integer continued fraction expansion of \( \frac{a}{b} \) is:

\[
[r_0, r_1, ..., r_n, \tau_\alpha(\frac{a}{b})]
\]

2756
Proof The integer continued fraction expansion of $\frac{c}{d}$ is associated to the path $<\infty, \ldots, \frac{c}{d}>$, in the Farey graph. Since the rationals $\frac{a}{b}$ and $\frac{c}{d}$ are adjacent in the Farey graph, one can extend this path to $\frac{a}{b}$ as $<\infty, \ldots, \frac{c}{d}, \frac{a}{b}>$. This path represents an integer continued fraction expansion for $\frac{a}{b}$. Hence, we can write,

$$\frac{a}{b} = [r_0, r_1, \ldots, r_n, r_{n+1}]$$

In this equation one can solve $r_{n+1} = \tau_\alpha(\frac{a}{b})$.

We can use this result to obtain an element in the modular group as a word in generators.

**Corollary 3.6** Let $V = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ be an element in the modular group and let $\alpha = [r_0, r_1, \ldots, r_n]$ be an integer continued fraction expansion of the rational $\frac{c}{d}$ then;

$$V = U^{r_0} . T . U^{r_1} . T . \ldots . U^{r_n} . T . U^{\tau_\alpha(\frac{a}{b})} . T$$

**Proof**

If $V = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is an element in $\Gamma$ then $ad - bc = 1$ i.e the rationals $\frac{a}{b}$ and $\frac{c}{d}$ are adjacent in the Farey graph. We need an integer continued fraction expansion of $\frac{c}{d}$ such that the last convergent is $\frac{c}{d}$, to obtain the element $V$ as a word in generators. Such an integer continued fraction expansion is given in Theorem 3.5.

Every element in $\Gamma$ can be expressed as a word of $T$ and $S$ denoted by $W(T, S)$. Consider the blocks;

$$TS = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad TS^2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Using these blocks every reduced word $W(T, S)$ in $\Gamma$ can be expressed as:

$$S^i (TS)^{m_0} (TS^2)^{n_0} \ldots (TS)^{m_k} (TS^2)^{n_k} T^j$$

Here $i = 0, 1, 2, j = 0, 1 \ m_0$ and $n_k$ may be zero and other exponents are positive integers. This representation is known as block reduced form [21]. For example the block reduced form of the word $W(T, S) = T S T S T S T S T S T S T S$ is $(TS)^2 . (TS^2)^2 . T$. Trace classes of the modular group and extended modular group are studied in [21, 22] by using block reduced form. Also relations between cusp points of the modular group and block reduced forms are investigated in [23].

Here we express the elliptic and parabolic elements obtained from Theorem 3.1, 3.2 or 3.4 in block reduced form.

**Theorem 3.7** Let $x = \frac{a}{b}$ be a reduced rational such that one of the conditions 3.3 or 3.4 holds, and $\frac{c}{d}$ be the corresponding rational, calculated from Theorem 3.1, 3.2 or 3.4, to obtain an elliptic or parabolic element in $\Gamma$. If $\frac{c}{d}$ has integer continued fraction expansion $\alpha = [r_0, r_1, \ldots, r_n]$ then the block reduced form of the elliptic or parabolic element $V$ is;

$$V = (TS)^{r_0-1} . TS^2 . (TS)^{r_1-2} . TS^2 . (TS)^{r_2-2} . TS^2 \ldots . (TS)^{r_n-2} . TS^2 . (TS)^{\tau_\alpha(x)-1} . T$$
Proof For a given rational \( x = \frac{p}{q} \) and calculated \( x = \frac{r}{s} \) we have the aforementioned element;

\[
V = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \in \Gamma
\]

Using the integer continued fraction expansion of \( x = \frac{r}{s} \) we obtain this element as a word in generators \( W(U, T) \):

\[
V = U^{\tau_0}.T.U^{\tau_1}.T.\ldots.U^{\tau_n}.T.U^{\tau_0(\frac{p}{q})}.T
\]

(3.5)

Now we consider;

\[
U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = TS
\]

We write \( U = TS \) in 3.5;

\[
V = (TS)^{\tau_0}.T.(TS)^{\tau_1}.T.\ldots.(TS)^{\tau_n}.T.(TS)^{\tau_0(\frac{p}{q})}.T = (TS)^{\tau_0-1}.TS.TS.(TS)^{\tau_1-2}.TS.T.\ldots.TS.(TS)^{\tau_n-2}TS.TS.(TS)^{\tau_0(\frac{p}{q})-1}.T
\]

Since the elliptic generator \( T \) is of order 2, we have the result. \( \square \)

Now we sum up all our results with two examples.

Example 3.8 Consider the rational \( \frac{18}{7} \). By Theorem 3.2 there exists an elliptic element of order 3 in the modular group;

\[
\begin{pmatrix} 18 & -49 \\ 7 & -19 \end{pmatrix}
\]

Now we need an integer continued fraction expansion of \( \frac{49}{19} \). One can obtain this expansion by using the next multiple algorithms or by considering the consecutive vertices of a path from infinity to \( \frac{49}{19} \) in the Farey graph, as convergents of the expansion.

\[
\frac{49}{19} = [3, 3, 2, 3, 2]
\]

Next step we obtain the integer continued fraction expansion of \( \frac{18}{7} \) via the \( \tau \) function where \( \alpha = [3, 3, 2, 3, 2] \)

\[
\tau_\alpha\left(\frac{18}{7}\right) = 1
\]

Hence using Corollary 3.6 we get the elliptic element as

\[
\]

Finally, by Theorem 3.7, we have the block reduced form of this word;

\[
(TS)^2TS^2TS(TS^2)^2TS(TS^2)^2T
\]
Example 3.9 Let the given rational be $\frac{15}{4}$. By Theorem 3.4 we get the parabolic element:

$$
\begin{pmatrix}
15 & -64 \\
4 & -17
\end{pmatrix}
$$

The integer continued fraction expansion of $\frac{64}{17}$ is:

$$
\alpha = [4, 5, 2, 2]
$$

This expansion can be obtained by choosing a path from infinity to $\frac{64}{17}$. Here we use $< \infty, \frac{10}{3}, \frac{34}{9}, \frac{49}{13}, \frac{64}{17}>$. The last digit of the integer continued fraction expansion of $\frac{15}{4}$ is;

$$
\tau_\alpha(\frac{15}{4}) = 1
$$

Hence we obtain a word form of the parabolic element by Corollary 3.6;

$$
$$

Finally, by Theorem 3.7, we have the block reduced form of this word;

$$
(TS)^3.TS^2.(TS)^3.(TS^2)^4.T
$$

4. Conclusion

In this study, we focus on the parabolic and elliptic elements in the modular group. These elements play an important role in describing the algebraic group structure and obtaining the presentation. We give conditions for the existence of such elements in $\Gamma$ with given cusp point. Then we use the Farey graph and continued fractions to find the word form of these elements. We give an algorithm for obtaining elliptic and parabolic elements as words in terms of generators. Finally, we study the block-reduced forms of these elements. For further research one can consider the new block reduced forms defined in [24] to obtain these elliptic and parabolic elements as a product of matrices that have entries as Fibonacci numbers.

Acknowledgment

We would like to thank the anonymous reviewer for valuable comments which have improved our paper. This research received no external funding.

References