Solving the membership problem for certain subgroups of $SL_2(\mathbb{Z})$

Sandie Han, Ariane Masuda, Satyanand Singh, and Johann Thiel

Department of Mathematics, New York City College of Technology

Abstract

For positive integers u and v, let $L_u = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$ and $R_v = \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix}$. Let $G_{u,v}$ be the group generated by L_u and R_v. The membership problem for $G_{u,v}$ asks the following question: given a 2-by-2 matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, is there a relatively straightforward method for determining if M is a member of $G_{u,v}$? In the case where $u = 2$ and $v = 2$, Sanov was able to show that simply checking some divisibility conditions for a, b, c, and d is enough to make this determination. In a previous paper, the authors answered this question by finding a characterization of matrices M in $G_{u,v}$ when $u, v \geq 3$ in terms of the short continued fraction representation of b/d. By modifying our previous work, we are able to extend our previous result to the case where $u, v \geq 2$ with $uv \neq 4$.

Background

For positive integers u and v, let $L_u = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$, $R_v = \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix}$, and $G_{u,v}$ be the group generated by L_u and R_v. Furthermore, using the notation from [1], let

$$\mathscr{G}_{u,v} = \left\{ \begin{bmatrix} 1 + uvn_1 & vn_2 \\ un_3 & 1 + uvn_4 \end{bmatrix} \in SL_2(\mathbb{Z}) \ : \ (n_1, n_2, n_3, n_4) \in \mathbb{Z}^4 \right\}.$$

Note that $\mathscr{G}_{u,v}$ is a group and that $G_{u,v} \subseteq \mathscr{G}_{u,v}$ when $u, v \geq 2$ [2, Proposition 1.1].

Given a rational number q, if there exist integers $q_0, q_1, \ldots, q_r$ (referred to as partial quotients) such that

$$q = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_r}}},$$

then we refer to such an identity as a continued fraction representation of q and denote it by $[q_0, q_1, \ldots, q_r]$. We refer to the unique such representation where $q_i \geq 1$ for $0 < i < r$ and $q_r > 1$ for $r > 0$ as *the* short continued fraction representation of q.

In [1], Esbelin and Gutan gave the following clear characterization of members of $G_{u,v}$ in terms of related continued fraction representations.

Theorem 1 (Esbelin and Gutan [1]) *Suppose that $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathscr{G}_{k,k}$ for some $k \geq 2$. Then $M \in G_{k,k}$ if and only if at least one of the rationals c/a and b/d has a continued fraction expansion having all partial quotients in $k\mathbb{Z}$.*

In [2], we showed that Theorem 1 could be modified and written in terms of the short continued fraction representations of either c/a or b/d, when $u, v \geq 3$. In particular, we developed a simple algorithm that, when applied to the short continued fraction representation of b/d, determines whether or not the sought after continued fraction expansion in Theorem 1 exists.

Preliminaries

Let $A = \bigcup_{r=0}^{\infty} (\mathbb{Z} \times \mathbb{Z}_{\neq 0}^{r})$. We denote an element of A by $\llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket$. Let

$$-\llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket := \llbracket -q_0, -q_1, -q_2, \ldots, -q_r \rrbracket.$$

For any nonnegative integers m and n, let

$$\llbracket q_0, q_1, q_2, \ldots, q_m \rrbracket \oplus \llbracket p_0, p_1, p_2, \ldots, p_n \rrbracket := \begin{cases} \llbracket q_0, q_1, q_2, \ldots, q_m, p_0, p_1, p_2, \ldots, p_n \rrbracket & \text{if } p_0 \neq 0, \\ \llbracket q_0, q_1, q_2, \ldots, q_m + p_1, p_2, \ldots, p_n \rrbracket & \text{otherwise.} \end{cases}$$

Let

$$A_0 = \{ \llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket \in A : [q_i, \ldots, q_r] \neq 0 \text{ when } 0 < i < r \},$$
$$A_1 = \{ \llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket \in A_0 : q_i \geq 1 \text{ when } 0 < i < r, \text{ and } q_r > 1 \text{ when } r > 0 \}, \text{ and}$$
$$A_2 = \{ \llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket \in A_0 : |q_i| > 1 \text{ when } 0 < i \leq r \}.$$

Define the function $C : \mathbb{Q} \to A_1$ by

$$C(x) = \llbracket x_0, x_1, x_2, \ldots, x_r \rrbracket$$

if $[x_0, x_1, x_2, \ldots, x_r]$ is the short continued fraction representation of x. We say that $\llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket \in A$ satisfies the (u, v)-divisibility property if $v | q_i$ when i is even and $u | q_i$ when i is odd.

Define $f_{u,v} : A_1 \to A_2$ recursively by

$$f_{u,v}(\llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket) = \begin{cases} \llbracket q_0 \rrbracket & \text{if } r = 0, \\ \llbracket q_0 + 1, 1 \rrbracket \oplus -f_{v,u}(\llbracket q_2 + 1, q_3, \ldots, q_r \rrbracket) & \text{if } v \nmid q_0 \text{ and } q_1 = 1, \\ \llbracket q_0 + 1 \rrbracket \oplus f_{v,u}(\llbracket -2, q_2 + 1, q_3, \ldots, q_r \rrbracket) & \text{if } v \nmid q_0,\ q_1 = 2, \text{ and } r > 1, \\ \llbracket q_0 + 1, -2 \rrbracket & \text{if } v \nmid q_0,\ q_1 = 2, \text{ and } r = 1, \\ \llbracket q_0 \rrbracket \oplus f_{v,u}(\llbracket q_1, q_2, \ldots, q_r \rrbracket) & \text{otherwise.} \end{cases}$$

Define $g_{u,v} : A_2 \to A_1$ recursively by

$$g_{u,v}(\llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket) = \begin{cases} \llbracket q_0 \rrbracket & \text{if } r = 0, \\ \llbracket q_0 - 1, 1 \rrbracket \oplus g_{v,u}(-\llbracket q_1 + 1, q_2, \ldots, q_r \rrbracket) & \text{if either } q_1 < 0 \text{ and } u \neq 2, \text{ or } q_1 < -2 \text{ and } u = 2, \\ \llbracket q_0 - 1, 2 \rrbracket \oplus g_{v,u}(\llbracket q_2 - 1, q_3, \ldots, q_r \rrbracket) & \text{if } q_1 = -2,\ r > 1, \text{ and } u = 2, \\ \llbracket q_0 - 1, 2 \rrbracket & \text{if } q_1 = -2,\ r = 1, \text{ and } u = 2, \\ \llbracket q_0 \rrbracket \oplus g_{v,u}(\llbracket q_1, q_2, \ldots, q_r \rrbracket) & \text{otherwise.} \end{cases}$$

Results

Proposition 2 *Let $\llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket \in A_2$. If $\llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket$ satisfies the (u, v)-divisibility property, then*

$$f_{u,v}(g_{u',v'}(\llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket)) = \llbracket q_0, q_1, q_2, \ldots, q_r \rrbracket.$$

for any positive integers $u', v' \geq 2$ with $u'v' \neq 4$.

Proposition 3 *For a matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathscr{G}_{u,v}$, $(f_{u,v} \circ C)(c/a)$ satisfies the (v, u)-divisibility property if and only if $(f_{u,v} \circ C)(b/d)$ satisfies the (u, v)-divisibility property.*

Proposition 3 allows us to state our main theorem below in terms of b/d, ignoring c/a altogether.

Theorem 4 *For integers $u, v \geq 2$, with $uv \neq 4$, and a matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathscr{G}_{u,v}$, $M \in G_{u,v}$ if and only if $(f_{u,v} \circ C)(b/d)$ satisfies the (u, v)-divisibility property.*

A careful reading of Theorem 4 shows that our method allows one to determine the exponents in the alternating product representation of M, should it be the case that $M \in G_{u,v}$.

An example

$$\begin{aligned} (f_{2,3} \circ C)\left(\frac{12975}{1351}\right) &= f_{2,3}(\llbracket 9, 1, 1, 1, 1, 9, 2, 2, 5 \rrbracket) \\ &= \llbracket 9 \rrbracket \oplus f_{3,2}(\llbracket 1, 1, 1, 1, 9, 2, 2, 5 \rrbracket) \\ &= \llbracket 9 \rrbracket \oplus (\llbracket 2 \rrbracket \oplus -f_{2,3}(\llbracket 2, 1, 9, 2, 2, 5 \rrbracket)) \\ &= \llbracket 9 \rrbracket \oplus (\llbracket 2 \rrbracket \oplus -(\llbracket 3 \rrbracket \oplus -f_{3,2}(\llbracket 10, 2, 2, 5 \rrbracket))) \\ &= \llbracket 9 \rrbracket \oplus (\llbracket 2 \rrbracket \oplus -(\llbracket 3 \rrbracket \oplus -(\llbracket 10 \rrbracket \oplus f_{2,3}(\llbracket 2, 2, 5 \rrbracket)))) \\ &= \llbracket 9 \rrbracket \oplus (\llbracket 2 \rrbracket \oplus -(\llbracket 3 \rrbracket \oplus -(\llbracket 10 \rrbracket \oplus (\llbracket 3 \rrbracket \oplus \\ &\qquad f_{3,2}(\llbracket -2, 6 \rrbracket))))) \\ &= \llbracket 9 \rrbracket \oplus (\llbracket 2 \rrbracket \oplus -(\llbracket 3 \rrbracket \oplus -(\llbracket 10 \rrbracket \oplus (\llbracket 3, -2 \rrbracket \oplus \\ &\qquad f_{2,3}(\llbracket 6 \rrbracket))))) \\ &= \llbracket 9 \rrbracket \oplus (\llbracket 2 \rrbracket \oplus -(\llbracket 3 \rrbracket \oplus -(\llbracket 10 \rrbracket \oplus (\llbracket 3, -2 \rrbracket \oplus \\ &\qquad \llbracket 6 \rrbracket)))) \\ &= \llbracket 9, 2, -3, 10, 3, -2, 6 \rrbracket, \end{aligned}$$

which does satisfy the $(2, 3)$-divisibility property, as desired, and encodes the exponents in the product representation of $M = \begin{bmatrix} 2401 & 12975 \\ 250 & 1351 \end{bmatrix} = R_3^3 L_2 R_3^{-1} L_2^5 R_3 L_2^{-1} R_3^2$.

References

[1] Henri-Alex Esbelin and Marin Gutan. “On the membership problem for some subgroups of $SL_2(\mathbb{Z})$”. In: *Ann. Math. Qué.* 43.2 (2019), pp. 233–247.

[2] Sandie Han et al. “Subgroups of $SL_2(\mathbb{Z})$ characterized by certain continued fraction representations”. In: *Proc. Amer. Math. Soc.* 148.9 (2020), pp. 3775–3786.