Chin. Ann. of Math.
23B:4(2002),455-460.

CRITERION FOR SL(2,Z)-MATRIX TO BE CONJUGATE TO ITS INVERSE**

LONG Yiming*

Abstract

This paper gives a necessary and sufficient condition for a matrix in $\mathrm{SL}(2,\mathbf{Z})$ to be conjugate to its inverse. This condition reduces the determination of the conjugation to solving some indeterminate equation of second degree. It yields an algorithm to determine this conjugation in finite steps based on the elementary number theory.

Keywords SL(2,Z) matrix, Inverse, Mixed stability
2000 MR Subject Classification 20H05, 11A55, 34D99
Chinese Library Classification O152.3, O156.1, O175.13 **Document Code** A
Article ID 0252-9599(2002)04-0455-06

§1. Main Results

Let $\mathbf{R}$, $\mathbf{Z}$, and $\mathbf{N}$ denote the sets of real, integral, and natural numbers respectively. Let $\mathcal{G}$ be any given group. For any two matrices M and $N \in \mathrm{SL}(n,\mathcal{G})$, as usual M is conjugate to N in $\mathrm{SL}(n,\mathcal{G})$ if $M = P^{-1}NP$ for some $P \in \mathrm{SL}(n,\mathcal{G})$, and we write $M \approx N$ in $\mathrm{SL}(n,\mathcal{G})$. Recently L. Polterovich and Z. Rudnick proved the following interesting Theorem 2 of [5]: A hyperbolic element $h \in \mathrm{SL}(2,\mathbf{Z})$ is stably mixing if and only if it is not conjugate to its inverse in $\mathrm{SL}(2,\mathbf{Z})$, and mentioned that "No complete description of $\mathrm{SL}(2,\mathbf{Z})$-matrices which are conjugate to their inverse is known (cf. [1])". The aim of this short note is to give a necessary and sufficient condition for any matrix in $\mathrm{SL}(2,\mathbf{Z})$ to be conjugate to its inverse in $\mathrm{SL}(2,\mathbf{Z})$ in Theorem 1.1 below. This condition reduces the determination of this conjugation to solving some indeterminate equation of second degree. Then we give more explicit criterions for matrices in $\mathrm{SL}(2,\mathbf{Z})$ which are conjugate to their own inverses based on the elementary number theory in Corollaries 1.1 and 1.2, Theorem 3.1, and Corollary 3.1.

For any $a_1,\cdots,a_n \in \mathbf{Z}$ which are not all zero, as usual we denote their largest common factor by $(a_1,\cdots,a_n)$. Note that $(a_1,\cdots,a_n) = |(a_1,\cdots,a_n)| \geq 1$. We let $(0,\cdots,0) = 1$. Then for any $a_1,\cdots,a_n \in \mathbf{Z}$ and $w \in \{a_1,\cdots,a_n\}$, there is a unique number $\phi_{a_1,\cdots,a_n}(w) \in \mathbf{Z}$ such that

$$w = \phi_{a_1,\cdots,a_n}(w)(a_1,\cdots,a_n). \tag{1.1}$$

Manuscript received September 5, 2001.

*Nankai Institute of Mathematics, Nankai University, Tianjin 300071, China.
E-mail: longym@nankai.edu.cn.

**Project supported by the 973 Program of STM, MCME, RFDP, PMC Key Lab of EM of China, S. S. Chern Foundation, CEC of Tianjin, and Nankai University.

Then we have specially $\phi_{a,b,0}(0)=0$, and $\phi_{0,b,0}(0)=\mathrm{sgn}(b)$ for a and $b\in\mathbf{Z}$, where $\mathrm{sgn}(b)=\pm1$ if $\pm b>0$, and $\mathrm{sgn}(0)=0$. The main result of this paper is:

Theorem 1.1. *Given a matrix*

$$M=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in \mathrm{SL}(2,\mathbf{Z}), \tag{1.2}$$

let $\phi_M(w)=\phi_{a-d,b,c}(w)$ *for* $w\in\{a-d,b,c\}$. *Then* $M\approx M^{-1}$ *in* $\mathrm{SL}(2,\mathbf{Z})$ *if and only if one of the following two cases happens*:

$\langle1\rangle$ $b=c=0$,

$\langle2\rangle$ $b\neq0$ *and the following indeterminate equation of second degree*

$$\phi_M(b)x^2+\phi_M(a-d)xy-\phi_M(c)y^2=-\phi_M(b) \tag{1.3}$$

possesses at least an integer solution (x,y) *satisfying*

$$\phi_M(a-d)x-\phi_M(c)y\in\phi_M(b)\mathbf{Z}. \tag{1.4}$$

Note that in (1.2), we call M the matrix formed by the vector (a,b,c,d).

Next for $M\in\mathrm{SL}(2,\mathbf{Z})$ formed by the vector (a,b,c,d), we give a more explicit criterion to determine whether $M\approx M^{-1}$ in $\mathrm{SL}(2,\mathbf{Z})$. Let

$$A=\phi_M(b),\quad B=\phi_M(a-d),\quad C=-\phi_M(c), \tag{1.5}$$

$$D=B^2-4AC=\phi_M(d-a)^2+4\phi_M(b)\phi_M(c). \tag{1.6}$$

Then the equation (1.3) is equivalent to the following

$$(2Ax+By)^2-Dy^2=-4A^2. \tag{1.7}$$

Corollary 1.1. *For* $M\in\mathrm{SL}(2,\mathbf{Z})$ *formed by a vector* (a,b,c,d) *with* $b\neq0$, *using the above notations, one and only one of the following* 3 *cases must happen*:

$\langle1\rangle$ *If* $D\leq0$, *then* $M\not\approx M^{-1}$ *in* $\mathrm{SL}(2,\mathbf{Z})$.

$\langle2\rangle$ *If* $D=p^2$ *for some integer* $p>0$, *then* $M\approx M^{-1}$ *in* $\mathrm{SL}(2,\mathbf{Z})$ *if and only if there exist* s *and* $t\in\mathbf{Z}$ *such that*

$$st=-4A^2, \tag{1.8}$$

$$s+t\quad\textit{and}\quad\frac{s-t}{p}\in2\mathbf{Z}, \tag{1.9}$$

$$p(s+t)-B(s-t)\ \in\ 4Ap\mathbf{Z}. \tag{1.10}$$

$\langle3\rangle$ *If* $D>0$ *is not a square of any integer, then* $M\approx M^{-1}$ *in* $\mathrm{SL}(2,\mathbf{Z})$ *if and only if the indeterminate equation*

$$u^2-Dy^2=-4A^2 \tag{1.11}$$

possesses an integer solution (u,y) *such that*

$$u-By\in2A\mathbf{Z}. \tag{1.12}$$

Remark 1.1. For the case $\langle3\rangle$, one can determine whether (1.11) possesses an integer solution in finite steps following the method in Section 11.5 in L.-K. Hua's celebrated book [2].

Note that when $|\phi_M(b)|=1$, we have $b\neq0$ and (1.4) always holds. Thus Theorem 1.1 yields:

Corollary 1.2. *Given a matrix* M *formed by a vector* (a,b,c,d) *with* $|\phi_M(b)|=1$, *then* $M\approx M^{-1}$ *in* $\mathrm{SL}(2,\mathbf{Z})$ *if and only if the following indeterminate equation of second degree*

$$x^2+\mathrm{sgn}(b)\phi_M(a-d)xy-\mathrm{sgn}(b)\phi_M(c)y^2=-1 \tag{1.13}$$

possesses at least an integer solution (x,y).

Above results are proved in Section 2. It is well known that symmetric $\mathrm{SL}(2,\mathbf{Z})$ matrices are conjugate to their inverses. In Section 3, we exhibit two infinite families of asymmetric $\mathrm{SL}(2,\mathbf{Z})$ matrices which are or are not conjugate to their inverses.

§2. Proofs

Proof of Theorem 1.1. Fix a matrix $M \in \mathrm{SL}(2,\mathbf{Z})$ formed by a vector (a,b,c,d) as in (1.2). We need to solve for the matrix $Q \in \mathrm{SL}(2,\mathbf{R})$ formed by the vector $q=(q_1,q_2,q_3,q_4)$ from the nonlinear system in Q:

$$Q^{-1}MQ = M^{-1}.$$

Instead of doing so, we study the following equivalent linear system in Q:

$$MQM - Q = 0. \tag{2.1}$$

Because $ad-bc = \det M = 1$, the system (2.1) becomes

$$Kq = 0, \tag{2.2}$$

where the coefficient matrix K is given by

$$K = \begin{pmatrix} a^2-1 & ac & ab & bc \\ ab & ad-1 & b^2 & bd \\ ac & c^2 & ad-1 & cd \\ bc & cd & bd & d^2-1 \end{pmatrix} = \begin{pmatrix} a^2-1 & ac & ab & bc \\ ab & bc & b^2 & bd \\ ac & c^2 & bc & cd \\ bc & cd & bd & d^2-1 \end{pmatrix}. \tag{2.3}$$

Because

$$\det K = 0, \tag{2.4}$$

the system (2.2) is always solvable on the field $\mathbf{R}$.

For the conjugation in $\mathrm{SL}(2,\mathbf{Z})$, we consider three cases.

Case 1. $b \neq 0$.

In this case, by direct computation the solution space S of (2.2) is given by $S = \mathrm{span}\{\xi,\eta\}$ with

$$\xi = \Big(0, -\frac{c}{b}, 1, 0\Big)^T, \quad \eta = \Big(-1, \frac{a-d}{b}, 0, 1\Big)^T, \tag{2.5}$$

where q^T denotes the transpose of q. Then $M \approx M^{-1}$ if and only if there exist α and $\beta \in \mathbf{Z}$ such that

$$\psi \equiv \alpha\xi^T + \beta\eta^T = \Big(-\beta, -\alpha\frac{c}{b} + \beta\frac{a-d}{b}, \alpha, \beta\Big) \tag{2.6}$$

forms a matrix Ψ in $\mathrm{SL}(2,\mathbf{Z})$, i.e., $\psi \in \mathbf{Z}^4$ and $\det\Psi = 1$. That is,

$$\frac{c}{b}\alpha^2 - \frac{a-d}{b}\alpha\beta - \beta^2 = 1, \tag{2.7}$$

$$\frac{c}{b}\alpha - \frac{a-d}{b}\beta \in \mathbf{Z}. \tag{2.8}$$

Then solving the system (2.7),(2.8) for α and $\beta \in \mathbf{Z}$ is equivalent to solving the indeterminate equation (1.3) for x and $y \in \mathbf{Z}$ satisfying (1.4) by using the largest common factor $(a-d,b,c)$.

Case 2. $b = 0$ and $c \neq 0$.

In this case, there must hold $a = d = 1$ or $a = d = -1$. Thus K in (2.3) becomes

$$K = \begin{pmatrix} 0 & ac & 0 & 0 \\ 0 & 0 & 0 & 0 \\ ac & c^2 & 0 & ac \\ 0 & ac & 0 & 0 \end{pmatrix}. \tag{2.9}$$

Then the solution space S of (2.2) is given by $S = \{\alpha(0,0,1,0)^T + \beta(-1,0,0,1)^T \mid \alpha, \beta \in \mathbf{R}\}$. Because the matrix Ψ formed by $\psi = (-\beta, 0, \alpha, \beta)$ satisfies $\det \Psi = -\beta^2 < 1$, in this case $M \not\approx M^{-1}$ in $\mathrm{SL}(2, \mathbf{Z})$.

Case 3. $b = c = 0$.

In this case, there must hold $a = d = 1$ or $a = d = -1$. Then there holds $M \approx M^{-1} = M$ in $\mathrm{SL}(2, \mathbf{Z})$.

Thus Theorem 1.1 holds.

Proof of Corollary 1.1. Fix M by (1.2). We study each case separately.

$\langle 1 \rangle$ Note that the equation (1.3) is equivalent to the equation (1.7). Then $b \neq 0$ implies that the right hand side of (1.7) is strictly negative, and $D \leq 0$ implies that the left hand side of (1.7) is non-negative. This contradiction proves that (1.7) possesses no integer solution, and then (1.3) has no integer solutions. Thus $\langle 1 \rangle$ holds.

$\langle 2 \rangle$ Rewrite the equivalent equation (1.7) of (1.3) into

$$(2Ax + By - py)(2Ax + By + py) = -4A^2. \tag{2.10}$$

Then this equation has integer solution (x, y) if and only if conditions (1.8)–(1.10) hold. Thus $\langle 2 \rangle$ holds.

$\langle 3 \rangle$ follows from the fact that (1.3) possesses an integer solution if and only if (1.11) and (1.12) hold.

The proof is complete.

§3. Asymmetry and Conjugation to Inverses

To illustrate our above results, we give following examples.

Example 3.1 (**Symmetric implies $M \approx M^{-1}$ in** $\mathrm{SL}(2, \mathbf{Z})$). Suppose $M \in \mathrm{SL}(2, \mathbf{Z})$ formed by the vector $(a, b, c, d)^T$ via (1.2) is symmetric, i.e., $b = c$, then $\phi_M(b) = \phi_M(c)$. Then (1.3) has an integer solution $(x, y) = (0, 1)$ satisfying (1.4). Thus as well-known $M \approx M^{-1}$ in $\mathrm{SL}(2, \mathbf{Z})$.

Example 3.2 (**Asymmetric $M \not\approx M^{-1}$ in $\mathrm{SL}(2, \mathbf{Z})$**).

Example 3.2.1. The matrix $M = \begin{pmatrix} 6 & -5 \\ 5 & -4 \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z})$ is formed by the vector $(a, b, c, d) = (6, -5, 5, -4)$. Then $\phi_M(b) = -\phi_M(c) = -1$ and $\phi_M(a - d) = 2$. Thus $D = 0$. Then $M \not\approx M^{-1}$ in $\mathrm{SL}(2, \mathbf{Z})$ by $\langle 1 \rangle$ of Corollary 1.1.

Example 3.2.2. Note that the example $M = \begin{pmatrix} 4 & 9 \\ 7 & 16 \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z})$ formed by $(a, b, c, d) = (4, 9, 7, 16)$ given by [5] is asymmetric, and possesses $(a - d, b, c) = 1$, $\phi_M(b) = 9$, $\phi_M(c) = 7$, $\phi_M(a - d) = -12$. Thus (1.3)–(1.4) become

$$9x^2 - 12xy - 7y^2 = -9, \tag{3.1}$$

$$12x + 9y \in 7\mathbf{Z}. \tag{3.2}$$

Let $u = 3x - 2y$. (3.1) becomes

$$u^2 - 11y^2 = -9. \tag{3.3}$$

Consider the indeterminate equation in m:

$$m^2 = 11 + 9h \quad \text{for } 0 \leq h \leq \left[\frac{(9/2)^2}{9}\right] = 2. \tag{3.4}$$

Then for $h = 0, 1, 2$, (3.4) possesses no integer solutions. By the study in §11.5 of [2], (3.3) and then (3.1) has no integer solutions. Thus $M \not\approx M^{-1}$ in $\mathrm{SL}(2, \mathbf{Z})$ as claimed in [5] by a different method.

Example 3.2.3. By our Theorem 1.1, it is easy to construct infinitely many asymmetric matrices $M \not\approx M^{-1}$ in $\mathrm{SL}(2,\mathbf{Z})$. For example, let $M = \begin{pmatrix} a & 1 \\ a^2-1 & a \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z})$ with $a \in \mathbf{N}$ and $a \geq 2$. Then $c = a^2 - 1 \geq 3$, $(a-d, b, c) = (0, 1, c) = 1$, $\phi_M(b) = 1$, $\phi_M(c) = c$, $\phi_M(a-d) = 0$. The equation (1.3) becomes

$$x^2 - cy^2 = -1. \tag{3.5}$$

One can show that the continued fraction expansion of $\sqrt{c}$ is $\sqrt{c} = \sqrt{a^2-1} = \langle a - 1, \overline{1, 2a-2}\rangle$ (cf. Exercise 7 on p.359 of [4]) and thus it has period 2. Then by Theorem 1 of §7.6 of [4] or Theorem 7.25 of [3], the equation (3.5) possesses no integer solutions. Thus by Corollary 1.2, we obtain $M \not\approx M^{-1}$ in $\mathrm{SL}(2,\mathbf{Z})$.

Because of these examples, a natural question is whether every asymmetric matrix $M \in \mathrm{SL}(2,\mathbf{Z})$ is not conjugate to its inverse in $\mathrm{SL}(2,\mathbf{Z})$. Our following results answer this question negatively. We write $a|b$ for $a, b \in \mathbf{Z}$ if $b = ac$ for some $c \in \mathbf{Z}$. For M formed by a vector (a, b, c, d) we denote

$$E \equiv \frac{\phi_M(a-d)^2}{4} + \mathrm{sgn}(b)\phi_M(c). \tag{3.6}$$

Theorem 3.1. *Given a matrix M formed by a vector (a, b, c, d) satisfying $|\phi_M(b)| = 1$ and $2|\phi_M(a-d)$, then $M \approx M^{-1}$ in $\mathrm{SL}(2,\mathbf{Z})$ if and only if either $E = 1$, or $E > 0$ is not a square of any integer and the period m of the continued fraction*

$$\sqrt{E} = \langle a_0, \cdots, a_n, \overline{a_{n+1}, \cdots, a_{n+m-1}}\rangle$$

is odd.

Proof. Because $|\phi_M(b)| = 1$, the condition (1.4) always holds, and the equation (1.3) becomes

$$x^2 + \mathrm{sgn}(b)\phi_M(a-d)xy - \mathrm{sgn}(b)\phi_M(c)y^2 = -1. \tag{3.7}$$

Because $2|\phi_M(a-d)$, the indeterminate equation (3.7) is equivalent to the following indeterminate equation

$$\left(x + \frac{\mathrm{sgn}(b)\phi_M(a-d)}{2}y\right)^2 - Ey^2 = -1. \tag{3.8}$$

We continue our study in three cases.

Case 1. $E \leq 0$.

In this case, (3.8) has no integer solution at all. Thus $M \not\approx M^{-1}$ in $\mathrm{SL}(2,\mathbf{Z})$.

Case 2. $E = p^2$ for some $p \in \mathbf{N}$.

In this case, (3.8) becomes

$$u^2 - (py)^2 = -1, \tag{3.9}$$

where $u = x + \frac{\mathrm{sgn}(b)\phi_M(a-d)}{2}y$. This implies $u = 0$ and $p^2y^2 = 1$. Specially this implies $p^2 = 1$. Therefore $M \not\approx M^{-1}$ in $\mathrm{SL}(2,\mathbf{Z})$ if $E = p^2 > 1$.

When $p^2 = 1$, (3.9) has solutions $(u, y) = (0, 1)$ and $(0, -1)$. From the definition of u, we obtain $x = u - \frac{\mathrm{sgn}(b)\phi_M(a-d)}{2}y \in \mathbf{Z}$. Thus (3.8) has at least an integer solution (x, y). This proves $M \approx M^{-1}$ in $\mathrm{SL}(2,\mathbf{Z})$.

Case 3. $E \in \mathbf{N} \setminus \{1\}$ is not a square of any integer.

In this case, (3.8) becomes

$$u^2 - Ey^2 = -1, \tag{3.10}$$

$$x = u - \frac{\mathrm{sgn}(b)\phi_M(a-d)}{2}y. \tag{3.11}$$

Denote by m the period of the continued fraction $\sqrt{E} = \langle a_0, \cdots, a_n, \overline{a_{n+1}, \cdots, a_{n+m-1}} \rangle$. Then by Theorem 1 of §7.6 of [4] or Theorem 7.25 of [3], the equation (3.10) possesses at least an integer solution (x, y) if and only if m is odd.

The proof is thus complete.

Corollary 3.1. *There exist infinitely many asymmetric matrices $M \in \mathrm{SL}(2, \mathbf{Z})$ satisfying $M \approx M^{-1}$ in $\mathrm{SL}(2, \mathbf{Z})$.*

Proof. We construct infinitely many such matrices by Theorem 3.1 as follows.

Firstly, we choose an integer $E > 4$ such that $E \neq p^2$ for any integer $p > 0$ and that the period m of the continued fraction representation of $\sqrt{E}$ is odd. For example, we can take $E = 73$ by the study in §7.6 of [4].

By Theorem 1 of §7.6 of [4] or Theorem 7.25 of [3], the indeterminate equation

$$u^2 - Eb^2 = 1 \tag{3.12}$$

possesses infinitely many integer solutions (u_i, b_i) for $i \in \mathbf{N}$. Define

$$M_i = \begin{pmatrix} u_i + 2b_i & b_i \\ (E-4)b_i & u_i - 2b_i \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z}) \tag{3.13}$$

for $i \in \mathbf{N}$. Then $\det M_i = u_i^2 - 4b_i^2 - (E-4)b_i^2 = u_i^2 - Eb_i^2 = 1$, i.e., $M_i \in \mathrm{SL}(2, \mathbf{Z})$ for $i \in \mathbf{N}$.

Secondly, fix any $i \in \mathbf{N}$. (1.4) always holds in this case. (1.3) becomes

$$x^2 + 4xy - (E-4)y^2 = -1. \tag{3.14}$$

The x defined by (3.11) is always an integer. Thus (3.14) is equivalent to (3.10). Because E is not a square of any integer and the continued fraction of $\sqrt{E}$ possesses an odd period, (3.10) possesses integer solutions by Theorem 1 of §7.6 of [4] or Theorem 7.25 of [3]. This proves $M_i \approx M_i^{-1}$ in $\mathrm{SL}(2, \mathbf{Z})$.

In the above construction, there are infinitely many ways to choose mutually different E's and (u_i, b_i)'s. Thus the conclusion of Corollary 3.1 holds.

Acknowledgements. The author would like to thank Professor Leonid Polterovich for providing to him the preprint [5] and interesting discussions with him. This paper was completed during the author's visits to the Mathematisches Forschungsinstitut Oberwolfach in July and the Pacific Institute for the Mathematical Sciences at UBC in August of 2001. The author would like to thank Professors H. Hofer, J. P. Yocooz, E. Zehnder, and N. Ghoussoub, M. Esteban, P. Rabinowitz for their invitations, and both of the institutes for their hospitalities.

References

[1] Baake, M. & Roberts, J., Reversing symmetry group of $Gl(2, \mathbf{Z})$ and $PGl(2, \mathbf{Z})$ matrices with connection to cat maps and trace maps [J], *J.Phys. A Math. Gen.,* **30m**(1997), 1549–1573.

[2] Hua, L. K., Introduction to number theory [M], Science Press, Beijing (Chinese Edition), 1957, Springer, Berlin (English Edition), 1982.

[3] Niven, I., Zuckerman, H. S. & Montgomery, H. L., An introduction to the theory of numbers [M], 5th ed. John Wiley & Sons, Inc. New York 1991.

[4] Pan, C. & Pan, C., Elementary number theory [M], Peking University Press, Beijing (Chinese Edition), 1992.

[5] Polterovich, L. & Rudnick, Z., Stable mixing for cat maps and quasi-morphisms of the modular group [R], Preprint, 2000.