The Similarity Problem for 3×3 Integer Matrices

Harry Appelgate and Hironori Onishi
Department of Mathematics
City College of New York
138th Street and Convent Avenue
New York, New York 10031

Submitted by Richard A. Brualdi

ABSTRACT

Using results from the similarity problem of 2×2 integer matrices, we derive an algorithm for the solution of the similarity problem for 3×3 integer matrices.

1.

The conjugacy problem in SL(n, Z) and related arithmetic groups was solved recently by Grunewald [5]. Grunewald and Segal [6] solved the conjugacy problem for a wider class of groups. Their method is powerful, but complicated mathematically and computationally. In our previous paper [1], we presented a very straightforward and efficient algorithm for the conjugacy problem in SL(2, Z) by means of the simple continued fraction algorithm. In this paper we describe a simple algorithm which solves the conjugacy problem in SL(3, Z). Our method is restricted to 3×3 matrices but is quite simple and is not obtained by specializing Grunewald's algorithm to the case $n=3$.

2.

Actually what we solve is the similarity problem for 3×3 integer matrices: given two 3×3 integer matrices A and B, decide if $A \sim B$ or not, i.e. if there exists $R \in \mathrm{GL}(3, Z)$ such that $RAR^{-1}=B$. Since $\det(-I)=-1$, we can always make sure that $R \in \mathrm{SL}(3, Z)$. Thus the conjugacy problem in SL(3, Z) is a special case of the similarity problem.

52 Vanderbilt Ave., New York, NY 10017 0024-3795/82/010159+16$02.75

3.

Let A and B be 3×3 integer matrices. If the characteristic polynomials of A and B are different, then $A \nsim B$. Given a monic polynomial $f(t)\in Z[t]$ of degree 3, let $S(f)$ denote the set of all 3×3 integer matrices having $f(t)$ as characteristic polynomial. We assume, then, that A and B are in $S(f)$ for some $f(t)$.

4.

First suppose that $f(t)$ is irreducible (over Q). Take a zero λ of $f(t)$ and put $K=Q(\lambda)$. Let X be an eigenvector of A belonging to λ with components in K. The components of X are linearly independent over Q. Let U be the Z-module in K generated by the components of X. Let V be the Z-module obtained from B in a similar way. The Lattimer–MacDuffee theorem [7, p. 53] says that $A\sim B$ iff $U\sim V$, i.e. iff there is $\gamma\in K^X$ such that $\gamma U=V$. Now, as remarked in [4, p. 128], there is a decision procedure for the similarity problem of full modules in an algebraic number field. This solves the similarity problem in $S(f)$ in case $f(t)$ is irreducible.

5.

The decision procedure for the similarity of modules is not restricted to the case $n=3$; it works for any n. However, it is very tedious and involves much unnecessary computation. For $n=2$, much computation can be avoided by the use of continued fractions. In a separate paper [2], we describe a procedure which generalizes Berwick's method [3]. This procedure resembles the continued fraction algorithm in the sense that it generates a "graphically" periodic expansion of a module. In [2] we shall give examples as applied to the similarity problem of matrices. In any case, the existence of a decision procedure in case $f(t)$ is irreducible is established.

6.

We now consider the case when $f(t)$ is reducible, $n=3$. Take $e\in Z$ such that $f(e)=0$. Given $A\in S(f)$, by Theorem III.12 of [7], one can effectively find $R \in GL(3, Z)$ such that

$$RAR^{-1} = \begin{pmatrix} e & a \\ 0 & A_2 \end{pmatrix},$$

where A_2 is 2×2 and $a=(a_1, a_2)$. Briefly, this may be done as follows. Find a 3×1 integer vector X such that $AX=eX$. We may assume X is primitive, i.e. that the gcd of its components is 1. Then find $R \in GL(3, Z)$ such that $RX=(1,0,0)^T$. RAR^{-1} will have the desired form.

7.

If $f(t)=(t-e_1)(t-e_2)(t-e_3)$, $e_i \in Z$, then we can effectively find $R \in GL(3, Z)$ such that

$$RAR^{-1} = \begin{pmatrix} e_1 & a_1 & a_2 \\ 0 & e_2 & a_3 \\ 0 & 0 & e_3 \end{pmatrix}.$$

Again, this is a special case of Theorem III.12 of [7]. Briefly, with A_2 as in Section 6, find $R_2 \in GL(2, Z)$ such that

$$R_2 A_2 R_2^{-1} = \begin{pmatrix} e_2 & a_3 \\ 0 & e_3 \end{pmatrix}.$$

Then

$$R = \begin{pmatrix} 1 & 0 \\ 0 & R_2 \end{pmatrix}.$$

8.

We now take care of the special case $f(t)=(t-e)^3$. We may assume that $A \neq eI$. By Section 7 we may assume that

$$A = \begin{pmatrix} e & a_1 & a_2 \\ 0 & e & a_3 \\ 0 & 0 & e \end{pmatrix}.$$

9.

LEMMA. *If $a_1a_3=0$ in the matrix A of Section 8, i.e. if $A-eI$ has* rank 1, *then we can effectively find $R\in GL(3,\mathbf{Z})$ such that*

$$RAR^{-1}=\begin{pmatrix} e & 0 & d\\ 0 & e & 0\\ 0 & 0 & e\end{pmatrix},\qquad d>0.$$

Proof. If $a_1=0$, then let $d=\gcd(a_2,a_3)$ and find $R_2\in \mathrm{GL}(2,\mathbf{Z})$ such that

$$R_2(a_2,a_3)^T=(d,0)^T.$$

Then with $a'=(a_2,a_3)^T$,

$$\begin{pmatrix} R_2 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix} eI_2 & a'\\ 0 & e\end{pmatrix}\begin{pmatrix} R_2 & 0\\ 0 & 1\end{pmatrix}^{-1}$$

has the desired form. If $a_3=0$, then let $d=\gcd(a_1,a_2)$ and find $R_2\in \mathrm{GL}(2,\mathbf{Z})$ such that

$$(a_1,a_2)R_2^{-1}=(0,d).$$

Then with $a=(a_1,a_2)$,

$$\begin{pmatrix} 1 & 0\\ 0 & R_2\end{pmatrix}\begin{pmatrix} e & a\\ 0 & eI_2\end{pmatrix}\begin{pmatrix} 1 & 0\\ 0 & R_2\end{pmatrix}^{-1}$$

has the desired form. ■

10.

It is clear that two matrices of the form in Section 9 are similar over Z iff they are identical.

11.

LEMMA. *In the matrix A of Section* 8, *if* $a_1 a_3 \neq 0$, *i.e.* $A - eI$ *has* rank 2, *then we can effectively find* $R \in GL(3, Z)$ *such that* RAR^{-1} *has the same form but satisfies the extra conditions that*

$$a_1 > 0, \qquad a_3 > 0, \quad \textit{and} \quad 0 \leqslant a_2 < \gcd(a_1, a_3).$$

Proof. Choosing a suitable diagonal matrix $R = \operatorname{diag}(\pm 1, 1, \pm 1)$, we can make a_1 and a_3 positive. Let $d = \gcd(a_1, a_3)$, put $a_2 = qd + r$, $0 \leqslant r < d$, and find x and $y \in Z$ such that $a_1 x - a_3 y = qd$. Then with

$$R = \begin{pmatrix} 1 & y & 0 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix},$$

we have

$$RAR^{-1} = \begin{pmatrix} e & a_1 & r \\ 0 & e & a_3 \\ 0 & 0 & e \end{pmatrix}. \qquad \blacksquare$$

12.

LEMMA. *Two matrices of the form in Section* 8 *satisfying the extra conditions in Section* 11 *are similar over* Z *iff they are identical.*

Proof. Let A and B be such matrices, and suppose $RA = BR$ for some $R \in GL(3, Z)$. Then with $E_1 = (1,0,0)^T$, $BRE_1 = RAE_1 = eRE_1$. Since $B - eI$ has rank 2, $RE_1 = u_1 E_1$ for some $u_1 \in Z$. Thus the first column of R is $(u_1, 0, 0)^T$ and $u_1 = \pm 1$. Next, considering the left eigenvector $(0,0,1)$ of B belonging to e, we get that the last row of R is $(0, 0, u_3)$ with $u_3 = \pm 1$. Thus R is upper triangular and the diagonal entries u_1, u_2, u_3 are ± 1. Put

$$R = \begin{pmatrix} u_1 & x_1 & x_2 \\ 0 & u_2 & x_3 \\ 0 & 0 & u_3 \end{pmatrix}.$$

Then the equality $RA=BR$ is equivalent to the equalities

$$u_1a_1=u_2b_1, \qquad u_2a_3=u_3b_3,$$

$$u_1a_2+a_3x_1=b_1x_3+u_3b_2.$$

Since a_1, b_1, a_3, b_3 are positive, $u_1=u_2=u_3=u$. Thus $a_1=b_1$ and $a_3=b_3$, and also $u(a_2-b_2)=a_1x_3-a_3x_1$. Since $u=\pm 1$, $d=\gcd(a_1, a_3)$ divides a_2-b_2 and hence $a_2=b_2$. ■

13.

In the rest we assume that $f(t)=(t-e)g(t)$ and $g(e)\neq 0$. [If $g(e)=0$ but $f(t)\neq(t-e)^3$, then use the other zero of $g(t)$ for e.] $g(t)$ may or may not be reducible. We can deal with both cases simultaneously. However, we need some results from the case $n=2$. They are:

(i) Given 2×2 matrices A and B over Z, we can effectively decide if $A\sim B$.

(ii) In case $A\sim B$, we can effectively find $R\in \mathrm{GL}(2, \mathrm{Z})$ such that $RAR^{-1}=B$.

(iii) Given a 2×2 matrix A over Z other than a scalar matrix, we can effectively find $A_1\in \mathrm{GL}(2, \mathrm{Z})$ such that A_1 and $-I$ generate the centralizer

$$\mathrm{Z}(A)=\{R\in \mathrm{GL}(2, \mathrm{Z})|RA=AR\}.$$

14.

These results for $n=2$ are worked out in [1]. However, some remarks are in order, especially about (iii), and also because in that paper the given matrix A is in $\mathrm{SL}(2, \mathrm{Z})$, while now A is an arbitrary 2×2 integer matrix. Let $g(t)=t^2-\tau t+\delta$, where τ and δ are in Z. Let $A\in S(g)$, but A not a scalar matrix.

15.

If $g(t)=(t-e)^2$, $e \in Z$, then we can effectively find $R \in GL(2, Z)$ such that

$$RAR^{-1}=\begin{pmatrix} e & a \\ 0 & e \end{pmatrix}, \qquad a>0.$$

Two matrices of the form on the right above are similar iff they are identical. The centralizer of such a matrix is generated by $-I$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

16.

If $g(t)=(t-e_1)(t-e_2)$, $e_1 \neq e_2$, integers, then we can effectively find $R \in GL(2, Z)$ such that

$$RAR^{-1}=\begin{pmatrix} e_1 & a \\ 0 & e_2 \end{pmatrix}, \qquad 0 \leqslant a \leqslant \frac{|e_1-e_2|}{2}.$$

Two matrices of the form on the right are similar over Z iff they are identical. The centralizer of such a matrix is generated by

(a) $-I$ if $0 \leqslant 2a < |e_1-e_2|$;

(b) $-I$ and $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ if $2a=e_1-e_2>0$;

(c) $-I$ and $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ if $2a=e_2-e_1>0$.

17.

Assume $g(t)$ is irreducible. Let $\lambda=(\tau+\sqrt{\Delta})/2$, $\Delta=\tau^2-4\delta$. Given

$$A=\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in S(g),$$

let $\varphi(A)=(\lambda-d)/b$; $(\varphi(A),1)^T$ is an eigenvector of A belonging to λ. Then the map φ is one-to-one on $S(g)$ and $\varphi(RAR^{-1})=R\cdot\varphi(A)$ for any $R \in GL(2, Z)$ (cf. (1), (2), (3) of [1]). Let $\alpha=\varphi(A) \in Q(\lambda)$, and consider the module $U=\langle\alpha,1\rangle$ and its coefficient ring O_U. We have the isomorphism between $Z(A)$ and O_U^X determined by

$$B(\alpha,1)^T=\varepsilon(\alpha,1)^T, \qquad B\in Z(A), \quad \varepsilon\in O_U^X.$$

18.

Suppose $\Delta<0$ in Section 17. Then $\alpha=\varphi(A)$ is a complex number, and we know (i) and (ii) of Section 13 as explained in (4) of [1]. As for (iii), O_U^X is a finite cyclic group. Pick a generator of O_U^X, and pick a corresponding $A_1\in Z(A)$.

19.

Suppose $\Delta>0$ in Section 17. Then we know (i) and (ii), as explained in (5) and (8) of [1]. (iii) is implicit in (12) of [1]. Let $\alpha=\varphi(A)$, and

$$\alpha=\left[q_1,\ldots,q_k,\overline{q_{k+1},\ldots,q_m}\right]$$

be the continued fraction of α. For $n>0$ let

$$A_n=\begin{pmatrix} q_1 & 1\\ 1 & 0\end{pmatrix}\cdots\begin{pmatrix} q_n & 1\\ 1 & 0\end{pmatrix}$$

Then $Z(A)$ is generated by $-I$ and $A_mA_k^{-1}$.

20.

Now that the results (i), (ii), and (iii) of Section 13 have been clarified, we can continue with the discussion started there. Let A and B be in $S(f)$. We may assume that

$$A=\begin{pmatrix} e & a\\ 0 & A_2\end{pmatrix} \quad\text{and}\quad B=\begin{pmatrix} e & b\\ 0 & B_2\end{pmatrix}.$$

Decide if $A_2\sim B_2$ over Z. If $A_2\nsim B_2$ then $A\nsim B$. In fact, if $RA=BR$ for some

$R\in GL(3, Z)$, then R is of the form

$$\begin{pmatrix} u & r \\ 0 & R_2 \end{pmatrix}$$

and $R_2A_2=B_2R_2$. In the rest we assume that $A_2\sim B_2$. Find $R_2\in GL(2, Z)$ such that $R_2A_2R_2^{-1}=B_2$. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & R_2 \end{pmatrix}^{-1}\begin{pmatrix} e & b \\ 0 & B_2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & R_2 \end{pmatrix}=\begin{pmatrix} e & bR_2 \\ 0 & A_2 \end{pmatrix}.$$

Thus we may assume that $A_2=B_2$. Let $g(t)=t^2-\tau t+\delta$, which is the characteristic polynomial of A_2.

21.

Suppose that $A_2=cI$. Considering $A-cI$, we may assume that $A_2=0$.

LEMMA. *If*

$$A=\begin{pmatrix} e & a \\ 0 & 0 \end{pmatrix},$$

we can effectively find $R\in GL(3, Z)$ *such that*

$$RAR^{-1}=\begin{pmatrix} e & 0 & d \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

where d *is a (positive) divisor of* e. *Two matrices of this form are similar iff they are identical.*

Proof. If $a=0$, then

$$R=\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{gives} \quad \begin{pmatrix} e & 0 & e \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Suppose $a=(a_1, a_2)\neq 0$. Let $c=\gcd(a_1, a_2)$, and find $R_2\in GL(2, Z)$ such that

$$(a_1, a_2)R_2^{-1} = (0, c).$$

Then

$$R = \begin{pmatrix} 1 & 0 \\ 0 & R_2 \end{pmatrix} \quad \text{gives} \quad \begin{pmatrix} e & 0 & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Now let $d = \gcd(e, c)$, and put $e = e_1 d$, $c = c_1 d$. Find x, y in Z such that $e_1 x + c_1 y = 1$. Then find u, v in Z such that $uy - ve_1 = 1$. Then we check that

$$\begin{pmatrix} e & 0 & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & -c_1 & x \\ 0 & u & v \\ 0 & e_1 & y \end{pmatrix} = \begin{pmatrix} 1 & -c_1 & x \\ 0 & u & v \\ 0 & e_1 & y \end{pmatrix} \begin{pmatrix} e & 0 & d \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \quad \blacksquare$$

22.

Now assume that A_2 is not a scalar matrix. Let

$$m = e\tau - e^2 - \delta \quad \text{and} \quad A_0 = A_2 - (\tau - e)I_2.$$

Since $g(e) \neq 0$, we get that $m \neq 0$ and A_0 is nonsingular. Let

$$A = \begin{pmatrix} e & a \\ 0 & A_2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} e & b \\ 0 & A_2 \end{pmatrix}.$$

LEMMA. *$A \sim B$ iff there is $R_2 \in Z(A_2)$ and $u = \pm 1$ such that*

$$bA_0 R_2 \equiv uaA_0 \pmod{m}. \qquad (1)$$

REMARK. Since $Z(A_2)$ is generated by A_1 modulo $\pm I$, and we can effectively find A_1, and A_1 has finite multiplicative order mod m, the congruence (1) can be checked in a finite number of steps.

Proof of lemma. Suppose $RA=BR$ for some $R\in GL(3, Z)$. Then R is of the form

$$R=\begin{pmatrix} u & r \\ 0 & R_2 \end{pmatrix},$$

and the equality $RA=BR$ says that $R_2\in Z(A_2)$ and

$$ua+rA_2=er+bR_2. \tag{2}$$

Write (2) as $bR_2-ua=r(A_2-eI_2)$. Since A_0 is nonsingular, this is equivalent to

$$bR_2A_0-uaA_0=r(A_2-eI_2)A_0.$$

Since $R_2A_2=A_2R_2$ and $(A_2-eI_2)A_0=mI_2$, this is equivalent to

$$bA_0R_2-uaA_0=mr, \tag{3}$$

which implies the congruence (1). Conversely, suppose that the congruence (1) holds for some $R_2\in Z(A_2)$ and $u=\pm 1$. Then define a vector r by (3). This gives the desired R. ∎

23.

EXAMPLE.

$$A=\begin{pmatrix} -15 & -3 & 7 \\ 38 & 8 & -16 \\ -17 & -3 & 10 \end{pmatrix}, \qquad B=\begin{pmatrix} 9 & 9 & 7 \\ -3 & -10 & -3 \\ 2 & 30 & 4 \end{pmatrix}.$$

A and B have the same characteristic polynomial

$$f(t)=(t-2)(t^2-t+7).$$

Using the eigenvalue 2, we get the first reduction

$$R_1AR_1^{-1}=\begin{pmatrix}2&-3&7\\0&5&-9\\0&3&-4\end{pmatrix}\qquad\text{with}\quad R_1=\begin{pmatrix}1&0&0\\1&1&0\\-2&0&1\end{pmatrix},$$

$$R_2BR_2^{-1}=\begin{pmatrix}2&9&7\\0&-10&-3\\0&39&11\end{pmatrix}\qquad\text{with}\quad R_2=\begin{pmatrix}1&0&0\\0&1&0\\1&0&1\end{pmatrix}.$$

$g(t)=t^2-t+7$ is the characteristic polynomial of

$$A_2=\begin{pmatrix}5&-9\\3&-4\end{pmatrix}\quad\text{and}\quad B_2=\begin{pmatrix}-10&-3\\39&11\end{pmatrix}.$$

$\lambda=(1+i3\sqrt{3})/2$ is a zero of $g(t)$. In terms of $\rho=(1+i\sqrt{3})/2$, a primitive 6th root of unity, we have $\lambda=3\rho-1$. Then

$$\alpha=\varphi(A_2)=\frac{\lambda+4}{3}=\rho+1,$$

$$\beta=\varphi(B_2)=\frac{\lambda-11}{39}=\frac{\rho-4}{13}.$$

Since $-1/\beta=-13/(\rho-4)=\rho+3=\alpha+2$,

$$\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}1&2\\0&1\end{pmatrix}=\begin{pmatrix}0&-1\\1&2\end{pmatrix}$$

sends α to β. Thus $A_2\sim B_2$ and

$$\begin{pmatrix}0&-1\\1&2\end{pmatrix}A_2\begin{pmatrix}2&1\\-1&0\end{pmatrix}=B_2.$$

Hence

$$R_3^{-1}(R_2BR_2^{-1})R_3=\begin{pmatrix}2&7&5\\0&5&-9\\0&3&-4\end{pmatrix},\qquad R_3=\begin{pmatrix}1&0&0\\0&0&-1\\0&1&2\end{pmatrix}.$$

Since $U=\langle\alpha,1\rangle=\langle\rho,1\rangle=O_K$, then $K=Q(\lambda)=Q(\rho)$, $O_U^X=\langle\rho\rangle$. We have

$$A_1(\alpha,1)^T=\rho(\alpha,1)^T,\qquad A_1=\begin{pmatrix}2&-3\\1&-1\end{pmatrix}.$$

Thus A_1 generates $Z(A_2)$ and

$$A_1^2=\begin{pmatrix}1&-3\\1&-2\end{pmatrix},\qquad A_1^3=-I.$$

We now check the congruence (1). First note that

$$m=-9\quad\text{and}\quad A_0=A_2+I_2=\begin{pmatrix}6&-9\\3&-3\end{pmatrix}=3A_1.$$

So the congruence (1) is

$$(7,5)3A_1A_1^n\equiv\pm(-3,7)3A_1 \pmod 9),$$

which is equivalent to

$$(1,-1)A_1^n\equiv(0,\pm1) \pmod 3).$$

$n=2$ is a solution. Thus $A\sim B$. To find

$$R_4=\begin{pmatrix}u&r\\0&A_1^2\end{pmatrix}$$

in GL(3, Z) such that

$$R_4\begin{pmatrix}2&-3&7\\0&5&-9\\0&3&-4\end{pmatrix}R_4^{-1}=\begin{pmatrix}2&7&5\\0&5&-9\\0&3&-4\end{pmatrix},$$

we have to find $u=\pm1$ and r such that

$$(7,5)3A_1A_1^2-u(-3,7)3A_1=-9r.$$

$u=-1$ and $r=(2,1)$ is a solution. Thus

$$R_4=\begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & -3 \\ 0 & 1 & -2 \end{pmatrix}.$$

Altogether we have

$$R_4R_1AR_1^{-1}R_4^{-1}=R_3^{-1}R_2BR_2^{-1}R_3.$$

Thus $RAR^{-1}=B$ with

$$R=\begin{pmatrix} -1 & 2 & 1 \\ -5 & -1 & 2 \\ 18 & 1 & -8 \end{pmatrix}.$$

24.

EXAMPLE.

$$A=\begin{pmatrix} 12 & 7 & 8 \\ 107 & -8 & 29 \\ 73 & -50 & -7 \end{pmatrix}, \qquad B=\begin{pmatrix} 64 & 140 & 23 \\ -19 & -59 & 2 \\ -41 & -103 & -8 \end{pmatrix}.$$

A and B have the same characteristic polynomial

$$f(t)=(t-2)(t^2+5t+3).$$

Using the eigenvalue 2, we get the first reduction

$$R_1AR_1^{-1}=\begin{pmatrix} 2 & 7 & 8 \\ 0 & -22 & 13 \\ 0 & -29 & 17 \end{pmatrix}, \qquad R_1=\begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix},$$

$$R_2BR_2^{-1}=\begin{pmatrix} 2 & 19 & -2 \\ 0 & 7 & 29 \\ 0 & -3 & -12 \end{pmatrix}, \qquad R_2=\begin{pmatrix} 0 & -1 & 0 \\ 1 & 3 & 0 \\ 0 & -2 & 1 \end{pmatrix},$$

$$A_2=\begin{pmatrix} -22 & 13 \\ -29 & 17 \end{pmatrix}, \qquad B_2=\begin{pmatrix} 7 & 29 \\ -3 & -12 \end{pmatrix}.$$

$g(t)=t^2+5t+3$ is the characteristic polynomial of A_2 and B_2, and

$$\lambda=\frac{-5+\sqrt{13}}{2},$$

$$\alpha=\varphi(A_2)=\frac{39-\sqrt{13}}{58},$$

$$\beta=\varphi(B_2)=-\frac{19+\sqrt{13}}{6}.$$

Computing the continued fractions for α and $\gamma=-\beta$, we get that $\alpha\sim\beta$ and hence $A_2\sim B_2$. In fact $\begin{pmatrix}-3 & 1\\ 2 & -1\end{pmatrix}$ maps α to β, and hence

$$\begin{pmatrix}-3 & 1\\ 2 & -1\end{pmatrix}A_2\begin{pmatrix}-3 & 1\\ 2 & -1\end{pmatrix}^{-1}=B_2.$$

This gives

$$\begin{pmatrix}1 & 0 & 0\\ 0 & -1 & -1\\ 0 & -2 & -3\end{pmatrix}\begin{pmatrix}2 & 19 & -2\\ 0 & 7 & 29\\ 0 & -3 & -12\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & -3 & 1\\ 0 & 2 & -1\end{pmatrix}=\begin{pmatrix}2 & -61 & 21\\ 0 & -22 & 13\\ 0 & -29 & 17\end{pmatrix}.$$

With $a=(7,8)$ and $b=(-61,21)$ we have to check the congruence (1). $m=-17$ and

$$A_0=A_2+7I_2\equiv\begin{pmatrix}2 & -4\\ 5 & 7\end{pmatrix}\pmod{17}.$$

The centralizer $Z(A_2)$ is generated by $\pm I$ and

$$C=\begin{pmatrix}-18 & 13\\ -29 & 21\end{pmatrix},$$

which corresponds to $(3+\sqrt{13})/2$. Computing C^n mod 17, we get $C^8\equiv -I_2$ (mod 17) and $aA_0\equiv(3,-6)$ (mod 17). Next compute bA_0C^n mod 17 for $n=0,1,\ldots,7$. We get $(7,0)$, $(-7,6)$, $(3,1)$, $(2,-8)$, $(-8,-6)$, $(-5,8)$, $(-6,1)$, $(-6,-6)$. Since none of these is congruent to $\pm(3,-6)$ (mod 17), we conclude that $A\nsim B$.

REFERENCES

1 H. Appelgate and H. Onishi, Continued fractions and the conjugacy problem in SL(2, Z), *Comm. Algebra* 9(11):1121–1130 (1981).
2 H. Appelgate and H. Onishi, Periodic expansion of module and its relation to units, *J. Number Theory*, to appear.
3 W. E. H. Berwick, The classification of ideal numbers that depend on a cubic irrationality, *Proc. London Math. Soc.* 12:343–429 (1913).
4 Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic, New York, 1966.
5 F. Grunewald, Solution of the conjugacy problem in certain arithmetic groups, in *Word Problems II* (S. I. Adian, W. W. Boone, and G. Higman, Eds.), North-Holland, 1979.
6 F. Grunewald and D. Segal, The solubility of certain decision problems in arithmetic and algebra, *Bull. Amer. Math. Soc.* 1:915–918 (1979).
7 M. Newman, *Integral Matrices*, Academic, New York, 1972.

Received 9 February 1981; revised 15 May 1981