PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 87, Number 2, February 1983

SIMILARITY PROBLEM OVER $SL(n, Z_p)$

H. APPELGATE AND H. ONISHI

ABSTRACT. The question of conjugacy separability in $SL(n, Z)$ leads to the conjugacy problem in $SL(n, Z_p)$ for various primes p. We present a simple solution to the similarity problem over $SL(n, Z_p)$, which solves the conjugacy problem as a special case.

(1) In [**10**] Stebe gives a pair of 2×2 irreducible integer matrices A and B of determinant 1 satisfying the following two conditions.

(i) A and B are not conjugate in $GL(2, Z)$.

(ii) For every integer $m > 1$, there exists a 2×2 integer matrix X such that $AX \equiv XB \pmod{m}$ and $\det X \equiv 1 \pmod{m}$.

He used them to prove that $GL(n, Z)$ and $SL(n, Z)$ are not conjugacy separable for $n > 2$. It is easily seen that the condition (ii) is equivalent to the condition

(iii) For every prime p, A and B are conjugate in $SL(2, Z_p)$, where Z_p denotes the ring of p-adic integers.

(2) It is well known that the conjugacy problem in $GL(2, Z)$ and in $SL(2, Z)$ has a solution. For example, see [**8**, p. 214]. For an efficient algorithm, see [**1**]. Recently Grunewald [**5**] solved the conjugacy problem in $SL(n, Z)$ for any $n \geq 2$. See [**6**] for a more general result. For $n = 3$, see [**2**]. Now turning to the condition (iii) we encounter the conjugacy problem in $SL(2, Z_p)$, and more generally, in $SL(n, Z_p)$. Despite the fact that $SL(n, Z_p)$ is uncountable, there is a surprisingly simple solution to the conjugacy problem in $SL(n, Z_p)$. In this paper we shall present such a solution.

(3) Actually what we solve is the similarity problem over $SL(n, Z_p)$, i.e., given two $n \times n$ matrices A and B over Z_p, decide in a finite number of steps if there exists X in $SL(n, Z_p)$ such that $AX = XB$. Slightly more generally, we can replace Z_p by the ring $\mathcal{O}$ of integers of any locally compact nonarchimedian field F. Let π be a prime element of F. Given a square matrix C over $\mathcal{O}$, consider its invariant factors

$$(\pi^{\nu_1}, \dots, \pi^{\nu_r}, 0, \dots, 0)$$

and let $\mu = \mu(C) = \nu_r$; note that $r = \operatorname{rank} C$ and $0 \leq \nu_1 \leq \cdots \leq \nu_r$.

(4) LEMMA. *Let C be a square matrix over $\mathcal{O}$ and let b be a column vector over $\mathcal{O}$ such that $C\xi = b$ for some column vector ξ over F. If there is a column vector x' over $\mathcal{O}$ such that*

$$Cx' \equiv b \pmod{\pi^{\mu+\lambda}},$$

where $\mu = \mu(C)$ and λ is a rational integer ≥ 0, then there is a column vector x over $\mathcal{O}$ such that

$$Cx = b \quad \textit{and} \quad x \equiv x' \pmod{\pi^{\lambda}}.$$

Received by the editors June 17, 1981.
1980 *Mathematics Subject Classification*. Primary 15A36; Secondary 10C20.

PROOF. Take P and Q in $GL(n, \mathcal{O})$ such that

$$PCQ = D = \mathrm{diag}(\pi^{\nu_1}, \ldots, \pi^{\nu_r}, 0, \ldots, 0).$$

Let $c = Pb$ and $\eta = Q^{-1}\xi$. Then $D\eta = c$ and hence

$$c = (c_1, \ldots, c_r, 0, \ldots, 0)^T,$$

where $c_i \in \mathcal{O}$. Let $y' = Q^{-1}x'$. Then

$$Dy' \equiv c \pmod{\pi^{\mu+\lambda}}.$$

This says that

$$\pi^{\nu_i} y_i' \equiv c_i \pmod{\pi^{\mu+\lambda}} \quad \text{for } 1 \le i \le r.$$

Since $\nu_i \le \mu + \lambda$, π^{ν_i} divides c_i. Put

$$y_i = c_i \pi^{-\nu_i} \in \mathcal{O} \quad \text{for } 1 \le i \le r.$$

Since $\pi^{\nu_i} y_i \equiv \pi^{\nu_i} y_i' \pmod{\pi^{\mu+\lambda}}$ and $\nu_i \le \mu$,

$$y_i \equiv y_i' \pmod{\pi^{\lambda}}.$$

Let $y = (y_1, \ldots, y_r, 0, \ldots, 0)^T$ and $x = Qy$. Since $Dy = c$, $Cx = b$. Since $y \equiv y' \pmod{\pi^\lambda}$, $x \equiv x' \pmod{\pi^\lambda}$.

(5) Given two $n \times n$ matrices A and B over $\mathcal{O}$, consider the $n^2 \times n^2$ matrix C which represents the linear transformation $X \mapsto AX - XB$ on the vector space of $n \times n$ matrices over F (with respect to the natural basis) and let $\mu = \mu(C) = \mu(A, B)$.

(6) Given an integer $n > 1$, we know that there is an integer $\lambda > 0$ such that given $x \in \mathcal{O}^\times$ (the units of $\mathcal{O}$), if $x \equiv 1 \pmod{\pi^\lambda}$, then there exists $u \in \mathcal{O}^\times$ such that $x = u^n$ and such an exponent λ can be effectively found; for example, $\lambda = 1 + 2\nu_F(n)$ will do, where ν_F is the order function on F. See [**7**, p. 42].

(7) THEOREM. *Let A and B be $n \times n$ matrices over $\mathcal{O}$. If there is an $n \times n$ matrix X' over $\mathcal{O}$ such that*

$$AX' \equiv X'B \pmod{\pi^{\mu+\lambda}} \quad \text{and} \quad \det X' \equiv 1 \pmod{\pi^\lambda},$$

where $\mu = \mu(A, B)$ as in (5) *and λ is as in* (6), *then there exists $X \in SL(n, \mathcal{O})$ such that $AX = XB$.*

PROOF. By Lemma (4), there is an $n \times n$ matrix X over $\mathcal{O}$ such that

$$AX = XB \quad \text{and} \quad X \equiv X' \pmod{\pi^\lambda}.$$

Since $\det X' \equiv 1 \pmod{\pi^\lambda}$, $\det X \equiv 1 \pmod{\pi^\lambda}$. Thus by (6), there exists $u \in \mathcal{O}^\times$ such that $u^n = \det X$. Let $Y = u^{-1}X$. Then

$$AY = YB \quad \text{and} \quad \det Y = u^{-n} \det X = 1.$$

(8) Theorem (7) solves the similarity problem over $SL(n, \mathcal{O})$; compute μ and λ and decide if there is an $n \times n$ matrix X over $\mathcal{O}$ such that

$$AX \equiv XB \pmod{\pi^{\mu+\lambda}} \quad \text{and} \quad \det X \equiv 1 \pmod{\pi^\lambda}.$$

Since the residue ring $\mathcal{O}/(\pi^\nu)$ is finite, these conditions can be checked in a finite number of steps.

(9) In the rest we look at some special cases of interest. Given a monic polynomial $f(t)$ over $\mathcal{O}$ of degree n, let $S(f)$ denote the set of $n \times n$ matrices over $\mathcal{O}$ whose characteristic polynomial is $f(t)$. Write $A \sim B$ to mean that A and B are similar over $SL(n, \mathcal{O})$.

(10) LEMMA. *Let $A \in S(f)$. If $f = f_1 f_2$ over $\mathcal{O}$ and* g.c.d.$(f_1, f_2) \equiv 1 \pmod{\pi}$, *then we can find $A_1 \in S(f_1)$ and $A_2 \in S(f_2)$ such that*

$$A \sim \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

PROOF. Since $f = f_1 f_2$, we can find $A_1 \in S(f_1)$ and $A_2 \in S(f_2)$ such that

$$A \sim \begin{pmatrix} A_1 & B \\ 0 & A_2 \end{pmatrix}$$

for some B (cf. Theorem III.12, in [**9**]). Since g.c.d.$(f_1, f_2) \equiv 1 \pmod{\pi}$, the linear transformation $X \mapsto A_1 X - X A_2$ is nonsingular mod π. Thus $\mu(A_1, A_2) = 0$ and for any B, there is an X' over $\mathcal{O}$ such that

$$A_1 X' - X' A_2 \equiv B \pmod{\pi}.$$

Since the linear transformation $X \mapsto A_1 X - X A_2$ is nonsingular over F, there is an X over F such that $A_1 X - X A_2 = B$. Thus by Lemma (4), there is an X over $\mathcal{O}$ such that $A_1 X - X A_2 = B$. (This can be proved more directly by induction on the exponent of modulus π^ν.) With this X,

$$\begin{pmatrix} A_1 & B \\ 0 & A_2 \end{pmatrix} \begin{pmatrix} I_1 & X \\ 0 & I_2 \end{pmatrix} = \begin{pmatrix} I_1 & X \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

(11) THEOREM. *Let Δ be the discriminant of $f(t)$. If $\Delta \not\equiv 0 \pmod{\pi}$, then any two matrices in $S(f)$ are similar over $SL(n, \mathcal{O})$.*

PROOF. First suppose that f is irreducible mod π. Let λ be an eigenvalue of $A \in S(f)$ and let $K = F(\lambda)$. Since $\Delta \not\equiv 0 \pmod{\pi}$, K/F is an unramified extension and $\mathcal{O}_K = \mathcal{O}[\lambda]$ and $N\mathcal{O}_K^\times = \mathcal{O}^\times$, where N is the norm $K \to F$. (See [**7**, p. 50].) Let Y be an eigenvector of A belonging to λ with components in $\mathcal{O}_K$ and $Y \not\equiv 0 \pmod{\pi_K}$, where π_K is a prime element of K. Put $Y = B\Lambda$, where $\Lambda = (1, \lambda, \ldots, \lambda^{n-1})^T$ and B is an $n \times n$ matrix over $\mathcal{O}$. Since Y is an eigenvector of $A \bmod \pi_K$ belonging to λ, the components of Y are linearly independent mod π_K and hence $\det B \not\equiv 0 \pmod{\pi}$. Take $\xi \in \mathcal{O}_K^\times$ such that $N\xi = \det B^{-1} \Delta^{-1}$ and let $X = T(\xi Y)$, where T is the trace $K \to F$. Consider the $n \times n$ matrix $R = (X, AX, \ldots, A^{n-1}X)$ over $\mathcal{O}$. We have $AR = RC$, where C is the companion matrix of f. On the other hand,

$$\begin{aligned} \det R &= \det(T(\xi Y), T(\xi A Y), \ldots, T(\xi A^{n-1} Y)) \\ &= \det(T(\xi Y), T(\xi \lambda Y), \ldots, T(\xi \lambda^{n-1} Y)) \\ &= N\xi \det(\Lambda_1, \ldots, \Lambda_n) \det(Y_1, \ldots, Y_n), \end{aligned}$$

where the subscripts $1, \ldots, n$ denote the conjugates over F. Since

$$\det(Y_1, \ldots, Y_n) = \det B \det(\Lambda_1, \ldots, \Lambda_n)$$

and $\det(\Lambda_1, \ldots, \Lambda_n)^2 = \Delta$, we get that $\det R = N\xi \cdot \det B \cdot \Delta = 1$.

Now suppose that f is reducible mod π. Since $\Delta \not\equiv 0 \pmod{\pi}$, f is separable mod π and hence by Hensel's Lemma, f is reducible over $\mathcal{O}$. Let $f = f_1 f_2$ be a nontrivial factorization over $\mathcal{O}$. Then g.c.d.$(f_1, f_2) \equiv 1 \,(\mathrm{mod}\,\pi)$. Thus by Lemma (10),

$$A \sim \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

for some $A_1 \in S(f_1)$ and $A_2 \in S(f_2)$. By induction, $A_i \sim C_i$, where C_i is the companion matrix of f_i. Thus

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \sim \begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix} \sim C.$$

We have shown that every A in $S(f)$ is similar to the companion matrix C of f.

(12) Given A and B in $S(f)$, in deciding if $A \sim B$, we may assume that neither is a scalar matrix. If A is a scalar $\mathrm{mod}\,\pi$, i.e., $A = e_1 I + \pi A_1$, then unless B is also the same scalar $\mathrm{mod}\,\pi$, $A \not\sim B$. If $B = e_1 I + \pi B_1$, then $A \sim B$ if and only if $A_1 \sim B_1$. Since A is not a scalar matrix, there is an integer $\nu \geq 0$ such that $A = e_\nu I + \pi^\nu A_\nu$ and A_ν is not a scalar $\mathrm{mod}\,\pi$. In this way we can reduce the problem to the case when neither A nor B is a scalar $\mathrm{mod}\,\pi$.

(13) Let us look at the case when $n = 2$ and $\mathcal{O} = Z_p$. In this case Theorem (7) specializes to the following: Given A and B in $S(f)$ neither of which is a scalar $\mathrm{mod}\,p$, if there is a 2×2 matrix X over Z_p such that

$$AX \equiv XB \quad \text{and} \quad \det X \equiv 1 \quad (\mathrm{mod}\,p)\,\text{or}\,(\mathrm{mod}\,8)$$

$(\mathrm{mod}\,8$ if $p = 2)$, then $A \sim B$.

PROOF. In view of Theorem (11), we may assume that $\Delta \equiv 0 \,(\mathrm{mod}\,p)$. Let

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

If $a_2 \equiv a_3 \equiv 0 \,(\mathrm{mod}\,p)$, then since $\Delta \equiv 0 \,(\mathrm{mod}\,p)$, $a_1 \equiv a_4 \,(\mathrm{mod}\,p)$ and A is a scalar $\mathrm{mod}\,p$. Thus $a_2 \not\equiv 0$ or $a_3 \not\equiv 0 \,(\mathrm{mod}\,p)$. Likewise $b_2 \not\equiv 0$ or $b_3 \not\equiv 0 \,(\mathrm{mod}\,p)$. Thus we get that $\mu(A, B) = 0$. On the other hand, $\lambda = 1$ if $p \neq 2$ and $\lambda = 3$ if $p = 2$.

(14) Suppose that $\Delta \equiv 0 \,(\mathrm{mod}\,p)$ and let A and B be as in (13). Conjugating by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, we may assume that $a_3 b_3 \not\equiv 0 \,(\mathrm{mod}\,p)$. For $p \neq 2$, the condition that $AX \equiv XB$ and $\det X \equiv 1 \,(\mathrm{mod}\,p)$ for some integer matrix X amounts to that $a_3 b_3$ is a square $\mathrm{mod}\,p$. Thus $A \sim B$ if and only if $a_3 b_3$ is a square $\mathrm{mod}\,p$.

(15) Suppose that $p = 2$ in (14). In this case $\Delta = 4\Delta_1$ for some $\Delta_1 \in Z_p$ and we verify that the condition that $AX \equiv XB$ and $\det X \equiv 1 \,(\mathrm{mod}\,8)$ for some integer matrix X amounts to that the congruence equation

$$x^2 - \Delta_1 y^2 \equiv a_3 b_3 \,(\mathrm{mod}\,8)$$

is solvable in integers. It is easily verified that the residues mod 8 of the form $x^2 - \Delta_1 y^2$ are

$$\begin{array}{lll} 1, 3, 5, 7 & \text{if } \Delta_1 \equiv 1, 5 & (\mathrm{mod}\,8), \\ 1, 5 & \text{if } \Delta_1 \equiv 3, 7, 4 & (\mathrm{mod}\,8), \\ 1 & \text{if } \Delta_1 \equiv 0 & (\mathrm{mod}\,8), \\ 1, 7 & \text{if } \Delta_1 \equiv 2 & (\mathrm{mod}\,8), \\ 1, 3 & \text{if } \Delta_1 \equiv 6 & (\mathrm{mod}\,8). \end{array}$$

(16) Consider the case when A and B are matrices over the rational integers, assumed to have the same characteristic polynomial $f(t)$ with the discriminant Δ. Let R be the semilocal ring of rational fractions whose denominators are coprime to Δ. Assume that neither A nor B is a scalar mod any prime factor p of Δ. In this case we can show that $A \sim B$ over $SL(2, Z_p)$ for every prime p (dividing Δ, in view of Theorem (11)) if and only if $A \sim B$ over $SL(2, R)$.

PROOF. Since $R \subset Z_p$ for every p dividing Δ, the sufficiency is trivial. With A and B as in (13), let

$$h(x) = a_3x^2 - ex - a_2, \qquad e = a_1 - a_4.$$

For any p dividing Δ, since A is not a scalar mod p, $h(x) \not\equiv 0 \pmod p$ and hence $h(x_p) \not\equiv 0 \pmod p$ for some rational integer x_p. Choose a rational integer x such that $x \equiv x_p \pmod p$ for every p dividing Δ. Then $(h(x), \Delta) = 1$. Since

$$\begin{pmatrix} 0 & 1 \\ -1 & x \end{pmatrix}\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\begin{pmatrix} x & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_4 + a_3x & -a_3 \\ h(x) & a_1 - a_3x \end{pmatrix},$$

we may assume that $(a_3, \Delta) = 1$. Similarly, $(b_3, \Delta) = 1$. If $\Delta < 0$, make sure that $a_3b_3 > 0$. Note that $\Delta = e^2 + 4a_2a_3$. Consider the equation

$$x^2 - \Delta y^2 = 4a_3b_3. \tag{1}$$

$A \sim B$ over $SL(2, Z_p)$ if and only if equation (1) has a solution in Z_p. $A \sim B$ over $SL(2, R)$ if and only if equation (1) has a solution in R. In case Δ is even, (1) can be replaced by the equation

$$x^2 - \Delta_1 y^2 = a_3b_3,$$

where $\Delta = 4\Delta_1$. In view of this, the necessity follows from the following result due to Dirichlet (cf. [**4**, §§156–157]. Also [**3**, p. 423]): let b and c be nonzero integers, not both negative and $(b, c) = 1$. If b is a square mod c and c is a square mod b, then there are nonzero integers x, y and z such that

$$x^2 = by^2 + cz^2, \quad (y, c) = 1, \quad (z, b) = 1.$$

(17) EXAMPLE. For $f(t) = t^2 - 20t + 1$, $S(f)$ consists of five distinct conjugacy classes of $GL(2, Z)$ and of ten distinct conjugacy classes of $SL(2, Z)$. They are represented by

$$\begin{pmatrix} 19 & 18 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 19 & 9 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 19 & 6 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 18 & 7 \\ 5 & 2 \end{pmatrix}, \begin{pmatrix} 17 & 10 \\ 5 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 19 & 1 \\ 18 & 1 \end{pmatrix}, \begin{pmatrix} 19 & 2 \\ 9 & 1 \end{pmatrix}, \begin{pmatrix} 19 & 3 \\ 6 & 1 \end{pmatrix}, \begin{pmatrix} 17 & 5 \\ 10 & 3 \end{pmatrix}, \begin{pmatrix} 18 & 5 \\ 7 & 2 \end{pmatrix}.$$

The two matrices in each column are conjugate in $GL(2, Z)$. Now look at the two pairs

$$\begin{pmatrix} 19 & 18 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 19 & 2 \\ 9 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 18 & 7 \\ 5 & 2 \end{pmatrix}, \begin{pmatrix} 17 & 10 \\ 5 & 3 \end{pmatrix}$$

(or their transposes). $\Delta = 4 \cdot 9 \cdot 11$. By the criterions given in (14) and (15), we see that the two matrices in each pair are similar over $SL(2, Z_p)$ for $p = 2, 3$ and 11, and hence for all p. It turns out that in $SL(2, Z)$, 20 is the least nonnegative trace for which such an example exists.

(18) EXAMPLE. Let R be the semilocal ring of rational fractions whose denominators are coprime to 2, 3 and 11. Consider the pair $\left(\begin{smallmatrix}19&18\\1&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}19&2\\9&1\end{smallmatrix}\right)$ given in (17). The polynomial $h(x)$ in (16) for the second matrix is $h(x)=9x^2-18x-2$. $h(3)=25$ is coprime to Δ. Thus

$$\begin{pmatrix}19&2\\9&1\end{pmatrix}\begin{pmatrix}3&-1\\1&0\end{pmatrix}=\begin{pmatrix}3&-1\\1&0\end{pmatrix}\begin{pmatrix}28&-9\\25&-8\end{pmatrix}.$$

The quadratic equation in (16) for the pair $\left(\begin{smallmatrix}19&18\\1&1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}28&-9\\25&-8\end{smallmatrix}\right)$ is $x^2-99y^2=25$. This has an easy solution $(5,0)$. This gives the matrix

$$X=\begin{pmatrix}5&-9/5\\0&1/5\end{pmatrix}\in SL(2,R)$$

such that $AX=XB$ and hence we get that

$$\begin{pmatrix}19&18\\1&1\end{pmatrix}\begin{pmatrix}9/5&-2/5\\-1/5&3/5\end{pmatrix}=\begin{pmatrix}9/5&-2/5\\-1/5&3/5\end{pmatrix}\begin{pmatrix}19&2\\9&1\end{pmatrix}.$$

REFERENCES

1. H. Appelgate and H. Onishi, *Continued fractions and the conjugacy problem in $SL_2(Z)$*, Comm. Algebra **9** (1981), 1121–1130.
2. ——, *The similarity problem for* 3×3 *integer matrices*, Linear Algebra Appl. **42** (1982), 159–174.
3. L. Dickson, *History of the theory of numbers*, Vol. II, Chelsea, New York, 1966.
4. P. Dirichlet, *Vorlesungen über Zahlentheorie*, Chelsea, New York, 1968.
5. F. Grunewald, *Solution of the conjugacy problem in certain arithmetic groups*, Word Problems II, Eds., S. Adjan, W. Boone and G. Higman, North-Holland, Amsterdam, 1979.
6. F. Grunewald and D. Segal, *The solubility of certain decision problems in arithmetic and algebra*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), 915–918.
7. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.
8. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory*, Pure and Applied Math., Vol. XIII, Interscience, New York, 1966.
9. M. Newman, *Integral matrices*, Academic Press, New York, 1972.
10. P. Stebe, *Conjugacy separability of groups of integer matrices*, Proc. Amer. Math. Soc. **32** (1972), 1–7.

DEPARTMENT OF MATHEMATICS, CITY COLLEGE, CITY UNIVERSITY OF NEW YORK, NEW YORK, NEW YORK 10031