Honors 1
MATH 541: Abstract Algebra 1
Spring 2023

HONGTAO ZHANG, YIBO WU

Lemma 1. *a,b,c,d are coprime.*

Proof. Assume they are not coprime, without loss of generality, let $\gcd(a, c) = k$

$$(ad - bc) = k(ld - nb) = 1 \implies k = 1$$

$\square$

We can tackle this problem by utilizing the algorithm of finding a matrix inverse. To find a matrix inverse, we can use the following algorithm:

1. Do row operation to make the matrix into an upper triangular matrix.
2. Do row operation to make the matrix into an identity matrix.
3. The inverse of the original matrix is the matrix we get from the elementary row operation matrix product.

If we can represent all the row operation needed to reduce $S \in SL_2(\mathbb{Z})$ to I, then we can represent S^{-1} as $E^0E^1E^2...E^n$, where E^i is the elementary row operation matrix, which means we can reproduce S.

Then if we can represent the elementary row operation matrix we need to reduce S to I as a composition of A, B, we can find S^{-1} by composition of A, B, which means we can reproduce S with A, B.

There are four types of E, which is

$$E_1 = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}, \quad E_2 = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}, \quad E_3 = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}, \quad E_4 = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$$

Lemma 2. *Row operation for adding $k \in \mathbb{Z}$ times the bottom row to the top row can be represented as A^k. (i.e. E_1)*

Proof. Proof by induction:

Base case is trivial so left as an exercise to reader.

Inductive Step: Given $A^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$, we have $A^{k+1} = A \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}$ $\square$

Lemma 3. *Row operation for adding $k \in \mathbb{Z}$ times the top row to the bottom row by k can be represented as $B^3A^{-k}B$. (i.e. E_2)*

Proof.

$$\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : B \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -c & -d \\ a & b \end{bmatrix}$$

By Lemma 2, After A^{-k}, it becomes $\begin{bmatrix} -c-ka & -d-kb \\ a & b \end{bmatrix}$

$$\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : B^3 \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ -a & -b \end{bmatrix}$$

Then we can get E_2 by composition of $B^3 A^{-k} B$

□

Theorem 1. *Nontrivial (i.e. $a \neq 1$) E_3, E_4 is not possible in $SL_2(\mathbb{Z})$.*

Proof. If we have E_3, E_4, we will change the determinant of the matrix by a, which means the space is not closed.

□

Theorem 2. *We can reduce any matrix in $SL_2(\mathbb{Z})$ to I by using E_1, E_2*

Proof. By lemma 1, we know that a, b, c, d are coprime.

Therefore, $\gcd(a, c) = 1$.

If we do row operation following the Euclidean algorithm, we are guaranteed to reduce a, c to be 1. Then, if we do one more time, we can make c to be 0.

The operation will be $\max(a, c) = \max(a, c) - \min(a, c)$.

We know that $ad - bc = 1$, with $c = 0, a = 1$, we can get $d = 1$.

Therefore, by subtracting the bottom row from the top row the remaining b times, we can get I. □

Therefore, we can reduce S to I, which means A, B can formulate S^{-1} by multiplication and inversion, which by one more inverse, we can get S.

Examples

1: Find the inverse of the following matrix.

$$C = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

The first step is to reduce 1 bottom row from the top row by multiplying A^{-1}

$$A^{-1}C = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

Then apply $B^3 AB$

$$B^3 ABA^{-1}C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Then we can remove the 1 times the bottom row from the top row by multiplying A^{-1}

$$A^{-1}B^3ABA^{-1}C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore, the inverse of C is $A^{-1}B^3ABA^{-1}$.
which means $C = (A^{-1}B^3ABA^{-1})^{-1}$.

2:

$$D = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

We just need to let the second row subtract first row once.

$$B^3ABD = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Then $B^3AB = D^{-1} \implies (B^3AB)^{-1} = D$

3:

$$E = \begin{bmatrix} 3 & 5 \\ 4 & 7 \end{bmatrix}$$

First we will let the second row subtract the first row once.

$$B^3ABE = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$$

Then we will let the first row subtract the second row twice.

$$A^{-2}B^3ABE = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

Then we will let the second row subtract the first row once.

$$B^3ABA^{-2}B^3ABE = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Then we will let the first row subtract the second row once.

$$A^{-1}B^3ABA^{-2}B^3ABE = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore, $E = (A^{-1}B^3ABA^{-2}B^3AB)^{-1}$

□