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.

We know that I can be written as A^0, 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 $A^0A^1A^2...A^n$, where A^i is the elementary row operation matrix, which means we can reproduce S.

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

Proof. Proof is trivial so left as an exercise to the reader. $\square$

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

Proof.

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

through matrix multiplication

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

which means

$$B^{-3}A^{-k}B\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ ak+c & bk+d \end{bmatrix}$$

$\square$

Then what we need to show is we can reduce to I without scaling multiplication of a row.

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.

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.

$\square$