The Euclidean Algorithm and $S\ell(2,\mathbb{Z})$

Michael Taylor

Take $a, b \in \mathbb{N},\ b < a$. The Euclidean algorithm computes

$$\gamma = \gcd(a,b) \tag{A}$$

and produces $x, y \in \mathbb{Z}$ such that

$$ax + by = \gamma. \tag{B}$$

We recall how this works and draw conclusions about the discrete group $S\ell(2,\mathbb{Z})$.

To start, set

$$a = k_1 b + a_1, \quad a_1, k_1 \in \mathbb{Z}^+, \quad 0 \le a_1 < b. \tag{1}$$

We have

$$\gcd(a,b) = \gcd(a_1,b). \tag{2}$$

Also

$$\begin{pmatrix} a_1 \\ b \end{pmatrix} = \begin{pmatrix} a - k_1 b \\ b \end{pmatrix} = \begin{pmatrix} 1 & -k_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}. \tag{3}$$

If $a_1 = 0$, stop. If $a_1 > 0$, write

$$b = \ell_1 a_1 + b_1, \quad b_1, \ell_1 \in \mathbb{Z}^+, \quad 0 \le b_1 < a_1. \tag{4}$$

Then

$$\gcd(a_1,b_1) = \gcd(a_1,b) = \gcd(a,b), \tag{5}$$

and

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} a_1 \\ b - \ell_1 a_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\ell_1 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\ell_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -k_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}. \tag{6}$$

If $a_1 = 0$, just set $\ell_1 = 0,\ b_1 = b$.

Now apply this process to the new pair (a_1, b_1). Continue until you get

$$\begin{pmatrix} a_N \\ b_N \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\ell_N & 1 \end{pmatrix} \begin{pmatrix} 1 & -k_N \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ -\ell_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -k_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \tag{7}$$

with either $a_N = 0$ or $b_N = 0$. The right side of (7) has the form

$$A_N \begin{pmatrix} a \\ b \end{pmatrix}, \quad A_N \in S\ell(2,\mathbb{Z}). \tag{8}$$

We hence have

$$A_N \begin{pmatrix} a \\ b \end{pmatrix} = \gamma \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ or } \gamma \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \gamma = \gcd(a,b). \tag{9}$$

Equivalently,

$$\frac{1}{\gamma} \begin{pmatrix} a \\ b \end{pmatrix} = \text{ one column of } A_N^{-1}. \tag{10}$$

Note that

$$A_N^{-1} = \begin{pmatrix} 1 & k_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \ell_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & k_N \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \ell_N & 1 \end{pmatrix} \in S\ell(2,\mathbb{Z}). \tag{11}$$

In fact, each $k_j, \ell_j \in \mathbb{Z}^+$. If, for example, (10) is the first column of A_N^{-1}, we have

$$A_N^{-1} = \begin{pmatrix} a/\gamma & -y \\ b/\gamma & x \end{pmatrix}, \quad x, y \in \mathbb{Z}, \quad 1 = \det A_N^{-1} = \frac{1}{\gamma}(ax + by), \tag{12}$$

yielding (B). A similar calculation holds if (10) is the second column of A_N^{-1}.
Using the calculations done above, we can establish the following.

Proposition 1. *The group $S\ell(2,\mathbb{Z})$ is generated by the two elements*

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \tag{13}$$

Proof. Denote by G the subgroup of $S\ell(2,\mathbb{Z})$ generated by U and L. Take

$$X = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in S\ell(2,\mathbb{Z}). \tag{14}$$

For now, we treat X under the additional hypothesis that

$$0 < b < a. \tag{14A}$$

We have $\gcd(a,b) = 1$, and calculations yielding (10)–(11) apply, with $\gamma = 1$. Since

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = U^k, \quad \begin{pmatrix} 1 & 0 \\ \ell & 1 \end{pmatrix} = L^\ell, \tag{15}$$

we see that $A_N^{-1} \in G$.

Suppose $\binom{a}{b}$ is the left column of A_N^{-1}, so

$$A_N^{-1} = \begin{pmatrix} a & -y \\ b & x \end{pmatrix}. \tag{16}$$

We have

$$X\begin{pmatrix}1\\0\end{pmatrix} = A_N^{-1}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}, \tag{17}$$

hence

$$A_N X\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}, \text{ so } A_N X = \begin{pmatrix} 1 & \xi \\ 0 & \eta \end{pmatrix}, \ \xi, \eta \in \mathbb{Z}. \tag{18}$$

Since $\det A_N X = 1$, $\eta = 1$, so

$$X = A_N^{-1}\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \in G. \tag{19}$$

On the other hand, if $\binom{a}{b}$ is the right column of A_N^{-1}, so

$$A_N^{-1} = \begin{pmatrix} y & a \\ -x & b \end{pmatrix}, \tag{20}$$

then

$$X\begin{pmatrix}1\\0\end{pmatrix} = A_N^{-1}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}, \tag{21}$$

so

$$A_N X\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}, \quad \text{so} \quad A_N X = \begin{pmatrix} 0 & \xi \\ 1 & \eta \end{pmatrix}, \quad \xi, \eta \in \mathbb{Z}. \tag{22}$$

Since $\det A_N X = 1$, $\xi = -1$, so

$$X = A_N^{-1}\begin{pmatrix} 0 & -1 \\ 1 & \eta \end{pmatrix}. \tag{23}$$

The proof that $X \in G$ (under the hypothesis (14A)) is finished off by a calculation yielding

$$\begin{pmatrix} 0 & -1 \\ 1 & \eta \end{pmatrix} \in G, \quad \forall\, \eta \in \mathbb{Z}, \tag{24}$$

which which we will attend to presently.

At this point, to prove Proposition 1 we have two tasks remaining. One is to establish (24), and the other is to remove the extra hypothesis (14A) on X.

To this end, we record some general facts about $S\ell(2,\mathbb{Z})$, its special elements U and L, and another special element,

$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J^2 = -I,\ J^3 = -J = J^{-1}. \tag{25}$$

A calculation gives the following extension of (15),

$$U^k L^\ell = \begin{pmatrix} 1+k\ell & k \\ \ell & 1 \end{pmatrix}. \tag{26}$$

Then

$$JU = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = U^{-1}L, \tag{27}$$

so

$$J = U^{-1}LU^{-1} \in G. \tag{28}$$

Hence, for $k \in \mathbb{Z}$,

$$JU^k = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} \in G, \tag{29}$$

and we have (24).

Hence indeed $X \in G$ whenever $X \in S\ell(2,\mathbb{Z})$ satisfies (14A).

We also note that, by (28),

$$-I = J^2 \in G, \quad \text{so } \ X \in G \Leftrightarrow -X \in G. \tag{30}$$

Furthermore, since $U^t = L$,

$$X \in G \Longleftrightarrow X^t \in G. \tag{31}$$

Moving beyond (14A), we see that if X is as in (14),

$$\begin{aligned} b = 0 &\Longrightarrow a = c = \pm 1, \text{ so } \pm X = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}, \ \xi \in \mathbb{Z} \\ &\Longrightarrow X \in G. \end{aligned} \tag{32}$$

Next,

$$b < 0 \Longrightarrow -X = \begin{pmatrix} -a & -c \\ -b & -d \end{pmatrix}, \tag{33}$$

and (30) holds, so it suffices to show that

$$X = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in S\ell(2,\mathbb{Z}),\ b > 0 \Longrightarrow X \in G. \tag{34}$$

Indeed, for such X,

$$U^k X = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a + kb & c + kd \\ b & a \end{pmatrix} = \begin{pmatrix} \tilde{a} & \tilde{c} \\ \tilde{b} & \tilde{d} \end{pmatrix} = \widetilde{X}, \tag{35}$$

and if $k \in \mathbb{N}$ is large enough, $b > 0 \Rightarrow \tilde{a} > \tilde{b} > 0$, and we are in the situation covered by (14A). The argument in the first part of the proof of Proposition 1 implies $\widetilde{X} \in G$, hence

$$X = U^{-k} \widetilde{X} \in G, \tag{36}$$

and we are done with the proof of Proposition 1.

Here is another identity connecting U, L, and J:

$$JUJ^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = L^{-1}. \tag{37}$$

This leads to the following complement to Proposition 1.

Corollary 2. *The group $S\ell(2,\mathbb{Z})$ is generated by the two elements*

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{38}$$

For an alternative proof, note that (27) implies

$$UJU = L. \tag{39}$$