Appendix 1A: Reformulating the Euclidean Algorithm

In section 1.5 we saw that the Euclidean algorithm may be usefully re-formulated in terms of continued fractions. In this appendix we re-formulate the Euclidean Algorithm in two further ways: Firstly, in terms of matrix multiplication, which makes many of the calculations easier; and secondly, in terms of a dynamical system, which will be useful later when we develop similar ideas in a more general context.

1.8. Euclid matrices, and Euclid's algorithm

In discussing the Euclidean algorithm we showed that $\gcd(85, 48) = \gcd(48, 37)$ from noting that $85 - 1 \cdot 48 = 37$. In this we changed our attention from the pair $85, 48$ to the pair $48, 37$. Writing this down using matrices, we performed this change via the map

$$\begin{pmatrix} 85 \\ 48 \end{pmatrix} \to \begin{pmatrix} 48 \\ 37 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 85 \\ 48 \end{pmatrix}.$$

Next we went from the pair $48, 37$ to the pair $37, 11$ via the map

$$\begin{pmatrix} 48 \\ 37 \end{pmatrix} \to \begin{pmatrix} 37 \\ 11 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 48 \\ 37 \end{pmatrix},$$

and then, from the pair $37, 11$ to the pair $11, 4$ via the map

$$\begin{pmatrix} 37 \\ 11 \end{pmatrix} \to \begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 37 \\ 11 \end{pmatrix}.$$

We can compose these maps so that

$$\begin{pmatrix} 85 \\ 48 \end{pmatrix} \to \begin{pmatrix} 48 \\ 37 \end{pmatrix} \to \begin{pmatrix} 37 \\ 11 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 48 \\ 37 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 85 \\ 48 \end{pmatrix}$$

and then

$$\begin{pmatrix} 85 \\ 48 \end{pmatrix} \to \begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 37 \\ 11 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 85 \\ 48 \end{pmatrix}.$$

Continuing on to the end of the Euclidean algorithm, via $11 = 2\cdot 4+3$, $4 = 1\cdot 3+1$ and $3 = 3\cdot 1+0$, we have

$$\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}85\\48\end{pmatrix}.$$

Since $\begin{pmatrix}0 & 1\\1 & -x\end{pmatrix}\begin{pmatrix}x & 1\\1 & 0\end{pmatrix} = I$ for any x, we can invert to obtain

$$\begin{pmatrix}85\\48\end{pmatrix} = M\begin{pmatrix}1\\0\end{pmatrix}$$

where

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

Here we used that the inverse of a product of matrices is the product of the inverses of those matrices, in reverse order. If we write

$$M := \begin{pmatrix}\alpha & \beta\\\gamma & \delta\end{pmatrix}$$

where $\alpha, \beta, \gamma, \delta$ are integers (since the set of integer matrices are closed under multiplication), then

$$\alpha\delta - \beta\gamma = \det M = (-1)^6 = 1,$$

since M is the product of six matrices, each of determinant -1, and the determinant of the product of matrices, equals the product of the determinants. Now

$$\begin{pmatrix}85\\48\end{pmatrix} = M\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\alpha & \beta\\\gamma & \delta\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\alpha\\\gamma\end{pmatrix}$$

so that $\alpha = 85$ and $\gamma = 48$. This implies that

$$85\,\delta - 48\,\beta = 1;$$

that is, the matrix method gives us the solution to (1.2.1) without extra effort.

If we multiply the matrices defining M together in order, we obtain the sequence

$$\begin{pmatrix}1 & 1\\1 & 0\end{pmatrix},\ \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\1 & 0\end{pmatrix} = \begin{pmatrix}2 & 1\\1 & 1\end{pmatrix},\ \begin{pmatrix}2 & 1\\1 & 1\end{pmatrix}\begin{pmatrix}3 & 1\\1 & 0\end{pmatrix} = \begin{pmatrix}7 & 2\\4 & 1\end{pmatrix},$$

and then

$$\begin{pmatrix}16 & 7\\9 & 4\end{pmatrix},\ \begin{pmatrix}23 & 16\\13 & 9\end{pmatrix},\ \begin{pmatrix}85 & 23\\48 & 13\end{pmatrix}.$$

We notice that the columns give us the numerators and denominators of the convergents of the continued fraction for $85/48$, as discussed in section 1.5.

We can generalize this discussion to formally explain the Euclidean algorithm:

Let $u_0 := a \geq u_1 := b \geq 1$. Given $u_j \geq u_{j+1} \geq 1$,

- Let $a_j = [u_j/u_{j+1}]$, an integer ≥ 1;
- Let $u_{j+2} = u_j - a_j u_{j+1}$ so that $0 \leq u_{j+2} \leq u_{j+1} - 1$;
- If $u_{j+2} = 0$ then $g :=\gcd(a, b) = u_{j+1}$, and terminate algorithm;
- Otherwise, repeat these steps with the new pair u_{j+1}, u_{j+2}.

The first two steps work by Lemma 1.1.1; the third by exercise 1.1.3(i). We end up with the continued fraction

$$a/b = [a_0, a_1, \ldots, a_k]$$

for some $k \geq 0$. The convergents $p_j/q_j = [a_0, a_1, \ldots, a_j]$ are most easily calculated by matrix arithmetic as

$$\begin{pmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \tag{1.8.1}$$

so that $a/g = p_k$ and $b/g = q_k$, where $g = \gcd(a, b)$.

Exercise 1.8.1. Prove that this description of the Euclidean algorithm really works.

Exercise 1.8.2. (a) Show that $p_j q_{j-1} - p_{j-1} q_j = (-1)^{j+1}$ for all $j \geq 0$.
(b) Explain how to use the Euclidean algorithm, along with (1.8.1), to determine, for given positive integers a and b, an integer solution u, v to the equation $au + bv = \gcd(a, b)$.

Exercise 1.8.3. With the notation as above, show that $[a_k, \ldots, a_0] = a/c$ for some integer c for which $0 < c < a$ and $bc \equiv (-1)^k \pmod{a}$.

Exercise 1.8.4. Prove that for every $n \geq 1$ we have

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n,$$

where F_n is the nth Fibonacci number.

My favourite open question in this area is Zaremba's conjecture: He conjectured that there is an integer $B \geq 1$ such that for every integer $n \geq 2$ there exists a fraction m/n, where m is an integer, $1 \leq m \leq n-1$, coprime with n, for which the continued fraction $m/n = [a_0, a_1, \ldots, a_k]$ has each $a_k \leq B$. Calculations suggest one can take $B = 5$.

1.9. Euclid matrices, and ideal transformations

In section 1.3 we used Euclid's algorithm to transform the basis of the ideal $I(85, 48)$, to $I(48, 37)$, and on, until we showed that it equals $I(1, 0) = I(1)$. The transformation rested on the identity

$$85m + 48n = 48m' + 37n', \text{ where } m' = m + n, \text{ and } n' = n;$$

a transformation we can write as

$$(m, n) \to (m', n') = (m, n) \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

The transformation of linear forms can then be seen by

$$48m' + 37n' = (m', n') \begin{pmatrix} 48 \\ 37 \end{pmatrix} = (m, n) \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 48 \\ 37 \end{pmatrix} = (m, n) \begin{pmatrix} 85 \\ 48 \end{pmatrix} = 85m + 48n.$$

The inverse map can be found simply by inverting the matrix:

$$\begin{pmatrix} m' \\ n' \end{pmatrix} \to \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} m' \\ n' \end{pmatrix}.$$

These linear transformations can be composed by multiplying the relevant matrices, which are the same matrices that arise in the previous section, section 1.8. For example, after three steps, the change is

$$\big(m,n\big) \to \big(m_3,n_3\big) = \big(m,n\big)\begin{pmatrix}7 & 2\\ 4 & 1\end{pmatrix},$$

so that $11m_3 + 4n_3 = 85m + 48n$.

Exercise 1.9.1. (a) With the notation of section 1.8, establish that $xu_j + yu_{j+1} = ma + nb$ where the variables x and y are obtained from the variables m and n by a linear transformation.

(b) Deduce that $I(u_j, u_{j+1}) = I(a,b)$ for $j = 0, \ldots, k$.

1.10. The dynamics of the Euclidean algorithm

We now explain a dynamical perspective on the Euclidean algorithm, by focusing on each individual transformation of the pair of numbers with which we work. In our example, we began with the pair of numbers $(85, 48)$, subtracted the smaller from the larger to get $(37, 48)$, and then swapped the order to obtain $(48, 37)$. Now we begin with the fraction $x := 85/48$; the first step transforms $x \to y := x-1 = 37/48$, and the second transforms $y \to 1/y = 48/37$. The Euclidean algorithm can easily be broken down into a series of steps of this form

$$\begin{aligned}\frac{85}{48} \to \frac{37}{48} \to \frac{48}{37} \to \frac{11}{37} \to \frac{37}{11} \to \frac{26}{11} \to \frac{15}{11} \to \frac{4}{11}\\ \to \frac{11}{4} \to \frac{7}{4} \to \frac{3}{4} \to \frac{4}{3} \to \frac{1}{3} \to \frac{3}{1} \to \frac{2}{1} \to \frac{1}{1} \to \frac{0}{1}.\end{aligned}$$

It is possible that the map $x \to x - 1$ is repeated several times consecutively (for example, as we went from 37/11 to 4/11), the number of times corresponding to the quotient, $[x]$. On the other hand, the map $y \to 1/y$ is not immediately repeated, since repeating this map sends y back to y, which corresponds to swapping the order of a pair numbers twice, sending the pair back to their original order.

These two linear maps correspond to our matrix transformations:

$$x \to x-1 \text{ corresponds to } \begin{pmatrix}1 & -1\\ 1 & 0\end{pmatrix}, \text{ so that } \begin{pmatrix}37\\ 48\end{pmatrix} = \begin{pmatrix}1 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}85\\ 48\end{pmatrix};$$

$$\text{and } y \to 1/y \text{ corresponds to } \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \text{ so that } \begin{pmatrix}48\\ 37\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}37\\ 48\end{pmatrix}.$$

The Euclidean algorithm is therefore a series of transformations of the form $x \to x - 1$ and $y \to 1/y$, and defines a finite sequence of these transformations that begins with any given positive rational number, and ends with 0. One can invert that sequence of transformations, to transformations of the form $x \to x + 1$ and $y \to 1/y$, to begin with 0, and to end at any given rational number.

Determinant 1 transformations. Foreshadowing later results, it is more useful to develop a variant on the Euclidean algorithm in which the matrices of all of the transformations have determinant 1. To begin with, we break each transformation down into the two steps:

- Beginning with the pair $85, 48$ the first step is to subtract 1 times 48 from 85; and in general we subtract q times b from a. This transformation is therefore given by

$$\begin{pmatrix} a \\ b \end{pmatrix} \to \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \text{ and notice that } \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-q}.$$

- The second step swaps the roles of $37 (= 85 - 48)$ and 48, corresponding to a matrix of determinant -1. Here we do something unintuitive which is to change 48 to -48, so that the matrix has determinant 1:

$$\begin{pmatrix} 37 \\ 48 \end{pmatrix} \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 37 \\ 48 \end{pmatrix}, \text{ and more generally } \begin{pmatrix} a \\ b \end{pmatrix} \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

One then sees that if $g = \gcd(a, b)$ and $a/b = [a_0, \dots, a_k]$ then

$$\begin{pmatrix} 0 \\ g \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-a_k} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-a_{k-1}} \cdots \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-a_0} \begin{pmatrix} a \\ b \end{pmatrix}.$$

We write $S := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Taking inverses here we get

$$\begin{pmatrix} a \\ b \end{pmatrix} = S^{a_0} T S^{a_1} T \cdots S^{a_{k-1}} T S^{a_k} \begin{pmatrix} 0 \\ g \end{pmatrix}.$$

If a and b are coprime then this implies that

$$S^{a_0} T S^{a_1} T \cdots S^{a_{k-1}} T S^{a_k} = \begin{pmatrix} c & a \\ d & b \end{pmatrix} \tag{1.10.1}$$

for some integers c and d. The left-hand side is the product of determinant one matrices, and so the right-hand side also has determinant one; that is, $cb - ad = 1$. This is therefore an element of $\mathrm{SL}(2, \mathbb{Z})$, the subgroup (under multiplication) of 2-by-2 integer matrices of determinant one; more specifically

$$\mathrm{SL}(2, \mathbb{Z}) := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \ \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \ \alpha\delta - \beta\gamma = 1 \right\}.$$

Theorem 1.2. *Each matrix in* $\mathrm{SL}(2, \mathbb{Z})$ *can be represented as* $S^{e_1} T^{f_1} \cdots S^{e_r} T^{f_r}$ *for integers* $e_1, f_1, \dots, e_r, f_r$.

Proof. Suppose that we are given $\begin{pmatrix} x & a \\ y & b \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. Taking determinants we see that $bx - ay = 1$. Therefore $\gcd(a, b) = 1$, and so above we saw how to construct an element of $\mathrm{SL}(2, \mathbb{Z})$ with the same last column. In Theorem 3.5 we will show that every other integer solution to $bx - ay = 1$ is given by $x = c - ma, y = d - mb$ for some integer m. Therefore

$$\begin{pmatrix} x & a \\ y & b \end{pmatrix} = \begin{pmatrix} c & a \\ d & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix}.$$

One can easily verify that

$$T^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ so that } T^{-1} S T = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$

and therefore

$$\begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix} = (T^{-1}ST)^m = T^{-1}S^mT.$$

Combining these last two statements together with (1.10.1) completes the proof of the theorem. □