Worksheet 15: The Euclidean Algorithm

To find the greatest common measure of two numbers... (Euclid, The Elements, Book VII, Proposition 2)

Starting with two positive integers $x_0$ and $x_1$, the Euclidean algorithm recursively defines two sequences of integers $x_0, x_1, x_2, \ldots$ and $a_1, a_2, a_3, \ldots$ as follows: For $n \geq 2$, we have

$$x_n = x_{n-2} - a_{n-1}x_{n-1}$$

with $0 \leq x_n < x_{n-1}$. The algorithm terminates when $x_n = 0$.

**Problem 15.1.** Compute the sequences $x_n$ and $a_n$ with $x_0 = 321$ and $x_1 = 123$.

**Problem 15.2.** Show that $\text{GCD}(x_0, x_1) = \text{GCD}(x_1, x_2) = \cdots = \text{GCD}(x_{n-1}, x_n) = x_{n-1}$, where $x_n = 0$.

Let this common GCD be $g$.

**Problem 15.3.** Show that there is an elementary matrix $E$ with $E \begin{bmatrix} x_{n-2} \\ x_{n-1} \end{bmatrix} = \begin{bmatrix} x_n \\ x_{n-1} \end{bmatrix}$. Recall that a $2 \times 2$ elementary matrix is one of the form $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

**Problem 15.4.** Show that there is a product of elementary matrices $F$, with $F \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} = \begin{bmatrix} g \\ 0 \end{bmatrix}$. (Hint: Remember Problem Set 1?)

**Problem 15.5.** Show that there exist sequences $b_k$ and $c_k$ such that $b_kx_k + c_kx_{k+1} = g$ and show how to compute the $b$'s and $c$'s using the $a$'s.

**Problem 15.6.** Demonstrate that your method works by finding $b$ and $c$ such that $b \cdot 321 + c \cdot 123 = 3$.

---

¹First recorded by Euclid, a Greek mathematician who lived in roughly 300 BCE.