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[1] recursively defines two sequences of integers x_0, x_1, x_2, ... and a_1, a_2, a_3, ... 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 $\mathrm{GCD}(x_0, x_1) = \mathrm{GCD}(x_1, x_2) = \cdots = \mathrm{GCD}(x_{n-1}, x_n) = x_{n-1}$, where $x_n = 0$.

Let this common GCD be g.

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

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

Problem 15.5. Show that there exist sequences b_k and c_k such that $b_k x_k + c_k x_{k+1} = g$ 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 $b \cdot 321 + c \cdot 123 = 3$.

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