1. This is a programming exercise. Use the language of your choice. You will need language or library support for “big integers”.

You should write two programs. The first program should take as input positive integers $\ell$ and $n$. It should use a built-in random number generator to compute a random $\ell$-bit integer $m$ (i.e., $2^{\ell-1} \leq m < 2^\ell$), along with random $a, b, x_0 \in \{0, \ldots, m - 1\}$. It should output the first $n + 1$ elements $x_0, \ldots, x_n$ in the linear congruential sequence defined by these parameters.

The second program should take as input a sequence $x_0, \ldots, x_n$ as output by the first program. It should then compute and output the values $m_1, \ldots, m_n$ and $a_n$ as defined in the LCG handout. If things are working as expected, the sequence of $m_i$’s should converge quite quickly to the value of $m$. This program may also halt and output “error” if you do not find a $t$ such that $e_t \mid y_{t+1}$ as in Lemma 2 of the LCG handout.