1. Write down the first 30 digits of the key defined by $\bar{s} = [1; 1; 0; 0]$ and $\bar{c} = [1; 0; 0; 1]$. Can you see what the key length is?

2. The recursive method of producing a key can also be used to produce pseudorandom numbers. These are numbers that appear random but are not (generating random numbers and even defining what it means to be random is a difficult thing).

Create the first ten digits of a pseudorandom string of numbers between 0 and 15 as follows:

(a) Consider the key defined by the vectors $\bar{s} = [1; 0; 1; 1; 1; 0; 0]$ and $\bar{c} = [1; 0; 1; 1; 0; 0; 0]$. Write down 40 bits of this key.

(b) Break the key into 4-bit chunks and convert each chunk from binary to decimal.

3. Suppose when attempting to break a recursively defined key (from a key fragment you have) you apply the Theorem and find for $m = 1, 2, \ldots$ that:

$$\det(M_m) = 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0,$$

at which point you can no longer calculate determinants because you run out of key fragment.

(a) What is your guess for the length of the recursive relation?

(b) Suppose you solve for the corresponding $c_i$ but they don’t actually work when applied to the key fragment. What does this mean?