Exercise sheet 2, 19 November 2026

For computing orders of matrices and to factor polynomials you should use a computer algebra system, except for the very small examples which you should solve by hand.
Some convenient computer algebra systems are Sage http://sagemath.org/and for small computations Pari-GP http://pari.math.u-bordeaux.fr/. I made a Sage "cheat sheet" http://hyperelliptic.org/tanja/teaching/crypto21/sage-ref.pdf for the algebra class.
We study LFSRs where the state register has n entries. The $n \times n$ matrix C defined in class is called the *state-update matrix*. The characteristic polynomial $P(x)$ of a matrix C is defined as $P(x) = \det(xI - C)$. We will show in class later today that

$$P(x) = x^n - \sum_{i=0}^{n-1} c_i x^i.$$

For the exercises below you should use this as the definition of the characteristic polynomial. Over $\mathbb{F}_2$ we have $P(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$, so the minus sign matters only for the Fibonacci sequence below.

1. The following LFSRs are given by how they update the last bit.

   (a) $s_{j+2} = s_j + s_{j+1}$, i.e., $f(x_0, x_1) = x_0 + x_1$;

   (b) $s_{j+3} = s_j + s_{j+1}$;

   (c) $s_{j+3} = s_j$;

   (d) $s_{j+7} = s_j + s_{j+1} + s_{j+5} + s_{j+6}$;

   (e) $s_{j+6} = s_j + s_{j+1} + s_{j+2} + s_{j+3}$;

   (f) $s_{j+10} = s_j + s_{j+1} + s_{j+2} + s_{j+7}$.

   For each of these LFSRs

   (a) Draw the LFSR and write out the update polynomial f (given only for (a)).

   (b) Compute the order of the state-update matrix.

   (c) For all starting vectors find the period; you only need to compute and state this for one representative for each sequence; one sequence should be started at $S_0 = (s_0\, s_1\, s_2\, \ldots\, s_{k-1}) = (0\, 0\, \ldots\, 0\, 1)$.

   (d) Write down the characteristic polynomial and factor it over $\mathbb{F}_2$.

   (e) The order of a polynomial $F(x) \in \mathbb{F}_2[x]$ is the smallest integer $\ell > 0$ with $x^\ell \equiv 1 \bmod F(x)$. Compute the *order* of each factor.

   Based on the data you just produced, can you find any relation between the degrees of the factors and the largest of the periods? Can you prove your conjecture(s)?

2. The sequence $s_{n+2} = s_n + s_{n+1}$ over the integers with starting values $s_0 = 0, s_1 = 1$ is called the Fibonacci sequence. Compute the first 10 elements. Factor the characteristic polynomial of this sequence and call the roots α and $\bar{\alpha}$. Compute $(\alpha^j - \bar{\alpha}^j)/\sqrt{5}$ for $0 \leq j \leq 10$. What do you notice?

3. Can you find a similar result for the sequences over $\mathbb{F}_2$?