LFSR = Linear Feedback Shift Register

1. The following is a binary Vigenere encipherment of a plaintext using the key

11100010100010. Decipher and decode the message into English text, regarding each 7-bit block as an ASCII value. SHOW WORK.

0100010 1100111 0111101 1101110 0100010 1110110 0111110 1100001 0111010

1. Complete the table of outputs for the following LFSR, with the given initial state. What is the period? Show work.



1. Find the 4-bit LFSR equation that produced the following output stream. If you have taken calculus use a matrix to solve for full credit. Show work.

10100010

1. Suppose that the bit sequence 0000010111 was generated by a LFSR. Could that register have 3 bits? 4? 5? Clearly explain.
2. Determine the tap polynomial for each of the three LFSRs used in A5/1 (see page 526 of your book).
3. Will the LFSR represented by the tap polynomial p(x) = x4+x3+x2+x+1 yield a maximal period in a 4-bit register? What is its period? Prove and clearly explain your answer using the methods from class to determine if the p(x) is irreducible and primitive; DO NOT just write down a register output list and see how long it is.
4. Suppose a LFSR is used in a 5-bit register. Find a tap polynomial that produces an output of maximal period (25-1 = 31). Use the methods from class and show work. Once you’ve found your equation, choose an initial value and show the output gives the desired period of 31. You may use excel and maple but please indicate when and how you have used these resources.