Tasks for Week 5 tutorial

1) Solve the leftover problems from Week 4 tutorial

2) Determine whether x^5+x^4+1 is

   i) irreducible
   ii) primitive

3) The following ciphertext has been created using a stream cipher on the alphabet $\{0,1\}$ whose key is generated by a 7-bit shift register:

   0 0 0 0 1 1 0 1 1 0 1 1 1 0 1 0 1 0 (CT)

   Suppose the initial 14 bits of the plaintext are known:

   1 0 1 0 0 1 1 1 1 1 0 1 0 1 (PT).

   Determine the rest of the plaintext.

4) Attempt Q4 of Exercise sheet 5

5) Bring your own questions to the tutorial.

6) Now that the past papers are available, have a look at them and if there is anything you need help with ask me in this, or subsequent, tutorials.