Error-correcting codes

1. Find a polynomial of degree at most 2 which passes through the points $(1,2), (2,5), (3,12)$. Use linear equations as opposed to Lagrangian interpolation.

2. When working in $GF(11)$, we want to send a message $(5,2)$. The message we send might get corrupted at $k = 1$ place.

   (a) First find a polynomial $P(x)$ such that $P(1) = 5, P(2) = 2$.

   (b) You should be sending more than two characters to ensure that you can recover from 1 general error. How many should you send?

   (c) Assuming the answer to the previous question was m, find out the actual message you'll be sending by evaluating $P(x)$ at $x = 1, 2, \ldots, m$.

   (d) Assume that the message you send gets corrupted at the 2nd character. Increase the value you computed by 1 to get the corrupted character. Remember that the person receiving the message does not know that it was the 2nd character that got corrupted. What will the error-locating polynomial be here?

   (e) To decode the message you set-up the polynomial $Q(x)$ as $P(x)E(x)$ where P is the original polynomial and E is the error-locating polynomial. Remember that the receiver does not know what any of these polynomials are yet. What is the degree of Q?

   (f) Remember that the equation $Q(x) = r_x E(x)$ is satisfied where $x = 1, \ldots, m$ and r_x is the x-th character received. Why is this true? Give a short justification.

   (g) Now the receiver writes $Q(x)$ and $E(x)$ in the most general format possible (i.e. with arbitrary coefficients). Write $Q(x)$ and $E(x)$ replacing their coefficients with variables. Remember that even though the receiver knows nothing about the message yet, he knows one of the coefficients of $E(x)$. What is that coefficient?

   (h) Now write down the system of linear equations corresponding to $Q(x) = r_x E(x)$. The variables are the coefficients of Q and E.

   (i) Solve the linear system. Did you get the error-locating polynomial you expected?

   (j) How would one go from knowing E and Q to finding P?

3. What happens in the error-correcting method if there are actually no errors? Try the previous problem but don't corrupt the 2nd character.