18.310 Homework # 5

1: Consider the following polynomials

i) $1 + x + x^2 + x^4 + x^6$

ii) $1 + x^2 + x^6$

iii) $1 + x + x^5 + x^7$

iv) $1 + x + x^3 + x^5 + x^7$

v) $1 + x + x^2 + x^5 + x^7$

1a: You should be able to tell that two of these are not primitive without using a spreadsheet. Which two and why?
1b: Use a spreadsheet to construct the remainder tables for the other polynomials and decide which one of the others is primitive.

2: A silly code
What happens when you try to apply the procedure for constructing a 2-error-correcting BCH code with the polynomial $x^3 + x + 1$? What is $p_3(x)$? How many bits does this code encode? What polynomial do you multiply by to do the encoding? Describe this code more simply. How many errors does this code actually correct? (You can do this problem using a spreadsheet, but the calculations aren't too hard to do it by hand.)

3: Our 2-error correcting BCH codes are binary linear codes, and thus there are two matrices C and D with CD=0 so that you can encode by taking the message m and using binary matrix multiplication to get the encoded message mC. Similarly, you can find which bits are in error by taking the received message r and using binary matrix multiplication to get a "syndrome" rD which depends only on the error. From this syndrome (after some processing) you can determine the position of the errors, assuming there are at most two of them. Describe these matrices C and D in terms of $p(x)$, $p_3(x)$, remainder tables, and so on.

4: For the primitive polynomial $1 + x + x^6$, construct a remainder table and an up-by-three remainder table, and use these to find $p_3(x)$ for this polynomial.

5: For the primitive polynomial $p(x) = 1+x+x^6$, construct a spreadsheet program which will let you input remainders $\text{rem}(x^a)$ and $\text{rem}(x^b)$ and will find the roots (solutions) of the polynomial $y^3 + x^a y + x^b = 0$. You will need to construct a remainder table and an up-by-3 remainder table for $p(x)$ (you already did these). By feeding the input into the first row of these tables, use these to calculate, for each j between 0 and 62, the result of plugging $\text{rem}(x^j)$ into the polynomial. Then pick out the zeros. How many solutions does the polynomial $y^3 + y + 1$ have? Find values for $\text{rem}(x^a)$ and $\text{rem}(x^b)$ which give only one solution. Factor the polynomial $y^3 + \text{rem}(x^a)y + \text{rem}(x^b)$ for this case.