18.310 Assignment 5 Due MONDAY October 6

1. Find a primitive polynomial of degree 6 and one of degree 7.

2. Given the primitive polynomial, p $p(x)= 1 + x^2 + x^5$ find the polynomial equation in the field or remainders on dividing by p that is satisfied by x^3 (find a linear dependence among the remainders of 1, x^3, x^6, …, x^{15} and then divide the powers by 3)

3. Find the remainder table for the p of problem 2. Also find a table for the remainders when the powers go up by 2 from row to row, and up by 3 from row to row. (powers go as 0,2,4,6,…, and as 0,3,6,9,…) (these allow computation of t2 and t3 where tj is the sum of the jth powers of the errors.) do these on a spreadsheet

4 Set up a spreadsheet that encodes a message of length 26 in the polynomial code with coding polynomial the p of problems 2 and 3. add a column that allows addition to the encoding polynomial of errors, and insert one error. Take the resulting erroneous message and have your spreadsheet find and correct the error. Then divide to find the original message.

5. Set up your spreadsheet to do the following things.

A take a column in which you can enter a 21 bit message and encode it using the polynomial p above times the p3 you found in problem 2.

B add another column in which you can add errors to the encoded message and add one or two of them.

C calculate t1 and t3 by taking appropriate dot products of tables with your erroneous message

D calculate $t1^3$ (by finding the entry in the up by 3 table corresponding to the t1 entry in the original table.)

E for each power y create the sum $t1*y^2 + t1^2*y + (t1^3+t3)$. If this sum is always all 0's there are no errors, Otherwise if there are at most two errors, the all 0's entries for these sums of remainders will be the locations of the errors.

F Correct the errors and divide by p and by p3 to find the original message.