CMSC 442 Fall 2003
Homework 2

- READING ASSIGNMENT: Peterson & Weldon, **"Error-Correcting Codes,"** MIT Press, (Second Edition), (1986), Chapter 3, pages 19-25, and Chapter 6, pages 144-164.
- OPTIONAL READING ASSIGNMENT: MacWilliams & Sloane, **"The Theory of Error-Correcting Codes,"** North-Holland (Second Edition), (1983), Chapter 4, pages 93-106.

1. Construct the multiplication table of the group given by the presentation:

$$(r, s \mid r^4 = s^2 = 1,\ sr = r^3 s)$$

Assume that the distinct group elements are:

$$1, r, r^2, r^3, s, rs, r^2 s, r^3 s$$

2. The polynomial

$$p(x) = x^6 + x^5 + 1$$

is primitive (hence, irreducible) over $GF(2)$. Use $p(x)$ to construct a log/antilog table for $GF(2^6)$.

3. The polynomial

$$p(x) = x^2 + x + 2$$

is primitive (hence, irreducible) over $GF(3)$. Use $p(x)$ to construct a log/antilog table for $GF(3^2)$.

4. Consider the following degree 4 irreducible polynomial $p(x)$ given in Peterson's Table of Irreducible Polynomials over $GF(2)$

DEGREE 4 ... 3 37D ...

a) Write down $p(x)$.

b) Since $p(x)$ is irreducible and of degree 3, it follows that

$$GF(2^4) = GF(2)[x] \bmod p(x)$$

List all the elements of $GF(2^4)$ in the above representation, i.e., in terms of

$$\xi = x \bmod p(x)$$

c) Let $\xi = x \bmod p(x)$. Why is $\{\xi^k\}$ not a complete list of all the non-zero elements of $GF(2^4)$?