CMSC 442 Fall 2003
Homework 6

- READING ASSIGNMENT: Peterson & Weldon, **"Error-Correcting Codes,"** MIT Press, (Second Edition), (1986), Chapter 2, pages 19-39, and Chapter 6, pages 144-154.

1) Compute the addition and multiplication tables for the ring

$$R_3 = GF(2)[x]/\left\langle x^3+1\right\rangle$$

Also express each of the following ideals in the ring R_3 as a set of elements of R_3.

$$\langle 0\rangle,\ \langle 1+x\rangle,\ \left\langle x^2+x+1\right\rangle,\ \langle 1\rangle,\ \left\langle x^2+1\right\rangle,\ \left\langle x^3+1\right\rangle,\ \left\langle x^5+x+1\right\rangle,\ \left\langle x^6+1, x^2+x+1\right\rangle.$$

For example,

$$\langle 0\rangle = \{0\} \text{ and } \left\langle x^4+x^2+1\right\rangle = \{0, x^2+x+1\}$$

2) Let ξ be the primitive element of $GF(2^6)$ defined by $\xi = x \bmod x^6+x+1$. Compute the orders of the elements of ξ^i for $i = 0, 1, ..., 62$. Summarize your results in a log/order table. For which i's are the ξ^i's primitive? Do you see a pattern? Make a conjecture about this pattern. [Recall that the **order** of an element a is the smallest positive integer k such that $a^k = 1$. Also recall that an element of $GF(2^6)$ is **primitive** if its order is $2^6 - 1 = 15$.]

3) Let R be a commutative ring for which there exist non-zero elements a and b such that

$$ab = 0$$

Prove that R is not a field.

4) In the ring $GF(2)[x]$, compute

$$\gcd\left(x^8+x^6+x^4+x^3+x+1, x^6+x^5+x^4+x^2+x+1\right)$$