CMSC 442 Fall 2001
Instructor: Dr. Lomonaco
Homework 7

- READING ASSIGNMENT: Peterson & Weldon, **"Error-Correcting Codes,"** MIT Press, (Second Edition), (1986), Chapter 6
- OPTIONAL READING ASSIGNMENT: MacWilliams & Sloane, **"The Theory of Error-Correcting Codes,"** North-Holland (Second Edition), (1983), Chapter 4.

Prob. 1. 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 $GF(2^6)$.

Prob. 2. 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 $GF(3^2)$.

Prob. 3. The polynomial

$$p(x) = x^4 + x^3 + x^2 + x + 1$$

is irreducible over $GF(2)$, and therefore the algebra of polynomials modulo $p(x)$ is $GF(2^4)$. Let

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

Show that ξ is not a primitive element, and therefore $p(x)$ is not a primitive polynomial. Show that

$$\alpha = 1 + \xi$$

is primitive, i.e., show that the smallest positive integer k such that $\alpha^k = 1$ is $k = 2^4 - 1$.

Prob. 4. 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 $i = 0, 1, 2, \ldots, 62$. 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. For your calculations, please make use of the following Antilog/Log table of $GF(2^6)$ based on the primitive polynomial

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

Antilog $a_0a_1a_2a_3a_4a_5$	Log		Antilog $a_0a_1a_2a_3a_4a_5$	Log
000000	$-\infty$		000101	15
100000	0		110010	16
010000	1		011001	17
001000	2		111100	18
000100	3		011110	19
000010	4		001111	20
000001	5		110111	21
110000	6		101011	22
011000	7		100101	23
001100	8		100010	24
000110	9		010001	25
000011	10		111000	26
110001	11		011100	27
101000	12		001110	28
010100	13		000111	29
001010	14		110011	30

Antilog $a_0a_1a_2a_3a_4a_5$	Log		Antilog $a_0a_1a_2a_3a_4a_5$	Log
101001	31		111001	47
100100	32		101100	48
010010	33		010110	49
001001	34		001011	50
110100	35		110101	51
011010	36		101010	52
001101	37		010101	53
110110	38		111010	54
011011	39		011101	55
111101	40		111110	56
101110	41		011111	57
010111	42		111111	58
111011	43		101111	59
101101	44		100111	60
100110	45		100011	61
010011	46		100001	62