CMSC 442/653
Instructor: Dr. Lomonaco
Homework 7

- **Optional listening assignment:** Listen to Rosini's Il barbiere di Siviglia (The Barber of Seville)
- **Optional reading assignment:** Peterson, "Error-Correcting Codes," MIT Press, (1961), Chapters 8.

1) You will find below the Antilog/Log table of $GF\left(2^6\right)$ based on the primitive polynomial

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

Use this table to compute the minimum polynomial $m_5(x)$ of ξ^5, where ξ is the primitive element defined by $p(x)$. Please note that the AntiLog is listed in the order $a_0a_1a_2a_3a_4a_5$.

Antilog	Log	Antilog	Log	Antilog	Log	Antilog	Log
000000	$-\infty$	000101	15	101001	31	111001	47
100000	0	110010	16	100100	32	101100	48
010000	1	011001	17	010010	33	010110	49
001000	2	111100	18	001001	34	001011	50
000100	3	011110	19	110100	35	110101	51
000010	4	001111	20	011010	36	101010	52
000001	5	110111	21	001101	37	010101	53
110000	6	101011	22	110110	38	111010	54
011000	7	100101	23	011011	39	011101	55
001100	8	100010	24	111101	40	111110	56
000110	9	010001	25	101110	41	011111	57
000011	10	111000	26	010111	42	111111	58
110001	11	011100	27	111011	43	101111	59
101000	12	001110	28	101101	44	100111	60
010100	13	000111	29	100110	45	100011	61
001010	14	110011	30	010011	46	100001	62

2) Consider $GF\left(3^3\right)$ defined by the primitive polynomial $p(x)=x^3+2x+1$, and let $\xi = x \bmod p(x)$. Find the minimum polynomial $m_5(x)$ of ξ^5. You may assume the following theorems:

- $a^p = a$ for all a in $GF(p)$ for p a prime integer.
- $\left(\sum_{j=1}^{n} a_j\right)^p = \sum_{j=1}^{n} a_j{}^p$ in any field of characteristic p.

You may use the following table for you calculations:

$GF\left(3^3\right)$ defined by the primitive polynomial $p(x)=x^3+2x+1$

AntiLog	Log	Antilog	Log
000	$-\infty$		
100	0	200	13
010	1	020	14
001	2	002	15
210	3	120	16
021	4	012	17
212	5	121	18
111	6	222	19
221	7	112	20
202	8	101	21
110	9	220	22
011	10	022	23
211	11	122	24
201	12	102	25

Please note that the AntiLog is listed in the order $a_0a_1a_2$.