Homework 2

1a) 1110010100010101000011010101110
100110100000101111

b) 111100101000110101100001110101011110100110100001011111
⊕ 100010110101000000001101110110110101110111110100
011011 | 100101 | 010101 | 010110 | 011101 | 000001 | 111111 | 010100
B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8

c) $B_1 \to$ 01 → i 1101 → j row 1 Column 13
The # is 5 so **0101**
$B_2 \to$ 11 → i 0010 → j row 3 Column 2
is 10 so **1010**
$B_3 \to$ 01 → i 1010 → j row 1 Column 10
is 5 so **0101**
$B_4 \to$ 00 → i 1011 → j row 0 Column 11
is 5 so **0101**
$B_5 \to$ 01 → i 1110 → j row 1 Column 14
is 8 so **1000**
$B_6 \to$ 01 → i 0000 → j row 1 Column 0
is 10 so **1010**
$B_7 \to$ 11 → i 1111 → j row 3 column 15
is 12 so **1100**
$B_8 \to$ 00 → i 1010 → j row 0 column 10
is 3 so **0011**

01011010010101011000101011000011
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

d) 11010101001110111001100000000011

2a) 1100 0001 0001 1001 1100 1100 0001 0000
C 1 1 9 C C 1 0
0101 0110 0101 0000 0000 1010 0101 1100
5 6 5 0 0 A 5 C

0011 1101 0000 0110 1011 0111 0011 1000
3 D 0 6 B 7 3 8

1010 0111 0011 0100 1010 1010 0000 1110
A 7 3 4 A A 0 7

b)

c1	56	3d	a7
19	50	06	34
cc	0a	b7	aa
10	5c	38	07

c)

78	b1	27	5c
d4	53	6f	18
4b	67	a9	ac
ca	4a	07	c5

3a) gcd(17, 43)

$43 = 17 \cdot 2 + 9$ $\quad 9 = 43 - 17 \cdot 2$

$17 = 9 \cdot 1 + 8$ $\quad 8 = 17 - 9 \cdot 1$

$9 = 8 \cdot 1 + 1$ $\quad \Rightarrow 1 = 9 - 8 \cdot 1$

$8 = 1 \cdot 8 + 0$

$\gcd(17, 43) = 1$

Substitution:

$1 = 9 - (17 - 9 \cdot 1) \cdot 1$

$= 9 - 17 + 9 \cdot 1 \cdot 1$

$= 9 \cdot 2 - 17$

$= (43 - 17 \cdot 2) \cdot 2 - 17$

$1 = 43 \cdot 2 - 17 \cdot 5$

$1 = 2 \cdot 43 - 5 \cdot 17$

$17^{-1} \pmod{43} \equiv -5 \equiv 38$

38 mod 43

Ex. Euc. Alg

$3^{-1} \bmod 17$

5(x) $(x^2+1) \bmod (x^3+x^2+1)$ + $GF(2^3)$ mod 2

So $-1=1$ b/c $2-1=1$

$x^3 = -x^2-1 = x^2+1$

b)

$$\begin{array}{r} x+1 \quad R\ -x \\ x^2+1 \overline{)\ x^3+x^2+1} \\ -x^3+x \\ \hline x^2-x+1 \\ -x^2+1 \\ \hline -x \end{array}$$

$$\begin{array}{r} -x+2 \quad R\ -3 \\ -x+2 \overline{)\ x^2+1} \\ -x^2-2x \\ \hline -2x+1 \\ -2x+4 \\ \hline -3 \end{array}$$

$$\begin{array}{r} -x \quad R\ 1 \\ -x \overline{)\ x^2+1} \\ x^2 \\ \hline 0+1 \end{array}$$

$x^3+x^2+1 = (x^2+1)(x+1) - x$

$x^2+1 = -x \cdot (-x) + 1$

$-x = 1 \cdot (-x) + 0$

$\hookrightarrow \gcd(x^3+x^2+1,\ x^2+1) = 1$

$1 = x^2+1 - x \cdot x$

$x = -(x^3+x^2+1) + (x^2+1)(x+1)$

$1 = (x^2+1) - (-(x^3+x^2+1) + (x^2+1)(x+1)) \cdot x$

$1 = 1(x^2+1) + (x^3+x^2+1)x - (x^2+1)(x+1)(x)$

$\hookrightarrow (x^2+1)\ [-(x^2+x)+1]$

$1 = (x)(x^3+x^2+1) + (x^2+1)(-x^2-x+1)$

x^2+x+1

c)

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

$= x^4+x^3+2x^2+x+1$

$x^3+x^2+1=0$

$x^3 = -x^2-1$

$x^3 = x^2+1$

$x^4 = x \cdot x^3$

$= x \cdot (x^2+1)$

$= x^3+x$

$= (x^2+1)+x$

$= x^2+x+1$

$-1=1$ because of mod 2 so $2-1=1$

$= (x^2+x+1)+(x^2+1)+2x^2+x+1$

$= 4x^2+2x+3 \bmod 2$

$= 0 \quad 0+1$

$= \boxed{1}$