HOMEWORK 4

1. Define a field and distinguish between an infinite field and a finite field.
2. Use the extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in $GF(2^5)$ using the modulus $(x^5 + x^2 + 1)$.
3. Create a table for addition and multiplication for $GF(2^4)$, using $(x^4 + x^3 + 1)$ as the modulus.
4. Using Table 1, perform the following operations:
   a) $(100) \div (010)$
   b) $(100) \div (000)$
   c) $(101) \div (011)$
   d) $(000) \div (111)$
5. Show how to multiply $(x^3 + x^2 + x + 1)$ by $(x^2 + 1)$ in $GF(2^4)$ using the algorithm in Table 2. Use$(x^4 + x^3 + 1)$ as modulus.
6. Show how to multiply (10101) by (10000) in $GF(2^5)$ using the algorithm in Table 3. Use$(x^5 + x^2 + 1)$ as modulus.

Example:
Find the result of multiplying $\mathbf{P_1} = (x^5 + x^2 + x)$, $\mathbf{P_2}(x^7 + x^4 + x^3 + x^2 + x)$ in $\mathbf{GF(2^8)}$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$.

Table 1: *Multiplication table for* $\mathbf{GF}(\mathbf{2^3})$ *with irreducible poynomial* (x^3+x^2+1)

$\otimes$	000 ($\mathbf{0}$)	001 ($\mathbf{1}$)	010 (x)	011 ($x+1$)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)
001 (1)	000 (0)	001 (1)	010 (x)	011 ($x+1$)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
010 (x)	000 (0)	010 (x)	100 (x^2)	110 (x^2+x)	101 (x^2+1)	111 (x^2+x+1)	001 (1)	011 ($x+1$)
011 ($x+1$)	000 (0)	011 ($x+1$)	110 (x^2+x)	101 (x^2+1)	001 (1)	010 (x)	111 (x^2+x+1)	100 (x^2)
100 (x^2)	000 (0)	100 (x^2)	101 (x^2+1)	001 (1)	111 (x^2+x+1)	011 ($x+1$)	010 (x)	110 (x^2+x)
101 (x^2+1)	000 (0)	101 (x^2+1)	111 (x^2+x+1)	010 (x)	011 ($x+1$)	110 (x^2+x)	100 (x^2)	001 (1)
110 (x^2+x)	000 (0)	110 (x^2+x)	001 (1)	111 (x^2+x+1)	010 (x)	100 (x^2)	011 ($x+1$)	101 (x^2+1)
111 (x^2+x+1)	000 (0)	111 (x^2+x+1)	011 ($x+1$)	100 (x^2)	110 (x^2+x)	001 (1)	101 (x^2+1)	010 (x)

Table 2: *An efficient alogorithm for multiplication using poynomials(Example)*

Posers	*Operation*	*New Result*	*Reduction*
$x^0 \otimes \mathbf{P_2}$		$x^7+x^4+x^3+x^2+x$	No
$x^1 \otimes \mathbf{P_2}$	$x \otimes (x^7+x^4+x^3+x^2+1)$	x^5+x^2+x+1	**Yes**
$x^2 \otimes \mathbf{P_2}$	$x \otimes (x^5+x^2+x+1)$	$x^6+x^3+x^2+x$	No
$x^3 \otimes \mathbf{P_2}$	$x \otimes (x^6+x^3+x^2+x)$	$x^7+x^4+x^3+x^2$	No
$x^4 \otimes \mathbf{P_2}$	$x \otimes (x^7+x^4+x^3+x^2)$	x^5+x+1	**Yes**
$x^5 \otimes \mathbf{P_2}$	$x \otimes (x^5+x+1)$	x^6+x^2+x	No
$\mathbf{P_1} \times \mathbf{P_2} = (x^6+x^2+x)+(x^6+x^3+x^2+x+1)+(x^5+x^2+x+1) = x^5+x^3+x^2+x+1$			

Table 3: *An efficient algorithm for multiplication using n-bit words*

Powers	*Shift-Left Operation*	*Exclusive-Or*
$x^0 \otimes \mathbf{P_2}$		1001111
$x^1 \otimes \mathbf{P_2}$	00111100	$(00111100) \oplus (00011011) =$ **00100111**
$x^2 \otimes \mathbf{P_2}$	01001110	**01001110**
$x^3 \otimes \mathbf{P_2}$	10011100	10011100
$x^4 \otimes \mathbf{P_2}$	00111000	$(00111000) \oplus (00011011) = 00100011$
$x^5 \otimes \mathbf{P_2}$	01000110	**01000110**
$\mathbf{P_1} \otimes \mathbf{P_2} = (\mathbf{00100111}) \oplus (\mathbf{01001110}) \oplus (\mathbf{01000110}) = \mathbf{00101111}$		