UEE4611 Assignment #4 Solution

1.Demonstrate whether each of these statements is true or false for polynomials over a field.

(a) The product of monic polynomials is monic.
(b) The product of polynomials of degrees m and n has degree $m+n$.
(c) The sum of polynomials of degrees m and n has degree $\max\{m,n\}$.

Let A(x) and B(x) be two polynomials as follows

$$A(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_0,$$
$$B(x) = b_n x^n + b_{n-1}x^{n-1} + ... + b_0,$$

where m,n,a_i,$b_j \in Z$ for $i = 0, 1, ..., m$ and $j = 0, 1, ..., n$, respectively, and $a_m \neq 0$, $b_n \neq 0$.

(a) If A(x) and B(x) are monic polynomials, a_m and b_n are both 1.
Because the leading term of the product of $A(x)$ and $B(x)$ is $c_{m+n}x^{m+n}$, and its coefficient is the product of a_m and b_n, which is 1.
So the product of monic polynomials is also monic.

(b) While a_m and b_n are both nonzero, the coefficient of $x^{m+n} \neq 0$. So the the product of $A(x)$ and $B(x)$ has degree $m + n$.

(c) False.
If $m = n$ and $a_m = -b_n$, then the degree of $A(x) + B(x)$ is less than $n = m = \max\{m, n\}$.

2. Determine which of the following polynomials are reducible over $GF(2)$.

(a) $x^2 + 1$**.**
(b)$x^2 + x + 1$**.**
(c)$x^4 + x + 1$**.**

(a)

$$\begin{aligned} x^2 + 1 &= x^2 - 1 \\ &= (x+1)(x-1) \\ &= (x+1)(x+1) \end{aligned}$$

$x^2 + 1$ is reducible over $GF(2)$.

(b)

Let $f(x) = x^2 + x + 1$.
$f(0) = 1$, which mean x is not a factor of $x^2 + x + 1$.
$f(1) = 1$, which mean $x + 1$ is not a factor of $x^2 + x + 1$.
So $x^2 + x + 1$ is irreducible over $GF(2)$.

(c)

Let $f(x) = x^4 + x + 1$.
$f(0) = 1$, which mean x is not a factor of $x^4 + x + 1$.
$f(1) = 1$, which mean $x + 1$ is not a factor of $x^4 + x + 1$.
So there is no first-order factor$\Rightarrow$ no degree-3 factors.

The possible second order factors are $x^2 + x + 1$ and $x^2 + 1$. We divide $x^4 + x + 1$ by them, respectively, and find out these two are not factors of $x^4 + x + 1$.

Thus $x^4 + x + 1$ is irreducible.

3. Determine the gcd of the following pairs of polynomials.

(a)(x^3+x+1) **and** (x^2+1) **over** $GF(3)$**.**
(b)(x^3-2x+1) **and** (x^2-x-2) **over** $GF(5)$**.**

(a) Use Euclidean Algorithm

$$\begin{aligned} &(x^3+x+1) = (x^2+1)\times x+1 \\ \Rightarrow\, &\gcd(x^3+x+1, x^2+1) = 1 \qquad \text{over } GF(3) \end{aligned}$$

(b) Use Euclidean Algorithm

$$\begin{aligned} &(x^3-2x+1) = (x^2-x-2)\times(x+1)+(x+3) \\ &(x^2-x-2) = (x+3)\times(x+1) \\ \Rightarrow\, &\gcd(x^3-2x+1, x^2-x-2) = (x+3) \qquad \text{over } GF(5) \end{aligned}$$

4. Determine the multiplicative inverse of x^2+1 **in** $GF(2^3)$ **with** $m(x) = x^3+x-1$**.**

$$\begin{aligned} x^3+x+1 &= (x^2+1)x+1 \\ \Rightarrow (x^2+1)x &\equiv 1(\mod x^3+x+1) \\ &= 1(\mod x^3+x-1) \end{aligned}$$

So the multiplicative inverse of x^2+1 in $GF(2^3)$ with $m(x) = x^3+x-1$ is x.

5. Develop a set of tables similar to Table 5.3 for $GF(4)$ with $m(x) = x^2 + x + 1$.

Addition:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Multiplication:

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x