HW2 Written Problem.

1. (a) $(x^2+7x+9)(2x^3+9x^2+5)$

$$= 2x^5+9x^4+5x^2+14x^4+63x^3+35x+18x^3+81x^2+45$$

$$= 2x^5+23x^4+81x^3+86x^2+35x+45$$

$$= 2x^5+x^4+4x^3+9x^2+2x+1$$

(b) $(2x^5+3x+2) \bmod (5x^3+4)$ over $GF(7)=$

$$
\begin{array}{r|l}
 & 6x^2 \\
\hline
5x^3+4 & 2x^5+0+0+0+3x+2 \\
 & 2x^5 \qquad\qquad +24x^2 \\
\hline
 & \qquad\qquad -24x^2+3x+2
\end{array}
$$

$\frac{2}{5} = 2\times 5^{-1} = 2\times 3 = 6$

$5^{-1} \bmod 7 = 3$

$$-24x^2+3x+2 = 4x^2+3x+2$$

(C) $\gcd(x^4+8x^3+7x+8,\ 2x^3+9x^2+10x+1)$ over GF(11)

$$x^4+8x^3+7x+8=(6x+10)(2x^3+9x^2+10x+1)+(4x^2+9)$$

$$\begin{array}{rl}
 & 6x+10 \\
2x^3+9x^2+10x+1 \,) & x^4+8x^3+0+7x+8 \\
 & \underline{x^4+10x^3+5x^2+6x} \\
 & -2x^3-5x^2+x+8=9x^3+6x^2+x+8 \\
 & \underline{9x^3+2x^2+x+10} \\
 & 4x^2 \quad -2=4x^2+9
\end{array}$$

$2^{-1} \bmod 11=6$

$\frac{9}{2}=9\times 2^{-1}=9\times 6=54 \bmod 11=10$

$$2x^3+9x^2+10x+1=(6x+5)(4x^2+9)+0$$

$$\begin{array}{rl}
 & 6x+5 \\
4x^2+9 \,) & 2x^3+9x^2+10x+1 \\
 & \underline{2x^3+\quad 10x} \\
 & 9x^2 \quad +1 \\
 & \underline{9x^2 \quad +1} \\
 & 0
\end{array}$$

$2^{-1} \bmod 11=6$

$\frac{9}{4}=9\times 4^{-1}=9\times 3=27=5$

$4^{-1} \bmod 11=3$

$\therefore \gcd[(x^4+8x^3+7x+8),(2x^3+9x^2+10x+1)]=4x^2+9$

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

$$\begin{array}{r|l} & \quad x \\ \hline x^3+x+1 & x^4+0+0+x+1 \\ & x^4 \quad\; +x^2+x \\ \cline{2-2} & \qquad -x^2 \quad +1 = x^2+1 \end{array}$$

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

$$\begin{array}{r|l} & \quad x \\ \hline x^2+1 & x^3+0+x+1 \\ & x^3 \quad +x \\ \cline{2-2} & \qquad\qquad 1 \end{array}$$

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

$=(x^3+x+1)-x[(x^4+x+1)-x(x^3+x+1)]$

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

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

$\therefore (x^2+1)=(x^3+x+1)^{-1} \bmod x^4+2x^2+1$. over GF(2). ※

2. (a) x^3+x+1.

Irreducible, because there is no linear factor of the form x or $(x+1)$

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

$\therefore$ reducible

3. Show that $d(x)=a(x)b(x) \bmod (x^4+1)=1$

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 0E \\ 09 \\ 0D \\ 0B \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$\{\{0E\}\cdot\{02\} \oplus \{09\}\cdot\{03\} \oplus \{0D\}\cdot\{01\} \oplus \{0B\}\cdot\{01\}\} = \{01\}$

$\{\{0E\}\cdot\{01\} \oplus \{09\}\cdot\{02\} \oplus \{0D\}\cdot\{03\} \oplus \{0B\}\cdot\{01\}\} = \{00\}$

$\{\{0E\}\cdot\{01\} \oplus \{09\}\cdot\{01\} \oplus \{0D\}\cdot\{02\} \oplus \{0B\}\cdot\{03\}\} = \{00\}$

$\{\{0E\}\cdot\{03\} \oplus \{09\}\cdot\{01\} \oplus \{0D\}\cdot\{01\} \oplus \{0B\}\cdot\{02\}\} = \{00\}$