Written Problem 109550096. 杜峯

Problem 1.

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

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

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

$\Rightarrow$ over $GF(11)$

$\Rightarrow 2x^5+x^4+4x^3+9x^2+2x+1$ #

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

$$\begin{array}{r|l} & -1+0+0 \\ \hline 5+0+0+4 & 2+0+0+0+3+2 \\ & -5+0+0-4 \\ \hline & 0+0+0+4+3+2 \end{array}$$

$\Rightarrow 4x^2+3x+2$ #

Use the extended Euclidean algorithm

(c) $\gcd(\overset{f(x)}{x^4+8x^3+7x+8}, \overset{g(x)}{2x^3+9x^2+10x+1})$ over $GF(11)$

give $a(x)$ and $b(x)$ s.t.

$a(x)(x^4+8x^3+7x+8)+b(x)(2x^3+9x^2+10x+1) = \gcd(f(x), g(x))$

let $[a_1(x)=1,\ b_1(x)=0],\ [a_2(x)=0,\ b_2(x)=1]$

---

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

$$\begin{array}{r|l} & -5-1 \\ \hline 2+9+10+1 & 1+8+0+7+8 \\ & -10-45-50-5 \\ \hline & 0+9+6+1+8 \\ & -2-9-10-1 \\ \hline & 0+4+0+9 \end{array}$$

$\Rightarrow -5x-1$ over $GF(11)$ $\Rightarrow 6x+10 = q_1(x)$

$\Rightarrow 4x^2+9 = r_1(x)$

$a_3(x) = a_1(x) - q_1(x)a_2(x) = 1$

$b_3(x) = b_1(x) - q_1(x)b_2(x) = -6x-10 \Rightarrow$ over $GF(11) = 5x+1$

---

$(2x^3+9x^2+10x+1) \bmod (4x^2+9)$ over $GF(11)$

$$\begin{array}{r|l} & -5-17 \\ \hline 4+0+9 & 2+9+10+1 \\ & -20+0-45 \\ \hline & 0+9+0+1 \\ & -68+0-153 \\ \hline & 0+0+0 \end{array}$$

$\Rightarrow q_2(x) = -5x-17$ over $GF(11)$ $\Rightarrow 6x+4$

$\Rightarrow r_2(x) = 0$

---

$a(x) = a_3(x) = 1$

$b(x) = b_3(x) = 5x+1$

$1 \cdot (x^4+8x^3+7x+8) + (5x+1)(2x^3+9x^2+10x+1) = \gcd(f(x), g(x))$

$= (x^4+8x^3+7x+8) + (10x^4+45x^3+50x^2+5x+2x^3+9x^2+10x+1)$

$= 11x^4+55x^3+59x^2+22x+9 = \gcd(f(x), g(x))$

over $GF(11) \Rightarrow 4x^2+9$ #

(d) $(x^3+x+1)^{-1} \bmod x^4+x+1$ over $GF(2)$

give $a(x)$ and $b(x)$ s.t.

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

$\Rightarrow a(x)(x^3+x+1) - b(x)(x^4+x+1) = 1$

let $[a_1(x)=1, b_1(x)=0]$, $[a_2(x)=0, b_2(x)=1]$

Use the extended Euclidean algorithm

---

$(x^3+x+1) \bmod (x^4+x+1) = (x^3+x+1)$

$\Rightarrow q_1(x) = 0$, $r_1(x) = x^3+x+1$

$a_3(x) = a_1(x) - q_1(x)a_2(x) = 1$

$b_3(x) = b_1(x) - q_1(x)b_2(x) = 0$

---

$(x^4+x+1) \bmod (x^3+x+1)$

$$\begin{array}{r|l} & 1 \\ \hline 1+0+1+1 & 1+0+0+1+1 \\ & 1+0+1+1 \\ \hline & 0+0+1+0+1 \end{array}$$

$\Rightarrow x = q_2(x)$

$\Rightarrow x^2+1 = r_2(x)$

$a_4(x) = a_2(x) - q_2(x)a_3(x) = -x \cdot 1 = -x$ over $GF(2) \Rightarrow x$

$b_4(x) = b_2(x) - q_2(x)b_3(x) = 1 - x \cdot 0 = 1$

---

$(x^3+x+1) \bmod (x^2+1)$

$$
\begin{array}{r|l}
 & 1 \\
\hline
1+0+1 & 1+0+1+1 \\
 & 1+0+1 \\
\hline
 & 0+0+0+1
\end{array}
\qquad \Rightarrow q_3(x) = x \qquad \Rightarrow r_3(x) = 1
$$

$a_5(x) = a_3(x) - q_3(x)a_4(x) = 1 - x \cdot x = 1 - x^2$ over $GF(2) \Rightarrow x^2+1$

$b_5(x) = b_3(x) - q_3(x)b_4(x) = -x \cdot 1 = -x$ over $GF(2) \Rightarrow x$

---

$(x^2+1) \bmod 1 = 0$

---

$a(x) = a_5(x) = x^2+1$

$b(x) = b_5(x) = x$

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

$\Rightarrow (x^3+x+1)^{-1} \bmod (x^4+x+1) = x^2+1$ #

## Problem 2.

(a) $x^3+x+1$ over $GF(2)$

$\Rightarrow$ irreducible, because there is no linear factor of the form

$x$ or $(x+1)$ or $x^2$ or $(x^2+1)$ or $(x^2+x)$ or $(x^2+x+1)$ □

(b) $x^4+x^2+x+1$ over $GF(2)$

$\because x^4+x^2+x+1$ over $GF(2)$

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

$\Rightarrow x^4+2x^3+x^2+x+1$ over $GF(2) = x^4+x^2+x+1$

$\therefore x^4+x^2+x+1$ is reducible over $GF(2)$ □

## Problem 3.

$b(y)a(y) \bmod (y^4+1) = 1 = c(y)$

$$
\begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix}
\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}
=
\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}
\begin{bmatrix} 0E \\ 09 \\ 0D \\ 0B \end{bmatrix}
=
\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix}
$$

$$[(0E \cdot 02) \oplus (09 \cdot 03) \oplus (0D \cdot 01) \oplus (0B \cdot 01)] = 01$$
$$[(0E \cdot 01) \oplus (09 \cdot 02) \oplus (0D \cdot 03) \oplus (0B \cdot 01)] = 00$$
$$[(0E \cdot 01) \oplus (09 \cdot 01) \oplus (0D \cdot 02) \oplus (0B \cdot 03)] = 00$$
$$[(0E \cdot 03) \oplus (09 \cdot 01) \oplus (0D \cdot 01) \oplus (0B \cdot 02)] = 00$$

$\Rightarrow C_0 = 01, C_1 = 00, C_2 = 00, C_3 = 00$ $\square$