Introduction to Cryptography, Spring 2021	**Due: 4/13/2021 (Tue.)**

Homework 3

Instructor: Prof. Wen-Guey Tseng

1. For polynomial arithmetic with coefficients in Z_{11} , perform the following calculations.
   a. $(x^2 + 2x + 9)(2x^3 + 9x^2 + x + 7)$
      $= 2x^5 + 9x^4 + x^3 + 7x^2 + 4x^4 + 18x^3 + 2x^2 + 14x + 18x^3 + 81x^2 + 9x + 63$
      $= 2x^5 + 13x^4 + 37x^3 + 90x^2 + 23x + 63$
      $= 2x^5 + 2x^4 + 4x^3 + 2x^2 + x + 8$
   b. $(8x^2 + 3x + 2)(5x^2 + 4)$
      $= 40x^4 + 32x^2 + 15x^3 + 12x + 10x^2 + 8$
      $= 40x^4 + 15x^3 + 42x^2 + 12x + 8$
      $= 7x^4 + 14x^3 + 9x^2 + 1x + 8$
2. Determine which of the following polynomials are reducible over GF(2).
   a. $x^2 + x + 1$ 。
      irreducible, because there is no linear factor of the form x or $(x + 1)$
   b. $x^7 + x^5 + x^3 + x^2 + x + 1$
      reducible, since $x^7 + x^5 + x^3 + x^2 + x + 1 = x^7 + 2x^6 + 3x^5 + 2x^4 + x^3 + x^2 + x + 1$
      $= (x^2 + x + 1)(x^5 + x^4 + x^3 + 1)$
3. Determine the gcd of the following pairs of polynomials: $(x^4 + 8x^3 + 7x + 8)$ and $(2x^3 + 9x^2 + 10x + 1)$ over GF(11)
   $x^4 + 8x^3 + 7x + 8 = (6x + 10)(2x^3 + 9x^2 + 10x + 1) + (4x^2 + 9)$
   $2x^3 + 9x^2 + 10x + 1 = (6x + 5)(4x^2 + 9) + 0$
   So, $gcd[(x^4 + 8x^3 + 7x + 8), (2x^3 + 9x^2 + 10x + 1)] = 4x^2 + 9$
4. Compute $(x^2+2x+2)^{-1} \bmod x^4+2x^2+1$, where the coefficients are over Z_3.
   $x^4+2x^2+1 = (x^2+1x+1)(x^2+2x+2)+(2x+2)$
   $(x^2+2x+2) = (2x+2)(2x+2)+1$

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

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

5. In the discussion of MixColumns and InvMixColumns in AES, it was stated that

b(x) = $a^{-1}(y) \bmod (y^4 + 1)$, where a(y) = {03}$y^3$ + {01}y^2 + {01}y + {02} and b(y) = {0B}y^3 + {0D}y^2 + {09}y +{0E} Show that this is true.

Show that d(x) = a(x)b(x) mod(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} · {02} $\oplus$ {09} · {03} $\oplus$ {0D} · {01} $\oplus$ {0B} · {01}) = {01}

({0E} · {01} $\oplus$ {09} · {02} $\oplus$ {0D} · {03} $\oplus$ {0B} · {01}) = {00}

({0E} · {01} $\oplus$ {09} · {01} $\oplus$ {0D} · {02} $\oplus$ {0B} · {03}) = {00}

({0E} · {03} $\oplus$ {09} · {01} $\oplus$ {0D} · {01} $\oplus$ {0B} · {02}) = {00}