CSci 4554 Assignment 6

Due Friday, April 2nd in class

Problem 1 (12 points). Consider $\mathbb{F}_3[x]$ - a field of polynomials with integer coefficients added and multiplied $\mod 3$.

- Find the following sum: $(2x^2 + x + 1) + (2x^2 + 2x + 1)$.
- Find the following product: $(x + 2)(x + 1)$.
- Divide $x^3 + 2x^2 + 2$ by $2x + 1$.
- Is the polynomial $x^2 + x + 1$ reducible in $\mathbb{F}_3[x]$? If yes, show at least one its representation as a product of two non-constant polynomials. If no, please explain why.

Problem 2 (8 points). Consider $\mathbb{F}_2[x]_f$, where $f = x^8 + x^4 + x^3 + x + 1$ (the polynomial used in AES). Compute the results of the following operations in this field, explain your answers. The polynomials are represented as bytes, in hexadecimal (see pp. 159-160 for more details on the field).

- Add $'A1'$ and $'59'$.
- Multiply $'03'$ by $'A2'$.