Homework 3*

Problem 1 (20 points) Divide $9x^2 + 3x + 5$ by $7x + 3$ assuming that the polynomials are over Z_{11}.

Problem 2 (20 points) Compute the following assuming the polynomials are over GF(2).

$$
\begin{array}{ccc}
(x^5 + x^3 + x^2 + x + 1) & + & (x^2 + x + 1) \\
(x^5 + x^3 + x^2 + x + 1) & - & (x^2 + x + 1) \\
(x^5 + x^3 + x^2 + x + 1) & \times & (x^2 + x + 1) \\
(x^5 + x^3 + x^2 + x + 1) & / & (x^2 + x + 1)
\end{array}
$$

Problem 3 (20 points) There are two different irreducible polynomials of degree 3 over GF(2):

$$
\begin{array}{r}
x^3 + x + 1 \\
x^3 + x^2 + 1
\end{array}
$$

The finite field GF(2^3) can be constructed with either of these two irreducible polynomials. Regardless which to use, we have the same bit patterns related to the eight polynomials in GF(2^3):

$$\{000, 001, 010, 011, 100, 101, 110, 111\}$$

- Find the multiplicative inverse (MI) of 010 when the irreducible polynomial $x^3 + x + 1$ is used to construct GF(2^3).
- Will the MI of 010 be different when the irreducible polynomial $x^3 + x^2 + 1$ is used?

*Your solutions must be typed, and to receive full credits, please show detailed steps/calculations. If you only show the final results, no credits will be given regardless the correctness of the results.

Problem 4 (20 points) Suppose the finite field GF(2^3) is constructed with the irreducible polynomial $x^3 + x + 1$. Perform the following calculations directly:

$$
\begin{array}{lcl}
(x^2 + x + 1) & + & (x^2 + 1) \\
(x^2 + x + 1) & - & (x^2 + 1) \\
(x^2 + x + 1) & x & (x^2 + 1) \\
(x^2 + x + 1) & / & (x^2 + 1)
\end{array}
$$

Will the results change if the modulus polynomial becomes to $x^3 + x^2 + 1$?

Problem 5 (20 points) Suppose GF(2^8) is constructed using $m(x) = x^8 + x^4 + x^3 + x + 1$ and $f(x)$ and $g(x)$ are defined as follows:

$$
\begin{aligned}
f(x) &= x^7 + x^5 + x^3 + x^2 + 1 \\
g(x) &= x^3 + x^2 + 1
\end{aligned}
$$

- Convert $f(x)$ and $g(x)$ into their binary representations based on which to compute $f(x) + g(x)$ and $f(x) \times g(x)$.
- Find the multiplicative inverses of $f(x)$ and $g(x)$ in GF(2^8) respectively.

Optional Problem (20 points) Implement a computer program that, given an irreducible polynomial that defines GF(2^n) and any $f(x)$ in GF(2^n), returns the multiplicative inverse of $f(x)$.