CPSC 418/MATH 318 Practice Problems

Polynomial Arithmetic

1. Consider the two polynomials $f(x) = 2x^4 + 3x^3 + 2x + 4$ and $g(x) = 3x^4 + x^2 + 2x + 1$ whose coefficients belong to $\mathbb{Z}_5$. For all polynomial arithmetic involving $f(x)$ and $g(x)$, be sure to express the coefficients of resulting polynomial as elements in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
   (a) Compute $f(x) + g(x)$.
   (b) Compute $f(x) - g(x)$.
   (c) Compute $f(x)g(x)$.

2. Consider the two binary polynomials $f(x) = x^3 + x^2 + 1$ and $g(x) = x^2 + 1$ whose coefficients belong to $\mathbb{Z}_2$. For all polynomial arithmetic involving $f(x)$ and $g(x)$, be sure to express the coefficients of resulting polynomial as elements in $\mathbb{Z}_2 = \{0, 1\}$.
   (a) Compute the remainder of $f(x)$ when divided by $g(x)$.
   (b) Compute $\gcd(f(x), g(x))$.
   (c) Does $f(x)$ have an inverse modulo $g(x)$ with binary coefficients? If yes, compute it.
   (d) Compute $f(x)^2 g(x) \pmod{m(x)}$ where $m(x) = x^8 + x^4 + x^3 + x + 1$ is the polynomial with binary coefficients used in the construction of the Rijndael field $GF(2^8)$.

3. Consider the polynomial $F(x) = (0001011)x^2 + (01110101)x + (0010010)$ whose coefficients are bytes, i.e. elements in the Rijndael field $GF(2^8)$.
   (a) Compute $G(x) = F(x)^2$ as a polynomial with coefficients in $GF(2^8)$.
   (b) Compute $G(x) \pmod{M(x)}$ where $M(x) = x^4 + 1$ is the polynomial used for 4-byte vector arithmetic in Rijndael.