HOMEWORK 2

Q1: Determine the multiplicative inverse of $x^3 + 1$ in $GF(2^4)$

Q2: Determine the multiplicative inverse of $x^3 + x + 1$ in $GF(2^4)$

Q3: Addition in $GF(2^4)$: Compute $A(x)+B(x) \bmod P(x)$ in $GF(2^4)$ using the irreducible polynomial $P(x) = x^4 + x + 1$. What is the influence of the choice of the reduction polynomial on the computation?

1. $A(x)=x^2+1$, $B(x)=x^3+x^2+1$
2. $A(x) = x^2 + 1$, $B(x) = x + 1$

Q4: Multiplication in GF(24): Compute $A(x)\cdot B(x) \bmod P(x)$ in $GF(2^4)$ using the irreducible polynomial $P(x) = x^4 + x + 1$. What is the influence of the choice of the reduction polynomial on the computation?

1. $A(x)=x^2+1$, $B(x)=x^3+x2+1$
2. $A(x) = x^2 + 1$, $B(x) = x + 1$

Q5: Using the extended Euclidean algorithm, find the multiplicative inverse of

A) 1234 mod 4321

B) 24140 mod 40902

C) 550 mod 1769

Q6:

A) Determine gcd(24140, 16762).

B) Determine gcd(4655, 12075).