**HOMEWORK 2**

Q1: Determine the multiplicative inverse of x3 + 1 in GF(24)

Q2: Determine the multiplicative inverse of x3 + x + 1 in GF(24)

Q3: Addition in GF(24): Compute A(x)+B(x) mod P(x) in GF(24) using the irreducible

polynomial P(x) = x4 + x + 1. What is the influence of the choice of the reduction

polynomial on the computation?

1. A(x)=x2+1, B(x)=x3+x2+1

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

Q4: Multiplication in GF(24): Compute A(x)·B(x) mod P(x) in GF(24) using the

irreducible polynomial P(x) = x4 + x + 1. What is the influence of the choice of the

reduction polynomial on the computation?

1. A(x)=x2+1, B(x)=x3+x2+1

2. A(x) = x2 + 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).