Cairo University
Faculty of Engineering
Computer Engineering Department

CMP N 426 (Computer Security)
Problem Set 4
Chapter 4: Number Theory

✓ **4.6) For each of the following find x**

a) 5 x = 4 (mod 3)
b) 7x = 6 (mod 5)

✓ **4.7) Solve the following**

a) 5 mod 3
b) 5 mod -3
c) -5 mod 3

✓ **4.19) Find multiplicative inverse of**

a) 1234 mod 4321
b) 24140 mod 40902

✓ **4.24) Determine which of the following are reducible over GF(2):**

a) x^3+1
b) $x^3+ x^2+ 1$
c) x^4+1

✓ **4.25) Determine the gcd of the following pairs of polynomials:**

a) $x^3+ x+ 1$ and $x^2+ x+ 1$ over GF(2).
b) $x^3- x+ 1$ and $x^2+ 1$ over GF(3).
c) $x^5 + x^4 + x^3 - x^2 -x+1$ and $x^3+x^2+ x+ 1$ over GF(3) .

MI = x^(7)

✓ **4.26) Find the multiplicative inverse of (x7 + x + 1) mod (x8 + x4 + x3 + x + 1) over GF(2)**

✓ **4.27) Find the multiplicative inverse of (x3 + x + 1) in GF(2^4) with m(x) = x4 + x +1.**

1 + x^(2)