ECE404 Introduction to Computer Security: Homework 03

Chan Ng Cashin

Spring 2024

Due Date: 5:59pm, February 1, 2024

Theory Problems

Problem 1

Given A = {0,1}, determine whether or not the set forms a group with the following binary operators:

- boolean and
- boolean or
- boolean xor

Solution

A group must follow the following rules: closure, associativity, identity element, invertibility. Knowing this we can figure out which binary operators form a group.

boolean and

1. Closure: 0*0=0, 0*1=0, 1*0=0, 1*1=1. All results are in the set {0,1}.
2. Associativity: AND operator is associative.
3. Identity Element: The identity element is 1 because 1*a=a*1=a for all a in {0,1}
4. Inverse Element: There is no element when ANDed with 0 that gives 1(the identity element)

boolean or

1. Closure: 0+0=0, 0+1=1, 1+0=1, 1+1=1. All results are in the set {0,1}.
2. Associativity: OR operator is associative.
3. Identity Element: The identity element is 0 because 0+a=a+0=a for all a in {0,1}
4. Inverse Element: There is no element when ORed with 1 that gives 0(the identity element)

boolean xor

1. Closure: 0 XOR 0 = 0, 0 XOR 1 = 1, 1 XOR 0 = 1, 1 XOR 1 = 0. All results are in the set {0,1}.
2. Associativity: XOR operator is associative.
3. Identity Element: The identity element is 0 because 0 XOR a = a XOR 0 = a for all a in {0,1}
4. Inverse Element: Each element is its own inverse element in XOR: 0 XOR 0 = 0, 1 XOR 1 = 0 (0 being the identity element). Because of this inverse element exists.

This set forms a group only with boolean xor operator.

Problem 2

Given W, the set of all unsigned integers, determine whether or not w forms a group under the gcd(·) operator.

Solution

A group must follow the following rules: closure, associativity, identity element, invertibility. Knowing this we can figure out whether or not w forms a group under the gcd(.) operator.

1. Closure: For any two unsigned integers a and b, gcd(a, b) will also come out to be an unsigned integer.
2. Associativity: For any three unsigned integers a, b, and c, gcd(a, gcd(b,c)) = gcd(gcd(a, b), c).
3. Identity Element: gcd(a, 1) = a for all a in W so 1 is the identity element.
4. Inverse Element: An element b is an inverse of a if gcd(a, b) = 1(the identity element). Because there isn't an element that satisfies this for all cases within W and the gcd operation this is where it fails.

Because set W under gcd fails to have an inverse element, it does not form a group.

Problem 3

Let's say we have a ring with the group operator + as addition and the ring operator × as multiplication. If you switch the two (i.e. multiplication is the group operator and addition is the ring operator), would it still be a ring? Explain why or why not (i.e. indicate all the properties that are true/not true that show it is/is not a ring).

Solution

A ring is a set with two binary operations that satisfy the following properties: closed with respect to the additional operator(usually multiplication), associativity with respect to the additional operator, and the additional operator must distribute over the group addition operator.

1. Closed with respect to the ring operator: Because addition is now the ring operator we must evaluate if the set is closed under addition. Most rings are closed under addition so this property holds.
2. Associativity with respect to the ring operator: Addition is the new rings operator and is associative, so this holds as well.
3. The ring operator must distribute over the group operator: This means that for elements a, b, and c in a group, a + (b × c) must equal a + b × a + c. Because of order of operations this is not always the case and so the group fails to be a ring.

Under the new conditions, this group isn't a ring.

Problem 4

Explain in detail how one would use Bezout's identity to find the multiplicative inverse of an integer in the field Zp, where p is a prime number. Then, use those steps to find the multiplicative inverse of 47 in Z_{97}.

Solution

For this problem we can use Bezout's identity which states that for any two integers a and b, there exists integers x and y so that ax+by = gcd(a, b). If b is a prime number and a is a multiple of b, gcd(a, b) = 1. Because we are finding the multiplicative inverse of Zp we can use this identity to find an integer x such that ax ≡ 1 mod p. In this case x is the multiplicative inverse of a in Zp.

To find the inverse of 47 in Z_{97}:

47x ≡ 1mod97

x = 64 because 47 * 64 mod 97 = 1

Problem 5

In the following, find the smallest possible integer x that solves the congruences. You should not solve them by simply plugging in arbitrary values of x until you get the correct value. Make sure to show your work.

a) 28x ≡ 34 (mod 37)
b) 19x ≡ 42 (mod 43)
c) 54x ≡ 69 (mod 79)
d) 153x ≡ 182 (mod 271)
e) 672x ≡ 836 (mod 997)

Solution

a) 28x ≡ 34 (mod 37)
    a. 28y mod 37 = 1
    b. y = 4 because 28 * 4 = 112 = 1 (mod 37)
    c. 34 * 4 = 136
    d. 136 mod 37 = 25
    e. x = 25
b) 19x ≡ 42 (mod 43)
    a. 19y mod 43 = 1
    b. y = 34
    c. 42 * 34 = 1428
    d. 1428 mod 43 = 9
    e. x = 9
c) 54x ≡ 69 (mod 79)

a. 54y mod 79 = 1
b. y = 60
c. 69 * 60 = 4140
d. 4140 mod 79 = 32
e. x = 32

d) $672x \equiv 836 \pmod{997}$
a. 672y mod 997 = 1
b. y = 408
c. 836 * 408 = 341088
d. 341088 mod 997 = 114
e. x = 114

Problem 6

Simplify the following polynomial expression in GF(89) (54x10 − 62x9 − 84x8 + 70x7 − 75x6 + x5 − 50x3 + 84x2 + 65x + 78) + (−67x9 +44x8 −26x7 −37x6 +61x5 +68x4 +22x3 +74x2 +87x+38)

Solution

$54x^{10}-129x^9-40x^8+44x^7-112x^6+62x^5+68x^4-28x^3+158x^2+152x+116$ is the result when combining the two polynomials.

Now let's preform mod 89 on each coefficient of the result:

$54x^{10}+49x^9+49x^8+44x^7+66x^6+62x^5+68x^4+61x^3+69x^2+27$

Problem 7

Simplify the following polynomial expression in GF(11) (8x3 + 6x2 + 8x + 1) × (3x3 + 9x2 + 7x + 5)

Solution

(8x3 + 6x2 + 8x + 1) × (3x3 + 9x2 + 7x + 5) = $24x^6+90x^5+134x^4+157x^3+95x^2+47x+5$

Now let's perform mod 11 on each coefficient of the result:

$2x^6+2x^5+2x^4+3x^3+7x^2+3x+5$

Problem 8

For the finite field GF(23), simplify the following expressions with modulus polynomial (x3 + x + 1):

a) (x2 + x + 1) × (x2 + x)
b) x2 − (x2 + x + 1)
c) x2+x+1 / x2+1

Solution

a) $(x^2 + x + 1) \times (x^2 + x) \bmod (x^3+x+1)$
    a. $(x^2 + x + 1) \times (x^2 + x) = x^4+2x^3+2x^2+x$
    b. $(x^4+2x^3+2x^2+x) \bmod (x^3+x+1)$:
        i. $x^4 = x$ and $x^3 = -x-1$ in GF(23)
    c. $x + 2(-x-1) + 3x^2 + 2x + 1 \bmod 23$
    d. $3x^2-2x-1$
b) $x^2 – (x^2 + x +1)$
    a. $x^2 – (x^2 + x +1) = -x-1$
    b. $-x-1$
c) x^3+x+1