ECE 40400: Introduction to Computer Security

Spring 2024

Prateek Yashwant Jannu

Purdue University, West Lafayette

Professor: Dr. Avinash C Kak

Theory Problems

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

• boolean and

Does not form a Group
Closure: Yes
Associative: Yes
Identity: 1 x+1=x
Inverse: No, Example - 0 does not have an inverse which would result in 1

• boolean or

Does not form a Group
Closure: Yes
Associative: Yes
Identity: 0 0+x=x
Inverse: No, Example 1 does not have an inverse which would result in 0

• boolean xor

Forms a Group
Closure: Yes
Associative: Yes
Identity: 0 x+0=x
Inverse: Yes All elements 1 has an inverse 1 and 0 has an inverse 0, hence inverse exists

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

Does not Form a Group
Closure: Yes
Associative: Yes
Identity: 0
Inverse: No, No multiplicative inverse because there is no element b such that gcd(a,b)=0 because gcd(0,a)=a for any a and cannot be 0

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)**

No, switching the two operators may not hold the ring properties, as addition and multiplication have different properties. The resulting set may not have the conditions to be considered a ring. I list the properties down below before and after switching

Before Switching

Additive Closure: For any elements a and b in the ring, the sum a + b is also in the ring.
Additive Associativity: For any elements a, b, and c in the ring, (a + b) + c = a + (b + c).
Additive Identity: There exists an additive identity element
Additive Inverse: For every element a in the ring, there exists an additive inverse
Multiplicative Closure: For any elements a and b in the ring, the product a x b is also in the ring.
Multiplicative Associativity: For any elements a, b, and c in the ring, (a x b) x c = a x (b x c).
Distributivity over group operator: For any elements a, b, and c in the ring, a x (b + c) = a x b + a x c and (a + b) x c = a xc + b x c.

After Switching
Multiplication as Group operator:
If group operator is replaced by multiplication, then properties of additive identity, and additive inverse may not hold for multiplication.

Addition as ring operator:
If multiplication is replaced by addition, the properties of multiplicative closure, multiplicative associativity, and left/right distributivity may not hold for addition.

Hence we **cannot assume** that when we switch the group and ring operators, it would still be a ring.

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 Z97.**
\\ Definitions and explanation taken from lecture notes
Bezout's Identity states that for two integers a and b, there exist integers x and y such that ax + by = gcd(a, b). This theorem is used for finding the multiplicative inverse of an integer in a finite field, where p is a prime number.

To find the multiplicative inverse of an integer a in the field, where p is prime number, you would use Bezout's Identity to find x and y such that ax +by = 1. The integer x will be the multiplicative inverse of a.

Here are the steps to find the multiplicative inverse of an integer a using Bezout's Identity:

1. Bezout's Identity:
   Write the equation ax+by=1 where b is the prime. This is guaranteed to be true since b is prime.
2. Use Extended Euclidean Algorithm:
   Use the extended Euclidean algorithm to find x and y such that ax+by = gcd(a, b).
3. Check if gcd(a, b) is 1:
   Make sure that gcd(a,b)=1 . If not, then a and b are not relatively prime, and a does not have a multiplicative inverse.

Let's find the multiplicative inverse of 47 modulo 97:

GCD (47,97)

= GCD (97,47) | residue= 47 =(47x1) + (97x0)
= GCD (47,3) | residue= 3 = -2*(47x1) + (97x1)
= GCD (3,2) | residue= 2 =(47x1) – 15*(-2*(47x1) + (97x1))
=(47x1)+30(47*1)-15(97*1)
=31(47x1)-15(97x1)
= GCD (2,1) | residue= 1 =-2*(47x1) + (97x1)-31(47x1)+15(97x1)
= -33*(47x1)+16*(97x1)

We get x=-33+97=64

The multiplicative inverse of 47 in Z97=64

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)
First find inverse using the bezout's identity
GCD(28,37)
GCD(37,28)=r=28=(28*1)+(37*0)
GCD(28,9)=r=9=(37*1)-(28*0)
GCD(9,1)=1=(28*1)+(37*0)-3(37*1)+3(28*0)
= 4*(28*1)-3(37*1)
Inverse=4
Now Multiply each side by the inverse to the question
4 * 28x= 34*4(mod 37)
X= 136 mod 37
X=25
QED x=25 where 28x≡ 34 (mod 37)

(b) 19x ≡ 42 (mod 43)
First find inverse using the bezout's identity
GCD(19,43)
GCD(43,19)=r=19=(19*1)+(43*0)
GCD(19,5)=r=5=(43*1)-2(19*1)
GCD(5,4)=r=4=(19*1)+(43*0)- 3*(43*1)+6*(19*1)
= 7*(19*1)-3(43*1)
GCD(4,1)=r=1=(43*1)-2(19*1)- 7*(19*1)+3(43*1)
=4*(43*1)-9(19*1)

Now Multiply each side by the inverse to the question
-9 * 19 x= 42*-9(mod 43)
X= -378 modulo 43
X=9

X=9

QED x=9 where 19x≡ 42 (mod 43)

(c) 54x ≡ 69 (mod 79)
First find inverse using the bezout's identity
GCD(54,79)
GCD(79,54)=r=54=(54*1)+(79*0)
GCD(54,25)=r=25=-1*(54*1)+1*(79*1)
GCD(25,4)=r=4= 3*(54*1)-2(79*1)
GCD(4,1)=r=1=-19(54*1)+13(79*1)

Now Multiply each side by the inverse to the question
-19 * 54 x= 69*-19(mod 79)
X= -1311 modulo 79
X=32

X=32
QED x=32 where 54x≡ 69 (mod 79)

(d) 153x ≡ 182 (mod 271)

First find inverse using the bezout's identity
GCD(153,271)
GCD(271,153)=r=118= (271*1)-(153*1)
GCD(153,118)=r=35= -1(271*1)+2(153*1)
GCD(118,35)=r=118= 4(271*1)-7(153*1)
GCD(35,13)=r=118= -9(271*1)+16(153*1)
GCD(13,9)=r=118= 13(271*1)-23(153*1)
GCD(9,4)=r=118= -35(271*1)+62(153*1)

Now Multiply each side by the inverse to the question
62 * 153 x= 182*62(mod 271)
X= 11284 mod 271
X=173

X=173
QED x=173 where 153x≡ 182 (mod 271)

(e) 672x ≡ 836 (mod 997)
(f) First find inverse using the bezout's identity
GCD(672,997)
=GCD(997,672)=r=672= (672*1) + 0(997*1)
=GCD(672,325)=r=325= -1(672*1) + (997*1)
=GCD(325,22)=r=22= 3(672*1) - 2(997*1)
=GCD(22,17)=r=17= -43(672*1) + 29(997*1)
=GCD(17,5)=r=5= 46(672*1) + -31(997*1)
=GCD(5,2)=r=2= -181(672*1) + 122(997*1)
=GCD(2,1)=r=1= 408(672*1) + -275(997*1)

Now Multiply each side by the inverse to the question
408*672x= 408*836(mod 997)
X= 341088 mod 997
X=114

X=114
QED x=114 where 672x ≡ 836 (mod 997)

6. **Simplify the following polynomial expression in GF(89) (54x 10 − 62x 9 − 84x 8 + 70x 7 − 75x 6 + x 5 − 50x 3 + 84x 2 + 65x + 78) + (−67x 9 + 44x 8 − 26x 7 − 37x 6 + 61x 5 + 68x 4 + 22x 3 + 74x 2 + 87x + 38)**

$$\mathbf{54x^{10} + 49x^{9} + 49x^{8} + 44x^{7} + 66x^{6} + 62x^{5} + 68x^{4} + 61x^{3} + 69x^{2} + 63x^{1} + 27}$$

7. **Simplify the following polynomial expression in GF (11) (8x 3 + 6x 2 + 8x + 1) × (3x 3 + 9x 2 + 7x + 5)**

   = $\mathbf{2x^{6} + 6x^{5} + 1x^{4} + 7x^{3} + 7x^{5} + 10x^{4} + 9x^{3} + 8x^{2} + 2x^{4} + 6x^{3} + 1x^{2} + 7x^{1} + 3x^{3} + 9x^{2} + 7x^{1} + 5}$

   = $\mathbf{2x^{6} + 2x^{5} + 2x^{4} + 3x^{3} + 7x^{2} + 3x^{1} + 5}$

8. **For the finite field GF(2^3), simplify the following expressions with modulus polynomial (x 3 + x + 1): (a) (x 2 + x + 1) × (x 2 + x)**
   (b) x 2 − (x 2 + x + 1) (c) x 2+x+1 x2+1
   a)

   a) (x^2 + x + 1) × (x^2 + x)
   X^4 + x
   X^4 /(x^3+x+1)
   =x^2+x+x

=**x^2**

b)

X^2-X^2+X+1

$=X+1$

Final answer=$x+1$

c) $(X^2+x+1)/(x^2+1)$

Multiplicative inverse of x^2+1 wrt to $(x^3 + x + 1)$

$GCD(x^3+x+1,x^2+1)=R=x^2+1=1*(x^2+1)+0*(x^3+x+1)$

$FCD(x^2+1,1)=R=1=x*(x^2+1)-1(x^3+x+1)$

We get MI=x

$(X^2+X+1) * X$

$=X^3+X+1$

Dividing x^3 by modulus polynomial $(x^3 + x + 1)$

We get = $X+1+X^2+X$

$= X^2+1$