**ECE404 Introduction to Computer Security: Homework 03**

**Spring 2024**

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

**Raghava Vivekananda Panchagnula**

**0033584584**

# Introduction

“It is almost impossible to fully understand practically any facet of modern cryptography and several important aspects of general computer security if you do not know what is meant by a finite field” [1]. Thus, the goal of this homework is to help further your understanding of finite fields in preparation for later topics to come. The assignment consists of a theory problem section whose details are specified below.

As always, please read the homework document in its entirety before coming to office hours with your questions. The teaching staff have spent a long time writing the assignment to cover many common questions you might have.

# Theory Problems

Solve the following theory problems. Your solutions must be typed in a PDF titled HW03 <last name> <first name>.pdf.

1. Given A = {0,1}, determine whether or not the set forms a group with the following binary operators:
   * Boolean and
     + Identity: Yes - 1
     + Inverse: There is no Inverse
     + Associative: And is associative
     + Closure: Yes
     + Verdict: Doesn’t form a group
   * Boolean or
     + Identity: Yes - 0
     + Inverse: No Inverse exists
     + Associative: OR is associative
     + Closure: Yes
     + Verdict: Doesn’t Form a group
   * Boolean xor
     + Identity: Yes - 0
     + Inverse: Yes, each element is it’s own inverse
     + Associative: Yes
     + Closure: Yes
     + Verdict: Forms a group
2. Given W, the set of all unsigned integers, determine whether or not w forms a group under the *gcd*(·) operator.

* Identity: The identity element is 0
* Inverse: The inverse of a GCD operator does not exist
* Associative: The GCD Operator is associative
* Closure: The GCD Operator is closed
* Verdict: Doesn’t form a group

1. 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).
   1. Assuming all properties hold initially, given a flip of the operators, the following properties must hold for it to be a ring.
      1. Multiplicative closure: The multiplicative closure must still exist
      2. Multiplicative associativity: This still holds as per the general rules of multiplication
      3. Multiplicative Identity: The existence of 1 isn’t guaranteed
      4. Multiplicative inverse: the existence of a multiplicative inverse isn’t guaranteed.
      5. Additive closure: After multiplication, additive closure isn’t guaranteed
      6. Additive Associativity: By definition of addition this is guaranteed
      7. Additive Identity: 0 may not be a value that exists in the ring after the flip
      8. Additive inverse: The existence of additive inverses aren’t guaranteed
   2. Due to the fact that some of these properties may not necessarily hold, the group may no longer be a ring.
2. 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.
   1. Bezout’s identity states that for any two integers a and b, there must exist integers x and y such that: ax + by = gcd(a,b)
      1. To find the multiplicative inverse of any number a, we can rearrange the equation such that such that ax + yn = 1
      2. To perform the multiplicative inverse, of 47 in Z97, lets start with:
      3. 97 = b \* 47 + r
         1. Find the largest b value and corresponding r
      4. 97 = 2 \* 47 + 3
      5. Then repeat this until you get the final remainder of 1, with the divided as the new divisor and the remainder as the new dividend
      6. 47 = b \* 3 + r = 15 \* 3 + 2
      7. 3 = 1 \* 2 + 1
      8. Now work backwards, and set up 1 = ax + yn with the previous equations to find the larger of the two in magnitude
      9. 1 = 3 – 2
      10. 2 = 47 – 15 \* 3
      11. 3 = 97 – 47 \* 2
      12. 1 = (97 – 47 \* 2) – (47 – 15 \* (97 – 47 \* 2))
      13. Simplify like terms
      14. 1 = 16 \* 97 – 33 \* 47
      15. Since 16 is the value that is tagged on to n, which is 97, we will use that.
      16. 16 is the multiplicative inverse of 47 in *Z*97
3. 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.
   1. 28x ≡ 34 (mod 37)
      1. X = MI(28) \* 34 mod 37
         1. MI(28):
            1. 37 = 28 \* 1 + 9
            2. 28 = 9 \* 3 + 1
            3. 9 = 1 \* 9 + 0
            4. GCD is therefore 1
            5. Now for the coefficients:
            6. 1 = 28 – 9 \* 3
            7. 1 = 28 – 3 \* (37 – 28)
            8. 1 = 4 \* 28 – 3 \* 37
            9. MI(28) = 4
         2. 4 \* 34 mod 37 = 136 mod 37 = 25 mod 37 = 25
         3. X = 25
   2. 19x ≡ 42 (mod 43)
      1. X = MI(19)\*42 mod 43
         1. MI(19):
            1. 43 = 2 \* 19 + 5
            2. 19 = 3 \* 5 + 4
            3. 5 = 1 \* 4 + 1
            4. 4 = 4 \* 1 + 0
            5. Now for the coefficients:
            6. 1 = 5 – 4
            7. 1 = (43 – 2\*19) – (19 – 3 \* (43 – 2\*19))
            8. 1 = 4 \* 43 – 9 \* 19
            9. MI(19) = 43 – 9 = 34
         2. X = 34 \* 42 mod 43 = 9
   3. 54x ≡ 69 (mod 79)
      1. X = MI(54)\*69 mod 79
         1. MI(54) mod 79
            1. 79 = 54 \* 1 +25
            2. 54 = 25 \* 2 + 4
            3. 25 = 4 \* 6 + 1
            4. 4 = 1 \* 4 + 0
            5. Now for the coefficients
            6. 1 = 25 – 4 \* 6
            7. 1 = (79 – 54 \* 1) – (54 – (79 – 54 \* 1) \* 2) \* 6
            8. 1 = -19 \* 54 + 13 \* 79
            9. MI(54) = 60
         2. X = 60 \* 69 mod 79 = 32
   4. 153x ≡ 182 (mod 271)
      1. X = MI(153) \* 182 (mod 271)
         1. MI 153
            1. 271 = 153 \* 1 + 118
            2. 153 = 118 \* 1 + 35
            3. 118 = 35 \* 3 + 13
            4. 35 = 13 \* 2 + 10
            5. 13 = 10 \* 1 + 3
            6. 10 = 3 \* 3 + 1
            7. 3 = 1 \* 3 + 0
            8. Now for the coefficients
            9. 1 = 10 – 3 \* 3
            10. 1 = (35 – 13 \* 2) – 3 \* (13 – 10)
            11. 1 = ((153 – (271 - 153)) – (118 – ((153 – (271 - 153))\* 3) \* 2) – 3 \* ((118 – ((153 – (271 - 153))\* 3) \* 2) – ((153 – (271 - 153)) – (118 – ((153 – (271 - 153))\* 3) \* 2)
            12. 1 = 62 \* 153 – 35 \* 271
            13. MI 153 = 62
         2. X = 62 \* 182 mod 271 = 173
   5. 672x ≡ 836 (mod 997)
      1. X = MI(672) \* 836 mod 997
         1. MI 672
            1. 997 = 672 \* 1 + 325
            2. 672 = 325 \* 2 + 22
            3. 325 = 22 \* 14 + 17
            4. 22 = 17 \* 1 + 5
            5. 15 = 5 \* 3 + 2
            6. 5 = 2 \* 2 + 1
            7. 2 = 1 \* 2 + 0
            8. Now for the coefficients
            9. 1 = 5 – 2\* 2
            10. 1 = (22 – 17) – 2 \* (15 – 5 \* 3)
            11. …
            12. MI(672) = 408
         2. X = 408\* 836 mod 997 = 114
4. Simplify the following polynomial expression in *GF*(89)

(54*x*10 − 62*x*9 − 84*x*8 + 70*x*7 − 75*x*6 + *x*5 − 50*x*3 + 84*x*2 + 65*x* + 78) +

(−67*x*9 +44*x*8 −26*x*7 −37*x*6 +61*x*5 +68*x*4 +22*x*3 +74*x*2 +87*x*+38)

54x10−(62+67)x9+(−84+44)x8+(70−26)x7+(−75−37)x6+(1+61)x5+68*x*4

+(−50+22)x3+(84+74)x2+(65+87)x+(78+38)​

Now simplify with modulo

**54x10+49x9+49x8+44x7+66x6+62x5+68*x*4+61x3+69x2+63x+27​**

1. Simplify the following polynomial expression in *GF*(11)

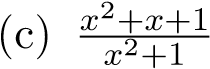
(8*x*3 + 6*x*2 + 8*x* + 1) × (3*x*3 + 9*x*2 + 7*x* + 5)

**24x6+90x5+134x4+157x3+95x2+47x+5**

**Now simplify**

**2x6+2x5+2x4+3x3+7x2+3x+5**

1. For the finite field *GF*(23), simplify the following expressions with modulus polynomial (*x*3 + *x* + 1):
   1. (*x*2 + *x* + 1) × (*x*2 + *x*)
      1. x4+2x3+2x2+x = x4+x
      2. x4+x mod (*x*3 + *x* + 1) = **x2**
   2. *x*2 − (*x*2 + *x* + 1)
      1. *x*2 − (*x*2 + *x* + 1) = -x – 1
      2. – x – 1 mod(2) = **x + 1**



X2 + x + 1/x2+1 = **x**

# Submission Instructions

• You must turn in a single PDF file on Brightspace containing your solutions to the theory questions in section 2. The PDF must have the following naming convention: HW03 *<*last name*> <*first name*>*.pdf. • You are allowed to include scans of handwritten work in the PDF, but please make sure it is legible.

# References

[1] ECE 404 Lecture Notes. URL [https://engineering.purdue.edu/kak/ compsec/Lectures.html.](https://engineering.purdue.edu/kak/compsec/Lectures.html)