ECE404 Introduction to Computer Security: Homework 03

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

1 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.

2 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`
   - `boolean or`
   - `boolean xor`
2. Given W, the set of all unsigned integers, determine whether or not w forms a group under the $gcd(\cdot)$ operator.
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).

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

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)

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

7. Simplify the following polynomial expression in $GF(11)$
   $(8x^3 + 6x^2 + 8x + 1) \times (3x^3 + 9x^2 + 7x + 5)$

8. For the finite field $GF(2^3)$, simplify the following expressions with modulus polynomial $(x^3 + x + 1)$:

   (a) $(x^2 + x + 1) \times (x^2 + x)$

   (b) $x^2 - (x^2 + x + 1)$

   (c) $\frac{x^2+x+1}{x^2+1}$

3 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.