Homework #4

Mathematical Foundations of Modern Cryptography

16 November 2022

Teacher: Andrei Golovanov pnqke

Deadline: Monday, 21st of November, 23:59 MSK

(for MF MC 1.1)

Rules

- For each homework, you must get:
  - 5 points if you send your solution before deadline
  - 8 points if you send your solution after deadline.
- Notice that the tasks in a homework sum up to more than 10–13 points, so you are free to choose which tasks to solve.
- Instead of giving just the final answer, give an explanation of your solution. If you make a program for your solution, give your code.
- If you cannot solve it to the end but you are sure you are on a right way, write your thoughts down, it may give you some points.
- Plagiarism is not allowed!
- Send your solutions to your teacher in any of user-friendly formats. The teacher will give you feedback, and you will probably have to correct your errors or answer some questions in text messages.

Materials

Books

1. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone *Handbook of Applied Cryptography*
   - ch. 2.5.2 Rings
   - ch. 2.5.3 Fields
   - ch. 2.5.4 Polynomial Rings
   - ch. 2.6 Finite Fields
   - ch. 12.7 Secret Sharing
2. Ch. Paar, J. Pelzl *Understanding Cryptography. A Textbook for Students and Practitioners*
   - ch. 4 The Advanced Encryption Standard (AES)
     - ch. 4.3 Some Mathematics: A Brief Introduction to Galois Fields
     - ch. 4.4 Internal Structure of AES
3. R. Lidl, H. Niederreiter *Finite Fields*

Videos

1. Playlist: Abstract Algebra by Socratica — especially those chapters dedicated to rings and fields
2. Secret Sharing Explained Visually by Art of the Problem

Tasks

Task 1 Operating Polynomials (4 points, $\frac{1}{2}$ each exercise)

Solve these exercises. All given polynomials are in $\mathbb{Z}_2[x]$, which means all their coefficients are from $\mathbb{Z}_2$

1. **Addition**. For polynomials

$$f(x) = x^{10} + x^9 + x^5 + x^3 + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

find $f(x) + g(x)$.

2. **Subtraction**. For polynomials

$$f(x) = x^{10} + x^9 + x^5 + x^3 + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

find $f(x) - g(x)$. See the similarity? Explain it.

3. **Multiplication**. For polynomials

$$f(x) = x^{10} + x^9 + x^5 + x^3 + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

find $f(x)g(x)$.

4. **Division**. For polynomials

$$f(x) = x^{10} + x^9 + x^5 + x^3 + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

find quotient polynomial $q(x)$ and remainder polynomial $r(x)$ for dividing $f(x)$ by $g(x)$.

5. **Factorization**. Factorize the polynomial: $f(x) = x^3 + 1$

6. **Multiplication modulo a polynomial**. For polynomials

$$f(x) = x^2 + x + 1$$

$$g(x) = x^3 + 1$$

$$h(x) = x^4 + x + 1$$

   find $f(x)g(x) \bmod h(x)$.

7. **GCD**. For polynomials

$$f(x) = x^5 + x^4 + 1$$

$$g(x) = x^5 + x^2 + x + 1$$

   find $\gcd(f(x), g(x))$ (use Euclidean algorithm for polynomials).

8. **Inversion**. For polynomials

$$f(x) = x^7 + x^4 + x + 1$$

$$g(x) = x^8 + x^4 + x^3 + x + 1$$

   find $f^{-1}(x) \bmod g(x)$ (use Extended Euclidean algorithm for polynomials).

TASK 2 Quiz: Is it a Ring, a Field, or Neither? (5 points in total)

In this task, you have to figure out if a given set under two given operations is a ring or field or neither of them. For each ring and field, show:

- which operation is additive or multiplicative
- its additive identity and multiplicative identity
- its order and characteristic
- is it a commutative ring or not?
- its multiplicative group

I bring you two examples of reasonings:

1. $\mathbb{Z}$ under addition "+" and multiplication "$\cdot$". The $\langle \mathbb{Z}, + \rangle$ is an abelian group, because "+" operation is:
   - closed: the sum of any two integers is an integer
   - associative: $(a + b) + c = a + (b + c)$
   - there exists an identity element 0: $\forall a \in \mathbb{Z} : a + 0 = a$.
   - every integer a has its inverse $-a$: $a + (-a) = 0$
   - commutative: $a + b = b + a$

   The "$\cdot$" operation is:
   - closed: the product of any two integers is an integer
   - associative: $(ab)c = a(bc)$
   - there exists an identity element 1 ($1 \neq 0$): $\forall a \in \mathbb{Z} : a \cdot 1 = a$.
   - distributive over "+": $a(b + c) = ab + ac$; $(b + c)a = ba + ca$.

Hence, $\langle \mathbb{Z}, +, \cdot \rangle$ is a ring, but not a field, because there are elements without multiplicative inverses, for example 2^{-1} is not presented in integer set.

Additive operation: $+$. Multiplicative operation: $\cdot$. Additive identity: 0. Multiplicative identity: 1.

It is a commutative ring, because "$\cdot$" is commutative: $\forall a, b \in \mathbb{Z} : ab = ba$.

Its order $|\mathbb{Z}| = \infty$, characteristic $char(\mathbb{Z}) = 0$, because the sum of m 1's is never a 0 for $m \geq 1$.

Multiplicative group of the ring is the set of all multiplicatively invertible elements, which is $\{1, -1\}$.

2. $\mathbb{Q}$ under addition and multiplication. The $\langle \mathbb{Q}, + \rangle$ is an abelian group (all the reasoning is analogous to the $\mathbb{Z}$ example).

   The "$\cdot$" operation is:

   - closed: the product of any two rationals is a rational
   - associative: $(ab)c = a(bc)$
   - there exists an identity element 1 ($1 \neq 0$): $\forall a \in \mathbb{Q} : a \cdot 1 = a$.
   - distributive over "+": $a(b + c) = ab + ac$; $(b + c)a = ba + ca$.
   - commutative: $\forall a, b \in \mathbb{Q} : ab = ba$
   - every non-zero rational $a = \frac{m}{n}$ is invertible: $a^{-1} = \frac{n}{m}$, so that $a \cdot a^{-1} = \frac{m}{n} \cdot \frac{n}{m} = 1$

   Hence, $\langle \mathbb{Q}, +, \cdot \rangle$ is a field.

   Additive and multiplicative operations and identities, order, and characteristic is identical to the $\mathbb{Z}$ example.

   Multiplicative group of $\langle \mathbb{Q}, +, \cdot \rangle$ is $\mathbb{Q} \setminus \{0\}$.

It might be helpful to recall Task 2 in Homework #2 (*Quiz: Group or Not Group?*). Also, take a look at Menezes' Handbook, chapters 2.5.1–2.5.4 (check the homework's materials).

The exercises:

(a) **($\frac{1}{2}$ points)** Set $\mathbb{Z}_n$ of all remainders modulo n, where n is an integer > 1, under operations:

- addition modulo n
- multiplication modulo n

(b) **($\frac{1}{2}$ points)** Set $\mathbb{Z}_p$ of all remainders modulo p, where p is a prime integer, under operations:

- addition modulo p
- multiplication modulo p

(c) **($\frac{1}{2}$ points)** Set $B = \{0, 1\}$ of Boolean values under operations:

- $\oplus$ (Boolean XOR)
- $\vee$ (Boolean OR)

(d) **($\frac{1}{2}$ points)** Set $B = \{0, 1\}$ of Boolean values under operations:

- $\oplus$ (Boolean XOR)
- $\wedge$ (Boolean AND)

(e) **($\frac{1}{2}$ points)** Set $B_n = \{0, 1\}^n$ of all n-bit binary strings under operations:

- $\oplus$ (bit-wise Boolean XOR)
- $\wedge$ (bit-wise Boolean AND)

(f) **($\frac{1}{2}$ points)** Set $\mathbb{Z}[x]$ of all polynomials $a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k$ (k is not a fixed number) with integer coefficients $a_i \in \mathbb{Z}$ under operations of addition and multiplication.

(g) **($\frac{1}{2}$ points)** Set $\mathbb{Q}[x]$ of all polynomials with rational coefficients (by analogy with previous exercise) under operations of addition and multiplication.

(h) **($\frac{3}{2}$ points)** This exercise is about two sets:

(1) Set $\mathbb{C}$ of complex numbers under operations of addition and multiplication.

(2) Set $\mathbb{C} \setminus \{0\}$ of non-zero complex numbers under operations:

- multiplication
- exponentiation

Task 3 Building $GF(p^m)$ (3 points)

Find all elements of Galois extension field $GF(2^4)$ with a fixed primitive polynomial $p(x) = x^4 + x^3 + 1$. Provide each element in both forms:

- a polynomial representation
- a power of primitive element x.

Task 4 AES internal structure (5 points)

AES (a. k. a. Rijndael) is a symmetric encryption scheme which uses Galois extension field operations.

Learn how two particular parts of AES work: S-box, ShiftRows and MixColumn (use materials for the homework).

Given a block of 16 bytes (hexadecimal representation):

`C877C34FFBEE137354CDCEA531E5F0EE`,

run S-box, ShiftRows and MixColumn on it (**one time only**).

Present all the calculations and provide the final result.

Task 5 Secret Sharing (5 points)

Cryptography is not only fruitful for encryption schemes or digital signatures. There are other wonderful results invented by cryptographers. For example, secret sharing. You can watch the colorful video about it, or you can go through the ch. 12.7 in Menezes' Handbook. Video is for encouraging you, but the book would be more helpful.

In a nutshell, secret sharing a technique for splitting the secret piece of data among a group of n people (called *users*) with some properties:

1. no one knows the secret information
2. they can recover the piece of data when they get together
3. there is a threshold k which means that if there are less then k users, they cannot recover even a bit of the data piece, but k users and more are able to recover the whole piece.

Each user in this scheme has their own *share* — some data which helps to recover the data. The third trusted person who establishes the scheme is called *dealer*.

Such scheme is called (n, k)-secret sharing scheme.

Adi Shamir could find a method to construct such secret sharing scheme, which is based on recovering polynomials in a field.

Let's look at an example. The group of 4 people with their public id's: $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4$ — they wanted to share some secret data $s \in \mathbb{Z}_p$ known by the dealer, using a $(4, 2)$-scheme. It means, that 4 users get their shares, and at least 2 users are necessary to recover the secret.

1. The dealer set the field $\mathbb{Z}_p$, where $p = 13$ is also a public parameter.
2. Also, the dealer generated random coefficient $a \in \mathbb{Z}_p$ for polynomial of degree 1 (the threshold minus 1): $f(x) = ax + s$. Note that $s = f(0)$.

3. Next, dealer calculated users' shares: $y_i = f(x_i)$ for $i = 1..4$.
4. The values y_i were transferred to the corresponding users through some secret channel.

Which shares the users have at the end of scheme establishing:

$$\begin{aligned}(x_1, y_1) &= (1, 10)\\(x_2, y_2) &= (2, 12)\\(x_3, y_3) &= (3, 8)\\(x_4, y_4) &= (4, 4)\end{aligned}$$

One of the users is trying to fool everyone, and changed the y_i value in order to get the wrong secret after recovering procedure. The task for you is to find the liar.

I am reminding you how you can find a formula $y = f(x)$ of a line given two points $(x_1, y_1), (x_2, x_2)$ of the line. It might help you:

$$y - y_1 = m(x - x_1),$$

where m is the slope of the line:

$$m = \frac{y_1 - y_2}{x_1 - x_2}.$$

(But remember we are working with $\mathbb{Z}_p$, not $\mathbb{R}$)