CSCI-4116
Assignment 2

Anas Alhadi

B00895875

January 24, 2025

Question 1

Part a)

We know that a residue class $a + m\mathbb{Z}$ is invertible iff $gcd(a, m) = 1$. Thus only the classes represented by $\{1, 3, 5, 7, 9, 11, 13, 15\}$ are invertible.

Given a residue class $a + m\mathbb{Z}$ the inverse is a residue class $a^{-1} + m\mathbb{Z}$ such that $a \times a^{-1} \equiv 1 (\text{mod } 16)$.[1] So we have it that:

- $1 \times 1 \quad \equiv 1 (\text{mod } 16)$
- $3 \times 11 \quad \equiv 1 (\text{mod } 16)$
- $5 \times 13 \quad \equiv 1 (\text{mod } 16)$
- $7 \times 7 \quad \equiv 1 (\text{mod } 16)$
- $9 \times 9 \quad \equiv 1 (\text{mod } 16)$
- $15 \times 15 \quad \equiv 1 (\text{mod } 16)$

aside: The format $x \times y \equiv 1 (\text{mod } m)$ just means that $y + m\mathbb{Z}$ is the inverse of $x + m\mathbb{Z}$ and vise versa. Since $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ is a commutative monoid we know that $a \cdot a^{-1} = a^{-1} \cdot a$.

[1] I'm using the euclidean algorithm to find a^{-1} but immiting the steps

Part b)

Group of Units

The group of units is the group of all invertible residue classes, and thus, is the group of all residue classes $a + 15\mathbb{Z}$ where $gcd(a, 15) = 1$. Then given the inverses(similar to partA):

- $1 \times 1 \quad \equiv 1 (\text{mod } 15)$
- $2 \times 8 \quad \equiv 1 (\text{mod } 15)$
- $4 \times 4 \quad \equiv 1 (\text{mod } 15)$
- $7 \times 13 \quad \equiv 1 (\text{mod } 15)$
- $11 \times 11 \quad \equiv 1 (\text{mod } 15)$
- $14 \times 14 \quad \equiv 1 (\text{mod } 15)$

We have it that $(\mathbb{Z}/15\mathbb{Z})^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Zero Divisors:

We know that the zero divisors of $\mathbb{Z}/m\mathbb{Z}$ are the residue classes where $1 < gcd(a, m) < m$. This means that the zero divisors is the set of all residue classes that are not in $(\mathbb{Z}/m\mathbb{Z})^*$ and not the class $0 + m\mathbb{Z}$. For $m = 15$ the zero divisors are:

- $3 + 15\mathbb{Z}$
- $5 + 15\mathbb{Z}$
- $6 + 15\mathbb{Z}$
- $9 + 15\mathbb{Z}$
- $10 + 15\mathbb{Z}$
- $12 + 15\mathbb{Z}$

Question 2

b) is cryptosystem while a) is not.

Reason:

Recall that one properity of a cryptosystem is that for all encryption keys in the keyspace there must exist a decryption key such that decrypting the encryption returns the original plain text.
In the context of the provided scheme, the mapping from $x(\text{mod } m) \mapsto kx(\text{mod } m)$ can be reversed by multiplying k with its inverse in modulo m.
Since scheme a) puts no restrictions on k this means that all keys in the keyspace must be invertible in m, which is only true when m is a prime number, and 26 is clearly not. Thus there exists a key where its inverse, k^{-1}, is not uniquely identifiable. Therefore there is no gaurentee that $\mathcal{D}_{k^{-1}}(\mathcal{E}_k(p)) = p$, thus the properity is not satisfied. (The restriction in scheme b gaurentees that all keys are invertible).

Cryptosystem's details: (scheme b)

- Plaintext Space: $\mathbb{Z}_{26}$
- Ciphertext Space: $\mathbb{Z}_{26}$
- Key Space: $\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25\}$. [2]

Question 3

1. $\varphi(2024) = 880$
2. $\varphi(2025) = 1080$
3. $\varphi(8958) = 2984$

[3]

[2] any value in $(\mathbb{Z}/26\mathbb{Z})^*$ is a valid key for the mapping.
[3] I wrote a C++ program to calculate Question 3 this for me

Question 4

Plain and Cipher Spaces:

The plain and cipher text can be any string over Σ. Thus the Plain text and Cipher text space is the set of all possible strings over the alphabet, denoted as Σ^*

aside:

The alphabet $\Sigma = \{A..Z\}$ can be mapped to integers $\mathbb{Z}_{26} = \{0..25\}$ in lexigraphical order.

Encryption and Decryption Functions

The described encryption and decryption procedures can each be represented as the composition of 2 functions:

- Encryption: function $\mathcal{E}'$ that shifts symbols and a function R that reverses a sequence
- Decryption: function R that reverses a sequence and a function $\mathcal{D}'$ that shifts symbols

First, let a string/sequence $X = \{x_i\}_{i=1}^n$

We now define the functions $\mathcal{E}', \mathcal{D}'$ and R as follows :

$$\mathcal{E}'_{k_1,k_2}(X): \quad \begin{array}{ll} x_i + k_2 (\text{mod } 26), & i|2 \\ x_i + k_1 (\text{mod } 26), & \text{otherwise} \end{array}$$

$$\mathcal{D}'_{k_1,k_2}(X): \quad \begin{array}{ll} x_i - k_2 (\text{mod } 26), & i|2 \\ x_i - k_1 (\text{mod } 26), & \text{otherwise} \end{array}$$

$$R(X): \qquad x_i = x_{n-i+1}$$

We can now write the Encryption and Decryption functions as:

$$\mathcal{E} = \mathcal{E}'_{k_1,k_2} \circ R$$

$$\mathcal{D} = R \circ \mathcal{D}'_{k_1,k_2}$$

Key Space:

Observe that the symbols and the operations $\mathcal{E}'$ and $\mathcal{D}'$ that we perform on them is just the group $(\mathbb{Z}/m\mathbb{Z}, +)$ with $m = 26$. So the inverse of any $k(\text{mod } 26)$ is $-k(\text{mod } 26)$. This means that any integer value of k is a valid key. Thus the keyspace is $\mathbb{Z}_{26}$.

Conclusion:

Since the procedure has:

1. a Plain text space
2. a Cipher text space
3. a Key space

4. an Encryption Function
5. a Decryption Function
6. Satisfies that $\mathcal{D}(\mathcal{E}(p)) = p$ (since all keys are invertible)

This means that it is a valid cryptosystem as it satisfies all the properities of one.

Question 5

Given the encryption function:

$$\mathcal{E}(x) = ax + b (\text{mod } m)$$

And the restriction that a needs to have a multiplicative inverse in m, we have it that for:

- **m=30:**

  $b \in \mathbb{Z}_{30}$ so b can have 30 different values
  $a \in (\mathbb{Z}/30\mathbb{Z})^*$ so a can have $\varphi(30) = 8$

  Thus there are $30 * 8 = 240$ possible keys

- **m=29:**

  $b \in \mathbb{Z}_{29}$ so b can have 29 different values
  $a \in (\mathbb{Z}/29\mathbb{Z})^*$ so a can have $\varphi(29) = 28$

  Thus there are $29 * 28 = 812$ possible keys