Question Number 5

A key is called involutory when $e_K = d_K$. Let an Affine Cipher be defined over $\mathbb{Z}_m$ with key $K = (a, b)$.

- Prove that K is an involutory key if and only if

$$a^{-1} \mod m = a \ \ \& \ \ b(a+1) \equiv 0 \mod m$$

- Now find all involutory keys in $\mathbb{Z}_{15}$ for the Affine Cipher
- Determine the number of keys in an Affine Cipher over $\mathbb{Z}_m$ for $m = 30, 100$ and 1225.

Solution.

Part1

Let an Affine Cipher be defined over $\mathbb{Z}_m$ with key $K = (a, b)$. We want to prove that K is an involutory key if and only if $a^{-1} \bmod m = a$ and $b(a + 1) \equiv 0 \pmod m$.

Proof

An Affine Cipher's encryption and decryption functions can be written as:

$$e_K(x) = (ax + b) \bmod m$$

$$d_K(y) = a^{-1}(y - b) \bmod m$$

For K to be involutory, applying the encryption function twice should result in the original plaintext x. This implies that:

$$e_K(e_K(x)) \equiv x \pmod m$$

Let's apply the encryption function twice:

$$e_K(e_K(x)) = e_K(ax + b) = a(ax + b) + b \bmod m$$
$$= (a^2x + ab + b) \bmod m$$

For K to be involutory, this expression must equal x modulo m:

$$a^2x + ab + b \equiv x \pmod m$$

Since this equation must hold for all $x \in \mathbb{Z}_m$, we can equate the coefficients of x and the constant terms separately:

$$a^2 \equiv 1 \pmod m$$

$$ab + b \equiv 0 \pmod m$$

Step 1: Analyzing $a^2 \equiv 1 \pmod{m}$

The equation $a^2 \equiv 1 \pmod{m}$ implies that a is a square root of 1 modulo m. The solutions to this equation are:

$$a \equiv 1 \pmod{m} \quad \text{or} \quad a \equiv m-1 \pmod{m}$$

Furthermore, from $a^2 \equiv 1 \pmod{m}$, we also have:

$$a \equiv a^{-1} \pmod{m}$$

This means that a must be its own inverse modulo m, i.e., $a^{-1} = a$.

Step 2: Analyzing $ab + b \equiv 0 \pmod{m}$

We can factor the second equation as:

$$b(a+1) \equiv 0 \pmod{m}$$

This implies that $b(a+1)$ is divisible by m. Therefore, for the equation to hold:

- If $a+1$ is not divisible by m, then b must be 0 modulo m.
- If $a+1 \equiv 0 \pmod{m}$ (i.e., $a \equiv m-1 \pmod{m}$), then b can be any value in $\mathbb{Z}_m$.

Conclusion

Combining these results, we conclude that $K = (a, b)$ is an involutory key if and only if:

$$a^{-1} \equiv a \pmod{m} \quad \text{and} \quad b(a+1) \equiv 0 \pmod{m}$$

Part 2

Finding All Involutory Keys in $\mathbb{Z}_{15}$ for the Affine Cipher

We need to find all values of a and b such that the key $K = (a, b)$ is involutory in $\mathbb{Z}_{15}$. For the key K to be involutory, it must satisfy:

$$a^{-1} \equiv a \pmod{15}$$

$$b(a+1) \equiv 0 \pmod{15}$$

First, we determine all values of a such that:

$$a^2 \equiv 1 \pmod{15}$$

This can be rewritten as:

$$a^2 - 1 \equiv 0 \pmod{15} \implies (a-1)(a+1) \equiv 0 \pmod{15}$$

We test values in $\mathbb{Z}_{15}$:

$$a = 1 \quad \text{and} \quad a = 14$$

These values satisfy:

$$1^2 \equiv 1 \pmod{15} \quad \text{and} \quad 14^2 \equiv 196 \equiv 1 \pmod{15}$$

Next, we find the corresponding values of b for each a such that:

$$b(a+1) \equiv 0 \pmod{15}$$

- For $a = 1$:

  $$b(1+1) = 2b \equiv 0 \pmod{15}$$

  This implies:

  $$2b \equiv 0 \pmod{15}$$

  The solutions are $b = 0$ (as $2b = 0$ in $\mathbb{Z}_{15}$).

- For $a = 14$:

  $$b(14+1) = 15b \equiv 0 \pmod{15}$$

  This is always satisfied for any $b \in \mathbb{Z}_{15}$ because $15b$ is always 0 modulo 15.

Thus, the involutory keys in $\mathbb{Z}_{15}$ are:

$$(1, 0) \quad \text{and} \quad (14, b) \text{ for all } b \in \mathbb{Z}_{15}$$

Note that $b = 15$ is equivalent to $b = 0$ modulo 15.

Part3

Determining the Number of Keys in an Affine Cipher over $\mathbb{Z}_m$ for $m = 30, 100,$ and 1225

The number of keys (a, b) for an Affine Cipher over $\mathbb{Z}_m$ is given by the product of the number of possible values for a and b. Specifically:

- a must be coprime to m (i.e., $\gcd(a, m) = 1$). - b can be any value in $\mathbb{Z}_m$, so there are m possible values for b.

The number of possible values for a is given by $\phi(m)$, where ϕ is the Euler's totient function.

- **For $m = 30$:**
$$\phi(30) = \phi(2 \cdot 3 \cdot 5) = (2-1)(3-1)(5-1) = 1 \cdot 2 \cdot 4 = 8$$
Thus, the number of keys is:
$$\phi(30) \times 30 = 8 \times 30 = 240$$

- **For $m = 100$:**
$$\phi(100) = \phi(2^2 \cdot 5^2) = (2^2 - 2^1)(5^2 - 5^1) = 2 \cdot 20 = 40$$
Thus, the number of keys is:
$$\phi(100) \times 100 = 40 \times 100 = 4000$$

- **For $m = 1225$:**
$$\phi(1225) = \phi(5^2 \cdot 7^2) = (5^2 - 5^1)(7^2 - 7^1) = 20 \cdot 42 = 840$$
Thus, the number of keys is:
$$\phi(1225) \times 1225 = 840 \times 1225 = 1029000$$

To find ϕ function values use pytyhon code from `eulerTotient.py`