Assignment 3

Konstantinos Filippou
ics23044

Exercise 1

Compute the following modular arithmetic expressions by hand:

$7\cdot 14 \pmod{11}, \quad 7\cdot 14 \pmod{13}, \quad 4\cdot 3 \pmod{12}, \quad -4\cdot 23 \pmod{21}, \quad 2^{10} \pmod{2}$

Solution

$$7 \cdot 14 = 98 \Rightarrow 98 = 8 \cdot 11 + 10$$
$$7 \cdot 14 \equiv 10 \pmod{11}$$

$$98 = 7 \cdot 13 + 7$$
$$7 \cdot 14 \equiv 7 \pmod{13}$$

$$4 \cdot 3 = 12 \Rightarrow 12 \equiv 0 \pmod{12}$$

$$-4 \cdot 23 = -92$$
$$-92 + 105 = 13$$
$$-4 \cdot 23 \equiv 13 \pmod{21}$$

$$2^{10} = 1024$$
$$1024 \equiv 0 \pmod{2}$$

Exercise 2

Find the multiplicative inverse of 5 in the rings $\mathbb{Z}_5$, $\mathbb{Z}_{25}$, and $\mathbb{Z}_{38}$.

Solution

In $\mathbb{Z}_5$ and $\mathbb{Z}_{25}$:

$$\gcd(5,5) = 5, \quad \gcd(5,25) = 5$$

Since the gcd is not 1, no multiplicative inverse exists.

In $\mathbb{Z}_{38}$:

$$\gcd(5,38) = 1$$

Using the Extended Euclidean Algorithm:

$$1 = 23 \cdot 5 - 3 \cdot 38$$

Thus:

$$5^{-1} \equiv 23 \pmod{38}$$

Verification:

$$5 \cdot 23 = 115 \equiv 1 \pmod{38}$$

The inverse depends on the modulus. Without specifying the modulus, the notion of inverse is meaningless.

The inverse is efficiently computed using the Extended Euclidean Algorithm.

Exercise 3

Compute Euler's phi function $\varphi(m)$ for:

$$m = 9, 17, 25, 33$$

Solution

For $m = 9$:

$$9 = 3^2$$

$$\varphi(9) = 9\left(1 - \frac{1}{3}\right) = 6$$

Relatively prime integers:

$$\{1, 2, 4, 5, 7, 8\}$$

For $m = 17$:

$$17 \text{ prime} \Rightarrow \varphi(17) = 16$$

For $m = 25$:

$$25 = 5^2$$

$$\varphi(25) = 25\left(1 - \frac{1}{5}\right) = 20$$

For $m = 33$:

$$33 = 3 \cdot 11$$

$$\varphi(33) = 33\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right) = 20$$

Exercise 4

Explain why the algebraic structures (Q, Δ) and $(P, \Diamond)$ are not groups.

Solution

For (Q, Δ):

- The operation is closed.
- There is no identity element.

Therefore inverses cannot exist and the structure is not a group.
For $(P, \Diamond)$:

- The operation is closed.
- There exists an identity element p_1.
- Inverses exist.

However, associativity fails:

$$(p_2 \Diamond p_2) \Diamond p_3 \neq p_2 \Diamond (p_2 \Diamond p_3)$$

Therefore $(P, \Diamond)$ is not a group.

Exercise 5

Affine cipher:

$$e_k(m) = k_1 m + k_2 \pmod{p}$$

$$d_k(c) = k_1^{-1}(c - k_2) \pmod{p}$$

Given:

$$p = 541, \quad k = (34, 71)$$

Encryption of $m = 204$

$$34 \cdot 204 + 71 = 7007$$

$$7007 \equiv 515 \pmod{541}$$

$$e_k(204) = 515$$

Decryption of $c = 431$

Using Extended Euclidean Algorithm:

$$34^{-1} \equiv 366 \pmod{541}$$

$$\begin{aligned} d_k(431) &= 366(431 - 71) \pmod{541} \\ &= 366 \cdot 360 \equiv 297 \pmod{541} \end{aligned}$$

Vulnerability

Two plaintext–ciphertext pairs are sufficient to recover the key, provided the difference of plaintexts is invertible modulo p.

Case $p = 601$

Solving the system yields:

$$k_1 = 41, \quad k_2 = 83$$

Encrypting $m_3 = 173$:

$$c_3 = 173 \cdot 41 + 83 \equiv 565 \pmod{601}$$

Exercise 6

For a successful Known Plaintext Attack (KPA), the key must be reused.

Case 1:

$$E \to M, \quad L \to V$$

Solving:

$$k_1 = 5, \quad k_2 = 18$$

Case 2:

$$M \to R, \quad Y \to V$$

This yields:

$$8k_1 \equiv 4 \pmod{26}$$

Since $\gcd(8, 26) \neq 1$, no inverse exists and no valid key can be recovered.

Improvement

Before inversion, check:

$$\gcd(k_1, 26) = 1$$