

# HW # 4

## Solution

1. (10 points) Examining the ring  $Z_m$ .

- (a) Find the additive inverse of all elements in  $Z_7$ .

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

element $a$	0	1	2	3	4	5	6
additive inverse $-a$	0	6	5	4	3	2	1

- (b) Which elements in  $Z_7$  and  $Z_{26}$  do have multiplicative inverses?

For  $Z_7$  these are 1, 2, 3, 4, 5, 6

For  $Z_{26}$  these are 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

- (c) What are the multiplicative inverses of all those elements in  $Z_{26}$ ? It is OK to use trial and error for finding the inverses.

$$Z_{26} \rightarrow 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$$

element $a$	1	3	5	7	9	11	15	17	19	21	23	25
multiplicative inverse $a^{-1}$	1	9	21	15	3	19	7	23	11	5	17	25

2. (2 points) What is the key space of the affine cipher?

$$26 \cdot 12 = 312$$

The key space of the affine cipher is 312 keys.

3. (10 points) Break the following ciphertext, knowing that it has been obtained by encrypting a short English message using the affine cipher:

TPOPE BFOKT TPYRG YRTPO UABZF TACRF OBKTE RFYKT POYRW AIOTE  
DOYRK TOYR

Please note that all spaces and punctuation characters have been removed from the message before encryption, and the letters of the ciphertext have been arranged for convenience and increased readability in the groups of five characters.

Please use the analytical method (i.e., for each possible hypothesis regarding the possible frequency of letters in a short English message, form and solve a set of two equations with two unknown). Use tables you have developed as a solution to the previous Problem to confirm or reject each hypothesis, and recover the correct key.

**Please note that an exhaustive key search attack, i.e., trying all possible keys, or solutions to the equations, one by one, using a computer, will not be accepted as a valid solution.**

The most common letter in a long English text is ‘E’ followed by ‘T’. In this short ciphertext the most frequent letter is ‘T’ followed by ‘O’. This would yield the following mapping:

$$\begin{aligned} E &\rightarrow T \\ T &\rightarrow O \end{aligned}$$

However, in this short text it turns out that ‘T’ is the most frequent letter followed by ‘E’ which yields this mapping:

$$\begin{aligned} E &\rightarrow O \\ T &\rightarrow T \end{aligned}$$

or in numbers

$$\begin{aligned} 4 &\rightarrow 14 \\ 19 &\rightarrow 19 \end{aligned}$$

This results in two equations for the affine cipher with two unknowns:

$$4 \cdot k_1 + k_2 \equiv 14 \pmod{26}$$

$$19 \cdot k_1 + k_2 \equiv 19 \pmod{26}$$

subtracting the first equation from the second:

$$15 \cdot k_1 \equiv 5 \pmod{26},$$

We need the multiplicative inverse of 15 mod 26 which we get from the table from question 1c) as 7.

$$k_1 = 5 \cdot 7 \equiv 9 \pmod{26}$$

Now we enter  $k_1$  into one of the two equations and get the value for  $k_2$ .

$$4 \cdot 9 + k_2 \equiv 14 \pmod{26}$$

$$k_2 = 14 - 36 \equiv 4 \pmod{26}$$

4. (8 points) Using the basic form of Euclid’s algorithm, compute the greatest common divisor of the following numbers. Write down every step.

(a) 4891 and 2847

$$4891 = 1 \cdot 2847 + 2044$$

$$2847 = 1 \cdot 2044 + 803$$

$$2044 = 2 \cdot 803 + 438$$

$$803 = 1 \cdot 438 + 365$$

$$438 = 1 \cdot 365 + 73$$

$$365 = 5 \cdot 73 + 0$$

$$\gcd(4891, 2847) = 73$$

(b) 5457 and 1823

$$5457 = 2 \cdot 1823 + 1811$$

$$1823 = 1 \cdot 1811 + 12$$

$$1811 = 150 \cdot 12 + 11$$

$$12 = 1 \cdot 11 + 1$$

$$11 = 11 \cdot 1 + 0$$

$$\gcd(5457, 1823) = 1$$

5. (10 points) Using the extended Euclidean algorithm to compute the inverse of elements  $\alpha$  in  $Z_m$ . Write down every step.

(a)  $a = 5, m = 34$

$$s \cdot 34 + t \cdot 5 = \gcd(34, 5)$$

$$34 = 6 \cdot 5 + 4 \quad q = 6 \quad s = 1 - 6 \cdot 0 = 1 \quad t = 0 - 6 \cdot 1 = -6$$

$$5 = 1 \cdot 4 + 1 \quad q = 1 \quad s = 0 - 1 \cdot 1 = -1 \quad t = 1 - 1 \cdot -6 = 7$$

$$\gcd(34, 5) = 1, \quad t = 7 \equiv 5^{-1} \pmod{34}$$

(b)  $a = 34, m = 283$

$$s \cdot 283 + t \cdot 34 = \gcd(283, 34)$$

$$283 = 8 \cdot 34 + 11 \quad q = 8 \quad s = 1 - 8 \cdot 0 = 1 \quad t = 0 - 8 \cdot 1 = -8$$

$$34 = 3 \cdot 11 + 1 \quad q = 3 \quad s = 0 - 3 \cdot 1 = -3 \quad t = 1 - 3 \cdot -8 = 25$$

$$\gcd(283, 34) = 1, \quad t = 25 \equiv 34^{-1} \pmod{283}$$