Homework 4

Eli Bullock-Papa

March 24, 2025

Problem 1

Determine the involutory keys in the affine cipher mod 26.

Solution:
For the affine cipher with key (a, b), the encryption function is:

$$E(x) = ax + b \bmod 26$$

But for involutory keys, the encryption function is the same as the decryption function, so encrypting twice returns the original message, meaning:

$$E(E(x)) = x$$

So we do this for the encryption function:

$$E(E(x)) = a(ax + b) + b \bmod 26 = a^2x + ab + b \bmod 26 \equiv x \pmod{26}$$

Then subtracting x from both sides, we get:

$$a^2x + ab + b - x \equiv 0 \pmod{26}$$

Then grouping the terms, we get:

$$(a^2 - 1)x + (ab + b) \equiv 0 \pmod{26}$$

Now we know that both:

$$a^2 - 1 \equiv 0 \pmod{26}$$
$$ab + b \equiv 0 \pmod{26}$$

First, let's solve for a in the equation $a^2 - 1 \equiv 0 \pmod{26}$ we must check for all possible values of a (note that a must be coprime to 26):

$$\begin{aligned}
1^2 &\equiv 1 \pmod{26} \quad \checkmark \\
3^2 = 9 &\not\equiv 1 \pmod{26} \\
5^2 = 25 &\not\equiv 1 \pmod{26} \\
7^2 = 49 \equiv 23 &\not\equiv 1 \pmod{26} \\
9^2 = 81 \equiv 3 &\not\equiv 1 \pmod{26} \\
11^2 = 121 \equiv 17 &\not\equiv 1 \pmod{26} \\
15^2 = 225 \equiv 17 &\not\equiv 1 \pmod{26} \\
17^2 = 289 \equiv 3 &\not\equiv 1 \pmod{26} \\
19^2 = 361 \equiv 23 &\not\equiv 1 \pmod{26} \\
21^2 = 441 \equiv 25 &\not\equiv 1 \pmod{26} \\
23^2 = 529 \equiv 9 &\not\equiv 1 \pmod{26} \\
25^2 = 625 \equiv 1 &\equiv 1 \pmod{26} \quad \checkmark
\end{aligned}$$

If we assume that $a = 1$ in the equation $ab + b \equiv 0 \pmod{26}$:

$$(1)b + b \equiv 0 \pmod{26}$$

$$2b \equiv 0 \pmod{26}$$

$$b \equiv 0 \pmod{26} \text{ } or \text{ } b \equiv 13 \pmod{26}$$

If we assume that $a = 25$ in the equation $ab + b \equiv 0 \pmod{26}$:

$$(25)b + b \equiv 0 \pmod{26}$$

$$26b \equiv 0 \pmod{26}$$

$$b \in \mathbb{Z}_{26}$$

Therefore, the complete set of involutory keys (a, b) for the affine cipher mod 26 is:

$$\{(1, 0), (1, 13)\} \cup \{(25, b) : b \in \mathbb{Z}_{26}\}$$

Problem 2

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 4 & 2 & 8 & 6 & 5 & 9 & 1 \end{pmatrix}$

(a) Write σ in one-row (cycle) notation.

$$\sigma = (1\ 7\ 5\ 8\ 9)(2\ 3\ 4)(6)$$

(b) What is the cycle type of σ?

The cycle type of σ is $[5, 3, 1]$.

(c) Write σ as a composition of (not necessarily disjoint) transpositions.

$$\sigma = (1\ 9)(1\ 8)(1\ 5)(1\ 7)(2\ 4)(2\ 3)$$

(d) Is σ an even permutation or an odd permutation?

Even, as it is composed of 6 transpositions.

(e) Is σ an involution?

No, as it violates the condition that the cycle decomposition must consist of only transpositions and fixed points.

(f) Now, let $\alpha = (1\,4\,8\,5)(1\,3\,6\,7)(2\,9)$. Compute the conjugate of σ by α.

Since these are not disjoint cycles, we can simplify into one mapping:

$$\text{Let } \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 6 & 8 & 1 & 7 & 4 & 5 & 2 \end{pmatrix}$$

That can also be written as:

$$\alpha = (1\ 3\ 6\ 7\ 4\ 8\ 5)(2\ 9)$$

Now we assemble $\alpha\sigma\alpha^{-1}$:

$$\sigma = (1\ 7\ 5\ 8\ 9)(2\ 3\ 4)(6)$$

$$\alpha^{-1} = (9\ 2)(5\ 8\ 4\ 7\ 6\ 3\ 1)$$

$$\alpha\sigma\alpha^{-1} = (1\ 3\ 6\ 7\ 4\ 8\ 5)(2\ 9)(1\ 7\ 5\ 8\ 9)(2\ 3\ 4)(6)(9\ 2)(5\ 8\ 4\ 7\ 6\ 3\ 1)$$

We can use the trick from Theorem 5.1 to match the cycles in σ to the conjugate and get:

$$\alpha\sigma\alpha^{-1} = (3\ 4\ 1\ 5\ 2)(9\ 6\ 8)(7)$$

(g) Is $\sigma\alpha\sigma\alpha^{-1}$ of matched cycle type? Explain why or why not.

$$\sigma = (1\ 7\ 5\ 8\ 9)(2\ 3\ 4)(6)$$

$$\alpha\sigma\alpha^{-1} = (3\ 4\ 1\ 5\ 2)(9\ 6\ 8)(7)$$
$$\sigma\alpha\sigma\alpha^{-1} = (1\ 7\ 5\ 8\ 9)(2\ 3\ 4)(6)(3\ 4\ 1\ 5\ 2)(9\ 6\ 8)(7)$$
$$\sigma\alpha\sigma\alpha^{-1} = (1\ 8)(2\ 4\ 7\ 5\ 3)(6\ 9)$$

The cycle type is $[5, 2, 2]$ which is not matched (no match for the cycle of length 5).