Exercise 4. Consider the following function:

\[ E : \{0, 1\}^4 \rightarrow \{0, 1\}^4, \quad m_1m_2m_3m_4 \mapsto E(m_1m_2m_3m_4) = c_1c_2c_3c_4, \]

where \( c_1, c_2, c_3, c_4 \) are calculated as follows:

\[ C = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} = A \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} + B. \]

The matrices \( A \) and \( B \) are of the form

\[ A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathbb{Z}_{2}^{2 \times 2} \]

and

\[ B = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \in \mathbb{Z}_{2}^{2 \times 2}. \]

The function \( E \) can be used to construct an encryption function \( e \) for a cryptosystem with \( X = Y = \{0, 1\} \). In this system each block of 4 Bits is encrypted using the function \( E \). The key of the system is \((A, B)\).

(a) Which properties do the matrices \( A \) and \( B \) have to fulfill in such a system? How many pairs \((A, B)\) of the given form exist with these properties?

(b) Encrypt the Bitstring

\[ 1001101111000100 \]

with the key \( A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \) and \( B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \).

Exercise 5.

(a) Prove the following statement:

A matrix \( A \in \mathbb{Z}_m^{n \times n} \) is invertible, if and only if \( \gcd(m, \det(A)) = 1 \).

(b) Is the following matrix invertible? If yes, compute the inverse matrix.

\[ M = \begin{pmatrix} 7 & 1 \\ 9 & 2 \end{pmatrix} \in \mathbb{Z}_{26}^{2 \times 2}. \]

Exercise 6. Show that the set of regular \( n \times n \) matrices over a field \( K \) together with the usual matrix multiplication is a group. Is it an abelian group?