Math 418/818

Assignment 3 - Solutions

[5] 1. Recall from class that the deciphering function is \( f^{-1}(\vec{x}) = A^{-1}(\vec{x}) - \vec{c}, \) where \( \vec{c} = A^{-1}\vec{b}. \) To find \( A^{-1} \in \text{GL}_2(\mathbb{Z}/26\mathbb{Z}) \), we row reduce the \( 3 \times 6 \) matrix \((A|I)\) to reduced row echelon form to get \((I|A^{-1}). \) This row reduction has to be done in \( \mathbb{Z}/26\mathbb{Z}. \) Note that \( 1/3 = 9 \) in \( \mathbb{Z}/26\mathbb{Z} \) because \( 3 \cdot 9 = 27 \equiv 1 \pmod{26}. \)

\[
(A|I) = \begin{pmatrix}
1 & 0 & 2 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & 0 & 2 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & -3 & 1 & 0 & 1 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & 0 & 2 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & -9 \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
1 & 0 & 0 & 9 & 0 & 18 \\
0 & 1 & 0 & -9 & 1 & 9 \\
0 & 0 & 1 & 9 & 0 & -9 \\
\end{pmatrix}.
\]

Thus, \( A^{-1} = \begin{pmatrix} 9 & 0 & 18 \\ -9 & 1 & 9 \\ 9 & 0 & -9 \end{pmatrix} \) and hence \( \vec{c} = A^{-1}\vec{b} = \begin{pmatrix} 9 & 0 & 18 \\ -9 & 1 & 9 \\ 9 & 0 & -9 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 63 \\ 20 \\ -18 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 20 \\ 8 \end{pmatrix} \pmod{26}. \)

Thus, if we write \( \vec{x} = (x_1, x_2, x_3), \) then the deciphering function is given by

\[
f^{-1}(\vec{x}) \equiv (9x_1 + 18x_3 - 11, x_2 - 9x_1 + 9x_3 - 20, 9x_1 - 9x_3 - 8) \pmod{26},
\]

because

\[
f^{-1}(\vec{x}) = A^{-1}\vec{x} - \vec{c} = \begin{pmatrix} 9 & 0 & 18 \\ -9 & 1 & 9 \\ 9 & 0 & -9 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} - \begin{pmatrix} 11 \\ 20 \\ 8 \end{pmatrix} = \begin{pmatrix} 9x_1 + 18x_3 - 11 \\ x_2 - 9x_1 + 9x_3 - 20 \\ 9x_1 - 9x_3 - 8 \end{pmatrix}.
\]

Applying this to the message \( \vec{y} = (9, 24, 9) \) (which corresponds to JYJ), we get \( f^{-1}(\vec{y}) = (70, 4, -8) \equiv (24, 4, 18) \pmod{26}. \) This corresponds to the message YES.

[4] 2. (a) View \( A \) as a matrix in \( M_2(\mathbb{Q}) \), and let \( L_A^Q : \mathbb{Q}^2 \rightarrow \mathbb{Q}^2 \) be the associated linear map. Since \( \det(A) = 1 \cdot 4 - 2 \cdot 3 = -2 \neq 0, \) we know by basic Linear Algebra (or by the Lemma in class) that \( L_A^Q \) is an isomorphism. Thus \( L_A^Q \) is injective, and hence so is its restriction \( L_A = (L_A^Q)|_{\mathbb{Z}^2} \) to \( \mathbb{Z}^2. \) This proves the first assertion.

To see that \( L_A \) is not injective, consider \( \vec{v} = (1, 0). \) We have that \( \vec{v} \notin \text{Im}(L_A) \) because otherwise there exist \( x, y \in \mathbb{Z} \) such that \( A(x, y) = (1, 0), \) so \( x + 2y = 1 \) and \( 3x + 4y = 0. \) Thus \( x = 1 - 2y \) and so \( 3 - 6y + 4y = 0 \) or \( 2y = 3, \) which is impossible because \( 2 \nmid 3. \) Thus, \( \vec{v} \notin \text{Im}(L_A) \) and hence \( L_A \) is not surjective.

(b)* If \( L_A \) is surjective, then there exist \( \vec{e}_1, \ldots, \vec{e}_n \in \mathbb{R}^n \) such that \( L_A(\vec{e}_i) = \vec{e}_i, \) where \( \vec{e}_1, \ldots, \vec{e}_n \) is the standard basis of \( \mathbb{R}^n. \) Thus, there is a matrix \( B \in \mathbb{R}^n \) such that \( B(\vec{e}_i) = \vec{e}_i, \) for \( 1 \leq i \leq n. \) Since \( L_{AB}(\vec{e}_i) = L_A(L_B(\vec{e}_i)) = L_A(\vec{e}_i) = \vec{e}_i, \) it follows that \( L_{AB} = \text{id} \) and so \( AB = I. \) Thus \( \det(A) \det(B) = \text{det}(AB) = \text{det}(I) = 1, \) and so \( \det(A) \in \mathbb{R}^\times. \) By the Lemma in class we know that \( A \) is invertible.

Thus, by the above we see that if \( L_A \) is surjective, then \( A \) is invertible and hence \( L_A \) is an isomorphism (by the Lemma in class). Conversely, if \( L_A \) is an isomorphism, then it is bijective, and hence surjective, and so the last assertion follows.

(c)* (i) \( L_A \) is surjective if and only if \( \det(A) = \pm 1. \)

Indeed, by part (b) we know that \( L_A \) is surjective \( \iff \) \( L_A \) is an isomorphism \( \iff \) \( \det(A) \in \mathbb{R}^\times, \) the latter by the Lemma in class. Since \( \mathbb{R}^\times = \{ \pm 1 \}, \) assertion (i) follows.

(ii) \( L_A \) is injective if and only if \( \det(A) \neq 0. \)

Recall from basic linear algebra that \( \det(A) \neq 0 \iff L_A^Q : \mathbb{Q}^n \rightarrow \mathbb{Q}^n \) is injective. Thus, it is enough to show that \( L_A \) is injective \( \iff L_A^Q \) is injective. To see this, note first that if \( L_A^Q \) is injective, then so is its restriction \( L_A \) to \( \mathbb{Z}^n. \) Conversely, if \( L_A \) is injective and if \( \vec{v} \in \mathbb{Q}^n \) is such that \( L_A(\vec{v}) = \vec{0}, \) then there is an integer \( m \in \mathbb{Z}, m \neq 0, \) such that \( \vec{v}' = m\vec{v} \in \mathbb{Z}^n. \) Then \( \vec{0} = L_A^Q(\vec{v}) = \frac{1}{m} L_A^Q(\vec{v}') = \frac{1}{m} L_A(\vec{v}'), \) so \( L_A(\vec{v}') = \vec{0} \) and hence \( \vec{v}' = \vec{0} \) because \( L_A \) is injective. Thus \( \vec{v} = \frac{1}{m} \vec{v}' = \vec{0}, \) so \( \text{Ker}(L_A^Q) = \{ \vec{0} \} \) and hence \( L_A^Q \) is injective.

[11] 3. (See the MAPLE solution on the course web-site.)