Inverting Matrices over Rings

D. R. Stinson

In a **Hill Cipher** defined over $\mathbb{Z}_n$, the key is an $m \times m$ invertible matrix $A = (a_{i,j})$. The encryption function is

$$e_A(x) = xA$$

and the corresponding decryption function is

$$d_A(y) = yA^{-1},$$

where all operations are performed modulo n.

If n is prime, then A is invertible if and only if $\det A \not\equiv 0 \bmod n$. In this case, A^{-1} can be computed by the formula given on page 17 of *Cryptography Theory and Practice*, or alternatively, using elementary row operations, if desired.

Here is an example to illustrate: suppose $n = 13$ and

$$A = \begin{pmatrix} 4 & 7 \\ 11 & 2 \end{pmatrix}.$$

Then we can compute

$$\begin{aligned} \det A &= 4 \times 2 - 7 \times 11 \bmod 13 \\ &= -69 \bmod 13 \\ &= 9, \end{aligned}$$

so A is invertible.

Using Theorem 1.3, we have that

$$\begin{aligned} A^{-1} &= 9^{-1} \times \begin{pmatrix} 2 & -7 \\ -11 & 4 \end{pmatrix} \\ &= 3 \times \begin{pmatrix} 2 & 6 \\ 2 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 6 & 5 \\ 6 & 12 \end{pmatrix}. \end{aligned}$$

The alternative method could proceed as follows. We begin by appending an identity matrix I to A, and then we use elementary row operations to convert $(A \mid I)$ to the form $(I \mid B)$. The matrix $B = A^{-1}$. We illustrate with the same matrix A considered above:

$$\begin{aligned}
\left(\begin{array}{cc|cc} 4 & 7 & 1 & 0 \\ 11 & 2 & 0 & 1 \end{array}\right) &\rightarrow \left(\begin{array}{cc|cc} 1 & 5 & 10 & 0 \\ 11 & 2 & 0 & 1 \end{array}\right) && \text{row } 1 = 10\times \text{ row } 1 \\
&\rightarrow \left(\begin{array}{cc|cc} 1 & 5 & 10 & 0 \\ 0 & 12 & 7 & 1 \end{array}\right) && \text{row } 2 = \text{row } 2 - 11\times \text{ row } 1 \\
&\rightarrow \left(\begin{array}{cc|cc} 1 & 5 & 10 & 0 \\ 0 & 1 & 6 & 12 \end{array}\right) && \text{row } 2 = 12\times \text{ row } 2 \\
&\rightarrow \left(\begin{array}{cc|cc} 1 & 0 & 6 & 5 \\ 0 & 1 & 6 & 12 \end{array}\right) && \text{row } 1 = \text{row } 1 - 5\times \text{ row } 2.
\end{aligned}$$

Hence, we obtain A^{-1} as before.

In the case where n is not prime, $\mathbb{Z}_n$ is not a field, and A is invertible if and only if $\gcd(\det A, n) = 1$. The formula given on page 17 can be applied, as before. However, if we attempt to use elementaary row operations, we may run into some complications.

Here is an example to consider. Suppose $n = 26$ and

$$A = \begin{pmatrix} 2 & 3 \\ 13 & 8 \end{pmatrix}.$$

Then $\det A = 3$, and since $\gcd(3, 26) = 1$, A is invertible.

Using Theorem 1.3, we have that

$$\begin{aligned}
A^{-1} &= 3^{-1} \times \begin{pmatrix} 8 & -3 \\ -13 & 2 \end{pmatrix} \\
&= 9 \times \begin{pmatrix} 8 & 23 \\ 13 & 2 \end{pmatrix} \\
&= \begin{pmatrix} 20 & 25 \\ 13 & 18 \end{pmatrix}
\end{aligned}$$

On the other hand, if we attempt to compute A^{-1} using elementary row operations, we would first try to multiply row 1 or row 2 by a constant so as to obtain a "1" in the first column. However, this cannot be done, since neither of the entries in the first column of A are invertible in $\mathbb{Z}_{26}$:

$\gcd(2, 26) = 2$ and $\gcd(13, 26) = 13$. (Note that it is possible to subtract $6\times$ row 1 from row 2 to get a 1 in the first column. The point here is that the algorithm to be followed is more complicated than in the case where the matrix is defined over a field.)