Cryptographie : Rappel sur l'inverse d'une matrice dans $\mathbb{Z}_n$

MOHAMED MEJRI

Groupe LSFM

Département d'Informatique et de Génie Logiciel

Université LAVAL

Québec, Canada

Exercice : un peu de mathématique

- Calculer les inverses, modulo m, des matrices suivantes :
  - $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad m = 2$ $\Big\|$ $E = \begin{pmatrix} 10 & 11 \\ 7 & 20 \end{pmatrix}, \quad m = 26$
  - $B = \begin{pmatrix} 4 & 3 \\ 1 & 3 \end{pmatrix}, \quad m = 5$ $\Big\|$ $F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad m = 26$
  - $C = \begin{pmatrix} 10 & 6 \\ 5 & 3 \end{pmatrix}, \quad m = 11$ $\Big\|$ $G = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad m = 26$

Exercice : Solution

Rappel : Soit A une matrice carrée de dimension n. Notons par A_{ij} la matrice A ôtée de la ligne i et la colonne j.

- Le déterminant de la matrice A se calcule en utilisant une des formules suivantes :
  - $det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} det(A_{ij})$ pour n'importe quelle valeur de j dans $\{1, \ldots, n\}$
  - $det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} det(A_{ij})$ pour n'importe quelle valeur de i dans $\{1, \ldots, n\}$
- Une matrice est inversible dans un ensemble E ($\mathbb{R}$, $\mathbb{Z}_n$, etc.), si et seulement si son déterminant est inversible dans E.
- Dans le cas où le déterminant de A est inversible, A^{-1} est définie par la formule suivante :
  $A^{-1}[i, j] = (det(A))^{-1} * (-1)^{i+j} * det(A_{ji})$
- si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $det(A) = (ad - cb)$ est inversible dans $\mathbb{Z}_m$ alors A est inversible dans $\mathbb{Z}_m$ et

  $$A^{-1} = det(A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} (mod\ m)$$

  avec $det(A)^{-1}$ est l'inverse de $det(A)$ dans $\mathbb{Z}_m$.

➳ $m = 2$

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \Rightarrow det(A) = 1 \Rightarrow A^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

➳ $m = 5$

$$B = \begin{pmatrix} 4 & 3 \\ 1 & 3 \end{pmatrix} \Rightarrow det(B) = 9 \equiv 4\ mod\ 5 \Rightarrow det(B)^{-1} = 4 \Rightarrow B^{-1} = 4 \begin{pmatrix} 3 & -3 \\ -1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}$$

➳ $m = 11$

$$C = \begin{pmatrix} 10 & 6 \\ 5 & 3 \end{pmatrix} \Rightarrow det(C) = 0 \Rightarrow C \text{ n'est pas inversible.}$$

- $m = 26$

$$E = \begin{pmatrix} 10 & 11 \\ 7 & 20 \end{pmatrix} \Rightarrow det(E) = 123 \equiv 19 \ mod \ 26 \Rightarrow det(E)^{-1} = 11 \Rightarrow E^{-1} = 11 \begin{pmatrix} 20 & -11 \\ -7 & 10 \end{pmatrix} = \begin{pmatrix} 12 & 9 \\ 1 & 6 \end{pmatrix}$$

- $m = 26$

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow det(F) = -1 \equiv 25 \ mod \ 26 \Rightarrow det(F)^{-1} = 25 \Rightarrow F^{-1} = 25 \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- $m = 26,$

$$G = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\Rightarrow det(G) = (-1)^{1+1} * 1 * det \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix} + (-1)^{1+2} * 2 * det \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + (-1)^{1+3} * 3 * det \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} = 3$$

$$\Rightarrow det(G)^{-1} = 9$$

$$\Rightarrow G^{-1} = \begin{pmatrix} (9 * (-1)^{1+1} * 2) \ mod \ 26 & (9 * (-1)^{1+2} * (-1)) \ mod \ 26 & (9 * (-1)^{1+3} * (-7))) \ mod \ 26 \\ (9 * (-1)^{2+1} * 1) \ mod \ 26 & (9 * (-1)^{2+2} * 1) \ mod \ 26 & (9 * (-1)^{2+3} * (-2))) \ mod \ 26 \\ (9 * (-1)^{3+1} * 1) \ mod \ 26 & (9 * (-1)^{3+2} * 1)) \ mod \ 26 & (9 * (-1)^{3+3} * 1)) \ mod \ 26 \end{pmatrix}$$

$$\Rightarrow G^{-1} = \begin{pmatrix} 18 & 9 & 15 \\ 17 & 9 & 18 \\ 9 & 17 & 9 \end{pmatrix}$$