Volume 1, No. 2, July-August 2010

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Modular Arithmetic Inverse of a Rectangular Matrix

V. Umakanta Sastry*
Department of Computer Science and Engineering
SreeNidhi Institute of Science and Technology
Hyderabad – 501 301, Andhra Pradesh, India
vuksastry@rediffmail.com

D. S. R. Murthy
Department of Information Technology
SreeNidhi Institute of Science and Technology
Hyderabad – 501 301, Andhra Pradesh, India
dsrmurthy@sreenidhi.edu.in

Abstract: In this paper, we have devoted our attention to the study of the modular arithmetic inverse of a rectangular matrix. Here, we have shown that (AB) mod N = I, where A is of size m x n and B is of size n x m in which m < n. We have also established that the modular arithmetic inverse of a rectangular matrix does not exist, when m > n.

Keywords: Rectangular matrix, Arithmetic inverse, Modular arithmetic inverse, Block cipher, Square matrix.

I. INTRODUCTION

The study of the arithmetic inverse of a rectangular matrix attracted the attention of several researchers [1 – 3] in view of its wide variety of applications in networks, regression analysis and least square curve fitting. The modular arithmetic inverse of a square matrix was introduced by Hill [4], and it was made use of in developing a block cipher in cryptography. In a recent paper, Sastry and Janaki [5] have developed a systematic procedure for obtaining the modular arithmetic inverse of a square matrix and they have employed it in the development of block ciphers in various ways [6 – 7].

In the present paper, our objective is to develop the modular arithmetic inverse of a rectangular matrix. Here, we have shown that the arithmetic inverse of a rectangular matrix of size m x n exists only when m < n. This implies that the modular arithmetic inverse of a rectangular matrix also exists only when m < n.

In what follows, we present the plan of this paper. In section 2, we have presented a method for obtaining the modular arithmetic inverse of a rectangular matrix of size m x n, when m < n. In this, we have illustrated the procedure by giving several examples. Then we have shown that the modular arithmetic inverse of a rectangular matrix does not exist, when m > n. Finally, section 3 is devoted to conclusions.

II. MODULAR ARITHMETIC INVERSE OF A RECTANGULAR MATRIX

Let A be an m x n matrix and B be an n x m matrix, where m < n. Let us assume that all the elements of A and B are positive integers, which are less than an integer N, and B is the modular arithmetic inverse of A. Then we can write an equation of the form

$$(A\,B) \bmod N = I, \qquad (2.1)$$

where I is an Identity matrix of size m.

On multiplying on both the sides of (2.1) by A^T, where T denotes the transpose of the matrix, we get

$$(Q\,B) \bmod N = A^T \qquad (2.2)$$

in which $Q = A^T A$ is a square matrix of order n.

We now obtain the arithmetic inverse of Q by using Gaussian reduction method [8]. Then we find the modular arithmetic inverse of Q.

Thus we have Q^{-1} governed by the relation

$$(Q^{-1}\,Q) \bmod N = (Q\,Q^{-1}) \bmod N = I. \qquad (2.3)$$

From (2.2) and (2.3), we have

$$B = (Q^{-1}\,A^T) \bmod N. \qquad (2.4)$$

In what follows, we present different rectangular matrices, denoted as A, and their corresponding modular arithmetic inverses, denoted as B, for various values of N, say N = 2, 128, and 256.

For N = 2, we have

For N = 2, we have

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

For N = 128, we have

$$A = \begin{bmatrix} 5 & 99 & 19 & 12 & 11 \\ 21 & 13 & 16 & 121 & 57 \\ 51 & 32 & 55 & 73 & 22 \end{bmatrix}, \qquad B = \begin{bmatrix} 93 & 9 & 93 \\ 111 & 113 & 116 \\ 102 & 67 & 55 \\ 93 & 2 & 61 \\ 31 & 13 & 102 \end{bmatrix}.$$

For N = 256, we have

$$A = \begin{bmatrix} 85 & 32 & 156 & 129 & 31 \\ 199 & 233 & 221 & 19 & 80 \\ 22 & 77 & 99 & 167 & 131 \end{bmatrix}, \qquad B = \begin{bmatrix} 49 & 0 & 191 \\ 216 & 151 & 87 \\ 184 & 121 & 251 \\ 179 & 63 & 243 \\ 119 & 187 & 242 \end{bmatrix}.$$

Some more examples related to the rectangular matrix and its modular arithmetic inverse, for various values of N, are presented in Appendix. In all the aforementioned examples, we have m < n.

Now let us examine the case when m > n. Let A be a matrix of size m x n, and D be a matrix of size n x m, where m > n. Let D be the arithmetic inverse of A. Then we have

$$A\,D = I, \qquad (1)$$

where I is a unit matrix of size m.

For simplicity, let us take an example, where

$$A = \begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{bmatrix}, \qquad (2)$$

$$\text{and } D = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_3 \end{bmatrix}. \qquad (3)$$

Here, m = 3, and n = 2.

From (1) – (3), we get a system of equations given by

$a_1 x_1 + a_2 y_1 = 1$ (4)
$a_1 x_2 + a_2 y_2 = 0$ (5)
$a_1 x_3 + a_2 y_3 = 0$ (6)
$b_1 x_1 + b_2 y_1 = 0$ (7)
$b_1 x_2 + b_2 y_2 = 1$ (8)
$b_1 x_3 + b_2 y_3 = 0$ (9)
$c_1 x_1 + c_2 y_1 = 0$ (10)
$c_1 x_2 + c_2 y_2 = 0$ (11)
$c_1 x_3 + c_2 y_3 = 1$ (12)

Here, x_1, y_1, x_2, y_2, and x_3, y_3 are known to us. Now, we are to obtain the unknowns a_1 and a_2 from (4) – (6), b_1 and b_2 from (7) – (9), and c_1 and c_2 from (10) – (12).

Considering (5) and (6), and assuming that there is a non-trivial solution for a_1 and a_2, we get

$x_2 y_3 – x_3 y_2 = 0.$ (13)

Similarly, from (7) and (9), we get

$x_1 y_3 – x_3 y_1 = 0,$ (14)

and from (10) and (11), we have

$x_1 y_2 – x_2 y_1 = 0.$ (15)

Thus, from (15), we can have

$$\frac{x_2}{x_1} = \frac{y_2}{y_1} = \lambda, \qquad (16)$$

where λ is a constant.

From (5) and (16), we get

$a_1 x_1 + a_2 y_1 = 0.$ (17)

On comparing, (5) and (17), we clearly see that they are inconsistent. Similarly, we can establish that, the second set (7) – (9), and the third set (10) – (12) are also inconsistent and hence, no solution can be obtained for (4) – (12). Thus, when A is given, D (the arithmetic inverse of A) cannot be determined, whenever m > n. As a consequence of this, the modular arithmetic inverse of A, say B, does not exist, in the case of a rectangular matrix, when m > n.

It is interesting to note that, the modular arithmetic inverse of a rectangular matrix can be determined, only when m < n.

III. CONCLUSIONS

In this paper, we have developed a procedure for obtaining the modular arithmetic inverse of a rectangular matrix. Here, we have shown that

(AB) mod N = I (3.1)

where A is of size m x n and B is of size n x m, in which m < n. In this case we have presented a number of examples. Further, we have established that the modular arithmetic inverse of a rectangular matrix does not exist, when m > n. Though we have illustrated the nonexistence of the modular arithmetic inverse of a rectangular matrix in a very simple case (m = 3, n = 2), this analysis can be generalised to any values of m and n, where m > n.

Here, it is interesting to note that the modular arithmetic inverse of a rectangular matrix is expected to find a vide variety of applications in the areas of cryptography.

IV. APPENDIX

When N = 2, we have

$$A = \begin{pmatrix}
1&0&0&0&0&0&1&1&0&0&0&1&1&1&1&1&0&0&0&1&0&0&1&0&0&0&1&1\\
1&0&1&1&1&1&1&1&1&1&1&0&0&1&1&1&1&1&1&0&0&1&1&1&0&0&0&1\\
0&1&1&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&1&1&0&1&1&1&0&1&0&0\\
1&1&0&0&0&1&1&1&0&1&0&0&0&1&1&0&1&1&1&1&1&0&0&1&1&1&1&1\\
1&1&1&1&0&1&0&1&1&1&0&1&1&1&1&1&1&0&1&0&1&1&1&1&0&0&1&1\\
0&0&1&0&1&1&1&0&1&0&1&0&0&1&1&0&1&0&1&1&1&1&1&0&1&0&0&1\\
0&1&0&0&1&0&1&0&0&0&1&0&1&1&1&1&1&0&0&1&0&1&0&0&0&0&1&1\\
1&1&1&0&0&1&0&1&0&0&0&0&1&1&1&1&0&0&1&0&1&0&0&0&1&0&1&1\\
1&0&1&0&1&1&1&1&1&0&1&0&0&1&0&0&1&0&1&1&1&0&1&0&1&0&0&1\\
1&1&1&0&1&0&1&1&1&1&0&0&1&1&1&1&1&1&0&1&0&1&1&1&0&1&1&1\\
1&1&0&1&1&1&1&0&0&0&1&1&1&1&1&1&0&0&0&1&1&1&0&1&0&0&0&1\\
1&1&1&0&1&1&0&1&1&1&0&1&0&0&0&1&1&0&0&0&0&0&0&1&1&1&1&1\\
1&1&0&0&1&1&1&0&0&1&1&1&1&1&1&1&0&0&0&1&1&1&0&1&0&0&0&1\\
1&1&0&0&0&1&0&0&1&0&1&0&1&1&1&0&0&0&0&0&1&1&0&0&0&1&1&1
\end{pmatrix}$$

$$B = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&1&0&1&0&0\\
0&0&1&1&1&0&0&0&1&0&1&0&1&1\\
0&0&1&0&1&1&0&1&0&1&0&0&0&1\\
1&1&1&0&1&0&1&0&0&1&0&1&0&1\\
0&0&0&0&1&0&1&0&0&1&1&0&0&1\\
0&1&0&1&0&1&1&0&1&1&1&0&1&1\\
0&1&1&0&1&1&0&0&0&1&0&1&1&1\\
1&1&0&1&1&0&0&1&0&0&1&0&0&1\\
0&0&1&0&1&0&1&1&1&1&0&1&1&0\\
1&1&1&0&1&0&1&0&0&1&1&1&1&1\\
1&1&0&0&0&1&0&0&1&1&1&1&1&1\\
0&0&1&1&1&1&0&0&1&1&1&1&1&1\\
0&1&0&1&1&1&1&0&1&0&0&1&0&1\\
1&1&1&0&1&1&0&0&0&1&1&1&0&0\\
1&1&0&1&0&1&0&0&0&0&0&0&1&0\\
1&1&0&0&0&0&1&1&0&1&0&1&0&0\\
0&1&0&1&0&0&0&0&1&0&1&0&0&0\\
1&0&0&0&0&0&1&0&0&1&0&0&1&0\\
0&1&1&0&0&1&1&0&1&1&0&1&1&1\\
1&1&0&0&1&1&0&0&1&1&0&0&1&0\\
1&0&0&1&1&1&1&1&0&0&1&1&1&1\\
1&0&0&0&1&0&0&1&1&1&1&1&1&1\\
1&1&0&0&1&0&0&0&1&1&1&0&0&0\\
0&1&1&0&0&0&0&0&1&1&0&1&1&1\\
0&1&1&0&1&1&1&1&0&1&1&0&1&1\\
0&1&0&1&1&0&0&1&0&1&0&1&1&1\\
1&0&1&0&1&1&0&1&0&1&1&1&0&1\\
1&0&0&0&0&1&0&1&0&0&1&1&0&1
\end{pmatrix}$$

When N = 128, we have

$$A = \begin{pmatrix}
75&73&76&76&32&65&76&76&32&84&72&69&32&84&69\\
82&82&79&82&73&83&84&83&32&65&84&32&79&78&69\\
32&83&84&82&79&75&69&31&66&89&80&85&81&84&73\\
78&71&80&79&73&83&79&78&32&73&78&32&84&72&69\\
73&82&32&77&69&65&76&65&78&68&32&68&82&73&78\\
75&46&32&68&79&32&78&79&84&87&65&73&84&32&65\\
78&89&32&77&79&81&69&46&32&85&82&71&69&78&84\\
74&33&26&79&37&65&67&71&32&88&77&91&93&28&57\\
123&77&70&71&33&67&47&97&83&88&17&69&93&38&19\\
76&32&84&72&69&32&84&69&75&73&76&76&32&65&76
\end{pmatrix}$$

$$B = \begin{pmatrix}
27&18&96&8&67&6&74&14&84&37\\
111&45&46&18&114&46&80&8&70&97\\
112&50&39&85&14&111&127&47&67&35\\
21&78&122&9&59&98&81&38&65&74\\
73&19&111&121&68&101&115&116&72&88\\
40&65&13&39&80&70&94&52&34&40\\
51&85&87&20&65&37&25&126&85&43\\
22&11&39&21&93&108&14&93&75&73\\
3&36&64&62&39&20&94&3&117&55\\
107&1&37&30&64&98&53&51&50&57\\
68&41&52&85&45&18&62&88&91&31\\
72&11&31&71&85&42&20&103&44&13\\
127&82&73&92&105&88&39&68&28&4\\
13&37&49&118&78&53&28&75&108&38\\
5&105&54&80&16&36&72&35&112&27
\end{pmatrix}$$

When N = 256, we have

$$A = \begin{pmatrix}
175&123&236&176&32&165&76&17&32&84&72&69&32&185&169\\
182&132&23&149&74&123&3&55&93&113&235&89&103&100&9\\
87&32&23&184&197&179&251&160&3&69&89&185&53&181&87\\
67&31&61&171&187&93&21&45&179&118&132&87&175&133&184\\
72&69&73&227&132&170&109&165&108&173&121&178&111&125&87\\
102&209&168&235&173&78&150&243&232&68&79&135&178&93&43\\
87&165&173&225&232&165&157&139&232&177&95&181&29&36&37\\
225&181&171&69&138&189&47&133&225&70&137&165&75&171&219\\
151&77&91&93&28&50&123&57&77&121&133&207&247&60&97\\
184&88&17&169&93&38&19&76&32&85&72&69&32&84&69
\end{pmatrix}$$

$$B = \begin{bmatrix} 202 & 57 & 108 & 237 & 254 & 207 & 137 & 7 & 51 & 204 \\ 251 & 207 & 142 & 176 & 146 & 71 & 9 & 129 & 2 & 207 \\ 39 & 169 & 218 & 37 & 187 & 228 & 226 & 144 & 121 & 121 \\ 41 & 104 & 255 & 40 & 0 & 46 & 8 & 185 & 11 & 80 \\ 70 & 83 & 16 & 78 & 23 & 243 & 161 & 122 & 91 & 150 \\ 175 & 115 & 152 & 103 & 124 & 96 & 156 & 214 & 220 & 115 \\ 209 & 107 & 206 & 45 & 43 & 202 & 90 & 54 & 255 & 133 \\ 21 & 51 & 253 & 89 & 243 & 185 & 67 & 0 & 48 & 242 \\ 67 & 201 & 66 & 121 & 124 & 94 & 33 & 112 & 193 & 177 \\ 157 & 37 & 27 & 57 & 10 & 177 & 131 & 55 & 28 & 73 \\ 105 & 43 & 119 & 80 & 245 & 83 & 2 & 222 & 41 & 69 \\ 237 & 82 & 17 & 76 & 123 & 194 & 225 & 37 & 90 & 31 \\ 212 & 80 & 66 & 85 & 109 & 115 & 223 & 88 & 231 & 190 \\ 66 & 230 & 79 & 150 & 198 & 249 & 147 & 178 & 137 & 114 \\ 251 & 6 & 117 & 219 & 116 & 58 & 115 & 103 & 150 & 29 \end{bmatrix}$$

REFERENCES

[1] E. V. Krishna Murthy, S. K. Sen, *Computer Based Numerical Algorithms*, East West Press, 1976.

[2] Rao C. R., Mitra S. K., *Generalised Inverse of Matrices and its Applications*, Wiley, New York, 1979.

[3] Penrose R, *A Generalized Inverse for matrices*, Proceedings of Cambridge Philosophical Society, **51**, 406 – 13, 1955.

[4] William Stallings, *Cryptography and Network Security*, Principles and Practice, Third Edition, Pearson, 2003.

[5] U. K. Sastry, V. Janaki, *On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher*, Proceedings of North American Technology and Business Conference, Sep. 2005, Canada.

[6] V. U. K. Sastry, V. Janaki, *A Modified Hill Cipher with Multiple Keys*, International Journal of Computational Science, Vol. 2, No. 6, 815 – 826, Dec. 2008.

[7] Janaki, *A Study of Some Problems in the Security of Files and Images*, PhD Thesis, JNTU, Hyderabad, July 2007.

[8] Kreyszig, E., *Advanced Engineering Mathematics*, Sixth Edition, Wiley, 1988.

Authors:

Dr. V. U. K. Sastry is presently working as Professor in the Dept. of Computer Science and Engineering (CSE), Director (SCSI), Dean (R & D), SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. He was Formerly Professor in IIT, Kharagpur,
India and worked in IIT, Kharagpur during 1963 – 1998. He guided 12 PhDs, and published more than 40 research papers in various international journals. He is a Member, Editorial Board and Reviewer of International Journal of Computational Intelligence and Information Security (IJCIIS), Senior Member of International Association of Computer Science and Information Technology (IACSIT) and Reviewer of International Journal of Computer and Network Security (IJCNS). His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic
Algorithms and published research papers in International Journal of Computer and Network Security (IJCNS), International Journal of Computer Theory and Engineering (IJCTE) and International Journal of Computational Intelligence and Information Security (IJCIIS).

Prof. D. S. R. Murthy obtained B. E. (Electronics) from Bangalore University in 1982, M. Tech. (CSE) from Osmania University in 1985 and presently pursuing Ph.D. from JNTUH, Hyderabad since 2007. He is presently working as Professor in the
Dept. of Information Technology (IT), SNIST since Oct. 2004. He earlier worked as Lecturer in CSE, NIT (formerly REC), Warangal, India during Sep. 1985 – Feb. 1993, as Assistant Professor in CSE, JNTUCE, Anantapur, India during Feb. 1993 – May 1998, as Academic Coordinator, ISM, Icfaian Foundation, Hyderabad, India during May 1998 – May 2001 and as Associate Professor in CSE, SNIST during May 2001 - Sept. 2004. He worked as Head of the Dept. of CSE, JNTUCE, Anantapur during Jan. 1996 – Jan 1998, Dept. of IT, SNIST during Apr. 2005 – May 2006, and Oct. 2007 – Feb. 2009. He is a Fellow of IE(I), Fellow of IETE, Senior Life Member of CSI, Life Member of ISTE, Life Member of SSI, DOEACC Expert member, and Chartered Engineer (IE(I) & IETE). He is a Reviewer of International Journal of Computational Intelligence and Information Security (IJCIIS) and member of International Association of Computer Science and Information Technology (IACSIT). He published a text book on C Programming & Data Structures. His research interests are Image Processing and Image Cryptography and published research papers in International Journal of Computer and Network Security (IJCNS), International Journal of Computer Theory and Engineering (IJCTE) and International Journal of Computational Intelligence and Information Security (IJCIIS).