The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

Computation of Multiplicative Inverses of non-zero Polynomials of $GF(7^3)$ by Gauss-Jordan method.

Dilshad Akhtar[1], Prof. M R Hassan[2], Neda Fatma[3],J K M Sadique Uz Zaman[4]
1,3. Research Scholar, Department of Mathematics, T.M Bhagalpur University, 812007 Bihar, India.
2. Professor, University Department of Mathematics,T.M Bhagalpur University, 812007, Bihar,India.
4. Assistant Professor, University Department of Computer Science, NBU Siliguri, West Bengal, India.
5. Corresponding Email:variantresearchcentre@gmail.com

Abstract: The present manuscript deals with the derivation of multiplicative inverses of all non-zero elemental polynomials of the Galois field $GF(7^3)$ with respect to the monic irreducible polynomials of degree 3 over the prime field $F_7 = \{0,1,2,3,4,5,6\}$ by Gauss-Jordan method as the Extended Euclidean Algorithm (EEA) is not always successful over the prime field $F_p = \{0,1,2,...,p-1\}$, when prime $p \geq 3$.

Keywords: Extended Euclidean Algorithm, Galois (finite) field, Multiplicative Inverse, Gauss-Jordan method, Irreducible polynomial.

1. Introduction: The Galois field(Finite field) of order p^n is denoted by $GF(p^n)$ and defined as $GF(p^n) = \{\frac{F_p}{\langle f(x)\rangle} = E(x) + \langle f(x)\rangle\}$, where $E(x) = \sum_{r=0}^{n-1} a_r x^r$ is a non-zero polynomial of degree

n-1 and $f(x) = \sum_{r=0}^{n} a_r x^r$ is an irreducible polynomial of degree n over F_p. This field is playing an important role in cryptography and cryptography is an integrated part of the study of network security. Particularly derivation of multiplicative inverses of elemental polynomials of $GF(p^n)$ with respect to the monic irreducible polynomials over F_p are very important. In this direction, so many authors worked on the multiplicative inverses of non-zero polynomials of $GF(2^m)$, $GF(7^3)$ etc. For the first time Toshiyo Itoh (1988) and Shigeo Tsuji derived multiplicative inverses of elemental polynomials of $GF(2^m)$. Hassan (1998) derived inverses in $GF(2^m)$ by solving a set of linear equations over the field $F_2 = \{0,1\}$. Arguello (2006) designed an algorithm based on Lahmer's algorithm for computing multiplicative inverses of non-zero polynomials of $GF(2^m)$, where Lahmer's algorithm is used for computing GCD of two integers.

Takogo Kobayshi etal (2007) derived the multiplicative inverse of elements of the finite field $GF(2^m)$ by using Extended Euclidean Algorithm (EEA). Later on in (2008) the members of Monzano High School team (New Maxico) calculated M.I.of the non-zero elements of $GF(2^m)$ by usig EEA and Lagrange's method. Christoforus Juan Benvenuto(2012)worked on multiplicative inverses over $GF(2^8)$.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

Sadique Uz Zaman etal (2015) have developed the multiplicative inverse of each elemental polynomials over a field $GF(2^8)$ and $GF(7^3)$. He successfully derived multiplicative inversess of each non-zero elemental polynomials of the Galois field $GF(2^8)$ by EEA with respect to monic irreducible polynomial over $F_2 = \{0,1\}$ but EEA became failure in computing the multiplicative inverses of non-zero polynomials of $GF(7^3)$ with respect to the monic irreducible polynomial over $F_7 = \{0,1,2,3,4,5,6\}$. Further he developed a new method called Algebraic method for deriving the multiplicative inverses of each non-zero polynomials of $GF(7^3)$ with respect to each monic irreducible polynomials over F_7. By this method he computed the multiplicative inverses of all 342 non-zero elemental polynomials of $GF(7^3)$ with respect to each irreducible polynomial over F_7.

Otokar Grose ketal (2018) used a long division method for computing multiplicative inverses of the elements of the finite fields $GF(p^n)$. If p is the prime order of the finite field then we can construct a fixed integer d(p) with the property that for any non-zero element 'a' of the field we can find its inverse by dividing d(p) by 'a' and reduce the result usig multiplication modulo p. In computing multiplicative inverse of non-zero elemental polynomials of $GF(7^3)$ we found the multiplicative inverse of 215 non-zero elemental polynomials only over $GF(7^3)$ arepossible with respect to the monic irreducible polynomial $x^3 + 6x^2 + 4x + 1$ over F_7. This number may very with respect to the other irreducible polynomial. That's why we proposed the Gauss-Jordan method for computing inverses of all the 342 non-zero polynomials over $GF(7^3)$ with respect to any monic irreducible polynomials over F_7. Before discussing Gauss-Jordan method, we would like to discuss first some of successful and failure cases of the EEA.

2. Extended Euclidean Algorithm (EEA) for Integers:

Statement: Let a and b be two integers, then EEA computes other two integers s and t such that

$$a \times s + b \times t = gcd(a,b) \qquad (1)$$

Which is the modification of Euclidean Algorithm.

Example: Let $a = 99$, $b = 34$ then there exist two integers $s = 11 \& t = -32$

such that $99 \times 11 + 34 \times (-32) = gcd(99,34) = 1.$

As $\gcd(99,34) = 1$ so $34^{-1} mod(99) = -32\ mod(99) = 67$

In general, if $\gcd(a,b) = 1$ then from (1), $b^{-1} (\mathrm{mod}\, a) = t (\mathrm{mod}\, a)$

2.1. Extended Euclidean Algorithm for polynomials:

Statement: Let $a(x)$ and $b(x)$ be two polynomials, then EEA computes other two polynomials $p(x)$ and $q(x)$ such that $a(x)p(x) + b(x)q(x) = \gcd(a(x), b(x))$.

If $\gcd(a(x), b(x)) = 1$ then $b(x)q(x) = 1 \bmod(a(x)) \Rightarrow b(x)^{-1} \bmod(a(x)) = q(x) \bmod(a(x))$

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

2.2 Illustration of Extended Euclidean Algorithm:

Let $a(x)$ be a monic irreducible polynomial over F_p and $b(x)$ be a non-zero elemental polynomial over $GF(p^n)$ then to find the polynomials $p(x)$ and $q(x)$ using EEA with iterations.

Initialization:

Choosing, $A_1 = 1$, $A_2 = 0$, $A_3 = a(x)$, $B_1 = 0$, $B_2 = 1$, $B_3 = b(x)$ then

Iterations are as follows:

$Q \leftarrow A_3 / B_3$, $A_1 \leftarrow B_1$, $A_2 \leftarrow B_2$, $A_3 \leftarrow B_3$

$B_1 \leftarrow A_1 - Q \times B_1$, $B_2 \leftarrow A_2 - Q \times B_2$, $B_3 \leftarrow A_3 - Q \times B_3$ in all the iterations successively until the remainder is zero.

Tabular form:

	A_1	A_2	A_3	B_1	B_2	B_3
Initialization:	1	0	$a(x)$	0	1	$b(x)$
Iterations:						
$Q=A_3/B_3$	0	1	$b(x)$	$1-Q\times 0$	$0-Q\times 1$	$a(x)-Q\times b(x)$

The iterations terminate when the remainder become zero , that is when the column B_3 become zero and gcd (a(x), b(x)) is the last non-zero value of column B_3 .If gcd (a(x), b(x)) = 1 then we can find the multiplicative inverse of b(x) with respect to a(x).

2.2 Success of EEA for finding the multiplicative inverse of polynomials over $GF(7^3)$.

Let $a(x)=x^3+6x^2+4x+1$ be a monic irreducible polynomial over $GF(7)$ and $b(x)= x^2+3$ be an elemental polynomial over $GF(7^3)$.

We have to find the multiplicative inverse of $b(x)$ with respect to $a(x)$ using EEA.

	A_1	A_2	$A_3=a(x)$	B_1	B_2	$B=b(x)$
Initialization	1	0	x^3+6x^2+4x+1	0	1	x^2+3
Iteration1:						
$Q=x+6$	0	1	x^2+3	1	$6x+1$	$x+4$
Iteration2:						
$Q= x+3$ Iteration3:	1	$6x+1$	$x+4$	$6x+4$	x^2+2x+5	5
$Q=3x$	$6x+4$	x^2+2x+5	5	$3x^2+2x+1$	$4x^3+x^2+5x+1$	4
Iteration4:						
$Q=1$	$3x^2+2x+1$	$4x^3+x^2+5x+1$	4	$4x^2+4x+3$	$3x^3+4x+4$	1
Iteration5:						
$Q=4$	$4x^2+4x+3$	$3x^3+4x+4$	1	x^2+3	$6x^3+x^2+3x+6$	0

Here, we get the last non-zero number in Iteration 4 is equal to 1, so we can claim that $\gcd(a(x),b(x))=1$

i.e, $\gcd(x^3+6x^2+4x+1, x^2+3)=1$

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

Hence, $\left(x^2+3\right)^{-1} = 3x^3+4x+4 \bmod (x^3+6x^2+4x+1)$

$= 3x^2+6x+1$

2.4. Failure of EEA for finding multiplicative inverse of polynomials over $GF(7^3)$.

Let $a(x) = x^3+6x^2+4x+1$ be a monic irreducible polynomial over $GF(7)$ and $b(x) = 2x^2+5$ be an elemental polynomial over $GF(7^3)$.

We have to find the multiplicative inverse of b(x) with respect to a(x) using EEA.

	A_1	A_2	$A_3 = a(x)$	B_1	B_2	$B_3 = b(x)$
Initialization:	1	0	x^3+6x^2+4x+1	0	1	$2x^2+5$
Iteration1:						
Q= $4x+3$	0	1	$2x^2+5$	1	$3x+4$	$5x$
Iteration2:						
Q= $6x$	1	$3x+4$	$5x$	x	$3x^2+4x+1$	5
Iteration3:						
Q= x	x	$3x^2+4x+1$	5	$6x^2+1$	$4x^3+3x^2+2x+4$	0

Here, we get the last non-zero number in iteration 2 is 5 so, $\gcd(a(x), b(x)) = 5 \neq 1$, therefore we can't find the multiplicative inverse of $b(x) = 2x^2+5$ .Therefore in this case we conclude that the EEA failed to find the multiplicative inverse of $2x^2+5$ with respect to x^3+6x^2+4x+1

3. Gauss-Jordan method by solving System of Linear Equations:

Let $a(x) = x^3+a_2x^2+a_1x+a_0$ be a monic irreducible polynomial over F_7 and $b(x) = b_2x^2+b_1x+b_0$ bean elemental polynomial over a finite field $GF(7^3)$.

We have to find the multiplicative inverse of $b(x)$ with respect to $a(x)$ by solving a system of linear equations using Gauss-Jordan method.

Let $c(x) = c_2x^2+c_1x+c_0$ be the multiplicative inverse of elemental polynomial $b(x)$ over $GF(7^3)$ with respect to irreducible polynomial $a(x)$ over $GF(7)$.

Then we can write,

$[b(x)\ c(x)] \bmod (a(x)) = 1$

$[(b_2x^2+b_1x+b_0)\ (c_2x^2+c_1x+c_0)] \bmod (x^3+a_2x^2+a_1x+a_0) = 1$

$[b_2c_2x^4+(b_2c_1+b_1c_2)x^3+(b_2c_0+b_1c_1+b_0c_2)x^2+(b_1c_0+b_0c_1)x+b_0c_0] \bmod (x^3+a_2x^2+a_1x+a_0) = 1$

Or,

$[b_2c_2x(-a_2x^2-a_1x-a_0)+(b_2c_1+b_1c_2)(-a_2x^2-a_1x-a_0)+(b_2c_0+b_1c_1+b_0c_2)x^2+(b_1c_0+b_0c_1)x+b_0c_0] \bmod (x^3+a_2x^2+a_1x+a_0) = 1$

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

$Or,$

$[-a_2b_2c_2x^3 - a_1b_2c_2x^2 - a_0b_2c_2x - a_2b_2c_1x^2 - a_1b_2c_1x - a_0b_2c_1 - a_2b_1c_2x^2 - a_1b_1c_2x - a_0b_1c_2$
$+(b_2c_0 + b_1c_1 + b_0c_2)x^2 + (b_1c_0 + b_0c_1)x + b_0c_0]mod\,(x^3 + a_2x^2 + a_1x + a_0) = 1$

Or, $[-a_2b_2c_2(-a_2x^2 - a_1x - a_0) + (-a_1b_2c_2 - a_2b_2c_1 - a_2b_1c_2 + b_2c_0 + b_1c_1 + b_0c_2)x^2$
$+(-a_0b_2c_2 - a_1b_2c_1$
$-a_1b_1c_2 + b_1c_0 + b_0c_1)x + (a_0b_2c_1 - a_0b_1c_2 + b_0c_0)] \bmod (x^3 + a_2x^2 + a_1x + a_0) = 1$

Or, $[\{(a_2^2b_2 - a_1b_2 - a_2b_1 + b_0)c_2 + (b_1 - a_2b_2)c_1 + b_2c_0\}x^2 + \{(a_1a_2b_2 - a_0b_2 - a_1b_1)c_2 + (b_0 - a_1b_2)c_1$
$+b_1c_0\}x + \{(a_0a_2b_2 - a_0b_1)c_2 - a_0b_2c_1 + b_0c_0\}] \bmod (x^3 + a_2x^2 + a_1x + a_0) = 1$

It is clear from the above analytic discussion, dividend is smaller than divisor and hence for the remainder to be 1, the following properties must hold:

The coefficient of $x^2 \equiv 0 \bmod 7$, the coefficient of $x \equiv 0 \bmod 7$, the constant part $\equiv 1 \bmod 7$

$$\{(a_2^2b_2 - a_1b_2 - a_2b_1 + b_0)c_2 + (b_1 - a_2b_2)c_1 + b_2c_0\} \bmod 7 = 0$$
$$\{(a_1a_2b_2 - a_0b_2 - a_1b_1)c_2 + (b_0 - a_1b_2)c_1 + b_1c_0\} \bmod 7 = 0$$
$$\{(a_0a_2b_2 - a_0b_1)c_2 - a_0b_2c_1 + b_0c_0\} \bmod 7 = 1$$

In modular arithmetic with modulo 7, -1 can be written as 6 and consequently $-x$ can be written as $6x$.

Hence, above equations reduced to,

$$\{(a_2^2b_2 + 6a_1b_2 + 6a_2b_1 + b_0)c_2 + (b_1 + 6a_2b_2)c_1 + b_2c_0\} \bmod 7 = 0$$
$$\{(a_1a_2b_2 + 6a_0b_2 + 6a_1b_1)c_2 + (b_0 + 6a_1b_2)c_1 + b_1c_0\} \bmod 7 = 0$$
$$\{(a_0a_2b_2 + 6a_0b_1)c_2 + 6a_0b_2c_1 + b_0c_0\} \bmod 7 = 1$$

The above equations can be written as,

$$(k_{00}c_0 + k_{01}c_1 + k_{02}c_2) \bmod 7 = 0$$
$$(k_{10}c_0 + k_{11}c_1 + k_{12}c_2) \bmod 7 = 0$$
$$(k_{20}c_0 + k_{21}c_1 + k_{22}c_2) \bmod 7 = 1$$

Which is the system of 3 linear equations in three unknowns as c_0, c_1 and c_2.

Where,

$k_{00} = (b_2)\%7$, $k_{01} = (b_1 + 6a_2b_2)\%7$, $k_{02} = (a_2^2b_2 + 6a_1b_2 + 6a_2b_1 + b_0)\%7$ (2)

$k_{10} = (b_1)\%7, k_{11} = (b_0 + 6a_1b_2)\%7, k_{12} = (a_1a_2b_2 + 6a_0b_2 + 6a_1b_1)\%7$ (3)

$k_{20} = (b_0)\%7, k_{21} = (6a_0b_2)\%7, k_{22} = (a_0a_2b_2 + 6a_0b_1)\%7$ (4)

3.1. Gauss-Jordan method:

The above system of equations can be written as,

$$\begin{bmatrix} k_{00} & k_{01} & k_{02} \\ k_{10} & k_{11} & k_{12} \\ k_{20} & k_{22} & k_{23} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

A C B

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

$$(A,B)=\left[\begin{array}{ccc|c} k_{00} & k_{01} & k_{02} & 0 \\ k_{10} & k_{11} & k_{12} & 0 \\ k_{20} & k_{21} & k_{22} & 1 \end{array}\right] \qquad (5)$$

Gauss-Jordan method is a modification of Gauss-elimination method. In this method, the coefficient matrix A of the system of equations is reduced to a unit matrix using row elementary operations. By this method the system of equations will reduce to the form

$$(A,B)=\left[\begin{array}{ccc|c} 1 & 0 & 0 & q_0 \\ 0 & 1 & 0 & q_1 \\ 0 & 0 & 1 & q_2 \end{array}\right]$$

Where q_0, q_1, q_2 are constants.

From above , we get , $c_0 = q_0$, $c_1 = q_1$, $c_2 = q_2$.

Therefore, $[b(x)]^{-1} = c(x) = c_2x^2 + c_1x + c_0 = q_2x^2 + q_1x + q_0$

3.2 Some examples based on Gauss-Jordan Method to find the multiplicative inverse of polynomials over $GF(7^3)$.

Ex-1. Let $a(x) = x^3 + 6x^2 + 4x + 1$ be a monic irreducible polynomial over $GF(7)$ and $b(x) = x^2 + 3$ be an elemental polynomial over $GF(7^3)$.

We have to find $(b(x))^{-1} = c(x) = c_2x^2 + c_1x + c_0$ with respect to irreducible polynomial $a(x)$.

Here, $a_2 = 6, a_1 = 4, a_0 = 1$

$b_2 = 1, b_1 = 0, b_0 = 3$

From (2), (3) and (4), we get,

$k_{00} = 1, k_{01} = 1, k_{02} = 0$

$k_{10} = 0, k_{11} = 6, k_{12} = 2$

$k_{20} = 3, k_{21} = 6, k_{22} = 6$

Therefore, from (5), we get,

$$(A,B)=\left[\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 6 & 2 & 0 \\ 3 & 6 & 6 & 1 \end{array}\right] = \text{the augmented matrix.}$$

Using the elementary operations $(R_3 \to R_3 - 3R_1)$, $(R_2 \to \frac{1}{6}R_2)$, $(R_3 \to R_3 - 3R_2)$,

$(R_2 \to R_2 - R_3), (R_1 \to R_1 - R_2), (R_3 \to \frac{1}{5}R_3)$ successively,we get,

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

$$(A,B) \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 3 \end{array}\right],$$

Therefore, we get, $c_2 = 3,\ c_1 = 6,\ c_0 = 1$

Hence by Gauss-Jordan method, $[b(x)]^{-1} = c(x) = c_2 x^2 + c_1 x + c_0 = 3x^2 + 6x + 1$

$$i.e,\ (x^2+3)^{-1} = 3x^2 + 6x + 1$$

Ex-2. Let $a(x) = x^3 + 6x^2 + 4x + 1$ be a monic irreducible polynomial over $GF(7)$ and $b(x) = 2x^2 + 5$ be an elemental polynomial over $GF(7^3)$.

We have to find $[b(x)]^{-1} = c(x) = c_2 x^2 + c_1 x + c_0$ with respect to irreducible polynomial $a(x)$.

Here, $a_2 = 6, a_1 = 4, a_0 = 1$

$b_2 = 2, b_1 = 0, b_0 = 5$

From (2), (3) and (4) we get,

$$k_{00} = 2, k_{01} = 2, k_{02} = 6$$
$$k_{10} = 0, k_{11} = 4, k_{12} = 4$$
$$k_{20} = 5, k_{21} = 5, k_{22} = 5$$

Therefore, from (5), we get,

$$(A,B) = \left[\begin{array}{ccc|c} 2 & 2 & 6 & 0 \\ 0 & 4 & 4 & 0 \\ 5 & 5 & 5 & 1 \end{array}\right]$$

By applying consecutive elementary operations $(R_3 \to R_3 - 6R_1), (R_1 \to \frac{1}{2}R_1), (R_2 \to \frac{1}{4}R_2)$

$(R_3 \to \frac{1}{4}R_3), (R_1 \to R_1 - 3R_3), (R_2 \to R_2 - R_3), (R_1 \to R_1 - R_2)$

$$(A,B) \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 5 \\ 0 & 0 & 1 & 2 \end{array}\right]$$

Therefore, we get, $c_2 = 2, c_1 = 5, c_0 = 3$ and hence by Gauss-Jordan method

$(2x^2 + 5)^{-1} = 2x^2 + 5x + 3$

Gauss-Jordan method is successful to find the multiplicative inverse of all non-zero polynomials over $GF(7^3)$ whether it is successful or failure in case of extended Euclidean algorithm.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

3. List of elemental polynomials and multiplicative inversesfound using Gauss-Jordan method with respect to irreducible polynomial x^3+6x^2+4x+1.

Serial no.	Elemental polynomials	Inverses	Serial no.	Elemental polynomials	Inverses
01	000	Doesn't exist	48	065	425
02	001	001	49	066	463
03	002	004	50	100	423
04	003	005	51	101	453
05	004	002	52	102	330
06	005	003	53	103	361
07	006	006	54	104	043
08	010	613	55	105	150
09	011	314	56	106	436
10	012	352	57	110	306
11	013	326	58	111	140
12	014	246	59	112	262
13	015	116	60	113	434
14	016	402	61	114	152
15	020	345	62	115	530
16	021	123	63	116	015
17	022	542	64	120	554
18	023	443	65	121	421
19	024	561	66	122	431
20	025	201	67	123	021
21	026	513	68	124	236
22	030	251	69	125	302
23	031	552	70	126	130
24	032	132	71	130	126
25	033	156	72	131	224
26	034	603	73	132	032
27	035	362	74	133	622
28	036	143	75	134	565
29	040	526	76	135	611
30	041	634	77	136	404
31	042	415	78	140	111
32	043	104	79	141	516
33	044	621	80	142	414
34	045	645	81	143	036
35	046	225	82	144	520
36	050	432	83	145	546
37	051	264	84	146	400
38	052	506	85	150	105
39	053	216	86	151	342
40	054	334	87	152	114
41	055	235	88	153	241
42	056	654	89	154	564
43	060	164	90	155	644
44	061	305	91	156	033

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

45	062	661	92	160	566
46	063	531	93	161	445
47	064	451	94	162	411
95	163	313	148	300	631
96	164	060	149	301	540
97	165	403	150	302	125
98	166	642	151	303	641
99	200	215	152	304	612
100	201	025	153	305	061
101	202	265	154	306	110
102	203	460	155	310	504
103	204	550	156	311	266
104	205	253	157	312	365
105	206	534	158	313	163
106	210	444	159	314	011
107	211	610	160	315	426
108	212	643	161	316	556
109	213	623	162	320	532
110	214	242	163	321	255
111	215	200	164	322	233
112	216	053	165	323	336
113	220	503	166	324	606
114	221	461	167	325	424
115	222	420	168	326	013
116	223	650	169	330	102
117	224	131	170	331	410
118	225	046	171	332	616
119	226	252	172	333	560
120	230	406	173	334	054
121	231	632	174	335	543
122	232	521	175	336	323
123	233	322	176	340	422
124	234	442	177	341	601
125	235	055	178	342	151
126	236	124	179	343	664
127	240	662	180	344	263
128	241	153	181	345	020
129	242	214	182	346	655
130	243	501	183	350	555
131	244	254	184	351	462
132	245	450	185	352	012
133	246	014	186	353	452
134	250	633	187	354	600
135	251	030	188	355	430
136	252	226	189	356	656
137	253	205	190	360	446
138	254	244	190	361	103
139	255	321	192	362	035
140	256	545	193	363	635

141	260	413	194	364	510
142	261	636	195	365	312
143	262	112	196	366	615
144	263	344	197	400	146
145	264	051	198	401	660
146	265	202	199	402	016
147	266	311	200	403	165
201	404	136	254	511	466
202	405	652	255	512	505
203	406	230	256	513	026
204	410	331	257	514	433
205	411	162	258	515	665
206	412	465	259	516	141
207	413	260	260	520	144
208	414	142	261	521	232
209	415	042	262	522	456
210	416	604	263	523	533
211	420	222	264	524	502
212	421	121	265	525	551
213	422	340	266	526	040
214	423	100	267	530	115
215	424	325	268	531	063
216	425	065	269	532	320
217	426	315	270	533	523
218	430	355	271	534	206
219	431	122	272	535	563
220	432	050	273	536	624
221	433	514	274	540	301
222	434	113	275	541	653
223	435	626	276	542	022
224	436	106	277	543	335
225	440	605	278	544	455
226	441	454	279	545	256
227	442	234	280	546	145
228	443	023	281	550	204
229	444	210	282	551	525
230	445	161	283	552	031
231	446	360	284	553	646
232	450	245	285	554	120
233	451	064	286	555	350
234	452	353	287	556	316
235	453	101	288	560	333
236	454	441	289	561	024
237	455	544	290	562	500
238	456	522	291	563	535
239	460	203	292	564	154
240	461	221	293	565	134
241	462	351	294	566	160
242	463	066	295	600	354

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

243	464	614	296	601	341
244	465	412	297	602	620
245	466	511	298	603	034
246	500	562	299	604	416
247	501	243	300	605	440
248	502	524	301	606	324
249	503	220	302	610	211
250	504	310	303	611	135
251	505	512	304	612	304
252	506	052	305	613	010
253	510	364	306	614	464
307	615	366	326	643	212
308	616	332	327	644	155
309	620	602	328	645	045
310	621	044	329	646	553
311	622	133	330	650	223
312	623	213	331	651	640
313	624	536	332	652	405
314	625	663	333	653	541
315	626	435	334	654	056
316	630	666	335	655	346
317	631	300	336	656	356
318	632	231	337	660	401
319	633	250	338	661	062
320	634	041	339	662	240
321	635	363	340	663	625
322	636	261	341	664	343
323	640	651	342	665	515
324	641	303	343	666	630
325	642	166			

4. List of elemental polynomials and multiplicative inverse found using Gauss-Jordan method with respect to irreducible polynomial $x^3 + 4x + 1$.

Serial no.	Elemental polynomials	Inverses	Serial no.	Elemental polynomials	Inverses
01	000	Doesn't exist	43	060	104
02	001	001	44	061	662
03	002	004	45	062	535
04	003	005	46	063	324
05	004	002	47	064	215
06	005	003	48	065	626
07	006	006	49	066	524
08	010	603	50	100	462
09	011	253	51	101	123
10	012	151	52	102	132
11	013	562	53	103	252
12	014	453	54	104	060

13	015	242	55	105	116
14	016	115	56	106	351
15	020	305	57	110	420
16	021	265	58	111	510
17	022	165	59	112	614
18	023	121	60	113	541
19	024	464	61	114	534
20	025	446	62	115	016
21	026	631	63	116	105
22	030	201	64	120	611
23	031	363	65	121	023
24	032	423	66	122	314
25	033	341	67	123	101
26	034	554	68	124	646
27	035	641	69	125	556
28	036	545	70	126	211
29	040	506	71	130	555
30	041	232	72	131	653
31	042	136	73	132	102
32	043	223	74	133	526
33	044	436	75	134	142
34	045	354	76	135	544
35	046	414	77	136	042
36	050	402	78	140	440
37	051	146	79	141	250
38	052	331	80	142	134
39	053	313	81	143	234
40	054	656	82	144	245
41	055	612	83	145	304
42	056	512	84	146	051
85	150	523	138	254	620
86	151	012	139	255	360
87	152	216	140	256	336
88	153	551	141	260	666
89	154	400	142	261	421
90	155	514	143	262	365
91	156	366	144	263	622
92	160	212	145	264	401
93	161	206	146	265	021
94	162	540	147	266	613
95	163	665	148	300	623
96	164	511	149	301	552
97	165	022	150	302	343
98	166	022	151	303	531
99	200	231	152	304	145
100	201	030	153	305	020
101	202	415	154	306	513
102	203	443	155	310	431
103	204	451	156	311	456

104	205	564	157	312	445
105	206	161	158	313	053
106	210	220	159	314	122
107	211	126	160	315	600
108	212	260	161	316	352
109	213	502	162	320	444
110	214	452	163	321	466
111	215	064	164	322	432
112	216	152	165	323	241
113	220	210	166	324	063
114	221	652	167	325	563
115	222	640	168	326	503
116	223	043	169	330	630
117	224	342	170	331	052
118	225	406	171	332	465
119	226	624	172	333	450
120	230	615	173	334	504
121	231	200	174	335	416
122	232	041	175	336	256
123	233	642	176	340	353
124	234	143	177	341	033
125	235	533	178	342	224
126	236	664	179	343	302
127	240	344	180	344	240
128	241	323	181	345	455
129	242	015	182	346	460
130	243	663	183	350	660
131	244	542	184	351	106
132	245	144	185	352	316
133	246	404	186	353	340
134	250	141	187	354	045
135	251	644	188	355	364
136	252	103	189	356	516
137	253	011	190	360	255
191	361	442	244	465	332
192	362	505	245	466	321
193	363	031	246	500	546
194	364	355	247	501	616
195	365	262	248	502	513
196	366	156	249	503	326
197	400	154	250	504	334
198	401	264	251	505	362
199	402	050	252	506	040
200	403	632	253	510	111
201	404	246	254	511	164
202	405	434	255	512	056
203	406	225	256	513	306
204	410	522	257	514	155
205	411	621	258	515	412

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

206	412	515	259	516	356
207	413	422	260	520	636
208	414	046	261	521	441
209	415	202	262	522	410
210	416	335	263	523	150
211	420	110	264	524	066
212	421	261	265	525	604
213	422	413	266	526	133
214	423	032	267	530	433
215	424	430	268	531	303
216	425	461	269	532	633
217	426	601	270	533	235
218	430	424	271	534	114
219	431	310	272	535	062
220	432	322	273	536	454
221	433	530	274	540	162
222	434	405	275	541	113
223	435	553	276	542	244
224	436	044	277	543	634
225	440	140	278	544	135
226	441	521	279	545	036
227	442	361	280	546	500
228	443	203	281	550	560
229	444	320	282	551	153
230	445	312	283	552	301
231	446	025	284	553	435
232	450	333	285	554	034
233	451	204	286	555	130
234	452	214	287	556	125
235	453	014	288	560	550
236	454	536	289	561	625
237	455	345	290	562	013
238	456	311	291	563	325
239	460	346	292	564	205
240	461	425	293	565	610
241	462	100	294	566	651
242	463	655	295	600	315
243	464	024	296	601	426
297	602	661	321	635	643
298	603	010	322	636	520
299	604	525	323	640	222
300	605	645	324	641	035
301	606	654	325	642	233
302	610	565	326	643	635
303	611	120	327	644	251
304	612	055	328	645	605
305	613	266	329	646	124
306	614	112	330	650	166
307	615	230	331	651	566

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1183 - 1198

308	616	501	332	652	221
309	620	254	333	653	131
310	621	411	334	654	606
311	622	263	335	655	463
312	623	300	336	656	054
313	624	226	337	660	350
314	625	561	338	661	602
315	626	065	339	662	061
316	630	330	340	663	243
317	631	026	341	664	236
318	632	403	342	665	163
319	633	532	343	666	260
320	634	543			

6.Conclusion:

In the discussion of different sections above it is to be noted that the inverses of only 215 polynomials over GF(7^3) with respect to the monic irreducible polynomial x^3+6x^2+4x+1 are successfully found by EEA but in 127 cases it became failure. Here in our work we have found the inverse of all 342 polynomials over GF(7^3) successfully by Gauss-Jordan method . Thus we conclude that theGauss-Jordan method is a generalization of EEA for finding the multiplicative inverses.

7. Acknowledgements:

We express our gratitude to Md. Quamar Talib Shahab for his suggestions and arrangement of books. We are also thankful to Prof. Ranjana, Head of the University Department of Mathematics, T.M. Bhagalpur University, Bhagalpur for providing her moral support and guidance. We would like to express my gratitude to the Variant Research Centre for providing necessary facilities towards research activities.

8. References:

[1] Otokar Grosek, Computing multiplicative inverses in finite fields by long division , Journal of ELECTRICAL ENGINEERING, VOL 69 (2018), NO5, 400-402.

[2] J.K.M. Sadique Uz Zaman, Multiplicative polynomial inverse over $GF(7^3)$: Crisis of EEA and its solution. Springer India (2015),R Chaki et al.(eds.),Applied Computation and security system, Advances in Intelligent System and Computing 305, DOI 10.1007/978-81-322-1988-0_6 .

[3] Forouzan, B.A.,Mukhopadhyay, D.: Cryptography and Network Security, 2nd end. TMH, New Delhi (2011).

[4] Knuth, D.E.: The Art of Computer Programming Seminumerical Algorithms, 3rd edn, Vol. 2.

[5] Arguello, F.: Lehmer-based algorithm for computing inverses in Galois field $GF(7^3)$.

[6] Electron. Lett. IET J. Mag. 42(5), 270-271(2006).

[7] Hassan, M.A. : Double-basis multiplicative inversion over GF(2^m). IEEE Trans. Compute. 47(9) 960-970 (1998).

[8] Stallings, W.: Cryptography and Network Security Principles and Practices, 7th edn. Person Education, Delhi (2008).

[9] Lidl, R., Niederreiter, H.: Finite fields, encyclopedia of mathematics and its applications vol. 20. Addition-Wesley Publishing Company, Boston (1983).
[10] Church, R.: Tables of irreducible polynomials for the first four prime moduli. Ann. Math. 36(1), 198-209(1935).
[11] Brassoud, D., and Wagon, S. computational Number Theory. Emerville, CA: Key College, 2000.
[12] Rosen, K. Elementary Number Theory. Reading, MA: Addition-Wesley,2006.
[13] Stinson, D. Cryptography: Theory and Practice. New York: Chapman & Hall/CRC, 2006.
[14] Leveque, W. Elementary Theory of Numbers. New York: Dover, 1990.
[15] Rabin, M. "Probabilistic Algorithms for Primality Testing." Journal of Number Theory, December 1980.
[16] Ribenboim, P. The New Book of Prime Number Records. New York: Springer-Verlag, 1996.
[17] https://www.academia.edu/attachments/32975915/download_file
[18] Toshiya Itoh, Shigeo Tsujii, Structure of parallel multipliers for a class of fields GF(2m), Information and Computation, Volume 83, Issue 1, 1989 , (https://www.sciencedirect.com/science/article/pii/089054018990045X)