The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

Diminution of Extended Euclidean Algorithm for Finding Multiplicative Inverse in Galois Field $GF\left(p^m\right)$

[1]Neda Fatma, [2]Prof. M.R. Hassan, [3]Dilshad Akhtar, and [4]J.K.M.S. Zaman

[1,3]Research Scholar in Mathematics, T.M. Bhagalpur University, Bhagalpur-812007, India

[2]Professor, University Department of Mathematics, T.M. Bhagalpur University, Bhagalpur, India

[4]Assistant Professor, Department of Computer Science & Application, N.B.U, Siliguri, west Bengal- India

Abstract

This manuscript deals with the theorem on diminution of the Extended Euclidean Algorithm for finding the multiplicative inverse of non-zero elemental polynomials of Galois field $GF\left(p^m\right)$ with respect to a monic irreducible polynomial $I\left(x\right)$ over $F_p=\{0,1,2,3,...,p-1\}$, where p is a prime and m is any positive integer. This method became successful in finding the multiplicative inverse of all those non-zero polynomials for which the Extended Euclidean Algorithm fails. We find the inverse of all 342 non-zero elemental polynomials of $GF\left(7^3\right)$ using an irreducible polynomial $I(x)=x^3+x^2+5x+1$. We also used Cayley Hamilton's theorem for finding the multiplicative inverse of the non-zero elemental polynomials of a finite field.

Keywords: Euclidean Algorithm, Extended Euclidean Algorithm, Galois field, Multiplicative inverse, Irreducible polynomial, Cayley Hamilton's Theorem.

1. Introduction: Generally finite fields are called the Galois field, named after Evariste Galois (1811-1832). The field of order p^m can be generally represented as $GF\left(p^m\right)=\left\{\dfrac{F_p}{\langle I\left(x\right)\rangle}=E\left(x\right)\right\}$, where $F_p=\{0,1,2,3,...,p-1\}$ is the prime field under addition and multiplication modulo p, $I\left(x\right)=\sum_{i=0}^{m}b_ix^i\ \left(b_i\in F_p,b_m\neq 0\right)$ is an irreducible polynomial of a degree m over F_p and $E\left(x\right)=\sum_{i=0}^{m-1}b_ix^i\left(\mathrm{mod}\,I(x)\right)$ is an elemental polynomial of $GF\left(p^m\right)$. It is to be noted that the multiplicative inverse of each non-zero elemental polynomial of $GF\left(p^m\right)$ exist in $GF\left(p^m\right)$ with respect to each irreducible polynomial and multiplicative inverse of non-zero polynomials have a vital role in the field of cryptography. So, Toshiyo Itoh and Shigeo Tsuji (2004) derived the multiplicative inverse of the elemental polynomial of $GF\left(2^m\right)$. Later on, (in 2008) members of the Monzano High School team (New Mexico) calculated the multiplicative inverse of non-zero elements of finite field $GF\left(2^m\right)$ by using EEA (Extended Euclidean Algorithm) and Lagrange's Method. Takagi Kobayshi et al (2007)

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

derived the multiplicative inverse of the finite field $GF\left(2^m\right)$ by using EEA. Christoforus Juan Benvenuto (2012) given basics of Galois Field as well as its implementation in storing data. J.K.M SadiqueUz Zaman et al (2015) studied the multiplicative inverse of the elements of $GF\left(2^8\right)$ and $GF\left(7^3\right)$ by using EEA and he got success to find the multiplicative inverse of all non-zero elemental polynomials over $F_2=\{0,1\}$ but EEA become failure for finding the multiplicative inverse of non-zero elemental polynomials of $GF\left(7^3\right)$ with respect to the irreducible polynomial over $F_7=\{0,1,2,3,4,5,6\}$ in some cases, over $GF\left(7^3\right)$ it is successful when $GCD\left(I(x),E(x)\right)=1$ but when $GCD\left(I(x),E(x)\right)\neq 1$ it becomes a failure. To come over this crisis J.K.M. SadiqueUz Zaman et al (2015) developed a new and successful Algebraic method by which derivation of multiplicative inverses of all the non-zero elemental polynomials of $GF\left(7^3\right)$ with respect to a monic irreducible polynomial become possible. At present we have proposed to diminish the EEA by reducing the number of iterations and find the multiplicative inverses of all non-zero polynomials of $GF\left(7^3\right)$ with respect to each of the monic irreducible polynomial even though the GCD of an irreducible and non-zero elemental polynomial is not unity. For this let us first discuss the EEA, then its success and failure by citing some suitable examples.

2. Extended Euclidean Algorithm (EEA)

It is an extension of the Euclidean Algorithm conceived by the French mathematician Claude Gaspard Bachet De Mezeriac (1581-1638).

Statement If 'a' and 'b' are two positive integers then (by EEA) there exist two integers 'x' and 'y' such that $ax+by=GCD(a,b)$.

Proof Let $a>b$ then by Euclidean Algorithm there exist two integers q_1 and r_1 such that

$a=bq_1+r_1$; $0\le r_1<b$.....(1).

If $r_1\neq 0$ then there exist two integers q_2 and r_2 such that

$b=r_1q_2+r_2$; $0\le r_2<r_1$.....(2).

If $r_2\neq 0$ then again there exist two integers q_3 and r_3 such that

$r_1=r_2q_3+r_3$; $0\le r_3<r_2$.....(3).

Continuing this successive division until the remainder is zero i.e,

$r_{k-3}=r_{k-2}q_{k-1}+r_{k-1}$; $0\le r_{k-1}<r_{k-2}$.....(4).

$r_{k-2}=r_{k-1}q_k+r_k\,(=0)$.....(5).

As we have proposed the diminution of EEA to find the inverse of elements of a finite field by reducing the number of iterations. Hence let us discuss the process to find 'x' and 'y' by iteration.

Initializing the process by taking $A_0=1, A_1=0$ and $B_0=0, B_1=1$, and continuing the iteration as follows.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

$Index(i)$	$Quotient(q_i)$	A_{i+1}	$Remainder(r_i)$
1	q_1	$A_2 = A_0 - q_1 A_1$	r_1
2	q_2	$A_3 = A_1 - q_2 A_2$	r_2
3	q_3	$A_4 = A_2 - q_3 A_3$	r_3
..	..	..	..
$k-1$	q_{k-1}	$A_k = A_{k-2} - q_{k-1} A_{k-1}$	r_{k-1}
k	q_k	$A_{k+1} = A_{k-1} - q_k A_k$	$r_k (= 0)$

By recursive relation and using the above equations we get $aA_{k+1} + bB_{k+1} = r_k$.

Therefore, $aA_k + bB_k = r_{k-1} = GCD(a,b)$

Let, $A_k = x$ and $B_k = y$

$\therefore ax + by = GCD(a,b)$

Example 1 Let us find integers $'x'$ and $'y'$ such that $864x + 128y = GCD(864,128)$

By EA we find $GCD(864,128)$.

$864 = 128 \times 6 + 96$

$128 = 96 \times 1 + 32$

$96 = 32 \times 3 + 0$

$\therefore GCD(864,128) = 32.$

Now, by EEA we can find $'x'$ and $'y'$ such that $864x + 128y = 32$.

Initializing the process by taking $A_0 = 1, A_1 = 0 \;\&\; B_0 = 0, B_1 = 1$ and continuing the iteration as follows.

$Index(i)$	$Quotient(q_i)$	A_{i+1}	B_{i+1}	$Remainder(r_i)$
1	$q_1 = 6$	$A_2 = A_0 - A_1 q_1 = 1$	$B_2 = B_0 - B_1 q_1 = -6$	$r_1 = 96$
2	$q_2 = 1$	$A_3 = A_1 - A_2 q_2 = -1$	$B_3 = B_1 - B_2 q_2 = 7$	$r_2 = 32$
3	$q_3 = 3$	$A_4 = A_2 - A_3 q_3 = 4$	$B_4 = B_2 - B_3 q_3 = -27$	$r_3 = 0$

$\therefore 864 \times A_3 + 128 \times B_3 = r_2$ (By using EEA)

$\Rightarrow 864(-1) + 128(7) = 32$

$\therefore x = -1 \;\&\; y = 7$

2.1. Multiplicative Inverse Of An Element By Using EEA

We use EEA to find the multiplicative inverse of $b \pmod a$ when $GCD(a,b) = 1.$

By EEA, $ax + by = GCD(a,b)$

$\Rightarrow (ax + by) \pmod a = GCD(a,b) \pmod a$

$\Rightarrow ax \pmod a + by \pmod a = 1$

$\Rightarrow 0.x + by \pmod a = 1$

$\Rightarrow by \pmod a = 1$

$\Rightarrow y \pmod a = b^{-1}$

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

$\therefore y$ is the inverse of b under modulo a.

2.2. Multiplicative Inverse Of Elements Of Finite Field Using EEA

Let, $a(x)$ and $b(x)$ be two non-zero elements of $GF\left(p^m\right)$, then (by EEA) there exist two polynomials $p(x)$ and $q(x)$ such that

$a(x)\times p(x)+b(x)\times q(x)=GCD\left(a(x),b(x)\right)$.

If $I(x)$ and $E(x)$ are two polynomials then by EEA there exists two polynomials $P(x)$ and $Q(x)$ such that

$I(x)\times P(x)+E(x)\times Q(x)=GCD\left(I(x),E(x)\right)$.....(6).

Now, if $I(x)$ is an irreducible polynomial over F_p and $E(x)$ is an elemental polynomial of $GF\left(p^m\right)$ such that $GCD\left(I(x),E(x)\right)=1$ then from equation (6)

$\left(I(x)\times P(x)+E(x)\times Q(x)\right)\left(\bmod I(x)\right)=GCD\left(I(x),E(x)\right)$

$\Rightarrow I(x)\times P(x)\left(\bmod I(x)\right)+E(x)\times Q(x)\left(\bmod I(x)\right)=1$

$\Rightarrow E(x)\times Q(x)\left(\bmod I(x)\right)=1$

Therefore, $Q(x)$ is the multiplicative inverse of $E(x)$ in $GF\left(p^m\right)$.

2.3. Successful Application Of EEA

The Galois field (finite field) $GF\left(7^3\right)$ contains 343 elements out of which 342 are non-zero.

(i). Let us find the multiplicative inverse of $E(x)=4x^2+x+2$ with respect to the monic irreducible polynomial $I(x)=x^3+x^2+5x+1$ over F_7.

Apply EA on $I(x)$ and $E(x)$

$x^3+x^2+5x+1=\left(4x^2+x+2\right)\left(2x+5\right)+3x+5$

$4x^2+x+2=\left(3x+5\right)\left(6x+2\right)+6$

$3x+5=6\times 4x+5$

$6=5\times 1+1$

$5=1\times 5+0$

$\therefore GCD\left(I(x),E(x)\right)=1$. Thus, we observe that EEA is applicable to find the inverse of $E(x)$.

Initializing the process by taking $A_0=0$ & $A_1=1$ and continue the iteration as follows.

Index(i)	*Quotient*(q_i)	A_{i+1}	*Remainder*(r_i)
1	$q_1=2x+5$	$A_2=A_0-q_1A_1=-(2x+5)$	$r_1=3x+5$
2	$q_2=6x+2$	$A_3=A_1-q_2A_2=5x^2+6x+4$	$r_2=6$
3	$q_3=4x$	$A_4=A_2-q_3A_3=x^3+4x^2+3x+2$	$r_3=5$
4	$q_4=1$	$A_5=A_3-q_4A_4=6x^3+x^2+3x+2$	$r_4=1$
5	$q_5=5$	$A_6=A_4-q_5A_5=-x^3-x^2+2x-1$	$r_5=0$

In iteration 4 we get A_5 and corresponding remainder r_4 such that, $E(x)A_5\left(\bmod I(x)\right)=r_4$

$\Rightarrow\left(4x^2+x+2\right)\left(6x^3+6x^2+2x+6\right)\left(\bmod x^3+x^2+5x+1\right)=1$.....(7).

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

As, $6x^3+x^2+3x+2\left(\bmod x^3+x^2+5x+1\right)=-x^3-x^2-5x-1+x^2+5x+1+x^2+3x+2$

$=-\left(x^3+x^2+5x+1\right)+\left(2x^2+x+3\right)$

$=2x^2+x+3$

$\therefore$ From equation (7), $\left(2x^2+6x+2\right)\left(2x^2+x+3\right)\left(\bmod x^3+x^2+5x+1\right)=1$.

Therefore, the inverse of $2x^2+6x+2$ is $2x^2+x+3$.

We write $2x^2+6x+2$ as 262 and $2x^2+x+3$ as 213

Therefore, $(262)^{-1} = (213)$

(ii). Let us find the multiplicative inverse of $E(x)=3x^2+6x+2$ with respect to the irreducible polynomial $I(x)=x^3+x^2+5x+1$ over F_7.

Apply EA on $I(x)\,\&\,E(x)$

$x^3+x^2+5x+1=\left(3x^2+x+6\right)(5x+3)+5x+4$

$3x^2+4x+6=(5x+4)(2x+2)+5$

$5x+4=5\times x+4$

$5=4\times 1+1$

$4=1\times 4+0$

$\therefore GCD\left(I(x),E(x)\right)=1$, then EEA is applicable to find the inverse of $E(x)$.

Initializing the process by taking $A_0=0\,\&\,A_1=1$ and continue the iteration as follows.

$Index(i)$	$Quotient(q_i)$	A_{i+1}	$Remainder(r_i)$
1	$q_1=5x+3$	$A_2=A_0-q_1A_1=-(5x+3)$	$r_1=5x+4$
2	$q_2=2x+2$	$A_3=A_1-q_2A_2=3x^2+2x$	$r_2=5$
3	$q_3=x$	$A_4=A_2-q_3A_3=4x^3+5x^2+2x+4$	$r_3=4$
4	$q_4=1$	$A_5=A_3-q_4A_4=3x^3+5x^2+3$	$r_4=1$
5	$q_5=4$	$A_6=A_4-q_5A_5=-x^3-x^2+2x-1$	$r_5=0$

In iteration 4 we get A_5 and the corresponding remainder r_4 such that $E(x)A_5\left(\bmod I(x)\right)=r_4$

$\Rightarrow\left(3x^2+4x+6\right)\left(3x^3+5x^2+3\right)\left(\bmod x^3+x^2+5x+1\right)=1$

$\Rightarrow\left(3x^2+4x+6\right)\left(2x^2+6x\right)\left(\bmod x^3+x^2+5x+1\right)=1$

As, $\left(3x^3+5x^2+3\right)\left(\bmod x^3+x^2+5x+1\right)=2x^2+6x$

$\therefore 2x^2+6x$ is the inverse of $3x^2+4x+6$

(iii). Let us find the multiplicative inverse of $2x^2+6x+6$ with respect to the irreducible polynomial $I(x)=x^3+5x^2+2x+4$ over F_7.

Initializing the process by taking $A_0=0\,\&\,A_1=1$ and continue the iteration as follows.

$Index(i)$	$Quotient(q_i)$	A_{i+1}	$Remainder(r_i)$
1	$q_1=4x+1$	$A_2=A_0-A_1q_1=-(4x+1)$	$r_1=5$
2	$q_2=6x^2+4x+1$	$A_3=A_1-A_2q_2=3x^3+x^2+x+2$	$r_2=1$

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

$\therefore E(x)A_3 \left(\bmod I(x)\right) = r_2$

$\Rightarrow (2x^2+6x+6)(3x^3+x^2+x+2)\left(\bmod I(x)\right) = 1$

$\Rightarrow (2x^2+6x+6)(2x+4)\left(\bmod I(x)\right) = 1.$

Therefore, $2x+4$ is the inverse of $2x^2+6x+6$

2.4. Failure Case of EEA

Let us find the multiplicative inverse of $E(x) = 4x^2+6x+1$ with respect to the irreducible polynomial $I(x) = x^3+5x^2+2x+4$ over F_7.

Apply EA on $I(x) \& E(x)$

$$x^3+5x^2+2x+4 = \left(4x^2+6x+1\right)\left(2x+6\right)+2x+2$$

$$4x^2+6x+1 = \left(2x+2\right)\left(2x+1\right)+6$$

$$2x+2 = 6\times 5x+2$$

$$6 = 2\times 6+0$$

Thus, this method becomes a failure to find GCD because always the $GCD\left(I(x),E(x)\right)$ will be 1.

$\therefore$ EEA does not apply to finding the multiplicative inverse of $E(x)$.

3. Theorem. Diminution Of Extended Euclidean Algorithm (DEEA).

Statement If $I(x)$ is an irreducible polynomial of a degree m over the prime field $F_p = \{0,1,2,3,....., p-1\}$ and $E(x)(\neq 0) \in GF\left(p^m\right)$ then there exists an element $Q(x)(\neq 0) \in GF\left(p^m\right)$ such that $E(x)Q(x)\left(\bmod I(x)\right) = g \in \{2,3,4,.....p-1\}$ Also $Q(x)g^{-1}$ $\left(\bmod I(x)\right)$ is the inverse of $E(x)$ and $E(x)g^{-1}\left(\bmod I(x)\right)$ is the inverse of $Q(x)$, where p is the prime number and m is a positive integer.

Proof Let $GF\left(p^m\right) = \left\{\dfrac{F_p}{\langle I(x)\rangle} = E(x)\right\}$ where $I(x)$ is an irreducible polynomial and $E(x)(\neq 0)$ is a non-constant element of $GF\left(p^m\right)$, Here degree of $I(x) >$ degree $E(x)$ as $E(x)$ is an element of $GF\left(p^m\right)$.

Apply Division Algorithm on $I(x)$ and $E(x)$, then there exists a quotient q_1 and remainder r_1 such that

$I(x) = E(x)q_1 + r_1$; $\deg r_1 < \deg E(x)$.....(8).

If r_1 is not a non-zero constant then we apply Division Algorithm again on $E(x)$ and r_1, then there exists a quotient q_2 and remainder r_2 such that

$E(x) = r_1q_2 + r_2$; $\deg r_2 < \deg r_1$.....(9).

Similarly, we continue the application of the Division Algorithm until the remainder is non-zero constant.

$r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}(=g)$; $\deg r_{k-1} < \deg r_{k-2}$.....(10).

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

Suppose that r_{k-1} is a non-zero constant.

To find $Q(x)(\neq 0)$, initialise the process by taking $A_0 = 0 \& A_1 = 1$ and continuing the iteration as follows.

$Index(i)$	$Quotient(q_i)$	A_{i+1}	$Remainder(r_i)$
1	q_1	$A_2 = A_0 - q_1 A_1$	r_1
2	q_2	$A_3 = A_1 - q_2 A_2$	r_2
3	q_3	$A_4 = A_2 - q_3 A_3$	r_3
..	..	..	..
$k-2$	q_{k-2}	$A_{k-1} = A_{k-3} - q_{k-2} A_{k-2}$	r_{k-2}
$k-1$	q_{k-1}	$A_k = A_{k-2} - q_{k-1} A_{k-1}$	r_{k-1}

Now, $E(x)A_2 \pmod{I(x)} = E(x)(A_0 - q_1 A_1) \pmod{I(x)}$

$= E(x)(0 - q_1) \pmod{I(x)}$

$= r_1$ (By equation (8).)

$E(x)A_3 \pmod{I(x)} = E(x)(A_1 - q_2 A_2)$

$= E(x)A_1 - E(x)A_2 q_2$

$= E(x) - r_1 q_2$

$= r_2$ (By equation (9).)

……

……

Similarly, $E(x)A_k = E(x)(A_{k-2} - q_{k-1} A_{k-1})$

$= E(x)A_{k-2} - E(x)A_{k-1} q_{k-1}$

$= r_{k-3} - r_{k-2} q_{k-1}$

$= r_{k-1}$ (By equation 10)

$\therefore E(x)A_k = r_{k-1}$, for $k = 2,3,4,...,n$

Let, $A_k = Q(x)$ and $r_{n-1} = g$

$\therefore E(x)Q(x) \pmod{I(x)} = g$

$\Rightarrow E(x)Q(x)g^{-1} \pmod{I(x)} = gg^{-1}$

$\Rightarrow E(x)(Q(x)g^{-1}) \pmod{I(x)} = 1$

$\Rightarrow (E(x)g^{-1})Q(x) \pmod{I(x)} = 1$

$\therefore E(x)g^{-1}$ is the inverse of $Q(x)$ and $Q(x)g^{-1}$ is the inverse of $E(x)$.

Hence the theorem.

Example 1 Let us find the multiplicative inverse of $E(x) = 3x^2 + 6x + 2$ with respect to the irreducible polynomial $I(x) = x^3 + x^2 + 5x + 1$ over F_7.

Apply EA on $I(x)$ and $E(x)$

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

$$x^3+x^2+5x+1=\left(3x^2+6x+2\right)\left(5x+2\right)+4x+4$$

$$3x^2+6x+2=\left(4x+4\right)\left(6x+6\right)+6$$

$$4x+4=6\times 3x+4$$

$$6=4\times 1+2$$

$$4=2\times 2+0$$

$\therefore GCD\left(I(x),E(x)\right)\neq 1$

$\therefore$ EEA is not applicable to find the multiplicative inverse of $E(x)$.

Now, we apply our newly developed method Diminution of Extended Euclidean Algorithm. Initializing the process by taking $A_0=0\ \&\ A_1=1$ and continue the iteration as follows.

$Index(i)$	$Quotient(q_i)$	A_{i+1}	$Remainder(r_i)$
1	$q_1=5x+2$	$A_2=A_0-A_1q_1=-(5x+2)$	$r_1=4x+4$
2	$q_2=6x+6$	$A_3=A_1-A_2q_2=2x^2+6$	$r_2=6$

$\therefore E(x)A_3\left(\bmod I(x)\right)=r_2$

$\Rightarrow (3x^2+6x+2)(2x^2+6)\left(\bmod I(x)\right)=6$

$\Rightarrow \left((3x^2+6x+2)(2x^2+6)6\right)\left(\bmod I(x)\right)=6\times 6.....(11).$

$\Rightarrow (3x^2+6x+2)(5x^2+1)\left(\bmod I(x)\right)=1$

$\therefore 5x^2+1$ is the inverse of $3x^2+6x+2$.

Also, from equation (11), $6(3x^2+6x+2)(2x^2+6)=6\times 6$

$\Rightarrow (4x^2+x+5)(2x^2+6)=1$

$\therefore 4x^2+x+5$ is the inverse of $2x^2+6$.

Example 2 Let us find the multiplicative inverse of $E(x)=2x^2+6x+2$ with respect to the monic irreducible polynomial $I(x)=x^3+x^2+5x+1$ over F_7.

Apply EA on $I(x)$ and $E(x)$.

$$x^3+x^2+5x+1=\left(2x^2+6x+2\right)\left(4x+6\right)+3x+3$$

$$2x^2+6x+2=\left(3x+3\right)\left(3x+6\right)+5$$

$$3x+3=5\times 2x+3$$

$$5=3\times 1+2$$

$$3=2\times 1+1$$

$$2=1\times 2+0$$

Initializing the process by taking $A_0=0\ \&\ A_1=1$ and continue the iteration as follows.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

Index(i)	*Quotient*(q_i)	A_{i+1}	*Remainder*(r_i)
1	$q_1 = 4x+6$	$A_2 = A_0 - q_1 A_1 = -(4x+6)$	$r_1 = 3x+3$
2	$q_2 = 3x+6$	$A_3 = A_1 - q_2 A_2 = 5x^2+2$	$r_2 = 5$
3	$q_3 = 2x$	$A_4 = A_2 - q_3 A_3 = 4x^3+6x+1$	$r_3 = 3$
4	$q_4 = 1$	$A_5 = A_3 - q_4 A_4 = 3x^3+5x^2+x+1$	$r_4 = 2$
5	$q_5 = 1$	$A_6 = A_4 - q_5 A_5 = x^3+2x^2+5x$	$r_5 = 1$
6	$q_6 = 2$	$A_7 = A_5 - q_6 A_6 = x^3+x^2+5x+1$	$r_6 = 0$

$\therefore GCD\left(I(x), E(x)\right) = 1$. Therefore, EEA is applicable to find the inverse of $E(x)$. In iteration 5 we get A_6 and the corresponding remainder r_5 such that

$E(x)A_6 \left(\bmod I(x)\right) = 1$

$\Rightarrow \left(2x^2+6x+2\right)\left(x^3+2x^2+5x\right)\left(\bmod x^3+x^2+5x+1\right) = 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (12).$

As $x^3+2x^2+5x\left(\bmod x^3+x^2+5x+1\right) = x^3+2x^2+5x+x^2-x^2+1-1$

$= \left(x^3+x^2+5x+1\right)\left(x^2-1\right)$

$= x^2+6$

$\therefore$ From equation (12), $\left(2x^2+6x+2\right)\left(x^2+6\right)\left(\bmod x^3+x^2+5x+1\right) = 1$

Therefore, the inverse of $2x^2+6x+2$ is x^2+6.

Now, we apply the Diminution of Extended Euclidean Algorithm to find the inverse of $E(x)$.

Here, r_2 is the first non-zero constant therefore by DEEA we get,

$E(x)A_3 \left(\bmod I(x)\right) = r_2$

$\Rightarrow E(x)(5x^2+2)\left(\bmod I(x)\right) = 5$

$\Rightarrow \left(E(x)(5x^2+2)3\right)\left(\bmod I(x)\right) = 5\times 3$

$\Rightarrow E(x)(x^2+6)\left(\bmod I(x)\right) = 1$

$\therefore x^2+6$ is the inverse of $2x^2+6x+2$.

Thus, by DEEA we find the multiplicative inverse of $E(x)$ in the second iteration, but by EEA we find the multiplicative inverse of $E(x)$ in the fifth iteration, therefore DEEA is a very short method to find the multiplicative inverse of elements in a finite field.

Example 3 Let us find the multiplicative inverse of $4x+3$ with respect to the irreducible polynomial $I(x) = x^3+5x^2+2x+4$ over F_7.

Initializing the process by taking $A_0 = 0$ & $A_1 = 1$ and continue the iteration as follows.

Index(i)	*Quotient*(q_i)	A_{i+1}	*Remainder*(r_i)
1	$q_1 = 2x^2+5x+2$	$A_2 = A_0 - q_1 A_1 = -(2x^2+5x+2)$	$r_1 = 5$
2	$q_2 = 2x+2$	$A_3 = A_1 - q_2 A_2 = 3x^3+4x^2+3x+1$	$r_2 = 3$
3	$q_3 = x$	$A_4 = A_2 - q_3 A_3 = 4x^3+x^2+6x+4$	$r_3 = 2$
4	$q_4 = 1$	$A_5 = A_3 - q_4 A_4 = 6x^3+3x^2+4x+4$	$r_4 = 1$
5	$q_5 = 4$	$A_6 = A_4 - q_5 A_5 = -x^3-x^2+2x-1$	$r_5 = 0$

In iteration 4 we get A_5 and the corresponding remainder r_4 such that

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

$E(x)A_5 \left(\mathrm{mod}\, I(x)\right) = 1$

$\Rightarrow \left(2x^2+6x+2\right)\left(6x^3+3x^2+4x+4\right)\left(\mathrm{mod}\, x^3+x^2+5x+1\right)=1$

$\Rightarrow \left(2x^2+6x+2\right)\left(x^2+6x+1\right)\left(\mathrm{mod}\, x^3+x^2+5x+1\right)=1$

Therefore, the inverse of $4x+3$ is x^2+6x+1.

Now, we find the inverse of $E(x)$ by our newly developed method DEEA.

Here, the first remainder is a non-zero constant therefore by DEEA,

$E(x)A_2 = r_1$

$\Rightarrow E(x)(-2x^2-5x-2)=5$

$\Rightarrow E(x)(5x^2+2x+5)3=5\times 3$

$\Rightarrow E(x)(x^2+6x+1)=1$

Therefore, the inverse of $E(x)=4x+3$ is x^2+6x+1.

4. Cayley Hamilton's Theorem

A matrix satisfies its characteristic equation. That is if the characteristic equation of a $n\times n$ matrix A is

$\lambda^n + a_{n-1}\lambda^{n-1} + ... + a_1\lambda + a_0 = 0$, then

$A^n + a_{n-1}A^{n-1} + ... + a_1A + a_0 = 0$

4.1. The Multiplicative Inverse Of Elements Of $GF\left(7^3\right)$ By Using Cayley Hamilton's Theorem

Let $I(x) = x^3 + r_2x^2 + r_1x + r_0$ be a monic irreducible polynomial over $GF(7)$.

We have to find the multiplicative inverse of $a(x) = a_2x^2 + a_1x + a_0$ under the irreducible polynomial $I(x)$

Let, $c(x) = c_2x^2 + c_1x + c_0$ .....(13)

be the multiplicative inverse of the elemental polynomial $a(x)$ over

$GF(7^3)$ with respect to irreducible polynomial $I(x)$ over $GF(7)$.

Then we can write,

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

$\Rightarrow [\,(a_2x^2+a_1x+a_0)\ (c_2x^2+c_1x+c_0)\,] \bmod (x^3+r_2x^2+r_1x+r_0) = 1$

$\Rightarrow [a_2c_2x^4 + (a_2c_1+a_1c_2)x^3 + (a_2c_0+a_1c_1+a_0c_2)x^2 + (a_1c_0+a_0c_1)x + a_0c_0]$

$\mathrm{mod}(x^3+r_2x^2+r_1x+r_0)=1$

$\Rightarrow [a_2c_2x(-r_2x^2-r_1x-r_0)+(a_2c_1+a_1c_2)(-r_2x^2-r_1x-r_0)+(a_2c_0+a_1c_1+a_0c_2)x^2+(a_1c_0+a_0c_1)x+a_0c_0]$

$\mathrm{mod}(x^3+r_2x^2+r_1x+r)_0=1$

$\Rightarrow [-r_2a_2c_2x^3 - r_1a_2c_2x^2 - r_0a_2c_2x - r_2a_2c_1x^2 - r_1a_2c_1x - r_0a_2c_1 - r_2a_1c_2x^2$

$-r_1a_1c_2x - r_0a_1c_2 + (a_2c_0+a_1c_1+a_0c_2)x^2 + (a_1c_0+a_0c_1)x + a_0c_0]\, mod\,(x^3+r_2x^2+r_1x+r_0)=1$

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

$\Rightarrow [-r_2a_2c_2(-r_2x^2-r_1x-r_0)+(-r_1a_2c_2-r_2a_2c_1-r_2a_1c_2+a_2c_0+a_1c_1+a_0c_2)x^2+(-r_0a_2c_2-r_1a_2c_1$
$-r_1a_1c_2+a_1c_0+a_0c_1)x+(r_0a_2c_1-r_0a_1c_2+a_0c_0)] \bmod (x^3+r_2x^2+r_1x+r_0)=1$
$\Rightarrow [\{(r_2^2a_2-r_1a_2-r_2a_1+a_0)c_2+(a_1-r_2a_2)c_1+a_2c_0\}x^2+\{(r_1r_2a_2-r_0a_2-r_1a_1)c_2+(a_0-r_1a_2)c_1$
$+a_1c_0\}x+\{(r_0r_2a_2-r_0a_1)c_2-r_0a_2c_1+a_0c_0\}] \bmod (x^3+r_2x^2+r_1x+r_0)=1$

Equating the coefficient of both sides, then the coefficient of $x^2 \equiv 0 \bmod 7$, the coefficient of $x \equiv 0 \bmod 7$, the constant part $\equiv 1 \bmod 7$

$$\{(r_2^2a_2-r_1a_2-r_2a_1+a_0)c_2+(a_1-r_2a_2)c_1+a_2c_0\}x^2 \bmod 7=0$$
$$\{(r_1r_2a_2-r_0a_2-r_1a_1)c_2+(a_0-r_1a_2)c_1+a_1c_0\} \bmod 7=0$$
$$\{(r_0r_2a_2-r_0a_1)c_2-r_0a_2c_1+a_0c_0\} \bmod 7=1$$

Above equations reduced to,

$$\{(a_2^2b_2+6r_1a_2+6r_2a_1+a_0)c_2+(a_1+6r_2a_2)c_1+a_2c_0\} \bmod 7=0$$
$$\{(r_1r_2a_2+6r_0a_2+6r_1a_1)c_2+(a_0+6r_1a_2)c_1+a_1c_0\} \bmod 7=0$$
$$\{(r_0r_2a_2+6r_0a_1)c_2+6r_0a_2c_1+a_0c_0\} \bmod 7=1$$

The above equations can be written as,

$$\left.\begin{aligned}(l_{00}c_0+l_{01}c_1+l_{02}c_2) \bmod 7=0\\(l_{10}c_0+l_{11}c_1+l_{12}c_2) \bmod 7=0\\(l_{20}c_0+l_{21}c_1+l_{22}c_2) \bmod 7=1\end{aligned}\right\} \quad \text{.....(14)}$$

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

Where,

$l_{00}=(a_2)\%7, l_{01}=(a_1+6r_2a_2)\%7, l_{02}=(r_2^2a_2+6r_1a_2+6r_2a_1+a_0)\%7$.....(15)

$l_{10}=(a_1)\%7, l_{11}=(a_0+6r_1a_2)\%7, l_{12}=(r_1r_2a_2+6r_0a_2+6r_1a_1)\%7$.....(16)

$l_{20}=(a_0)\%7, l_{21}=(6r_0a_2)\%7, l_{22}=(r_0r_2a_2+6r_0a_1)\%7$.....(17)

Equation (14) can be written as,

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

$lc=m$

Where, $l=\begin{bmatrix}l_{00} & l_{01} & l_{02}\\ l_{10} & l_{11} & l_{12}\\ l_{20} & l_{22} & l_{23}\end{bmatrix}$, $c=\begin{bmatrix}c_0\\c_1\\c_2\end{bmatrix}$ and $m=\begin{bmatrix}0\\0\\1\end{bmatrix}$

$\therefore c = l^{-1}m$

To find l^{-1} we use Cayley Hamilton's theorem and after that we get c. We substitute this value in equation (13) and get the inverse of $a(x)=a_2x^2+a_1x+a_0$.

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

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

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

Here, $r_2 = 1, r_1 = 5, r_0 = 1$

$a_2 = 3, a_1 = 0, a_0 = 2$

From (15), (16) and (17), we get,

$l_{00} = 3, l_{01} = 4, l_{02} = 4$

$l_{10} =, l_{11} = 1, l_{12} = 5$

$l_{20} = 2, l_{21} = 4, l_{22} = 3$

Therefore,

$$\begin{bmatrix} 3 & 4 & 4 \\ 0 & 1 & -2 \\ 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 3 & 4 & 4 \\ 0 & 1 & -2 \\ 2 & 4 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad \text{.....(18)}$$

Let, $l = \begin{bmatrix} 3 & 4 & 4 \\ 0 & 1 & -2 \\ 2 & 4 & 3 \end{bmatrix}$

$$\therefore |\lambda I - l| = \begin{vmatrix} \lambda - 3 & -4 & -4 \\ 0 & \lambda - 1 & 2 \\ -2 & -4 & \lambda - 3 \end{vmatrix}$$

$\Rightarrow |\lambda I - l| = (\lambda - 3)\{(\lambda - 1)(\lambda - 3) + 1\} + 4(4) - 4\{2(\lambda - 1)\}$

$= (\lambda - 3)\{\lambda^2 - 4\lambda + 4\} + 2 - \lambda + 1$

$= \lambda^3 - 4\lambda^2 + 4\lambda - 3\lambda^2 + 5\lambda - \lambda + 3$

$= \lambda^3 + \lambda - 2$

Therefore, the characteristic equation is $\lambda^3 + \lambda - 2 = 0$.

By Cayley Hamilton's theorem

$l^3 + l - 2 = 0$

$\Rightarrow l(l^2 + I - 2l^{-1}) = 0$

$\Rightarrow (l^2 + I - 2l^{-1}) = 0$

$\Rightarrow l^{-1} = \frac{1}{2}(l^2 + I)$

$\Rightarrow l^{-1} = 4(l^2 + I)$

$$\Rightarrow l^{-1} = \begin{bmatrix} 2 & 2 & 1 \\ 5 & 4 & 3 \\ 6 & 5 & 5 \end{bmatrix}$$

Now, $c = l^{-1}m$

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

$$\Rightarrow \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 1 \\ 5 & 4 & 3 \\ 6 & 5 & 5 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\therefore \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix}$$

Thus, the inverse of $3x^2 + 2$ is $5x^2 + 3x + 1$.

The complete list of elemental polynomials of $GF(7^3)$ and their inverse with respect to irreducible polynomial $x^3 + x^2 + 5x + 1$ are given in Table1 and Table2.

Table 1: $GF(7^3)$ elements and its inverse on which EEA, Cayley Hamilton's and diminution of EEA all applicable.

Serial Number	Elements	Inverse	Serial Number	Elements	Inverse
1.	001	001	38.	064	546
2.	002	004	39.	065	160
3.	003	005	40.	100	543
4.	004	002	41.	101	221
5.	005	003	42.	103	123
6.	006	006	43.	105	022
7.	010	662	44.	106	262
8.	011	203	45.	110	466
9.	012	610	46.	111	345
10.	014	216	47.	112	511
11.	015	325	48.	113.	421
12.	016	650	49.	114	202
13.	020	331	50.	115	060
14.	021	143	51.	116	651
15.	022	105	52.	120	061
16.	023	516	53.	122	524
17.	024	340	54.	125	465
18.	025	360	55.	130	615
19.	030	223	56.	132	363
20.	031	134	57.	135	463
21.	032	315	58.	140	136
22.	034	240	59.	144	603
23.	035	352	60.	145	124
24.	036	250	61.	146	313
25.	040	554	62.	150	255
26.	041	520	63.	151	354

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

27.	042	425	64.	152	500
28.	043	530	65.	154	026
29.	044	406	66.	160	065
30.	045	462	67.	166	230
31.	050	446	68.	200	625
32.	051	623	69.	201	355
33.	052	410	70.	204	161
34.	053	430	71.	206	415
35.	055	602	72.	210	453
36.	060	115	73.	212	435
37.	061	120	74.	215	545

Serial Number	Elements	Inverse	Serial Number	Elements	Inverse
75.	220	233	123.	360	025
76.	221	101	124.	365	564
77.	222	526	125.	400	316
78.	223	030	126.	403	454
79.	224	644	127.	405	246
80.	225	364	128.	410	052
81.	226	214	129.	411	341
82.	230	166	130.	412	213
83.	231	013	131.	414	645
84.	232	562	132.	415	206
85.	234	600	133.	420	265
86.	235	263	134.	421	113
87.	240	034	135.	425	042
88.	241	426	136.	426	241
89.	244	612	137.	430	053
90.	250	036	138.	433	460
91.	251	555	139.	434	401
92.	253	555	140.	435	212
93.	254	320	141.	436	366
94.	255	150	142.	440	155
95.	260	346	143.	441	322
96.	261	054	144.	442	404
97.	262	106	145.	443	532
98.	263	235	146.	444	613
99.	300	461	147.	445	142
100.	301	033	148.	446	050

101.	310	344	149.	450	523
102.	311	660	150.	451	656
103.	315	032	151.	453	210
104.	316	400	152.	460	433
105.	320	254	153.	462	045
106.	321	621	154.	463	135
107.	323	303	155.	464	631
108.	325	015	156.	465	125
109.	326	121	157.	500	152
110.	330	622	158.	501	362
111.	331	020	159.	502	646
112.	332	635	160.	504	066
113.	334	245	161.	510	431
114.	335	303	162.	511	112
115.	336	455	163.	512	350
116.	340	024	164.	513	242
117.	341	411	165.	515	601
118.	346	360	166.	520	041
119.	350	512	167.	521	353
120.	352	035	168.	524	122
121.	353	521	169.	525	605
122.	354	151	170.	530	043

Serial Number	Elements	Inverse	Serial Number	Elements	Inverse
171.	531	302	197.	615	130
172.	534	541	198.	620	522
173.	535	264	199.	621	321
174.	536	351	200.	624	361
175.	540	611	201.	626	423
176.	545	215	202.	630	641
177.	550	544	203.	631	464
178.	551	563	204.	634	056
179.	552	413	205.	636	614
180.	553	133	206.	640	162
181.	554	040	207.	643	046
182.	555	251	208.	645	414
183.	556	606	209.	646	502
184.	560	324	210.	650	016
185.	561	063	211.	651	116

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1222 - 1240

186.	562	232	212.	653	632
187.	564	365	213.	654	604
188.	566	402	214.	655	253
189.	600	234	215.	656	451
190.	602	055	216.	660	311
191.	603	144	217.	661	126
192.	604	654	218.	662	010
193.	605	525	219.	663	505
194.	610	012	220.	664	356
195.	612	244	221.	665	266
196.	614	636	222.	666	432

Table 2: List of elements and its inverse on which EEA failed butCayley Hamilton's and DEEA applied.

Serial Number	Elements	Inverse	Serial Number	Elements	Inverse
1.	013	231	16.	131	205
2.	026	154	17.	133	553
3.	033	301	18.	134	031
4.	046	643	19.	136	140
5.	054	261	20.	141	163
6.	056	634	21.	142	445
7.	062	452	22.	143	021
8.	063	561	23.	153	416
9.	066	504	24.	155	440
10.	102	252	25.	156	456
11.	104	633	26.	161	204
12.	121	326	27.	162	640
13.	123	103	28.	163	141
14.	124	245	29.	164	333
15.	126	661	30.	165	533
Serial Number	Elements	Inverse	Serial Number	Elements	Inverse
31.	202	114	76.	413	552
32.	203	011	77.	416	153
33.	205	131	78.	422	506
34.	211	305	79.	423	626
35.	213	412	80.	424	256
36.	214	445	81.	431	510
37.	216	014	82.	432	062

38.	233	220	83.	452	062
39.	236	243	84.	454	403
40.	242	513	85.	455	336
41.	243	236	86.	456	156
42.	245	334	87.	461	300
43.	246	405	88.	466	110
44.	252	102	89.	503	616
45.	256	424	90.	505	663
46.	264	535	91.	506	422
47.	265	420	92.	514	542
48.	266	665	93.	516	023
49.	302	531	94.	522	620
50.	303	335	95.	523	450
51.	304	323	96.	526	222
52.	305	211	97.	532	443
53.	306	343	98.	533	165
54.	312	652	99.	541	534
55.	313	146	100.	542	514
56.	314	642	101.	543	100
57.	322	441	102.	544	550
58.	324	560	103.	546	064
59.	333	164	104.	563	551
60.	342	565	105.	565	342
61.	343	306	106.	601	515
62.	344	310	107.	606	556
63.	345	111	108.	611	540
64.	351	536	109.	613	444
65.	355	201	110.	616	503
66.	356	664	111.	622	330
67.	361	624	112.	623	051
68.	362	501	113.	625	200
69.	363	132	114.	632	653
70.	364	225	115.	633	104
71.	366	436	116.	635	332
72.	401	434	117.	641	630
73.	402	566	118.	642	314
74.	404	442	119.	644	224
75.	406	044	120.	652	312

5. Conclusion

In sections 1 & 2 of the present work we have discussed the Euclidean Algorithm and Extended Euclidean Algorithm with examples. In section 3 we have established a new

theorem “Diminution of Extended Euclidean Algorithm” by which multiplicative inverse of all non-zero elemental polynomials were established in fewer steps in comparison of the others. Out of 342 non-zero elemental polynomials of $GF\left(7^3\right)$ we got success to find the multiplicative inverse of only 222 elemental polynomials using EEA under the monic irreducible polynomial $I(x) = x^3 + x^2 + 5x + 1$ and this process fails for remaining 120 elemental polynomials. For which we applied the DEEA and we got successto find the multiplicative inverse. Cayley Hamilton’s theorem also became successful to find the multiplicative inverse of all the elemental polynomials of $GF\left(p^m\right)$.

6. Acknowledgments

express my gratitude towards Md. Quamar Talib Shahab for his useful suggestion and arrangement of the paper. I am also thankful to Prof. Ranjana, HOD of the university department of mathematics, T.M. Bhagalpur university, Bhagalpur, for her moral support and inspiration. I express my heartiest gratitude tothe variant research centre (India) for providing the necessary facilities toward research.

7. References

[1] Abdalbasit Mohammed, Nurhayat Varol.: 2019.A Review Paper on Cryptography.

[2] Anton Iliev, et al. ‘New algorithms for finding modular multiplicative inverse.’ Neural, Parallel and Scientific Computations October 2020.

[3] Arguello, F.: Lehmer-based algorithm for computing inverses in Galois field $GF(7^3)$. Electron. Lett. IET J. Mag. 42(5), 270-271(2006).

[4] Behrouz A. Forouzan, Debdeep Mukhopadhyay: ‘Cryptography and Network Security’, Mc Graw Hill publication.

[5] Brunner, H., Curiger, A., and Hofstetter, M.: ‘On computing multiplicative inverses in GF(2^m)’, IEEE Trans. Comput., 1993, 42, (8), pp. 1010–1015.

[6] David S. Dummit, Richard M. Foote: ‘Abstract Algebra, Second Edition’, Willey-India.

[7] Douglas R. Stinson, Maura B. Paterson: ‘Cryptography Theory and Practice’, Fourth Edition, CRC Press.

[8] Guo, J.-H., and Wang, C.-L.: ‘Systolic array implementation of Euclid’s algorithm for inversion and division in GF(2^m)’, IEEE Trans. Comput., 1998, 47, (10), pp. 1161–1167

[9] J.K.M. SadiqueUz Zaman, Ranjan Ghosh: ‘Multiplicative Polynomial Inverse Over $GF\left(7^3\right)$’: Crisis Of EEA and its Solution, Springer India 2015.

[10] Joseph A.Gallian: ‘Contemporary Abstract Algebra’, Fourth Edition, Narosa Publishing House. Chapter 22.

[11] K. Kobayashi, N. Takagi and K. Takagi, "An Algorithm for Inversion in GF(2^m) Suitable for Implementation Using a Polynomial Multiply Instruction on GF(2)," 18th IEEE Symposium on Computer Arithmetic (ARITH '07), Montpellier, France, 2007, pp. 105-112, doi: 10.1109/ARITH.2007.9.

[12] Knuth, Donald.: ‘The Art of Computer Programming. Addison-Wesley’. Volume 2, Chapter 4.

[13] Lehmer, D.H.: 'Euclid's algorithm for large numbers', Am. Math. Mon., 1938, 45, pp. 227–233.

[14] R. Church: 'The Annals of Mathematics', Second Series, Vol. 36, No. 1 (Jan., 1935), Pp. 198-209.

[15] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein.: 'Introduction to Algorithms, Second Edition'. Mit Press and Mcgraw-Hill, 2001. ISBN 0-262-03293-7.

[16] 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)

[17] W.Stallings,: ' Cryptography and Network Security', 7th Edition, Pearson Education.

[18] Yan, Z., and Starwate, D.V.: 'New systolic architectures for inversion and division in GF(2^m)', IEEE Trans. Comput., 2003, 52, (11), pp. 1514– 1519.