**International Journal of Mathematics and Computer Research**

**ISSN: 2320-7167**

**Volume 09 Issue 09 September 2021, Page no. – 2381-2389**

**Index Copernicus ICV: 57.55, Impact Factor: 7.184**

**DOI: 10.47191/ijmcr/v9i9.02**

# GCD of Aunu Binary Polynomials of Cardinality Seven Using Extended Euclidean Algorithm

**Ibrahim A. A.[1], S.I. Abubakar[2], I. Zaid[3], S. Shehu[4], A. Rufa'i[5]**

[1]Department of Mathematics, Umaru Ali Shinkafi Polytechnic Sokoto

[2,3,4,5] Department of Mathematics, Sokoto State University, Sokoto, Nigeria

**ARTICLE INFO**

Published Online:
24 September 2021

Corresponding Author:
**S.I. Abubakar**

**ABSTRACT**

Finite fields is considered to be the most widely used algebraic structures today due to its applications in cryptography, coding theory, error correcting codes among others. This paper reports the use of extended Euclidean algorithm in computing the greatest common divisor (gcd) of Aunu binary polynomials of cardinality seven. Each class of the polynomial is permuted into pairs until all the succeeding classes are exhausted. The findings of this research reveals that the gcd of most of the pairs of the permuted classes are relatively prime. This results can be used further in constructing some cryptographic architectures that could be used in design of strong encryption schemes.

**KEYWORDS:** Aunu Binary, Polynomials, gcd, Extended Euclidean, Algorithm, Finite Fields

## I. INTRODUCTION

The use of modern means of communication for transmitting information over an insecure channels has been the business of the day due to the advent of information and communication technologies. Cryptography as a discipline provides security by ensuring that information reached its destination without being tempered by an eavesdropper and the medium of communication are properly secured from replay attack, side channel attack, brute force attack, public key exponent attack, short decryption exponent attack, partial key exposure attack, among others.

The origin of finite fields started from the 17th and 18th centuries. The first steps were done by Fermet (1601- 1665), Euler (1707-1783), Lagrange (1736-1813), Legendre (1752-1833), [1]. All of them worked for some special fields: $F_p$ where $p$ is a prime. The elements in this field is integer modulo $p$.

The theory of finite fields was constructed at the end of 18th and during the 19th century by Carl Friendrich Guass (1775-1855) and Evariste Galois (1811-1832). Guass worked on problems in finite fields around 1779-1798, at the time when he was working on his famous DisquisitionesArithmeticcae (1801). His work gave much emphasis on the factorization of polynomials over finite fields. The other giant, Galois, lived a very short life but very interesting one. His paper Sur la theorie des mumbres marked the beginning of finite field or Galois field. The complete work of Galois was compiled by Liouville in 1846, [1].

Finite fields are widely used in modern cryptographic designs and architecture of both symmetric and asymmetric cryptosystems such as RSA, pairing based cryptography advanced encryption standard and elliptic curve cryptography. The arithmetic operations of a finite field when performed efficiently can improve the execution speed of a cryptosystem and requires a small amount of space in design process. Binary finite field is fast and simple to implement in hardware and software design of modern cryptosystem as reported by [2].

Aunu permutation pattern has been reported to be of combinatorial and group theoretical importance, [3]. Binary polynomials of Aunu permutation pattern satisfying some pattern avoidance and their arithmetic operations was reported earlier by the authors in [4] and [5].

The computation of greatest common divisor (gcd) of two polynomials over some fields or unique factorization domain remains a fundamental and significant problem in mathematics and computer science community. Euclid was the first to develop an algorithm of computing gcd of two integers and it has emerged to become one of the most useful tools in mathematics today, [6]. The system was later improved to compute the gcd of polynomials using extended Euclidean algorithm.

In the area of cryptography, many researches has been published. Agnew, G. B, Beth, T. Mullin, R. C., (1993) presented work on Arithmetic operations in GF ($2^m$) where they discussed various techniques of computing multiplicative inverses and exponentiation as reported in [1]. Other applications of finite fields can be found in [7],[8],[9],[10], [11],[12],[13],[14] and [15].

This paper reports a new technique of computing the gcd of Aunu binary polynomials of cardinality seven using extended Euclidean algorithm where each class of the polynomials is permutated up to the number of its succeeding classes by pairing. In the first stage, the paper uses the binary polynomials as constructed by the authors and reported in [4] and [5]. Then, the permutations of the polynomials in pairs follow i.e for $p_1(x)$, it is permutated into six pairs as outlined below:1. $(p_2(x), p_1(x))$ 2. $(p_3(x), p_1(x))$ 3. $(p_4(x), p_1(x))$ 4. $(p_5(x), p_1(x))$ 5. $(p_6(x), p_1(x))$, 6. $(p_7(x), p_1(x))$ and computation of the gcd of each pair of the polynomial was carried out using extended Euclidean algorithm. $p_2(x)$ can be permuted into five classes as follows:1. $(p_3(x), p_2(x))$ 2. $(p_4(x), p_2(x))$ 3. $(p_5(x), p_2(x))$ 4. $(p_6(x), p_2(x))$ 5. $(p_7(x), p_2(x))$. $p_3(x)$ can be permuted into four classes as follows: 1. $(p_4(x), p_3(x))$ 2. $(p_5(x), p_3(x))$ 3. $(p_6(x), p_3(x))$ 4. $(p_7(x), p_3(x))$. $p_4(x)$ can be permuted into three classes as follows: 1. $(p_5(x), p_4(x))$, 2. $(p_6(x), p_4(x))$ 3. $(p_7(x), p_4(x))$. $p_5(x)$ can be permuted into two classes as follows: 1. $(p_6(x), p_5(x))$ 2. $(p_7(x), p_5(x))$. $p_6(x)$ can be permuted into one class as follows: 1. $(p_7(x), p_6(x))$. The findings of this work is expected to be of cryptographic significant as most of the gcd found are relatively prime. Some of the gcd’s are found to be a divisor of the dividend polynomials.

This paper is divided into five sections. Section one covers introduction part of the paper, section two gives some definitions of basic terms as used in the paper, section three reports the methodology of the paper i.e extended Euclidean algorithm, section four presents the major findings of the paper and finally, section five gives conclusion of the paper.

## II. DEFINITION OF BASIC TERMS

A. Aunu Polynomials

The Aunu polynomials were derived from binary codes generated in which an algorithm was constructed to convert the Aunu permutation pattern into binary codes using a defined generating function, as reported in [4,5].

B. Greatest Common Divisor

For a pair of polynomials $p_1, p_2 \in F_q[x]$ there exists a uniquely determined monic polynomial

$d \in F_q[x]$ such that:

1. d divides $p_1$ *and* $p_2$

2. any polynomial $k \in F_q[x]$ dividing both $p_1$ *and* $p_2$ *also divides d.*

The polynomial d is called the greatest common divisor of $p_1$ *and* $p_2$ and is denoted by $\gcd(p_1, p_2)$.

C. The Extended Euclidean Algorithm (EEA) computes the greatest common divisor of two polynomials and also establishes an equation relating them. Let $p, k \in F_q[x]$, then extended Euclidean algorithm gives polynomials $a, b \in F_q[x]$, *such that*

$$\mathrm{ap} + \mathrm{bk} = gcd(\mathrm{p}, \mathrm{k}).$$

## III. PROCEDURE/METHODOLOGY

The procedure of computing gcd using EEA is given in steps. Each step is a reduction algorithm of the form $D - q.d = r$ where the parameters $(D, q, d, r)$ stand for dividend, quotient, divisor and remainder respectively. For each such line, the next replaces the previous dividend $D$ by the previous divisor $d$, and replaces the divisor by the previous remainder $r$. The algorithm terminates when the right hand side (remainder) is 0. The last non-zero remainder is the greatest common divisor.

Each step in the Euclidean algorithm is a division with remainder, and the dividend for the next step is the divisor of the current step, the next divisor is the current remainder, and a new remainder is computed.

That is, to compute the gcd of polynomials $f(x) and\ g(x), initialize\ F(x) = f(x), G(x) = g(x)$

$R(x) = f(x)g(x)$

While $R(x) \neq 0$

$replace\ F(x) by\ G(x)$

$replace\ G(x) by\ R(x)$

$recompute\ R(x) = F(x).G(x)$

When $R(x) = 0,\ G(x) = \gcd(f(x), g(x))$.

Alternatively, the gcd can be computed using the following algorithm

Algorithm

$f = q_1 g + r_1$

$g = q_2 r_1 + r_2$

$g = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

.

.

.

$r_{l-1} = q_l r_l + 0$

We have $\gcd(f, g) = r_l$ .

The Euclidean algorithm for polynomials with coefficients in a field $(F_{2={}^{z}/_{2}})$ is exactly parallel in structure to the Euclidean algorithm for integers.

## IV. RESULTS

This section presents constructed polynomials representation of Aunu permutation of cardinality seven as reported in [3,4]. We also use the Extended Euclidean algorithm in the computation of the gcd for pairs of polynomials in this category.

$p_1(x) = x^2 + x + 1$

$p_2(x) = x^4 + x^3 + 1$

$p_3(x) = x^8 + x^6 + x^4 + x^2 + x + 1$

$p_4(x) = x^{12} + x^9 + x^7 + x^6 + x^5 + 1$

$p_5(x) = x^{14} + x^8 + x^7 + x^5 + x^2 + x + 1$

$p_6(x) = x^{16} + x^{15} + x^{14} + x^{11} + x^9 + x^8 + x^7 + x^4 + 1$

$p_7(x) = x^{19} + x^{18} + x^{15} + x^{12} + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$

The computation of the gcd of the above binary polynomials using EEA is presented below:

A. $p_1(x)$ can be permuted into six classes and their gcd is computed as follows:

1.$(p_2(x), p_1(x))$ 2.$(p_3(x), p_1(x))$ 3. $(p_4(x), p_1(x))$ 4. $(p_5(x), p_1(x))$5. $(p_6(x), p_1(x))$, 6. $(p_7(x), p_1(x))$.

1. Compute the gcd of $p_2(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$p_2(x) = x^4 + x^3 + 1, \qquad p_1(x) = x^2 + x + 1$

$x^4 + x^3 + 1 + (x^2 + x + 1)(x^2 + 1) = x + 1$

$x^2 + x + 1 + (x + 1)(x) = 1$

$x + 1 + (1)(x + 1) = 0$

$\therefore \textit{the} \gcd \textit{of} \ (p_2(x), p_1(x)) = 1$

2. Compute the gcd of $p_3(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$p_3(x) = x^8 + x^6 + x^4 + x^2 + x + 1, \qquad p_1(x) = x^2 + x + 1$

$x^8 + x^6 + x^4 + x^2 + x + 1 + (x^2 + x + 1)(x^6 + x^5 + x^4 + 1) = 0$

$\therefore p_1(x)$ is a factor of $p_3(x)$

3. Compute the gcd of $p_4(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$p_4(x) = x^{12} + x^9 + x^7 + x^6 + x^5 + 1, \qquad p_1(x) = x^2 + x + 1$

$x^8 + x^6 + x^4 + x^2 + x + 1 + (x^2 + x + 1)(x^{10} + x^9 + x^5) = 1$

$x^2 + x + 1 + (1)(x^2 + x + 1) = 0$

$\therefore \textit{The} \gcd \textit{of} \ (p_4(x), p_1(x)) = 1$

4. Compute the gcd of $p_5(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$p_5(x) = x^{14} + x^8 + x^7 + x^5 + x^2 + x + 1, \qquad p_1(x) = x^2 + x + 1$

$x^{14} + x^8 + x^7 + x^5 + x^2 + x + 1 + (x^2 + x + 1)(x^{12} + x^{11} + x^9 + x^5 + x^4 + x^3 + x + 1) = 1$

$x^2 + x + 1 + (1)(x^2 + x + 1) = 0$

$\therefore The\,\mathrm{gcd}\,of\ (p_5(x), p_1(x)) = 1$

5. Compute the gcd of $p_6(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$p_6(x) = x^{16} + x^{15} + x^{14} + x^{11} + x^9 + x^8 + x^7 + x^4 + 1, \qquad p_1(x) = x^2 + x + 1$

$x^{16} + x^{15} + x^{14} + x^{11} + x^9 + x^8 + x^7 + x^4 + 1 + (x^2 + x + 1)(x^{14} + x^9 + x^7 + x^2 + x) = x + 1$

$x^2 + x + 1 + (x + 1)(x) = 1$

$x + 1 + (1)(x + 1) = 0$

$\therefore The\,\mathrm{gcd}\,of\ (p_6(x), p_1(x)) = 1$

6. Compute the gcd of $p_7(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$p_7(x) = x^{19} + x^{18} + x^{15} + x^{12} + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1, \qquad p_1(x) = x^2 + x + 1$

$x^{19} + x^{18} + x^{15} + x^{12} + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1 + (x^2 + x + 1)(x^{17} + x^{15} + x^{14} + x^{13} + x^{11}$
$+ x^9 + x^8 + x^3 + x) = 1$

$x^2 + x + 1 + (x^2 + x + 1)(1) = 0$

$\therefore The\,\mathrm{gcd}\,of\ (p_7(x), p_1(x)) = 1$

B. $p_2(x)$ can be permuted into five classes and their gcd is computed as follows:

1. $(p_3(x), p_2(x))$ 2. $(p_4(x), p_2(x))$ 3. $(p_5(x), p_2(x))$ 4. $(p_6(x), p_2(x))$
5. $(p_7(x), p_2(x))$.

1. Compute the gcd of $p_3(x)$ and $p_2(x)$ as polynomials with coefficients in GF (2)

$p_3(x) = x^8 + x^6 + x^4 + x^2 + x + 1, \qquad p_2(x) = x^4 + x^3 + 1$

$x^8 + x^6 + x^4 + x^2 + x + 1 + (x^4 + x^3 + 1)(x^4 + x^3) = x^3 + x^2 + x + 1$

$x^4 + x^3 + 1 + (x^3 + x^2 + x + 1)(x) = x^2 + x + 1$

$x^3 + x^2 + x + 1 + (x^2 + x + 1)(x) = 1$

$x^2 + x + 1 + (1)(x^2 + x + 1) = 0$

$\therefore the\,\mathrm{gcd}\,of\ (p_3(x), p_2(x)) = 1$

2. Compute the gcd of $p_4(x)$ and $p_2(x)$ as polynomials with coefficients in GF (2)

$p_4(x) = x^{12} + x^9 + x^7 + x^6 + x^5 + 1, \qquad p_2(x) = x^4 + x^3 + 1$

$x^{12} + x^9 + x^7 + x^6 + x^5 + 1 + (x^4 + x^3 + 1)(x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1) = x^2$

$x^4 + x^3 + 1 + (x^2)(x^2 + x) = 1$

$x^2 + (1)(x^2) = 0$

$\therefore the\,\mathrm{gcd}\,of\ (p_4(x), p_2(x)) = 1$

3. Compute the gcd of $p_5(x)$ and $p_2(x)$ as polynomials with coefficients in GF (2)

$p_5(x) = x^{14} + x^8 + x^7 + x^5 + x^2 + x + 1, \qquad p_2(x) = x^4 + x^3 + 1$

$x^{14} + x^8 + x^7 + x^5 + x^2 + x + 1 + (x^4 + x^3 + 1)(x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + x$
$= x^3 + 1$

$x^4 + x^3 + 1 + (x^3 + 1)(x + 1) = x$

$x^3 + 1 + (x)(x^2) = 1$

$x + (1)(x) = 0$

$\therefore The \gcd of\ (p_5(x), p_2(x)) = 1$

4. Compute the gcd of $p_6(x)$ and $p_2(x)$ as polynomials with coefficients in GF (2)

$p_6(x) = x^{16} + x^{15} + x^{14} + x^{11} + x^9 + x^8 + x^7 + x^4 + 1, \qquad p_2(x) = x^4 + x^3 + 1$

$x^{16} + x^{15} + x^{14} + x^{11} + x^9 + x^8 + x^7 + x^4 + 1 + (x^4 + x^3 + 1)(x^{12} + x^{10} + x^9 + x^7 + x^4 + x^3 + x^2 + x + 1) = x^2 + x$

$x^4 + x^3 + 1 + (x^2 + x)(x^2) = 1$

$x^2 + x + (1)(x^3 + x) = 0$

$\therefore The \gcd of\ (p_6(x), p_2(x)) = 1$

5. Compute the gcd of $p_7(x)$ and $p_2(x)$ as polynomials with coefficients in GF (2)

$p_7(x) = x^{19} + x^{18} + x^{15} + x^{12} + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1, \qquad p_2(x) = x^4 + x^3 + 1$

$x^{19} + x^{18} + x^{15} + x^{12} + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1 + (x^4 + x^3 + 1)(x^{15} + x^8 + x^7 + x^6 + x^5 + 1) = x^3 + 1$

$x^4 + x^3 + 1 + (x^3 + 1)(x + 1) = x$

$x^3 + 1 + (x)(x^2) = 1$

$x + (1)(x) = 0$

$\therefore The \gcd of\ (p_7(x), p_2(x)) = 1$

C. $p_3(x)$ can be permuted into four classes and their gcd is computed as follows:

1. $(p_4(x), p_3(x))$ 2. $(p_5(x), p_3(x))$ 3. $(p_6(x), p_3(x))$ 4. $(p_7(x), p_3(x))$

1. Compute the gcd of $p_4(x)$ and $p_3(x)$ as polynomials with coefficients in GF (2)

$p_4(x) = x^{12} + x^9 + x^7 + x^6 + x^5 + 1, \qquad p_3(x) = x^8 + x^6 + x^4 + x^2 + x + 1$

$x^{12} + x^9 + x^7 + x^6 + x^5 + 1 + (x^8 + x^6 + x^4 + x^2 + x + 1)(x^4 + x^2 + x) = x^6 + x^5 + x + 1$

$x^8 + x^6 + x^4 + x^2 + x + 1 + (x^6 + x^5 + x + 1)(x^2 + x) = x^4 + x^3 + x + 1$

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

$x^4 + x^3 + x + 1 + (x^3 + x^2 + x + 1)(x) = x^2 + 1$

$x^3 + x^2 + x + 1 + (x^2 + 1)(x + 1) = 0$

$\therefore the \gcd of\ (p_4(x), p_3(x)) = x^2 + 1$

2. Compute the gcd of $p_5(x)$ and $p_3(x)$ as polynomials with coefficients in GF (2)

$p_5(x) = x^{14} + x^8 + x^7 + x^5 + x^2 + x + 1, \qquad p_3(x) = x^8 + x^6 + x^4 + x^2 + x + 1$

$x^{14} + x^8 + x^7 + x^5 + x^2 + x + 1 + (x^8 + x^6 + x^4 + x^2 + x + 1)(x^6 + x^4 + 1) = x^6$

$(x^8 + x^6 + x^4 + x^2 + x + 1 + (x^6)(x^2 + 1) = x^4 + x^2 + x + 1$

$x^6 + (x^4 + x^2 + x + 1)(x^2 + 1) = x^3 + x + 1$

$x^4 + x^2 + x + 1 + (x^3 + x + 1)(x) = 1$

$x^3 + x + 1 + (1)(x^3 + x + 1) = 0$

$\therefore the \gcd of\ (p_5(x), p_3(x)) = 1$

3. Compute the gcd of $p_6(x)$ and $p_3(x)$ as polynomials with coefficients in GF (2)

$p_6(x) = x^{16} + x^{15} + x^{14} + x^{11} + x^9 + x^8 + x^7 + x^4 + 1, \qquad p_3(x) = x^8 + x^6 + x^4 + x^2 + x + 1$

$$x^{16}+x^{15}+x^{14}+x^{11}+x^{9}+x^{8}+x^{7}+x^{4}+1+(x^{8}+x^{6}+x^{4}+x^{2}+x+1)(x^{8}+x^{7}+x^{5}+x^{4}+x^{3}+x=x^{4}+x^{2}+x+1$$

$$x^{8}+x^{6}+x^{4}+x^{2}+x+1+(x^{4}+x^{2}+x+1)(x^{4}+x)=x^{3}+1$$

$$x^{4}+x^{2}+x+1+(x^{3}+1)(x)=x^{2}+1$$

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

$$x^{2}+1+(x+1)(x)=x+1$$

$$x+1+(1)(x+1)=0$$

$$\therefore The\ \text{gcd}\ of\ \ (p_6(x),p_3(x))=x+1$$

4. Compute the gcd of $p_7(x)$ and $p_3(x)$ as polynomials with coefficients in GF (2)

$$p_7(x)=x^{19}+x^{18}+x^{15}+x^{12}+x^{7}+x^{6}+x^{5}+x^{4}+x^{2}+x+1,$$
$$p_3(x)=x^{8}+x^{6}+x^{4}+x^{2}+x+1$$

$$x^{19}+x^{18}+x^{15}+x^{12}+x^{7}+x^{6}+x^{5}+x^{4}+x^{2}+x+1+(x^{8}+x^{6}+x^{4}+x^{2}+x+1)(x^{11}+x^{10}+x^{9}+x^{8}+x^{6}+x^{5}+x^{3}+x^{2}+x+1)=x^{5}+x^{4}+1$$

$$x^{8}+x^{6}+x^{4}+x^{2}+x+1+(x^{5}+x^{4}+1)(x^{3}+x^{2})=\ x^{4}+x^{3}+x^{2}+1$$

$$x^{4}+x^{2}+(x^{4}+x^{3}+x^{2}+1)(x)=x^{3}+x^{2}$$

$$x^{4}+x^{3}+x^{2}+1+(x^{3}+x^{2})(x)=x^{2}+x+1$$

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

$$x^{2}+x+1+(x)(x+1)=1$$

$$x+(1)(x)$$

$$\therefore The\ \text{gcd}\ of\ \ (p_7(x),p_3(x))=1$$

D. $p_4(x)$ can be permuted into three classes and their gcd is computed as follows:

1. $(p_5(x),p_4(x))$ 2. $(p_6(x),p_4(x))$ 3. $(p_7(x),p_4(x))$

1. Compute the gcd of $p_5(x)$ and $p_4(x)$ as polynomials with coefficients in GF (2)

$$p_5(x)=x^{14}+x^{8}+x^{7}+x^{5}+x^{2}+x+1,\qquad p_4(x)=x^{12}+x^{9}+x^{7}+x^{6}+x^{5}+1$$

$$x^{14}+x^{8}+x^{7}+x^{5}+x^{2}+x+1+(x^{12}+x^{9}+x^{7}+x^{6}+x^{5}+1)(x^{2})=x^{11}+x^{9}+x^{5}+x+1$$

$$x^{12}+x^{9}+x^{7}+x^{6}+x^{5}+1+(x^{11}+x^{9}+x^{5}+x+1)(x)=x^{10}+x^{9}+x^{7}+x^{5}+x^{2}+x+1$$

$$x^{11}+x^{9}+x^{5}+x+1+(x^{10}+x^{9}+x^{7}+x^{5}+x^{2}+x+1)(x+1)=x^{8}+x^{7}+x^{6}+x^{3}+x$$

$$x^{10}+x^{9}+x^{7}+x^{5}+x^{2}+x+1+(x^{8}+x^{7}+x^{6}+x^{3}+x)(x^{2}+1)=x^{6}+x^{2}+1$$

$$x^{8}+x^{7}+x^{6}+x^{3}+x+(x^{6}+x^{2}+1)(x^{2}+x+1)=x^{4}+1$$

$$x^{6}+x^{2}+1+(x^{4}+1)(x^{2})=1$$

$$x^{4}+1+(1)(x^{4}+1)=0$$

$$\therefore the\ \text{gcd}\ of\ \ (p_5(x),p_4(x))=1$$

2. Compute the gcd of $p_6(x)$ and $p_4(x)$ as polynomials with coefficients in GF (2)

$$p_6(x)=x^{16}+x^{15}+x^{14}+x^{11}+x^{9}+x^{8}+x^{7}+x^{4}+1,\qquad p_4(x)=x^{12}+x^{9}+x^{7}+x^{6}+x^{5}+1$$

$$x^{16}+x^{15}+x^{14}+x^{11}+x^{9}+x^{8}+x^{7}+x^{4}+1+(x^{12}+x^{9}+x^{7}+x^{6}+x^{5}+1)(x^{4}+x^{3}+x^{2}+x+1)=x^{8}+x^{7}+x^{6}+x^{5}+x^{3}+x^{2}+1$$

$$x^{12}+x^{9}+x^{7}+x^{6}+x^{5}+1+(x^{8}+x^{7}+x^{6}+x^{5}+x^{3}+x^{2}+1)(x^{4}+x^{3}+x)=x^{5}+x^{3}+x^{2}$$

$x^8+x^7+x^6+x^5+x^3+x^2+1+(x^5+x^3+x^2)(x^3+x^2+1)=x^4+x$

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

$x^4+x+(x^3)(x)=x$

$x^3+(x)(x^2)=0$

$\therefore\ the\ \mathrm{gcd}\ of\ \ (p_6(x),p_4(x))=x$

3. Compute the gcd of $p_7(x)$ and $p_4(x)$ as polynomials with coefficients in GF (2)

$p_7(x)=x^{19}+x^{18}+x^{15}+x^{12}+x^7+x^6+x^5+x^4+x^2+x+1,$

$p_4(x)=x^{12}+x^9+x^7+x^6+x^5+1$

$$x^{19}+x^{18}+x^{15}+x^{12}+x^7+x^6+x^5+x^4+x^2+x+1+(x^{12}+x^9+x^7+x^6+x^5+1)(x^7+x^6+x^4+x^2)=x^{11}+x^9+x^7+x^5$$

$x^{12}+x^9+x^7+x^6+x^5+1+(x^{11}+x^9+x^7+x^5)(x)=x^{10}+x^9+x^8+x^7+x^5+1$

$x^{11}+x^9+x^7+x^5+(x^{10}+x^9+x^8+x^7+x^5+1)(x+1)=x^9+x^6+x+1$

$x^{10}+x^9+x^8+x^7+x^5+1+(x^9+x^6+x+1)(x+1)=x^8+x^6+x^5+x+1$

$x^9+x^6+x+1+(x^8+x^6+x^5+x+1)(x)=x^7+x^3+x^2+x$

$x^8+x^6+x^5+x+1+(x^7+x^3+x^2+x)(x)=x^6+x^5+x^4+x^3+x+1$

$x^7+x^3+x^2+x+(x^6+x^5+x^4+x^3+x+1)(x+1)=x^4+x^3+x+1$

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

$x^4+x^3+x+1+(x^3+x^2)(x)=x+1$

$x^3+x^2+(x+1)(x^2)=0$

$\therefore\ The\ \mathrm{gcd}\ of\ \ (p_7(x),p_4(x))=x+1$

E. $p_5(x)$ can be permuted into two classes and their gcd is computed as follows:

1. $(p_6(x),p_5(x))$ 2. $(p_7(x),p_5(x))$

1. Compute the gcd of $p_6(x)$ and $p_5(x)$ as polynomials with coefficients in GF (2)

$p_6(x)=x^{16}+x^{15}+x^{14}+x^{11}+x^9+x^8+x^7+x^4+1,\qquad p_5(x)=x^{14}+x^8+x^7+x^5+x^2+x+1$

$$x^{16}+x^{15}+x^{14}+x^{11}+x^9+x^8+x^7+x^4+1+(x^{14}+x^8+x^7+x^5+x^2+x+1)(x^2+x+1)=x^{11}+x^{10}+x^9+x^8+x^7+x^6$$

$x^{14}+x^8+x^7+x^5+x^2+x+1+(x^{11}+x^{10}+x^9+x^8+x^7+x^6)(x^3+x^2)=x^7+x^5+x+1$

$x^{11}+x^{10}+x^9+x^8+x^7+x^6+(x^7+x^5+x+1)(x^4+x^3+1)=x^6+x^3+x+1$

$x^7+x^5+x+1+(x^6+x^3+x+1)(x)=x^5+x^4+x^2+1$

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

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

$x^4+x^2+(x^3+1)(x)=x^2+x$

$x^3+1+(x^2+x)(x+1)=x+1$

$x^2+x+(x+1)(x)=0$

$\therefore\ the\ \mathrm{gcd}\ of\ \ (p_6(x),p_5(x))=x+1$

2. Compute the gcd of $p_7(x)$ and $p_5(x)$ as polynomials with coefficients in GF (2)

$p_7(x)=x^{19}+x^{18}+x^{15}+x^{12}+x^7+x^6+x^5+x^4+x^2+x+1,$

$p_5(x)=x^{14}+x^8+x^7+x^5+x^2+x+1$

$$x^{19}+x^{18}+x^{15}+x^{12}+x^7+x^6+x^5+x^4+x^2+x+1$$
$$+(x^{14}+x^8+x^7+x^5+x^2+x+1)(x^5+x^4+x)$$
$$=x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^3+1$$

$$x^{14}+x^8+x^7+x^5+x^2+x+1+(x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^3+1)(x+1)$$
$$=x^{10}+x^9+x^8+x^7+x^4+x^3+x^2$$

$$x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^3+1+(x^{10}+x^9+x^8+x^7+x^4+x^3+x^2)(x^3)$$
$$=x^8+x^3+x$$

$$x^{10}+x^9+x^8+x^7+x^4+x^3+x^2+(x^8+x^3+x)(x^2+x+1)=x^7+x^6+x+1$$

$$x^8+x^3+x+(x^7+x^6+x+1)(x+1)=x^6+x^3+x^2$$

$$x^7+x^6+x+1+(x^6+x^3+x^2)(x+1)=x^4+x^2+x+1$$

$$x^6+x^3+x^2+(x^4+x^2+x+1)(x^2+1)=x^2+x+1$$

$$x^4+x^2+x+1+(x^2+x+1)(x^2+x+1)=x$$

$$x^2+x+1+(x)(x+1)=1$$

$$x+(1)(x)=0$$

$$\therefore \mathit{the}\ \mathrm{gcd}\ \mathit{of}\ \ (p_7(x),p_5(x))=1$$

F. Compute the gcd of $p_7(x)$ and $p_6(x)$ as polynomials with coefficients in GF (2)

$$p_7(x)=x^{19}+x^{18}+x^{15}+x^{12}+x^7+x^6+x^5+x^4+x^2+x+1,$$
$$p_6(x)=x^{16}+x^{15}+x^{14}+x^{11}+x^9+x^8+x^7+x^4+1$$

$$x^{19}+x^{18}+x^{15}+x^{12}+x^7+x^6+x^5+x^4+x^2+x+1$$
$$+(x^{16}+x^{15}+x^{14}+x^{11}+x^9+x^8+x^7+x^4+1)(x^3+x+1)$$
$$=x^{15}+x^{12}+x^7+x^6+x^3+x^2$$

$$x^{16}+x^{15}+x^{14}+x^{11}+x^9+x^8+x^7+x^4+1+(x^{15}+x^{12}+x^7+x^6+x^3+x^2)(x+1)$$
$$=x^{14}+x^{13}+x^{12}+x^{11}+x^9+x^3$$

$$x^{15}+x^{12}+x^7+x^6+x^3+x^2+(x^{14}+x^{13}+x^{12}+x^{11}+x^9+x^3)(x+1)$$
$$=x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^3+x^2$$

$$x^{14}+x^{13}+x^{12}+x^{11}+x^9+x^3+(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^3+x^2)(x^2)$$
$$=x^{10}+x^7+x^6+x^5+x^4$$

$$x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^3+x^2+(x^{10}+x^7+x^6+x^5+x^4)(x^2+x+1)$$
$$=x^8+x^6+x^4+x^3+x^2$$

$$x^{10}+x^7+x^6+x^5+x^4+(x^8+x^6+x^4+x^3+x^2)(x^2+1)=x^7+x^6+x^4+x^3+x^2$$

$$x^8+x^6+x^4+x^3+x^2+(x^7+x^6+x^4+x^3+x^2)(x+1)=x^5+x^4+x^3$$

$$x^7+x^6+x^4+x^3+x^2+(x^5+x^4+x^3)(x^2+1)=x^2$$

$$x^5+x^4+x^3+(x^2)(x^3+x^2+x)=0$$

$$\therefore \mathit{the}\ \mathrm{gcd}\ \mathit{of}\ \ (p_7(x),p_6(x))=x^2$$

## V. CONCLUSION

The greatest common divisor of Aunu binary polynomials using extended Euclidean algorithm has been successfully reported by this paper. The results of this paper shows that the gcd are found to be coprime in most of the permuted pairs while some are factors of their permuted pairs. The result also gives polynomials as gcd of some classes of the computed pairs of polynomials. This has an important application in cryptographic design as it could be further treated for the construction of strong encryption schemes.

**REFERENCES**

1. Daniel Panario (2006). A Minicourse in Finite Fields and Applications, School of Mathematics and Statistics, Carleton University.
2. Dawood Shah and Tariq Shah (2021). Binary Galois field extension dependents multimedia data security scheme. *Micropocessors and Microsystems*, 77, 103181.
3. A.A Ibrahim (2007). An Enumeration Scheme and Algebraic properties of a Special (132)-avoiding Class of permutation Pattern. *Trends in Applied sciences Research Academic Journals Inc. USA.* 2(4) 334-340.
4. Abubakar S.I, Shehu S., Ibrahim Z. Ibrahim A.A (2014). Some polynomials representation using the 123-avoiding class of the Aunu permutation patterns of cardinality five using binary codes. *International Journal of Scientific and Engineering Research* 5(8), 1-4.
5. Saidu Isah Abubakar , Aminu Alhaji Ibrahim (2014). Polynomial Representation of Aunu Permutation Patterns (123-Avoiding), published by Lambert Publishing Company ISBN 978-3-659-63532-8.
6. Qiang Zhou, T. Chenliang, Z. Hanlin, J. Yu, Fengjun Li (2020). How to securely outsource the extended Euclidean algorithm for large scale polynomials over finite fields. *Information Sciences*, 641-660.
7. Cenk, M., Hassan, M.A. (2014). Some new results on binary polynomial multiplication. *Journal of Cryptographic Engineering*, 5(4), 289-303.
8. D’angella, D., Schiavo, C.V., Visconti, A (2013). Tight upper bounds for polynomial multiplication. In: *Applied Computing Conference* 2013. Acc’13. WEAS. 31-37.
9. McEliece, R.J. (1987). Finite fields for computer scientists and engineers, vol.23. Kluwer Academic Publishers Boston (1987).
10. Homma, N., Saito, K., Aoki, T. (2014). Toward formal design of practical cryptographic hardware based on Galois field arithmetic. *IEEE Transactions on Computers*, 63(10), 2604-2613.
11. Benvenuto, C. J. (2012). Galois field in cryptography. *University of Washington*, *1*(1), 1-11.
12. Savas, E., & Koç, Ç. K. (2010). Finite field arithmetic for cryptography. *IEEE Circuits and Systems Magazine*, *10*(2), 40-56.
13. Guajardo, J., Güneysu, T., Kumar, S. S., Paar, C., & Pelzl, J. (2006). Efficient hardware implementation of finite fields with applications to cryptography. *Acta Applicandae Mathematica*, *93*(1-3), 75-118.
14. Wolf, C., & Preneel, B. (2004). Asymmetric Cryptography: Hidden Field Equations. *IACR Cryptology ePrint Archive*, *2004*, 72.
15. Shparlinski, I. (2013). *Finite Fields: Theory and Computation: The meeting point of number theory, computer science, coding theory and cryptography* Vol. 477. Springer Science & Business Media.