JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-17, No.-1, January (2022) pp 1-19 ISSN (Print) 0973-8975

EXTENDED EUCLIDEAN ALGORITHM OF AUNU BINARY POLYNOMIALS OF CARDINALITY ELEVEN

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

[1,2,4,5] Department of Mathematics, Sokoto State University, Sokoto, Nigeria.

[3]Department of Mathematics, Umaru Ali Shinkali Polytechnic, Sokoto, Nigeria.

[1]siabubakar82@gmail.com, [2]malamzaid2@gmail.com
[3] aminualhaji40@gmail.com [4]sadiqshehuzezi@gmail.com

https://doi.org/10.26782/jmcms.2022.01.00001

(Received: November 3, 2021; Accepted:January 1, 2022)

Abstract

Binary polynomials representation of Aunu permutation patterns has been used to perform arithmetic operations on words and sub-words of the polynomials using addition, multiplication, and division modulo two. The polynomials were also found to form some mathematical structures such as group, ring, and field. This paper presents the extension of our earlier work as it reports the Aunu binary polynomials of cardinality eleven and how to find their greatest common divisor (gcd) using the extended Euclidean algorithm. The polynomials are pairly permuted and the results found showed that one polynomial is a factor of the other polynomial or one polynomial is relatively prime to the other and some gave different results. This important feature is of combinatorial significance and can be investigated further to formulate some theoretic axioms for this class of Aunu permutation pattern. Binary polynomials have important applications in coding theory, circuit design, and the construction of cryptographic primitives.

Keywords: Algorithm, Aunu, Cryptography, Euclidean, Extended, Galois field, Greatest common divisor, Permutation, Patterns, Polynomials, Binary

I. Introduction

Aunu permutation patterns have been reported to be a class of permutation avoidance which is of combinatorics and group-theoretic importance,[I,II,III]. The binary polynomials were generated from the Aunu permutation patterns and some arithmetic operations were performed as reported in [IV,V].

Finite fields are discrete mathematical objects satisfying all the axioms of a field, much as for the real and complex numbers except for their finiteness. They are also finite sets of objects which have arithmetic that allows the usual operations of addition, subtraction, multiplication, and division except that the set contains only a finite number of distinct elements. They are also referred to as the Galois field after the French mathematician Evariste Galois who was one of the first to show interest in them. It is easy to show that such objects exist only when the number of their elements is a power of a prime number, [VI].

Finite fields have been noticed to be the most widely used algebraic structure in the design of cryptographic schemes. The finite fields have many applications in the areas of coding theory, signal processing, cryptography, combinatorics, engineering, and so on, [VII].

The arithmetic operations of the finite field of characteristic 2 known as binary fields are considered to be very attractive for several cryptographic applications. Such applications usually need efficient implementation in both hardware and software, thus a fast execution of arithmetic operations over a finite field is of utmost importance,[VIII,IX].

One of the approaches to increase the cryptosystems performance is the increasing of the performance of finite field arithmetic in a multiplication operation. Galois field allows manageable and effective data manipulation by using Advanced Encryption Standard (AES) algorithm, [IX].

It has been reported that finite fields are by far, the most widely used algebraic structure in the construction of cryptographic schemes,[VII,X,XI]. The Aunu polynomials generated were also found to form some of these algebraic structures which by extension may likely make it suitable for the construction of such cryptographic schemes.

Over 2300 years ago, Euclid described, in Book 7 proposition 1 and 2 of his elements (c. 300 B.C), a simple algorithm for finding the greatest common divisor of two integers, [8]. The algorithm was chosen by Euclid to be the first step in his development of the theory of numbers. The greatest common divisor of two integers m and n gcd(m,n) is the largest integer that evenly divides both m and n.

A binary greatest common divisor was devised by Stein (1961) as reported in [XII]. This algorithm was based on three simple facts:

1. if m and n are even, $gcd\ (m, n) = gcd\ (\frac{m}{2}, \frac{n}{2})$;

2. If m is even and n is odd, then $gcd(m, n\ ) = gcd\ (\frac{m}{2}, n)$;

3. If m and n are both odd, then m-n is even and $\text{gcd}(m, n) = \text{gcd}(m - n, n)$.

This algorithm relies solely on the subtraction, parity testing, and right shifting of even numbers and requires no division. It is thus more suitable for binary arithmetic.

An algorithm for calculating the modular inverse of an integer can be traced back to the Aryabhatta (A.D 499) of northern India. The multiplicative inverse of an integer m mod n exists if and only if m and n are relatively prime, i.e gcd(m,n) =1. We know that the greatest common divisor of two integers can be expressed as a linear combination of the two numbers. Therefore, we look for two integers r and s that satisfy the equation $mr + ns = 1$. Further, this linear equation says that $mr \equiv 1\ mod\ n$; therefore r is the inverse of m mod n. By reversing the steps in the Euclidean algorithm, one can deriver and s while calculating $gcd(m, n)$. This reversed procedure is known as the Extended Euclidean algorithm, [VI].

This paper presents the use of an extended Euclidean algorithm to find the gcd of Aunu polynomials of cardinality eleven by pairing the polynomials in such a way that it is permutated to all the words and sub-words as the case may be. The paper is divided into five sections which comprise: Introduction, definitions of basic terms, methodology, results, and conclusion.

II. Definitions of Basic Terms

II.i. 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 [IV,V].

II.ii. Greatest Common Divisor

For a pair of polynomials $f1, f2 \in F_q[x]$ there exists a uniquely determined monic polynomial $d \in F_q[x]$ such that:

1. d divides $f1\ and\ f2$

2. any polynomial $g \in F_q[x]$ dividing both $f1\ and\ f2\ also\ divides\ d.$

The polynomial d is called the greatest common divisor of $f1\ and\ f2$ and is denoted by $\gcd(f1, f2)$.

II.iii. The Extended Euclidean Algorithm (EEA) gives not only the greatest common divisor of two polynomials but also an equation relating them. Let $f, g \in F_q[x]$, then Extended Euclidean algorithm gives polynomials $s, t \in F_q[x], such\ that$
$sf + tg = \gcd(f, g)$.

III. Procedure/Methodology

Each step is a reduction algorithm step of the form $D - q.d = r$. For each such line, the next replaces the previous dividend D with the previous divisor d, and replaces the divisor with 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 $R(x) = 0,\ G(x) = \gcd\big(f(x), g(x)\big).$

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

In what follows, we provide derived polynomials representation of Aunu permutation of cardinality eleven using a similar technique as reported [IV,V]. We also use the Extended Euclidean algorithm in the computation of the gcd for pairs of polynomials in this category.

$p_1(x) = x^3 + x + 1$

$p_2(x) = x^6 + x^5 + x^4 + x^3 + 1$

$p_3(x) = x^9 + x^7 + x^4 + x^3 + 1$

$p_4(x) = x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + 1$

$p_5(x) = x^{17} + x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^4 + x^3 + x + 1$

$p_6(x) = x^{20} + x^{19} + x^{17} + x^{16} + x^{11} + x^5 + x^3 + x + 1$

$p_7(x) = x^{24} + x^{21} + x^{19} + x^{16} + x^{14} + x^{12} + x^{11} + x^8 + x^7 + x^6 + x + 1$

$$p_8(x) = x^{27} + x^{26} + x^{23} + x^{22} + x^{18} + x^{17} + x^{15} + x^{14} + x^{12} + x^{11} + x^9 \\ + x^8 + x^6 + x^5 + 1$$

$$p_9(x) = x^{31} + x^{27} + x^{26} + x^{23} + x^{19} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x^{10} \\ + x^8 + x^5 + x^3 + x + 1$$

$$p_{10}(x) = x^{33} + x^{32} + x^{27} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{16} \\ + x^{15} + x^{13} + x^{12} + x^7 + x^6 + x^4 + x^3 + 1$$

$$p_{11}(x) = x^{38} + x^{33} + x^{30} + x^{29} + x^{27} + x^{26} \\ + x^{24} + x^{24} + x^{23} + x^{22} + x^{21} + x^{18} + x^{17} + x^{15} + x^{12} \\ + x^{11} + x^8 + x^6 + x^4 + x + 1$$

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

1. $\big(p_2(x), p_1(x)\big)$ 2. $(p_3(x), p_1(x))$ 3. $\big(p_4(x), p_1(x)\big)$ 4. $(p_5(x), p_1(x))$

5. $\big(p_6(x), p_1(x)\big)$, 6. $(p_7(x), p_1(x))$, 7. $(p_8(x), p_1(x))$, 8. $(p_9(x), p_1(x))$

9. $(p_{10}(x), p_1(x))$, 10. $(p_{11}(x), p_1(x))$

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

$p_2(x) = x^6 + x^5 + x^4 + x^3 + 1, \qquad p_1(x) = x^3 + x + 1$

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

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

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

$\therefore$ gcd($p_2(x)$ $p_1(x)$) = 1

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

$p_3(x)=x^9+x^7+x^4+x^3+1, \quad p_1(x)=x^3+x+1$

$x^9+x^7+x^4+x^3+1+(x^3+x+1)(x^6+x^3)=x^3+x+1$

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

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

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

$p_4(x)=x^{13}+x^{12}+x^{11}+x^8+x^5+x^4+1 \quad , \qquad p_1(x)=x^3+x+1$

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

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

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

$\therefore$ gcd$(p_4(x),p_1(x))=1$

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

$$p_5(x)=x^{17}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^4+x^3+x+1, \quad p_1(x) \\ =x^3+x+1$$

$$x^{17}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^4+x^3+x \\ +(x^3+x+1)(x^{14}+x^{12}+x^7+x^2+x^2)=x^2+x+1$$

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

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

$x+1(x)=0$

$\therefore$ gcd$(p_5(x),p_1(x))=1$

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

$$p_6(x)=x^{20}+x^{19}+x^{17}+x^{16}+x^{11}+x^5+x^3+x+1,\ p_1(x) \\ =x^3+x+1$$

$$x^{20}+x^{19}+x^{17}+x^{16}+x^{11}+x^5+x^3+x+1 \\ +(x^3+x \\ +1)(\ x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{10}+x^7+x^5+x^4 \\ +x^3+x^2+1)=x^2$$

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

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

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

$$\therefore \gcd(p_6(x), p_1(x)) = \ x+1$$

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

$$p_7(x) = x^{24}+x^{21}+x^{19}+x^{16}+x^{14}+x^{12}+x^{11}+x^{8}+x^{7}+x^{6}+x+1,$$
$$p_1(x) = x^3+x+1$$

$$p_7(x) = x^{24}+x^{21}+x^{19}+x^{16}+x^{14}+x^{12}+x^{11}+x^{8}+x^{7}+x^{6}+x+1$$
$$+(x^3+x+1)(x^{21}+x^{19}+x^{17}+x^{15}+x^{14}+x^{9}+x^{8}+x^{7}+x^{5}+x^{2}+x)$$
$$= x^2$$

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

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

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

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

$$\therefore \gcd(p_7(x), p_1(x)) = \ 1$$

7. Compute the gcd of $p_8(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$$p_8(x) = x^{27}+x^{26}+x^{23}+x^{22}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^{11}+x^{9}$$
$$+x^{8}+x^{6}+x^{5}+1, \qquad p_1(x) = x^3+x+1$$

$$x^{27}+x^{26}+x^{23}+x^{22}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^{11}+x^{9}+x^{8}$$
$$+x^{6}+x^{5}+1$$
$$+(x^3+x+1)(x^{24}+x^{23}+x^{22}+x^{18}+x^{17}+x^{15}+x^{14}$$
$$+x^{12}+x^{10}+x^{7}+x^{6}+x^{5}+x^{3}+x+1) = x^2$$

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

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

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

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

$$\therefore \gcd(p_8(x), p_1(x)) = 1$$

8. Compute the gcd of $p_9(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$$p_9(x) = x^{31}+x^{27}+x^{26}+x^{23}+x^{19}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{10}$$
$$+x^{8}+x^{5}+x^{3}+x+1, \ p_1(x) = x^3+x+1$$

$$x^{31}+x^{27}+x^{26}+x^{23}+x^{19}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{10}+x^{8}+x^{5}$$
$$+x^{3}+x+1$$
$$+(x^3+x$$
$$+1)(x^{28}+x^{26}+x^{25}+x^{23}+x^{23}+x^{22}+x^{21}+x^{20}+x^{17}$$
$$+x^{16}+x^{15}+x^{14}+x^{13}+x^{10}+x^{5}+x^{3}+x) = x^2+1$$

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

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

$$\therefore \gcd(p_9(x), p_1(x)) = \ 1$$

9. Compute the gcd of $p_{10}(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$$\begin{aligned} p_{10}(x) = x^{33} + x^{32} + x^{27} &\\ &+ x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{16} + x^{15} \\ &+ x^{13} + x^{12} + x^{7} + x^{6} + x^{4} + x^{3} + 1,\ \ p_1(x) = x^3 + x + 1 \end{aligned}$$

$$\begin{aligned} x^{33} + x^{32} + x^{27} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{16} + x^{15} &\\ &+ x^{13} + x^{12} + x^{7} + x^{6} + x^{4} + x^{3} + 1 \\ &+ (x^3 + x + 1)(x^{30} + x^{29} + x^{28} + x^{25} + x^{24} + x^{23} + x^{21} \\ &+ x^{20} + x^{18} + x^{13} + x^{12} + x^{11} + x^{10} + x^{9} + x^{6} + x + 1) \\ &= x^2 \end{aligned}$$

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

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

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

$$\therefore \gcd(p_{10}(x), p_1(x)) = 1$$

10. Compute the gcd of $p_{11}(x)$ and $p_1(x)$ as polynomials with coefficients in GF (2)

$$\begin{aligned} p_{11}(x) = x^{38} + x^{33} + x^{30} + x^{29} + x^{27} + x^{26} &\\ &+ x^{24} + x^{24} + x^{23} + x^{22} + x^{21} + x^{18} + x^{17} + x^{15} + x^{12} \\ &+ x^{11} + x^{8} + x^{6} + x^{4} + x + 1\ \ ,\qquad p_1(x) = x^3 + x + 1 \end{aligned}$$

$$\begin{aligned} x^{38} + x^{33} + x^{30} + x^{29} + x^{27} + x^{26} &\\ &+ x^{24} + x^{24} + x^{23} + x^{22} + x^{21} + x^{18} + x^{17} + x^{15} + x^{12} \\ &+ x^{11} + x^{8} + x^{6} + x^{4} + x + 1 + (x^3 + x \\ &+ 1)(x^{35} + x^{33} + x^{32} + x^{31} + x^{30} + x^{26} + x^{21} + x^{20} + x^{18} \\ &+ x^{17} + x^{16} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^{9} + x^{8} + x^{6} \\ &+ x) = x^2 + 1 \end{aligned}$$

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

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

$$\therefore \gcd(p_{11}(x), p_1(x)) =\ 1$$

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

1. $(p_3(x), p_2(x))$ 2. $(p_4(x), p_2(x))$3. $\big(p_5(x), p_2(x)\big)$ 4. $(p_6(x), p_2(x))$

5. $\big(p_7(x), p_2(x)\big)$, 6. $(p_8(x), p_2(x))$, 7. $(p_9(x), p_2(x))$, 8. $(p_{10}(x), p_2(x))$

9. $(p_{11}(x), p_2(x))$.

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

$$p_3(x) = x^9 + x^7 + x^4 + x^3 + 1, \qquad p_2(x) = x^6 + x^5 + x^4 + x^3 + 1$$

$$\begin{aligned} x^9 + x^7 + x^4 + x^3 + 1 + (x^6 + x^5 + x^4 + x^3 + 1)(x^3 + x^2 + x + 1) &\\ &= x^2 + 1 \end{aligned}$$

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

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

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

$$\therefore gcd(p_3(x)\,,p_2(x))=1$$

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

$$p_4(x)=x^{13}+x^{12}+x^{11}+x^8+x^5+x^4+1,\ p_2(x)=x^6+x^5+x^4+x^3+1$$

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

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

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

$$\therefore gcd(p_4(x)\,,p_2(x))=1$$

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

$$p_5(x)=x^{17}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^4+x^3+x+1\,,\quad p_2(x)=x^6+x^5+x^4+x^3+1$$

$$x^{17}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^4+x^3+x+1+(x^6+x^5+x^4+x^3+1)(x^{11}+x^{10}+x^8+x^7+x^6+x^3+x^2)=x^3+1$$

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

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

$$\therefore gcd(p_5(x)\,,p_2(x))=\ x^2+x+1$$

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

$$p_6(x)=x^{20}+x^{19}+x^{17}+x^{16}+x^{11}+x^5+x^3+x+1,\quad p_2(x)=x^6+x^5+x^4+x^3+1$$

$$x^{20}+x^{19}+x^{17}+x^{16}+x^{11}+x^5+x^3+x+1+(x^6+x^5+x^4+x^3+1)(x^{14}+x^{12}+x^{11}+x^{10}+x^9+x^4+x^2+1)=x^5+x^3+x^2+x$$

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

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

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

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

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

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

$$p_7(x)=x^{24}+x^{21}+x^{19}+x^{16}+x^{14}+x^{12}+x^{11}+x^8+x^7+x^6+x+1,\quad p_2(x)=x^6+x^5+x^4+x^3+1$$

$$x^{24}+x^{21}+x^{19}+x^{16}+x^{14}+x^{12}+x^{11}+x^{8}+x^{7}+x^{6}+x+1$$
$$+(x^{6}+x^{5}+x^{4}+x^{3}+1)(x^{18}$$
$$+x^{17}+x^{15}+x^{14}+x^{13}+x^{9}+x^{9}+x^{7}+x^{5}+x^{2}+x$$
$$+1)=x^{3}+x^{2}$$

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

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

$$\therefore gcd(p_7(x)\ ,p_2(x))=\ x^{3}+x^{2}$$

6. Compute the gcd of $p_8(x)$ and $p_2(x)$ as polynomials with coefficients in GF (2)

$$p_8(x)=x^{27}+x^{26}+x^{23}+x^{22}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^{11}+x^{9}$$
$$+x^{8}+x^{6}+x^{5}+1,\qquad p_2(x)=x^{6}+x^{5}+x^{4}+x^{3}+1$$

$$x^{27}+x^{26}+x^{23}+x^{22}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^{11}+x^{9}+x^{8}$$
$$+x^{6}+x^{5}+1$$

$$+(x^{6}+x^{5}+x^{4}+x^{3}+1)(x^{21}+x^{19}+x^{13}+x^{10}+x^{6}+x^{2}+x)$$
$$=x^{5}+x^{4}+x^{2}+x+1$$

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

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

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

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

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

$$\therefore gcd(p_8(x)\ ,p_2(x))=\ 1$$

7. Compute the gcd of $p_9(x)$ and $p_2(x)$ as polynomials with coefficients in GF (2)

$$p_9(x)=x^{31}+x^{27}+x^{26}+x^{23}+x^{19}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{10}+x^{8}$$
$$+x^{5}+x^{3}+x+1,\qquad p_2(x)=x^{6}+x^{5}+x^{4}+x^{3}+1$$

$$x^{31}+x^{27}+x^{26}+x^{23}+x^{19}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{10}+x^{8}+x^{5}$$
$$+x^{3}+x+1$$
$$+(x^{6}+x^{5}+x^{4}+x^{3}+1)(x^{25}+^{24}+x^{20}+x^{19}+x^{18}+x^{15}$$
$$+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3})=x^{3}+x^{2}+x$$

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

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

$$\therefore gcd(p_9(x)\ ,p_2(x))=\ x^{2}+x+1$$

8. Compute the gcd of $p_{10}(x)$ and $p_2(x)$ as polynomials with coefficients in GF (2)

$$p_{10}(x)=x^{33}+x^{32}+x^{27}$$
$$+x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{16}+x^{15}$$
$$+x^{13}+x^{12}+x^{7}+x^{6}+x^{4}+x^{3}+1,\ \ p_2(x)$$
$$=x^{6}+x^{5}+x^{4}+x^{3}+1$$

$$x^{33}+x^{32}+x^{27}+x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{16}+x^{15}+x^{13}+x^{12}+x^{7}+x^{6}+x^{4}+x^{3}+1+(x^{6}+x^{5}+x^{4}+x^{3}+1)(x^{27}+x^{25}+x^{23}+x^{21}+x^{16}+x^{15}+x^{14}+x^{12}+x^{10}+x^{4}+x^{3}+x+1)=x^{3}+1$$

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

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

$$\therefore gcd(p_{10}(x)\ ,p_{2}(x))=\ x^{2}+x+1$$

9. Compute the gcd of $p_{11}(x)$ and $p_{2}(x)$ as polynomials with coefficients in GF (2)

$$p_{11}(x)=x^{38}+x^{33}+x^{30}+x^{29}+x^{27}+x^{26}+x^{24}+x^{24}+x^{23}+x^{22}+x^{21}+x^{18}+x^{17}+x^{15}+x^{12}+x^{11}+x^{8}+x^{6}+x^{4}+x+1\ ,\ \ p_{2}(x)=x^{6}+x^{5}+x^{4}+x^{3}+1$$

$$x^{38}+x^{33}+x^{30}+x^{29}+x^{27}+x^{26}+x^{24}+x^{24}+x^{23}+x^{22}+x^{21}+x^{18}+x^{17}+x^{15}+x^{12}+x^{11}+x^{8}+x^{6}+x^{4}+x+1+(x^{6}+x^{5}+x^{4}+x^{3}+1)(x^{32}+x^{31}+x^{28}+x^{24}+x^{20}+x^{19}+x^{17}+x^{16}+x^{12}+x^{11}+x^{10}+x^{7}+x^{6}+x^{4}+x^{2}+x)=x^{3}+x^{2}+1$$

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

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

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

$$\therefore gcd(p_{11}(x)\ ,p_{2}(x))=\ 1$$

C. $p_{3}(x)$ can be permuted into eight classes and their gcd is computed as follows:

1. $(p_{4}(x),p_{3}(x))$ 2. $(p_{5}(x),p_{3}(x))$ 3. $\big(p_{6}(x),p_{3}(x)\big)$ 4. $(p_{7}(x),p_{3}(x))$
5. $\big(p_{8}(x),p_{3}(x)\big)$, 6. $(p_{9}(x),p_{3}(x))$, 7. $(p_{10}(x),p_{3}(x))$, 8. $(p_{11}(x),p_{3}(x))$.

1. Compute the gcd of $p_{4}(x)$ and $p_{3}(x)$ as polynomials with coefficients in GF (2)

$$p_{4}(x)=x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4}+1\ \ p_{3}(x)=x^{9}+x^{7}+x^{4}+x^{3}+1$$

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

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

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

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

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

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

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

$$\therefore \text{gcd}\ (p_{4}(x),p_{3}(x))=1$$

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

$$p_5(x) = x^{17} + x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^4 + x^3 + x + 1,\ p_3(x) = x^9 + x^7 + x^4 + x^3 + 1$$

$$x^{17} + x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^4 + x^3 + x + 1 + (x^9 + x^7 + x^4 + x^3 + 1)(x^8 + x^6 + x^5 + x^3 + x^2 + x + 1) = x^6 + x^5 + x^4 + x^3 + x^2$$

$$(x^9 + x^7 + x^4 + x^3 + 1 + (x^6 + x^5 + x^4 + x^3 + x^2)(x^3 + x^2 + x + 1) = x^3 + x^2 + 1$$

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

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

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

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

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

$$p_6(x) = x^{20} + x^{19} + x^{17} + x^{16} + x^{11} + x^5 + x^3 + x + 1,\quad p_3(x) = x^9 + x^7 + x^4 + x^3 + 1$$

$$x^{20} + x^{19} + x^{17} + x^{16} + x^{11} + x^5 + x^3 + x + 1 + (x^9 + x^7 + x^4 + x^3 + 1)(x^{11} + x^{10} + x^9 + x^6 + x^4 + x^3 + x^2 + x + 1) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2$$

$$x^9 + x^7 + x^4 + x^3 + 1 + (x^7 + x^6 + x^5 + x^4 + x^3 + x^2)(x^2 + x + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$$

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

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

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

$\therefore$ gcd $(p_6(x), p_3(x)) = x + 1$

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

$$p_7(x) = x^{24} + x^{21} + x^{19} + x^{16} + x^{14} + x^{12} + x^{11} + x^8 + x^7 + x^6 + x + 1,\ p_3(x) = x^9 + x^7 + x^4 + x^3 + 1$$

$$x^{24} + x^{21} + x^{19} + x^{16} + x^{14} + x^{12} + x^{11} + x^8 + x^7 + x^6 + x + 1 + (x^9 + x^7 + x^4 + x^3 + 1)(x^{15} + x^{13} + x^{12} + x^{11} + x^{10} + x^7 + x^6 + x^4 + x + 1) = x^8 + x^5 + x^4 + x^3$$

$$x^9 + x^7 + x^4 + x^3 + 1 + (x^8 + x^5 + x^4 + x^3)(x) = x^7 + x^6 + x^5 + x^3 + 1$$

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

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

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

$\therefore$ gcd $(p_7(x), p_3(x)) = 1$

5. Compute the gcd of $p_8(x)$ and $p_3(x)$ as polynomials with coefficients in GF (2)

$$\begin{aligned} p_8(x) = x^{27} + x^{26} + x^{23} + x^{22} + x^{18} + x^{17} + x^{15} + x^{14} + x^{12} + x^{11} + x^9 \\ + x^8 + x^6 + x^5 + 1, \quad p_3(x) = x^9 + x^7 + x^4 + x^3 + 1 \end{aligned}$$

$$\begin{aligned} x^{27} + x^{26} + x^{23} + x^{22} + x^{18} + x^{17} + x^{15} + x^{14} + x^{12} + x^{11} + x^9 + x^8 \\ + x^6 + x^5 + 1 \\ + (x^9 + x^7 + x^4 + x^3 + 1)(x^{18} + x^{17} + x^{16} + x^{15} + x^{13} \\ + x^{11} + x^8 + x^4 + 1) = x^8 + x^5 + x \end{aligned}$$

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

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

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

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

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

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

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

$\therefore$ gcd $(p_8(x), p_3(x)) = 1$

6. Compute the gcd of $p_9(x)$ and $p_3(x)$ as polynomials with coefficients in GF (2)

$$\begin{aligned} p_9(x) = x^{31} + x^{27} + x^{26} + x^{23} + x^{19} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x^{10} \\ + x^8 + x^5 + x^3 + x + 1, \\ p_3(x) = x^9 + x^7 + x^4 + x^3 + 1 \end{aligned}$$

$$\begin{aligned} x^{31} + x^{27} + x^{26} + x^{23} + x^{19} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x^{10} + x^8 \\ + x^5 + x^3 + x + 1 \\ +(x^9 + x^7 + x^4 + x^3 + 1)(x^{22} + x^{20} + x^{16} + x^{15} + x^{14} + x^{12} + x^9 + x^2 \\ + x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1 \end{aligned}$$

$$\begin{aligned} x^9 + x^7 + x^4 + x^3 + 1 + (x^6 + x^5 + x^4 + x^3 + x^2 + 1)(x^3 + x^2 + x + 1) \\ = x + 1 \end{aligned}$$

$$x^6 + x^5 + x^4 + x^3 + x^2 + 1 + (x + 1)(x^5 + x^3 + x + 1) = 0$$

$\therefore$ gcd $(p_9(x), p_3(x)) = x + 1$

7. Compute the gcd of $p_{10}(x)$ and $p_3(x)$ as polynomials with coefficients in GF (2)

$$\begin{aligned} p_{10}(x) = x^{33} + x^{32} + x^{27} \\ + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{16} + x^{15} \\ + x^{13} + x^{12} + x^7 + x^6 + x^4 + x^3 + 1, \\ p_3(x) = x^9 + x^7 + x^4 + x^3 + 1 \end{aligned}$$

$$\begin{aligned} x^{33} + x^{32} + x^{27} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{16} + x^{15} + \\ x^{13} + x^{12} + x^7 + x^6 + x^4 + x^3 + 1 + (x^9 + x^7 + x^4 + x^3 + 1)(x^{24} +^{23}+ \\ x^{22} + x^{21} + x^{20} + x^{14} + x^{12} + x^8 + x^6 + x^5 + x^2) = x^8 + x^6 + x^5 + x^4 + \\ x^2 + x+1 \end{aligned}$$

$$\begin{aligned} x^9 + x^7 + x^4 + x^3 + 1 + (x^8 + x^6 + x^5 + x^4 + x^2 + x + 1)(x) \\ = x^6 + x^4 + x^2 + x + 1 \end{aligned}$$

$$x^8+x^6+x^5+x^4+x^2+x+1+(x^6+x^4+x^2+x+1)(x^2)$$
$$=x^5+x^3+x+1$$
$$x^6+x^4+x^2+x+1+(x^5+x^3+x+1)(x)=1$$
$$x^5+x^3+x+1+(1)(x^5+x^3+x+1)=0$$
$$\therefore \text{gcd}\,(p_{10}(x),p_3(x))=\ x^5+x^3+x+1$$

8. Compute the gcd of $p_{11}(x)$ and $p_3(x)$ as polynomials with coefficients in GF (2)

$$p_{11}(x)=x^{38}+x^{33}+x^{30}+x^{29}+x^{27}+x^{26}$$
$$+x^{24}+x^{24}+x^{23}+x^{22}+x^{21}+x^{18}+x^{17}+x^{15}+x^{12}$$
$$+x^{11}+x^8+x^6+x^4+x+1,\ \ p_3(x)$$
$$=x^9+x^7+x^4+x^3+1$$
$$x^{38}+x^{33}+x^{30}+x^{29}+x^{27}+x^{26}$$
$$+x^{24}+x^{24}+x^{23}+x^{22}+x^{21}+x^{18}+x^{17}+x^{15}+x^{12}$$
$$+x^{11}+x^8+x^6+x^4+x+1$$
$$+(x^9+x^7+x^4+x^3$$
$$+1)(x^{29}+x^{27}+x^{25}+x^{22}+x^{19}+x^{17}+x^{13}+x^{10}+x^9$$
$$+x^6+x^5+x^3+x^2+x)=x^7+x^5+x^3+x^2+1$$
$$x^9+x^7+x^4+x^3+1+(x^7+x^5+x^3+x^2+1)(x^2)$$
$$=x^5+x^3+x^2+1$$
$$x^7+x^5+x^3+x^2+1+(x^5+x^3+x^2+1)(x^2)=x^4+x^3+1$$
$$x^5+x^3+x^2+1+(x^4+x^3+1)(x+1)=x^2+x$$
$$x^4+x^3+1+(x^2+x)(x^2)=1$$
$$x^2+x+(1)(x^2+x)=0$$
$$\therefore \text{gcd}\,(p_{11}(x),p_3(x))=\ 1$$

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

1. $(p_5(x),p_4(x))$ 2. $(p_6(x),p_4(x))$3. $\left(p_7(x),p_4(x)\right)$ 4. $(p_8(x),p_4(x))$

5. $\left(p_9(x),p_4(x)\right)$, 6. $(p_{10}(x),p_4(x))$, 7. $(p_{11}(x),\,p_4(x))$.

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

$$p_5(x)=x^{17}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^4+x^3+x+1,$$
$$p_4(x)=x^{13}+x^{12}+x^{11}+x^8+x^5+x^4+1$$

$$x^{17}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^4+x^3+x+1$$
$$+(x^{13}+x^{12}+x^{11}+x^8+x^5+x^4+1)(x^4+x^3+1)$$
$$=x^{12}+x^{10}+x^9+x^7+x^5+x^4+x$$

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

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

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

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

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

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

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

$$\therefore \gcd(p_5(x), p_4(x)) = 1$$

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

$$p_6(x) = x^{20} + x^{19} + x^{17} + x^{16} + x^{11} + x^5 + x^3 + x + 1,\ p_4(x) = x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + 1$$

$$x^{20} + x^{19} + x^{17} + x^{16} + x^{11} + x^5 + x^3 + x + 1 + (x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + 1)(x^7 + x^5 + x^2 + x + 1) = x^{12} + x^{11} + x^8 + x^4 + x^3 + x^2$$

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

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

$$x^{11} + x^9 + x^8 + x^2 + 1 + (x^{10} + x^2 + x + 1)(x) = x^9 + x^8 + x^2 + x + 1$$

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

$$x^9 + x^8 + x^2 + x + 1 + (x^8 + x^3 + x^2 + x)(x + 1) = x^4 + x^2 + 1$$

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

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

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

$$\therefore \gcd(p_6(x), p_4(x)) = 1$$

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

$$p_7(x) = x^{24} + x^{21} + x^{19} + x^{16} + x^{14} + x^{12} + x^{11} + x^8 + x^7 + x^6 + x + 1,\quad p_4(x) = x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + 1$$

$$x^{24} + x^{21} + x^{19} + x^{16} + x^{14} + x^{12} + x^{11} + x^8 + x^7 + x^6 + x + 1 + (x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + 1)(x^{11} + x^{10}) = x^{12} + x^{10} + x^8 + x^7 + x^6 + x + 1$$

$$\begin{aligned} &x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4}+1 \\ &\qquad +(x^{12}+x^{10}+x^{8}+x^{7}+x^{6}+x+1)(x+1) \\ &\qquad =x^{10}+x^{9}+x^{8}+x^{6}+x^{5}+x^{4}+x^{2} \end{aligned}$$

$$\begin{aligned} &(x^{12}+x^{10}+x^{8}+x^{7}+x^{6}+x+1) \\ &\qquad +(x^{10}+x^{9}+x^{8}+x^{6}+x^{5}+x^{4}+x^{2})(x^{2}+x+1) \\ &\qquad =x^{8}+x^{7}+x^{3}+x^{2}+x+1 \end{aligned}$$

$$\begin{aligned} &x^{10}+x^{9}+x^{8}+x^{6}+x^{5}+x^{4}+x^{2} \\ &\qquad +(x^{8}+x^{7}+x^{3}+x^{2}+x+1)(x^{2}+1) \\ &\qquad =x^{7}+x^{6}+x^{2}+x+1 \end{aligned}$$

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

$$x^{7}+x^{6}+x^{2}+x+1+(1)(x^{7}+x^{6}+x^{2}+x+1)=0$$

$$\therefore \gcd(p_7(x),p_4(x))= \ x+1$$

4. Compute the gcd of $p_8(x)$ and $p_4(x)$ as polynomials with coefficients in GF (2)

$$\begin{aligned} p_8(x)&=x^{27}+x^{26}+x^{23}+x^{22}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^{11}+x^{9} \\ &\quad +x^{8}+x^{6}+x^{5}+1, \\ &\quad p_4(x)=x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4}+1 \end{aligned}$$

$$\begin{aligned} &x^{27}+x^{26}+x^{23}+x^{22}+x^{18}+x^{17}+x^{15}+x^{14}+x^{12}+x^{11}+x^{9}+x^{8} \\ &\qquad +x^{6}+x^{5}+1 \\ &\qquad +(x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4}+1)(x^{14}+x^{12}+x^{11} \\ &\qquad +x^{10}+x^{8}+x^{6}+x^{4}+x^{2}+x+1) \\ &\qquad =x^{10}+x^{9}+x^{7}+x^{5}+x^{2}+x \end{aligned}$$

$$\begin{aligned} &x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4}+1 \\ &\qquad +(x^{10}+x^{9}+x^{7}+x^{5}+x^{2}+x)(x^{3}+x) \\ &\qquad =x^{8}+x^{6}+x^{3}+x^{2}+1 \end{aligned}$$

$$\begin{aligned} &x^{10}+x^{9}+x^{7}+x^{5}+x^{2}+x+(x^{8}+x^{6}+x^{3}+x^{2}+1)(x^{2}+x+1) \\ &\qquad =x^{6}+x^{2}+1 \end{aligned}$$

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

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

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

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

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

$$\therefore \gcd\ (p_8(x),p_4(x))= \ 1$$

5. Compute the gcd of $p_9(x)$ and $p_4(x)$ as polynomials with coefficients in GF (2)

$$\begin{aligned} p_9(x)&=x^{31}+x^{27}+x^{26}+x^{23}+x^{19}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11} \\ &\quad +x^{10}+x^{8}+x^{5}+x^{3}+x+1, \quad p_4(x) \\ &\quad =x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4}+1 \end{aligned}$$

$$\begin{aligned} x^{31}+x^{27}+x^{26}+x^{23}+x^{19}+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{10}+x^{8} \\ +x^{5}+x^{3}+x+1 \\ +(x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4}+1)(\,x^{18}+x^{17}+x^{15} \\ +x^{14}+x^{10}+x^{7}+x^{6}+x^{4}+1) \\ =x^{12}+x^{10}+x^{7}+x^{6}+x^{3}+1 \end{aligned}$$

$$\begin{aligned} x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4}+1 \\ +(x^{12}+x^{10}+x^{7}+x^{6}+x^{3}+1)(x+1) \\ =x^{10}+x^{6}+x^{5}+x^{3}+x \end{aligned}$$

$$\begin{aligned} x^{12}+x^{10}+x^{7}+x^{6}+x^{3}+1+(x^{10}+x^{6}+x^{5}+x^{3}+x)(x^{2}+1) \\ =x^{8}+x^{3}+x+1 \end{aligned}$$

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

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

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

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

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

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

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

$$\therefore \gcd(p_{9}(x),p_{4}(x))=\ 1$$

6. Compute the gcd of $p_{10}(x)$ and $p_{4}(x)$ as polynomials with coefficients in GF (2)

$$\begin{aligned} p_{10}(x)=x^{33}+x^{32}+x^{27} \\ +x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{16}+x^{15} \\ +x^{13}+x^{12}+x^{7}+x^{6}+x^{4}+x^{3}+1, p_{4}(x) \\ =x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4}+1 \end{aligned}$$

$$\begin{aligned} x^{33}+x^{32}+x^{27}+x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{16}+x^{15} \\ +x^{13}+x^{12}+x^{7}+x^{6}+x^{4}+x^{3}+1 \\ +(x^{13}+x^{12}+x^{11}+x^{8}+x^{5}+x^{4} \\ +1)(x^{20}+x^{18}+x^{17}+x^{14}+x^{12}+x^{11}+x^{9}+x^{8}+x^{7} \\ +x^{6}+x^{2})=x^{11}+x^{9}+x^{8}+x^{7}+x^{6}+x^{4}+x^{3}+x^{2}+1 \end{aligned}$$

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

$$\begin{aligned} x^{11}+x^{9}+x^{8}+x^{7}+x^{6}+x^{4}+x^{3}+x^{2}+1 \\ +(x^{8}+x^{7}+x^{6}+x^{4}+x^{3}+x^{2}+1)(x^{3}+x^{2}+x) \\ =x^{5}+x^{2}+x+1 \end{aligned}$$

$$\begin{aligned} x^{8}+x^{7}+x^{6}+x^{4}+x^{3}+x^{2}+1+(x^{5}+x^{2}+x+1)(x^{3}+x^{2}+x) \\ =x^{4}+x^{2}+1 \end{aligned}$$

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

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

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

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

$\therefore \text{gcd } (p_{10}(x), p_4(x)) = \ 1$

7. Compute the gcd of $p_{11}(x)$ and $p_4(x)$ as polynomials with coefficients in GF (2)

$$\begin{aligned} p_{11}(x) = x^{38} + x^{33} + x^{30} + x^{29} + x^{27} + x^{26} \\ + x^{24} + x^{24} + x^{23} + x^{22} + x^{21} + x^{18} + x^{17} + x^{15} + x^{12} \\ + x^{11} + x^8 + x^6 + x^4 + x + 1, \\ p_4(x) = x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + 1 \end{aligned}$$

$x^{38} + x^{33} + x^{30} + x^{29} + x^{27} + x^{26} + x^{24} + x^{24} + x^{23} + x^{22} + x^{21} + x^{18} + x^{17} + x^{15} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x + 1 + (x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + 1)(x^{25} + x^{24} + x^{22} + x^{21} + x^{17} + x^{16} + x^{14} + x^{11} + x^7 + x^6 + x^4 + x^3) = \ x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^3 + x+1$

$$\begin{aligned} x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + 1 \\ + (\ x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^3 + x + 1)(x) \\ = x^{10} + x^9 + x^8 + x^5 + x^2 + x + 1 \end{aligned}$$

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

$$\begin{aligned} x^{10} + x^9 + x^8 + x^5 + x^2 + x + 1 + (x^9 + x^8 + x^7 + x^4 + x^2 + 1)(x) \\ = x^3 + 1 \end{aligned}$$

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

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

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

$\therefore \text{gcd}(p_{11}(x), p_4(x)) = \ 1$

V. Conclusion

The paper presented results on the gcd of binary polynomials of Aunu permutation patterns of cardinality eleven using an extended Euclidean algorithm. It was established that most of the gcd of the permuted classes of words and sub-words were coprime. This has an application in the construction of cryptographic schemes that requires a public key and private key to be coprime. The results presented are for $p_1(x), p_2(x), p_3(x)$ and $p_4(x)$. The remaining classes of the polynomials will be presented in our future research.

Conflicts of Interest:

The authors declare that they have no conflicts of interest regarding the paper.

Reference

I. 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.*

II. Aminu Alhaji Ibrahim and Sa'idu Isah Abubakar (2016). Aunu Integer Sequence as Non-Associative Structure and Their Graph Theoretic Properties. Advances in Pure Mathematics, (6), 409-419 http://www.scirp.org/journal/apm
http://dx.doi.org/10.4236/apm.2016.66028

III. Aminu Alhaji Ibrahim, Saidu Isah Abubakar (2016). Non-Associative Property of 123-Avoiding Class of Aunu Permutation Patterns Advances in Pure Mathematics, 2016, 6, 51-57 http://www.scirp.org/journal/apm http://dx.doi.org/10.4236/apm.2016.62006.

IV. 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.

V. Abubakar S.I, Ibrahim Z. Ibrahim A.A (2014). Binary polynomials representation using the 123-avoiding class of the Aunu permutation patterns of cardinality seven. A paper presented at the 1st National Conference organized by Faculty of Science, Sokoto State University in conjunction with The Algebra Group Usmanu Danfodiyo University, Sokoto held at Sokoto State University from 17th-20th March, 2014.

VI. Benvenuto, C. J. (2012). Galois field in cryptography. *University of Washington*, *1*(1), 1-11.

VII. Daniel Panario (June 2006). A Minicourse in Finite Fields and Applications, School of Mathematics and Statistics, Carleton University.

VIII. De Piccoli, A., Visconti, A., & Rizzo, O. G. (2018). Polynomial multiplication over binary finite fields: new upper bounds. *Journal of Cryptographic Engineering*, 1-14.

IX. 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.*

XI. Paul Pollack (2008). Prime Polynomials over Finite Fields; A PhD Thesis, Darmouth College.

XII. Sheueling Chang Shantz (2001). From Eculid's GCD to Montgomery Multiplication to the Great Divide" sun Microsystems laboratories MSLI TR-2001-95.

XIII. Shparlinski, I. (2013). *Finite Fields: Theory and Computation: The meeting point of number theory, computer science, coding theory and cryptography* 477.

XIV. Stein J. (1961). Computational problems associated with Racah algebra. *Journal Computational Physics*, 1.