Journal of Advances in Mathematics and Computer Science

Volume 39, Issue 6, Page 27-42, 2024; Article no.JAMCS.116921

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

On the Generalization of the Number of Cyclic Codes Over the Prime Field GF(37)

Pancras Ongili [a*], Lao Hussein Mude [a] and Kinyanjui Jeremiah Ndung'u [a]

[a] *Department of Pure and Applied Sciences, Kirinyaga University, P. O. Box 143-10300, Kerugoya, Kenya.*

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JAMCS/2024/v39i61899

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/116921

Received: 02/03/2024
Accepted: 04/05/2024
Published: 07/05/2024

Original Research Article

Abstract

Research has explored the characterization of cyclic codes over $GF(P)$, where P is prime for $P \leq 23$. However, no study has characterized GF(37). Additionally, no study has generalized enumeration of the number of cyclic codes of the cyclotomic polynomials $u^n - 1$ over $GF(P)$. In particular, the generalization of the number of cyclic codes over $GF(37)$ for $u^n - 1$ is also lacking in research. This study focused on the monic irreducible polynomials of $u^n - 1$ over the finite field GF(37) with the main objective of generalizing the enumeration of the number of distinct cyclic codes. The methodology involved determining the number of

**Corresponding author: E-mail: opancras@gmail.com;*

irreducible monic polynomials of the cyclotomic polynomial $u^n - 1$ over $GF(37)$. These polynomials were found to correspond to the number of cyclotomic cosets of 37 mod n over $GF(37)$. The study concluded that the number of cyclic codes over $GF(37)$ can be generalized by $N_{GF(37)} = (37^y + 1)^{C_x m}$ $\forall x, y, m \in Z^+$. The findings provide insights into abstract algebraic concepts in coding theory that can be used to generalize number of cyclic codes over a prime field $GF(P)$

Keywords: Generalization over GF(37); GF(P); $u^n - 1$; irreducible factors; cyclotomic cosets; cyclotomic polynomials; cyclic codes.

2010 Mathematics Subject Classification: 53C25; 83C05; 57N16.

1 Introduction

The exploration of cyclic codes has captured the interest of many researchers, especially with the rise of cryptography [1][2][3][4][5]. Cyclic codes are particularly significant in coding theory, notably for error correction purposes [6][7][8][9][10][11]. The quest for optimal codes that can efficiently transmit diverse messages and correct numerous errors has been a driving force in this area of study [12][13]. Cyclic codes of length n over finite fields GF(P) for which $P \leq 23$ have been fully characterized [14][15], and a specific formula for computing the number of cyclic codes of some values of n for $u^n - 1$ over $GF(P)$ have been given [16][17][18][19][20]. Runji [19] specifically investigated the enumeration of cyclic codes over $GF(5)$, aiming to determine the count of cyclic codes of length n in $GF(5)$. This led to a generalized conclusion for cases where $n = 5m, n = 5^m$, and the gcd, $(m, 5) = 1$. Lao et al. [16] and Lao et al. [17] advanced the study on cyclic codes of length n over $\mathbb{Z}_{13}$ and $\mathbb{Z}_{17}$, uncovering that the number of cyclic codes of length n over these finite fields for the values $13k, 13^k, 17k$, and 17^k. Maganga & Kivunge [18] considered the number of irreducible polynomials $y^n - 1$ over $\mathbb{Z}_{19}$, concluding the generalization of the enumeration of the number of cyclic codes for values $n = 19, 19m$, and 19^m. A recent establishment by Simatwo et al. [20] investigated $GF(23)$, generalizing enumeration of cyclic codes for values $23m$, and 23^m. However, $\mathbb{Z}_{37}$ has not been characterized, and there is no general formula for computing the number of cyclic codes over this field. Additionally, the general formula for the generalization of the enumeration of cyclic codes over these fields for broader values of n is lacking. Factorization of polynomial $u^n - 1$ over finite fields has been a longstanding problem as there is no known general formula. In this study, the number of cyclic codes over GF(37) is determined, and a general formula is reached, providing a breakthrough in the subsequent generalization of the enumeration of the cyclic codes over prime fields GF(P).

1.1 Definitions

1. **A Code:** A block , C, of a code of length k is a set of n-tuples of vectors $(x_1, x_2, \ldots, x_n)$ where x_i are elements of a finite set with q symbols. The finite set, say F, is referred to as alphabets. For example, a simple alphabet consists of only two elements; 0 and 1. The codes formed from these alphabets are called binary codes, represented as $C = \{0, 1\}$.

2. **Cyclic Codes:** A linear code C is said to be cyclic over a finite field GF(q^k) if any cyclic shift of a codeword in C is also a codeword in C. For example; if a codeword, $(a_1 a_2 \ldots a_n) \in C$, then, $(a_n a_1 a_2 \ldots a_{n-1}) \in C$. Thus, a cyclic code is a linear code that is invariant under all cyclic shifts.

3. **Cyclotomic cosets** The cyclotomic coset is a set of integers that are relatively prime to a chosen integer, modulo another specific integer. It is defined by $C_i = \{i \cdot q^j \mod n \in \mathbb{Z} : j = 0, 1, 2, \ldots\}$, where q and n have a greatest common divisor of 1, i.e., $\gcd(q, n) = 1$.

4. **Cyclotomic Polynomial** A polynomial of the form $u^n - 1$ whose roots are all n^{th} primitive roots of unity.

2 Results and Discussion

Cyclotomic cosets play a crucial role in constructing q-array cyclic codes with a length of n. These cosets are defined by establishing a binary relation on integers ranging from 0 to $n-1$. The formula for cyclotomic cosets of a number q modulo n is given by $C_j = \{j \cdot q^k \mod n \in \mathbb{Z}_n : k = 0, 1, 2, \ldots\}$ where j is a nonnegative integer, and q and n are relatively prime. In the context of $GF(37)$, $q = 37$. The cyclotomic cosets of 37 modulo n are crucial in the factorization of $(u^n - 1)$ into irreducible polynomials over $GF(37)$. The cyclotomic cosets correspond to factors of an irreducible polynomial, and the factorization is expressed as a product of these irreducible polynomials. The specific form of the factorization over $\mathbb{Z}_{37}$ depends on the values of n.

2.1 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = 2^m \cdot 37^m$

Let $m \in \mathbb{Z}$, then;
$(u^n - 1) = (u^{2^m \cdot 37^m} - 1)$
$(u^n - 1) = (u^{2^m \cdot 37^m} - 1)$

1. When $m = 1$, then $n = 2^1 \cdot 37^1$
   $(u^n - 1) = (u^{2^{\cdot} 37} - 1) = (u^2 - 1)^{37} = ((u + 36)(u + 1))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^2$
2. When $m = 2$, then $n = 2^2 \cdot 37^2$
   $(u^n - 1) = (u^{2^2 \cdot 37^2} - 1) = (u^4 - 1)^{37^2}$
   $= ((u^2 + 1)(u + 1)(u - 1))^{37^2}$
   $= ((u + 36)(u + 1)(u + 6)(u + 31))^{37^2}$
   Hence, Number of cyclic codes; $(37^2 + 1)^4$
3. When $m = 3$, then $n = 2^3 \cdot 37^3$
   $(u^n - 1) = (u^{2^3 \cdot 37^3} - 1) = (u^8 - 1)^{37^3}$
   $= ((u^4 + 1)(u^2 + 1)(u + 1)(u - 1))^{37^3}$
   $= ((u^2 + 6)(u^2 + 31)(u + 6)(u + 31)(u + 1)(u + 36))^{37^3}$
   Hence, Number of cyclic codes; $(37^3 + 1)^6$
4. When $m = 4$, then $n = 2^4 \cdot 37^4$
   $(u^n - 1) = (u^{2^4 \cdot 37^4} - 1) = (u^{16} - 1)^{37^4}$
   $= ((u^8 - 1)(u^8 + 1))^{37^4}$
   $= ((u^2 + 6)(u^2 + 31)(u + 6)(u + 31)(u + 1)(u + 36)(u^4 + 6)(u^4 + 31)^{37^4}$
   Hence, Number of cyclic codes; $(37^4 + 1)^8$
5. When $m = 5$, then $n = 2^5 \cdot 37^5$
   $(u^n - 1) = (u^{2^5 \cdot 37^5} - 1) = (u^{32} - 1)^{37^5}$
   $= ((u + 36)(u + 1)(u^2 + 6)(u^2 + 31)(u + 6)(u + 31)(u^8 + 31)(u^8 + 6)(u^4 + 31)(u^4 + 6))^{37^5}$
   Hence, Number of cyclic codes; $(37^5 + 1)^{10}$
6. When $m = 6$, then $n = 2^6 \cdot 37^6$
   $(u^n - 1) = (u^{2^6 \cdot 37^6} - 1) = (u^{64} - 1)^{37^6}$
   $= ((u^{16} + 1)(u^{16} + 36)(u + 36)(u + 1)(u^2 + 6)(u^2 + 31)(u + 6)(u + 31)(u^8 + 31)(u^8 + 6)(u^4 + 31)(u^4 + 6))^{37^6}$
   Hence, Number of cyclic codes; $(37^6 + 1)^{12}$

The summary of the Number of Cyclic Code for $n = 2^m \cdot 37^m$ over $GF(37)$ is as shown in the Table 1;

Table 1. Summary of the Number of Cyclic Code for $n = 2^m \cdot 37^m$ over $GF(37)$

Value of m	**Number of factors of $u^n - 1$ for $n = 2^m \cdot 37^m$**	**Number of cyclic codes (N)**
1	2	$(37+1)^2$
2	4	$(37^2+1)^4$
3	6	$(37^3+1)^6$
4	8	$(37^4+1)^8$
5	10	$(37^5+1)^{10}$
6	12	$(37^6+1)^{12}$
7	14	$(37^7+1)^{14}$
8	16	$(37^8+1)^{16}$
9	18	$(37^9+1)^{18}$
10	20	$(37^{10}+1)^{20}$
11	22	$(37^{11}+1)^{22}$
12	24	$(37^{12}+1)^{24}$
13	26	$(37^{13}+1)^{26}$
14	28	$(37^{14}+1)^{28}$
15	30	$(37^{15}+1)^{30}$
16	32	$(37^{16}+1)^{32}$
17	34	$(37^{17}+1)^{34}$
18	36	$(37^{18}+1)^{36}$
19	38	$(37^{19}+1)^{38}$
20	40	$(37^{20}+1)^{40}$
21	42	$(37^{21}+1)^{42}$
22	44	$(37^{22}+1)^{44}$
23	46	$(37^{23}+1)^{46}$
24	48	$(37^{24}+1)^{48}$
25	50	$(37^{25}+1)^{50}$
26	52	$(37^{26}+1)^{52}$
27	54	$(37^{27}+1)^{54}$
28	56	$(37^{28}+1)^{56}$
29	58	$(37^{29}+1)^{58}$
30	60	$(37^{30}+1)^{60}$
31	62	$(37^{31}+1)^{62}$
32	64	$(37^{32}+1)^{64}$
33	66	$(37^{33}+1)^{66}$
34	68	$(37^{34}+1)^{68}$
35	70	$(37^{35}+1)^{70}$
36	72	$(37^{36}+1)^{72}$
37	74	$(37^{37}+1)^{74}$

In general, it can be inferred from the above summary that when $n = 2^m \cdot 37^m$ such that $m \in \mathbb{Z}^+$, $u^n - 1$ factors into $2m$ irreducible monic polynomials over $GF(37)$ such that the number of cyclic codes, N is given by; $N = (37^m + 1)^{2m}$

Conjecture 1. *Suppose $n = 2^m \cdot 37^m$ and $2m$ is the number of cyclotomic cosets of 37 mod 2^m, then the number of cyclic codes over $GF(37)$ of $u^n - 1$, N is given by;* $N = (37^m + 1)^{2m}$

2.2 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = 3^m \cdot 37^m$

Let $m \in \mathbb{Z}^+$, then;
$(u^n - 1) = (u^{3^m \cdot 37^m} - 1)$

1. When $m = 1$, then $n = 3^1 \cdot 37^1$
   $(u^n - 1) = (u^{3 \cdot 37} - 1) = (u^3 - 1)^{37}$
   $= ((u + 36)(u + 10)(u + 26))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^3$
2. When $m = 2$, then $n = 3^2 \cdot 37^2$
   $(u^n - 1) = (u^{3^2 \cdot 37^2} - 1) = (u^9 - 1)^{37^2}$
   $= ((u + 36)(u + 10)(u + 26)(u + 3)(u + 4)(u + 11)(u + 21)(u + 25)(u + 28))^{37^2}$
   Hence, Number of cyclic codes; $(37^2 + 1)^9$
3. When $m = 3$, then $n = 3^3 \cdot 37^3$
   $(u^n - 1) = (u^{3^3 \cdot 37^3} - 1) = (u^{27} - 1)^{37^3}$
   $= ((u+1)(u+30)(u+28)(u+27)(u+25)(u+21)(u+11)(u+4)(u+3)(u^3+30)(u^3+28)(u^3+25)(u^3+21)(u^3+4)(u^3+3))^{37^3}$
   Hence, Number of cyclic codes; $(37^3 + 1)^{15}$
4. When $m = 4$, then $n = 3^4 \cdot 37^4$
   $(u^n - 1) = (u^{3^4 \cdot 37^4} - 1) = (u^{81} - 1)^{37^4}$
   Hence, Number of cyclic codes; $(37^4 + 1)^{21}$
5. When $m = 5$, then $n = 3^5 \cdot 37^5$
   $(u^n - 1) = (u^{3^5 \cdot 37^5} - 1) = (u^{243} - 1)^{37^5}$
   Hence, Number of cyclic codes; $(37^5 + 1)^{27}$

The summary of the Number of Cyclic Code for $n = 3^m \cdot 37^m$ over $GF(37)$ for $1 \leq m < 16$ is as shown in the Table 2;

Table 2. Summary of the Number of Cyclic Code for $n = 3^m \cdot 37^m$ over $GF(37)$ for $1 \leq m < 16$

Value of m	**$u^n - 1$ for $n = 3^m \cdot 37^m$**	**Number of cyclic codes (N)**
1	$(u-1)^{3^1 \cdot 37^1}$	$(37+1)^3$
2	$(u-1)^{3^2 \cdot 37^2}$	$(37^2+1)^9$
3	$(u-1)^{3^3 \cdot 37^3}$	$(37^3+1)^{15}$
4	$(u-1)^{3^4 \cdot 37^4}$	$(37^4+1)^{21}$
5	$(u-1)^{3^5 \cdot 37^5}$	$(37^5+1)^{27}$
6	$(u-1)^{3^6 \cdot 37^6}$	$(37^6+1)^{33}$
7	$(u-1)^{3^7 \cdot 37^7}$	$(37^7+1)^{39}$
8	$(u-1)^{3^8 \cdot 37^8}$	$(37^8+1)^{45}$
9	$(u-1)^{3^9 \cdot 37^9}$	$(37^9+1)^{51}$
10	$(u-1)^{3^{10} \cdot 37^{10}}$	$(37^{10}+1)^{57}$
11	$(u-1)^{3^{11} \cdot 37^{11}}$	$(37^{11}+1)^{63}$
12	$(u-1)^{3^{12} \cdot 37^{12}}$	$(37^{12}+1)^{69}$
13	$(u-1)^{3^{13} \cdot 37^{13}}$	$(37^{13}+1)^{75}$
14	$(u-1)^{3^{14} \cdot 37^{14}}$	$(37^{14}+1)^{81}$
15	$(u-1)^{3^{15} \cdot 37^{15}}$	$(37^{15}+1)^{87}$

In general, it can be inferred from the above summary that when $n = 3^m \cdot 37^m$ such that $m \in \mathbb{Z}^+$, $u^n - 1$ factors into irreducible monic polynomials over $GF(37)$ such that the number of cyclic codes, N is given by; $N = (37^m + 1)^{(6m-3)}$.

Conjecture 2. *Suppose $n = 3^m \cdot 37^m$ and $(6m-3)$ is the number of cyclotomic cosets of 37 mod 3^m, then the number of cyclic codes over $GF(37)$ of $u^n - 1$, N is given by;* $N = (37^m + 1)^{(6m-3)}$

2.3 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = 4^m \cdot 37^m$

Let $m \in \mathbb{Z}^+$, then;
$(u^n - 1) = (u^{4^m \cdot 37^m} - 1)$
$(u^n - 1) = (u^{4^m \cdot 37^m} - 1)$

1. When $m = 1$, then $n = 4^1 \cdot 37^1$
   $(u^n - 1) = (u^{4 \cdot 37} - 1) = (u^4 - 1)^{37}$
   $= ((u + 36)(u + 1)(u + 6)(u + 31))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^4$
2. When $m = 2$, then $n = 4^2 \cdot 37^2$
   $(u^n - 1) = (u^{4^2 \cdot 37^2} - 1) = (u^{16} - 1)^{37^2}$
   $= ((u^2 + 6)(u^2 + 31)(u + 6)(u + 31)(u + 1)(u + 36)(u^4 + 6)(u^4 + 31))^{37^2}$
   Hence, Number of cyclic codes; $(37^2 + 1)^8$
3. When $m = 3$, then $n = 4^3 \cdot 37^3$
   $(u^n - 1) = (u^{3^3 \cdot 37^3} - 1) = (u^{64} - 1)^{37^3}$
   Hence, Number of cyclic codes; $(37^3 + 1)^{12}$
4. When $m = 4$, then $n = 4^4 \cdot 37^4$
   $(u^n - 1) = (u^{4^4 \cdot 37^4} - 1) = (u^{256} - 1)^{37^4}$
   Hence, Number of cyclic codes; $(37^4 + 1)^{16}$
5. When $m = 5$, then $n = 4^5 \cdot 37^5$
   $(u^n - 1) = (u^{3^5 \cdot 37^5} - 1) = (u^{1024} - 1)^{37^5}$
   Hence, Number of cyclic codes; $(37^5 + 1)^{20}$

The summary of the Number of Cyclic Code for $n = 4^m \cdot 37^m$ over $GF(37)$ for $1 \leq m < 16$ is as shown in the Table 3;

Table 3. Summary of the Number of Cyclic Code for $n = 4^m \cdot 37^m$ over $GF(37)$ for $1 \leq m < 16$

Value of m	$u^n - 1$ for $n = 4^m \cdot 37^m$	Number of cyclic codes (N)
1	$(u-1)^{4^1 \cdot 37^1}$	$(37+1)^4$
2	$(u-1)^{4^2 \cdot 37^2}$	$(37^2+1)^8$
3	$(u-1)^{4^3 \cdot 37^3}$	$(37^3+1)^{12}$
4	$(u-1)^{4^4 \cdot 37^4}$	$(37^4+1)^{16}$
5	$(u-1)^{4^5 \cdot 37^5}$	$(37^5+1)^{20}$
6	$(u-1)^{4^6 \cdot 37^6}$	$(37^6+1)^{24}$
7	$(u-1)^{4^7 \cdot 37^7}$	$(37^7+1)^{28}$
8	$(u-1)^{4^8 \cdot 37^8}$	$(37^8+1)^{32}$
9	$(u-1)^{4^9 \cdot 37^9}$	$(37^9+1)^{36}$

Value of m	$u^n - 1$ **for** $n = 4^m \cdot 37^m$	**Number of cyclic codes** (N)
10	$(u-1)^{4^{10} \cdot 37^{10}}$	$(37^{10}+1)^{40}$
11	$(u-1)^{4^{11} \cdot 37^{11}}$	$(37^{11}+1)^{44}$
12	$(u-1)^{4^{12} \cdot 37^{12}}$	$(37^{12}+1)^{48}$
13	$(u-1)^{4^{13} \cdot 37^{13}}$	$(37^{13}+1)^{52}$
14	$(u-1)^{4^{14} \cdot 37^{14}}$	$(37^{14}+1)^{56}$
15	$(u-1)^{4^{15} \cdot 37^{15}}$	$(37^{15}+1)^{60}$

In general, it can be inferred from the above summary that when $n = 4^m \cdot 37^m$ such that $m \in \mathbb{Z}^+$, $u^n - 1$ factors into irreducible monic polynomials over $GF(37)$ such that the number of cyclic codes, N is given by; $N = (37^m + 1)^{4m}$.

Conjecture 3. *Suppose* $n = 4^m \cdot 37^m$ *and* $4m$ *is the number of cyclotomic cosets of* 37 *mod* 4^m*, then the number of cyclic codes over* $GF(37)$ *of* $u^n - 1$*,* N *is given by;* $N = (37^m + 1)^{4m}$

2.4 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = 5^m \cdot 37^m$

Let $m \in \mathbb{Z}^+$, then;
$(u^n - 1) = (u^{5^m \cdot 37^m} - 1)$

1. When $m = 1$, then $n = 5^1 \cdot 37^1$
   $(u^n - 1) = (u^{5 \cdot 37} - 1) = (u^5 - 1)^{37}$
   $= ((u-1)(u^4 + u^3 + u^2 + u + 1) = (u+36)(u^4 + u^3 + u^2 + u + 1))^{37}$
   Hence, Number of cyclic codes; $(37+1)^2$

2. When $m = 2$, then $n = 5^2 \cdot 37^2$
   $(u^n - 1) = (u^{3^2 \cdot 37^2} - 1) = (u^{25} - 1)^{37^2}$
   $= ((u+36)(u^4 + u^3 + u^2 + u + 1)(u^{20} + u^{15} + u^{10} + u^5 + 1))^{37^2}$
   Hence, Number of cyclic codes; $(37^2+1)^3$

3. When $m = 3$, then $n = 5^3 \cdot 37^3$
   $(u^n - 1) = (u^{3^3 \cdot 37^3} - 1) = (u^{125} - 1)^{37^3}$
   Hence, Number of cyclic codes; $(37^3+1)^4$

4. When $m = 4$, then $n = 5^4 \cdot 37^4$
   $(u^n - 1) = (u^{3^4 \cdot 37^4} - 1) = (u^{625} - 1)^{37^4}$
   Hence, Number of cyclic codes; $(37^4+1)^5$

5. When $m = 5$, then $n = 5^5 \cdot 37^5$
   $(u^n - 1) = (u^{5^5 \cdot 37^5} - 1) = (u^{3125} - 1)^{37^5}$
   Hence, Number of cyclic codes; $(37^5+1)^6$

In general, it can be inferred from the above that when $n = 5^m \cdot 37^m$ such that $m \in \mathbb{Z}^+$, $u^n - 1$ factors into irreducible monic polynomials over $GF(37)$ such that the number of cyclic codes, N is given by; $N = (37^m + 1)^{(m+1)}$.

Conjecture 4. *Suppose* $n = 5^m \cdot 37^m$ *and* $(m+1)$ *is the number of cyclotomic cosets of* 37 *mod* 5^m*, then the number of cyclic codes over* $GF(37)$ *of* $u^n - 1$*,* N *is given by;* $N = (37^m + 1)^{(m+1)}$

2.5 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = 37^m$

Let $m \in \mathbb{Z}$, then;
$(u^n - 1) = (u^{37^m} - 1)$
$(u^n - 1) = (u^{37^m} - 1) = (u - 1)^{37^m}$

1. When $m = 1$, then $n = 37^1$
   $(u^n - 1)$=$(u^{37} - 1) = (u - 1)^{37}$
   Hence, Number of cyclic codes; $(37 + 1)$
2. When $m = 2$, then $n = 37^2$
   $(u^n - 1) = (u^{37^2} - 1) = (u - 1)^{37^2}$
   Hence, Number of cyclic codes; $(37^2 + 1)$
3. When $m = 3$, then $n = 37^3$
   $(u^n - 1) = (u^{37^3} - 1) = (u - 1)^{37^3}$
   Hence, Number of cyclic codes; $(37^3 + 1)$
4. When $m = 4$, then $n = 37^4$
   $(u^n - 1) = (u^{37^4} - 1) = (u - 1)^{37^4}$
   Hence, Number of cyclic codes; $(37^4 + 1)$
5. When $m = 5$, then $n = 37^5$
   $(u^n - 1) = (u^{37^5} - 1) = (u - 1)^{37^5}$
   Hence, Number of cyclic codes; $(37^5 + 1)$
6. When $m = 6$, then $n = 37^6$
   $(u^n - 1) = (u^{37^6} - 1) = (u - 1)^{37^6}$
   Hence, Number of cyclic codes; $(37^6 + 1)$

The summary of the Number of Cyclic Code for $n = 37^m$ over $GF(37)$ for $1 \leq m < 15$ is as shown in the Table 4;

Table 4. Summary of the Number of Cyclic Code for $n = 37^m$ over $GF(37)$ for $1 \leq m < 15$

Value of m	$u^n - 1$ **for** $n = 37^m$	**Number of cyclic codes (N)**
1	$(u-1)^{37^1}$	$(37+1)$
2	$(u-1)^{37^2}$	(37^2+1)
3	$(u-1)^{37^3}$	(37^3+1)
4	$(u-1)^{37^4}$	(37^4+1)
5	$(u-1)^{37^5}$	(37^5+1)
6	$(u-1)^{37^6}$	(37^6+1)
7	$(u-1)^{37^7}$	(37^7+1)
8	$(u-1)^{37^8}$	(37^8+1)
9	$(u-1)^{37^9}$	(37^9+1)
10	$(u-1)^{37^{10}}$	$(37^{10}+1)$
11	$(u-1)^{37^{11}}$	$(37^{11}+1)$
12	$(u-1)^{37^{12}}$	$(37^{12}+1)$
13	$(u-1)^{37^{13}}$	$(37^{13}+1)$
14	$(u-1)^{37^{14}}$	$(37^{14}+1)$

In general, it can be inferred from the above summary that when $n = 37^m$ such that $m \in \mathbb{Z}^+$, $u^n - 1$ factors into irreducible monic polynomials over $GF(37)$ such that the number of cyclic codes, N is given by; $N = (37^m + 1)$

Conjecture 5. *Suppose that the number of cyclic codes over GF(37) of $u^n - 1$ is given by $N = 37^m + 1$. Then, the number of cyclotomic cosets of 37 mod $a^m = 1$ $\forall n = a^m \cdot 37^m$, where $a \in \mathbb{Z}^+$.*

2.6 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = m \cdot 37$

Let $m \in \mathbb{Z}$, then;
$(u^n - 1) = (u^{m \cdot 37} - 1)$

1. When $m = 1$, then $n = 1 \cdot 37$
   $(u^n - 1) = (u^{1 \cdot 37} - 1) = (u - 1)^{37}$
   Hence, Number of cyclic codes; $(37 + 1)$
2. When $m = 2$, then $n = 2 \cdot 37$
   $(u^n - 1) = (u^{2 \cdot 37} - 1) = (u^2 - 1)^{37}$
   $= ((u + 36)(u + 1))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^2$
3. When $m = 3$, then $n = 3 \cdot 37$
   $(u^n - 1) = (u^{3 \cdot 37} - 1) = (u^3 - 1)^{37}$
   $= ((u + 36)(u + 10)(u + 26))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^3$
4. When $m = 4$, then $n = 4 \cdot 37$
   $(u^n - 1) = (u^{4 \cdot 37} - 1) = (u^4 - 1)^{37}$
   $= ((u + 36)(u + 1)(u + 6)(u + 31))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^4$
5. When $m = 5$, then $n = 5 \cdot 37$
   $(u^n - 1) = (u^{5 \cdot 37} - 1) = (u^5 - 1)^{37}$
   $= ((u + 36)(u^4 + u^3 + u^2 + u + 1))$
   Hence, Number of cyclic codes; $(37 + 1)^2$
6. When $m = 6$, then $n = 6 \cdot 37$
   $(u^n - 1) = (u^{6 \cdot 37} - 1) = (u^6 - 1)^{37}$
   $= ((u + 1)(u + 36)(u + 10)(u + 26)(u + 27)(u + 11))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^6$
7. When $m = 7$, then $n = 7 \cdot 37$
   $(u^n - 1) = (u^{7 \cdot 37} - 1) = (u^7 - 1)^{37}$
   $= ((u + 36)(u^3 + 9u^2 + 8u + 36)(u^3 + 29u^2 + 28u + 36))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^3$
8. When $m = 8$, then $n = 8 \cdot 37^8$
   $(u^n - 1) = (u^{8 \cdot 37} - 1) = (u^8 - 1)^{37}$
   $= ((u^2 + 6)(u^2 + 31)(u + 6)(u + 31)(u + 1)(u + 36))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^6$
9. When $m = 9$, then $n = 9 \cdot 37$
   $(u^n - 1) = (u^{9 \cdot 37} - 1) = (u^9 - 1)^{37}$
   $= ((u + 36)(u + 10)(u + 26)(u + 3)(u + 4)(u + 11)(u + 21)(u + 25)(u + 28))^{37}$ Hence, Number of cyclic codes; $(37 + 1)^9$
10. When $m = 10$, then $n = 10 \cdot 37$
    $(u^n - 1) = (u^{10 \cdot 37} - 1) = (u^{10} - 1)^{37}$
    $= (u + 1)(u + 36)(u^4 + 36u^3 + u^2 + 36u + 1)(u^4 + u^3 + u^2 + u + 1))^{37}$
    Hence, Number of cyclic codes; $(37 + 1)^4$

2.7 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = 2m \cdot 37^m$

Let $m \in \mathbb{Z}^+$, then;
$(u^n - 1) = (u^{2m \cdot 37^m} - 1)$
$(u^n - 1) = (u^{2m \cdot 37^m} - 1) = (u^{2m} - 1)^{37^m}$

1. When $m = 1$, then $n = 2 \cdot 1 \cdot 37^1$
   $(u^n - 1) = (u^{2 \cdot 37} - 1) = (u^2 - 1)^{37} = ((u + 36)(u + 1))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^2$
2. When $m = 2$, then $n = 2 \cdot 2 \cdot 37^2$
   $(u^n - 1) = (u^{2 \cdot 2 \cdot 37^2} - 1) = (u^4 - 1)^{37^2}$
   $= ((u^2 + 1)(u + 1)(u - 1))^{37^2}$
   $= ((u + 36)(u + 1)(u + 6)(u + 31))^{37^2}$
   Hence, Number of cyclic codes; $(37^2 + 1)^4$
3. When $m = 3$, then $n = 2 \cdot 3 \cdot 37^3$
   $(u^n - 1) = (u^{2 \cdot 3 \cdot 37^3} - 1) = (u^6 - 1)^{37^3}$
   $= ((u + 1)(u + 36)(u + 10)(u + 26)(u + 27)(u + 11))^{37^3}$
   Hence, Number of cyclic codes; $(37^3 + 1)^6$
4. When $m = 4$, then $n = 2 \cdot 4 \cdot 37^4$
   $(u^n - 1) = (u^{2 \cdot 4 \cdot 37^4} - 1) = (u^8 - 1)^{37^4}$
   $= ((u^2 + 6)(u^2 + 31)(u + 6)(u + 31)(u + 1)(u + 36))^{37^4}$
   Hence, Number of cyclic codes; $(37^4 + 1)^6$
5. When $m = 5$, then $n = 2 \cdot 5 \cdot 37^5$
   $(u^n - 1) = (u^{2 \cdot 5 \cdot 37^5} - 1) = (u^{10} - 1)^{37^5}$
   $= ((u + 1)(u + 36)(u^4 + 36u^3 + u^2 + 36u + 1)(u^4 + u^3 + u^2 + u + 1))^{37^5}$
   Hence, Number of cyclic codes; $(37^5 + 1)^4$
6. When $m = 6$, then $n = 2 \cdot 6 \cdot 37^6$
   $(u^n - 1) = (u^{2 \cdot 6 \cdot 37^6} - 1) = (u^{12} - 1)^{37^6}$
   $= ((u + 6)(u + 31)(u + 1)(u + 36)(u + 11)(u + 27)(u + 10)(u + 26)(u + 14)(u + 8)(u + 29)(u + 23))^{37^6}$
   Hence, Number of cyclic codes; $(37^6 + 1)^{12}$
7. When $m = 7$, then $n = 2 \cdot 7 \cdot 37^7$
   $(u^n - 1) = (u^{2 \cdot 7 \cdot 37^7} - 1) = (u^{14} - 1)^{37^7}$
   $= (((u + 36)(u + 1)(u^3 + 9u^2 + 8u + 36)(u^3 + 29u^2 + 28u + 36)(u^3 + 36u^2 + u + 36)(u^3 + 36))^{37^7}$
   Hence, Number of cyclic codes; $(37^7 + 1)^6$
8. When $m = 8$, then $n = 2 \cdot 8 \cdot 37^8$
   $(u^n - 1) = (u^{2 \cdot 8 \cdot 37^8} - 1) = (u^{16} - 1)^{37^8}$
   $= ((u^2 + 6)(u^2 + 31)(u + 6)(u + 31)(u + 1)(u + 36)(u^4 + 6)(u^4 + 31))^{37^8}$
   Hence, Number of cyclic codes; $(37^8 + 1)^8$
9. When $m = 9$, then $n = 2 \cdot 9 \cdot 37^9$
   $(u^n - 1) = (u^{2 \cdot 9 \cdot 37^9} - 1) = (u^{18} - 1)^{37^9}$
   $= ((u + 36)(u + 1)(u + 10)(u + 26)(u + 27)(u + 11)(u + 34)(u + 33)(u + 30)(u + 28)(u + 25)(u + 21)(u + 16)(u + 12)(u + 9)(u + 7)(u + 4)(u + 3))^{37^9}$
   Hence, Number of cyclic codes; $(37^9 + 1)^{18}$
10. When $m = 10$, then $n = 2 \cdot 10 \cdot 37^{10}$
   $(u^n - 1) = (u^{2 \cdot 10 \cdot 37^{10}} - 1) = (u^{20} - 1)^{37^{10}}$
   $= ((u + 1)(u + 36)(u + 6)(u + 31)(u^4 + 36u^3 + u^2 + 36u + 1)(u^4 + u^3 + u^2 + u + 1)(u^4 + 6)(u^4 + 31))^{37^{10}}$
   Hence, Number of cyclic codes; $(37^{10} + 1)^8$

2.8 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = 3m \cdot 37^m$

Let $m \in \mathbb{Z}^+$, then;
$(u^n - 1) = (u^{3m \cdot 37^m} - 1)$

1. When $m = 1$, then $n = 3 \cdot 1 \cdot 37^1$
   $(u^n - 1) = (u^{3 \cdot 37} - 1) = (u^3 - 1)^{37}$
   $= ((u + 36)(u + 10)(u + 26))^{37}$
   Hence, Number of cyclic codes; $(37 + 1)^3$
2. When $m = 2$, then $n = 3 \cdot 2 \cdot 37^2$
   $(u^n - 1) = (u^{3 \cdot 2 \cdot 37^2} - 1) = (u^6 - 1)^{37^2}$
   $= ((u + 1)(u + 36)(u + 10)(u + 26)(u + 27)(u + 11))^{37^2}$
   Hence, Number of cyclic codes; $(37^2 + 1)^6$
3. When $m = 3$, then $n = 3 \cdot 3 \cdot 37^3$
   $(u^n - 1) = (u^{3 \cdot 3 \cdot 37^3} - 1) = (u^9 - 1)^{37^3}$
   $= ((u + 36)(u + 10)(u + 26)(u + 3)(u + 4)(u + 11)(u + 21)(u + 25)(u + 28))^{37^3}$
   Hence, Number of cyclic codes; $(37^3 + 1)^9$
4. When $m = 4$, then $n = 3 \cdot 4 \cdot 37^4$
   $(u^n - 1) = (u^{3 \cdot 4 \cdot 37^4} - 1) = (u^{12} - 1)^{37^4}$
   $= ((u + 6)(u + 31)(u + 1)(u + 36)(u + 11)(u + 27)(u + 10)(u + 26)(u + 14)(u + 8)(u + 29)(u + 23))^{37^4}$
   Hence, Number of cyclic codes; $(37^4 + 1)^{12}$
5. When $m = 5$, then $n = 3 \cdot 5 \cdot 37^5$
   $(u^n - 1) = (u^{3 \cdot 5 \cdot 37^5} - 1) = (u^{15} - 1)^{37^5}$
   $= ((u + 36)(u^4 + u^3 + u^2 + u + 1)(u + 11)(u^4 + 10u^3 + 26u^2 + u + 10)(u + 27)(u^4 + 26u^3 + 10u^2 + 26))^{37^5}$
   Hence, Number of cyclic codes; $(37^5 + 1)^6$
6. When $m = 6$, then $n = 3 \cdot 6 \cdot 37^6$
   $(u^n - 1) = (u^{3 \cdot 6 \cdot 37^6} - 1) = (u^{18} - 1)^{37^6}$
   $= ((u + 36)(u + 1)(u + 10)(u + 26)(u + 27)(u + 11)(u + 34)(u + 33)(u + 30)(u + 28)(u + 25)(u + 21)(u + 16)(u + 12)(u + 9)(u + 7)(u + 4)(u + 3))^{37^6}$
   Hence, Number of cyclic codes; $(37^6 + 1)^{18}$
7. When $m = 7$, then $n = 3 \cdot 7 \cdot 37^7$
   $(u^n - 1) = (u^{3 \cdot 7 \cdot 37^7} - 1) = (u^{21} - 1)^{37^7}$
   $= ((u + 36)(u + 11)(u + 27)(u^3 + 12u^2 + 6u + 36)(u^3 + 9u^2 + 8u + 36)(u^3 + 14u^2 + 21u + 36)(u^3 + 16u^2 + 23u + 36)(u^3 + 29u^2 + 28u + 36)(u^3 + 31u^2 + 25u + 36))^{37^7}$ Hence, Number of cyclic codes; $(37^7 + 1)^9$
8. When $m = 8$, then $n = 3 \cdot 8 \cdot 37^8$
   $(u^n - 1) = (u^{3 \cdot 8 \cdot 37^8} - 1) = (u^{24} - 1)^{37^8}$
   $= ((u + 36)(u + 31)(u + 29)(u + 27)(u + 26)(u + 23)(u + 14)(u + 11)(u + 10)(u + 8)(u + 6)(u + 1)(u^2 + 31)(u^2 + 29)(u^2 + 23)(u^2 + 14)(u^2 + 8)(u^2 + 6))^{37^8}$
   Hence, Number of cyclic codes; $(37^8 + 1)^{18}$
9. When $m = 9$, then $n = 3 \cdot 9 \cdot 37^9$
   $(u^n - 1) = (u^{3 \cdot 9 \cdot 37^9} - 1) = (u^{27} - 1)^{37^9}$
   $= ((u + 1)(u + 30)(u + 28)(u + 27)(u + 25)(u + 21)(u + 11)(u + 4)(u + 3)(u^3 + 30)(u^3 + 28)(u^3 + 25)(u^3 + 21)(u^3 + 4)(u^3 + 3))^{37^9}$
   Hence, Number of cyclic codes; $(37^9 + 1)^{15}$
10. When $m = 10$, then $n = 3 \cdot 10 \cdot 37^{10}$
    $(u^n - 1) = (u^{3 \cdot 10 \cdot 37^{10}} - 1) = (u^{30} - 1)^{37^{10}}$

$= ((u+36)(u+1)(u+27)(u+26)(u+11)(u+10)(u^4+36u^3+u^2+36u+1)(u^4+27u^3+26u^2+36u+10)(u^4+26u^3+10u^2+u+26)(u^4+11u^3+10u^2+36u+26)(u^4+10u^3+26u^2+u+10)(u^4+u^3+u^2+u+1))^{37^{10}}$
Hence, Number of cyclic codes; $(37^{10}+1)^{12}$

2.9 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = 5m \cdot 37^m$

Let $m \in \mathbb{Z}^+$, then;
$(u^n - 1) = (u^{5m \cdot 37^m} - 1)$

1. When $m = 1$, then $n = 5 \cdot 1 \cdot 37^1$
   $(u^n - 1) = (u^{5 \cdot 37} - 1) = (u^5 - 1)^{37}$
   $= ((u+36)(u^4+u^3+u^2+u+1))^{37}$
   Hence, Number of cyclic codes; $(37+1)^2$
2. When $m = 2$, then $n = 5 \cdot 2 \cdot 37^2$
   $(u^n - 1) = (u^{5 \cdot 2 \cdot 37^2} - 1) = (u^{10} - 1)^{37^2}$
   $= ((u+1)(u+36)(u^4+36u^3+u^2+36u+1)(u^4+u^3+u^2+u+1))^{37^2}$
   Hence, Number of cyclic codes; $(37^2+1)^4$
3. When $m = 3$, then $n = 5 \cdot 3 \cdot 37^3$
   $(u^n - 1) = (u^{5 \cdot 3 \cdot 37^3} - 1) = (u^{15} - 1)^{37^3}$
   $= ((u+36)(u^4+u^3+u^2+u+1)(u^{10}+u^5+1) = (u+36)(u^4+u^3+u^2+u+1)(u+11)(u^4+10u^3+26u^2+u+10)(u+27)(u^4+26u^3+10u^2+26))^{37^3}$
   Hence, Number of cyclic codes; $(37^3+1)^6$
4. When $m = 4$, then $n = 5 \cdot 4 \cdot 37^4$
   $(u^n - 1) = (u^{5 \cdot 4 \cdot 37^4} - 1) = (u^{20} - 1)^{37^4}$
   $= ((u+1)(u+36)(u+6)(u+31)(u^4+36u^3+u^2+36u+1)(u^4+u^3+u^2+u+1)(u^4+6)(u^4+31))^{37^4}$
   Hence, Number of cyclic codes; $(37^4+1)^8$
5. When $m = 5$, then $n = 5 \cdot 5 \cdot 37^5$
   $(u^n - 1) = (u^{5 \cdot 5 \cdot 37^5} - 1) = (u^{25} - 1)^{37^5}$
   $= ((u+36)(u^4+u^3+u^2+u+1)(u^{20}+u^{15}+u^{10}+u^5+1))^{37^5}$
   Hence, Number of cyclic codes; $(37^5+1)^3$
6. When $m = 6$, then $n = 5 \cdot 6 \cdot 37^6$
   $(u^n - 1) = (u^{5 \cdot 6 \cdot 37^6} - 1) = (u^{30} - 1)^{37^6}$
   $= ((u+36)(u+1)(u+27)(u+26)(u+11)(u+10)(u^4+36u^3+u^2+36u+1)(u^4+27u^3+26u^2+36u+10)(u^4+26u^3+10u^2+u+26)(u^4+11u^3+10u^2+36u+26)(u^4+10u^3+26u^2+u+10)(u^4+u^3+u^2+u+1))^{37^6}$
   Hence, Number of cyclic codes; $(37^6+1)^{12}$
7. When $m = 7$, then $n = 5 \cdot 7 \cdot 37^7$
   $(u^n - 1) = (u^{5 \cdot 7 \cdot 37^7} - 1) = (u^{35} - 1)^{37^7}$
   $= ((u+36)(u^{12}+28u^{11}+36u^{10}+8u^9+u^8+29u^7+35u^6+9u^5+u^4+28u^3+36u^2+8u+1)(u^{12}+8u^{11}+36u^{10}+28u^9+u^8+9u^7+35u^6+29u^5+u^4+8u^3+36u^2+28u+1)(u^4+u^3+u^2+u+1)(u^3+29u^2+28u+36)(u^3+u^2+u+1))^{37^7}$
   Hence, Number of cyclic codes; $(37^7+1)^6$
8. When $m = 8$, then $n = 5 \cdot 8 \cdot 37^8$
   $(u^n - 1) = (u^{5 \cdot 8 \cdot 37^8} - 1) = (u^{40} - 1)^{37^8}$
   Hence, Number of cyclic codes; $(37^8+1)^{14}$
9. When $m = 9$, then $n = 5 \cdot 9 \cdot 37^9$
   $(u^n - 1) = (u^{5 \cdot 9 \cdot 37^9} - 1) = (u^{45} - 1)^{37^9}$
   Hence, Number of cyclic codes; $(37^9+1)^{18}$

10. When $m = 10$, then $n = 5 \cdot 10 \cdot 37^{10}$
$(u^n - 1) = (u^{5 \cdot 10 \cdot 37^{10}} - 1) = (u^{50} - 1)^{37^{10}}$
Hence, Number of cyclic codes; $(37^{10} + 1)^6$

2.10 Enumeration of the number of cyclic codes of $u^n - 1$ over $GF(37)$ when $n = p \cdot 37^m$ where p is prime, and $m \geq 0$

Let $m \in \mathbb{Z}$, then;
$(u^n - 1) = (u^{p \cdot 37^m} - 1)$

1. When $p = 2$, then $n = 2 \cdot 37^m$
$(u^n - 1) = (u^{2 \cdot 37^m} - 1)\ \forall m = 0, 1, 2, \ldots$
Let $m = 0, 1, 2, \ldots$, then $(u^n - 1) = (u^{2 \cdot 37^{0,1,2,\ldots}} - 1)$
Hence, $N_0 = (37^0 + 1)^2$, $N_1 = (37^1 + 1)^2$, $N_2 = (37^2 + 1)^2, \ldots$
In general, when $p = 2$, the number of cyclic codes of $(u^{p \cdot 37^m} - 1)$ over $GF(37)$ is given by $N = (37^m + 1)^2$ for all $m \geq 0$.
2. When $p = 3$, then $n = 3 \cdot 37^m$
$(u^n - 1) = (u^{3 \cdot 37^m} - 1)\ \forall m = 0, 1, 2, \ldots$
Let $m = 0, 1, 2, \ldots$, then $(u^n - 1) = (u^{3 \cdot 37^{0,1,2,\ldots}} - 1)$
Hence, $N_0 = (37^0 + 1)^3$, $N_1 = (37^1 + 1)^3$, $N_2 = (37^2 + 1)^3, \ldots$
In general, when $p = 3$, the number of cyclic codes of $(u^{p \cdot 37^m} - 1)$ over $GF(37)$ is given by $N = (37^m + 1)^3$ for all $m \geq 0$.
3. When $p = 5$, then $n = 5 \cdot 37^m$
$(u^n - 1) = (u^{5 \cdot 37^m} - 1)\ \forall m = 0, 1, 2, \ldots$
Let $m = 0, 1, 2, \ldots$, then $(u^n - 1) = (u^{5 \cdot 37^{0,1,2,\ldots}} - 1)$
Hence, $N_0 = (37^0 + 1)^2$, $N_1 = (37^1 + 1)^2$, $N_2 = (37^2 + 1)^2, \ldots$
In general, when $p = 5$, the number of cyclic codes of $(u^{p \cdot 37^m} - 1)$ over $GF(37)$ is given by $N = (37^m + 1)^2$ for all $m \geq 0$.
4. When $p = 7$, then $n = 7 \cdot 37^m$
$(u^n - 1) = (u^{7 \cdot 37^m} - 1)\ \forall m = 0, 1, 2, \ldots$
Let $m = 0, 1, 2, \ldots$, then $(u^n - 1) = (u^{7 \cdot 37^{0,1,2,\ldots}} - 1)$
Hence, $N_0 = (37^0 + 1)^3$, $N_1 = (37^1 + 1)^3$, $N_2 = (37^2 + 1)^3, \ldots$
In general, when $p = 5$, the number of cyclic codes of $(u^{p \cdot 37^m} - 1)$ over $GF(37)$ is given by $N = (37^m + 1)^3$ for all $m \geq 0$.
5. When $p = 11$, then $n = 11 \cdot 37^m$
$(u^n - 1) = (u^{11 \cdot 37^m} - 1)\ \forall m = 0, 1, 2, \ldots$
Let $m = 0, 1, 2, \ldots$, then $(u^n - 1) = (u^{11 \cdot 37^{0,1,2,\ldots}} - 1)$
Hence, $N_0 = (37^0 + 1)^3$, $N_1 = (37^1 + 1)^3$, $N_2 = (37^2 + 1)^3, \ldots$
In general, when $p = 11$, the number of cyclic codes of $(u^{p \cdot 37^m} - 1)$ over $GF(37)$ is given by $N = (37^m + 1)^3$ for all $m \geq 0$.
6. When $p = 13$, then $n = 13 \cdot 37^m$
$(u^n - 1) = (u^{13 \cdot 37^m} - 1)\ \forall m = 0, 1, 2, \ldots$
Let $m = 0, 1, 2, \ldots$, then $(u^n - 1) = (u^{13 \cdot 37^{0,1,2,\ldots}} - 1)$
Hence, $N_0 = (37^0 + 1)^2$, $N_1 = (37^1 + 1)^2$, $N_2 = (37^2 + 1)^2, \ldots$
In general, when $p = 13$, the number of cyclic codes of $(u^{p \cdot 37^m} - 1)$ over $GF(37)$ is given by $N = (37^m + 1)^2$ for all $m \geq 0$.
7. When $p = 17$, then $n = 17 \cdot 37^m$
$(u^n - 1) = (u^{17 \cdot 37^m} - 1)\ \forall m = 0, 1, 2, \ldots$
Let $m = 0, 1, 2, \ldots$, then $(u^n - 1) = (u^{17 \cdot 37^{0,1,2,\ldots}} - 1)$

Hence, $N_0 = (37^0 + 1)^2$, $N_1 = (37^1 + 1)^2$, $N_2 = (37^2 + 1)^2, \ldots$
In general, when $p = 17$, the number of cyclic codes of $(u^{p \cdot 37^m} - 1)$ over $GF(37)$ is given by $N = (37^m + 1)^2$ for all $m \geq 0$.

8. When $p = 19$, then $n = 19 \cdot 37^m$
$(u^n - 1) = (u^{19 \cdot 37^m} - 1)\ \forall m = 0, 1, 2, \ldots$
Let $m = 0, 1, 2, \ldots$, then $(u^n - 1) = (u^{19 \cdot 37^{0,1,2,\ldots}} - 1)$
Hence, $N_0 = (37^0 + 1)^{10}$, $N_1 = (37^1 + 1)^{10}$, $N_2 = (37^2 + 1)^{10}, \ldots$
In general, when $p = 19$, the number of cyclic codes of $(u^{p \cdot 37^m} - 1)$ over $GF(37)$ is given by $N = (37^m + 1)^{10}$ for all $m \geq 0$.

9. When $p = 23$, then $n = 23 \cdot 37^m$
$(u^n - 1) = (u^{23 \cdot 37^m} - 1)\ \forall m = 0, 1, 2, \ldots$
Let $m = 0, 1, 2, \ldots$, then $(u^n - 1) = (u^{23 \cdot 37^{0,1,2,\ldots}} - 1)$
Hence, $N_0 = (37^0 + 1)^2$, $N_1 = (37^1 + 1)^2$, $N_2 = (37^2 + 1)^2, \ldots$
In general, when $p = 23$, the number of cyclic codes of $(u^{p \cdot 37^m} - 1)$ over $GF(37)$ is given by $N = (37^m + 1)^2$ for all $m \geq 0$.

2.11 Generalization of the prime field $GF(37)$

Lemma 1. *Suppose $n = x^m \cdot 37^y$, let C_{x^m} be the number of cyclotomic cosets of 37 mod x^m of the cyclotomic polynomial $u^{x^m} - 1$, then the number of cyclic codes over a prime field $GF(37)$ of $u^n - 1$, denoted by $N_{GF(37)}$, is given by:*

$$N_{GF(37)} = (37^y + 1)^{C_{x^m}}$$

Proof. .
By induction, we need to show that $\forall n = x^m \cdot 37^y$, $N_{GF(37)} = (37^y + 1)^{C_{x^m}}$ where C_{x^m} is the number of cyclotomic cosets of 37 mod x^m
Assume the statement is true for some $n = x^m \cdot 37^y$, we need to show that the statement holds for $n = x^{m+1} \cdot 37^{y+1}$. That is, $N_{GF(37)} = (37^{m+1} + 1)^{C_{x^{m+1}}}$.

Base Case ($m = 0$):
Here, $x^m = 1$, $u^{x^m} - 1$
Consider the cyclotomic cosets of $37 \mod x^m = 37 \mod 1$ over $GF(37)$

$$C_j = \{j \cdot 37^k \mod 1 \in \mathbb{Z}_n : k = 0, 1, 2, \ldots\}$$

$u^{x^m} - 1$ is linear, so $C_{x^m} = 1$
Now, for any arbitrary value of y, let $n = 37^y$. When $y = 0$,
$N_{\mathrm{GF}(37)} = (37^y + 1)^{C_{x^m}} = (1 + 1)^1 = 2^\beta$
Where β is the number of cyclotomic cosets $\forall\ R_n = \mathrm{GF}(q)/\langle u^n - 1\rangle$.
Therefore, this holds true for the base case.

Inductive Step:
Assume the statement is true for some $m = \alpha$, i.e., for $n = x^\alpha \cdot 37^y$
We have

$$N_{GF(37)} = (37^y + 1)^{C_{x^\alpha}}$$

Now, consider $m = \alpha + 1$, so that $n = x^{\alpha+1} \cdot 37^y$.
The number of cyclotomic cosets of 37 mod $x^{\alpha+1}$ is $C_{x^{\alpha+1}}$
By the inductive hypothesis,

$$N_{GF(37)} = (37^y + 1)^{C_{x^m}}$$

We show that for $m = \alpha + 1$,
$N_{GF(37)} = (37^y + 1)^{C_{x^{\alpha+1}}}$
From the Ring of polynomials, R_n, it can be inferred that the number of cyclic codes, denoted by N,
$N = 2^\beta = 2^{\beta+1} - 2^\beta$ where β is the number of cyclotomic cosets.
Therefore, we show that for arbitrary number of cyclotomic cosets x^α,
$N = (37^y + 1)^{x^{\alpha+1}} - (37^y + 1)^{x^\alpha}$

Using the property of exponents,
$\frac{(37^y+1)^{x^{\alpha+1}}}{(37^y+1)^{x^\alpha}} = (37^y + 1)^{x^{\alpha+1}} \cdot (37^y + 1)^{-x^\alpha}$
Since $x^{\alpha+1} - x^\alpha \subset C_{x^\alpha}$
$\implies (37^y + 1)^{x^{\alpha+1}} \cdot (37^y + 1)^{-x^\alpha} = (37^y + 1)^{x^{\alpha+1}-x^\alpha} = N$
Therefore, by induction, the statement holds for $m = 0$, $m = \alpha$, and $m = \alpha + 1$, thus holds for all $m \geq 0$.

□

3 Conclusion

The analysis focused on understanding the relationship between the number of irreducible monic polynomials that $u^n - 1$ factors into and the corresponding number of cyclic codes over $GF(37)$. The main findings from the investigation are summarized as follows:

1. The number of irreducible monic factors of $u^n - 1$ over $GF(37)$ correspond to the number of cyclotomic cosets of 37 mod n.
2. The number of cyclic codes over GF(37) of $u^n - 1$, denoted as N, is given by;
$$N = \begin{cases} 2^\beta, & \forall\beta \\ (37^m + 1)^{2m}, & \text{if } n = 2^m \cdot 37^m, \text{ where } m \in \mathbb{Z}^+ \\ (37^m + 1), & \text{if } n = 37^m, \text{ where } m \in \mathbb{Z}^+ \end{cases}$$
Where β is the number of cyclotomic cosents of 37 mod n of $u^n - 1$.
3. The cyclic codes over $GF(37)$ for a wide range of parameters where n can be expressed as $n = x^m \cdot 37^y$ can be enumerated by a relationship between the number of cyclotomic cosets of 37 mod x^m, C_{x^m}, and the resulting number of cyclic codes $N_{GF(37)}$, be given by the formula:
$$N_{GF(37)} = (37^y + 1)^{C_{x^m}}$$
$\forall x, y, m \in Z^+$.

Competing Interests

Authors have declared no competing interest.

References

[1] Wang J, Liu L, Lyu S, Wang Z, Zheng M, Lin F, Ling C. Quantum-safe cryptography: crossroads of coding theory and cryptography. Science China Information Sciences. 2022;65(1):111301.

[2] La Guardia GG, Alves MM. On cyclotomic cosets and code constructions. Linear Algebra and its Applications. 2016;488:302-319.

[3] Kahkeshan S, Homavazir Z. Enhancement of voice quality and system capacity by error detection and correction method in wireless digital communication. In 2023 IEEE 4th Annual Flagship India Council International Subsections Conference (INDISCON) IEEE. 2023, August. 65:1-7.

[4] Kandhway K. Modeling burst errors in a fading channel. In 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT) IEEE. 2022, April;409-414).

[5] Koroglu ME, Siap I. Quantum codes from a class of constacyclic codes over group algebras. Malaysian Journal of Mathematical Sciences. 2017;11(2):289-301.

[6] Childs LN, Childs LN. Rings and fields. Cryptology and Error Correction: An Algebraic Introduction and Real-World Applications. 2019;65-82.

[7] Hall S. Encoding and decoding the message. The discourse studies reader: Main currents in theory and analysis. 2014;111-121.

[8] Interlando JC, Palazzo R, Elia M. On the decoding of Reed-Solomon and BCH codes over integer residue rings. IEEE Transactions on Information Theory. 1997;43(3):1013-1021.

[9] Jakhar A. On the factors of a polynomial. Bulletin of the London Mathematical Society. 2020;52(1)158-160.

[10] Shannon EC. Error detection and correction using the BCH Code; 2019.

[11] Shparlinski I. Finite fields: Theory and computation: The meeting point of number theory, computer science, coding theory and cryptography. Springer Science & Business Media. 2013;477.

[12] Mesnager S. Linear codes from functions. In Concise Encyclopedia of Coding Theory. Chapman and Hall/CRC; 2021;463-526.

[13] Olege F. On the generators of codes of ideals of the polynomial ring for error control; 2017.

[14] Puchinger S. Construction and decoding of evaluation codes in Hamming and rank metric (Doctoral dissertation, Universit¨at Ulm); 2018.

[15] Raghunandan K. Wireless Systems—Technologies. In Introduction to Wireless Communications and Networks: A Practical Perspective. Cham: Springer International Publishing. 2022;39-57

[16] Lao H, Kivunge B, Kimani P, Muthoka G. On the Number of Cyclotomic Cosets and Cyclic Codes over Z_{13}; 2015

[17] Lao H, Kivunge B, Muthoka G, Mwangi P. Enumeration of cyclic codes over GF (17); 2017.

[18] Maganga BM, Joash MN. Enumeration of cyclic codes over GF (19). Kenyatta University; (2017).

[19] Runji, Flora Mati. Enumeration of cyclic codes over GF (5). 2014;4(4):3241-3302.

[20] Simatwo KB, Mati RF, Karieko OR. Enumeration of cyclic codes over GF (23). Journal of Advances in Mathematics and Computer Science. 2023;38(9):194-206.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
https://www.sdiarticle5.com/review-history/116921