



# On the Number of Cyclic Codes Over $\mathbb{Z}_{31}$

John Joseph O. Ondiany<sup>a\*</sup>, Obogi Robert Karioko<sup>a</sup>,  
Lao Hussein Mude<sup>b</sup> and Fred Nyamitago Monari<sup>a</sup>

<sup>a</sup>Department of Mathematics and Actuarial Sciences, Kisii University, P. O. Box 1957-40200, Kisii, Kenya.

<sup>b</sup>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: <https://doi.org/10.9734/jamcs/2024/v39i71912>

## 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/119485>

Received: 27/04/2024

Accepted: 02/07/2024

Published: 10/07/2024

Original Research Article

## Abstract

Let  $n$  be a positive integer,  $y^n - 1$  cyclotomic polynomial and  $\mathbb{Z}_q$  be a given finite field. In this study we determined the number of cyclic codes over  $\mathbb{Z}_{31}$ . First, we partitioned the cyclotomic polynomial  $y^n - 1$  using cyclotomic cosets  $31 \bmod n$  and factorized  $y^n - 1$  using case to case basis. Each monic divisor obtained is a generator polynomial and generate cyclic codes. The results obtained are useful in the field of coding theory and more especially, in error correcting codes.

Keywords: Code; cyclic codes; cyclotomic coset.

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

\*Corresponding author: E-mail: [jondiany5@gmail.com](mailto:jondiany5@gmail.com);

Cite as: Ondiany, John Joseph O., Obogi Robert Karioko, Lao Hussein Mude, and Fred Nyamitago Monari. 2024. "On the Number of Cyclic Codes Over  $\mathbb{Z}_{31}$ ". *Journal of Advances in Mathematics and Computer Science* 39 (7):55-69. <https://doi.org/10.9734/jamcs/2024/v39i71912>.

## 1 Introduction

The study of cyclic codes have attracted attention of many researchers since the advent of cryptography, this is because cyclic codes have direct applications in coding theory in particular error correction coding [1, 2, 3]. The problem of finding codes which are optimal, that will transmit a wide varieties of messages fast and correct many errors has been a motivating factor in the study of codes [4, 5, 6, 7]. Factorization of polynomials over a finite field is of interest in algebraic coding theory, computational number theory, computer algebra, and cryptography among other areas see [8, 9, 10, 11, 12]. Cyclotomic cosets has been used to partition Cyclotomic polynomials  $y^n - 1$  [13, 14, 15]. Cyclic codes of length  $n$  over finite fields  $\mathbb{Z}_q$  for which  $q \leq 23$  has been fully characterized and a general formula for computing the number of cyclic codes given see [16, 17, 18, 4, 19, 20, 21, 22]. In this study the number of cyclic codes over  $\mathbb{Z}_{31}$  are determined and generalizations made over  $\mathbb{Z}_{31}$ .

### 1.1 Definitions

- i. **Code:** Let  $F$  be a finite set with  $q$  symbols, there are  $q^n$  different sequences of length  $n$ , of these only  $q^k$  are codewords since the  $r$  check digits within any codeword are completely determined by the  $k$  message digits. The set consisting of  $q^k$  codewords of length  $n$  is called a code.
- ii. **Cyclic Code:** Let  $C$  be a linear code over a finite field  $GF(q)$  of block  $n$ ,  $C$  is called a cyclic code, if for every codeword  $a_0, a_1, a_2, \dots, a_n$  from  $C$ , the word  $a_n, a_0, a_1, a_2, \dots, a_{n-1}$  in  $C$  obtain by a cyclic right shift of component is also a codeword. This also involves the left shift. Therefore a linear code  $C$  is cyclic precisely when it is invariant under all cyclic shifts.
- iii. **Cyclotomic Coset:** Let  $n$  be relatively to  $q$ . The cyclotomic coset of  $q \bmod n$  is defined by  $C_i = \{i \cdot q^j \bmod n \in \mathbb{Z}_n, j = 0, 1, 2, 3, \dots\}$

## 2 Main Results

### 2.1 Number of cyclotomic cosets and factorization of $y^n - 1$ over $\mathbb{Z}_{31}$

- i. Let  $n = 1$ , Then  $C_i = \{i \cdot 31^j \bmod 1 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$  We get 1 cyclotomic cosets 31 mod 1. We factorize  $y - 1$ .  $y - 1 = (y + 30)$ . The number of irreducible monic polynomial is 1 of degree 1.
- ii. Let  $n = 2$ , Then  $C_i = \{i \cdot 31^j \bmod 2 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1\}$ . We get 2 cyclotomic cosets 31 mod 2. We factorize  $y^2 - 1$ .  $y^2 - 1 = (y - 1)(y + 1) = (y + 30)(y + 1)$ . The number of irreducible monic polynomial are also 2 of degree 1.
- iii. Let  $n = 3$ , Then  $C_i = \{i \cdot 31^j \bmod 3 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1\}$ ,  $C_2 = \{2\}$ . We get 3 cyclotomic cosets 31 mod 3. We factorize  $y^3 - 1$ .  $y^3 - 1 = (y - 1)(y^2 + y + 1) = (y + 30)(y + 26)(y + 6)$ . The number of irreducible monic polynomial are also 3 of degree 1.
- iv. Let  $n = 4$ , Then  $C_i = \{i \cdot 31^j \bmod 4 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 3\}$ ,  $C_2 = \{2\}$ . We get 3 cyclotomic cosets 31 mod 4. We factorize  $y^4 - 1$ .  $y^4 - 1 = (y^2 - 1)(y^2 + 1) = (y - 1)(y + 1)(y^2 + 1)$ . The number of irreducible monic polynomial are also 3, 2 of degree 1 and 1 of degree 2.
- v. Let  $n = 5$ , Then  $C_i = \{i \cdot 31^j \bmod 5 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1\}$ ,  $C_2 = \{2\}$ ,  $C_3 = \{3\}$ ,  $C_4 = \{4\}$ . We get 5 cyclotomic cosets 31 mod 5. We factorize  $y^5 - 1$ .  $y^5 - 1 = (y - 1)(y^4 + y^3 + y^2 + y + 1) = (y + 30)(y + 29)(y + 27)(y + 15)(y + 23)$ . The number of irreducible monic polynomial are also 5 of degree 1.
- vi. Let  $n = 6$ , Then  $C_i = \{i \cdot 31^j \bmod 6 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1\}$ ,  $C_2 = \{2\}$ ,  $C_3 = \{3\}$ ,  $C_4 = \{4\}$ ,  $C_5 = \{5\}$ . We get 6 cyclotomic cosets 31 mod 6. We factorize  $y^6 - 1$ .  $y^6 - 1 = (y^3 - 1)(y^3 + 1) = (y + 30)(y + 26)(y + 6)(y + 1)(y + 5)(y + 25)$ . The number of irreducible monic polynomial are also 6 of degree 1.

- vii. Let  $n = 7$ , Then  $C_i = \{i.31^j \bmod 7 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 2, 3, 4, 5, 6\}$ . We get 2 cyclotomic cosets 31 mod 7. We factorize  $y^7 - 1$ .  $y^7 - 1 = (y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)$ . The number of irreducible monic polynomial are also 2, 1 of degree 1 and 1 of degree 7.
- viii. Let  $n = 8$ , Then  $C_i = \{i.31^j \bmod 8 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 7\}$ ,  $C_2 = \{2, 6\}$ ,  $C_3 = \{3, 5\}$ ,  $C_4 = \{4\}$ . We get 5 cyclotomic cosets 31 mod 8. We factorize  $y^8 - 1$ .  $y^8 - 1 = (y^4 - 1)(y^4 + 1) = (y^2 - 1)(y^2 + 1)(y^4 + 1) = (y + 30)(y + 1)(y^2 + 1)(y^4 + 1) = (y + 30)(y + 1)(y^2 + 1)(y^2 + 8y + 1)(y^2 + 23y + 1)$ . The number of irreducible monic polynomial are also 5, 2 of degree 1 and 3 of degree 2.
- ix. Let  $n = 9$ , Then  $C_i = \{i.31^j \bmod 9 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 4, 7\}$ ,  $C_2 = \{2, 6, 8\}$ ,  $C_3 = \{3\}$ ,  $C_5 = \{5\}$ . We get 5 cyclotomic cosets 31 mod 9. We factorize  $y^9 - 1$ .  $y^9 - 1 = (y - 1)(y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y + 26)(y + 6)(y^3 + 1)(y^3 + 26)$ . The number of irreducible monic polynomial are also 5, 3 of degree 1 and 2 of degree 3.
- x. Let  $n = 10$ , Then  $C_i = \{i.31^j \bmod 10 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1\}$ ,  $C_2 = \{2\}$ ,  $C_3 = \{3\}$ ,  $C_4 = \{4\}$ ,  $C_5 = \{5\}$ ,  $C_6 = \{6\}$ ,  $C_7 = \{7\}$ ,  $C_8 = \{8\}$ ,  $C_9 = \{9\}$ . We get 10 cyclotomic cosets 31 mod 10. We factorize  $y^{10} - 1$ .  $y^{10} - 1 = (y^5 - 1)(y^5 + 1) = (y + 30)(y + 29)(y + 27)(y + 15)(y + 23)(y^5 + 1) = (y + 30)(y + 29)(y + 27)(y + 15)(y + 23)(y + 1)(y + 2)(y + 4)(y + 8)(y + 16)$ . The number of irreducible monic polynomial are also 10 of degree 1.
- xi. Let  $n = 11$ , Then  $C_i = \{i.31^j \bmod 11 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 9, 4, 3, 5\}$ ,  $C_2 = \{2, 6, 7, 8, 10\}$ . We get 3 cyclotomic cosets 31 mod 11. We factorize  $y^{11} - 1$ .  $y^{11} - 1 = (y - 1)(y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y^5 + 10y^4 + 30y^3 + y^2 + 9y + 30)(y^5 + 22y^4 + 30y^3 + y^2 + 21y + 30)$ . The number of irreducible monic polynomial are also 3, 1 of degree 1 and two of degree 5.
- xii. Let  $n = 12$ , Then  $C_i = \{i.31^j \bmod 12 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 7\}$ ,  $C_2 = \{2\}$ ,  $C_3 = \{3, 9\}$ ,  $C_4 = \{4\}$ ,  $C_5 = \{5, 11\}$ ,  $C_6 = \{6\}$ ,  $C_8 = \{8\}$ ,  $C_{10} = \{10\}$ . We get 9 cyclotomic cosets 31 mod 12. We factorize  $y^{12} - 1$ .  $y^{12} - 1 = (y^6 - 1)(y^6 + 1) = (y^3 - 1)(y^3 + 1)(y^6 + 1) = (y + 30)(y + 26)(y + 6)(y + 1)(y + 5)(y + 25)(y^2 + 1)(y^2 + 5)(y^2 + 25)$ . The number of irreducible monic polynomial are also 9, 6 of degree 1 and 3 of degree 2.
- xiii. Let  $n = 13$ , Then  $C_i = \{i.31^j \bmod 13 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 5, 8, 12\}$ ,  $C_2 = \{2, 10, 11, 13\}$ ,  $C_4 = \{4, 7, 9, 6\}$ . There are 4 cyclotomic cosets 31 mod 13. We factorize  $y^{13} - 1$ .  $y^{13} - 1 = (y - 1)(y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y^4 + 4y^3 + 11y^2 + 4y + 1)(y^4 + 6y^3 + 29y^2 + 6y + 1)(y^4 + 22y^3 + 27y^2 + 22y + 1)$ . The number of irreducible monic polynomial are also 4, 1 of degree 1 and 3 of degree 4.
- xiv. Let  $n = 14$ , Then  $C_i = \{i.31^j \bmod 14 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 3, 9, 13, 11, 5\}$ ,  $C_2 = \{2, 4, 6, 8, 10, 12\}$ ,  $C_7 = \{7\}$  4 cyclotomic cosets 31 mod 14 are obtained. We factorize  $y^{14} - 1$ .  $y^{14} - 1 = (y^7 - 1)(y^7 + 1) = (y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y^7 + 1) = (y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y + 1)(y^6 + 30y^5 + y^4 + 30y^3 + y^2 + 30y + 1)$ . The number of irreducible monic polynomial are also 4, 2 of degree 1 and 2 of degree 6.
- xv. Let  $n = 15$ , Then  $C_i = \{i.31^j \bmod 15 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1\}$ ,  $C_2 = \{2\}$ ,  $C_3 = \{3\}$ ,  $C_4 = \{4\}$ ,  $C_5 = \{5\}$ ,  $C_6 = \{6\}$ ,  $C_7 = \{7\}$ ,  $C_8 = \{8\}$ ,  $C_9 = \{9\}$ ,  $C_{10} = \{10\}$ ,  $C_{11} = \{11\}$ ,  $C_{12} = \{12\}$ ,  $C_{13} = \{13\}$ ,  $C_{14} = \{14\}$ . There are 15 cyclotomic cosets 31 mod 15. We factorize  $y^{15} - 1$ .  $y^{15} - 1 = (y - 1)(y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y + 26)(y + 6)(y + 3)(y + 21)(y + 29)(y + 23)(y + 27)(y + 17)(y + 11)(y + 24)(y + 22)(y + 12)(y + 13)(y + 15)$ . The number of irreducible monic polynomial are also 15 of degree 1.
- xvi. Let  $n = 16$ , Then  $C_i = \{i.31^j \bmod 16 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 15\}$ ,  $C_2 = \{2, 14\}$ ,  $C_3 = \{3, 13\}$ ,  $C_4 = \{4, 12\}$ ,  $C_5 = \{5, 11\}$ ,  $C_6 = \{6, 10\}$ ,  $C_8 = \{8\}$ ,  $C_9 = \{9, 7\}$ . There are 9 cyclotomic cosets 31 mod 16. We factorize  $y^{16} - 1$ .  $y^{16} - 1 = (y^8 - 1)(y^8 + 1) = (y^2 - 1)(y^2 + 1)(y^4 + 1)(y^8 + 1) = (y + 30)(y + 1)(y^2 + 1)(y^2 + 8y + 1)(y^2 + 23y + 1)(y^8 + 1) = (y + 30)(y + 1)(y^2 + 1)(y^2 + 8y + 1)(y^2 + 26y + 1)(y^2 + 23y + 1)(y^2 + 5y + 1)(y^2 + 14y + 1)(y^2 + 17y + 1)$ . The number of irreducible monic polynomial are also 9, 2 of degree 1 and 7 of degree 2.

- xvii. Let  $n = 17$ , Then  $C_i = \{i \cdot 31^j \bmod 17 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$  There are 2 cyclotomic cosets 31 mod 17. We factorize  $y^{17} - 1$ .  $y^{17} - 1 = (y - 1)(y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)$ . The number of irreducible monic polynomial are also 2, 1 of degree 1 and 1 of degree 16.
- xviii. Let  $n = 18$ , Then  $C_i = \{i \cdot 31^j \bmod 18 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 7, 13\}$ ,  $C_2 = \{2, 8, 14\}$ ,  $C_3 = \{3\}$ ,  $C_4 = \{4, 10, 16\}$ ,  $C_5 = \{5, 11, 17\}$ ,  $C_6 = \{6\}$ ,  $C_9 = \{9\}$ ,  $C_{12} = \{12\}$ ,  $C_{15} = \{15\}$ . There are 10 cyclotomic cosets 31 mod 18. We factorize  $y^{18} - 1$ .  $y^{18} - 1 = (y^9 - 1)(y^9 + 1) = (y + 30)(y + 26)(y + 6)(y^3 + 6)(y^3 + 26)(y^9 + 1) = (y + 30)(y + 26)(y + 6)(y^3 + 6)(y^3 + 26)(y + 1)(y + 5)(y + 25)(y^3 + 5)(y^3 + 25)$ . The number of irreducible monic polynomial are also 10, 6 of degree 1 and 4 of degree 3.
- xix. Let  $n = 19$ , Then  $C_i = \{i \cdot 31^j \bmod 19 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 8, 10, 11, 12, 18\}$ ,  $C_2 = \{2, 3, 5, 14, 16, 17\}$ ,  $C_4 = \{4, 6, 7, 9, 13, 15\}$ . There are 4 cyclotomic cosets 31 mod 19. We factorize  $y^{19} - 1$ .  $y^{19} - 1 = (y - 1)(y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y^6 + 4y^5 + 14y^4 + 18y^3 + 14y^2 + 4y + 1)(y^6 + 5y^5 + 25y^4 + y^3 + 5y^2 + 25y + 1)(y^6 + 25y^5 + 5y^4 + y^3 + 25y^3 + 5y + 1)$ . The number of irreducible monic polynomial are also 4, 1 of degree 1 and 3 of degree 6.
- xx. Let  $n = 20$ , Then  $C_i = \{i \cdot 31^j \bmod 20 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 11\}$ ,  $C_2 = \{2\}$ ,  $C_3 = \{3, 13\}$ ,  $C_4 = \{4\}$ ,  $C_5 = \{5, 15\}$ ,  $C_6 = \{6\}$ ,  $C_7 = \{7, 17\}$ ,  $C_8 = \{8\}$ ,  $C_9 = \{9, 19\}$ ,  $C_{10} = \{10\}$ ,  $C_{12} = \{12\}$ ,  $C_{14} = \{14\}$ ,  $C_{16} = \{16\}$ ,  $C_{18} = \{18\}$ . There are 15 cyclotomic cosets 31 mod 20. We factorize  $y^{20} - 1$ .  $y^{20} - 1 = (y^{10} - 1)(y^{10} + 1) = (y^5 - 1)(y^5 + y)(y^{10} + 1) = (y + 30)(y + 29)(y + 27)(y + 15)(y + 23)(y + 1)(y + 2)(y + 4)(y + 8)(y + 16)(y^{10} + 1) = (y + 30)(y + 29)(y + 27)(y + 15)(y + 23)(y + 1)(y + 2)(y + 4)(y + 8)(y + 16)(y^2 + 1)(y^2 + 2)(y^2 + 4)(y^2 + 8)(y^2 + 16)$ . The number of irreducible monic polynomial are also 15, 10 of degree 1 and 5 of degree 2.
- xxi. Let  $n = 21$ , Then  $C_i = \{i \cdot 31^j \bmod 21 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 4, 10, 13, 16, 19\}$ ,  $C_2 = \{2, 5, 8, 11, 17, 20\}$ ,  $C_3 = \{3, 6, 9, 12, 15, 18\}$ ,  $C_7 = \{7\}$ ,  $C_{14} = \{14\}$ . There are 6 cyclotomic cosets 31 mod 21. We factorize  $y^{21} - 1$ .  $y^{21} - 1 = (y - 1)(y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y + 6)(y + 26)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y^{12} + 30y^{11} + y^{10} + 30y^9 + y^8 + 30y^7 + y^6 + 30y^5 + y^4 + 30y^3 + y^2 + 30y + 1) = (y + 30)(y + 6)(y + 26)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y^6 + 5y^5 + 25y^4 + y^3 + 5y^2 + 25y + 1)(y^6 + 25y^5 + 5y^4 + y^3 + 25y^2 + 5y + 1)$ . The number of irreducible monic polynomial are also 6, 3 of degree 1 and 3 of degree 6.
- xxii. Let  $n = 22$ , Then  $C_i = \{i \cdot 31^j \bmod 22 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 3, 5, 9, 15\}$ ,  $C_2 = \{2, 6, 8, 10, 18\}$ ,  $C_4 = \{4, 14, 12, 16, 20\}$ ,  $C_7 = \{7, 13, 17, 19, 21\}$ ,  $C_{11} = \{11\}$ . There are 6 cyclotomic cosets 31 mod 22. We factorize  $y^{22} - 1$ .  $y^{22} - 1 = (y^{11} - 1)(y^{11} + 1) = (y + 30)(y^5 + 10y^4 + 30y^3 + y^2 + 9y + 30)(y^5 + 22y^4 + 30y^3 + y^2 + 21y + 30)(y + 1)(y^{10} + 30y^9 + y^8 + 30y^7 + y^6 + 30y^5 + y^4 + 30y^3 + y^2 + 30y + 1) = (y + 30)(y + 1)(y^5 + 9y^4 + 30y^3 + 30y^2 + 21y + 1)(y^5 + 10y^4 + 30y^3 + y^2 + 9y + 30)(y^5 + 21y^4 + 30y^3 + 30y^2 + 9y + 1)(y^5 + 22y^4 + 30y^3 + y^2 + 21y + 30)$ . The number of irreducible monic polynomial are also 6, 2 of degree 1 and 4 of degree 5.
- xxiii. Let  $n = 23$ , Then  $C_i = \{i \cdot 31^j \bmod 23 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ ,  $C_5 = \{5, 10, 11, 14, 7, 15, 17, 19, 20, 21, 22\}$  There are 3 cyclotomic cosets 31 mod 23. We factorize  $y^{23} - 1$ .  $y^{23} - 1 = (y - 1)(y^{22} + y^{21} + y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y^{11} + 8y^{10} + 5y^9 + 27y^8 + 20y^7 + 14y^6 + 18y^5 + 27y^4 + 4y^3 + 10y^2 + 7y + 30)(y^{11} + 24y^{10} + 21y^9 + 27y^8 + 4y^7 + 13y^6 + 17y^5 + 11y^4 + 4y^3 + 26y^2 + 23y + 30)$  The number of irreducible monic polynomial are also 3, 1 of degree 1 and 2 of degree 11. xxiv Let  $n = 24$ , Then  $C_i = \{i \cdot 31^j \bmod 24 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 7\}$ ,  $C_2 = \{2, 14\}$ ,  $C_3 = \{3, 21\}$ ,  $C_4 = \{4\}$ ,  $C_5 = \{5, 11\}$ ,  $C_6 = \{6, 18\}$ ,  $C_8 = \{8\}$ ,  $C_9 = \{9, 15\}$ ,  $C_{12} = \{12\}$ ,  $C_{13} = \{13, 19\}$ ,  $C_{16} = \{16\}$ ,  $C_{10} = \{10, 22\}$ ,  $C_{17} = \{17, 23\}$ ,  $C_{20} = \{20\}$ . There are 15 cyclotomic cosets 31 mod 24. We factorize  $y^{24} - 1$ .  $y^{24} - 1 = (y^{12} - 1)(y^{12} + 1) = (y^6 - 1)(y^6 + 1)(y^{12} + 1) = (y^3 - 1)(y^3 + 1)(y^6 + 1)(y^{12} + 1) = (y + 30)(y + 26)(y + 6)(y + 1)(y + 5)(y + 25)(y^2 + 1)(y^2 + 5)(y^2 + 25)(y^{12} + 1) = (y + 30)(y + 26)(y + 6)(y + 1)(y + 5)(y + 25)(y^2 + 1)(y^2 + 5)(y^2 + 25)(y^2 + 8y + 1)(y^2 + 23y + 1)(y^2 +$

$17y + 5)(y^2 + 14y + 5)(y^2 + 22y + 25)(y^2 + 9y + 25)$ . The number of irreducible monic polynomial are also 15, 6 of degree 1 and 9 of degree 2.

- xxv. Let  $n = 25$ , Then  $C_i = \{i.31^j \bmod 25 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 6, 11, 16, 21\}$ ,  $C_2 = \{2, 7, 12, 17, 22\}$ ,  $C_3 = \{3, 18, 8, 23, 13\}$ ,  $C_4 = \{4, 24, 19, 14, 9\}$ ,  $C_5 = \{5\}$ ,  $C_{10} = \{10\}$ ,  $C_{15} = \{15\}$ ,  $C_{20} = \{20\}$  There are 9 cyclotomic cosets 31 mod 25. We factorize  $y^{25} - 1$ .  $y^{25} - 1 = (y - 1)(y^{24} + y^{23} + y^{22} + y^{21} + y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y + 29)(y + 27)(y + 23)(y + 15)(y^5 + 15)(y^5 + 23)(y^5 + 29)(y^5 + 27)$ . The number of irreducible monic polynomial are also 9, 5 of degree 1 and 4 of degree 4.
- xxvi. Let  $n = 26$ , Then  $C_i = \{i.31^j \bmod 26 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 5, 21, 25\}$ ,  $C_2 = \{2, 10, 16, 24\}$ ,  $C_3 = \{3, 11, 15, 23\}$ ,  $C_4 = \{4, 20, 22, 6\}$ ,  $C_7 = \{7, 9, 19, 17\}$ ,  $C_8 = \{8, 14, 18, 12\}$ ,  $C_{13} = \{13\}$ . There are 8 cyclotomic cosets 31 mod 26. We factorize  $y^{26} - 1$ .  $y^{26} - 1 = (y^{13} - 1)(y^{13} + 1) = (y - 1)(y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y^{13} + 1) = (y + 30)(y^4 + 4y^3 + 11y^2 + 4y + 1)(y^4 + 6y^3 + 29y^2 + 6y + 1)(y^4 + 22y^3 + 27y^2 + 22y + 1)(y^{13} + 1) = (y + 1)(y + 30)(y^4 + 4y^3 + 11y^2 + 4y + 1)(y^4 + 6y^3 + 29y^2 + 6y + 1)(y^4 + 22y^3 + 27y^2 + 22y + 1)(y^4 + 9y^3 + 27y^2 + 9y + 1)(y^4 + 27y^3 + 11y^2 + 27y + 1)(y^4 + 25y^3 + 29y^2 + 25y + 1)$ . The number of irreducible monic polynomial are also 8, 2 of degree 1 and 6 of degree 4.
- xxvii. Let  $n = 27$ , Then  $C_i = \{i.31^j \bmod 27 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 4, 16, 10, 13, 25, 19, 22, 7\}$ ,  $C_2 = \{2, 8, 5, 20, 26, 23, 11, 17, 14\}$ ,  $C_3 = \{3, 12, 21\}$ ,  $C_6 = \{6, 24, 15\}$ ,  $C_9 = \{9\}$ ,  $C_{18} = \{18\}$ . There are 7 cyclotomic cosets 31 mod 27. We factorize  $y^{27} - 1$ .  $y^{27} - 1 = (y - 1)(y^{26} + y^{25} + y^{24} + y^{23} + y^{22} + y^{21} + y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y + 6)(y + 26)(y^3 + 6)(y^3 + 26)(y^9 + 6)(y^9 + 16)$ . The number of irreducible monic polynomial are also 7, 3 of degree 1, 2 of degree 3 and 2 of degree 9.
- xxviii. Let  $n = 28$ , Then  $C_i = \{i.31^j \bmod 28 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 3, 9, 27, 25, 19\}$ ,  $C_2 = \{2, 6, 18, 26, 22, 10\}$ ,  $C_4 = \{4, 12, 8, 24, 16, 20\}$ ,  $C_5 = \{5, 15, 17, 23, 13, 11\}$ ,  $C_7 = \{7, 21\}$ ,  $C_{14} = \{14\}$  There are 7 cyclotomic cosets 31 mod 28. We factorize  $y^{28} - 1$ .  $y^{28} - 1 = (y^{14} - 1)(y^{14} + 1) = (y^7 - 1)(y^7 + 1)(y^{14} + 1) = (y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y^7 + 1)(y^{14} + 1) = (y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y + 1)(y^6 + 30y^5 + y^4 + 30y^3 + y^2 + 30y + 1)(y^{14} + 1) = (y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y + 1)(y^6 + 30y^5 + y^4 + 30y^3 + y^2 + 30y + 1)(y^{12} + 30y^{10} + y^8 + 30y^6 + y^4 + 30y^2 + 1) = (y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y + 1)(y^6 + 30y^5 + y^4 + 30y^3 + y^2 + 30y + 1)(y^2 + 1)(y^6 + 10y^5 + 3y^4 + 10y^3 + 3y^2 + 10y + 1)(y^6 + 21y^5 + 3y^4 + 21y^3 + 3y^2 + 21y + 1)$ . The number of irreducible monic polynomial are also 7, 2 of degree 1 and 1 of degree 2, 4 of degree 6.
- xxix. Let  $n = 29$ , Then  $C_i = \{i.31^j \bmod 29 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29\}$ . There are 2 cyclotomic cosets 31 mod 29. We factorize  $y^{29} - 1$ .  $y^{29} - 1 = (y - 1)(y^{28} + y^{27} + y^{26} + y^{25} + y^{24} + y^{23} + y^{22} + y^{21} + y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1) = (y + 30)(y^{28} + y^{27} + y^{26} + y^{25} + y^{24} + y^{23} + y^{22} + y^{21} + y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)$ . The number of irreducible monic polynomial are also 2, 1 of degree 1, 1 of degree 28.
- xxx Let  $n = 30$ , Then  $C_i = \{i.31^j \bmod 15 \in \mathbb{Z}_{31} : j = 0, 1, 2, \dots\}$ ,  $C_0 = \{0\}$ ,  $C_1 = \{1\}$ ,  $C_2 = \{2\}$ ,  $C_3 = \{3\}$ ,  $C_4 = \{4\}$ ,  $C_5 = \{5\}$ ,  $C_6 = \{6\}$ ,  $C_7 = \{7\}$ ,  $C_8 = \{8\}$ ,  $C_9 = \{9\}$ ,  $C_{10} = \{10\}$ ,  $C_{11} = \{11\}$ ,  $C_{12} = \{12\}$ ,  $C_{13} = \{13\}$ ,  $C_{14} = \{14\}$ ,  $C_{15} = \{15\}$ ,  $C_{16} = \{16\}$ ,  $C_{17} = \{17\}$ ,  $C_{18} = \{18\}$ ,  $C_{19} = \{19\}$ ,  $C_{20} = \{20\}$ ,  $C_{21} = \{21\}$ ,  $C_{22} = \{22\}$ ,  $C_{23} = \{23\}$ ,  $C_{24} = \{24\}$ ,  $C_{25} = \{25\}$ ,  $C_{26} = \{26\}$ ,  $C_{27} = \{27\}$ ,  $C_{28} = \{28\}$ ,  $C_{29} = \{29\}$ . There are 30 cyclotomic cosets 31 mod 15. We factorize  $y^{30} - 1$ .  $y^{30} - 1 = (y^{15} - 1)(y^{15} + 1) = (y + 30)(y + 26)(y + 6)(y + 3)(y + 21)(y + 29)(y + 23)(y + 27)(y + 17)(y + 11)(y + 24)(y + 22)(y + 12)(y + 13)(y + 15)(y^{15} + 1) = (y + 30)(y + 26)(y + 6)(y + 3)(y + 21)(y + 29)(y + 23)(y + 27)(y + 17)(y + 11)(y + 24)(y + 22)(y + 12)(y + 13)(y + 15)(y + 12)(y + 13)(y + 15)(y + 4)(y + 5)(y + 7)(y + 8)(y + 9)(y + 10)(y + 14)(y + 16)(y + 18)(y + 19)(y + 20)(y + 25)(y + 28)(y + 1)(y + 2)$   
The number of irreducible monic polynomial are also 30 of degree 1.

**Conjecture 2.1.** Suppose  $h$  is the number of cyclotomic coset 31 mod  $n$ , then the number of cyclic codes over  $N$  over  $\mathbb{Z}_{31}$  is given by  $N = 2^h$

**Table 1.**The number of cyclic code of length  $n = 1, 2, 3, \dots, 30$  over  $\mathbb{Z}_{31}$

$n$	$y^n - 1$	Number of $q$ Cyclotomic Cosets equal $h$	Number of Cyclic code equal $2^h$
1	$y - 1$	1	$2^1 = 2$
2	$y^2 - 1$	2	$2^2 = 4$
3	$y^3 - 1$	3	$2^3 = 8$
4	$y^4 - 1$	3	$2^3 = 8$
5	$y^5 - 1$	5	$2^5 = 32$
6	$y^6 - 1$	6	$2^6 = 64$
7	$y^7 - 1$	2	$2^2 = 4$
8	$y^8 - 1$	5	$2^5 = 32$
9	$y^9 - 1$	5	$2^5 = 32$
10	$y^{10} - 1$	10	$2^{10} = 1,024$
11	$y^{11} - 1$	3	$2^3 = 8$
12	$y^{12} - 1$	9	$2^9 = 512$
13	$y^{13} - 1$	4	$2^4 = 16$
14	$y^{14} - 1$	4	$2^4 = 16$
15	$y^{15} - 1$	15	$2^{15} = 32,768$
16	$y^{16} - 1$	9	$2^9 = 512$
17	$y^{17} - 1$	2	$2^2 = 4$
18	$y^{18} - 1$	10	$2^{10} = 1,024$
19	$y^{19} - 1$	4	$2^4 = 16$
20	$y^{20} - 1$	15	$2^{15} = 32,768$
21	$y^{21} - 1$	6	$2^6 = 64$
22	$y^{22} - 1$	6	$2^6 = 64$
23	$y^{23} - 1$	3	$2^3 = 8$
24	$y^{24} - 1$	15	$2^{15} = 32,768$
25	$y^{25} - 1$	9	$2^9 = 512$
26	$y^{26} - 1$	8	$2^8 = 256$
27	$y^{27} - 1$	7	$2^7 = 128$
28	$y^{28} - 1$	7	$2^7 = 128$
29	$y^{29} - 1$	2	$2^2 = 4$
30	$y^{30} - 1$	30	$2^{30} = 1,073,741,824$

## 2.2 Number of cyclic codes when $n = 31w$ , $1 \leq w \leq 15$

$$y^n - 1 = (y - 1)^n = ((y + 30)^n) = (y + 30)^{31w}$$

- i. Let  $w = 1$ , then  $n = 31$  and  $y^{31} - 1 = (y - 1)^{31} = (y + 30)^{31}$ . Number of cyclic codes are,  $(31 + 1) = 32$ .
- ii. Let  $w = 2$ , then  $n = 62$  and  $y^{62} - 1 = (y^2 - 1)^{31} = (y - 1)^{31}(y + 1)^{31} = (y + 30)^{31}(y + 1)^{31}$ . Number of cyclic codes are,  $(31 + 1)^2 = 32^2 = 1,024$ .
- iii. Let  $w = 3$ , then  $n = 93$  and  $y^{93} - 1 = (y^3 - 1)^{31} = (y + 30)(y + 26)(y + 6)$
- iv. Let  $w = 4$ , then  $n = 124$  and  $y^{124} - 1 = (y^4 - 1)^{31} = (y^2 - 1)(y^2 + 1) = (y + 30)^{31}(y + 1)^{31}(y^2 + 1)^{31}$   
Number of cyclic codes are,  $(31 + 1)^3 = 32^3 = 32,768$ .
- v. Let  $w = 5$ , then  $n = 155$  and  $y^{155} - 1 = (y^5 - 1)^{31} = ((y - 1)(y^4 + y^3 + y^2 + y + 1))^{31} = ((y + 30)(y + 29)(y + 27)(y + 15)(y + 23))^{31}$  Number of cyclic codes are,  $(31 + 1)^5 = 32^5 = 33,554,432$ .
- vi. Let  $w = 6$ , then  $n = 186$  and  $y^{186} - 1 = (y^6 - 1)^{31} = ((y^3 - 1)(y^3 + 1))^{31} = ((y + 30)(y + 26)(y + 6)(y + 1)(y + 5)(y + 25))^{31}$  Number of cyclic codes are,  $(31 + 1)^6 = 32^6 = 887,503,681$ .

- vii. Let  $w = 7$ , then  $n = 217$  and  $y^{217} - 1 = (y^7 - 1)^{31} = ((y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1))^{31}$  Number of cyclic codes are,  $(31 + 1)^2 = 32^2 = 1,024$ .
- viii. Let  $w = 8$ , then  $n = 248$  and  $y^{248} - 1 = (y^8 - 1)^{31} = ((y^4 - 1)(y^4 + 1))^{31} = ((y + 30)^{31}(y + 1)^{31}(y^2 + 1)^{31}(y^2 + 8y + 1)(y^2 + 23y + 1))^{31}$  Number of cyclic codes are,  $(31 + 1)^5 = 32^5 = 28,629,151$ .
- ix. Let  $w = 9$ , then  $n = 279$  and  $y^{279} - 1 = (y^9 - 1)^{31} = ((y + 30)(y + 26)(y + 6)(y^3 + 6)(y^3 + 26))^{31}$  Number of cyclic codes are,  $(31 + 1)^5 = 32^5 = 28,629,151$ .
- x. Let  $w = 10$ , then  $n = 310$  and  $y^{310} - 1 = (y^{10} - 1)^{31} = ((y^5 - 1)(y^5 + 1))^{31} = ((y + 30)(y + 29)(y + 27)(y + 15)(y + 23)(y + 1)(y + 2)(y + 4)(y + 8)(y + 16))^{31}$  Number of cyclic codes are,  $(31 + 1)^{10} = 32^{10} = 819,628,286,980,801$ .
- xi. Let  $w = 11$ , then  $n = 341$  and  $y^{341} - 1 = (y^{11} - 1)^{31} = ((y - 1)(y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1))^{31} = ((y + 30)(y^5 + 10y^4 + 30y^3 + y^2 + 9y + 30)(y^5 + 22y^4 + 30y^3 + y^2 + 21y + 30))^{31}$  Number of cyclic codes are,  $(31 + 1)^3 = 32^3 = 29,791$ .
- xii. Let  $w = 12$ , then  $n = 372$  and  $y^{372} = (y^{12} - 1)^{31} = ((y^6 - 1)(y^6 + 1))^{31} = ((y + 30)(y + 26)(y + 6)(y + 1)(y + 5)(y + 25)(y^2 + 1)(y^2 + 5)(y^2 + 25))^{31}$  Number of cyclic codes are,  $(31 + 1)^9 = 32^9 = 26,439,622,160,671$ .
- xiii. Let  $w = 13$ , then  $n = 403$  and  $y^{403} - 1 = (y^{13} - 1)^{31} = ((y + 30)(y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1))^{31}$  Number of cyclic codes are,  $(31 + 1)^4 = 32^4 = 923,521$ .
- xiv. Let  $w = 14$ , then  $n = 434$  and  $y^{434} - 1 = (y^{14} - 1)^{31} = ((y^7 - 1)(y^7 + 1))^{31} = ((y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y^7 + 1))^{31} = ((y + 30)(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)(y + 1)(y^6 + 30y^5 + y^4 + 30y^3 + y^2 + 30y + 1))^{31}$  Number of cyclic codes are,  $(31 + 1)^4 = 32^4 = 923,521$ .
- xv. Let  $w = 15$ , then  $n = 465$  and  $y^{465} - 1 = (y^{15} - 1)^{31} = ((y - 1)(y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1))^{31} = ((y + 30)(y + 26)(y + 6)(y + 3)(y + 21)(y + 29)(y + 23)(y + 27)(y + 17)(y + 11)(y + 24)(y + 22)(y + 12)(y + 13)(y + 15))^{31}$  Number of cyclic codes are,  $(31 + 1)^{15} = 32^{15} = 23,465,261,991,844,685,929,951$ .

The Table 2 gives summary of the number of cyclic code

**Table 2. The number of cyclic code for  $n = 31w$  over  $\mathbb{Z}_{31}$**

$w$	$n = 31w$	Number of Factors	Number of Cyclic code
1	31	1	$32^1 = 32$
2	62	2	$32^2 = 1,024$
3	93	3	$32^3 = 32,768$
4	124	3	$32^3 = 32,768$
5	155	5	$32^5 = 33,554,432$
6	186	6	$32^6 = 1,073,741,824$
7	217	2	$32^2 = 1,0244$
8	248	5	$32^5 = 33,554,432$
9	279	5	$32^5 = 33,554,432$
10	310	10	$32^{10} = 1,125,899,906,842,624$
11	341	3	$32^3 = 32,768$
12	372	9	$32^9 = 35,184,372,088,832$
13	403	4	$32^4 = 1,048,576$
14	434	4	$32^4 = 1,048,576$
15	465	15	$32^{15} = 32,768$

**Conjecture 2.2.** Suppose  $n = 31w, w \in \mathbb{Z}^+$  and  $y^n - 1$  factorizes into  $f$  linear factors then the number of cyclic code  $N$  over  $\mathbb{Z}_{31}$  is given by;  $N = 32^f$

### 2.3 Number of Cyclic Codes when $n = 31^w, 1 \leq w \leq 10$

- i. Let  $w = 1$ , then  $n = 31$  and  $y^{31} - 1 = (y - 1)^{31} = (y + 30)^{31}$ . Number of cyclic codes are,  $31^1 + 1 = 31 + 1 = 32$
- ii. Let  $w = 2$ , then  $n = 31^2$  and  $y^{31^2} - 1 = (y - 1)^{31^2} = (y + 30)^{31^2}$  Number of cyclic codes are,  $31^2 + 1 = 961 + 1 = 962$
- iii. Let  $w = 3$ , then  $n = 31^3$  and  $y^{31^3} - 1 = (y - 1)^{31^3} = (y + 30)^{31^3}$  Number of cyclic codes are,  $31^3 + 1 = 29,791 + 1 = 29,792$
- iv. Let  $w = 4$ , then  $n = 31^4$  and  $y^{31^4} - 1 = (y - 1)^{31^4} = (y + 30)^{31^4}$ . Number of cyclic codes are,  $31^4 + 1 = 923,521 + 1 = 923,522$
- v. Let  $w = 5$ , then  $n = 31^5$  and  $y^{31^5} - 1 = (y - 1)^{31^5} = (y + 30)^{31^5}$  Number of cyclic codes are,  $31^5 + 1 = 31 + 1 = 28,629,152$
- vi. Let  $w = 6$ , then  $n = 31^6$  and  $y^{31^6} - 1 = (y - 1)^{31^6} = (y + 30)^{31^6}$  Number of cyclic codes are,  $31^6 + 1 = 887,503,681 + 1 = 887,503,682$
- vii. Let  $w = 7$ , then  $n = 31^7$  and  $y^{31^7} - 1 = (y - 1)^{31^7} = (y + 30)^{31^7}$  Number of cyclic codes are,  $31^7 + 1 = 27,512,614,111 + 1 = 27,512,614,112$
- viii. Let  $w = 8$ , then  $n = 31^8$  and  $y^{31^8} - 1 = (y - 1)^{31^8} = (y + 30)^{31^8}$  Number of cyclic codes are,  $31^8 + 1 = 852,891,037,441 + 1 = 852,891,037,442$
- ix. Let  $w = 9$ , then  $n = 31^9$  and  $y^{31^9} - 1 = (y - 1)^{31^9} = (y + 30)^{31^9}$  Number of cyclic codes are,  $31^9 + 1 = 26,439,622,160,671 + 1 = 26,439,622,160,672$
- x. Let  $w = 10$ , then  $n = 31^{10}$  and  $y^{31^{10}} - 1 = (y - 1)^{31^{10}} = (y + 30)^{31^{10}}$  Number of cyclic codes are,  $31^{10} + 1 = 819,628,286,980,801 + 1 = 819,628,286,980,802$

The Table 3 gives summary of the number of cyclic code.

**Table 3.** The number of cyclic code for  $n = 31^w$  over  $\mathbb{Z}_{31}$

$w$	$n = 31^w$	Factors	Number of Cyclic code
1	$31^1$	$(y - 1)^{31^1}$	$31^1 + 1$
2	$31^2$	$(y - 1)^{31^2}$	$31^2 + 1$
3	$31^3$	$(y - 1)^{31^3}$	$31^3 + 1$
4	$31^4$	$(y - 1)^{31^4}$	$31^4 + 1$
5	$31^5$	$(y - 1)^{31^5}$	$31^5 + 1$
6	$31^6$	$(y - 1)^{31^6}$	$31^6 + 1$
7	$31^7$	$(y - 1)^{31^7}$	$31^7 + 1$
8	$31^8$	$(y - 1)^{31^8}$	$31^8 + 1$
9	$31^9$	$(y - 1)^{31^9}$	$31^9 + 1$
10	$31^{10}$	$(y - 1)^{31^{10}}$	$31^{10} + 1$



In general one can easily infer that for any positive  $w$  then,  $y^{31^w} - 1 = (y - 1)^{31^w} = (y + 30)^{31^w}$ . and the number of cyclic codes is given by  $31^w + 1$ .

**Conjecture 2.3.** Suppose  $n = 31^w, w \in \mathbb{Z}^+$  and  $y^n - 1$  factorizes into  $f$  linear factors such that  $y^n - 1 = (y - 1)^n = (y - 1)^{31^w}$  then the number of cyclic code  $N$  over  $\mathbb{Z}_{31}$  is given by  $N = 31^w + 1$

## 2.4 Number of cyclic codes when $n = q \cdot 31^r$ where $r = 0, 1, 2, 3, \dots$ , and $q$ is prime

- i. Let  $q = 2$  then  $n = 2(31)^r$  for  $r = 0, 1, 2, \dots$  and  $y^{2(31)^r} - 1 = (y^2 - 1)^{31^r} = (y + 30)^{31^r}(y + 1)^{31^r}$   
 when  $r = 0, (y^2 - 1)^{31^0} = y^2 - 1 = (y + 30)(y + 1)$ . The number of factors  $f$  equals  $(31^0 + 1) = 2$  and the number cyclic codes =  $f^2 = 4$   
 When  $r = 1, (y^2 - 1)^{31^1} = (y^2 - 1)^{31} = ((y + 30)(y + 1))^{31} = (y + 30)^{31}(y + 1)^{31}$ , number of factors  $f$  equals  $31^1 + 1 = 32$  number of cyclic codes =  $(31 + 1)^2 = 1024$   
 when  $r = 2, y^n - 1 = (y + 30)^{31^2}(y + 1)^{31^2}$ , number of factors  $f$  equals  $31^2 + 1 = 62$  number of cyclic codes =  $(31^2 + 1)^2 = 925, 444$   
 In general,  $y^{2(31^r)} - 1 = [(y - 1)^{31^r}]^2$ . number of factors  $f$  equals =  $31^r + 1$  and number of cyclic codes =  $(31^r + 1)^2$
- ii. Let  $q = 3$  then  $n = 3(31)^r$  for  $r = 0, 1, 2, \dots$  and  $y^n - 1 = y^{3(31^r)} - 1 = (y^3 - 1)^{31^r} = (y + 30)^{31^r}(y + 26)^{31^r}(y + 6)^{31^r}$   
 When  $r = 0, y^n - 1 = (y + 30)^{31^0}(y + 26)^{31^0}(y + 6)^{31^0}$ . Number of cyclic codes =  $(31^0 + 1)^3 = 8$ .  
 When  $r = 1, y^n - 1 = (y + 30)^{31^1}(y + 26)^{31^1}(y + 6)^{31^1}$  Number of cyclic codes =  $(31^1 + 1)^3 = 32, 768$ .  
 When  $r = 2, y^n - 1 = (y + 30)^{31^2}(y + 26)^{31^2}(y + 6)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^3$ . In general, number of cyclic codes =  $(31^r + 1)^3$ .
- iii. Let  $q = 5$  then  $n = 5(31)^r, r = 0, 1, 2, \dots$  and  $y^n - 1 = y^{5(31^r)} - 1 = (y^5 - 1)^{31^r} = (y + 30)^{31^r}(y + 29)^{31^r}(y + 27)^{31^r}(y + 15)^{31^r}(y + 23)^{31^r}$   
 When  $r = 0, y^n - 1 = (y + 30)(y + 29)(y + 27)(y + 15)(y + 23)$ . Number of cyclic codes =  $(31^0 + 1)^5 = 32$ .  
 When  $r = 1, y^n - 1 = (y + 30)^{31}(y + 29)^{31}(y + 27)^{31}(y + 15)^{31}(y + 23)^{31}$ . Number of cyclic codes =  $(31^1 + 1)^5$   
 When  $r = 2, y^n - 1 = (y + 30)^{31^2}(y + 29)^{31^2}(y + 27)^{31^2}(y + 15)^{31^2}(y + 23)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^5$ .  
 In general, number of cyclic codes =  $(31^r + 1)^5$ .
- iv. Let  $q = 7$  then  $n = 7(31)^r, r = 0, 1, 2, \dots$  and  $y^n - 1 = y^{7(31^r)} - 1 = (y^7 - 1)^{31^r} = (y + 30)^{31^r}(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)^{31^r}$ .  
 When  $r = 0, y^n - 1 = (y + 30)^{31^0}(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)^{31^0}$ . Number of cyclic codes =  $(31^0 + 1)^2$   
 When  $r = 1, y^n - 1 = (y + 30)^{31^1}(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)^{31^1}$  Number of cyclic codes =  $(31^1 + 1)^2$ .  
 When  $r = 2, y^n - 1 = (y + 30)^{31^2}(y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)^{31^2}$  Number of cyclic codes =  $(31^2 + 1)^2$ . In general, number of cyclic codes =  $(31^r + 1)^2$ .
- v. Let  $q = 11$  then  $n = 11(31)^r, r = 0, 1, 2, \dots$  and  $y^n - 1 = y^{11(31^r)} - 1 = (y^{11} - 1)^{31^r} = (y + 30)^{31^r}(y^5 + 10y^4 + 30y^3 + y^2 + 9y + 30)^{31^r}(y^5 + 22y^4 + 30y^3 + y^2 + 21y + 30)^{31^r}$ .  
 When  $r = 0, y^n - 1 = (y + 30)^{31^0}(y^5 + 10y^4 + 30y^3 + y^2 + 9y + 30)^{31^0}(y^5 + 22y^4 + 30y^3 + y^2 + 21y + 30)^{31^0}$   
 Number of cyclic codes =  $(31^0 + 1)^3$ .  
 When  $r = 1, y^n - 1 = (y + 30)^{31^1}(y^5 + 10y^4 + 30y^3 + y^2 + 9y + 30)^{31^1}(y^5 + 22y^4 + 30y^3 + y^2 + 21y + 30)^{31^1}$   
 Number of cyclic codes =  $(31^1 + 1)^3$ .  
 When  $r = 2, y^n - 1 = (y + 30)^{31^2}(y^5 + 10y^4 + 30y^3 + y^2 + 9y + 30)^{31^2}(y^5 + 22y^4 + 30y^3 + y^2 + 21y + 30)^{31^2}$   
 Number of cyclic codes =  $(31^2 + 1)^3$ .
- vi. Let  $q = 13$  then  $n = 13(31)^r, r = 0, 1, 2, \dots$  and  $y^n - 1 = y^{13(31^r)} - 1 = (y^{13} - 1)^{31^r} = (y + 30)^{31^r}(y^4 + 4y^3 + 11y^2 + 4y + 1)^{31^r}(y^4 + 6y^3 + 29y^2 + 6y + 1)^{31^r}(y^4 + 22y^3 + 28y^2 + 22y + 1)^{31^r}$

- When  $r = 0$ ,  $y^n - 1 = (y + 30)^{31^0} (y^4 + 4y^3 + 11y^2 + 4y + 1)^{31^0} (y^4 + 6y^3 + 29y^2 + 6y + 1)^{31^0} (y^4 + 22y^3 + 28y^2 + 22y + 1)^{31^0}$ . Number of cyclic codes =  $(31^0 + 1)^4$ .
- When  $r = 1$ ,  $y^n - 1 = (y + 30)^{31^1} (y^4 + 4y^3 + 11y^2 + 4y + 1)^{31^1} (y^4 + 6y^3 + 29y^2 + 6y + 1)^{31^1} (y^4 + 22y^3 + 28y^2 + 22y + 1)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^4$ .
- When  $r = 2$ ,  $y^n - 1 = (y + 30)^{31^2} (y^4 + 4y^3 + 11y^2 + 4y + 1)^{31^2} (y^4 + 6y^3 + 29y^2 + 6y + 1)^{31^2} (y^4 + 22y^3 + 28y^2 + 22y + 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^4$ .
- vii. Let  $q = 17$  then  $n = 17(31)^r, r = 0, 1, 2, \dots$  and  $y^n - 1 = y^{17(31)^r} - 1 = (y^{17} - 1)^{31^r} = (y + 30)^{31^r} (y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)^{31^r}$ .
- When  $r = 0$ ,  $y^n - 1 = (y + 30)^{31^0} (y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)^{31^0}$ . Number of cyclic codes =  $(31^0 + 1)^2$ .
- When  $r = 1$ ,  $y^n - 1 = (y + 30)^{31^1} (y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^2$ . When  $r = 2$ ,  $y^n - 1 = (y + 30)^{31^2} (y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^2$ .
- viii. Let  $q = 19$  then  $n = 19(31)^r, r = 0, 1, 2, \dots$  and  $y^n - 1 = y^{19(31)^r} - 1 = (y^{19} - 1)^{31^r} = (y + 30)^{31^r} (y^6 + 4y^5 + 14y^4 + 18y^3 + 14y^2 + 4y + 1)^{31^r} (y^6 + 5y^5 + 25y^4 + y^3 + 5y^2 + 25y + 1)^{31^r} (y^6 + 25y^5 + 5y^4 + y^3 + 25y^3 + 5y + 1)^{31^r}$ .
- when  $r = 0$ ,  $y^n - 1 = (y + 30)^{31^0} (y^6 + 4y^5 + 14y^4 + 18y^3 + 14y^2 + 4y + 1)^{31^0} (y^6 + 5y^5 + 25y^4 + y^3 + 5y^2 + 25y + 1)^{31^0} (y^6 + 25y^5 + 5y^4 + y^3 + 25y^3 + 5y + 1)^{31^0}$ . Number of cyclic codes =  $(31^0 + 1)^4$ .
- When  $r = 1$ ,  $y^n - 1 = (y + 30)^{31^1} (y^6 + 4y^5 + 14y^4 + 18y^3 + 14y^2 + 4y + 1)^{31^1} (y^6 + 5y^5 + 25y^4 + y^3 + 5y^2 + 25y + 1)^{31^1} (y^6 + 25y^5 + 5y^4 + y^3 + 25y^3 + 5y + 1)^{31^1}$ . Number of cyclic codes =  $(31^0 + 1)^4$ .
- When  $r = 2$ ,  $y^n - 1 = (y + 30)^{31^2} (y^6 + 4y^5 + 14y^4 + 18y^3 + 14y^2 + 4y + 1)^{31^2} (y^6 + 5y^5 + 25y^4 + y^3 + 5y^2 + 25y + 1)^{31^2} (y^6 + 25y^5 + 5y^4 + y^3 + 25y^3 + 5y + 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^4$ .
- ix. Let  $q = 23$  then  $n = 23(31)^r, r = 0, 1, 2, \dots$  and  $y^n - 1 = y^{23(31)^r} - 1 = (y^{23} - 1)^{31^r} = (y + 30)^{31^r} (y^{11} + 8y^{10} + 5y^9 + 27y^8 + 20y^7 + 14y^6 + 18y^5 + 27y^4 + 4y^3 + 10y^2 + 7y + 30)^{31^r} (y^{11} + 24y^{10} + 21y^9 + 27y^8 + 4y^7 + 13y^6 + 17y^5 + 11y^4 + 4y^3 + 26y^2 + 23y + 30)^{31^r}$ .
- When  $r = 0$ ,  $y^n - 1 = (y + 30)^{31^0} (y^{11} + 8y^{10} + 5y^9 + 27y^8 + 20y^7 + 14y^6 + 18y^5 + 27y^4 + 4y^3 + 10y^2 + 7y + 30)^{31^0} (y^{11} + 24y^{10} + 21y^9 + 27y^8 + 4y^7 + 13y^6 + 17y^5 + 11y^4 + 4y^3 + 26y^2 + 23y + 30)^{31^0}$ . Number of cyclic codes =  $(31^0 + 1)^3$ .
- When  $r = 1$ ,  $y^n - 1 = (y + 30)^{31^1} (y^{11} + 8y^{10} + 5y^9 + 27y^8 + 20y^7 + 14y^6 + 18y^5 + 27y^4 + 4y^3 + 10y^2 + 7y + 30)^{31^1} (y^{11} + 24y^{10} + 21y^9 + 27y^8 + 4y^7 + 13y^6 + 17y^5 + 11y^4 + 4y^3 + 26y^2 + 23y + 30)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^3$ .
- When  $r = 2$ ,  $y^n - 1 = (y + 30)^{31^2} (y^{11} + 8y^{10} + 5y^9 + 27y^8 + 20y^7 + 14y^6 + 18y^5 + 27y^4 + 4y^3 + 10y^2 + 7y + 30)^{31^2} (y^{11} + 24y^{10} + 21y^9 + 27y^8 + 4y^7 + 13y^6 + 17y^5 + 11y^4 + 4y^3 + 26y^2 + 23y + 30)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^3$ .
- x. Let  $q = 29$  then  $n = 29(31)^r, r = 0, 1, 2, \dots$  and  $y^n - 1 = y^{29(31)^r} - 1 = (y^{29} - 1)^{31^r} = (y + 30)^{31^r} (y^{28} + y^{27} + y^{26} + y^{25} + y^{24} + y^{23} + y^{22} + y^{21} + y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1)^{31^r}$ .
- When  $r = 0$ ,  $(y^{29} - 1) = ((y + 30)(y^{28} + y^{27} + y^{26} + y^{25} + y^{24} + y^{23} + y^{22} + y^{21} + y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1))$ . Number of cyclic codes  $(31^0 + 1)^2$ .
- When  $r = 1$ ,  $(y^{29} - 1)^{31} = ((y + 30)(y^{28} + y^{27} + y^{26} + y^{25} + y^{24} + y^{23} + y^{22} + y^{21} + y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1))^{31}$ . Number of cyclic

codes  $(31^1 + 1)^2$  When  $r = 2$ ,  $(y^{29} - 1)^{31^2} = ((y + 30)(y^{28} + y^{27} + y^{26} + y^{25} + y^{24} + y^{23} + y^{22} + y^{21} + y^{20} + y^{19} + y^{18} + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + y^2 + y + 1))^{31^2}$   
 Number of cyclic codes  $(31^2 + 1)^2$

The Table 4 gives summary of the number of cyclic code.

**Table 4. The number of cyclic code for  $n = q.31^r$  over  $\mathbb{Z}_{31}$**

$q$	$n = q.31^r$	Factors	number of factors in $y^q - 1$	Number of Cyclic code
2	$2.31^r$	$(y^2 - 1)^{31^r}$	2	$(31^r + 1)^2$
3	$3.31^r$	$(y^3 - 1)^{31^r}$	3	$(31^r + 1)^3$
5	$5.31^r$	$(y^5 - 1)^{31^r}$	5	$(31^r + 1)^5$
7	$7.31^r$	$(y^7 - 1)^{31^r}$	2	$(31^r + 1)^2$
11	$11.31^r$	$(y^{11} - 1)^{31^r}$	3	$(31^r + 1)^3$
13	$13.31^r$	$(y^{13} - 1)^{31^r}$	4	$(31^r + 1)^4$
17	$17.31^r$	$(y^{17} - 1)^{31^r}$	2	$(31^r + 1)^2$
19	$19.31^r$	$(y^{19} - 1)^{31^r}$	4	$(31^r + 1)^4$
23	$23.31^r$	$(y^{23} - 1)^{31^r}$	3	$(31^r + 1)^3$
29	$29.31^r$	$(y^{29} - 1)^{31^r}$	2	$(31^r + 1)^2$

**Conjecture 2.4.** Suppose  $n = q.31^r, r = 0, 1, 2, \dots, q$  prime and  $y^n - 1 = (y - 1)^n = (y - 1)^{q.31^r}$  factorizes into  $31^r + 1$  linear factors then the number of cyclic code  $N$  over  $\mathbb{Z}_{31}$  is given by  $N = (31^r + 1)^q$

### 2.5 Number of cyclic codes when $n = q^r.31^r$ where $r = 1, 2, 3, \dots$ , and $q$ is prime

- i. Let  $q = 2$  then,  $n = 2^r(31)^r$  for  $r = 1, 2, \dots$  and  $y^{2^r(31)^r} - 1 = (y^{2^r} - 1)^{31^r}$ .  
 When  $r = 1$ ,  $(y^{2^1} - 1)^{31^1} = (y^2 - 1)^{31} = ((y + 30)(y + 1))^{31} = (y + 30)^{31}(y + 1)^{31}$ ,  
 then the number of cyclic codes  $= (31 + 1)^2 = 1024$ .  
 When  $r = 2$ ,  $y^n - 1 = (y^{2^2} - 1)^{31^2}$ , then the number of cyclic codes  $= (31^2 + 1)^{2^2}$ .  
 In general, number of cyclic codes  $= (31^r + 1)^{2^r}$ .
- ii. Let  $q = 3$  then  $n = 3^r(31)^r$  for  $r = 1, 2, \dots$  and  $y^n - 1 = y^{3^r(31)^r} - 1 = (y^{3^r} - 1)^{31^r}$ .  
 When  $r = 1$ ,  $y^n - 1 = y^{3^1(31^1)} - 1 = (y^{3^1} - 1)^{31^1}$ ,  
 then the number of cyclic codes  $= (31^1 + 1)^{3^1} = 32,768$ .  
 When  $r = 2$ ,  $y^n - 1 = (y^{3^2} - 1)^{31^2}$ , then the number of cyclic codes  $= (31^2 + 1)^{3^2}$ .  
 In general, number of cyclic codes  $= (31^r + 1)^{3^r}$ .
- iii. Let  $q = 5$  then  $n = 5^r(31)^r, r = 1, 2, \dots$  and  $y^n - 1 = y^{5^r(31)^r} - 1 = (y^{5^r} - 1)^{31^r}$ .  
 When  $r = 1$ ,  $y^n - 1 = (y^{5^1} - 1)^{31^1}$ , then the number of cyclic codes  $= (31^1 + 1)^{5^1}$ .  
 When  $r = 2$ ,  $y^n - 1 = (y^{5^2} - 1)^{31^2}$ , then the number of cyclic codes  $= (31^2 + 1)^{5^2}$ .  
 In general, number of cyclic codes  $= (31^r + 1)^{5^r}$ .
- iv. Let  $q = 7$  then  $n = 7^r(31)^r, r = 1, 2, \dots$  and  $y^n - 1 = y^{7^r(31)^r} - 1 = (y^{7^r} - 1)^{31^r}$ .  
 When  $r = 1$ ,  $y^n - 1 = (y^{7^1} - 1)^{31^1}$ , then the number of cyclic codes  $= (31^1 + 1)^{7^1}$ .  
 When  $r = 2$ ,  $y^n - 1 = (y^{7^2} - 1)^{31^2}$ , then the number of cyclic codes  $= (31^2 + 1)^{7^2}$ .  
 In general, number of cyclic codes  $= (31^r + 1)^{7^r}$ .
- v. Let  $q = 11$  then  $n = 11^r(31)^r, r = 1, 2, \dots$  and  $y^n - 1 = y^{11^r(31)^r} - 1 = (y^{11^r} - 1)^{31^r}$ .  
 When  $r = 1$ ,  $y^n - 1 = (y^{11^1} - 1)^{31^1}$ , then the number of cyclic codes  $= (31^1 + 1)^{11^1}$ .  
 When  $r = 2$ ,  $y^n - 1 = (y^{11^2} - 1)^{31^2}$ , then the number of cyclic codes  $= (31^2 + 1)^{11^2}$ .  
 In general, number of cyclic codes  $= (31^r + 1)^{11^r}$ .

- vi. Let  $q = 13$  then  $n = 13^r(31)^r, r = 1, 2, \dots$  and  $y^n - 1 = y^{13^r(31)^r} - 1 = (y^{13^r} - 1)^{31^r}$ .  
 When  $r = 1, y^n - 1 = (y^{13^1} - 1)^{31^1}$ , then the number of cyclic codes  $= (31^1 + 1)^{4^1}$ .  
 When  $r = 2, y^n - 1 = (y^{13^2} - 1)^{31^2}$ , then the number of cyclic codes  $= (31^2 + 1)^{4^2}$ .  
 In general, number of cyclic codes  $= (31^r + 1)^{4^r}$ .
- vii. Let  $q = 17$  then  $n = 17^r(31)^r, r = 1, 2, \dots$  and  $y^n - 1 = y^{17^r(31)^r} - 1 = (y^{17^r} - 1)^{31^r}$ .  
 When  $r = 1, y^n - 1 = (y^{17^1} - 1)^{31^1}$ , then the number of cyclic codes  $= (31^1 + 1)^{2^1}$ .  
 When  $r = 2, y^n - 1 = (y^{17^2} - 1)^{31^2}$ , then the number of cyclic codes  $= (31^2 + 1)^{2^2}$ .  
 In general, number of cyclic codes  $= (31^r + 1)^{2^r}$ .
- viii. Let  $q = 19$  then  $n = 19^r(31)^r, r = 1, 2, \dots$  and  $y^n - 1 = y^{19^r(31)^r} - 1 = (y^{19^r} - 1)^{31^r}$ .  
 When  $r = 1, y^n - 1 = (y^{19^1} - 1)^{31^1}$ . then the number of cyclic codes  $= (31^1 + 1)^{4^1}$ .  
 When  $r = 2, y^n - 1 = (y^{19^2} - 1)^{31^2}$ . then the number of cyclic codes  $= (31^2 + 1)^{4^2}$ .  
 In general, number of cyclic codes  $= (31^r + 1)^{4^r}$ .
- ix. Let  $q = 23$  then  $n = 23^r(31)^r, r = 1, 2, \dots$  and  $y^n - 1 = y^{23^r(31)^r} - 1 = (y^{23^r} - 1)^{31^r}$ .  
 When  $r = 1, y^n - 1 = (y^{23^1} - 1)^{31^1}$ , then the number of cyclic codes  $= (31^1 + 1)^{3^1}$ .  
 When  $r = 2, y^n - 1 = (y^{23^2} - 1)^{31^2}$ , then the number of cyclic codes  $= (31^2 + 1)^{3^2}$ .  
 In general, number of cyclic codes  $= (31^r + 1)^{3^r}$ .
- x. Let  $q = 29$  then  $n = 29^r(31)^r, r = 1, 2, \dots$  and  $y^n - 1 = y^{29^r(31)^r} - 1 = (y^{29^r} - 1)^{31^r}$ .  
 When  $r = 1, y^n - 1 = (y^{29^1} - 1)^{31^1}$ , then the number of cyclic codes  $= (31^1 + 1)^{2^1}$ .  
 When  $r = 2, y^n - 1 = (y^{29^2} - 1)^{31^2}$ . then the number of cyclic codes  $= (31^2 + 1)^{2^2}$ ,  
 In general, number of cyclic codes  $= (31^r + 1)^{2^r}$ .

The Table 5 gives summary of the number of cyclic code.

**Table 5. The number of cyclic code for  $n = q^r \cdot 31^r$  over  $\mathbb{Z}_{31}$**

$q$	$n = q^r \cdot 31^r$	Factors	number of factors in $y^q - 1$	Number of Cyclic code
2	$2^r \cdot 31^r$	$(y^{2^r} - 1)^{31^r}$	2	$(31^r + 1)^{2^r}$
3	$3^r \cdot 31^r$	$(y^{3^r} - 1)^{31^r}$	3	$(31^r + 1)^{3^r}$
5	$5^r \cdot 31^r$	$(y^{5^r} - 1)^{31^r}$	5	$(31^r + 1)^{5^r}$
7	$7^r \cdot 31^r$	$(y^{7^r} - 1)^{31^r}$	2	$(31^r + 1)^{2^r}$
11	$11^r \cdot 31^r$	$(y^{11^r} - 1)^{31^r}$	3	$(31^r + 1)^{3^r}$
13	$13^r \cdot 31^r$	$(y^{13^r} - 1)^{31^r}$	4	$(31^r + 1)^{4^r}$
17	$17^r \cdot 31^r$	$(y^{17^r} - 1)^{31^r}$	2	$(31^r + 1)^{2^r}$
19	$19^r \cdot 31^r$	$(y^{19^r} - 1)^{31^r}$	4	$(31^r + 1)^{4^r}$
23	$23^r \cdot 31^r$	$(y^{23^r} - 1)^{31^r}$	3	$(31^r + 1)^{3^r}$
29	$29^r \cdot 31^r$	$(y^{29^r} - 1)^{31^r}$	2	$(31^r + 1)^{2^r}$

**Conjecture 2.5.** Suppose  $n = q^r \cdot 31^r, r = 1, 2, \dots, q$  prime and  $y^n - 1 = (y - 1)^n = (y - 1)^{q^r \cdot 31^r}$  is such that the number of factors in  $y^q - 1$  is  $f$  then the number of cyclic code  $N$  over  $\mathbb{Z}_{31}$  is given by  $N = (31^r + 1)^{f^r}$

## 2.6 Number of cyclic codes when $n = q^k \cdot 31^r$ where $r = 1, 2, 3, \dots$ , and $k = 1, 2, \dots$ $q$ is prime

- i. Let  $q = 2$  the  $n = 2^k(31)^r$  for  $r = 1, 2, \dots$  and  $y^{2^k(31)^r} - 1 = (y^{2^k} - 1)^{31^r}$ .  
 Let  $k = 1$  be fixed then  $y^n - 1 = y^{2^1(31)^r} - 1 = y^{2(31)^r} - 1$ . When  $r = 1, (y^2 - 1)^{31^1} = (y^2 - 1)^{31} = ((y + 30)(y + 1))^{31} = (y + 30)^{31}(y + 1)^{31}$ . Number of cyclic codes  $= (31 + 1)^2 = 1024$ . When  $r = 2,$

- $y^n - 1 = (y^2 - 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^2$ . In general,  $y^{2^r(31^r)} - 1 = [(y - 1)^{31^r}]^2$  and Number of cyclic codes =  $(31^r + 1)^2$
- ii. Let  $q = 3$  then  $n = 3^k(31)^r$  for  $r = 1, 2, \dots$  and  $y^n - 1 = y^{3^r(31^r)} - 1 = (y^{3^k} - 1)^{31^r}$ .  
Let  $k = 1$  be fixed then  $y^n - 1 = y^{3^1(31)^r} - 1 = y^{3(31)^r} - 1$ . When  $r = 1$ ,  $y^n - 1 = y^{3(31^1)} - 1 = (y^3 - 1)^{31^1}$ .  
Number of cyclic codes =  $(31^1 + 1)^3 = 32,768$ . When  $r = 2$ ,  $y^n - 1 = (y^3 - 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^3$ . In general, number of cyclic codes =  $(31^r + 1)^3$
- iii. Let  $q = 5$  then  $n = 5^r(31)^r$ ,  $r = 1, 2, \dots$  and  $y^n - 1 = y^{5^k(31)^r} - 1 = (y^{5^k} - 1)^{31^r}$ .  
Let  $k = 1$  be fixed then  $y^n - 1 = y^{5^1(31)^r} - 1 = y^{5(31)^r} - 1$ . When  $r = 1$ ,  $y^n - 1 = (y^5 - 1)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^5$ . When  $r = 2$ ,  $y^n - 1 = (y^5 - 1)^{31^2}$ . number of cyclic codes =  $(31^2 + 1)^5$ . In general, number of cyclic codes =  $(31^r + 1)^5$ .
- iv. Let  $q = 7$  then  $n = 7^k(31)^r$ ,  $r = 1, 2, \dots$  and  $y^n - 1 = y^{7^k(31)^r} - 1 = (y^{7^k} - 1)^{31^r}$ .  
Let  $k = 1$  be fixed then  $y^n - 1 = y^{7^1(31)^r} - 1 = y^{7(31)^r} - 1$ . When  $r = 1$ ,  $y^n - 1 = (y^7 - 1)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^2$ . When  $r = 2$ ,  $y^n - 1 = (y^7 - 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^2$ . In general, number of cyclic codes =  $(31^r + 1)^2$ .
- v. Let  $q = 11$  then  $n = 11^k(31)^r$ ,  $r = 1, 2, \dots$  and  $y^n - 1 = y^{11^k(31)^r} - 1 = (y^{11^k} - 1)^{31^r}$ .  
Let  $k = 1$  be fixed then  $y^n - 1 = y^{11^1(31)^r} - 1 = y^{11(31)^r} - 1$ . When  $r = 1$ ,  $y^n - 1 = (y^{11} - 1)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^3$ . When  $r = 2$ ,  $y^n - 1 = (y^{11} - 1)^{31^2}$ . Number of cyclic codes =  $(31 + 1)^{3^2}$ . In general, number of cyclic codes =  $(31^r + 1)^{3^r}$ .
- vi. Let  $q = 13$  then  $n = 13^k(31)^r$ ,  $r = 1, 2, \dots$  and  $y^n - 1 = y^{13^k(31)^r} - 1 = (y^{13^k} - 1)^{31^r}$ .  
Let  $k = 1$  be fixed then  $y^n - 1 = y^{13^1(31)^r} - 1 = y^{13(31)^r} - 1$ . When  $r = 1$ ,  $y^n - 1 = (y^{13} - 1)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^4$ . When  $r = 2$ ,  $y^n - 1 = (y^{13} - 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^4$ . In general, number of cyclic codes =  $(31^r + 1)^4$
- vii. Let  $q = 17$  then  $n = 17^k(31)^r$ ,  $r = 1, 2, \dots$  and  $y^n - 1 = y^{17^k(31)^r} - 1 = (y^{17^k} - 1)^{31^r}$ .  
Let  $k = 1$  be fixed then  $y^n - 1 = y^{17^1(31)^r} - 1 = y^{17(31)^r} - 1$ . When  $r = 1$ ,  $y^n - 1 = (y^{17} - 1)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^2$ . When  $r = 2$ ,  $y^n - 1 = (y^{17} - 1)^{31^2}$  Number of cyclic codes =  $(31^2 + 1)^2$ . In general, number of cyclic codes =  $(31^r + 1)^2$
- viii. Let  $q = 19$  then  $n = 19^k(31)^r$ ,  $r = 1, 2, \dots$  and  $y^n - 1 = y^{19^k(31)^r} - 1 = (y^{19^k} - 1)^{31^r}$ .  
Let  $k = 1$  be fixed then  $y^n - 1 = y^{19^1(31)^r} - 1 = y^{19(31)^r} - 1$ . When  $r = 1$ ,  $y^n - 1 = (y^{19} - 1)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^4$ . When  $r = 2$ ,  $y^n - 1 = (y^{19} - 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^4$ . In general, number of cyclic codes =  $(31^r + 1)^4$
- ix. Let  $q = 23$  then  $n = 23^k(31)^r$ ,  $r = 1, 2, \dots$  and  $y^n - 1 = y^{23^k(31)^r} - 1 = (y^{23^k} - 1)^{31^r}$ .  
Let  $k = 1$  be fixed then  $y^n - 1 = y^{23^1(31)^r} - 1 = y^{23(31)^r} - 1$   
When  $r = 1$ ,  $y^n - 1 = (y^{23} - 1)^{31^1}$ . Number of cyclic codes =  $(31^1 + 1)^3$ . When  $r = 2$ ,  $y^n - 1 = (y^{23} - 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^3$ . In general, number of cyclic codes =  $(31^r + 1)^3$ .
- x. Let  $q = 29$  then  $n = 29^r(31)^r$ ,  $r = 1, 2, \dots$  and  $y^n - 1 = y^{29^k(31)^r} - 1 = (y^{29^k} - 1)^{31^r}$ .  
Let  $k = 1$  be fixed then  $y^n - 1 = y^{29^1(31)^r} - 1 = y^{29(31)^r} - 1$ . When  $r = 1$ ,  $y^n - 1 = (y^{29} - 1)^{31^1}$ . Number of cyclic codes =  $(31 + 1)^2$ . When  $r = 2$ ,  $y^n - 1 = (y^{29} - 1)^{31^2}$ . Number of cyclic codes =  $(31^2 + 1)^2$ . In general, number of cyclic codes =  $(31^r + 1)^2$ .

The Table 6 gives summary of the number of cyclic code.

**Conjecture 2.6.** Suppose  $n = q^k \cdot 31^r$ ,  $r, k \in \mathbb{Z}^+$ ,  $q$  prime and  $y^n - 1 = (y - 1)^n = (y - 1)^{q^k \cdot 31^r}$  is such that the number of factors in  $y^q - 1$  is  $f$  then for a fixed  $k$  the number of cyclic code  $N$  over  $\mathbb{Z}_{31}$  is given by  $N = (31^r + 1)^{f^k}$

**Table 6. The number of cyclic code for  $n = q^k \cdot 31^r$  over  $\mathbb{Z}_{31}$**

$q$	$n = q^k \cdot 31^r$	Factors	number of factors in $y^q - 1$	Number of Cyclic code
2	$2^k \cdot 31^r$	$(y^{2^k} - 1)^{31^r}$	2	$(31^r + 1)^{2^k}$
3	$3^k \cdot 31^r$	$(y^{3^k} - 1)^{31^r}$	3	$(31^r + 1)^{3^k}$
5	$5^k \cdot 31^r$	$(y^{5^k} - 1)^{31^r}$	5	$(31^r + 1)^{5^k}$
7	$7^k \cdot 31^r$	$(y^{7^k} - 1)^{31^r}$	2	$(31^r + 1)^{2^k}$
11	$11^k \cdot 31^r$	$(y^{11^k} - 1)^{31^r}$	3	$(31^r + 1)^{3^k}$
13	$13^k \cdot 31^r$	$(y^{13^k} - 1)^{31^r}$	4	$(31^r + 1)^{4^k}$
17	$17^k \cdot 31^r$	$(y^{17^k} - 1)^{31^r}$	2	$(31^r + 1)^{2^k}$
19	$19^k \cdot 31^r$	$(y^{19^k} - 1)^{31^r}$	4	$(31^r + 1)^{4^k}$
23	$23^k \cdot 31^r$	$(y^{23^k} - 1)^{31^r}$	3	$(31^r + 1)^{3^k}$
29	$29^k \cdot 31^r$	$(y^{29^k} - 1)^{31^r}$	2	$(31^r + 1)^{2^k}$

### 3 Conclusion

In this study, we partitioned cyclotomic polynomial  $y^n - 1$  using cyclotomic cosets  $31 \pmod n$  and factorize  $y^n - 1$  using case to case basis. We then investigated the number of cyclic codes for each case. The following conclusions were made.

1. The number of cyclotomic cosets equals to the number of irreducible monic factors in  $y^n - 1$
2. Let  $h$  be the number of cyclotomic cosets, then the number of cyclic codes equal to  $2^h$
3. Let  $\mathbb{Z}_{31}$  be a given finite field,  $y^n - 1$  be cyclotomic polynomial and  $f$  be the number of irreducible factors in  $y^n - 1$ . Then the number of cyclic codes  $N$  over  $\mathbb{Z}_{31}$  is given by;

$$N = \begin{cases} (31 + 1)^f & : n = 31w, w \in \mathbb{Z}^+ \\ 31^w + 1 & : n = 31^w, w \in \mathbb{Z}^+ \\ (31^r + 1)^f & : n = q \cdot 31^r, r = 0, 1, 2, \dots, q \text{ is prime} \\ (31^r + 1)^{f^r} & : n = q^r \cdot 31^r, r \in \mathbb{Z}^+ \\ (31^r + 1)^{f^k} & : n = q^k \cdot 31^r, k, r \in \mathbb{Z}^+ \end{cases}$$

### Disclaimer (Artificial Intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of manuscripts.

### Competing Interests

Authors have declared that no competing interests exist.

### References

- [1] Pretzel O. Error correcting codes and finite fields. Oxford: Clarendon Press. [10] Roth, R. 2006). Introduction to Coding Theory. New York, USA: Cambridge University Press; 1992.
- [2] Richa G, Bhudev S. Generation of variable length error correcting codes over using constant length error correcting codes. International journal of emerging trends in engineering and development. 2012;1(2):269-279.

- [3] Kandhway K. Modeling burst errors in a fading channel. In 2022 IEEE 11th International Conference on Communication System and Network Technologies (CSNT) IEEE. 2022, April;409-414.
- [4] Maganga NJ, Kivunge BM. Enumeration of cyclic codes over GF(19). International Journal of Science and Research. 2017;6(4). ISSN: 2319-7064
- [5] Koopman P. Software and digital systems program, data integrity techniques (Contract DTFACT-11-C-00005) Brendan Hall Honeywell Laboratories; 2014.
- [6] Mesnager S. Linear codes from functions. In Concise Encyclopedia of Coding Theory. Chapman and Hall/CRC; 2021;463-526.
- [7] Oleg F. On the generators of codes of ideals of the polynomial ring for error control; 2017.
- [8] Adams SS. Introduction to Coding Theory, (3rd ed.), Cornell University Press, Berlin; 2008.
- [9] Berlekamp E. Algebraic Coding Theory. New York, USA: McGraw-Hill Book company; 1968.
- [10] Bierbrauer J. Introduction to Coding Theory. Chapman & Hall/CRC; 2004.
- [11] Blake IF. Codes over certain rings. Information and Control. 1972;20(4):396-404.
- [12] Hill R. A first course in coding theory. Oxford: Clarendon Press; 1986.
- [13] Arnold A, Monagan M. Calculating cyclotomic polynomials. Mathematics of Computation. 2011;80(276):2359-2379.
- [14] Bamunoba A. Cyclotomic Polynomials. London: Oxford; 2011.
- [15] Ranjeet S. Cyclotomic Cosets in the Ring  $\mathbb{R}_{2p^m q} = \frac{\text{GF}(l)[y]}{y^{2p^m q} - 1}$ ,  $1 \leq n$ . International Journal of Mathematics Trends and Technology. April 2022;68(4):84-86. ISSN: 2231 - 5373.
- [16] Jia Y, Ling S, Xing C. On self dual cyclic codes over finite fields. IEEE Transactions on Information Theory. 2011;57(4):2243-2251.
- [17] Lao H, Kivunge B, Muthoka G, Mwangi P. On the number of cyclotomic cosets and cyclic codes over  $\mathbb{Z}_{13}$ . International Journal of Scientific Research and Innovative Technology. 2018;5(6). ISSN: 2313-3759
- [18] Lao H, Kivunge B, Muthoka G, Mwangi P. Enumeration of cyclic codes over GF [17]. International Journal of Scientific Research and Innovative Technology. May 2015;2(5). ISSN: 2313-3759
- [19] Manish G, Bhullar JS, Vinocha OP. On the Combination of five cyclic code. Int. J. Contemp. Math. Sciences. 2010;5(33):1627-1635.
- [20] Runji FM. Enumeration of cyclic codes over GF(5). International Journal of Multi Disciplinary Research. 2014;1(6):2348-2052.
- [21] Ongili P. On the Generalization of the Number of Cyclic codes Over the Prime Field GF(37). Journal of Advances in Mathematics and Computing Science. 2024;39(6). ISSN 2456-9968.
- [22] Simatwo KB. Enumeration of cyclic codes over GF(23). Journal of Advances in Mathematics and Computing Science 2023;38(9). ISSN 2456-9968.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the publisher and/or the editor(s). This publisher and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

---

© 2023 Anabike et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

**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/119485>