**Journal of Advances in Mathematics and Computer Science**

**Volume 38, Issue 9, Page 194-206, 2023; Article no.JAMCS.103549**

*ISSN: 2456-9968*

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

# Enumeration of Cyclic Codes Over $GF(23)$

**Kimtai Boaz Simatwo [a*], Runji Flora Mati [b] and Obogi Robert Karieko [a]**

[a] *Department of Mathematics and Actuarial Science, Kisii University, P. O. Box 408-40200, Kisii, Kenya.*

[b] *Department of Mathematics, Statistics and Actuarial Sciences, Karatina University, P. O. Box 1957-10101, Karatina, 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/2023/v38i91815

**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/103549

***Received: 04/06/2023***
***Accepted: 06/08/2023***
***Published: 22/08/2023***

***Original Research Article***

## Abstract

In this paper, we investigate the number of irreducible polynomials of $\langle x^n - 1\rangle$ over $GF(23)$. First, We factorize $\langle x^n - 1\rangle$ into irreducible polynomials over $GF(23)$ using the cyclotomic cosets of 23 modulo $n$. The number of irreducible polynomial factors of $\langle x^n - 1\rangle$ over $GF(23)$ is equal to the number of cyclotomic cosets of 23 modulo $n$ and each monic divisor of $\langle x^n - 1\rangle$ is a generator polynomial of cyclic codes in $GF(23)$. Succeedingly, we confirm that the number of cyclic codes of length $n$ over a finite field $GF(23)$ is equivalent to the number of polynomials that divide $\langle x^n - 1\rangle$.
In conclusion, we enumerate the number of cyclic codes of length $n$ for $1 \leq n < 24$ and as $n = 23k, n = 23^k$ for $1 \leqslant k < 24$.

*Keywords: Code; cyclic code; cyclotomic cosets.*

**Corresponding author: E-mail: kimtaiboaz96@gmail.com;*

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

# 1 Introduction

Most investigations and explanations executed in coding theory are persuaded largely by the vexaticity of codes that subsist effectiveness and efficiency in certain functioning along with the deliguence with regard to decoding complications of coding theory particularly in communication through deceptive carriers whose outcomes are inaccurate in the conveyed acceptation. In point of fact, the latest aggregate of scholars have procured out-turns exemplifying te cyclic codes see [1, 2, 3, 4, 5, 6, 7, 8], accordingly beneficient into the current literature reviews as well the convey that multitude of researchers and investigators recommenced to reckon with no generation of new formulas on enumeration of cyclic codes. For comprehensive studies in regard to coding types see [9, 10, 11], researchers have contrived direct applications on cryptography, perfect codes of ideals of the polynomial rings for error detections and controls therefore granting escalations to perfect repetion codes. Perhaps, may be in view of the fact that there isn't an inconsiderable errand thus setting out an emanate of an exceedingly protracted standing problem in coding theory. Recent explorations on detailed coding theory have been justified see [12, 13, 14, 15, 16, 17] where encoding moreover decoding theory have multitudinal applications in the theory of computer science. Aforementioned set to contribute to this knowledge gap by formulating some conventional results on maximal plausibility decoding on intercommunication channels, algorithms, architectures, applications on the generatorsof codes of ideals of the polynomial rings for error control and ultimately applications on error control in computer on perfect repetitions codes. It is significant perceiving that the theory of error-correcting concern on an account of the assumed recalcitrant of auditioning message accurately. Entropy is consigned along a channel that is liable to inaccuracy. The medium can be a telephone line, a high frequency radio network in turn with satellite delivery link. The noise can be humanoid errors, lightning, thermal noise deficiency in accessories e.t.c. The goal of on error correcting intend to encode the finding affixing considerable redundancy to the message in that the foremost message can be recovered. Researchers consequently chase down for an $(n, k, d) - code$ with disseminate an extensive collection of messages efficiently and correct multiple errors particularly small n, large $k$, and large d. These are contradicting aims and this is usually pertained to as the utmost coding theory problem. Along with these practicable applications, encoding theory has multiple applications in the theory of computer science. As such it is a concept of significance to both practitioners and theoreticians.

## 1.1 Definitions

i) **Code:** Let $\mathbb{F}$ be a finite set with $q$ elements, 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 $k$ message digits. The set constisting of $q^k$ codewords of length $n$ is called a code. The length $n$ is a range of $n$-tuples $(a_1, a_2, a_3, \ldots, a_n)$ where the $a_i$ 's belong to a finite set $\mathbb{F}$ beside two symbols or digits called alphabets hence, a code of length $n$ from $\mathbb{F}$ is on element of $\mathbb{F}^n$ (the set of all n-tuples from $\mathbb{F}$ ).

ii) **Cyclic code:** A linear block is stated to be cyclic code when it is constant under entire cyclic shifts that is if $a_0, a_1, a_2, \ldots a_n$ is codeword, therefore $a_n, a_1, a_2, \ldots a_{n-1}$ and $a_2, a_3, \ldots a_n, a_1$, This indicate that a cyclic code is achieved by a cyclic right shift of the determinant is also a codeword and this furthermore implicate the left shift. Consequently a linear code $C$ is cyclic absolutely so long as it is an invariant under all cyclic shifts.

iii) **Cyclotomic cosets:** Let n be co-prime to q, the cyclotomic cosets of n mod q containing i is defined by:

$$C_i = \Big\{ i.q^j \bmod n \in \mathbb{Z}_n : \{j = 0, 1, 2, 3, \ldots\}$$

A subset $\{i_1, i_2, \ldots i_n\}$ of $\mathbb{Z}_n$ is called a a complete set of representatives of cyclotomic cosete of $q$ mod $n$ if $C_{i_1}, C_{i_2}, \ldots, C_{i_n}$, is distinguishable and $U_j^t = 1$, $C_{j^2}^{i} = \mathbb{Z}_n$.

# 2 Main Results:

A code $C$ is shown to be cyclic when and only when it is a linear code and its invariant under way every cyclic shift. In finding cyclic codes we factorize $x^n - 1$ into irreducible polynomials and achieve all monic polynomials that divide $x^n - 1$. Every such monic polynomial is a generator polynomial and generate a cyclic code. Afterwords we generate the number of cyclic codes of length $n$ over GF(23)

## 2.1 Factorization of $x^n - 1$ into irreducible polynomial over $GF(23)$

Let $n$ be a positive integer with $q$ and $n$ relatively prime. The number of irreducible polynomial factors of $x^n - 1$ over $\mathbb{F}_q$ is equal to the number of cyclotomic cosets of q mod n and when:

1) $n = 1$
   $x - 1 = x + 22$ is a linear factor.
   $x - 1 = x + 22$ is an irreducible polynomial of degree 1 over $GF(23)$.
   $C_0 = \{0.23^0 \bmod 1\} = \{0\}$ over $GF(23)$
   $C_0$: Let $n$ be a co-prime to $q$, the cyclotomic coset of $n$ mod $q$ containing $i$ is defined by $C_0 = \{0.q^j \bmod n \in \mathbb{Z}_n : \{j = 0$ $C_0$ is distiguishabble when $C^i_{j^2} = \mathbb{Z}_n$.

2) $n = 2$
   $x^2 - 1$; Consider the cyclotomic cosets 23 mod 2 over $GF(23)$:
   $C_i = \{i.23^j \bmod 2 : j = 0, 1, 2, 3, ...\}$
   $C_0 = \{0\}, C_1 = \{1\}$
   Therefore, $x^2 - 1$ is a quadratic expression and factorizes into two irreducible linear factors;
   There are only two cyclotomic cosets of 23 mod 2 over $GF(23)$. On the other hand, the number of irreducible polynomials will only be two irreducible polynomials:
   $x^2 - 1 = (x - 1)(x + 1)$
   $= (x + 22)(x + 1)$ over $GF(23)$

3) $n = 3$
   $x^3 - 1$; Consider the cyclotomic cosets of 23 mod 3 over $GF(23)$:
   $C_i = \{i.23^j \bmod 3 : j = 0, 1, 2, 3, ...\}$
   $C_0 = \{0\}, C_1 = \{1, 2\}$
   Therefore $x^3 - 1$ factorizes into two irreducible factors that divide $x^3 - 1$ over $GF(23)$:
   $x^3 - 1 = (x - 1)(x^2 + x + 1)$
   $= (x + 22)(x^2 + x + 1)$ over GF(23)

4) $n = 4$
   $x^4 - 1$; Consider the cyclotomic cosets of 23 mod 4 over $GF(23)$:
   $C_i = \{i.23^j \bmod 4 : j = 0, 1, 2, 3, ...\}$
   $C_0 = \{0\}, C_1 = \{1, 3\}, C_2 = \{2\}$
   Therefore $x^4 - 1$ factorizes into three irreducible linear factors that is one of degree two and the other two linear factors:

   $x^4 - 1 = (x^2 - 1)(x^2 + 1)$
   $= (x - 1)(x + 1)(x^2 + 1)$
   $= (x + 22)(x + 1)(x^2 + 1)$ over $GF(23)$

5) $n = 5$
   $x^5 - 1$; Consider the cyclotomic cosets of 23 mod 5 over $GF(23)$:
   $C_i = \{i.23^j \bmod 5 : j = 0, 1, 2, 3, ...\}$
   $C_0 = \{0\}, C_1 = \{1, 2, 3, 4\}$ over $GF(23)$

There are only two cyclotomic cosets of 23 mod 5 over $GF(23)$
Therefore the number of irreducible polynomials will be two
$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$
$= (x+22)(x^4 + x^3 + x^2 + x + 1)$ over $GF(23)$

6) $n = 6$
$x^6 - 1$; Consider the cyclotomic cosets of 23 mod 6 over $GF(23)$
$C_i = \{i.23^j \bmod 6 : j = 0, 1, 2, 3, ...\}$
$C_0 = \{0\}, C_1 = \{1, 5\}, C_2 = \{2, 4\}, C_3 = \{3\}$
Therefore $x^6 - 1$ factorizes into four irreducible polynomials, two of degree one and two of degree two over $GF(23)$:
$x^6 - 1 = (x^3 - 1)(x^3 + 1)$
$= (x-1)(x^2 + x + 1)(x+1)(x^2 - x + 1)$
$= (x+22)(x^2 + x + 1)(x+1)(x^2 + 22x + 1)$ over $GF(23)$

7) $n = 7$
$x^7 - 1$; Consider the cyclotomic cosets of 23 mod 7 over $GF(23)$:
$C_i = \{i.23^j \bmod 7 : j = 0, 1, 2, 3, ...\}$
$C_0 = \{0\}, C_1 = \{1, 2, 4\}$, $C_3 = \{3, 5, 6\}$ over $GF(23)$
Therefore $x^7 - 1$ factorizes into three irreducible polynomial factors, one of degree one and two of degree three:
$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$
$= (x+22)(x^3 + 10x^2 + 9x + 22)(x^3 + 14x^2 + 13x + 22)$ over $GF(23)$

8) $n = 8$
$x^8 - 1$. Consider the cyclotomic cosets of 23 mod 8 over $GF(23)$
$C_i = \{i.23^j \bmod 8 : j = 0, 1, 2, 3, ...\}$
$C_0 = \{0\}, C_1 = \{1, 7\}, C_2 = \{2, 6\}, C_3 = \{3, 5\}, C_4 = \{4\}$ over $GF(23)$
Therefore $x^8 - 1$ factorizes into five irreducible polynomial factors, two of degree one and three of degree two that is
$x^8 - 1 = (x^4 - 1)(x^4 + 1)$
$= (x^2 - 1)(x^2 + 1)(x^4 + 1)$
$= (x-1)(x+1)(x^2 + 1)(x^4 + 1)$
$= (x+22)(x+1)(x^2 + 1)(x^2 + 5x + 1)(x^2 + 18x + 1)\, over\, GF(23)$

9) $n = 9$
$x^9 - 1$; Consider the cyclotomic cosets of 23 mod 9 over $GF(23)$.
$C_i = \{i.23^j \bmod 9 : j = 0, 1, 2, 3, ...\}, C_0 = \{0\}, C_1 = \{1, 2, 4, 5, 7, 8\}, C_3 = \{3, 6\}$ over $GF(23)$
Therefore $x^9 - 1$ factorizes into three irreducible polynomial factors, one of degree one, one of degree two and one of degree six, that is
$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$
$= (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$
$= (x+22)(x^2 + x + 1)(x^6 + x^3 + 1)$ over $GF(23)$

10) $n = 10$
$x^{10} - 1$; Consider the cyclotomic cosets of 23 mod 10 over $GF(23)$
$C_i = \{i.23^j \bmod 10 : j = 0, 1, 2, 3, ...\}$
$C_0 = \{0\}, C_1 = \{1, 3, 7, 9\}, C_2 = \{2, 4, 6, 8\}, C_5 = \{5\}$ over $GF(23)$
Therefore $x^{10} - 1$ factorizes into four irreducible polynomial factors, two of degree one and two of degree four that is:
$x^{10} - 1 = (x^5 - 1)(x^5 + 1)$
$= (x-1)(x^4 + x^3 + x^2 + x + 1)(x+1)(x^4 - x^3 + x^2 - x + 1)$
$= (x+22)(x^4 + x^3 + x^2 + x + 1)(x+1)(x^4 + 22x^3 + x^2 + 22x + 1)$ over $GF(23)$

11) $n = 11$
$x^{11} - 1$; Consider the cyclotomic cosets of 23 mod 11 over $GF(23)$.
$C_i = \{i.23 \text{ mod}^j 11 : j = 0, 1, 2, 3, ...\}$
$C_0 = \{0\}, C_1 = \{1\}, C_2 = \{2\}, C_3 = \{3\}, C_4 = \{4\}, C_5 = \{5\}, C_6 = \{6\}, C_7 = \{7\}, C_8 = \{8\}, C_9 = \{9\}, C_{10} = \{10\}$ over $GF(23)$.
Therefore, $x^{11} - 1$ factorises into eleven monic irreducible polynomial factors, each of degree one that is
$x^{11} - 1 = (x - 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$
$= (x + 22)(x + 20)(x + 5)(x + 7)(x + 19)(x + 17)(x + 11)(x + 10)(x + 14)(x + 15)(x + 21)$ over $GF(23)$

12) $n = 12$
$x^{12} - 1$; Consider the cyclotomic cosets of 23 mod 12: over $GF(23)$
$C_i = \{i.23^j \text{ mod } 12 : j = 0, 1, 2, 3, ...\}$
$C_0 = \{0\}, C_1 = \{1, 11\}, C_2 = \{2, 10\}, C_3 = \{3, 9\}, C_4 = \{4, 8\}, C_5 = \{5, 7\}, C_6 = \{6\}$ over $GF(23)$
Therefore, $x^{12} - 1$ factorizes into seven irreducible polynomial factors, two of degree one and five of degree two, that is:
$x^{12} - 1 = (x^4 - 1)(x^8 + x^4 + 1)$
$= (x^2 - 1)(x^2 + 1)(x^8 + x^4 + 1)$
$= (x + 22)(x + 1)(x^2 + 1)(x^2 + x + 1)(x^2 + 22x + 1)(x^4 + 22x^2 + 1)$
$= (x+22)(x+1)(x^2+1)(x^2+x+1)(x^2+22x+1)(x^2+7x+1)(x^2+16x+1)$ over $GF(23)$

13) $n = 13$
$x^{13} - 1$; Consider the cyclotomic cosets of 23 mod 13 over $GF(23)$
$C_i = \{i.23^j \text{ mod } 13 : j = 0, 1, 2, 3, ...\}$
$C_0 = \{0\}, C_1 = \{1, 3, 4, 9, 10, 12\}, C_2 = \{2, 5, 6, 7, 8, 11\}$ over $GF(23)$
Therefore $x^{13} - 1$ factorizes into three irreducible polynomial factors, one of degree one and two of degree six that is
$x^{13} - 1 = (x - 1)(x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$
$= (x + 22)(x^6 + 9x^5 + 2x^4 + 8x^3 + 2x^2 + 9x + 1)(x^6 + 15x^5 + 2x^4 + 14x^3 + 2x^2 + 15x + 1)$ over $GF(23)$

14) $n = 14$
$x^{14} - 1$; Consider the cyclotomic cosets of 23 mod 14 over $GF(23)$:
$C_i = \{i.23^j \text{ mod } 14 : j = 0, 1, 2, 3, ...\}$
$C_0 = \{0\}, C_1 = \{1, 9, 11\}, C_2 = \{2, 4, 8\}, C_3 = \{3, 5, 13\}, C_4 = \{6, 10, 12\}, C_7 = \{7\}$ over $GF(23)$ .
Therefore $x^{14} - 1$ factorizes into six irreducible polynomial factors, two of degree one and four of degree three that is $(x^{14} - 1) = (x^7 - 1)(x^7 + 1)$
$= (x + 22)(x^3 + 20x^2 + 2x + 22)(x^3 + 21x^2 + 3x + 22)(x^7 + 1)$
$= (x + 22)(x + 1)(x^3 + 9x^2 + 13x + 1)(x^3 + 10x^2 + 9x + 22)(x^3 + 13x^2 + 9x + 1)(x^3 + 14x^2 + 13x + 22)$ over $GF(23)$

15) $n = 15$
$x^{15} - 1$; Consider the cyclotomic cosets of 23 mod 15 over $GF(23)$
$C_i = \{i.23^j \text{ mod } 15 : j = 0, 1, 2, 3, ...\}$
$C_0 = \{0\}, C_1 = \{1, 2, 4, 8\}, C_3 = \{3, 6, 9, 12\}, C_5 = \{5, 10\}, C_7 = \{7, 11, 13, 14\}$
Therefore, $x^{15} - 1$ factorizes into five irreducible polynomial factors, one of degree one, one of degree two and three of degree four that is
$x^{15} - 1 = (x^5 - 1)(x^{10} + x^5 + 1)$
$= (x+22)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+6x^3+21x^2+16x+1)(x^4+16x^3+21x^2+6x+1)$ over $GF(23)$

16) $n = 16$

$x^{16}-1$; Consider the cyclotomic cosets of 23 mod 16 over $GF(23)$
$C_i = \{i.23^j \bmod 16 : j = 0,1,2,3,...\}$
$C_0 = \{0\}, C_1 = \{1,7\}, C_2 = \{2,14\}, C_3 = \{3,5\}, C_4 = \{4,12\}, C_6 = \{6,10\}, C_8 = \{8\}, C_9 = \{9,15\}, C_{11} = \{11,13\}$
Therefore, $x^{16}-1$, factorizes into nine irreducible polynomial factors, two of degree one and seven of degree two that is
$x^{16}-1 = (x^8-1)(x^8+1)$
$= (x^4-1)(x^4+1)(x^8+1)$
$= (x+22)(x+1)(x^2+1)(x^2+4x+22)(x^2+5x+1)(x^2+7x+22)(x^2+16x+22)(x^2+18x+1)(x^2+19x+22)$ over $GF(23)$

17) $n = 17$
$x^{17}-1$; Consider the cyclotomic coset of 23 mod 17 over $GF(23)$
$C_i = \{i.23^j \bmod 17 : j = 0,1,2,3,...\}, C_0 = \{0\}, C_1 = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$
Therefore, $x^{17}-1$ factorizes into two irreducible polynomial factors, one of degree one and one of degree sixteen, that is
$: (x^{17}-1) = (x-1)(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
$= (x+22)(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$ over $GF(23)$

18) $n = 18$
$x^{18}-1$; Consider the cyclotomic cosets of 23 mod 18 over $GF(23)$
$C_i = \{i.23 \bmod^j 18 : j = 0,1,2,3,...\}, C_0 = \{0\}, C_1 = \{1,5,7,11,13,17\}, C_2 = \{2,4,8,10,14,16\}, C_3 = \{3,15\}, C_6 = \{6,12\}, C_9 = \{9\}$
Therefore, $x^{18}-1$ factorizes into six irreducible polynomial factors, two of degree one, two of degree two and two of degree six, that is
$(x^{18}-1) = (x+1)(x-1)(x^2+x+1)(x^2+22x+1)(x^6+x^3+1)(x^6+22x^3+1)$
$= (x+1)(x+22)(x^2+x+1)(x^2+22x+1)(x^6+x^3+1)(x^6+22x^3+1)$
over $GF(23)$

19) $n = 19$
$x^{19}-1$, consider the cyclotomic cosets of 23 mod 19 over $GF(23)$:
$C_i = \{i.23^j \bmod 19 : j = 0,1,2,3,....\}, C_0 = \{0\}, C_1 = \{1,4,5,6,7,9,11,16,17\}, C_2 = \{2,3,8,10,12,13,14,15,18\}$

Therefore, $x^{19}-1$ factorizes into three irreducible polynomial factors, one of degree one and two of degree nine, that is
$x^{19}-1 = (x+22)(x^9+11x^8+21x^7+14x^6+13x^5+8x^4+11x^3+2x^2+10x+22)(x^9+13x^8+21x^7+12x^6+15x^5+10x^4+9x^3+2x^2+12x+22)$ over $GF(23)$

20) $n = 20$
$x^{20}-1$; Consider the cyclotomic cosets of 23 mod 20 over $GF(23)$
$C_i = \{i.23^j \bmod 20 : j = 0,1,2,3,...\}, C_0 = \{0\}, C_1 = \{1,3,7,9\}, C_2 = \{2,6,14,18\}, C_4 = \{4,8,12,16\}, C_5 = \{5,15\}, C_{10} = \{10\}, C_{11} = \{11,13,17,19\}$
Therefore, $x^{20}-1$ factorizes into seven irreducible polynomial factors, two of degree one, one of degree two and four of degree four, that is
$x^{20}-1 = (x^{10}-1)(x^{10}+1)$
$= (x^5-1)(x^5+1)(x^{10}+1)$
$= (x+22)(x^4+x^3+x^2+x+1)(x+1)(x^4+22x^3+x^2+22x+1)(x^2+1)(x^4+8x^3+20x^2+15x+1)(x^4+15x^3+20x^2+8x+1)$ over $GF(23)$

21) $n = 21$
$x^{21}-1$; Consider the cyclotomic cosets of 23 mod 21 over $GF(23)$

$C_i = \{i.23^j \bmod 21 : j = 0,1,2,3,...\}, C_0 = \{0\}, C_1 = \{1,2,4,8,11,16\}, C_2 = \{3,6,12\}, C_5 = \{5,10,13,17,19,20\}, C_7 = \{7,14\}, C_9 = \{9,15,18\}$
Therefore, $x^{21}-1$ factorizes into six irreducible polynomial factors, one of degree one, one of degree two, two of degree three and two of degree six. That is
$x^{21}-1 = (x^7-1)(x^{14}+x^7+1)$
$= (x+22)(x^3+10x^2+9x+22)(x^3+14x^2+13x+22)(x^{14}+x^7+1)$
$= (x+22)(x^3+10x^2+9x+22)(x^3+14x^2+13x+22)(x^2+x+1)(x^6+9x^5+22x^4+22x^2+13x+1)(x^6+13x^5+22x^4+22x^2+9x+1)$ over $GF(23)$

22) $n = 22$
$x^{22}-1$; Consider the cyclotomic cosets of 23 mod 22 over $GF(23)$
$C_i = \{i.23^j \bmod 22 : j = 0,1,2,3,...\}$
$C_0 = \{0\}, C_1 = \{1\}, C_2 = \{2\}, C_3 = \{3\}, C_4 = \{4\}, C_5 = \{5\}, C_6 = \{6\}, C_7 = \{7\}, C_8 = \{8\}, C_9 = \{9\}, C_{10} = \{10\}, C_{11} = \{11\}, C_{12} = \{12\}, C_{13} = \{13\}, C_{14} = \{14\}, C_{15} = \{15\}, C_{16} = \{16\}, C_{17} = \{17\}, C_{18} = \{18\}, C_{19} = \{19\}, C_{20} = \{20\}, C_{21} = \{21\}$
Therefore, $x^{22}-1$ factorizes into twenty two irreducible polynomial factors that is monic factors, all of degree one that is (all linear factors over $GF(23)$) $x^{22}-1 = (x+1)(x+2)(x+3)(x+4)(x+5)(x+6)(x+7)(x+8)(x+9)(x+10)(x+11)(x+12)(x+13)(x+14)(x+15)(x+16)(x+17)(x+18)(x+19)(x+20)(x+21)(x+22)$ over $GF(23)$

23) $n = 23$
$C_i = \{i.23^j \bmod 23 : j = 0,1,2,3,...\}$
$x^{23}-1$; Consider the cyclotomic cosets of 23 mod 23 over $GF(23)$
Therefore, $x^{23}-1$ factorizes into twenty three irreducible polynomials, all linear factors over $GF(23)$
That is $x^{23}-1 = (x-1)^{23} = (x+22)^{23}$

**THEOREM 1.1:** The number of cyclic codes in $R_n = \frac{\mathbb{F}_q[x]}{<x^n-1>}$ is equal to $2^m$ where $m$ is the number of m cyclotomic cosets mod n.
Consider the number of cyclic code of length n.
$n = 1,2,3,...,23$ over $GF(23)$
The number of cyclic codes is summarized in the table below:

**Table 1.**

| $x^n-1$ | Number of irreducible factors of $x^n-1$ | Number of cyclic codes |
|---|---|---|
| $x^1-1$ | 1 | $2^1=2$ |
| $x^2-1$ | 2 | $2^2=4$ |
| $x^3-1$ | 2 | $2^2=4$ |
| $x^4-1$ | 3 | $2^3=8$ |
| $x^5-1$ | 2 | $2^2=4$ |
| $x^6-1$ | 4 | $2^4=16$ |
| $x^7-1$ | 3 | $2^3=8$ |
| $x^8-1$ | 5 | $2^5=32$ |
| $x^9-1$ | 3 | $2^3=8$ |
| $x^{10}-1$ | 4 | $2^4=16$ |
| $x^{11}-1$ | 11 | $2^{11}=2048$ |
| $x^{12}-1$ | 7 | $2^7=128$ |
| $x^{13}-1$ | 3 | $2^3=8$ |
| $x^{14}-1$ | 6 | $2^6=64$ |
| $x^{15}-1$ | 5 | $2^5=32$ |
| $x^{16}-1$ | 9 | $2^9=512$ |
| $x^{17}-1$ | 2 | $2^2=4$ |
| $x^{18}-1$ | 6 | $2^6=64$ |
| $x^{19}-1$ | 3 | $2^3=8$ |
| $x^{20}-1$ | 7 | $2^7=128$ |
| $x^{21}-1$ | 6 | $2^6=64$ |
| $x^{22}-1$ | 22 | $2^{22}=4194304$ |
| $x^{23}-1$ | 1 | $2^1=2$ |

## 2.2 Factorization of $x^n - 1$ into irreducible polynomial over $GF(23)$ when $n = 23k$ for $1 \leq k < 24$

a) $k = 1 : x^{23} - 1 = (x-1)^{23} = (x+22)^{23}$ :
The number of cyclic codes $= (23+1) = 24$

b) $k = 2 : x^{56} - 1 = (x^2-1)^{23} = (x-1)^{23}(x+1)^{23} = (x+22)^{23}(x+1)^{23}$
The number of cyclic codes $= (23+1)^2 = 24^2$

c) $k = 3 : x^{69} - 1 = (x^3-1)^{23} = (x+22)^{23}(x^2+x+1)^{23}$
Number of cyclic codes $= (23+1)^2 = 24^2$

d) $k = 4 : x^{92} - 1$
$= (x^2-1)^{23}(x^2+1)^{23}$
$= (x-1)^{23}(x+1)^{23}(x^2+1)^{23}$
$= (x+22)^{23}(x+1)^{23}(x^2+1)^{23}$
Number of cyclic codes $= (23+1)^3 = 24^3$

e) $k = 5 : x^{115} - 1 = (x^5-1)^{23} = (x-1)^{23}(x^4+x^3+x^2+x+1)^{23}$
$= (x+22)^{23}(x^4+x^3+x^2+x+1)^{23}$
Number of cyclic codes $= (23+1)^2 = 24^2$

f) $k = 6 : x^{138} - 1 = (x^6-1)^{23} = (x^3-1)^{23}(x^3+1)^{23}$
$= (x-1)^{23}(x^2+x+1)^{23}(x+1)^{23}(x^2-x+1)^{23}$
$= (x+22)^{23}(x^2+x+1)^{23}(x+1)^{23}(x^2+22x+1)^{23}$
Number of cyclic codes $= (23+1)^4 = 24^4$

g) $k = 7 : x^{161} - 1 = (x^7-1)^{23} = (x-1)^{23}(x^6+x^5+x^4+x^3+x^2+x+1)^{23}$
$= (x+22)^{23}(x^3+10x^2+9x+22)^{23}(x^3+14x^2+13x+22)^{23}$
Number of cyclic codes $= (23+1)^3 = 24^3$

h) $k = 8 : x^{184} - 1 = (x^8-1)^{23} = (x^4-1)^{23}(x^4+1)^{23}$
$= (x^2-1)^{23}(x^2+1)^{23}(x^4+1)^{23}$
$= (x-1)^{23}(x+1)^{23}(x^2+1)^{23}(x^4+1)^{23}$
$= (x+22)^{23}(x+1)^{23}(x^2+1)^{23}(x^2+5x+1)^{23}(x^2+18x+1)^{23}$
Number of cyclic codes $= (23+1)^5 = 24^5$

i) $k = 9 : x^{207} - 1 = (x^9-1)^{23} = (x^3-1)^{23}(x^6+x^3+1)^{23}$
$= (x-1)^{23}(x^2+x+1)^{23}(x^6+x^3+1)^{23}$
$= (x+22)^{23}(x^2+x+1)^{23}(x^6+x^3+1)^{23}$
Number of cyclic codes $= (23+1)^3 = 24^3$

j) $k = 10 : x^{230} - 1 = (x^{10}-1)^{23} = (x^5-1)^{23}(x^5+1)^{23}$
$= (x-1)^{23}(x^4+x^3+x^2+x+1)^{23}(x+1)^{23}(x^4-x^3+x^2-x+1)^{23}$
$= (x+22)^{23}(x^4+x^3+x^2+x+1)^{23}(x+1)^{23}(x^4+22x^3+x^2+22x+1)^{23}$
Number of cyclic codes $= (23+1)^4 = 24^4$

k) $k = 11 : x^{253} - 1 = (x^{11}-1)^{23} = (x-1)^{23}(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)^{23}$
$= (x+22)^{23}(x+20)^{23}(x+5)^{23}(x+7)^{23}(x+19)^{23}(x+17)^{23}(x+11)^{23}(x+10)^{23}(x+14)^{23}(x+15)^{23}(x+21)^{23}$
Number of cyclic codes $= (23+1)^{11} = 24^{11}$

l) $k = 12 : x^{276} - 1 = (x^{12}-1)^{23} = (x^4-1)^{23}(x^8+x^4+1)^{23}$
$= (x^2-1)^{23}(x^2+1)^{23}(x^8+x^4+1)^{23}$
$= (x+22)^{23}(x+1)^{23}(x^2+x+1)^{23}(x^2+22x+1)^{23}(x^2+7x+1)^{23}(x^2+16x+1)^{23}$
$= (x+22)^{23}(x+1)^{23}(x^2+1)^{23}(x^2+x+1)^{23}(x^2+22x+1)^{23}(x^2+7x+1)^{23}(x^2+16x+1)^{23}$
Number of cyclic codes $= (23+1)^7 = 24^7$

m) $k = 13 : x^{299} - 1 = (x^{13} - 1)^{23} = (x - 1)^{23}(x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{23}$
$= (x+22)^{23}(x^6+9x^5+2x^4+8x^3+2x^2+9x+1)^{23}(x^6+15x^5+2x^4+14x^3+2x^2+15x+1)^{23}$.
Number of cyclic codes $= (23 + 1)^3 = 24^3$

n) $k = 14 : x^{322} - 1 = (x^{14} - 1)^{23} = (x^7 - 1)^{23}(x^7 + 1)^{23}$
$= (x + 22)^{23}(x^3 + 9x^2 + 13x + 1)^{23}(x^3 + 10x^2 + 9x + 22)^{23}(x^7 + 1)^{23}$
$= (x + 22)^{23}(x + 1)^{23}(x^3 + 9x^2 + 13x + 1)^{23}(x^3 + 10x^2 + 9x + 22)^{23}(x^3 + 13x^2 + 9x + 1)^{23}(x^3 + 14x^2 + 13x + 22)^{23}$
Number of cyclic codes $= (23 + 1)^6 = 24^6$

o) $k = 15 : x^{345} - 1 = (x^5 - 1)^{23}(x^{10} + x^5 + 1)^{23}$
$= (x + 22)^{23}(x^4 + x^3 + x^2 + x + 1)^{23}(x^2 + x + 1)^{23}(x^4 + 6x^3 + 21x^2 + 16x + 1)^{23}(x^4 + 16x^3 + 21x^2 + 6x + 1)^{23}$.
Number of cyclic codes $= (23 + 1)^5 = 24^5$

p) $k = 16 : x^{368} - 1 = (x^{16} - 1)^{23} = (x^8 - 1)^{23}(x^8 + 1)^{23}$
$= (x^4 - 1)^{23}(x^4 + 1)^{23}(x^8 + 1)^{23}$
$= (x+22)^{23}(x+1)^{23}(x^2+1)^{23}(x^2+4x+22)^{23}(x^2+5x+1)^{23}(x^2+7x+22)^{23}(x^2+16x+22)^{23}(x^2 + 18x + 1)^{23}(x^2 + 19x + 22)^{23}$.
Number of cyclic codes $= (23 + 1)^9 = 24^9$

q) $k = 17 : x^{391} - 1 = (x^{17} - 1)^{23} = (x - 1)^{23}(x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{23}$
$= (x+22)^{23}(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)^{23}$
Number of cyclic codes $= (23 + 1)^2 = 24^2$.

r) $k = 18 : x^{414}-1 = (x^{18}-1)^{23} = (x+1)^{23}(x-1)^{23}(x^2+x+1)^{23}(x^2+22x+1)^{23}(x^6+x^3+1)^{23}$
$= (x + 1)^{23}(x + 22)^{23}(x^2 + x + 1)^{23}(x^2 + 22x + 1)^{23}(x^6 + x^3 + 1)^{23}(x^6 + 22x^3 + 1)^{23}$
Number of cyclic codes $= (23 + 1)^6 = 24^6$

s) $k = 19 : x^{437} - 1 = (x^{19} - 1)^{23} = (x+1)^{23}(x^9 + 11x^8 + 21x^7 + 14x^6 + 13x^5 + 8x^4 + 11x^3 + 2x^2 + 10x + 22)^{23}(x^9 + 13x^8 + 21x^7 + 12x^6 + 15x^5 + 10x^4 + 9x^3 + 2x^2 + 12x + 22)^{23}$
Number of cyclic codes $= (23 + 1)^3 = 24^3$

t) $k = 20 : x^{460} - 1 = (x^{20} - 1)^{23} = (x^{10} - 1)^{23}(x^{10} + 1)^{23}$
$= (x^5 - 1)^{23}(x^5 + 1)^{23}(x^{10} + 1)^{23}$
$= (x + 22)^{23}(x^4 + x^3 + x^2 + x + 1)^{23}(x + 1)^{23}(x^4 + 22x^3 + x^2 + 22x + 1)^{23}(x^2 + 1)^{23}(x^4 + 8x^3 + 20x^2 + 15x + 1)^{23}(x^4 + 15x^3 + 20x^2 + 8x + 1)^{23}$
Number of cyclic codes $= (23 + 1)^7 = 24^7$

u) $k = 21 : x^{483} - 1 = (x^{21} - 1)^{23}$
$= (x^7 - 1)^{23}(x^{14} + x^7 + 1)^{23}$
$= (x + 22)^{23}(x^3 + 10x^2 + 9x + 22)^{23}(x^3 + 14x^2 + 13x + 22)^{23}(x^{14} + x^7 + 1)^{23}$
$= (x + 22)^{23}(x^3 + 10x^7 + 9x + 22)^{23}(x^3 + 14x^2 + 13x + 22)^{23}(x^2 + x + 1)^{23}(x^6 + 9x^5 + 22x^4 + 22x^2 + 13x + 1)^{23}(x^6 + 13x^5 + 22x^4 + 22x^2 + 9x + 1)^{23}$.
Number of cyclic codes $= (23 + 1)^6 = 24^6$

v) $k = 22 : x^{506} - 1 = (x^{22} - 1)^{23}$
$= (x + 1)^{23}(x + 2)^{23}(x + 3)^{23}(x + 4)^{23}(x + 5)^{23}(x + 6)^{23}(x + 7)^{23}(x + 8)^{23}(x + 9)^{23}(x + 10)^{23}(x + 11)^{23}(x + 12)^{23}(x + 13)^{23}(x + 14)^{23}(x + 15)^{23}(x + 16)^{23}(x + 17)^{23}(x + 18)^{23}(x + 19)^{23}(x + 20)^{23}(x + 21)^{23}(x + 22)^{23}$.
Number of cyclic codes $= (23 + 1)^{21} = 24^{21}$

w) $k = 23 : x^{529} - 1 = (x^{23} - 1)^{23} = x^{23} - 1 = (x - 1)^{23} = (x + 22)^{23}$
Number of cyclic codes $= (23 + 1)^{23} = 24^{23}$

## 2.3 Factorization of $x^n - 1$ into irreducible polynomial over $GF(23)$ when $n = 23k$ for $1 \leq k < 24$

1) When $n = 1$, we have $n = 23^1; x^{23^1} - 1 = (x-1)^{23^1} = (x+22)^{23^1}$
2) When $n = 2$, we have $n = 23^2; x^{23^2} - 1 = (x-1)^{23^2} = (x+22)^{23^2}$
3) When $n = 3$, we have $n = 23^3; x^{23^3} - 1 = (x-1)^{23^3} = (x+22)^{23^3}$
4) When $n = 4$, we have $n = 23^4; x^{23^4} - 1 = (x-1)^{23^4} = (x+22)^{23^4}$
5) When $n = 5$, we have $n = 23^5; x^{23^5} - 1 = (x-1)^{23^5} = (x+22)^{23^5}$
6) When $n = 6$, we have $n = 23^6; x^{23^6} - 1 = (x-1)^{23^6} = (x+22)^{23^6}$
7) When $n = 7$, we have $n = 23^7; x^{23^7} - 1 = (x-1)^{23^7} = (x+22)^{23^7}$
8) When $n = 8$, we have $n = 23^8; x^{23^8} - 1 = (x-1)^{23^8} = (x+22)^{23^8}$
9) When $n = 9$, we have $n = 23^9; x^{23^9} - 1 = (x-1)^{23^9} = (x+22)^{23^9}$
10) When $n = 10$, we have $n = 23^{10}; x^{23^{10}} - 1 = (x-1)^{23^{10}} = (x+22)^{23^{10}}$
11) When $n = 11$, we have $n = 23^{11}; x^{23^{11}} - 1 = (x-1)^{23^{11}} = (x+22)^{23^{11}}$
12) When $n = 12$, we have $n = 23^{12}; x^{23^{12}} - 1 = (x-1)^{23^{12}} = (x+22)^{23^{12}}$
13) When $n = 13$, we have $n = 23^{13}; x^{23^{13}} - 1 = (x-1)^{23^{13}} = (x+22)^{23^{13}}$
14) When $n = 14$, we have $n = 23^{14}; x^{23^{14}} - 1 = (x-1)^{23^{14}} = (x+22)^{23^{14}}$
15) When $n = 15$, we have $n = 23^{15}; x^{23^{15}} - 1 = (x-1)^{23^{15}} = (x+22)^{23^{15}}$
16) When $n = 16$, we have $n = 23^{16}; x^{23^{16}} - 1 = (x-1)^{23^{16}} = (x+22)^{23^{16}}$
17) When $n = 17$, we have $n = 23^{17}; x^{23^{17}} - 1 = (x-1)^{23^{17}} = (x+22)^{23^{17}}$
18) When $n = 18$, we have $n = 23^{18}; x^{23^{18}} - 1 = (x-1)^{23^{18}} = (x+22)^{23^{18}}$
19) When $n = 19$, we have $n = 23^{19}; x^{23^{19}} - 1 = (x-1)^{23^{19}} = (x+22)^{23^{19}}$
20) When $n = 20$, we have $n = 23^{20}; x^{23^{20}} - 1 = (x-1)^{23^{20}} = (x+22)^{23^{20}}$
21) When $n = 21$, we have $n = 23^{21}; x^{23^{21}} - 1 = (x-1)^{23^{21}} = (x+22)^{23^{21}}$
22) When $n = 22$, we have $n = 23^{22}; x^{23^{22}} - 1 = (x-1)^{23^{22}} = (x+22)^{23^{22}}$
23) When $n = 23$, we have $n = 23^{23}; x^{23^{23}} - 1 = (x-1)^{23^{23}} = (x+22)^{23^{23}}$
24) When $n = 24$, we have $n = 23^{24}; x^{23^{24}} - 1 = (x-1)^{23^{24}} = (x+22)^{23^{24}}$

Clearly, we can infer $x^{23^k} - 1 = (x-1)^{23^k}$

Factorization of $x^n - 1$ into irreducible monic polynomials over $GF(23)$ is summarized in the table below

**Table 2.**

| k | $(x^{23^k} - 1)$ | $(x-1)^{23^k}$ | $(x-1)^{23^k}$ |
|---|---|---|---|
| 1 | $(x^{23^1} - 1)$ | $(x-1)^{23^1}$ | $(x+22)^{23^1}$ |
| 2 | $(x^{23^2} - 1)$ | $(x-1)^{23^2}$ | $(x+22)^{23^2}$ |
| 3 | $(x^{23^3} - 1)$ | $(x-1)^{23^3}$ | $(x+22)^{23^3}$ |
| 4 | $(x^{23^4} - 1)$ | $(x-1)^{23^4}$ | $(x+22)^{23^4}$ |
| 5 | $(x^{23^5} - 1)$ | $(x-1)^{23^5}$ | $(x+22)^{23^5}$ |
| 6 | $(x^{23^6} - 1)$ | $(x-1)^{23^6}$ | $(x+22)^{23^6}$ |
| 7 | $(x^{23^7} - 1)$ | $(x-1)^{23^7}$ | $(x+22)^{23^7}$ |
| 8 | $(x^{23^8} - 1)$ | $(x-1)^{23^8}$ | $(x+22)^{23^8}$ |
| 9 | $(x^{23^9} - 1)$ | $(x-1)^{23^9}$ | $(x+22)^{23^9}$ |
| 10 | $(x^{23^{10}} - 1)$ | $(x-1)^{23^{10}}$ | $(x+22)^{23^{10}}$ |
| 11 | $(x^{23^{11}} - 1)$ | $(x-1)^{23^{11}}$ | $(x+22)^{23^{11}}$ |
| 12 | $(x^{23^{12}} - 1)$ | $(x-1)^{23^{12}}$ | $(x+22)^{23^{12}}$ |
| 13 | $(x^{23^{13}} - 1)$ | $(x-1)^{23^{13}}$ | $(x+22)^{23^{13}}$ |
| 14 | $(x^{23^{14}} - 1)$ | $(x-1)^{23^{14}}$ | $(x+22)^{23^{14}}$ |
| 15 | $(x^{23^{15}} - 1)$ | $(x-1)^{23^{15}}$ | $(x+22)^{23^{15}}$ |
| 16 | $(x^{23^{16}} - 1)$ | $(x-1)^{23^{16}}$ | $(x+22)^{23^{16}}$ |
| 17 | $(x^{23^{17}} - 1)$ | $(x-1)^{23^{17}}$ | $(x+22)^{23^{17}}$ |
| 18 | $(x^{23^{18}} - 1)$ | $(x-1)^{23^{18}}$ | $(x+22)^{23^{18}}$ |
| 19 | $(x^{23^{19}} - 1)$ | $(x-1)^{23^{19}}$ | $(x+22)^{23^{19}}$ |
| 20 | $(x^{23^{20}} - 1)$ | $(x-1)^{23^{20}}$ | $(x+22)^{23^{20}}$ |
| 21 | $(x^{23^{21}} - 1)$ | $(x-1)^{23^{21}}$ | $(x+22)^{23^{21}}$ |
| 22 | $(x^{23^{22}} - 1)$ | $(x-1)^{23^{22}}$ | $(x+22)^{23^{22}}$ |
| 23 | $(x^{23^{23}} - 1)$ | $(x-1)^{23^{23}}$ | $(x+22)^{23^{23}}$ |

**LEMMA 1.3:** Let $(f_1(x))^{k_1}, (f_2(x))^{k_2}, (f_3(x))^{k_3}, ..., (f_m(x))^{k_m}$ where $f_i(x) : i = 1, 2, 3, ..., m$ are irreducible polynomials over $F_q$, then the number of factors for $x^n - 1$ are given by:

$(k_1 + 1)(k_2 + 2)(k_3 + 1)...(k_m + 1) = \Pi_{i=1}^{m}(k_i + 1)$

The number of cyclic codes is summarized in the table below:

**Table 3.**

| k | n=23k | No.of codes | $n = 23^k$ | No.of codes |
|---|---|---|---|---|
| 1 | 23 | $24 = (23+1)^1$ | $23^1$ | $24 = 23^1 + 1$ |
| 2 | 46 | $= (23+1)^2$ | $23^2$ | $= 23^2 + 1$ |
| 3 | 69 | $= (23+1)^2$ | $23^3$ | $= 23^3 + 1$ |
| 4 | 92 | $= (23+1)^3$ | $23^4$ | $= 23^4 + 1$ |
| 5 | 115 | $= (23+1)^2$ | $23^5$ | $= 23^5 + 1$ |
| 6 | 138 | $= (23+1)^4$ | $23^6$ | $= 23^6 + 1$ |
| 7 | 161 | $= (23+1)^3$ | $23^7$ | $= 23^7 + 1$ |
| 8 | 184 | $= (23+1)^5$ | $23^8$ | $= 23^8 + 1$ |
| 9 | 207 | $= (23+1)^3$ | $23^9$ | $= 23^9 + 1$ |
| 10 | 230 | $= (23+1)^4$ | $23^{10}$ | $= 23^{10} + 1$ |
| 11 | 253 | $= (23+1)^{10}$ | $23^{11}$ | $= 23^{11} + 1$ |
| 12 | 276 | $= (23+1)^7$ | $23^{12}$ | $= 23^{12} + 1$ |
| 13 | 299 | $= (23+1)^3$ | $23^{13}$ | $= 23^{13} + 1$ |
| 14 | 322 | $= (23+1)^6$ | $23^{14}$ | $= 23^{14} + 1$ |
| 15 | 345 | $= (23+1)^5$ | $23^{15}$ | $= 23^{15} + 1$ |
| 16 | 368 | $= (23+1)^9$ | $23^{16}$ | $= 23^{16} + 1$ |
| 17 | 391 | $= (23+1)^2$ | $23^{17}$ | $= 23^{17} + 1$ |
| 18 | 414 | $= (23+1)^6$ | $23^{18}$ | $= 23^{18} + 1$ |
| 19 | 437 | $= (23+1)^3$ | $23^{19}$ | $= 23^{19} + 1$ |
| 20 | 460 | $= (23+1)^7$ | $23^{20}$ | $= 23^{20} + 1$ |
| 21 | 483 | $= (23+1)^6$ | $23^{21}$ | $= 23^{21} + 1$ |
| 22 | 506 | $= (23+1)^{21}$ | $23^{22}$ | $= 23^{22} + 1$ |
| 23 | 529 | $= (23+1)^{23}$ | $23^{23}$ | $= 23^{23} + 1$ |
| 24 | 552 | $= (23+1)^{13}$ | $23^{24}$ | $= 23^{24} + 1$ |

# 3 Conclusion

1) Let $\mathbb{Z}_q$ be a given field. If $x^n - 1$ factorizes into a product of linear factors over $\mathbb{Z}_q$ such that $x^n - 1 = (x-1)^n$ for the number of cyclic codes in
$R_n = \frac{\mathbb{F}_q[x]}{<x^n-1>}$
is given by $n+1$.
2) Let $\mathbb{Z}_q$ be a finite field and $x^n - 1$ be a given cyclic polynomial such that $x^n - 1 = (x - x_1), (x - x_2), (x - x_3), ..., (x - x_n)$ where $x_i \neq x_j \; \forall i, j$ and suppose that $n = qm$ where $m \in \mathbb{Z}^+$ then, the number of cyclic codes in $R_n = \frac{\mathbb{F}_q[x]}{<x^n-1>}$ is given by $(q+1)^k$ where $k$ is the number of distinct factor over $\mathbb{Z}_q$
3) Let $\mathbb{Z}_q$ be a given field and $x^n - 1$ be a given cyclotomic polynomial such that $x^n - 1 = (x-1)^n$ then the number of irreducible monic polynomials over $\mathbb{Z}_q$ is not equal to the number of cyclotomic cosets.
4) Considering the factorizations done in this work and the number of cyclotomic codes generated, we see that the number of cyclic codes over $GF(23)$ is given by
n= $\begin{cases} 2^k, & if\, n23 \nmid n \\ (23+1)^k, & if\, n = 23m, m \in \mathbb{Z}^+ \\ 23^m + 1, & if\, n = 23^m, m \in \mathbb{Z}^+ \end{cases}$
where k is the number of irreducible factors for $x^n - 1$.

# Competing Interests

Authors have declared that no competing interests exist.

# References


[1] Augot, Daniel, Betti, Emanuele, Orsini, Emmanuela. An introduction to linear and cyclic codes. Gröbner Bases, Coding, and Cryptography. Springer. 2009;47-68.

[2] Dinh, Hai Q, Li, Chengju, Yue, Qin. Recent progress on weight distributions of cyclic codes over finite fields.Journal of Algebra Combinatorics Discrete Structures and Applications. 2015;2(1):39-63.

[3] Fraleigh, John B. A first course in abstract algebra; 2008.

[4] Gupta Manish, Bhullar JS, Vinocha OP. On the combination of five cyclic code. Int. J. Contemp. Math. Sciences. 2010;5(33):1627-1635.

[5] Hussein, Lao, Kivunge, Bernard, Muthoka, Geoffrey, Mwangi, Patrick. Enumeration of cyclic codes over GF (17); 2015.

[6] Kivunge, Benard Muthiani, Maganga Nyanchama Joash. Enumeration of cyclic codes over GF (19). Kenyatta University; 2017.

[7] Runji, Flora Mati. Enumeration of cyclic codes over GF (5). 2010;4(4):3241-3302.

[8] Woo, Sung Sik. Cyclic codes of length 2n over Z 4. Communications of the Korean Mathematical Society. Korean Mathematical Society. 2013;28(1):39-54.

[9] Baldoni, Maria Welleda, Ciliberto, Ciro, Cattaneo, Giulia Maria Piacentini. Elementary number theory, cryptography and codes. Springer; 2009.

[10] Olege, Fanuel. On the generators of codes of ideals of the polynomial ring for error control; 2017.

[11] Olege F, Oduor MO, Aywa S, Okaka AC. Perfect repetition codes of ideals the polynomial ring Fn 2 [x] mod (xn- 1) for error control in computer applications. Journal of Mathematics and Statistical Sciences. 2016;2016(10):579-605.

[12] Caiafa, Cesar F, Barraza, Nestor R, Proto, Araceli N. Maximum likelihood decoding on a communication channel. RPIC Reuniones en Procesamiento de la Información y Control. Rio Gallegos. 2007;728-732.

[13] Galois, Évariste, Picard, Emile. Oeuvres mathématiques d'Évariste Galois. Gauthier-Villars et fils;1897.

[14] Neubauer, Andre, Freudenberger, Jurgen, Kuhn, Volker. Coding theory: algorithms, architectures and applications. John Wiley & Sons; 2007.

[15] Rosenthal, Joachim, Shokrollahi, Mohammad Amin. Coding Theory. Oberwolfach Reports. 2008;4(4):3241-3302.

[16] Roth, Ron M. Introduction to coding theory. IET Communications. IET. 2006;47(18-19):4.

[17] West, Joel. Commercializing open science: Deep space communications as the lead market for Shannon Theory, 1960-73. Journal of Management Studies. Wiley Online Library. 2008;45(8):1506-1532.

---



***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/103549*