**Earthline Journal of Mathematical Sciences**
E-ISSN: 2581-8147
Volume 15, Number 3, 2025, Pages 419-435
https://doi.org/10.34198/ejms.15325.419435

# On Counting the Number of Cyclic Codes of Length $n$ Over Prime Fields

Pancras Onyango Ongili[1,*], Lao Hussein Mude[2], Zachary Kayiita Kaunda[3] and Kennedy Karanu Kibe[4]

[1] Department of Pure and Applied Sciences, Kirinyaga University, P. O. Box 143-10300, Kerugoya, Kenya
e-mail: opancras@gmail.com

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

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

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

### Abstract

Cyclic codes are a cornerstone of coding theory. Many studies have extensively explored specific finite prime fields, $\mathrm{GF}(p)$. However, a generalized framework for $\mathrm{GF}(p)$ remains unexplored. Previous research has enumerated cyclic codes over $\mathrm{GF}(13), \mathrm{GF}(17), \mathrm{GF}(19), \mathrm{GF}(23), \mathrm{GF}(31), \text{and } \mathrm{GF}(37)$, deriving significant findings for special cases where $n$ assumes specific forms like $n = p^m$ or $n = a^m \cdot p^m$. Despite these advances, existing studies are often restricted to individual prime fields and lack a unified framework applicable across all $\mathrm{GF}(p)$. This research develops a mathematical framework for counting cyclic codes over any prime field $\mathrm{GF}(p)$. The methodology involves the use of rigorous mathematical derivations and proofs to establish the relationship between number of cyclic codes, cyclotomic cosets and the factorization of $x^n - 1$ into irreducible polynomials over $\mathrm{GF}(p)$. This framework provides a comprehensive understanding of how the structures of $n$ and $p$ influence the number of cyclic codes. The study concludes that the number of cyclic codes, $\mathcal{N}$, over the prime fields can be expressed as $\mathcal{N} = (p^y + 1)^C$, where $C$ is derived from the number of cyclotomic cosets modulo $k \; \forall \; n = k \cdot p^y$. This work contributes to the efficient design of error-correcting codes, strengthens the theoretical foundation for secure communication systems, and bridges theoretical concepts of pure mathematics.

## 1 Introduction

Cyclic codes, a fundamental class of linear codes, are extensively studied for their applications in error correction, data transmission, and cryptography [6] [10] [1] [4] [16]. They have attracted significant attention due to their efficiency in detecting and correcting errors, as well as their structural simplicity [2]

Received: January 15, 2025; Accepted: February 17, 2025; Published: March 17, 2025

2020 Mathematics Subject Classification: 11D61.

Keywords and phrases: cyclic code enumeration, prime fields $\mathrm{GF}(p)$, cyclic code enumeration index ($\mathcal{N}$), cyclotomic cosets over $\mathrm{GF}(p)$, irreducible polynomials factorization, counting cyclic codes.

[*] Corresponding author

[5]. Much of the literature has focused on specific prime finite fields GF($p$), where $p$ is a prime, providing valuable insights into the enumeration and construction of cyclic codes. Studies on GF(13), GF(17) and GF(19) explored enumeration techniques for cases where the code length $n$ takes specific forms, such as $n = p^m$ or $n = a^m \cdot p^m$ [7] [8] [9]. These works utilized cyclotomic cosets to determine irreducible factors of $x^n - 1$, directly linking them to the generator polynomials of cyclic codes. Similarly, research on GF(23)and GF(31) advanced these techniques by highlighting the role of cyclotomic cosets in defining the number of irreducible polynomial factors of $x^n - 1$. This provided a foundational framework for deriving the number of cyclic codes for specific cases like $n = 23^m$, $n = a^m \cdot 23^m$,$n = 31^m$, and $n = a^m \cdot 31^m$ with the results showing strong dependence on the structure of $n$ and the underlying field [14] [11]. A further study on GF(37) generalized these findings for this specific field, proposing a formula $N_{\mathrm{GF}(37)} = (37^y + 1)^{C_{x^m}}$ [12]. This emphasized the deep connection between cyclotomic cosets, irreducible polynomials, and cyclic code enumeration focusing solely on GF(37). While these studies have significantly advanced the understanding of cyclic code enumeration for individual prime fields, they remain limited in scope, addressing only specific cases without offering a generalized framework applicable to all GF($p$). This gap leaves an opportunity to unify these results into a broader mathematical context, enabling enumeration of cyclic codes over any prime field. This research aims to bridge this gap by developing a comprehensive framework for counting cyclic codes over GF($p$), where $p$ is any prime. Building on the methods of cyclotomic cosets and the factorization of $x^n - 1$ into irreducible polynomials [19] [15] [17] [18] [13] [20] [3], this work derives a generalized formula for the cyclic code enumeration index $\mathcal{N}$. By connecting the structure of $n$ and $p$ to the number of cyclic codes, this study unifies existing findings while advancing mathematical understanding through methods of proof. The results contribute to the efficient design of error-correcting codes and offer new insights for secure communication systems and mathematical coding theory.

### 1.1 Definitions

1. **Cyclic Code Counting:** The process of determining the total number of distinct cyclic codes of a given length $n$ over a finite field GF($p$). This involves counting the number of unique linear subspaces of the $n$-dimensional vector space over GF($p$) that are invariant under cyclic shifts of their elements.

2. **Prime Fields GF**($p$): The simplest type of finite field, consisting of exactly $p$ elements, where $p$ is a prime number with operations defined modulo $p$.

3. **Cyclic Code Enumeration Index** ($\mathcal{N}$): This represents the total number of cyclic codes for a given length $n$ over GF($p$). It is computed based on the number of irreducible polynomial factors of $x^n - 1$ over GF($p$), which corresponds to the number of cyclotomic cosets modulo $n$.

4. **Cyclotomic Cosets over GF**($p$): The equivalence classes of integers modulo $n$ under the relation

defined by powers of $p$. Each coset is represented as:

$$C_i = \{i \cdot p^j \mod n \mid j \geq 0\},$$

where $i$ is a representative integer, and $p$ and $n$ are relatively prime. Cyclotomic cosets play a critical role in determining the irreducible factors of $x^n - 1$ over GF$(p)$.

5. **Irreducible Polynomial**: A non-constant polynomial that cannot be factored into the product of two or more non-constant polynomials with coefficients in GF$(p)$. In cyclic codes over prime fields, the irreducible polynomial factors of $x^n - 1$ over GF$(p)$ correspond to the distinct generator polynomials for the cyclic codes. These factors are determined using cyclotomic cosets modulo $n$, and each irreducible polynomial plays a key role in the overall enumeration.

# 2 Results and Discussions

This section presents a comprehensive analysis of the cyclic code enumeration index $\mathcal{N}$ over prime fields GF$(p)$ using mathematical proofs. The results derive the general formula for $\mathcal{N}$ based on cyclotomic cosets and irreducible polynomial factorization, building on the foundational concepts established in the literature. Methods of mathematical proofs are applied to establish the validity of the derived formula. These techniques ensure clarity, precision, and general applicability of the results across all prime fields GF$(p)$. The findings highlight the relationship between the structure of $n$ and $p$, as well as the number of cyclotomic cosets, in determining $\mathcal{N}$. Additionally, numerical examples are provided to validate the theoretical results and illustrate their implications in the context of cyclic code enumeration.

## 2.1 The Cyclotomic Cosets for GF$(p)$ as $p \to \infty$

**Proposition 1:** ***Enumeration of cyclotomic cosets over prime fields extend to modulo $n$ over GF$(p)$ $\forall$ $p$.***

*Proof.*
**Base Case:**
For $n = 1$, $x^n - 1 = x - 1$.

$$C_i = \{i \cdot p^j \mod 1 \mid j \geq 0\}.$$

$\implies C_0 = \{0\}$
Regardless of $p$, $C_i$ trivially holds for $n = 1$.

**Inductive Step:**
By induction, assume that it is true for some $n = k \forall\ p$ and let $n = k+1$, we show that it also holds for $k+1$.
A cyclotomic coset modulo $k+1$ is defined as:

$$C_i = \{i \cdot p^j \mod (k+1) \mid j \geq 0\}.$$

Since $i \cdot p^j \mod (k+1)$ depends on the periodic behavior of $p^j \mod (k+1)$, it suffices to show:

1. The residues $p^j \mod (k+1)$ are periodic.
2. The cosets $C_i$ are finite and distinct.
3. The union of all cosets covers all residues modulo $k+1$.

**(a) Periodicity of Residues:** By properties of modular arithmetic, $p^j \mod (k+1)$ repeats with a period determined by the order of $p$ modulo $k+1$. Let $m$ be the smallest integer such that:

$$p^m \equiv 1 \mod (k+1).$$

Then, for any $i$, $i \cdot p^j \mod (k+1)$ also repeats with period $m$.
**(b) Finiteness of Cosets:**
The size of each coset $C_i$ is $m$, the order of $p$ modulo $k+1$. Since $m$ is finite, each coset is finite.
**(c) Distinctness and Completeness:**

- ***Distinctness:*** If $C_i \cap C_j \neq \emptyset$, then $i \cdot p^a \equiv j \cdot p^b \mod (k+1)$. By the properties of modular arithmetic, this implies $i = j$, so cosets are disjoint.
- ***Completeness:*** The union of all cosets,

$$\bigcup_{i \in \mathbb{Z}_{k+1}} C_i = \mathbb{Z}_{k+1}.$$

  Clearly, this union forms the complete residue set modulo $k+1$, as every integer modulo $k+1$ is covered by some coset.

Therefore, since cyclotomic coset enumeration holds for $n = 1$, $n = k$, and $n = k+1$, then, by induction, the cyclotomic coset formula holds for all cosets modulo $n$ for any $n$ and any prime $p$. Hence, it is valid as $p \to \infty$. □

## 2.2 The Cyclic Code Enumeration Index Formula, $\mathcal{N} = (p^y + 1)^C$

Cyclic codes of length $n$ over GF($p$) correspond to the ideals of the ring:

$$R = \mathrm{GF}(p)[x]/(x^n - 1).$$

These ideals of $R$ are determined by the divisors of $x^n - 1$ in GF($p$)[$x$], which are monic irreducible polynomials over GF($p$)[$x$].
Over GF($p$), $x^n - 1$ can be factored uniquely as:

$$x^n - 1 = \prod_{f_i \in S} f_i(x),$$

where:

- $S$ is the set of all irreducible monic polynomials dividing $x^n - 1$
- Each $f_i(x)$ corresponds to a unique cyclotomic coset modulo $k$,
- $|S| = C$, the number of cyclotomic cosets modulo $k$.

**Proposition 2:** ***Any positive integer*** $n$ ***is expressible in the form:*** $n = k \cdot p^y$, ***where*** $k$ ***is coprime to*** $p$ ***and*** $y \geq 0$***.***

*Proof.*
Given that $n$ is the length of a cyclic code, and GF($p$) is a finite field of order $p$, we show that any integer $n$ can be expressed as:

$$n = k \cdot p^y,$$

where: $k$ is an integer coprime to $p$, $y \geq 0$, and $p$ is a prime.
By the fundamental theorem of arithmetic, any positive integer $n$ can be uniquely expressed as:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m},$$

where:

- $p_1, p_2, \ldots, p_m$ are distinct prime factors,
- $\alpha_1, \alpha_2, \ldots, \alpha_m$ are non-negative integers (exponents of the prime factors).

To validate this assumption, we isolate the prime $p$ and show that k is a product of prime factors. Let $p$ be one of the prime factors of $n$, specifically the characteristic prime of the field GF($p$). Separate $p^y = p^{\alpha_i}$ (where $y = \alpha_i$) from the rest of the factorization.

The remaining factors of $n$, excluding $p$, are combined to form $k$. Similarly, by mathematical fundamental theorem of arithmetic:

$$k = \prod_{i \neq \text{index of } p} p_i^{\alpha_i},$$

where $p_i$ are the other primes in the factorization of $n$,

Hence, $k$ is the product of all prime factors of $n$ except $p$, ensuring $k$ is coprime to $p$ ( $\gcd(k, p) = 1$).

Therefore, since this decomposition is unique due to the uniqueness of prime factorization, it follows that:

$$n = k \cdot p^y \quad \forall n.$$

□

**Proposition 3:** ***The number of irreducible monic polynomials $|S|$ dividing $x^n - 1$ over GF($p$) is equal to $C$, the number of cyclotomic cosets modulo $k$.***

*Proof.*

$$C_i = \{i \cdot p^j \mod k \mid j \geq 0\}.$$

Let $S$ be the set of irreducible monic polynomials $f_i(x)$ dividing $x^n - 1$ over GF($p$), each cyclotomic coset $C_i$ modulo $k$ corresponds to a unique irreducible monic polynomial $f_i(x)$ in $S$ such that:

- The roots of $f_i(x)$ are associated with the elements of $C_i$.
- The degree of $f_i(x)$ is equal to the order of $C_i$, $|C_i|$, which is the smallest $m$ such that:

$$p^m \cdot i \equiv i \mod k.$$

Thus, there is a bijective mapping between $S$ and the set of cyclotomic cosets modulo $k$.

Also, the cyclotomic cosets modulo $k$ partition the set of integers $\{0, 1, \ldots, k - 1\}$ so that:

- Every integer $i \in \{0, 1, \ldots, k - 1\}$ belongs to exactly one coset $C_i$.
- The total number of cosets, $C$, satisfies:

$$\sum_{i=0}^{C-1} |C_i| = k.$$

Since each coset $C_i$ corresponds uniquely to an irreducible monic polynomial $f_i(x)$, the total number of irreducible monic polynomials in $S$ is therefore is equal to the number of cyclotomic cosets modulo $k$. Hence, $|S| = C$. □

It follows from the proof above that the degree, deg $f_i(x) = |C_i|$. Hence,

$$\sum_{i=0}^{C-1} |C_i| = \deg(x^n - 1) = n.$$

It follows from *proposition 2*, let $n = k \cdot p^y$, the total degree becomes:

$$\sum_{i=0}^{C-1} |C_i| = k \cdot p^y.$$

In $\mathrm{GF}(p^y)$, there are $p^y$ elements, represented as linear combinations of powers of a primitive element $\alpha$:

$$\mathrm{GF}(p^y) = \{c_0 + c_1\alpha + \cdots + c_{y-1}\alpha^{y-1} \mid c_i \in \mathrm{GF}(p)\}.$$

An irreducible polynomial $f_i(x)$ of degree, say $d$ over $\mathrm{GF}(p)$, defines an ideal in $\mathrm{GF}(p^y)[x]$ such that,

$$\langle f_i(x)\rangle = \{g(x) \cdot f_i(x) \mid g(x) \in \mathrm{GF}(p^y)[x]\}.$$

So, the number of distinct polynomials $g(x)$ in $\mathrm{GF}(p^y)[x]$ that can multiply $f_i(x)$ is determined by the coefficients of $g(x)$, which are chosen from $\mathrm{GF}(p^y)$.
Thus, including $f_i(x)$ itself and its multiples in $\mathrm{GF}(p^y)[x]$, the total number of divisors generated by $f_i(x)$ is:

$$\text{Number of divisors of } f_i(x) = p^y + 1.$$

Therefore then, each irreducible polynomial $f_i(x)$ has $p^y + 1$ divisors, corresponding to its multiples. The total number of divisors of $x^n - 1$ is:

$$\mathcal{N} = \prod_{f_i \in S} (p^y + 1).$$

Since there are $C$ irreducible polynomials, the formula simplifies to:

$$\mathcal{N} = (p^y + 1)^C,$$

where $C$ is the number of cyclotomic cosets modulo $k$. This is the cyclic code enumeration index $\mathcal{N}$.

### 2.2.1 Proof by Induction:

***Lemma***
Cyclic Codes over prime fields can be enumerated by the formula $\mathcal{N} = (p^y + 1)^C$ for all $n = k \cdot p^y$, where $k$ is coprime to $p$.

*Proof.*
**Base Case:** $(n = 1)$
When $n = 1$, $k = 1$ and $p^y = 1$.
The polynomial $x^1 - 1 = x - 1$ has one irreducible monic polynomial, $f(x) = x - 1$, and one cyclotomic coset, $C_0 = \{0\}$.
Substituting into the formula:

$$\mathcal{N} = (p^y + 1)^C = (1 + 1)^1 = 2.$$

This agrees with the cyclic code enumeration index, verifying the base case.
**Inductive Hypothesis:** *Assume the formula holds for $n = k \cdot p^y$, so that*

$$\mathcal{N} = (p^y + 1)^C,$$

*where $C$ is the number of cyclotomic cosets modulo $k$.*

**Inductive Step:** $(n = (k + 1) \cdot p^y)$ Let $n = (k + 1) \cdot p^y$.
The polynomial $x^n - 1$ can be factored as:

$$x^n - 1 = \prod_{f_i \in S} f_i(x),$$

where $S$ is the set of irreducible monic polynomials dividing $x^n - 1$.
Each polynomial $f_i(x)$ corresponds to a unique cyclotomic coset modulo $k + 1$,

$$C_i = \{i \cdot p^j \mod (k + 1) \mid j \geq 0\}.$$

Thus, the total number of distinct cosets modulo $k + 1$ is $C_{k+1}$.
Also, each coset $C_i$ corresponds to an irreducible monic polynomial $f_i(x)$ of degree equal to the size of the coset $|C_i|$.
The number of divisors of each irreducible polynomial is $p^y + 1$. Thus, the total number of divisors is:

$$\mathcal{N} = (p^y + 1)^{C_{k+1}}.$$

This agrees with the cyclic code index enumeration formula, and therefore, it is sufficient to conclude that by induction, the formula:

$$\mathcal{N} = (p^y + 1)^C$$

holds for all $n = k \cdot p^y$. □

## 2.3 The Application of Cyclic Enumeration Index Formula

**Problem 1: From GF(2)**

**Problem:** *Determine the number of cyclic codes of length* $6$ *over* $\mathbb{Z}_2$*, where* $n = 6$ *is the degree of the cyclotomic polynomial* $x^6 - 1$*.*

**Solution:**

Step 1: *Identify Parameters:*

Field: $\mathbb{Z}_2$ $(p = 2)$,

Polynomial degree: $n = 6$,

Decompose $n$: $n = k \cdot p^y$, where $k = 3$ and $y = 1$.

Step 2: *Compute Cyclotomic Cosets Modulo* $k = 3$*:*

Residues modulo 3: $\{0, 1, 2\}$.

Cosets:

$$C_0 = \{0\}, \quad C_1 = \{1, 2\}.$$

Number of cosets: $C = 2$.

Step 3: *Apply the Formula:*

Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (2^1 + 1)^2 = 3^2 = 9.$$

**Answer:** There are $\mathcal{N} = 9$ cyclic codes of length 6 over $\mathbb{Z}_2$.

**Problem 2: From GF(3)**

**Problem:** *Count the number of cyclic codes of length* $9$ *over* $\mathbb{Z}_3$ *for the cyclotomic polynomial* $x^9 - 1$*.*

**Solution:**

Step 1: *Identify Parameters:*

Field: $\mathbb{Z}_3$ $(p = 3)$,

Polynomial degree: $n = 9$,

Decompose $n$: $n = k \cdot p^y$, where $k = 1$ and $y = 2$.

Step 2: *Compute Cyclotomic Cosets Modulo* $k = 1$*:*

Since $k = 1$, all residues modulo 1 collapse into a single coset:

$$C_0 = \{0\}.$$

Number of cosets: $C = 1$.
Step 3: *Apply the Formula:*
Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (3^2 + 1)^1 = 9 + 1 = 10.$$

**Answer:** There are $\mathcal{N} = 10$ cyclic codes of length 9 over $\mathbb{Z}_3$.

**Problem 3: From GF**(5)

**Problem:** *Given the cyclotomic polynomial $x^{10} - 1$, determine the number of cyclic codes of length* 10 *over $\mathbb{Z}_5$.*
**Solution:**
Step 1: *Identify Parameters:*
Field: $\mathbb{Z}_5$ ($p = 5$),
Polynomial degree: $n = 10$,
Decompose $n$: $n = k \cdot p^y$, where $k = 2$ and $y = 1$.
Step 2: *Compute Cyclotomic Cosets Modulo $k = 2$:*
Residues modulo 2: $\{0, 1\}$.
Cosets:

$$C_0 = \{0\}, \quad C_1 = \{1\}.$$

Number of cosets: $C = 2$.
Step 3: *Apply the Formula:*
Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (5^1 + 1)^2 = 6^2 = 36.$$

**Answer:** There are $\mathcal{N} = 36$ cyclic codes of length 10 over $\mathbb{Z}_5$.

**Problem 4: From GF**(7)

**Problem:** *Determine the number of cyclic codes of length* 14 *over $\mathbb{Z}_7$, where $n = 14$ is the degree of the cyclotomic polynomial $x^{14} - 1$.*

**Solution:**

Step 1: *Identify Parameters:*
Field: $\mathbb{Z}_7$ ($p = 7$),
Polynomial degree: $n = 14$,
Decompose $n$: $n = k \cdot p^y$, where $k = 2$ and $y = 1$.
Step 2: *Compute Cyclotomic Cosets Modulo $k = 2$:*
Residues modulo 2: $\{0, 1\}$.
Cosets:

$$C_0 = \{0\}, \quad C_1 = \{1\}.$$

Number of cosets: $C = 2$.
Step 3: *Apply the Formula:*
Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (7^1 + 1)^2 = 8^2 = 64.$$

**Answer:** There are $\mathcal{N} = 64$ cyclic codes of length 14 over $\mathbb{Z}_7$.

**Problem 5: From GF(11)**

**Problem:** *Determine the number of cyclic codes of length* 22 *over* $\mathbb{Z}_{11}$*, where* $n = 22$ *is the degree of the cyclotomic polynomial* $x^{22} - 1$*.*

**Solution:**

Step 1: *Identify Parameters:*
Field: $\mathbb{Z}_{11}$ ($p = 11$),
Polynomial degree: $n = 22$,
Decompose $n$: $n = k \cdot p^y$, where $k = 2$ and $y = 1$.
Step 2: *Compute Cyclotomic Cosets Modulo $k = 2$:*
Residues modulo 2: $\{0, 1\}$.
Cosets:

$$C_0 = \{0\}, \quad C_1 = \{1\}.$$

Number of cosets: $C = 2$.
Step 3: *Apply the Formula:*
Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (11^1 + 1)^2 = 12^2 = 144.$$

**Answer:** There are $\mathcal{N} = 144$ cyclic codes of length 22 over $\mathbb{Z}_{11}\}$.

**Problem 6: From GF(17)**

**Problem:** *How many cyclic codes exist for the cyclotomic polynomial $x^{68} - 1$ over GF(17)?*
**Solution:**
Step 1: *Identify Parameters:*
Field: GF(17) ($p = 17$),
Polynomial degree: $n = 68$,
Decompose $n$: $n = k \cdot p^y$, where $k = 4$ and $y = 1$.
Step 2: *Compute Cyclotomic Cosets Modulo $k = 4$:*
Residues modulo 4: $\{0, 1, 2, 3\}$.
Cosets:

$$C_0 = \{0\}, \quad C_1 = \{1\}, \quad C_2 = \{2\}, \quad C_3 = \{3\}.$$

Number of cosets: $C = 4$.
Step 3: *Apply the Formula:*
Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (17^1 + 1)^4 = 18^4 = 104976.$$

**Answer:** There are $\mathcal{N} = 104976$ cyclic codes of length 68 over GF(17)$\}$.

**Problem 7: From GF(19)**

**Problem:** *Verify the number of cyclic codes generated by the irreducible factors of $x^{361} - 1$ over GF(19).*
**Solution:**
Step 1: *Identify Parameters:*
Field: GF(19) ($p = 19$),
Polynomial degree: $n = 361$,
Decompose $n$: $n = k \cdot p^y$, where $k = 1$ and $y = 2$.
Step 2: *Compute Cyclotomic Cosets Modulo $k = 1$:*

Since $k = 1$, all residues modulo 1 collapse into a single coset:

$$C_0 = \{0\}.$$

Number of cosets: $C = 1$.
Step 3: *Apply the Formula:*
Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (19^2 + 1)^1 = 361 + 1 = 362.$$

**Answer:** There are $\mathcal{N} = 362$ cyclic codes of length 361 over GF(19).

**Problem 8: From GF**(23)

**Problem:** *Determine the total number of cyclic codes of length $n = 69$ over GF(23).*
**Solution:**
Step 1: *Identify Parameters:*
Field: GF(23) ($p = 23$),
Polynomial degree: $n = 69$,
Decompose $n$: $n = k \cdot p^y$, where $k = 3$ and $y = 1$.
Step 2: *Compute Cyclotomic Cosets Modulo $k = 3$:*
Residues modulo 3: $\{0, 1, 2\}$.
Cosets:

$$C_0 = \{0\}, \quad C_1 = \{1, 2\}.$$

Number of cosets: $C = 2$.
Step 3: *Apply the Formula:*
Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (23^1 + 1)^2 = 24^2 = 576.$$

**Answer:** There are $\mathcal{N} = 576$ cyclic codes of length 69 over GF(23).

**Problem 9: From GF**(31)

**Problem:** *Determine the number of cyclic codes of length* 62 *over GF*(31)*, where* $n = 62$ *is the degree of the cyclotomic polynomial* $x^{62} - 1$*.*

**Solution:**

Step 1: *Identify Parameters:*

Field: GF(31) ($p = 31$),

Polynomial degree: $n = 62$,

Decompose $n$: $n = k \cdot p^y$, where $k = 2$ and $y = 1$.

Step 2: *Compute Cyclotomic Cosets Modulo* $k = 2$*:*

Residues modulo 2: $\{0, 1\}$.

Cosets:

$$C_0 = \{0\}, \quad C_1 = \{1\}.$$

Number of cosets: $C = 2$.

Step 3: *Apply the Formula:*

Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (31^1 + 1)^2 = 32^2 = 1024.$$

**Answer:** There are $\mathcal{N} = 1024$ cyclic codes of length 62 over GF(31).

**Problem 10: From GF**(37)

**Problem:** *A satellite communication system requires error-correcting codes to ensure data integrity during transmission. The system operates over GF*(37) *and uses cyclic codes of length* 74*. Determine the total number of distinct cyclic codes that can be generated for this system, ensuring robust error correction and redundancy.*

**Solution:**

Step 1: *Identify Parameters:*

Field: GF(37) ($p = 37$),

Polynomial degree: $n = 74$,

Decompose $n$: $n = k \cdot p^y$, where $k = 2$ and $y = 1$.

Step 2: *Compute Cyclotomic Cosets Modulo* $k = 2$*:*

Residues modulo 2: $\{0, 1\}$.

Cosets:

$$C_0 = \{0\}, \quad C_1 = \{1\}.$$

Number of cosets: $C = 2$.

Step 3: *Apply the Formula:*

Using the cyclic code enumeration index formula:

$$\mathcal{N} = (p^y + 1)^C.$$

Substituting values:

$$\mathcal{N} = (37^1 + 1)^2 = 38^2 = 1444.$$

**Answer:** There are $\mathcal{N} = 1444$ distinct cyclic codes that can be generated for the satellite communication system.

## Conclusion

This publication presents a comprehensive exploration of the cyclic code enumeration index formula

$$\mathcal{N} = (p^y + 1)^C,$$

providing both theoretical derivation and practical verification. The derivation demonstrates how the number of cyclic codes is intricately tied to the cyclotomic cosets modulo $k$ and the properties of the finite field GF($p$). The examples of problems that can be solved by this formula highlight the practical applicability in enumerating cyclic codes efficiently and accurately, regardless of the complexity of the finite field or the decomposition of $n$. The implications of this study are significant for coding theory and its applications in secure communication systems and error correction. The formula provides a universal framework for counting cyclic codes, laying the groundwork for the reinforcement of the mathematical foundations of cyclic code enumeration, bridging theoretical concepts with practical utility, and solidifying the role of cyclotomic cosets in coding theory.

### Competing Interests

Authors have declared no competing interest.

## References

[1] Aguilar-Melchor, C., Blazy, O., Deneuville, J. C., Gaborit, P., & Zémor, G. (2018). Efficient encryption from random quasi-cyclic codes. *IEEE Transactions on Information Theory, 64*(5), 3927-3943. https://doi.org/10.1109/TIT.2018.2804444

[2] Almazrouei, K., & Alnajjar, K. A. (2024). Error-correcting codes in communication systems. *2024 International Wireless Communications and Mobile Computing (IWCMC)*, 1-6. https://doi.org/10.1109/IWCMC61514.2024.10592361

[3] Ball, S. (2020). Finite fields. *A Course in Algebraic Error-Correcting Codes*, 17-27. https://doi.org/10.1007/978-3-030-41153-4_2

[4] Baylis, D. J. (2018). *Error Correcting Codes: A Mathematical Introduction.* Routledge.

[5] Childs, L. N. (2019). *Cryptology and Error Correction.* Springer International Publishing.

[6] Dumas, J. G., Roch, J. L., Tannier, E., & Varrette, S. (2015). *Foundations of Coding: Compression, Encryption, Error Correction.* John Wiley & Sons. https://doi.org/10.1002/9781119005940

[7] Hussein, L., Kivunge, B., Kimani, P., & Muthoka, G. (2018). On the number of cyclotomic cosets and cyclic codes over $Z_{13}$. *International Journal of Scientific Research and Innovative Technology, 5*(6), 58-68.

[8] Hussein, L., Kivunge, B., Muthoka, G., & Mwangi, P. (2015). Enumeration of cyclic codes over GF(17). *International Journal of Scientific Research and Innovative Technology, 2*(5), 103-111.

[9] Maganga, B. M., & Joash, M. N. (2017). Enumeration of cyclic codes over GF(19). Kenyatta University.

[10] Mesnager, S. (2021). Linear codes from functions. *In Concise Encyclopedia of Coding Theory*, 463-526. Chapman and Hall/CRC.

[11] Ondiany, J. J. O., Karieko, O. R., Mude, L. H., & Monari, F. N. (2024). On the number of cyclic codes over $Z_{31}$. *Journal of Advances in Mathematics and Computer Science, 39*(7), 55-69. https://doi.org/10.9734/jamcs/2024/v39i71912

[12] Ongili, P., Mude, L. H., & Ndung'u, K. J. (2024). On the generalization of the number of cyclic codes over the prime field GF(37). *Journal of Advances in Mathematics and Computer Science, 39*(6), 27-42. https://doi.org/10.9734/JAMCS/2024/v39i61899

[13] Runji, F. M. (2014). Enumeration of cyclic codes over GF (5). *Express Journal, 1*(6). http://express-journal.com/pdf/june14issue6/enumerationofcycliccodesovergf(5).pdf

[14] Simatwo, K. B., Mati, R. F., & Karieko, O. R. (2023). Enumeration of cyclic codes over GF(23). *Journal of Advances in Mathematics and Computer Science, 38*(9), 194-206. https://doi.org/10.9734/jamcs/2023/v38i91815

[15] Singh, M., & Deepak. (2025). The set of representatives and explicit factorization of $x^n - 1$ over finite fields. *Journal of Algebra and Its Applications, 24*(07), 2550170. https://doi.org/10.1142/S0219498825501701

[16] Tinnirello, C. (2016). *Cyclic Codes: Low-Weight Codewords and Locators.*

[17] van Zanten, A. J. (2019). Primitive idempotent tables of cyclic and constacyclic codes. *Designs, Codes and Cryptography, 87*, 1199-1225. https://doi.org/10.1007/s10623-018-0495-0

[18] Vega, G. (2021). Explicit factorization of some period polynomials. *In Arithmetic of Finite Fields: 8th International Workshop, WAIFI 2020, Rennes, France, July 6-8, 2020, Revised Selected and Invited Papers*, 222-233. Springer International Publishing. https://doi.org/10.1007/978-3-030-68869-1_13

[19] Zhu, L., Liu, J., & Wu, H. (2024). Explicit representatives and sizes of cyclotomic cosets and their application to cyclic codes over finite fields. *arXiv preprint arXiv:2410.12122.*

[20] Zhu, L., Liu, J., & Wu, H. (2024). Cyclotomic system and their arithmetic. *arXiv preprint arXiv:2412.12455.*