Enumeration of Cyclic Codes over GF(19)

Maganga Nyanchama Joash¹, Dr. Benard M. Kivunge²

Department of Mathematics Kenyatta University P.o. Box 43844-00100, Nairobi, Kenya

Abstract: In this paper we seek the number of irreducible polynomials of \(x^n - 1\) over GF(19). First, we factorize \(x^n - 1\) into irreducible polynomials over GF(19) using cyclotomic cosets of 19 modulo \(n\). The number of irreducible polynomial factors of \(x^n - 1\) over GF(19) is equal to the number of cyclotomic cosets of 19 modulo \(n\) and each monic divisor of \(x^n - 1\) is a generator polynomial of a cyclic code in GF(19). Next, we show that the number of cyclic codes of length \(n\) over a finite field GF(19) is equal to the number of polynomials that divide \(x^n - 1\). Lastly, we enumerate the number of cyclic codes of length \(n\), for \(1 \leq n \leq 20\) and when \(n = 19k, n = 19^k\) for \(1 \leq k \leq 20\)

Keywords: Code, Cyclic Code, Cyclotomic cosets

1. Introduction

Most research carried out in Coding Theory is motivated mainly by the problem of finding codes which are optimal in some sense, and the problem of decoding such codes efficiently. The theory of error-correcting codes deals with the general problem of transmitting messages reliably. Information is sent via a channel which is prone to errors. The channel may be a telephone line, a high frequency radio link or a satellite communication link. The noise may be human error, lightning, thermal noise, imperfections in equipments, etc. The objective of an error correcting code is to encode the data by adding a certain amount of redundancy to the message, so that the original message can be recovered. Researchers therefore seek for an \((n,k,d)\)-code that transmits a wide variety of messages fast and corrects many errors; i.e. small \(n\), large \(k\), and large \(d\). These are conflicting aims and this is often referred to as the main Coding Theory problem.

1.1 Definitions

i) Code: A block code of length \(n\) is a set of \(n\)-tuples \((a_1,a_2,a_3,...,a_n)\) where the \(a_i\)'s belong to a finite set \(F\) with \(q\) symbols or digits known as alphabets. Thus a code of length \(n\) from \(F\) is an element of \(F^n\) (the set of all \(n\)-tuples from \(F\)).

ii) Cyclic Code: A linear block code is said to be a cyclic code if it is invariant under all cyclic shifts i.e. if \(a_0,a_1,a_2,...,a_n\) is a codeword, so are \(a_n,a_1,a_2,...,a_{n-1}\) and \(a_2,a_3,...,a_n,a_1\).

iii) Cyclotomic cosets: Let \(n\) be co-prime to \(q\). The cyclotomic coset of \(a mod n\) containing \(i\) is defined by

\[ C_i = \{ i, q^j n \in Z_n, j = 0,1,2,3, ... \} \]

A subset \(\{i_1,i_2, ..., i_l\}\) of \(Z_n\) is called a complete set of representatives of cyclotomic cosets of \(a mod n\) if \(C_{i_1}, C_{i_2}, ..., C_{i_l}\) are distinct and \(U_{j=1}^{l} C_{i_j} = Z_n\).

2. Preliminary Results

A cyclic code is a linear code which is invariant under any cyclic shift. In order to find the number of cyclic codes over GF(19), we factorize \(x^n - 1\) into irreducible polynomials and obtain all monic polynomials that divide \(x^n - 1\). Each monic polynomial is then a generator for a cyclic code.

2.1 Factorization of \(x^n - 1\) into irreducible polynomials over \(Z_{19}\)

Let \(n\) be a positive integer with \((q,n) = 1\). Then the number of monic irreducible polynomial factors of \(x^n - 1\) over \(F_19\) is equal to the number of cyclotomic cosets of \(q\) modulo \(n\). Now:

(a) When \(n = 1, x - 1 = x + 18\) is a linear factor.

(b) When \(n = 2\), the cyclotomic cosets of 19 mod 2 are:

\[ C_i = \{ i, 19^j mod 2, j = 0,1,2,... \} \]

\[ C_0 = \{0\}, C_1 = \{1\} \Rightarrow x^2 - 1 \text{ is a quadratic expression and so factorizes into two irreducible linear factors; } \]

\[ x^2 - 1 = (x + 1)(x - 1) = (x + 1)(x + 18) \]

(c) When \(n = 3\), the cyclotomic cosets of 19 mod 3 are:

\[ C_i = \{ i, 19^j mod 3, j = 0,1,2,... \} \]

\[ C_0 = \{0\}, C_1 = \{1\}, C_2 = \{2\} \Rightarrow x^3 - 1 \]

factorizes into three irreducible monic polynomials, all linear factors. We find an \(m\), such that \(3|(19^m - 1)\). Let \(m = 1\) so that we have \(3|18\)

\[
r = \frac{18^2 - 1}{3} = \frac{324 - 1}{3} = \frac{323}{3} = 107 = 6. \]

Next, we list all cyclotomic cosets of 19 mod 18 containing multiples of 6. These are: \(C_0 = \{0\}, C_6 = \{6\}, C_{12} = \{12\}\.

Let \(a\) be a primitive element in \(Z_{19}\) then, the minimal polynomials of \(a^x\) are:

\[
M(0)(x) = (x - a^0) = (x - 1) \]

\[
M(6)(x) = (x - a^6) = (x - 7) \]

\[
M(12)(x) = (x - a^{12}) = (x - 11) \]

Now,

\[
x^3 - 1 = M(0)(x), M(6)(x), M(12)(x) \]

\[
= (x + 1)(x - 7)(x - 11) = (x + 18)(x + 12x + 8) \]

When \(n = 4\), the cyclotomic cosets of 19 mod 4 are:

\[ C_i = \{ i, 19^j mod 4, j = 0,1,2,... \} \]

\[ C_0 = \{0\}, C_1 = \{1,3\}, C_2 = \{2\} \Rightarrow x^4 - 1 \text{ factorizes into three irreducible monic polynomials, one of degree two and other two linear factors. We shall use the Mobius and Euler functions to factorize this; } \]

\[
x^n - 1 = \prod_{d|n} \phi_d(x) \text{ where } \phi_d(x) \text{ are cyclotomic polynomials of divisors of } n. \]
The formula $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$ gives the cyclotomic polynomials of $n$. The factors of 4 are 1, 2, and 4. $\Phi_1(x) = (x - 1)^{\mu(1)} = (x - 1)$

$\Phi_2(x) = \prod_{d|2} (x^d - 1)^{\mu(n/d)} = (x - 1)^{\mu(2)}(x^2 - 1)^{\mu(1)} = (x - 1)^{-1}(x^2 - 1) = (x + 1)$

$\Phi_4(x) = \prod_{d|4} (x^d - 1)^{\mu(n/d)} = (x - 1)^{\mu(4)}(x^4 - 1)^{\mu(1)} = (x - 1)^{-1}(x^4 - 1) = (x - i\sqrt{2})(x + i\sqrt{2})(x - i\sqrt{2})(x + i\sqrt{2})$

The following factorization of $x^n - 1$ was obtained by applying the procedures as in the cases when $n = 3$ and $n = 4$ above.

When $n = 5$, the cyclotomic cosets of $19 \bmod 5$ are:

$C_0 = \{1, 6, 11, 16, 21\} \Rightarrow x^5 - 1$ factors into five irreducible monic polynomials, all linear factors; i.e.

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

When $n = 6$, the cyclotomic cosets of $19 \bmod 6$ are:

$C_0 = \{0, 1, 2, 3, 4, 5\} \Rightarrow x^6 - 1$ factors into six irreducible monic polynomials, all linear factors; i.e.

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

When $n = 7$, the cyclotomic cosets of $19 \bmod 7$ are:

$C_0 = \{0, 1, 2, 3, 4, 5, 6\} \Rightarrow x^7 - 1$ factors into seven irreducible monic polynomials, all of degree two; i.e.

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

When $n = 8$, the cyclotomic cosets of $19 \bmod 8$ are:

$C_0 = \{0, 1, 2, 3, 4, 5, 6, 7\} \Rightarrow x^8 - 1$ factors into eight irreducible monic polynomials, all of which are linear factors and three of degree two; i.e.

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

When $n = 9$, the cyclotomic cosets of $19 \bmod 9$ are:

$C_0 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} \Rightarrow x^9 - 1$ factors into nine irreducible monic polynomials, all of which are linear factors and three of degree two; i.e.

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

When $n = 10$, the cyclotomic cosets of $19 \bmod 10$ are:

$C_0 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \Rightarrow x^{10} - 1$ factors into ten irreducible monic polynomials, two of which are linear factors and four of degree two; i.e.

$x^{10} - 1 = (x^5 + 1)(x^5 - 1) = (x^5 + x^4 + x^3 + x^2 + x + 1)(x^5 - x^4 + x^3 - x^2 + x - 1)$

When $n = 11$, the cyclotomic cosets of $19 \bmod 11$ are:

$C_0 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \Rightarrow x^{11} - 1$ factors into eleven irreducible monic polynomials, one of degree ten and the other a linear factor; i.e.

$x^{11} - 1 = (x - 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x + 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$
\[ \Rightarrow x^{15} - 1 \text{ factors into nine irreducible monic polynomials, three of which are linear factors and six of degree two; i.e.} \]
\[ x^{15} - 1 = (x - 1)(x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x - 1)(x - 7x + 11x + 7x + 7x + 3 + 1 + 3 + 7 + 7 + 7 + 1) \]
\[ = (x + 18)(x + 12)(x + 8)(x^2 + 5x + 1)(x^2 + 15x + 1)(x^2 + 16x + 11)(x^2 + 13x + 7)(x^2 + 2)x + 1) + 1) \]
\[ \Rightarrow \text{factors of } x^{15} - 1 \text{ into seven irreducible monic polynomials, three of degree two, two of degree four and the other two linear factors; i.e.} \]
\[ x^{16} - 1 = (x^8 + 1)(x^8 - 1) = (x^4 + 13x^2 - 1)(x^4 + 6x^2 - 1)(x^2 + 3x + 8)(x^2 + 6x + 18)(x^2 + 1)(x + 1)(x - 1) \]
\[ = (x^4 + 13x^2 + 18)(x^4 + 6x^2 + 18)(x^2 + 13x + 18)(x^2 + 6x + 18)(x^2 + 1)(x + 1)(x - 1) \]
\[ \Rightarrow \text{factors of } x^{16} - 1 \text{ into three irreducible monic polynomials, one linear factor and two of degree eight; i.e.} \]
\[ x^{17} - 1 = (x - 1)(x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x + 18)(x^8 + 13x^7 + 15x^6 + 16x^5 + 8x^4 + 16x^3 + 15x^2 + 13x + 18x + 7x^6 + 9x^6 + 10x^5 + 15x^4 + 10x^3 + 9x^2 + 7x + 1) \]
\[ \Rightarrow \text{factors of } x^{16} - 1 \text{ into three irreducible monic polynomials, all linear factors; i.e.} \]
\[ x^{18} - 1 = (x^3 + 1)(x^3 - 1) = (x^3 - 1)(x + 15)(x + 13)(x + 12x + 10x + 8x + 3 + x + 2) \]
\[ = (x + 18)(x + 17)(x + 16)(x + 15)(x + 14)(x + 13)(x + 12x + 11x + 10x + 9x + 8x + 7x + 6x + 5x + 4x + 3x + 2x + 1) \]

When \( n = 19 \), the cyclotomic cosets of \( 19 \) mod 19 are:
\[ C_i = \{i.19^{19} \text{ mod } 19 = 0, 1, 2, \ldots, 19 \} \]
\[ C_0 = \{0\}, C_1 = \{1, 2, 3, \ldots, 18\}, C_2 = \{2, 4, 8, 16, 15, 13, 9, 3\}, C_3 = \{3, 6, 12, 7, 14, 11, 5, 10\}, \]
\[ \Rightarrow \text{factors of } x^{19} - 1 \text{ into irreducible monic polynomials over } \mathbb{Z}_{19} \text{ when } n = 19k \text{ for } 1 \leq k \leq 20 \]

2.2 Factorization of \( x^n - 1 \) into irreducible monic polynomials when \( n = 19k \) for \( 1 \leq k \leq 20 \)

a) When \( k = 1 \), we have \( n = 19 \);
\[ x^{19} - 1 = (x - 1)^{19} = (x + 18)^{19}. \]

b) When \( k = 2 \), we have \( n = 19 \times 2 = 38 \);
\[ x^{38} - 1 = (x^{19} + 1)(x^{19} - 1) = (x + 1)(x - 1)^{19}. \]

c) When \( k = 3 \), we have \( n = 19 \times 3 = 57 \);
\[ x^{57} - 1 = x^{19 \times 3} - 1 = (x^3 - 1)^{19} = (x + 18)(x + 12)(x + 8). \]

d) When \( k = 4 \), we have \( n = 19 \times 4 \);
\[ x^{76} - 1 = (x^{19} - 1)^{19} = (x^2 + 1)(x + 1)(x + 18)^{19}. \]
e) When \( k = 5 \), we have \( n = 19 \times 5 \);
\[ x^{95} - 1 = (x^5 - 1)^{19} = (x + 18)(x^2 + 5x + 1)(x^2 + 15x + 1)^{19}. \]

f) When \( k = 6 \), we have \( n = 19 \times 6 \);

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

<table>
<thead>
<tr>
<th>( n )</th>
<th>Number of irreducible factors of ( x^n - 1 )</th>
<th>Number of cyclic codes</th>
<th>( n )</th>
<th>Number of irreducible factors of ( x^n - 1 )</th>
<th>Number of cyclic codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>11</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>12</td>
<td>9</td>
<td>512</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>8</td>
<td>13</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>8</td>
<td>14</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>8</td>
<td>15</td>
<td>9</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>64</td>
<td>16</td>
<td>7</td>
<td>128</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>4</td>
<td>17</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>32</td>
<td>18</td>
<td>18</td>
<td>262,144</td>
</tr>
<tr>
<td>9</td>
<td>8</td>
<td>256</td>
<td>19</td>
<td>1</td>
<td>20</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
<td>64</td>
<td>20</td>
<td>11</td>
<td>2048</td>
</tr>
</tbody>
</table>
\[
\begin{align*}
x^6 \cdot 19 - 1 &= (x^6 - 1)^{19} \\
&= (x + 1)(x + 2)(x + 3)(x + 4)(x + 5)(x + 6) \\
g) \text{ When } k = 7, \text{ we have } n = 19 \times 7: \\
x^{7 \cdot 19} - 1 &= (x^7 - 1)^{19} = (x + 1)(x^2 + x^5 + x^4 + x^3 + x^2 + 1)^{19} \\
h) \text{ When } k = 8, \text{ we have } n = 19 \times 8: \\
x^{8 \cdot 19} - 1 &= (x^8 - 1)^{19} = (x^2 + 3x + 18)(x^2 + 6x + 18)(x^2 + 1)(x + 19)^{19} \\
i) \text{ When } k = 9, \text{ we have } n = 19 \times 9: \\
x^{9 \cdot 19} - 1 &= (x^9 - 1)^{19} = (x + 18)(x + 15)(x + 14)(x + 13x + 12x^2 + 10x + 8x + 3(x^2 + 2))^{19} \\
j) \text{ When } k = 10, \text{ we have } n = 19 \times 10: \\
x^{10 \cdot 19} - 1 &= (x^10 - 1)^{19} \\
k) \text{ When } k = 11, \text{ we have } n = 19 \times 11: \\
x^{11 \cdot 19} - 1 &= (x^{11} - 1)^{19} \\
l) \text{ When } k = 12, \text{ we have } n = 19 \times 12: \\
x^{12 \cdot 19} - 1 &= (x^{12} - 1)^{19} \\
m) \text{ When } k = 13, \text{ we have } n = 19 \times 13: \\
x^{13 \cdot 19} - 1 &= (x^{13} - 1)^{19} \\
n) \text{ When } k = 14, \text{ we have } n = 19 \times 14: \\
x^{14 \cdot 19} - 1 &= (x^{14} - 1)^{19} \\
o) \text{ When } k = 15, \text{ we have } n = 19 \times 15: \\
x^{15 \cdot 19} - 1 &= (x^{15} - 1)^{19} \\
p) \text{ When } k = 16, \text{ we have } n = 19 \times 16: \\
x^{16 \cdot 19} - 1 &= (x^{16} - 1)^{19} \\
q) \text{ When } k = 17, \text{ we have } n = 19 \times 17: \\
x^{17 \cdot 19} - 1 &= (x^{17} - 1)^{19} \\
r) \text{ When } k = 18, \text{ we have } n = 19 \times 18: \\
x^{18 \cdot 19} - 1 &= (x^{18} - 1)^{19} \\
s) \text{ When } k = 19, \text{ we have } n = 19 \times 19: \\
x^{19 \cdot 19} - 1 &= (x^{19} - 1)^{19}
\end{align*}
\]

2.2 Factorization of \(x^n - 1\) into irreducible monic polynomials over \(\mathbb{Z}_{19}\) when \(n = 19^k\) for \(1 \leq k \leq 20\)

1) When \(k = 1\), we have \(n = 19; x^{19^1} - 1 = (x - 1)^{19^1} = (x + 18)^{19^1}\).
2) When \(k = 2\), we have \(n = 19^2; x^{19^2} - 1 = (x - 1)^{19^2} = (x + 18)^{19^2}\).
3) When \(k = 3\), we have \(n = 19^3; x^{19^3} - 1 = (x - 1)^{19^3} = (x + 18)^{19^3}\).
4) When \(k = 4\), we have \(n = 19^4; x^{19^4} - 1 = (x - 1)^{19^4} = (x + 18)^{19^4}\).
5) When \(k = 5\), we have \(n = 19^5; x^{19^5} - 1 = (x - 1)^{19^5} = (x + 18)^{19^5}\).

Clearly, we can infer that \(x^{19^k} - 1 = (x - 1)^{19^k}\).

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

\[(k_1 + 1)(k_2 + 1)(k_3 + 1) \ldots (k_m + 1) = \prod_{i=1}^{m}(k_i + 1)\]

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

<table>
<thead>
<tr>
<th>(k)</th>
<th>(n = 19^k)</th>
<th>No of codes</th>
<th>(n = 19^k)</th>
<th>No of codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>19</td>
<td>20 = 19 + 1</td>
<td>19</td>
<td>20 = 19^1 + 1</td>
</tr>
<tr>
<td>2</td>
<td>38</td>
<td>400 = (19 + 1)^2</td>
<td>19^2</td>
<td>19^2 + 1</td>
</tr>
<tr>
<td>3</td>
<td>57</td>
<td>8000 = (19 + 1)^3</td>
<td>19^3</td>
<td>19^3 + 1</td>
</tr>
<tr>
<td>4</td>
<td>76</td>
<td>8000 = (19 + 1)^4</td>
<td>19^4</td>
<td>19^4 + 1</td>
</tr>
<tr>
<td>5</td>
<td>95</td>
<td>8000 = (19 + 1)^5</td>
<td>19^5</td>
<td>19^5 + 1</td>
</tr>
<tr>
<td>6</td>
<td>114</td>
<td>20^6 = (19 + 1)^6</td>
<td>19^6</td>
<td>19^6 + 1</td>
</tr>
<tr>
<td>7</td>
<td>133</td>
<td>400 = (19 + 1)^7</td>
<td>19^7</td>
<td>19^7 + 1</td>
</tr>
<tr>
<td>8</td>
<td>152</td>
<td>20^5 = (19 + 1)^8</td>
<td>19^8</td>
<td>19^8 + 1</td>
</tr>
<tr>
<td>9</td>
<td>171</td>
<td>20^6 = (19 + 1)^9</td>
<td>19^9</td>
<td>19^9 + 1</td>
</tr>
<tr>
<td>10</td>
<td>190</td>
<td>20^6 = (19 + 1)^10</td>
<td>19^10</td>
<td>19^10 + 1</td>
</tr>
<tr>
<td>11</td>
<td>209</td>
<td>400 = (19 + 1)^11</td>
<td>19^11</td>
<td>19^11 + 1</td>
</tr>
<tr>
<td>12</td>
<td>228</td>
<td>20^7 = (19 + 1)^12</td>
<td>19^12</td>
<td>19^12 + 1</td>
</tr>
<tr>
<td>13</td>
<td>247</td>
<td>400 = (19 + 1)^13</td>
<td>19^13</td>
<td>19^13 + 1</td>
</tr>
<tr>
<td>14</td>
<td>266</td>
<td>20^8 = (19 + 1)^14</td>
<td>19^14</td>
<td>19^14 + 1</td>
</tr>
<tr>
<td>15</td>
<td>285</td>
<td>20^7 = (19 + 1)^15</td>
<td>19^15</td>
<td>19^15 + 1</td>
</tr>
<tr>
<td>16</td>
<td>304</td>
<td>20^7 = (19 + 1)^16</td>
<td>19^16</td>
<td>19^16 + 1</td>
</tr>
<tr>
<td>17</td>
<td>323</td>
<td>8000 = (19 + 1)^17</td>
<td>19^17</td>
<td>19^17 + 1</td>
</tr>
<tr>
<td>18</td>
<td>342</td>
<td>20^8 = (19 + 1)^18</td>
<td>19^18</td>
<td>19^18 + 1</td>
</tr>
<tr>
<td>19</td>
<td>361</td>
<td>362 = 19^2 + 1</td>
<td>19^19</td>
<td>19^19 + 1</td>
</tr>
<tr>
<td>20</td>
<td>380</td>
<td>20^11 = (19 + 1)^20</td>
<td>19^20</td>
<td>19^20 + 1</td>
</tr>
</tbody>
</table>

Volume 6 Issue 4, April 2017

www.ijsr.net
Licensed Under Creative Commons Attribution CC BY

Paper ID: ART20172199
DOI: 10.21275/ART20172199

582
3. Conclusion

Considering the above factorizations and number of cyclic codes generated, we see that the number of cyclic codes over \( \mathbb{Z}_{19} \) is given by:

\[
    n = \begin{cases} 
    2^k & \text{if } n \text{ divides } 19 \text{ } n \\
    (19 + 1)^k & \text{if } n = 19m, m \in \mathbb{Z}^+ \\
    19^m + 1 & \text{if } n = 19^m, m \in \mathbb{Z}^+
    \end{cases}
\]

where \( k \) is the number of irreducible factors of \( x^n - 1 \).

Generally,

Let \( \mathbb{Z}_q \), \( q \)-prime, be a given field, and \( R_n = \mathbb{F}_q[x]/(x^n - 1) \).

i) If \( n = mq, m \in \mathbb{Z}^+ \), then the number of cyclic codes of length \( n \) is \( (q + 1)^k \) where \( k \) is the number of cyclotomic cosets of \( q \) mod \( n \).

ii) If \( x^n - 1 \) factorizes into a product of irreducible factors \( f_1(x)f_2(x)f_3(x) \ldots f_m(x) \), none of which is repeated, then the number of cyclic codes of length \( n \) is \( 2^m \).

iii) If \( x^n - 1 \) factorizes into a product of linear factors over \( \mathbb{Z}_q \) such that \( x^n - 1 = (x - 1)^n \) then the number of cyclic codes in \( R_n \) is \( n + 1 \).

iv) If \( n = mq, m \in \mathbb{Z}^+ \), then the number of irreducible factors of \( x^n - 1 \) is equal to the number of cyclotomic cosets of \( q \) mod \( m \).

References


