International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Enumeration of Cyclic Codes over $GF(19)$

Maganga Nyanchama Joash[1], Dr. Benard M. Kivunge[2]

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 $1 \le n \le 20$ and when $n = 19k$, $n = 19^k$ for $1 \le k \le 20$***

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 $(a_1, a_2, a_3, \dots, a_n)$ 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 $a_0, a_1, a_2, \dots, a_n$ is a codeword, so are $a_n, a_1, a_2, \dots, a_{n-1}$ and $a_2, a_3, \dots, a_n, a_1$
iii) Cyclotomic cosets: Let n be co-prime to q. The cyclotomic coset of $q \bmod n$ containing i is defined by

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

A subset $\{i_1, i_2 \dots, i_t\}$ of $\mathbb{Z}_n$ is called a complete set of representatives of cyclotomic cosets of $q \bmod n$ if $C_{i_1}, C_{i_2}, \dots, C_{i_t}$ are distinct and $\bigcup_{j=1}^{t} C_{i_j} = \mathbb{Z}_n$.

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 $GF(q)$, 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 $\mathbb{Z}_{19}$

Let n be a positive integer with $(q, n) = 1$. Then the number of monic irreducible polynomial factors of $x^n - 1$ over F_q 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 $19 \bmod 2$ are: $C_i = \{i.19^j \bmod 2 \ j = 0,1,2, \dots\}$
$C_0 = \{0\}$, $C_1 = \{1\} \Rightarrow x^2 - 1$ 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 $19 \bmod 3$ are: $C_i = \{i.19^j \bmod 3 \ j = 0,1,2, \dots\}$
$C_o = \{0\}$, $C_1 = \{1\}$, $C_2 = \{2\}$, $\Rightarrow x^3 - 1$.
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 $3|18$

$$r = \frac{q^m - 1}{n} = \frac{19^1 - 1}{3} = \frac{18}{3} = 6.$$

Next, we list all cyclotomic cosets of $19 \bmod 18$ containing multiples of 6. These are: $C_0 = \{0\}$, $C_6 = \{6\}$, $C_{12} = \{12\}$. Let α be a primitive element in $\mathbb{Z}_{19}$ then, the minimal polynomials of α^i are:

$$M^{(0)}(x) = (x - \alpha^0) = (x - 1)$$
$$M^{(6)}(x) = (x - \alpha^6) = (x - 7)$$
$$M^{(12)}(x) = (x - \alpha^{12}) = (x - 11)$$

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 $19 \bmod 4$ are: $C_i = \{i.19^j \bmod 4 \ j = 0,1,2, \dots\}$
$C_0 = \{0\}$, $C_1 = \{1,3\}$, $C_2 = \{2\}$, $\Rightarrow x^4 - 1$ 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.
$x^n - 1 = \prod_{d|n} \Phi_d(x)$ where $\Phi_d(x)$ are cyclotomic polynomials of divisors of n.

The formula $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu\left(\frac{n}{d}\right)}$ gives the cyclotomic polynomials of n. The factors of 4 are $1, 2\ and\ 4$. $\Phi_1(x) = (x^1 - 1)^{\mu\left(\frac{1}{1}\right)} = (x - 1)$

$\Phi_2(x) = \prod_{d|2}(x^d - 1)^{\mu\left(\frac{2}{d}\right)} = (x^1 - 1)^{\mu\left(\frac{2}{1}\right)}(x^2 - 1)^{\mu\left(\frac{2}{2}\right)}$
$(x - 1)^{-1}(x^2 - 1) = (x + 1)$

$\Phi_4(x) = \prod_{d|4}(x^d - 1)^{\mu\left(\frac{4}{d}\right)} = (x^1 - 1)^{\mu\left(\frac{4}{1}\right)}(x^2 - 1)^{\mu\left(\frac{4}{2}\right)}(x^4 -$
1μ44

$= (x - 1)^0(x^2 - 1)^{-1}(x^4 - 1) = (x^2 + 1)$

$x^4 - 1 = \prod_{d|4}\Phi_d(x) = \Phi_1(x)\Phi_2(x)\Phi_4(x) = (x - 1)(x + 1)(x^2 + 1) = (x + 18)(x + 1)(x^2 + 1)$

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

When $n = 5$, the cyclotomic cosets of $19\ mod\ 5$ are:
$C_i = \{i.19^j\ mod\ 5\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1,4\},\ C_2 = \{2,3\},\ \Rightarrow x^5 - 1$ factorizes into three irreducible monic polynomials, one linear factor and two of degree two; i.e.

$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1) = (x - 1)(x^2 +$
5x+1(x2+15x+1)=x+18x2+5x+1x2+15x+1.

When $n = 6$, the cyclotomic cosets of $19\ mod\ 6$ are:
$C_i = \{i.19^j\ mod\ 6\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1\},\ C_2 = \{2\},\ C_3 = \{3\}, C_4 = \{4\}, C_5 = \{5\} \Rightarrow x^6 - 1$
factorizes into six irreducible monic polynomials, all linear factors; i.e.

$x^6 - 1 = (x^3 + 1)(x^3 - 1 = (x^3 + 1)(x + 8)(x + 12)(x +$
18=x−8x−12x−18x+8x+12x+18=x+11x+7x+1x+8x+12x+18

When $n = 7$, the cyclotomic cosets of $19\ mod\ 7$ are:
$C_i = \{i.19^j\ mod\ 7\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1,5,4,6,2,3\} \Rightarrow x^7 - 1$ factorizes into two irreducible monic polynomials, one of degree six and the other a linear factor; i.e.

$x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x + 18)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$

When $n = 8$, the cyclotomic cosets of $19\ mod\ 8$ are:
$C_i = \{i.19^j\ mod\ 8\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1,3\},\ C_2 = \{2,6\}, C_4 = \{4\}, C_5 = \{5,7\}$
$\Rightarrow x^8 - 1$
Factorizes into five irreducible monic polynomials, two of which are linear factors and three of degree two; i.e.

$x^8 - 1 = (x^4 + 1)(x^4 - 1) = (x^4 + 1)(x^2 + 1)(x^2 - 1)$
$= (x^4 + 1)(x^2 + 1)(x + 1)(x - 1)$
$= (x^2 + 13x - 1)(x^2 + 6x - 1)(x^2 + 1)(x + 1)(x - 1)$
$= (x^2 + 13x + 18)(x^2 + 6x + 18)(x^2 + 1)(x + 18)(x +$
1.

When $n = 9$, the cyclotomic cosets of $19\ mod\ 9$ are:
$C_i = \{i.19^j\ mod\ 9\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1\},\ C_2 = \{2\},\ C_3 = \{3\}, C_4 = \{4\}, C_5 = \{5\},\ C_6 = \{6\},\ C_7 = \{7\}, C_8 = \{8\} \Rightarrow x^9 - 1$ factorizes into eight irreducible monic polynomials, all linear factors; i.e.

$x^9 - 1 = (x - 1)(x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x - 1)(x - 4)(x - 5)(x - 6)(x - 7)(x - 9)(x - 11)(x - 16)(x - 17) = (x + 18)(x + 15)(x + 14)(x + 13)(x + 12)(x + 10)(x + 8)(x + 3)(x + 2)$

When $n = 10$, the cyclotomic cosets of $19\ mod\ 10$ are:
$C_i = \{i.19^j\ mod\ 10\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1,9\},\ C_2 = \{2,8\}, C_3 = \{3,7\}, C_4 = \{4,6\}, C_5 = \{5\}$
$\Rightarrow x^{10} - 1$ factorizes into six irreducible monic polynomials, two of which are linear factors and four of degree two; i.e.

$x^{10} - 1 = (x^5 + 1)(x^5 - 1) = (x^5 + 1)(x - 1)(x^2 +$
5x+1(x2+15x+1)
$= (x + 1)(x^4 - x^3 + x^2 - x + 1)(x + 18)(x^2 +$
5x+1x2+15x+1
$= (x + 1)(x^2 + 4x + 1)(x^2 + 14x + 1)(x +$
18x2+5x+1(x2+15x+1)
$= (x + 1)(x + 18)(x^2 + 4x + 1)(x^2 + 14x +$
1x2+5x+1x2+15x+1

When $n = 11$, the cyclotomic cosets of $19\ mod\ 11$ are:
$C_i = \{i.19^j\ mod\ 11\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1,8,9,6,4,10,3,2,5,7\} \Rightarrow x^{11} -$ 1 factorizes into two irreducible monic polynomials, one of degree ten and the other a linear factor; i.e.

$x^{11} - 1 = (x - 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x + 18)(x^{10} + x^9 + x^8 + x^7 + x^6 +$
x5+x4+x3+x2+x+1

When $n = 12$, the cyclotomic cosets of $19\ mod\ 12$ are:
$C_i = \{i.19^j\ mod\ 12\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1,7\},\ C_2 = \{2\}, C_3 = \{3,9\}, C_4 = \{4\}, C_5 = \{5,11\},\ C_6 = \{6\}, C_8 = \{8\}, C_{10} = \{10\}$
$\Rightarrow x^{12} - 1$ factorizes into nine irreducible monic polynomials, six of which are linear factors and three of degree two; i.e.

$x^{12} - 1 = (x^6 + 1)(x^6 - 1) = (x^6 + 1)(x + 11)(x +$
7x+1x+8x+12x+18=(x2+1)(x4−x2+1)x+11x+7x+1x+8x+12x+18=(x2+1)(x2+7)(x2+11)x+11x+7x+1x+8x+12x+18

When $n = 13$, the cyclotomic cosets of $19\ mod\ 13$ are:
$C_i = \{i.19^j\ mod\ 13\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1,,6,10,8,9,2,12,7,3,5,4,11\} \Rightarrow x^{13} -$ 1 factorizes into two irreducible monic polynomials, one of degree twelve and the other a linear factor; i.e.

$x^{13} - 1 = (x - 1)(x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$
$= (x + 18)(x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$

When $n = 14$, the cyclotomic cosets of $19\ mod\ 14$ are:
$C_i = \{i.19^j\ mod\ 14\ \ j = 0,1,2, \dots\}$
$C_0 = \{0\},\ C_1 = \{1,5,11,13,9,3\}, C_2 = \{2,10,8,12,4,6\},\ C_7 = \{7\}$
$\Rightarrow x^{14} - 1$ factorizes into four irreducible monic polynomials, two of degree six and the other two linear factors; i.e.

$x^{14} - 1 = (x^7 + 1)(x^7 - 1)$
$= (x + 1)(x^6 - x^5 + x^4 - x^3 + x^2 - x + 1)(x + 18)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$

When $n = 15$, the cyclotomic cosets of $19\ mod\ 15$ are:
$C_i = \{i.19^j\ mod\ 15\ \ j = 0,1,2, \dots\}$

$C_0 = \{0\},\ C_1 = \{1,4\},\ C_2 = \{2,8\}, C_3 = \{3,12\}, C_5 = \{5\}, C_6 = \{6,9\},\quad C_7 = \{7,13\}, C_{10} = \{10\}, C_{11} = \{11,14\}$

$\Rightarrow x^{15} - 1$ factorizes 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−11x4+x3+x2+x+1x8+x7+x5+x4+x3−x+1

$= (x-1)(x-7)(x-11)(x^2+5x+1)(x^2+15x+1)(x^2+16x+11)(x^2+13x+7)(x^2+17x+7)(x^2+10x+11)$

$= (x+18)(x+12)(x+8)(x^2+5x+1)(x^2+15x+1)(x^2+16x+11)(x^2+13x+7)(x^2+17x+7)(x^2+10x+11)$

When $n = 16$, the cyclotomic cosets of $19\ mod\ 16$ are: $C_i = \{i.19^j\ mod\ 16\ \ j = 0,1,2,\dots\}$

$C_0 = \{0\},\ C_1 = \{1,3,9,11\},\ C_2 = \{2,6\},\ C_4 = \{4,12\}\ C_5 = \{5,15,13,7\},\ C_8 = \{8\},\ C_{10} = \{10,14\}$

$\Rightarrow x^{16} - 1$ factorizes into seven irreducible monic polynomials, three of degree two, two of degree four and the other two linear factors; i.e.

$x^{16} - 1 = (x^8+1)(x^8-1)$

$= (x^4 + 13x^2 - 1)(x^4 + 6x^2 - 1)(x^2 + 13x + 18)(x^2 + 6x + 18)(x^2 + 1)(x+1)(x-1)$

$= (x^4 + 13x^2 + 18)(x^4 + 6x^2 + 18)(x^2 + 13x + 18)(x^2 + 6x + 18)(x^2 + 1)(x+1)(x+18)$

When $n = 17$, the cyclotomic cosets of $19\ mod\ 17$ are: $C_i = \{i.19^j\ mod\ 17\ \ j = 0,1,2,\dots\}$

$C_0 = \{0\},\ C_1 = \{1,2,4,8,16,15,13,9\},\ C_3 = \{3,6,12,7,14,11,5,10\},$

$\Rightarrow x^{17} - 1$ factorizes into three irreducible monic polynomials, one linear factor and two of degree eight; i.e.

$x^{17} - 1 = (x-1)(x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x+18)(x^8 + 13x^7 + 15x^6 + 16x^5 + 8x^4 + 16x^3 +$
15x2+13x+1x8+7x7+9x6+10x5+15x4+10x3+9x2+7x+1

When $n = 18$, the cyclotomic cosets of $19\ mod\ 18$ are: $C_i = \{i.19^j\ mod\ 18\ \ j = 0,1,2,\dots\}$

$C_0 = \{0\},\ C_1 = \{1\},\ C_2 = \{2\},\ C_3 = \{3\}, C_4 = \{4\}, C_5 = \{5\},\ C_6 = \{6\},\ C_7 = \{7\}, C_8 = \{8\}, C_9 = \{9\},\ C_{10} = \{10\},\ C_{11} = \{11\},\ C_{12} = \{12\}, C_{13} = \{13\},\ C_{14} = \{14\}, C_{15} = \{15\},\ C_{16} = \{16\},\ C_{17} = \{17\} \Rightarrow x^9 - 1$ factorizes into eighteen irreducible monic polynomials, all linear factors; i.e.

$x^{18} - 1 = (x^9+1)(x^9-1)$

$= (x^9-1)(x+18)(x+15)(x+14)(x+13)(x+$
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: $C_i = \{i.19^j\ mod\ 19\ \ j = 0,1,2,\dots\}$

$C_0 = \{0\},\ C_1 = \{1,0\},\ C_2 = \{2,0\},\ C_3 = \{3,0\}, C_4 = \{4,0\}, C_5 = \{5,0\},\ C_6 = \{6,0\},\ C_7 = \{7,0\}, C_8 = \{8,0\}, C_9 = \{9,0\},\ C_{10} = \{10,0\},\ C_{11} = \{11,0\},\ C_{12} = \{12,0\},\ C_{13} = \{13,0\}, C_{14} = \{14,0\}, C_{15} = \{15,0\},\ C_{16} = \{16,0\},\ C_{17} = \{17,0\}$

$C_{18} = \{18,0\}$

$\Rightarrow x^{19} - 1$ factorizes into nineteen irreducible monic polynomials; i.e.

$x^{19} - 1 = (x-1)^{19} = (x+18)^{19}$.

When $n = 20$, the cyclotomic cosets of $19\ mod\ 20$ are: $C_i = \{i.19^j\ mod\ 20\ \ j = 0,1,2,\dots\}$

$C_0 = \{0\},\ C_1 = \{1,19\},\ C_2 = \{2,18\}, C_3 = \{3,17\}, C_4 = \{4,16\}, C_5 = \{5,15\}, C_6 = \{6,14\}, C_7 = \{7,13\}, C_8 = \{8,12\}, C_9 = \{9,11\}, C_{10} = \{10\}$

$\Rightarrow x^{20} - 1$ factorizes into eleven irreducible monic polynomials, two of which arelinear factors and nine of degree two; i.e.

$x^{20} - 1 = (x^{10}+1)(x^{10}-1)$

$= (x+1)(x+18)(x^2+1)(x^2+8x+1)(x^2+13x+$
1x2+11x+1x2+6x+1x2+4x+1x2+14x+1x2+5x+1x2+15x+1.

The number of cyclic codes is summarized in the table below

N	Number of irreducible factors of $x^n - 1$	Number of cyclic codes		n	Number of irreducible factors of $x^n - 1$	Number of Cyclic codes
1	1	2		11	2	4
2	2	4		12	9	512
3	3	8		13	2	4
4	3	8		14	4	16
5	3	8		15	9	512
6	6	64		16	7	128
7	2	4		17	3	8
8	5	32		18	18	262,144
9	8	256		19	1	20
10	6	64		20	11	2048

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

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 × 2 = 38;
$x^{38} - 1 = (x^{19}+1)(x^{19}-1) = ((x+1)(x-1))^{19}$.

c) When k = 3, we have n = 19 × 3 = 57;
$x^{57} - 1 = x^{3\times19} - 1 = (x^3-1)^{19} = ((x+18)(x+12)(x+8))^{19}$

d) When $k = 4$, we have $n = 19 \times 4$;
$x^{4\times19} - 1 = (x^4-1)^{19} = ((x^2+1)(x+1)(x+18))^{19}$

e) When $k = 5$, we have $n = 19 \times 5$;
$x^{5\times19} - 1 = (x^5-1)^{19} = ((x+18)(x^2+5x+1)(x^2+$
15x+1)19

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

$$x^{6\times19}-1=(x^6-1)^{19}$$
$$=((x+11)(x+7)(x+1)(x+8)(x+12)(x+18))^{19}$$

g) When $k=7$, we have $n=19\times7$;
$$x^{7\times19}-1=(x^7-1)^{19}=((x+18)(x^6+x^5+x^4+x^3+x2+x+1))19$$

h) When $k=8$, we have $n=19\times8$;
$$x^{8\times19}-1=(x^8-1)^{19}$$
$$=((x^2+13x+18)(x^2+6x+18)(x^2+1)(x+18)(x+1))^{19}$$

i) When $k=9$, we have $n=19\times9$;
$$x^{9\times19}-1=(x^9-1)^{19}=((x+18)(x+15)(x+14)(x+13x+12x+10x+8x+3(x+2))19$$

j) When $k=10$, we have $n=19\times10$;
$$x^{10\times19}-1=(x^{10}-1)^{19}$$
$$=((x+1)(x+18)(x^2+4x+1)(x^2+14x+1)(x^2+5x+1)(x^2+15x+1))^{19}$$

k) When $k=11$, we have $n=19\times11$;
$$x^{11\times19}-1=(x^{11}-1)^{19}$$
$$=((x+18)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1))^{19}$$

l) When $k=12$, we have $n=19\times12$;
$$x^{12\times19}-1=(x^{12}-1)^{19}$$
$$=((x^2+1)(x^2+7)(x^2+11)(x+11)(x+7)(x+1)(x+8x+12x+18)19.$$

m) When $k=13$, we have $n=19\times13$;
$$x^{13\times19}-1=(x^{13}-1)^{19}$$
$$=((x+18)(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1))^{19}$$

n) When $k=14$, we have $n=19\times14$;
$$x^{14\times19}-1=(x^{14}-1)^{19}$$
$$=((x+1)(x^6-x^5+x^4-x^3+x^2-x+1)(x+18)(x^6+x^5+x^4+x^3+x^2+x+1))^{19}$$

o) When $k=15$, we have $n=19\times15$;
$$x^{15\times19}-1=(x^{15}-1)^{19}$$
$$=((x^4+13x^2+18)(x^4+6x^2+18)(x^2+13x+18)(x^2+6x+18)(x^2+1)(x+1)(x+18))^{19}$$

p) When $k=16$, we have $n=19\times16$;
$$x^{3\times19}-1=(x^3-1)^{19}$$
$$=((x^4+13x^2+18)(x^4+6x^2+18)(x^2+13x+18)(x^2+6x+18)(x^2+1)(x+1)(x+18))^{19}$$

q) When $k=17$, we have $n=19\times17$;
$$x^{17\times19}-1=(x^{17}-1)^{19}$$
$$=((x+18)(x^8+13x^7+15x^6+16x^5+8x^4+16x^3+15x^2+13x+1)(x^8+7x^7+9x^6+10x^5+15x^4+10x^3+9x^2+7x+1))^{19}$$

r) When $k=18$, we have $n=19\times18$;
$$x^{18\times19}-1=(x^{18}-1)^{19}$$
$$=((x+18)(x+17)(x+16)(x+15)(x+14)(x+13x+12x+11x+10x+9x+8x+7x+6x+5x+4x+3x+2x+1)19.$$

s) When $k=19$, we have $n=19\times19$;
$$x^{19\times19}-1=(x^{19}-1)^{19}$$
$$=((x+18)^{19})^{19}$$

t) When $k=20$, we have $n=19\times20$;
$$x^{20\times19}-1=(x^{20}-1)^{19}$$
$$=((x+1)(x+18)(x^2+1)(x^2+8x+1)(x^2+13x+1x2+11x+1x2+6x+1x2+4x+1x2+14x+1x2+5x+1x2+15x+1)19.$$

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

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

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

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

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:

$$n = \begin{cases} 2^k & if\ n\ 19 \nmid n \\ (19+1)^k & if\ n = 19m, m \in \mathbb{Z}^+ \\ 19^m + 1 & if\ n = 19^m, m \in \mathbb{Z}^+ \end{cases}$$

where k is the number of irreducible factors of $x^n - 1$.

Generally,

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

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 $f_1(x)f_2(x)f_3(x) \dots f_m(x)$ 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

[1] Arnold, A., & Monagan, M. (2011). Calculating cyclotomic polynomials. *Mathematics of Computation*, *80*(276), 2359–2379.
[2] Bamunoba, A. (2011). *Cyclotomic Polynomials*. London: Oxford.
[3] Berlekamp, E. (1968). *Algebraic Coding Theory*. New York, USA: McGraw-Hill Book company.
[4] Bierbrauer, J. (2004). *Introduction to Coding Theory*. Chapman & Hall/CRC.
[5] Blake, I. F. (1972). Codes over certain rings. *Information and Control*, *20*(4), 396–404.
[6] Dineva, R. (2005). The Euler Totient, the Möbius and the Divisor Functions. *Mount Holyoke College*. Retrieved from https://www.mtholyoke.edu/~robinson/reu/reu05/rdineva1.pdf
[7] Hill, R. (1986). *A first course in coding theory*. Oxford: Claredon Press.
[8] Pellikaan, R., Wu, X.-W., Bulygin, S., & Jurrius, R. (2012). *Error-correcting codes and cryptology*. Citeseer. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.459.30&rep=rep1&type=pdf
[9] Pretzel, O. (1992). *Error correcting codes and finite fields*. Oxford: Claredon Press.
[10] Roth, R. (2006). *Introduction to Coding Theory*. New York, USA: Cambridge University Press.
[11] Runji, S. (2010). *Enumeration of cyclic codes over GF(5)*. Kenyatta University, Nairobi, Kenya.
[12] Sala, M., Sakata, S., Mora, T., Traverso, C., & Perret, L. (Eds.). (2009). *Gröbner Bases, Coding, and Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://link.springer.com/10.1007/978-3-540-93806-4
[13] Seres, I. (1965). Irreducibility of polynomials. *Journal of Algebra*, *2*(3), 283–286.
[14] Spiegel, E. (1978). Codes over $\mathbb{Z}_m$, revisited. *Information and Control*, *37*(1), 100–104.
[15] Thangadurai, R. (2007). Irreducibility of polynomials whose coefficients are integers. *Mathematics Newsletter (RMS, India)*, *17*, 29–37