On the Number of Cyclotomic Cosets and Cyclic Codes over $\mathbb{Z}_{13}$

Lao Hussein[1], Benard Kivunge[2], Patrick Kimani[3], Geoffrey Muthoka[4]

[1,3]Department of Mathematics and Computer Science University of Kabianga

P.O. Box 2030- 00200 Kericho, Kenya

Email of the corresponding author: hlao@kabianga.ac.ke

[2]Department of Pure and Applied Mathematics Kenyatta University

P.O. Box 43844-00100 Nairobi, Kenya

[4]Department of Pure and Applied Sciences, Kirinyaga University

P.O. Box 143-10300 ,Kerugoya, Kenya

Abstract

Let $\mathbb{Z}_q$ be a finite field with q element and $x^n - 1$ be a given cyclotomic polynomial. The number of cyclotomic cosets and cyclic codes has not been done in general. Although for different values of q the polynomial $x^n - 1$ has been characterised. This paper will determine the number of irreducible monic polynomials and cyclotomic cosets of $x^n - 1$ over $\mathbb{Z}_{13}$ .The factorization of $x^n - 1$ over $\mathbb{Z}_{13}$ into irreducible polynomials using cyclotomic cosets of 13 modulo n will be established. The number of irreducible polynomials factors of $x^n - 1$ over $\mathbb{Z}_q$ is equal to the number of cyclotomic cosets of q modulo n. Each monic divisor of $x^n - 1$ is a generator polynomial of cyclic code in F_{q^n}. This paper will further show that the number of cyclic codes of length n over a finite field F is equal to the number of polynomials that divide $x^n - 1$. Finally, the number of cyclic codes of length n, when $n = 13k$, $n = 13^k, n = 13^k - 1, (k, 13) = 1$ are determine.

1. Introduction

The basic problem of coding theory is that of communication over unreliable channel that result in errors in the transmitted messages. It is worth noting that transmitted messages like data from a satellite are always subject to noise. It is important therefore, to be able to encode a message in such a way that if noise scramble it, it can be decoded to its original form. This is done by adding redundancy to the message so that the original form can be recovered if too many errors have not occurred. Sometimes where sensitive information is being transmitted the message is highly encoded and certain dummy parameters added to the message to avoid it correctly decoded in case it lands on wrong hands.

In addition to these practical application, coding theory has many application in theory of computer science. As such it is a topic of interest to both practitioners and theoreticians.

1.1 Definitions

Code: Let F be a finite set with q symbols, there are q^n different sequences of length n. Of these only q^k are codewords since the r check digits within any code word are completely determined by the k message digits. The set consisting ofq^k codewords of length n is called a code.

1.2 Cyclic code*:* Let C be a lnear code over a finite field $GF(q)$ of block n, C is called acyclic code, if for every codeword $a_0a_1a_2,\dots,a_n$ from C, the word $a_na_1a_2,\dots,a_{n-1}$ in C obtain by acyclic right shift of component is also a codeword. This also involves the left shift. Therefore a linear code C is cyclic precisely when it is invariant under all cyclic shifts.
the check polynomial of C.

1.3 Cyclotomic cosets: Let n be relatively to q. The cyclotomic cosets of $q\text{mod}n$ is defined by $C_i = \{i.q^j modn \in \mathbb{z}_n : j = 0,1,2,\dots\}$

1.4 Preliminary results

A code C is said to be cyclic if it is alinear code and it is invariant under any cyclic shift. In finding cyclic codes we factorise $x^n - 1$ into irreducible polynomials and obtain all monic polynomials that divide $x^n - 1$. Each such monic polynomial is a generator polynomial and generate a cyclic code. We wish to generate the number of cyclic code of length n over $GF(13)$.

2: Main Results: Factorization of $x^n - 1$ into irreducible polynomial over $\mathbb{Z}_{13}$

Let n be a positive integer with q and n relatively prime. The number of irreducible polynomial factors of $x^n - 1$ over F_q is equal to number of cyclotomic coset of $q(modn)n$ and if

$a)\ n = 1$

$x - 1 = x + 12$ is irreducible polynomial of degree 1 over $\mathbb{Z}_{13}$

$b)\ n = 2$: $x^2 - 1$ C_0={0} C_1={1}

There are only two cyclotomic cosets of $13(mod2)$ over $\mathbb{Z}_{13}$. Therefore the number of polynomial will only be two

$.x^2 - 1 = (x - 1)(x + 1) = (x + 12)(x + 1)$ over $\mathbb{Z}_{13}$

$c)\ n = 3 :\ x^3 - 1$

We need to find the number of cyclotomic cosets $13(mod3)$

$.C_i = \{i.13^j mod3:, j = 0,1,2,..\}$ C_0= {0} C_1= {1} C_2={2}

Therefore, there are 3 irreducible linear factors that divide $x^3 - 1$ over $\mathbb{Z}_{13}$ i.e

$.x^3 - 1 = (x + 12)(x^2 + x + 40) = (x + 12)(x + 10)(x + 4\ )$

$d)\ \ n = 4 : x^4 - 1$

We need to factorize $x^4 - 1$ over $\mathbb{Z}_{13}$ $C_i = \{i.q^j mod4: j = 0,1,2, \ldots\}$:

C_0={0} C_1={1} C_2={2} C_3={3}

Therefore $x^4 - 1$ can be factorized into 4 irreducible linear factors all of degree 1 over $\mathbb{Z}_{13}$ $i.e\ x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1) = (x + 12)(x + 1)(x^2 + 1) = (x + 12)(x + 1)(x + 8)(x + 5)$

$e)\ n = 5 :\ \ x^5 - 1$

We factorize $x^5 - 1$ over $\mathbb{Z}_{13}$ $C_i = \{i.q^j mod5 : j = 0,1,2, \ldots.\}$ C_0= {0} C_1= {1,2,4 ,3}

$x^5 - 1$ can be factorized into

$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1) = (x + 12)(x^4 + x^3 + x^2 + x + 1)$

$f)\ n = 6$: Factorize $x^6 - 1$ over $\mathbb{Z}_{13}$

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

$= (x - 1)(x + 4)(x + 10)(x^3 + 1) = (x - 1)(x + 4)(x + 10)(x^2 + 7x + 12)$

$= (x + 12)(x + 9)(x + 10)(x + 4)(x + 3)(x + 1)$

Therefore $x^6 - 1$ can be factorized into 6 monic irreducible polynomials over $\mathbb{Z}_{13}$ .all linear factors.

On the other hand the number of cyclotomic cosets $13(mod6)$ are

C_0= {0} C_1= (1) C= (2) C_3=(3) C_4=(4) C_5=(5)

$g)\ n = 7:\ \ x^7 - 1$

We factorize$x^7 - 1$ over $\mathbb{Z}_{13}.C_i = \{i.q^j mod7\ j = 0,1,\ \ 2,3,..\}$ C_0={0} C_1={1,6} C_2={2,5} C_3={3,4}

$x^7 - 1$ Can be factorized into

$x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + 1) = (x + 12)(x^2 + 3x + 1)(x^2 + 6x +)(x^2 + 5x + 1)$

Therefore $x^7 - 1$ Can be factorized into 4 monic irreducible polynomials. 1 of degree 1 and 3 of degree 2

$h)\ n = 8:\ x^8 - 1$ Consider the cyclotomic cosets 13 mod8 $C_i = \{i.13^j mod8\ \ j = 0,1,2,3\ , \ldots\}$

C_0={0} C_1={ 1,5} C_2={2} C_3={3,7} C_4={4} C_6={6}

Factorize $x^8 - 1$ over $\mathbb{Z}_{13}$

$x^8 - 1 = (x^4 - 1)(x^4 + 1) = (x^2 - 1)(x^2 + 1)(x^4 + 1) = (x + 12)(x + 1)(x + 5)(x + 8)(x^2 + 5)(x^2 + 8$

$x^8 - 1$ factors into 6 irreducible polynomials. 4of degree 1 and 2 of degree 2.

i) Factorize $x^9 - 1$ over $\mathbb{Z}_{13}$

$x^9 - 1 = (x - 1)(x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x + 12)(x - 9)(x - 3)(x^3 + 4)(x^3 + 10) = (x + 12)(x + 4)(x + 10)(x^3 + 4)(x^3 + 10)$

$x^9 - 1$ factors into 5 irreducible monic polynomials. 3 of degree 1 and 2 of degree 3. On the other hand the numbers of cyclotomic cosets are 5.

$C_i = \{i.13^j mod 9\ j = 0,1,2,3, \ldots\}$ C_0={0} C_1=(1,4,7} C_2={2,8,5} C_3={3} C_6={6}

j)We factorize $x^{10} - 1$over $\mathbb{Z}_{13}$.$C_i = \{i.13^j mod 10\ j = 0,1,2,3, \ldots\}$

C_0={0} C_1={1,3,9,7} C_2={2,6,8,4} C_5={5}

$x^{10} - 1$ Can be factorized into;

$x^{10} - 1 = (x^5 - 1)(x^5 + 1) = (x - 1)(x^4 + x^3 + x^2 + x + 1)(x^5 + 1) = (x + 12)(x^4 + x^3 + x^2 + x + 1x+11x4+2x3+4x2+8x+3$

$x^{10} - 1$ factors into 4 irreducible monic polynomials.2of degree 1 and 2 of degree 4.

k) We factorize $x^{11} - 1$over $\mathbb{Z}_{13}$. $C_i = \{i.13^j mod\ j = 0,1,2,3, \ldots\}$

C_0={0} C_1={1,2,4,8,5,10,9,7,3,6}

$x^{11} - 1$ Can be factorized into;

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

$x^{11} - 1$ can be factorized into 2 irreducible monic polynomials. 1of degree 1 and 1 of degree 10

l) We need to factorize $x^{12} - 1$ over $\mathbb{Z}_{13}$ $C_i = \{i.13^j mod\ j = 0,1,2,3, \ldots\}$

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}

$x^{12}-1$ Can be factorized into;

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

Therefore there are 12 irreducible monic polynomials of degree 1.

m) We need to factorize $x^{13}-1$ over $\mathbb{Z}_{13}$ $C_i=\{i.13^j mod\ j=0,1,2,3,\dots\}$

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}

$x^{13}-1$ Can be factorized into$x^{13}-1=(x-1)^{13}=(x+12)^{13}$

Therefore there are 13 irreducible monic polynomials of degree 1 with the same roots repeated 13 times.

n) Need to factorize $(x^{14}-1)$over $\mathbb{Z}_{13}.C_i=\{i.13^j mod 14\ j=0,1,2,3,\dots\}$

C_0= {0} C_1= {1,13} C_2={2,12} C_3=(3,11} C_4= {4, 10} C_5={5,9} C_7={7} C_6={6,8}

$x^{14}-1$ Can be factorized into;

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

$$(x^7+1)=(x+12)(x^2+3x+1)(x^2+6x+1)(x^2+5x+1)(x+1)\ (x^2+7x+1)\ (x^2+8x+1)(x^2+10x+1)$$

$x^{14}-1$ factors into 8, irreducible factors; 6 degree 2 and 2 of degree 1

o) Need to factorize.$x^{15}-1$ over $\mathbb{Z}_{13}$. $C_i=\{i.13^j mod 15\ j=0,1,2,3,\dots\}$

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

$x^{15}-1$ can be factorized into 5 irreducible monic polynomials. 1 of degree 1, 1 of degree 2 and 3 of degree 4.

$$x^{15}-1=(x-1)(x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$$
$$=(x+12)(x^2+ax+b)(x^4+3x^3+9x^2+x+3)(x^4+9x^3+3x^2+x+9)(x^4+x^3+x^2+x+1)$$

o) Need to factorize $x^{16}-1$ Over $\mathbb{Z}_{13}$.. $C_i=\{i.13^j mod 16\ j=0,1,2,3,\dots\}$

C_0={0} C_1={1,13,9,5} C_2={2,10} C_3={3,7,11,5}C_4={4} C_6={6,14} C_8={8} C_{12}={12}

$x^{16}-1$ Can be factorized into;

$x^{16}-1=(x^8-1)(x^8+1)=(x^4-1)(x^4+1)(x^8+1)\ =(x^2-1)(x^2+1)(x^4+1)(x^8+1)=$
$(x+12)(x+1)(x^2+1)(x^4+1)(x^8+1)=(x+12)(x+1)(x^2+1)(x^4+1)(x^4+5)(x^4+$
$8)=(x+12)(x+1)(x+5)(x+8)(x^2+5)(x^4+5)(x^2+8)(x^4+8)$

$x^{16}-1$ factors into 8, irreducible factors, 4 of degree1, 2 of degree 2 and 2 of degree 4

$p)\ n=17$: $x^{17}-1$ Consider the cyclotomic cosets 13 mod 17.

$C_i=\{i.13^j mod17\ \ j=0,1,2,3,\ldots\}$ $C_0=\{0\}$ $C_1=\{1,13,16,14\}$ $C_2=\{2,9,15,8\}$

$C_3=\{3,5,14,12\}$ $C_4=\{4,1,13,14\}$

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

$x^{17}-1$ can be factorized into 5, irreducible factors, 1 of degree1 and 4 of degree 4

$q)$ Need to factorize $x^{18}-1$ Over $\mathbb{Z}_{13}$. $C_i=\{i.13^j mod18\ \ j=0,1,2,3,\ldots\}$.

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

$x^{18}-1$ Can be factorized into;

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

Factors into 10, irreducible factors, 6 of degree1 and 4 of degree 3

$r)\ n=19$: $x^{19}-1$ Consider the cyclotomic cosets 13 mod 19

. $C_i=\{i.13^j mod19\ \ j=0,1,2,3,..\}$

$C_0=\{0\}$ $C_1=\{1,13,17,12,3,14,11,10,16\}$ $C_2=\{2,7,15,5,8,9,3,1,13\}$

$x^{19}-1$ Can be factorized 3 irreducible factors, 1 of degree 1and 2 of degree 9

$(x^{19}-1)=(x-1)(x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+$
$x4+x3+x2+1=x+12x9+ax8+bx7+cx6+dx5+ex4+fx3+gx2+hx+kx9+mx8+nx7+px6+qx5+rx4+s$
$x3+tx2+ux+v$

where $a, b, c, d, e, f, g, k, h, m, n, p, q, r, s, t, u, v \in \mathbb{Z}_{13}$

s) Need to factorize $x^{20} - 1$ over $\mathbb{Z}_{13}$. $C_i = \{i.13^j \, mod \, 20 \;\; j = 0,1,2,3, \dots, \}$

C_0={0} C_1={1,13,9,17} C_2={2,6,18,14}

C_4={4,12,16,8} C_5={5} C_{10}={10} C_3={3,19,7,11} C_{15}={15}

$x^{20} - 1$ Can be factorized into;

$x^{20} - 1 = (x^{10} - 1)(x^{10} + 1) = (x^5 - 1)(x^5 + 1)(x^{10} + 1) = (x - 1)(x^4 + x^3 + x^2 + x + 1)(x^{10} + 1) = (x + 12)(x^4 + x^3 + x^2 + x + 1)(x + 11)(x^4 + 2x^3 + 4x^2 + 8x + 3)(x + 5)(x^4 + 8x^3 + 12x^2 + 5x + 1x+8x4+5x3+12x2+8x+1$

Factors into 8, irreducible factors; 4 degree 4 and 4 of degree 1.

The number of irreducible factors in $(x^n - 1) mod 13$ is equal to the number of cyclotomic coset of $13 mod n$ provided (q, n)

The number of irreducible factors in $(x^n - 1) mod 13$ for $n = 1,2,3, \dots ,20$is summarized in the table below:

n	$x^n - 1$	$Number \; of \; irreducible \; factors \; in \; x^n - 1$
1	$x^1 - 1$	*1{1 of degree 1}*
2	$x^2 - 1$	*2{2 of degree1}*
3	$x^3 - 1$	*3{3 of degree 1}*
4	$x^4 - 1$	*4{4 of degree 1}*
5	$x^5 - 1$	*2{1 of degree1, 1 of degree 4}*
6	$x^6 - 1$	*6{6 of degree 1}*
7	$x^7 - 1$	*4{4 of degree1, 3 of degree 2}*
8	$x^8 - 1$	*6{4 of degree1, 2 of degree 2}*
9	$x^9 - 1$	*5{ 3 of degree1, 2 of degree 3}*
10	$x^{10} - 1$	*4{ 2 of degree 1, 2 of degree 4}*
11	$x^{11} - 1$	*2{ 1 of degree1, 1 of degree 10}*
12	$x^{12} - 1$	*12{ 12 of degree 1}*
13	$x^{13} - 1$	*13{13 of degree1}*
14	$x^{14} - 1$	*8{2 of degree1, 6 of degree 2}*
15	$x^{15} - 1$	*5{1 of degree1, 1 of degree2, 3 of degree 4}*
16	$x^{16} - 1$	*8{4 of degree1, 2 of degree2, 2 of degree 4}*
17	$x^{17} - 1$	*5{1 of degree1,4 of degree 4}*
18	$x^{18} - 1$	*10{6 of degree 1, 4 of degree 3}*
19	$x^{19} - 1$	*3{1 of degree1, 2 of degree 9}*
20	$x^{20} - 1$	*8{ 4 of degree1, 4 of degree 4}*

***Theorem* 3.1**: The number of cyclic code in $R_n = {F_q[x]}/{x^n - 1}$ is equal to 2^m where m is the number of m cyclotomic coset mod n. Consider the number of cyclic code of length $n = 1, 2, 3, \ldots, 20$ over $\mathbb{Z}_{13}$.

n	$x^n - 1$	$number of q\ cyclotomic\ coset = m$	$number of q cyclotomic coset = 2^m$
1	$x^1 - 1$	1	$2^1 = 2$
2	$x^2 - 1$	2	$2^2 = 4$
3	$x^3 - 1$	3	$2^3 = 8$
4	$x^4 - 1$	4	$2^4 = 16$
5	$x^5 - 1$	2	$2^2 = 4$
6	$x^6 - 1$	6	$2^6 = 64$
7	$x^7 - 1$	4	$2^4 = 16$
8	$x^8 - 1$	6	$2^6 = 64$
9	$x^9 - 1$	5	$2^5 = 32$
10	$x^{10} - 1$	4	$2^4 = 16$
11	$x^{11} - 1$	2	$2^2 = 4$
12	$x^{12} - 1$	12	$2^{12} = 4096$
13	$x^{13} - 1$	1	$13 + 1 = 14$
14	$x^{14} - 1$	7	$2^7 = 128$
15	$x^{15} - 1$	5	$2^5 = 32$
16	$x^{16} - 1$	8	$2^8 = 256$
17	$x^{17} - 1$	5	$2^5 = 32$
18	$x^{18} - 1$	10	$2^{10} = 1024$
19	$x^{19} - 1$	3	$2^3 = 8$
20	$x^{20} - 1$	8	$2^8 = 256$

3.2 Consider $x^n - 1$ when $n = 13k$, $(k, n) = 1$ $x^n - 1 = x^{13k} - 1 = (x^k - 1)^{13}$ and if

$a)\ k = 1$: $x^{13} - 1 = (x - 1)^{13}$

Number of cyclic codes $= 13 + 1 = 14$

$b)\ k = 2$ $x^{26} - 1 = (x^2 - 1)^{13} = (x - 1)^{13}(x + 1)^{13} = (x + 12)^{13}(x + 1)^{13}$ Number of cyclic codes $= (13 + 1)^2 = 14^2$

$.c)\ k = 3$: $(x^{39} - 1) = (x^3 - 1)^{13} = (x - 1)^{13}(x^2 + x + 1)^{13} = (x - 1)^{13}(x + 4)^{13}(x + 10)^{13} = (x + 12)^{13}x + 4)^{13}(x + 10)^{13}$

Number of cyclic code $s = (13 + 1)^3 = 14^3$

$d)\ k = 4$: $x^{52} - 1 = (x^4 - 1)^{13} = (x^2 - 1)^{13}(x^2 + 1)^{13} = (x - 1)^{13}(x + 1)^{13}(x + 8)^{13}(x + 5)^{13}$=*(x + 12)13(x+1)13(x+8)13(x+5)13*

Number of cyclic code $s = (13 + 1)^3 = 14^3$

$e)\ k = 5:\ x^{65} - 1 = (x^5 - 1)^{13} = (x-1)^{13}(x^4 + x^3 + x^2 + x + \ = (x-1)^{13}(x^4 + x^3 + x^2 + x + 1)^{13}$

Number of cyclic codes $= (13+1)^2 = 14^2$

$f)\ k = 6:\ x^{78} - 1 = (x^6 - 1)^{13} = (x^3 - 1)^{13}(x^3 + 1)^{13}$

$= (x+12)^{13}(x^2 + x + 1)^{13}(x^3 + 1)^{13}$

$= (x+12)^{13}(x+9)^{13}(x+10)^{13}(x+4)^{13}(x+3)^{13}(x\ +1)^{13}$

Number of cyclic codes $= (13+1)^6 = 14^6$

$g)\ k = 8; (x^{104} - 1) = (x^8 - 1)^{13} = (x^4 - 1)^{13}(x^4 + 1)^{13} = (x^2 - 1)^{13}(x^2 + 1)^{13}(x^4 + 1)^{13} = (x + 12)^{13}(x+1)^{13}(x+5)^{13}(x+8)^{13}(x^2 + 5)^{13}(x^2 + 8)^{13}$

Number of cyclic code$= (13+1)^6 = 14^6$

$h)\ k = 9:\ x^{117} - 1 = (x^9 - 1)^{13} = (x-1)^{13}(x-9)^{13}(x-3)^{13}(x^6 + x^3 + 1)^{13} = (x+12)^{13}(x + 4)^{13}(x+10)^{13}(x+10)^{13}(x^3 + 4)^{13}$

Number of cyclic codes $= (13+1)^5 = 14^5$

$i)\ k = 10:\ x^{130} - 1 = (x^{10} - 1)^{13} = (x^5 - 1)^{13}(x^5 + 1)^{13} = (x-1)^{13}(x^4 + x^3 + x^2 + x + +1)^{13}\ (x^5 + 1)^{13} == (x+12)^{13}(x^4 + x^3 + x^2 + x + 1)^{13}\ (x+1)^{13}(x^4 + 12x^3 + x^2 + 12x + 1)^{13}$

Number of cyclic codes $= (13+1)^4 = 14^4$

$j)\ k = 11:\ (x^{143} - 1) = (x^{11} - 1)^{13} = (x-1)^{13}(x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{13} = (x+12)^{13}(x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{13}$

Number of cyclic codes $= (13+1)^2 = 14^2$

$k)\ k = 12:\ x^{156} - \ 1 = (x^{12} - 1)^{13} = (x^6 - 1)^{13}(x^6 + 1)^{13} = (x^3 - 1)^{13}(x^3 + 1)^{13}(x^6 + 1)^{13} = (x + 1)^{13}(x+2)^{13}(x+3)^{13}(x+4)^{13}(x+5)^{13}(x+6)^{13}(x+7)^{13}(x+8)^{13}(x+9)^{13}(x+10)^{13}(x + 11)^{13}(x+12)^{13}$

Number of cyclic codes $= (13+1)^{12} = 14^{12}$

$l)\ k = 13:\ x^{169} - 1 = (x^{13} - 1)^{13} = (x^{13} + 12)^{13}$

Number of cyclic codes $= (13+1)^1 = 14^1$

m) $k = 16: (x^{208} - 1) = (x^{16} - 1)^{13} = (x^8 - 1)^{13}(x^8 + 1)^{13} = (x^4 - 1)^{13}(x^4 + 1)^{13}(x^8 + 1)^{13} = (x^2 - 1)^{13}(x^2 + 1)^{13}(x^4 + 1)^{13}(x^8 + 1)^{13} = (x+12)^{13}(x+1)^{13}(x+5)^{13}(x+8)^{13}(x^2 + 5)^{13}(x^2 + 8)^{13}(x^4 + 5)^{13}(x^4 + 8)^{13}$

Number of cyclic codes $= (13+1)^8 = 14^8$

$n)\ k = 20$: $(x^{260} - 1) = (x^{20} - 1)^{13} = (x^{10} - 1)^{13}(x^{10} + 1)^{13} = (x^5 - 1)^{13}(x^5 + 1)^{13}(x^{10} + 1)^{13} = (x + 12)^{13}(x^4 + x^3 + x^2 + x + 1)^{13}(x + 11)^{13}(x^4 + 2x^3 + 4x^2 + 8x + 3)^{13}(x + 5)^{13}(x^4 + 8x^3 + 12x^2 + 5x + 1)^{13}(x + 8)^{13}(x^4 + 5x^3 + 12x^2 + 8x + 1)^{13}$

Number of cyclic code$s = (13 + 1)^8 = 14^8$

The above is summarized in the table below

K	$x^n - 1\ when\ n = 13k$	$Number\ of\ factors$	$Number\ of\ cyclic\ code$
1	13	1	$(13 + 1)^1 = 14^1$
2	26	2	$(13 + 1)^2 = 14^2$
3	39	3	$(13 + 1)^3 = 14^3$
4	52	4	$(13 + 1)^4 = 14^4$
5	65	2	$(13 + 1)^2 = 14^2$
6	78	6	$(13 + 1)^6 = 14^6$
7	91	4	$(13 + 1)^4 = 14^4$
8	104	6	$(13 + 1)^6 = 14^6$
9	117	5	$(13 + 1)^5 = 14^5$
10	130	4	$(13 + 1)^4 = 14^4$
11	143	2	$(13 + 1)^2 = 14^2$
12	156	12	$(13 + 1)^{12} = 14^{12}$
13	169	1	$(13 + 1)^1 = 14^1$
14	182	7	$(13 + 1)^7 = 14^7$
15	195	5	$(13 + 1)^5 = 14^5$
16	208	8	$(13 + 1)^8 = 14^8$
17	221	5	$(13 + 1)^5 = 14^5$
8	234	10	$(13 + 1)^{10} = 14^{10}$
19	247	3	$(13 + 1)^3 = 14^{13}$
20	260	8	$(13 + 1)^8 = 14^8$

3.3 Consider $x^n - 1$ when $n = 13^k$ where $(k, 13) = 1$

The above is summarized in the table below:-

K	$x^n - 1$	$Factors$	$Number\ of\ cyclic\ code$
0	$x^{13^0} - 1$	$(x-1)^{13^0}$	$13^0 + 1 = 2$
1	$x^{13^1} - 1$	$(x-1)^{13^1}$	$13^1 + 1 = 14$
2	$x^{13^2} - 1$	$(x-1)^{13^2}$	$13^2 + 1 = 170$
3	$x^{13^3} - 1$	$(x-1)^{13^3}$	$13^3 + 1$
4	$x^{13^4} - 1$	$(x-1)^{13^4}$	$13^4 + 1$
5	$x^{13^5} - 1$	$(x-1)^{13^5}$	$13^5 + 1$
6	$x^{13^6} - 1$	$(x-1)^{13^6}$	$13^6 + 1$
7	$x^{13^7} - 1$	$(x-1)^{13^7}$	$13^7 + 1$
.	.	.	.
.	.	.	.
.	.	.	.
K	$x^{13^k} - 1$	$(x-1)^{13^k}$	$13^k + 1$

4. 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 $x^n - 1 = (x-1)^n$ then the number of cyclic code in$R_n = {F_q[x]}/{x^n - 1}$ is given by $n + 1$

2. Let $\mathbb{Z}_q$ be a finite field and $x^n - 1$ be given cyclotomic polynomial such that $x^n - 1 = (x - \alpha_1)(x - \alpha 2x - \alpha 3 \ldots . (x - \alpha n)$ where $\alpha i \neq \alpha j \forall\, i,j$ and suppose that $n = qm$ where $m \in \mathbb{Z}^+$ then, the number of cyclic codes in $R_n = {F_q[x]}/{x^n - 1}$ is given by $(q+1)^k$ where k is the number of distinct factors over $\mathbb{Z}_q$.

3. Let $\mathbb{Z}_q$ a given field and $x^n - 1$ be 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 coset.

References

1. Alex S. Bamunoba: Cyclotomic Polynomials, African Institute for Mathematical Sciences, 2011

2. Angela Barbero : Coding Theory and Application. Second Intentional Castle Meeting, ICMCTA, Castilio de la Mota, Medina del Campo, Spain , 2008

3. Andre Neubauer, Jurgen Freudenberger, Volker Kuhn: Coding Theory, Algorithms,

Architecture's and applications. John Wiley and sons Ltd, 2008.

4. Bazzil L. M .J Mitter S. K, "Some randomized code construction from group action". IEEE Transfer of information vol 52, p. 3210-3219, 2006.