# Enumeration of cyclic codes over $GF(17)$

**Lao Hussein, Benard Kivunge, Geoffrey Muthoka and Patrick Mwangi**

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 $GF(17)$. We factorize $x^n - 1$ over $GF(17)$ into irreducible polynomials using cyclotomic cosets of 17 modulo $n$. The number of irreducible polynomials factors of $x^n - 1$ over $F_q$ 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 $F_{q^n}$. We show that the number of cyclic codes of length $n$ over a finite field $F$ is equal to the number of polynomials that divide $x^n - 1$. Lastly, the number of cyclic codes of length $n$, when $n = 17k$, $n = 17^k, n = 17^k - 1, (k, 17) = 1$ are enumerated.*

## 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 codeword are completely determined by the $k$ message digits. The set consisting of $q^k$ 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.

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

### 1.3 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 $GF(17)$.

## 3 Factorization of $x^n - 1$ into irreducible polynomials over $\mathbb{Z}_{17}$

*Let* $n$ *be a positive integer with* $g.c.d\ (q, n) = 1$*. Then the number of monic irreducible polynomials factors of* $x^n - 1$ *over* $F_q$ *is equal to the number of cyclotomic coset q modulo n and if*

$a)\ n = 1$: $x - 1 \equiv x + 16$ is the irreducible polynomials of degree 1 over $\mathbb{Z}_{17}$

$b)\ n = 2$: $x^2 - 1$ Consider the cyclotomic cosets 17 mod 2

$C_i = \{i.17^j mod2\ j = 0,1,2,3, \dots.\}$ $C_0$= {0} $C_1$={1}

There are only two cyclotomic cosets of 17 mod 2 over $\mathbb{Z}_{17}$. On the other hand the number of irreducible polynomials will only be two

$$x^2 - 1 = (x - 1)(x + 1) = (x + 16)(x + 1)\ \ over\ \ \mathbb{Z}_{17}$$

$c)\ n = 3$: $x^3 - 1$ Consider the cyclotomic cosets17 mod 3

$C_i = \{i.17^j mod3\ j = 0,1,2,3, \dots\}$ $C_0$={0} $C_1$={1,2}

There are only two cyclotomic cosets 17 mod 3 over $\mathbb{Z}_{17}$ . Therefore the number of irreducible polynomials will only be two i.e

$x^3 - 1 = (x + 16)(x^2 + x + 1)$

$d)\ n = 4$: $x^4 - 1$ Consider the cyclotomic cosets17 mod 4 $C_i = \{i.17^j mod4\ \ j = 0,1,2,\}$

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

Number of irreducible monic factors will be four

$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1) = (x - 1)(x + 1)(x + 4)(x + 13) = (x + 16)(x + 1)(x +$ *4(x+13)*

$e)\ n = 5$: $x^5 - 1$ Consider the cyclotomic cosets 17 mod 5. $C_i = \{i.17^j mod5\ j = 0,1,2,3,..\}$

$C_0$={0} $C_1$={1,2,3,4} There are only 2 cyclotomic cosets 17 mod 5.

Therefore the number of irreducible polynomials will be two

.$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1) = (x + 16)(x^4 + x^3 + x^2 + x + 1)$

$f)\ \ n = 6$: $x^6 - 1$ Consider the cyclotomic cosets 17mod 6 $C_i = \{i.17^j mod6\ \ j = 0,1,2,3, \dots\}$

$C_0$={0} $C_1$={1,5} $C_2$={2,4} $C_3$={3}

There are 4 cyclotomic cosets 17 mod 6.Therefore the number of irreducible monic factors will be four

$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x^3 + 1) = (x + 16)(x^2 + x + 1)(x + 1)(x^2 + 16x + 1)$

$g)\ n = 7$: $x^7 - 1$ Consider the cyclotomic cosets 17 mod 7 $C_i = \{i.17^j mod7\ \ : j = 0,1,2,3, \dots\}$ $C_0$={{0} $C_1$={1,3,2,6,4,5}

There are only 2 cyclotomic cosets of 17mod7. Therefore the number of irreducible monic factors will be two.

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

$$= (x + 16)(x^6 + x^5 + x^4 + x^3 + x^2 + 1)$$

$h)\ n = 8$: $x^8 - 1$ Consider the cyclotomic cosets 17 mod 8. $C_i = \{i.17^j mod\ 8\ : j = 0,1,2,3, \ldots.\}$

$C_0$={0} $C_1$={1} $C_2$={2} $C_3$={3} $C_4$={4} $C_5$={5} $C_6$={6} $C_7$={7}

Therefore $x^8 - 1$ can be factorised into 8 monic irreducible polynomials all linear factors. $x^8 - 1 = (x^4 - 1)(x^4 +$ 1=x2−1x2+1x4+1=x−1x+1x+4x+13x4+1=x−1x+1x+4x+13x2+11x+18x2+10x+16=x+16x+1x+4x+13 x+2(x+8)(x+2)(x+9)

$i)\ n = 9: x^9 - 1$. Consider the cyclotomic cosets 17 mod 9 . $C_i = \{i.17^j mod 9 : j = 0,1,2,3, \ldots\}$

$C_0$= {0} $C_1$={1,8} $C_2$={2,7} $C_3$={3,6} $C_4$={4,5}

$x^9 - 1$ Can be factorized into 5 irreducible monic polynomials, 1 of degree 1 and 4 of degree 2.

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

$j)\ n = 10$: $x^{10} - 1$. Consider the cyclotomic cosets 17 and 10. $C_i = \{i.17^j mod 10\!: j = 0,1,2,3,..\}$

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

$x^{10} - 1$ Can be factorized into 4 irreducible monic polynomials, 2 of degree 1 and 2 of degree 4.

$x^{10} - 1 = (x^5 - 1)(x^5 + 1) = (x - 1)(x^4 + x^3 + x^2 + x + 1)(x^5 + 1) = (x + 16)(x^4 + x^3 + x^2 + x + 1)(x +$ 1x4+16x3+1

$k)\ n = 11$: $x^{11} - 1$. Consider the cyclotomic cosets 17 mod 11. $C_i = \{i.17^j mod 11\!: j = 0,1,2,3,..\}$

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

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

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

$l)\ n = 12: x^{12} - 1.$ Consider the cyclotomic cosets 17 mod 12 $C_i = \{i.17^j mod 12\!: j = 0,1,2,3,..\}$

$C_0$= {0} $C_1$= {1,5} $C_2$={2,10} $C_3$={3} $C_4$= {4 ,8} $C_6$={6} $C_7$={7,11} $C_9$={9}

$x^{12} - 1$ Can be factorized into 8 irreducible factors, 4 of degree 1 and 4 of degree 2.

$$(x^{12} - 1) = (x^6 - 1)(x^6 + 1) = (x^3 - 1)(x^3 + 1)(x^6 + 1)$$
$$= (x - 1)(x^2 + x + 1)(x^3 + 1)(x^6 + 1)$$
$$= (x + 16)(x^2 + x + 1)(x + 1)(x^2 + 16x + 1)(x + 4)(x^2 + 4x + 16)(x + 3)(x^2 + 13x + 16)$$

$m)\ n = 13$: $x^{13} - 1$. Consider the cyclotomic cosets17mod13. $C_i = \{i.17^j mod 13\!: j = 0,1,2,3,..\}$

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

$x^{13} - 1$. Can be factorized into 3 irreducible factors, 1 of degree 1 and 2 of degree 6

$x^{13}-1=(x-1)(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+1)=(x+16)(x^{12}+x^{11}+x^{10}+$
*x9+x8+x7+x6+x5+x4+x3+x2+1=x+16x6+13x5+2x4+12x3+2x2+13x+1)(x6+5x5+2x4+4x3+2x2+5x+1*

$n)$ $n=14$: $x^{14}-1$ . Consider the cyclotomic cosets 17 mod 14. $C_i=\{i.17^j mod 10\colon\ j=\ 0,1,2,3,..\}$

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

$x^{14}-1$ Can be factorized into 4 irreducible factors , 2 of degree 1 and 2 of degree 6.

$$\begin{aligned}(x^{14}-1)&=(x^7-1)(x^7+1)=(x-1)(\,x^6+x^5+x^4+x^3+x^2+1)(x^7+1)\\ &=(x+16)(x^6+x^5+x^4+x^3+x^2+1)\\ &=(x+16)(x^6+x^5+x^4+x^3+x^2+x+1)(x^6+16x^5+x^4+16x^3+x^2+16x+1)(x+1)\end{aligned}$$

$o)$ $n=15$: $x^{15}-1$. Consider the cyclotomic cosets 17 mod 15.

$C_i=\{i.17^j mod 15\colon\ j=0,1,2,3,..\}$

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

$x^{15}-1$ can be factorized into 5 irreducible monic polynomials. 1 of degree 1, 1 of degree2 and 3 of degree 4.

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

$p)$ $n=16$: $x^{16}-1$ Consider the cyclotomic cosets 17 mod 16.

$C_i=\{i.17^j mod 10\colon\ j=0,1,2,3,..\}$

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

$x^{16}-1$ Can be factorized 16 irreducible monic polynomials, all linear factors.

$x^{16}-1=(x^8-1)\,(x^8+1)=(x^4-1)\,(x^4+1)(x^8+1)=(x^2-1)(x^2+1)(x^4+1)(x^8+1)=(x-1)(x+$
*1x+4x+13x4+1x8+1=x−1x+1x+4x+13x2+11x+18x2+10x+16x8+1=(x+1)*
$(x+2)(x+3)(x+4)(x+5)(x+6)(x+7)(x+8)(x+9)(x+10)(x+11)(x+12)(x+13)(x+14)(x+$
$15)(x+16)$

$q)$ $n=17$: $x^{17}-1$. Consider the cyclotomic cosets 17 mod 17. $C_i=\{i.17^j mod 10\colon\ j=0,1,2,3,..\}$ $C_0=\{0\}$
$C_1=\{1,0\}$ $C_2=\{2,0\}$ $C_3=\{3,0\}$ $C_4=\{4,0\}$ $C_5=\{5,0\}$ $C_6=\{6,0\}$ $C_7=\{7,0\}$ $C_8=\{8,0\}$ $C_9=\{9,0\}$ $C_{10}=\{10,0\}$
$C_{11}=\{11,0\}$ $C_{12}=\{12,0\}$ $C_{13}=\{13,0\}$ $C_{14}=\{14,0\}$ $C_{15}=\{15,0\}$ $C_{16}=\{16,0\}$

$x^{17}-1$ Can be factorized into 17 irreducible monic polynomials, all linear factors.

$$(x^{17}-1)=(x-1)^{17}=(x+16)^{17}$$

$r)$ $n=18$: $x^{18}-1$ Consider the cyclotomic cosets 17 mod18.

$C_i=\{i.17^j mod 10\colon\ j=0,1,2,3,..\}$

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

$x^{18}-1$ Can be factorized 10 irreducible factors , 2 of degree 1 and 8 of degree 2.

$s)$ $n=19$: $x^{19}-1$ Consider the cyclotomic cosets 17 mod 19.

$C_i=\{i.17^j mod10: \ j=0,1,2,3,..\}$

$C_0=\{0\}$ $C_1=\{1,17,4,11,16,6,7,5,9\}$ $C_2=\{2,15,8,3,13,12,14,10,18\}$

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

$(x^{19}-1)=(x-1)(x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+$
*x2+1=(x−1) x9+ax8+bx7+cx6+dx5+ex4+fx3+gx2+hx+kx9+mx8+nx7+px6+qx5+rx4+sx3+tx2+ux+v*
where $a,b,c,d,e,f,g,k,h,m,n,p,q,r,s,t,u,v \in \mathbb{Z}_{17}$

$t)$ $n=20$: $x^{20}-1$. Consider the cyclotomic cosets 17 mod 20. $C_i=\{i.17^j mod10: \ j=0,1,2,3,..\}$

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

$x^{20}-1$ Can be factorized 10 irreducible factors 8. 4 of degree 1 and 4 of degree 4

$x^{20}-1=(x^{10}-1)(x^{10}+1)=(x^5-1)(x^5+1)(x^{10}+1)=(x-1)(x^4+x^3+x^2+x+1)(x^5+1)(x^{10}+1)=$
$(x+16)(x^4+x^3+x^2+x+1)(x+1)(x^4+16x^3+1)(x^{10}+1)=(x+16)(x^4+x^3+x^2+x+1)(x+1)(x^4+$
*16x3+1x+4x4+4x3+16x2+11x+10x+13x4+4x316x2+13x+1*

The number of irreducible factors in $(x^n-1)mod17$ 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 | $x^2-1$ | $2\{2\ of\ degree\ 1\}$ |
| 3 | $x^3-1$ | $2\{1\ of\ degree1, 1\ of\ degree\ 2\}$ |
| 4 | $x^4-1$ | $4\{\ 4\ of\ degree\ 1\}$ |
| 5 | $x^5-1$ | $2\{1\ of\ degree1, 1\ of\ degree\ 4)$ |
| 6 | $x^6-1$ | $4\{\ 2\ of\ degree1, 2\ of\ degree2, 2\ of\ degree\ 2\}$ |
| 7 | $x^7-1$ | $2\{1\ of\ degree\ 1, 1\ of\ degree\ 6\}$ |
| 8 | $x^8-1$ | $8\{8\ of\ degree\ 1\}$ |
| 9 | $x^9-1$ | $5\{1\ of\ degree1, 4\ of\ degree\ 2\}$ |
| 10 | $x^{10}-1$ | $4\{2\ of\ degree\ 1, 2\ of\ degree\ 4\}$ |
| 11 | $x^{11}-1$ | $2\{1\ of\ degree\ 1, 1\ of\ degree\ 10\}$ |
| 12 | $x^{12}-1$ | $7\{2\ of\ degree\ 1, 5\ of\ degree\ 2\}$ |
| 13 | $x^{13}-1$ | $3\{\ 1\ of\ degree1, 2\ of\ degree\ 6\}$ |
| 14 | $x^{14}-1$ | $4\{2\ of\ degree\ 1, 2\ of\ degree\ 6\}$ |
| 15 | $x^{15}-1$ | $5\{1\ of\ degree\ 1, 1\ of\ degree\ 2, 3\ of\ degree\ 4\}$ |
| 16 | $x^{16}-1$ | $16\{\ 16\ of\ degree\ 1\}$ |
| 17 | $x^{17}-1$ | $17\{17\ of\ degree\ 1\}$ |
| 18 | $x^{18}-1$ | $10\{2\ of\ degree\ 1, 8\ of\ degree\ 2\}$ |
| 19 | $x^{19}-1$ | $3\{\ 1\ of\ degree\ 1, 2\ of\ degree\ 9\}$ |
| 20 | $x^{20}-1$ | $8\{4\ f\ degree\ 1, 4\ of\ degree\ 4\}$ |

**$\boldsymbol{Theorem}$ 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 $n = 1, 2, 3, \dots .,\ 20$ over $\mathbb{Z}_{17}$.

**3.1 Consider the number of cyclic code of length $\boldsymbol{n = 1,\ 2,\ 3, \dots\ 20}$ over $\mathbb{Z}_{17}$**

| $n$ | $x^n - 1$ | $number\ of\ q\ cyclotomic\ coset\ equal\ m$ | $number\ of\ cyclic\ code\ equal\ 2^m$ |
|---|---|---|---|
| 1 | $x^1 - 1$ | 1 | $2^1 = 2$ |
| 2 | $x^2 - 1$ | 2 | $2^2 = 4$ |
| 3 | $x^3 - 1$ | 2 | $2^2 = 4$ |
| 4 | $x^4 - 1$ | 4 | $2^4 = 16$ |
| 5 | $x^5 - 1$ | 2 | $2^2 = 4$ |
| 6 | $x^6 - 1$ | 4 | $2^4 = 16$ |
| 7 | $x^7 - 1$ | 2 | $2^2 = 4$ |
| 8 | $x^8 - 1$ | 8 | $2^8 = 256$ |
| 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 | $x^{12} - 1$ | 8 | $2^8 = 256$ |
| 13 | $x^{13} - 1$ | 3 | $2^3 = 8$ |
| 14 | $x^{14} - 1$ | 4 | $2^4 = 16$ |
| 15 | $x^{15} - 1$ | 5 | $2^5 = 32$ |
| 16 | $x^{16} - 1$ | 16 | $2^{16} = 65536$ |
| 17 | $x^{17} - 1$ | 1 | $2^1 = 2$ |
| 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 $\boldsymbol{x^n - 1}$ when $\boldsymbol{n = 17k}$: $\boldsymbol{(k, 17) = 1}$**

$x^n - 1 = x^{17k} - 1$ and if

$a)$ $k = 1$: $x^{17} - 1 = (x - 1)^{17} = (x + 16)^{17}$ Number of cyclic codes $= 17 + 1 = 18$

$b)$ $k = 2$: $x^{34} - 1 = (x^2 - 1)^{17} = (x - 1)^{17}(x + 1)^{17} = (x + 16)^{17}(x + 1)^{17}$ Number of cyclic codes$= (17 + 1)^2 = 18^2$

$c)$ $k = 3$: $x^{51} - 1 = (x^3 - 1)^{17} = (x + 16)^{17}(x^2 + x + 1)^{17}$ Number of cyclic code$s$ $(17 + 1)^2 = 18^2$

$$d)\ \ k = 4:\ x^{68} - 1 = (x^4 - 1)^{17} = (x^2 - 1)^{17}(x^2 + 1)^{17} = (x - 1)^{17}(x + 1)^{17}(x^2 + 1)^{17}$$
$$= (x + 1)^{17}(x + 12)^{17}(x + 8)^{17}(x + 5)^{17}$$

Number of cyclic code$s$ $= (17 + 1)^4 = 18^4$

e) $k = 5$: $x^{85} - 1 = (x^5 - 1)^{17} = (x + 16)^{17}(x^4 + x^3 + x^2 + x + 1)^{17}$

Number of cyclic code$s = (17 + 1)^2$=$18^2$ = (17+1)$^2$=18$^2$

$f)$ $k = 6$: $x^{102} - 1 = (x^6 - 1)^{17} = (x^3 - 1)^{17}(x^3 + 1)^{17} = (x + 16)^{17}(x^2 + x + 1)^{17}(x + 1)^{17}(x^2 + 16x + 1)^{17}$

Number of cyclic code$s = (17 + 1)^4 = 18^4$

$g)$ $k = 7$: $x^{119} - 1 = (x^7 - 1)^{17} = (x - 1)^{17}(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{17} = (x + 16)^{17}(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{17}$

Number of cyclic code$s = (17 + 1)^2 = 18^2$

$h)$ $k = 8$: $x^{136} - 1 = (x^8 - 1)^{17} = (x^4 - 1)^{17}(x^4 + 1)^{17} = (x^2 - 1)^{17}(x^2 + 1)^{17}(x^4 + 1)^{17} = (x + 16)^{17}(x + 1)^{17}(x + 4)^{17}(x + 13)^{17}(x + 9)^{17}(x + 2)^{17}(x + 8)^{17}(x + 2)^{17}$

Number of cyclic code$s = (17 + 1)^8 = 18^8$

$i)$ $k = 9$: $x^{153} - 1 = (x^9 - 1)^{17} = (x - 1)^{17}(x^2 + x + 1)^{17}(x^6 + x^3 + 1)^{17} = (x + 16)^{17}(x^2 + x + 1)^{17}(x^2 + 3x + 1)^{17}(x^2 + 10x + 1)^{17}(x^2 + 4x + 1)^{17}$

Number of cyclic code$s = (17 + 1)^5 = 18^5$

$j)$ $k = 10$: $x^{170} - 1 = (x^{10} - 1)^{17} = (x^5 - 1)^{17}(x^5 + 1)^{17} = (x + 16)^{17}(x^5 + x^4 + x^3 + x^2 + x + 1)^{17}(x^5 + 1)^{17} = (x^5 - 1)^{17}(x^5 + 1)^{17} = (x + 16)^{17}(x^5 + x^4 + x^3 + x^2 + x + 1)^{17}(x + 1)^{17}(x^4 + 16x^3 + 1)^{17}$

Number of cyclic code$s = (17 + 1)^4 = 18^4$

k) $k = 11$: $x^{187} - 1 = (x^{11} - 1)^{17} = (x - 1)^{17}(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{17} = (x + 16)^{17}(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{17}$

Number of cyclic code$s = (17 + 1)^2 = 18^2$

$l)$ $k = 14$: $x^{238} - 1 = (x^{14} - 1)^{17} = (x^7 - 1)^{17}(x^7 - 1)^{17} = (x - 1)^{17}(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{17}(x - 16)^{17}(x^6 + 16x^5 + x^4 + 16x^3 + x^2 + 16x + 1)^{17} = (x + 16)^{17}(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{17}(x + 1)^{17}(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^{17}$

Number of cyclic code$s = (17 + 1)^4 = 18^4$

$m)$ $k = 20$: $x^{340} - 1 = (x^{20} - 1)^{17} = (x^{10} - 1)^{17}(x^{10} + 1)^{17} = (x^5 - 1)^{17}(x^5 + 1)^{17}(x^{10} + 1)^{17} = (x - 1)^{17}(x^4 + x^3 + x^2 + x + 1)^{17}(x - 16)^{17}(x^4 + 16x^3 + 1)^{17}(x - 13)^{17}(x^4 + 4x^3 + 16x^2 + 11x + 10)^{17}(x - 4)^{17}(x^4 + x^3 + x^2 + x + 1)^{17} = (x + 16)^{17}(x^4 + x^3 + x^2 + x + 1)^{17}(x + 1)^{17}(x^4 + 16x^3 + 1)^{17}(x + 4)^{17}(x^4 + 4x^3 + 16x^2 + 11x + 10)^{17}(x + 13)^{17}(x^4 + x^3 + x^2 + x + 1)^{17}$

Number of cyclic code$s = (17 + 1)^8 = 18^8$

The above is summarized in the table below

| $k$ | $x^n - 1 when\, n = 17k$ | $Number\ of\ factors$ | $Number\ of\ cyclic\ code$ |
|---|---|---|---|
| 1 | 17 | 1 | $(17+1)^1 = 18^1$ |
| 2 | 34 | 2 | $(17+1)^2 = 18^2$ |
| 3 | 51 | 2 | $(17+1)^2 = 18^2$ |
| 4 | 68 | 4 | $(17+1)^4 = 18^4$ |
| 5 | 85 | 3 | $(17+1)^3 = 18^3$ |
| 6 | 102 | 4 | $(17+1)^4 = 18^4$ |
| 7 | 119 | 3 | $(17+1)^3 = 18^3$ |
| 8 | 136 | 8 | $(17+1)^8 = 18^8$ |
| 9 | 153 | 5 | $(17+1)^5 = 18^5$ |
| 10 | 170 | 4 | $(17+1)^4 = 18^4$ |
| 11 | 187 | 2 | $(17+1)^2 = 18^2$ |
| 12 | 204 | 8 | $(17+1)^8 = 18^8$ |
| 13 | 221 | 3 | $(17+1)^3 = 18^3$ |
| 14 | 238 | 4 | $(17+1)^5 = 18^4$ |
| 15 | 255 | 5 | $(17+1)^5 = 18^5$ |
| 16 | 272 | 16 | $(17+1)^{16} = 18^{16}$ |
| 17 | 289 | 1 | $(17+1)^1 = 18^1$ |
| 18 | 306 | 10 | $(17+1)^{10} = 18^{10}$ |
| 19 | 323 | 3 | $(17+1)^3 = 18^3$ |
| 20 | 340 | 8 | $(17+1)^8 = 18^8$ |

### 3.3 Consider $x^n - 1$ when $n = 17^k$: $(k, 17) = 1$

The above is summarized in the table below

| $\boldsymbol{K}$ | $\boldsymbol{x^n - 1}$ | $\boldsymbol{Factors}$ | $\boldsymbol{Number\ of\ cyclic\ codes}$ |
|---|---|---|---|
| 0 | $x^{17^0} - 1$ | $(x-1)^{17^0}$ | $17^0 + 1 = 2$ |
| 1 | $x^{17^1} - 1$ | $(x-1)^{17^1}$ | $17^1 + 1 = 18$ |
| 2 | $x^{17^2} - 1$ | $(x-1)^{17^2}$ | $17^2 + 1 = 290$ |
| 3 | $x^{17^3} - 1$ | $(x-1)^{17^3}$ | $17^3 + 1$ |
| 4 | $x^{17^4} - 1$ | $(x-1)^{17^4}$ | $17^4 + 1$ |
| 5 | $x^{17^5} - 1$ | $(x-1)^{17^5}$ | $17^5 + 1$ |
| . | . | . | . |
| . | . | . | . |
| . | . | . | . |
| 10 | $x^{17^{10}} - 1$ | $(x-1)^{17^{10}}$ | $17^{10} + 1$ |
| . | . | . | . |
| . | . | . | . |
| . | . | . | . |
| $K$ | $x^{17^k} - 1$ | $(x-1)^{17^k}$ | $17^k + 1$ |

### 3.4 Consider $\boldsymbol{x^n - 1}$ when $\boldsymbol{n = 17^k - 1}$ in $\mathbb{Z}_{17}$.

Now $x^n - 1 = x^{17^k - 1} - 1 = \frac{x^{17}}{x} - 1 = \frac{x^{17^k} - x}{x}$ let $p = 17^k$ where $p$ is prime. Substituting for the value of $p$ we have $\frac{x^p - x}{x} = \frac{x(x^{p-1} - 1)}{x} = x^{p-1} - 1$. But we know that
$\frac{x^{p-1} - 1}{x-1} = x^{p-2} + x^{p-3} + x^{p-4} + \; \ldots . + x + 1$ giving $x^{p-1} - 1 = (x-1)(x^{p-2} + x^{p-3} + x^{p-4} + \; \ldots . + x + 1)$
Suppose that $\emptyset_{p-1}(\, x) = (x^{p-2} + x^{p-3} + x^{p-4} + \; \ldots . + x + 1)$
So that $x^{p-1} - 1 = (x-1)\emptyset_{p-1}(\, x)$. One notices that Eisenstein criterion is not directly applicable. We therefore substitute $(x+1)$ for $x$ in equation $x^{p-1} - 1 = (x-1)\emptyset_{p-1}(\, x)$. Now $(x+1)^{p-1} - 1 = ((x+1) - 1)\emptyset_{p-1}(\, x +$ *1* so that we have

$$x\emptyset_{p-1}(\, x+1) = x^{p-1} - 1 = \binom{p-1}{0} x^{p-1} + \binom{p-1}{1} x^{p-2} + \ldots + \binom{p-1}{p-2} x + \binom{p-1}{p-1} - 1$$

$$= \binom{p-1}{0} x^{p-1} + \binom{p-1}{1} x^{p-2} + \ldots + \binom{p-1}{p-2}$$

$$= \sum_{k=0}^{p-2} \binom{p-1}{k} x^{p-1-k}$$

We now apply Eisenstein criterion $p - 1 \big/ \binom{p-1}{k}$ for $k = 1,2,3, \ldots p-2$ so $p - 1 \nmid 1$ $(p-1)^2 \nmid \binom{p-1}{p-2}$ hence $\emptyset_{p-1}(x + 1)$ is irreducible over $\mathbb{Z}_{17}$ therefore $x^{p-1} - 1 = (x-1)\emptyset_{p-1}(x+1)$ is irreducible
Hence the number of cyclic code over $\mathbb{Z}_{17}$ when $n = 17^k - 1 \; is \; 2^2$=4

## 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 $R_n = {}^{F_q[x]}\big/_{x^n - 1}$ is given by $n + 1$

2. Let $\mathbb{Z}_q$ be a finite field and $x^n - 1$ be given cyclotomic polynomial such that $x^n - 1 = (x - \alpha_1)(x - \alpha_2)(x -$ *α3....(x−αn)* where *αi≠αj ∀ i,j* and suppose that
$n = qm$ where $m \in \mathbb{Z}^+$ then, the number of cyclic codes in $R_n = {}^{F_q[x]}\big/_{x^n - 1}$ 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. Hill. R:A first course in coding Theory. Claredon Press, oxford, 1986.
2.J. Bierbraeur: Intoduction to Coding Theory, Chapman and Hall. CRC press, 2005
3. Jacobs Kenneth: A survey of Modern Mathematical Cryptography, University of Tennesse, Honors Thesis Project, http://trace. tennesse.edu/uk. 2006.
10. K. Gyory : On the irreducibily of a class of Polynomial III, Number Theory 15, 1982.
Micheal Caderbank : An Introduction to Linear and cyclic codes, 2008
4. Tom Hansen, Gary L. Mullen: Primitive Polynomials over Finite Fields. Mathematics of Computation, vol 59 no. 200 p. 637-643, 1992.
12.Vankatesan G: Introduction to Coding Theory, Spring 2010.