
On the Zeros of Linear Factors of Cyclotomic Polynomials Over Galois Fields

a

Abstract

The study of cyclic codes via cyclotomic polynomial over Galois field has been active area of research. Perhaps, this could be due to the fact that cyclotomic polynomial have direct application as a major tool in generating the number of cyclic codes over Galois field. Let q be a prime number and \mathbb{F}_q be a given finite field with q elements. In this current research, the study of cyclotomic polynomial $y^n - 1$ for which $y^n - 1$ completely decomposes into linear factors over \mathbb{F}_q is discussed. In particular, the relationships between the field, sum and the product of the zeroes of linear factors over Galois field is presented.

Keywords: Primitive root of unity, Zeros, Cyclotomic Polynomials.

2010 Mathematics Subject Classification: 53C25; 83C05; 57N16.

1 Introduction

Cyclotomic polynomials are importance types of polynomials often appearing frequently throughout algebra, there factorizations are central in number theory and coding theory more specifically error correcting codes [4, 5, 6, 7, 8, 9, 10]. These polynomials factors into linear factors if $n \mid (q - 1)$ as shown in [2, 11, 12, 14, 15, 16, 17, 18], the understanding of their zeros are important in construction of generator polynomials [1, 3, 6]. In this paper zeros of the linear factors of cyclotomic polynomial $y^n - 1$ over finite field \mathbb{F}_q are investigated for $q \leq 37$ and $n \geq 2$, the result are summarized in the table and generalization made over Galois fields \mathbb{F}_q .

1.1 Definitions

- i) **n^{th} primitive root of unity:** Let \mathbb{F}_q be a finite field and $\alpha \in \mathbb{F}_q$. We say α is an n^{th} root of unity if $\alpha^n = 1$. An n^{th} root of unity is *primitive* if $\text{ord}(\alpha) = n$.
- ii) **Zeros of a polynomial:** Let \mathbb{F}_q be a finite field. An element $\alpha \in \mathbb{F}_q$ is a *zero* of $f(y) \in \mathbb{F}_q[y]$ if

$$f(\alpha) \equiv 0 \pmod{q}.$$

- iii) **Cyclotomic polynomial:** Let n be a positive integer. The n^{th} cyclotomic polynomial $\Phi_n(y)$ is the unique monic polynomial over \mathbb{Q} whose zeros are exactly the primitive n^{th} roots of unity. In particular, in a finite field \mathbb{F}_q , if $n \mid (q - 1)$, we have

$$y^n - 1 = \prod_{i=1}^n (y + \alpha_i),$$

where each α_i is an n^{th} root of unity, and

$$\Phi_n(y) = \prod_{\substack{1 \leq k \leq n \\ \text{gcd}(k, n) = 1}} (y + \alpha_k).$$

2 Main Results

2.1 Zeros of Cyclotomic Polynomials over \mathbb{F}_q

Conjecture 2.1. Let \mathbb{F}_q be a finite field and let $y^n - 1$ be a given cyclotomic polynomial and suppose $n \mid (q - 1)$, and $y^n - 1 = (y + \alpha_1)(y + \alpha_2)(y + \alpha_3) \dots (y + \alpha_n) = \prod_{i=1}^n (y + \alpha_i)$ Then, for $n \geq 2$;

- i) $\sum_{i=1}^n \alpha_i = K \cdot q$ where $k \in \mathbb{Z}^+$
- ii) $\prod_{i=1}^n \alpha_i = r \cdot n$ where $r \in \mathbb{Z}^+$
- iii) $\prod_{i=1}^n \alpha_i \equiv -1 \pmod{q}$
- iv) $(\frac{\prod_{i=1}^n \alpha_i}{n})^{-1} \equiv q - n \pmod{q}$

Let \mathbb{F}_q be a finite field and $y^n - 1 = (y + \alpha_1)(y + \alpha_2)(y + \alpha_3) \dots (y + \alpha_n) = \prod_{i=1}^n (y + \alpha_i)$ be a cyclotomic polynomial such that $n \mid (q - 1)$, then it splits completely over \mathbb{F}_q and all its zeros are in \mathbb{F}_q . The following cases give more pictures of the results.

Case 1: $n = 4, q = 5$

Consider \mathbb{F}_5 and $n = 4$. Since $4 \mid (5 - 1)$, we have

$$y^4 - 1 = (y + 4)(y + 3)(y + 2)(y + 1) \in \mathbb{F}_5,$$

and the zeros α_i are $\{4, 3, 2, 1\}$.

sum of the zeros $\sum_{i=1}^n \alpha_i = 4 + 3 + 2 + 1 = 10 \equiv 0 \pmod{5}$

and $\frac{\sum_{i=1}^n \alpha_i}{q} = \frac{10}{5} = 2. \implies \sum_{i=1}^n \alpha_i = k \cdot q$

$$\prod_{i=1}^n \alpha_i = 4 \times 3 \times 2 \times 1 = 24 \equiv -1 \pmod{5}$$

$$\frac{\prod_{i=1}^n \alpha_i}{n} = \frac{24}{4} = 6 \text{ and } \left(\frac{\prod_{i=1}^n \alpha_i}{n}\right)^{-1} = \frac{1}{6} \equiv 1 \pmod{5} \equiv q - n \pmod{q}.$$

Case 2: $n = 5, q = 11$

Consider \mathbb{F}_{11} and $n = 5$. Since $5 \mid (11 - 1)$, we have

$$y^5 - 1 = (y + 10)(y + 8)(y + 7)(y + 6)(y + 2) \text{ in } \mathbb{F}_{11},$$

and the zeros α_i are $\{10, 8, 7, 6, 2\}$.

sum of the zeros $\sum_{i=1}^n \alpha_i = 10 + 8 + 7 + 6 + 2 = 33 \equiv 0 \pmod{11}$

and $\frac{\sum_{i=1}^n \alpha_i}{q} = \frac{33}{11} = 3$

$\implies \sum_{i=1}^n \alpha_i = k \cdot q$

$$\prod_{i=1}^n \alpha_i = 10 \times 8 \times 7 \times 6 \times 2 = 6,720 \equiv -1 \pmod{11}$$

$$\frac{\prod_{i=1}^n \alpha_i}{n} = \frac{6,720}{5} = 1344 \equiv -1 \pmod{11} \text{ and } \left(\frac{\prod_{i=1}^n \alpha_i}{n}\right)^{-1} = \frac{1}{1344} \equiv \frac{1}{2} \pmod{11} = 6 \pmod{11} \equiv q - n \pmod{q}.$$

Case 3: $n = 6, q = 13$

Consider \mathbb{F}_{13} and $n = 6$. Since $6 \mid (13 - 1)$, we have

$$y^6 - 1 = (y + 12)(y + 10)(y + 9)(y + 4)(y + 3)(y + 1) \text{ in } \mathbb{F}_{13},$$

and the zeros α_i are $\{12, 10, 9, 4, 3, 1\}$.

sum of the zeros $\sum_{i=1}^n \alpha_i = 12 + 10 + 9 + 4 + 3 + 1 = 39 \equiv 0 \pmod{13}$

and $\frac{\sum_{i=1}^n \alpha_i}{q} = \frac{39}{13} = 3$

$\implies \sum_{i=1}^n \alpha_i = k \cdot q$

$$\prod_{i=1}^n \alpha_i = 12 \times 10 \times 9 \times 4 \times 3 \times 1 = 12,960 \equiv -1 \pmod{13}$$

$$\frac{\prod_{i=1}^n \alpha_i}{n} = \frac{12,960}{6} = 2,160 \text{ and } \left(\frac{\prod_{i=1}^n \alpha_i}{n}\right)^{-1} = \frac{1}{2,160} \equiv 7 \pmod{13} \equiv q - n \pmod{q}.$$

Case 4: $n = 8, q = 17$

Consider \mathbb{F}_{17} and $n = 8$. Since $8 \mid (17 - 1)$, we have

$$y^8 - 1 = (y + 16)(y + 15)(y + 13)(y + 9)(y + 8)(y + 4)(y + 2)(y + 1) \text{ in } \mathbb{F}_{17},$$

and the zeros α_i are $\{16, 15, 13, 9, 8, 4, 2, 1\}$.

sum of the zeros $\sum_{i=1}^n \alpha_i = 68 \equiv 0 \pmod{17}$

and $\frac{\sum_{i=1}^n \alpha_i}{q} = \frac{68}{17} = 4$

$\implies \sum_{i=1}^n \alpha_i = k \cdot q$

$$\prod_{i=1}^n \alpha_i = 16 \times 15 \times 13 \times 9 \times 8 \times 4 \times 2 \times 1 = 4,492,800 \equiv -1 \pmod{17}$$

$$\frac{\prod_{i=1}^n \alpha_i}{n} = \frac{4,492,800}{8} = 561,600 \text{ and } \left(\frac{\prod_{i=1}^n \alpha_i}{n}\right)^{-1} = \frac{1}{561,600} \equiv 9 \pmod{17} \equiv q - n \pmod{q}.$$

Case 5: $n = 6, q = 19$

Consider \mathbb{F}_{19} and $n = 6$. Since $9 \mid (19 - 1)$, we have

$$y^9 - 1 = (y + 18)(y + 12)(y + 11)(y + 8)(y + 7)(y + 1) \text{ in } \mathbb{F}_{19},$$

and the zeros α_i are $\{18, 12, 11, 8, 7, 1\}$.
 sum of the zeros $\sum_{i=1}^n \alpha_i = 57 \equiv 0 \pmod{19}$
 and $\frac{\sum_{i=1}^n \alpha_i}{q} = \frac{57}{19} = 3$
 $\Rightarrow \sum_{i=1}^n \alpha_i = k \cdot q$
 $\prod_{i=1}^n \alpha_i = 18 \cdot 12 \cdot 11 \cdot 8 \cdot 7 \cdot 1 = 133,056 \equiv -1 \pmod{19}$
 $\frac{\prod_{i=1}^n \alpha_i}{n} = \frac{133,056}{6} = 22,176$ and $(\frac{\prod_{i=1}^n \alpha_i}{n})^{-1} = \frac{1}{22,176} \equiv 13 \pmod{19} \equiv q - n \pmod{q}$.

Case 6: $n = 9, q = 19$

Consider \mathbb{F}_{19} and $n = 9$. Since $9 \mid (19 - 1)$, we have
 $y^9 - 1 = (y + 18)(y + 15)(y + 14)(y + 13)(y + 12)(y + 10)(y + 8)(y + 3)(y + 2) \pmod{19}$,
 and the zeros α_i are $\{18, 15, 13, 12, 10, 8, 3, 2\}$.
 sum of the zeros $\sum_{i=1}^n \alpha_i = 95 \equiv 0 \pmod{19}$
 and $\frac{\sum_{i=1}^n \alpha_i}{q} = \frac{95}{19} = 5$
 $\Rightarrow \sum_{i=1}^n \alpha_i = k \cdot q$
 $\prod_{i=1}^n \alpha_i = 18 \cdot 15 \cdot 13 \cdot 12 \cdot 10 \cdot 8 \cdot 3 \cdot 2 = 45,489,600 \equiv -1 \pmod{19}$
 $\frac{\prod_{i=1}^n \alpha_i}{n} = \frac{45,489,600}{9} = 5,054,400$ and $(\frac{\prod_{i=1}^n \alpha_i}{n})^{-1} = \frac{1}{5,054,400} \equiv 10 \pmod{19} \equiv q - n \pmod{q}$.

Case 7: $n = 22, q = 23$

Consider \mathbb{F}_{23} and $n = 22$. Since $22 \mid (23 - 1)$, we have
 $y^{22} - 1 = (y + 22)(y + 21)(y + 20)(y + 19)(y + 18)(y + 17)(y + 16)(y + 15)(y + 14)(y + 13)(y + 12)(y + 11)(y + 10)(y + 9)(y + 8)(y + 7)(y + 6)(y + 5)(y + 4)(y + 3)(y + 2)(y + 1) \pmod{23}$,
 and the zeros α_i are $\{22, 21, 20, \dots, 1\}$.
 sum of the zeros $\sum_{i=1}^n \alpha_i = 253 \equiv 0 \pmod{23}$
 and $\frac{\sum_{i=1}^n \alpha_i}{q} = \frac{253}{23} = 11$
 $\Rightarrow \sum_{i=1}^n \alpha_i = k \cdot q$
 $\prod_{i=1}^n \alpha_i = 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$
 $= 1,124,000,727,777,607,680,000 \equiv -1 \pmod{23}$
 $\frac{\prod_{i=1}^n \alpha_i}{n} = \frac{1,124,000,727,777,607,680,000}{22} = 51,090,942,171,709,440,000$, and
 $(\frac{\prod_{i=1}^n \alpha_i}{n})^{-1} = \frac{1}{51,090,942,171,709,440,000} \equiv 1 \pmod{23} \equiv q - n \pmod{q}$.

Case 8: $n = 10, q = 31$

Consider \mathbb{F}_{31} and $n = 10$. Since $10 \mid (31 - 1)$, we have
 $y^{10} - 1 = (y + 30)(y + 29)(y + 27)(y + 23)(y + 16)(y + 15)(y + 8)(y + 4)(y + 2)(y + 1) \pmod{31}$,
 and the zeros α_i are $\{30, 29, 27, 23, 16, 15, 8, 4, 2, 1\}$.
 sum of the zeros $\sum_{i=1}^n \alpha_i = 155 \equiv 0 \pmod{31}$
 and $\frac{\sum_{i=1}^n \alpha_i}{q} = \frac{155}{31} = 5$
 $\Rightarrow \sum_{i=1}^n \alpha_i = k \cdot q$
 $\prod_{i=1}^n \alpha_i = 30 \cdot 29 \cdot 27 \cdot 23 \cdot 16 \cdot 15 \cdot 8 \cdot 4 \cdot 2 \cdot 1 = 8,298,547,200 \equiv -1 \pmod{31}$
 $\frac{\prod_{i=1}^n \alpha_i}{n} = \frac{8,298,547,200}{10} = 829,854,720$ and
 $(\frac{\prod_{i=1}^n \alpha_i}{n})^{-1} = \frac{1}{829,854,720} \equiv 21 \pmod{31} \equiv q - n \pmod{q}$.

Case 9: $n = 5, q = 31$

Consider \mathbb{F}_{31} and $n = 5$. Since $5 \mid (31 - 1)$, we have

$$\begin{aligned}
 & y^4 0 - 1 = (y + 30)(y + 29)(y + 27)(y + 23)(y + 15) \quad \text{in } \mathbb{F}_{31}, \\
 & \text{and the zeros } \alpha_i \text{ are } \{30, 29, 27, 23, 15\}. \\
 & \text{sum of the zeros } \sum_{i=1}^n \alpha_i = 124 \equiv 0 \pmod{31} \\
 & \text{and } \frac{\sum_{i=1}^n \alpha_i}{q} = \frac{124}{31} = 4 \\
 & \Rightarrow \sum_{i=1}^n \alpha_i = k \cdot q \\
 & \prod_{i=1}^n \alpha_i = 30 \times 29 \times 27 \times 23 \times 15 = 8,104,050 \equiv -1 \pmod{31} \\
 & \frac{\prod_{i=1}^n \alpha_i}{n} = \frac{8,104,050}{5} = 1,620,810 \text{ and } \left(\frac{\prod_{i=1}^n \alpha_i}{n}\right)^{-1} = \frac{1}{1,620,810} \equiv 26 \pmod{31} \equiv q - n \pmod{q}.
 \end{aligned}$$

Case 10: $n = 4, q = 37$

Consider \mathbb{F}_{37} and $n = 4$. Since $4 \mid (37 - 1)$, we have

$$\begin{aligned}
 & y^4 0 - 1 = (y + 36)(y + 31)(y + 6)(y + 1) \quad \text{in } \mathbb{F}_{37}, \\
 & \text{and the zeros } \alpha_i \text{ are } \{36, 31, 6, 1\}. \\
 & \text{sum of the zeros } \sum_{i=1}^n \alpha_i = 124 \equiv 0 \pmod{37} \\
 & \text{and } \frac{\sum_{i=1}^n \alpha_i}{q} = \frac{74}{37} = 2 \\
 & \Rightarrow \sum_{i=1}^n \alpha_i = k \cdot q \\
 & \prod_{i=1}^n \alpha_i = 36 \times 31 \times 6 \times 1 = 6696 \equiv -1 \pmod{37} \\
 & \frac{\prod_{i=1}^n \alpha_i}{n} = \frac{6696}{4} = 1,674 \text{ and } \left(\frac{\prod_{i=1}^n \alpha_i}{n}\right)^{-1} = \frac{1}{1,674} \equiv 33 \pmod{37} \equiv q - n \pmod{q}.
 \end{aligned}$$

Case 11: $n = 6, q = 37$

Consider \mathbb{F}_{37} and $n = 6$. Since $6 \mid (37 - 1)$, we have

$$\begin{aligned}
 & y^6 0 - 1 = (y + 36)(y + 27)(y + 26)(y + 11)(y + 10)(y + 1) \quad \text{in } \mathbb{F}_{37}, \\
 & \text{and the zeros } \alpha_i \text{ are } \{36, 27, 26, 11, 10, 1\}. \\
 & \text{sum of the zeros } \sum_{i=1}^n \alpha_i = 111 \equiv 0 \pmod{37} \\
 & \text{and } \frac{\sum_{i=1}^n \alpha_i}{q} = \frac{111}{37} = 3 \\
 & \Rightarrow \sum_{i=1}^n \alpha_i = k \cdot q \\
 & \prod_{i=1}^n \alpha_i = 36 \times 27 \times 26 \times 11 \times 10 \times 1 = 2,779,920 \equiv -1 \pmod{37} \\
 & \frac{\prod_{i=1}^n \alpha_i}{n} = \frac{2,779,920}{6} = 463,320 \text{ and } \left(\frac{\prod_{i=1}^n \alpha_i}{n}\right)^{-1} = \frac{1}{463,320} \equiv 31 \pmod{37} \equiv q - n \pmod{q}.
 \end{aligned}$$

Case 12: $n = 9, q = 37$

Consider \mathbb{F}_{37} and $n = 9$. Since $9 \mid (37 - 1)$, we have

$$\begin{aligned}
 & y^9 0 - 1 = (y + 36)(y + 30)(y + 28)(y + 27)(y + 25)(y + 21)(y + 11)(y + 4)(y + 3) \quad \text{in } \mathbb{F}_{37}, \\
 & \text{and the zeros } \alpha_i \text{ are } \{36, 30, 28, 27, 25, 21, 11, 4, 3\}. \\
 & \text{sum of the zeros } \sum_{i=1}^n \alpha_i = 221 \equiv 0 \pmod{37} \\
 & \text{and } \frac{\sum_{i=1}^n \alpha_i}{q} = \frac{74}{37} = 2 \\
 & \Rightarrow \sum_{i=1}^n \alpha_i = k \cdot q \\
 & \prod_{i=1}^n \alpha_i = 36 \times 30 \times 28 \times 27 \times 25 \times 21 \times 11 \times 4 \times 3 = 56,582,064,000 \equiv -1 \pmod{37} \\
 & \frac{\prod_{i=1}^n \alpha_i}{n} = \frac{56,582,064,000}{9} = 6,286,896,000 \text{ and } \left(\frac{\prod_{i=1}^n \alpha_i}{n}\right)^{-1} = \frac{1}{6,286,896,000} \equiv 28 \pmod{37} \equiv q - n \pmod{q}.
 \end{aligned}$$

The table below gives summery for different values of q and n

q	n	α_i	$\sum_{i=1}^n \alpha_i$	$\frac{\sum_{i=1}^n \alpha_i}{q}$	$\prod_{i=1}^n \alpha_i$	$\frac{\prod_{i=1}^n \alpha_i}{n} \pmod q$	$(\frac{\prod_{i=1}^n \alpha_i}{n})^{-1}$
3	2	{2,1}	$3 \equiv 0 \pmod q$	1	$2 \equiv -1 \pmod q$	1	$1 \equiv q-n$
5	2	{4,1}	$5 \equiv 0 \pmod q$	1	$4 \equiv -1 \pmod q$	2	$3 \equiv q-n$
5	4	{4,3,2,1}	$10 \equiv 0 \pmod q$	2	$24 \equiv -1 \pmod q$	1	$1 \equiv q-n$
7	2	{6,1}	$7 \equiv 0 \pmod q$	1	$6 \equiv -1 \pmod q$	3	$5 \equiv q-n$
7	3	{6,5,3}	$14 \equiv 0 \pmod q$	2	$90 \equiv -1 \pmod q$	2	$4 \equiv q-n$
7	6	{6,5,4,3,2,1}	$21 \equiv 0 \pmod q$	3	$720 \equiv -1 \pmod q$	1	$1 \equiv q-n$
11	2	{10,1}	$11 \equiv 0 \pmod q$	1	$10 \equiv -1 \pmod q$	5	$9 \equiv q-n$
11	5	{10,8,7,6,2}	$33 \equiv 0 \pmod q$	3	$6,720 \equiv -1 \pmod q$	2	$6 \equiv q-n$
13	2	{12,1}	$13 \equiv 0 \pmod q$	1	$12 \equiv -1 \pmod q$	6	$11 \equiv q-n$
13	3	{12,10,4}	$26 \equiv 0 \pmod q$	2	$480 \equiv -1 \pmod q$	4	$10 \equiv q-n$
13	4	{12,5,1,8}	$26 \equiv 0 \pmod q$	2	$480 \equiv -1 \pmod q$	3	$9 \equiv q-n$
13	6	{12,10,9,4,3,1}	$39 \equiv 0 \pmod q$	3	$12,960 \equiv -1 \pmod q$	2	$7 \equiv q-n$
13	12	{12,11,10,...,1}	$78 \equiv 0 \pmod q$	6	$79,001,600 \equiv -1 \pmod q$	1	$1 \equiv q-n$
17	2	{16,1}	$17 \equiv 0 \pmod q$	1	$16 \equiv -1 \pmod q$	8	$15 \equiv q-n$
17	4	{14,13,16}	$34 \equiv 0 \pmod q$	2	$832 \equiv -1 \pmod q$	4	$13 \equiv q-n$
17	8	{12,4,8,9,13,15,16}	$68 \equiv 0 \pmod q$	4	$1,797,120 \equiv -1 \pmod q$	2	$9 \equiv q-n$
17	16	{16,15,...,1}	$136 \equiv 0 \pmod q$	8	$20,922,789,888,000 \equiv -1 \pmod q$	1	$1 \equiv q-n$
19	2	{18,1}	$19 \equiv 0 \pmod q$	1	$18 \equiv -1 \pmod q$	9	$17 \equiv q-n$
19	3	{8,12,18}	$38 \equiv 0 \pmod q$	2	$1,728 \equiv -1 \pmod q$	6	$16 \equiv q-n$
19	6	{1,7,8,11,12,18}	$57 \equiv 0 \pmod q$	3	$133,056 \equiv -1 \pmod q$	3	$13 \equiv q-n$
19	9	{2,3,8,10,12,13,14,15,18}	$95 \equiv 0 \pmod q$	5	$283,046,400 \equiv -1 \pmod q$	2	$10 \equiv q-n$
19	18	{1,2,3,...,18}	$171 \equiv 0 \pmod q$	9	$6,402,373,705,728,000 \equiv -1 \pmod q$	1	$1 \equiv q-n$
23	2	{22,1}	$23 \equiv 0 \pmod q$	1	$22 \equiv -1 \pmod q$	11	$21 \equiv q-n$
23	11	{5,7,10,11,14,15,17,19,20,21,22}	$161 \equiv 0 \pmod q$	7	$2,412,984,420,000 \equiv -1 \pmod q$	2	$12 \equiv q-n$
31	2	{30,1}	$31 \equiv 0 \pmod q$	1	$30 \equiv -1 \pmod q$	15	$29 \equiv q-n$
31	3	{6,26,30}	$62 \equiv 0 \pmod q$	2	$4,680 \equiv -1 \pmod q$	10	$28 \equiv q-n$
31	5	{15,23,27,29,30}	$124 \equiv 0 \pmod q$	4	$8,104,050 \equiv -1 \pmod q$	6	$26 \equiv q-n$
31	6	{1,5,6,25,26,30}	$93 \equiv 0 \pmod q$	3	$585,000 \equiv -1 \pmod q$	5	$25 \equiv q-n$
31	10	{1,2,4,8,15,16,23,27,29,30}	$155 \equiv 0 \pmod q$	5	$8,297,473,200 \equiv -1 \pmod q$	3	$21 \equiv q-n$
37	2	{36,1}	$37 \equiv 0 \pmod q$	1	$36 \equiv -1 \pmod q$	18	$35 \equiv q-n$
37	3	{36,27,11}	$74 \equiv 0 \pmod q$	2	$10,692 \equiv -1 \pmod q$	12	$34 \equiv q-n$
37	4	{36,31,6,1}	$74 \equiv 0 \pmod q$	2	$6,696 \equiv -1 \pmod q$	9	$33 \equiv q-n$
37	6	{36,27,26,11,10,1}	$111 \equiv 0 \pmod q$	3	$2,779,920 \equiv -1 \pmod q$	6	$31 \equiv q-n$
37	9	{36,30,28,27,25,21,11,4,3}	$185 \equiv 0 \pmod q$	5	$56,582,064,000 \equiv -1 \pmod q$	4	$28 \equiv q-n$
37	12	{36,31,29,27,26,23,14,11,10,8,6,1}	$222 \equiv 0 \pmod q$	6	$38,597,338,644,480 \equiv -1 \pmod q$	3	$25 \equiv q-n$

Table 1: Zeros of cyclotomic polynomials over \mathbb{F}_q

3 Conclusion

In this study, it has been established that provided $n \mid (q-1)$, the zeros of the linear factors of the cyclotomic polynomial $y^n - 1$ over \mathbb{F}_q exhibits predictable modular relationships. From the cases discussed and the data obtained in the table of *Zeros of cyclotomic polynomials over \mathbb{F}_q* confirms that for all tested pairs (q, n) with $n \mid (q-1)$, the linear factorization

$$y^n - 1 = \prod_{i=1}^n (y + \alpha_i) \quad \text{over } \mathbb{F}_q$$

satisfies the following identities:

- i. $\sum_{i=1}^n \alpha_i \equiv 0 \pmod q$,
- ii. $\prod_{i=1}^n \alpha_i \equiv -1 \pmod q$,
- iii. $(\frac{\prod_{i=1}^n \alpha_i}{n})^{-1} \equiv q-n \pmod q$.

These relations hold independently of the particular choice of primitive n th root of unity in \mathbb{F}_q . In coding theory the knowledge of specific roots of unity and their patterns enables the construction of generator polynomials with desired error correcting properties. The predictable nature of these sums and product could be exploited for efficient encoding

algorithm. Future investigations should strive to prove the above conjecture.

References

- [1] Richa G, Bhudev S. Generation of variable length error correcting codes over using constant length error correcting codes. *International journal of emerging trends in engineering and development*. 2012;1(2):269-279.
- [2] Maganga NJ, Kivunge BM. Enumeration of cyclic codes over $GF(19)$. *International Journal of Science and Research*. 2017;6(4).
ISSN: 2319-7064
- [3] Olege F. On the generators of codes of ideals of the polynomial ring for error control; 2017.
- [4] Adams SS. *Introduction to Coding Theory*, (3rd ed.), Cornel University Press, Berlin; 2008.
- [5] Berlekamp E. *Algebraic Coding Theory*. New York, USA: McGraw-Hill Book company; 1968.
- [6] Bierbrauer J. *Introduction to Coding Theory*. Chapman & Hall/CRC; 2004.
- [7] Blake IF. Codes over certain rings. *Information and Control*. 1972;20(4):396–404.
- [8] Hill R. *A first course in coding theory*. Oxford: Claredon Press; 1986.
- [9] Arnold A, Monagan M. Calculating cyclotomic polynomials. *Mathematics of Computation*. 2011;80(276):2359–2379.
- [10] Bamunoba A. *Cyclotomic Polynomials*. London: Oxford; 2011.
- [11] Lao H, Kivunge B, Muthoka G, Mwangi P. On the number of cyclotomic cosets and cyclic codes over \mathbb{Z}_{13} . *International Journal of Scientific Research and Innovative Technology*. 2018;5(6).
ISSN: 2313-3759
- [12] Lao H, Kivunge B, Muthoka G, Mwangi P. Enumeration of cyclic codes over $GF(17)$. *International Journal of Scientific Research and Innovative Technology*. May 2015;2(5).
ISSN: 2313-3759
- [13] Manish G, Bhullar JS, Vinocha OP. On the Combination of five cyclic code. *Int. J. Contemp. Math. Sciences*. 2010;5(33):1627-1635.
- [14] Runji FM. Enumeration of cyclic codes over $GF(5)$. *International Journal of Multi Disciplinary Research*. 2014;1(6):2348-2052.
- [15] Ongili P. On the Generalization of the Number of Cyclic codes Over the Prime Field $GF(37)$. *Journal of Advances in Mathematics and Computing Science*. 2024;39(6).
ISSN 2456-9968.
- [16] Simatwo KB. Enumeration of cyclic codes over $GF(23)$. *Journal of Advances in Mathematics and Computing Science* 2023;38(9).
ISSN 2456-9968.
- [17] Ondiany, J. J. O., Karioko, O. R., Mude, L. H., Monari, F. N. (2024). On the Number of Cyclic Codes Over \mathbb{Z}_{31} . *Journal of Advances in Mathematics and Computer Science*, 39(7), 55–69.
- [18] Ongili, P., Mude, L. H., Ndung'u, K. J. (2024). On the generalization of the number of cyclic codes over the prime field $GF(37)$.

