Journal of Advances in Mathematics and Computer Science

Volume XXX, Issue XX, Page XX-XX, 2024; Article no.JAMCS.116921

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

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

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JAMCS/2024/XXXXX

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here:

Received:DD/MM/20YY

Accepted:DD/MM/20YY

Published:DD/MM/20YY

Original Research Article

Abstract

Cite as:

Journal of Advances in Mathematics and Computer Science

Volume XXX, Issue XX, Page XX-XX, 2024; Article no.JAMCS.116921

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

JAMCS2.JPG

The study of cyclic codes via cyclotomic polynomial over Galois field has been active area of research due to their direct application in generating cyclic codes and error-correcting codes. Let q be a prime number and $\mathbb{F}_q$ be a given finite field with q elements. This research investigates the cyclotomic polynomial y^n-1 specifically focusing on cases where y^n-1 completely decomposes into linear factors over $\mathbb{F}_q$ for $q \leq 37$ and $n \geq 2$. The relationships between the field, the sum, and the product of the zeros of these linear factors are explored. The results shows that for each tested pair (q,n) where $n \mid (q-1)$, the sum of the roots is always $\equiv 0 \pmod{q}$, the product of the roots is $\equiv -1 \pmod{q}$ and the inverse of the ratio of the product of the roots to n is $\equiv q-n \pmod{q}$. The predictable modular relationships among the zeros, can be applied to the efficient design of generator polynomials with desired properties.

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]. These polynomials factors into linear factors if $n \mid (q-1)$ as shown in [2, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19]. The understanding of their zeros are important in construction of generator polynomials [1, 3, 5]. In this research 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

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

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 $y^n-1 = (y+\alpha_1)(y+\alpha_2)(y+\alpha_3)\ldots(y+\alpha_n) = \prod_{i=1}^{n}(y+\alpha_i)$ Then, for $n \geq 2$;*

i $\sum_{i=1}^{n} \alpha_i = K.q$ *where* $k \in \mathbb{Z}^+$

ii $\prod_{i=1}^{n} \alpha_i = r.n$ *where* $r \in \mathbb{Z}^+$

iii $\prod_{i=1}^{n} \alpha_i \equiv$*-1* $\pmod{q}$

Journal of Advances in Mathematics and Computer Science

Volume XXX, Issue XX, Page XX-XX, 2024; Article no.JAMCS.116921

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

iv $(\frac{\prod_{i=1}^{n}\alpha_i}{n})^{-1} \equiv q-n \mod q$

Let $\mathbb{F}_q$ be a finite field and $y^n-1=(y+\alpha_1)(y+\alpha_2)(y+\alpha_3)\ldots(y+\alpha_n)=\prod_{i=1}^{n}(y+\alpha_i)$ 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 $\sum_{i=1}^{n}\alpha_i = 4+3+2+1=10 \equiv 0 \mod 5$
and $\frac{\sum_{i=1}^{n}\alpha_i}{q} = \frac{10}{5} = 2. \implies \sum_{i=1}^{n}\alpha_i$ =k.q
$\prod_{i=1}^{n}\alpha_i = 4.3.2.1 = 24 \equiv -1 \mod 5$
$\frac{\prod_{i=1}^{n}\alpha_i}{n} = \frac{24}{4} = 6$ and $(\frac{\prod_{i=1}^{n}\alpha_i}{n})^{-1} = \frac{1}{6} \equiv 1 \mod 5 \equiv q-n \mod q$.

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

Consider $\mathbb{F}_{11}$ and $n=5$. Since $5 \mid (11-1)$, we have
$y^5-1=(y+10)(y+8)(y+7)(y+6)(y+2)$ in $\mathbb{F}_{11}$,
and the zeros α_i are $\{10,8,7,6,2\}$.
sum of the zeros $\sum_{i=1}^{n}\alpha_i = 10+8+7+6+2=33 \equiv 0 \mod 11$
and $\frac{\sum_{i=1}^{n}\alpha_i}{q} = \frac{33}{11} = 3$
$\implies \sum_{i=1}^{n}\alpha_i$ =k.q
$\prod_{i=1}^{n}\alpha_i = 10.8.7.6.2 = 6,720 \equiv -1 \mod 11$
$\frac{\prod_{i=1}^{n}\alpha_i}{n} = \frac{6,720}{5} = 1344 \equiv -1 \mod 11$ and $(\frac{\prod_{i=1}^{n}\alpha_i}{n})^{-1} = \frac{1}{1344} \equiv \frac{1}{2} \mod 11 = 6 \mod 11 \equiv q-n \mod q$.

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

Consider $\mathbb{F}_{13}$ and $n=6$. Since $6 \mid (13-1)$, we have
$y^6-1=(y+12)(y+10)(y+9)(y+4)(y+3)(y+1)$ in $\mathbb{F}_{13}$,
and the zeros α_i are $\{12,10,9,4,3,1\}$.
sum of the zeros $\sum_{i=1}^{n}\alpha_i = 12+10+9+4+3+1=39 \equiv 0 \mod 13$
and $\frac{\sum_{i=1}^{n}\alpha_i}{q} = \frac{39}{13} = 3$
$\implies \sum_{i=1}^{n}\alpha_i$ =k.q
$\prod_{i=1}^{n}\alpha_i = 12.10.9.4.3.1 = 12,960 \equiv -1 \mod 13$
$\frac{\prod_{i=1}^{n}\alpha_i}{n} = \frac{12,960}{6} = 2,160$ and $(\frac{\prod_{i=1}^{n}\alpha_i}{n})^{-1} = \frac{1}{2,160} \equiv 7 \mod 13 \equiv q-n \mod q$.

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

Consider $\mathbb{F}_{17}$ and $n=8$. Since $8 \mid (17-1)$, we have
$y^8-1=(y+16)(y+15)(y+13)(y+9)(y+8)(y+4)(y+2)(y+1)$ in $\mathbb{F}_{13}$,
and the zeros α_i are $\{16,15,13,9,8,4,2,1\}$.
sum of the zeros $\sum_{i=1}^{n}\alpha_i = 68 \equiv 0 \mod 17$
and $\frac{\sum_{i=1}^{n}\alpha_i}{q} = \frac{68}{17} = 4$
$\implies \sum_{i=1}^{n}\alpha_i$ =k.q
$\prod_{i=1}^{n}\alpha_i = 16.15.13.9.8.4.5.1 = 4,492,800 \equiv -1 \mod 17$
$\frac{\prod_{i=1}^{n}\alpha_i}{n} = \frac{4,492,800}{8} = 561,600$ and $(\frac{\prod_{i=1}^{n}\alpha_i}{n})^{-1} = \frac{1}{561,600} \equiv 9 \mod 17 \equiv q-n \mod q$.

Journal of Advances in Mathematics and Computer Science

Volume XXX, Issue XX, Page XX-XX, 2024; Article no.JAMCS.116921

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

JAMCS2.JPG

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

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

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

and the zeros α_i are $\{18, 12, 11, 8, 7, 1\}$.

sum of the zeros $\sum_{i=1}^{n} \alpha_i = 57 \equiv 0 \mod 19$

and $\frac{\sum_{i=1}^{n} \alpha_i}{q} = \frac{57}{19} = 3$

$\Longrightarrow \sum_{i=1}^{n} \alpha_i$ =k.q

$\prod_{i=1}^{n} \alpha_i = 18.12.11.8.7.1 = 133,056 \equiv -1 \mod 19$

$\frac{\prod_{i=1}^{n} \alpha_i}{n} = \frac{133,056}{6} = 22,176$ and $(\frac{\prod_{i=1}^{n} \alpha_i}{n})^{-1} = \frac{1}{22,176} \equiv 13 \mod 19 \equiv q - n \mod q$.

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

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

$y^9 - 1 = (y+18)(y+15)(y+14)(y+13)(y+12)(y+10)(y+8)(y+3)(y+2)$ in $\mathbb{F}_{19}$,

and the zeros α_i are $\{18, 15, 13, 12, 10, 8, 3, 2\}$.

sum of the zeros $\sum_{i=1}^{n} \alpha_i = 95 \equiv 0 \mod 19$

and $\frac{\sum_{i=1}^{n} \alpha_i}{q} = \frac{95}{19} = 5$

$\Longrightarrow \sum_{i=1}^{n} \alpha_i$ =k.q

$\prod_{i=1}^{n} \alpha_i = 18.15.13.12.10.8.3.2 = 45,489,600 \equiv -1 \mod 19$

$\frac{\prod_{i=1}^{n} \alpha_i}{n} = \frac{45,489,600}{9} = 7,581,600$ and $(\frac{\prod_{i=1}^{n} \alpha_i}{n})^{-1} = \frac{1}{7,581,600} \equiv 10 \mod 19 \equiv q - n \mod q$.

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

Consider $\mathbb{F}_{23}$ and $n = 22$. Since $22 \mid (23-1)$, we have

$y^{22} - 1 = (y+22)(y+21)(y+20)(y+19)(y+18)(y+17)(y+16)(y+15)(y+14)(y+13)(y+12)(y+11)(y+10)(y+9)(y+8)(y+7)(y+6)(y+5)(y+4)(y+3)(y+2)(y+1)$ in $\mathbb{F}_{23}$,

and the zeros α_i are $\{22, 21, 20, ..., 1\}$.

sum of the zeros $\sum_{i=1}^{n} \alpha_i = 253 \equiv 0 \mod 23$

and $\frac{\sum_{i=1}^{n} \alpha_i}{q} = \frac{253}{23} = 11$

$\Longrightarrow \sum_{i=1}^{n} \alpha_i$ =k.q

$\prod_{i=1}^{n} \alpha_i = 22.21.20.19.18.17.16.15.14.13.12.11.10.9.8.7.6.5.4.3.2.1$

$= 1,124,000,727,777,607,680,000 \equiv -1 \mod 23$

$\frac{\prod_{i=1}^{n} \alpha_i}{n} = \frac{1,124,000,727,777,607,680,000}{22} = 51,090,942,171,709,440,000$,and

$(\frac{\prod_{i=1}^{n} \alpha_i}{n})^{-1} = \frac{1}{51,090,942,171,709,440,000} \equiv 1 \mod 23 \equiv q - n \mod q$.

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

Consider $\mathbb{F}_{31}$ and $n = 10$. Since $10 \mid (31-1)$, we have

$y^{10} - 1 = (y+30)(y+29)(y+27)(y+23)(y+16)(y+15)(y+8)(y+4)(y+2)(y+1)$ in $\mathbb{F}_{31}$,

and the zeros α_i are $\{30, 29, 27, 23, 16, 15, 8, 4, 2, 1\}$.

sum of the zeros $\sum_{i=1}^{n} \alpha_i = 155 \equiv 0 \mod 19$

and $\frac{\sum_{i=1}^{n} \alpha_i}{q} = \frac{155}{31} = 5$

$\Longrightarrow \sum_{i=1}^{n} \alpha_i$ =k.q

$\prod_{i=1}^{n} \alpha_i = 30.29.27.23.16.15.8.4.2.1 = 8,298,547,200 \equiv -1 \mod 31$

$\frac{\prod_{i=1}^{n} \alpha_i}{n} = \frac{8,298,547,200}{10} = 829,854,720$ and

$(\frac{\prod_{i=1}^{n} \alpha_i}{n})^{-1} = \frac{1}{829,854,720} \equiv 21 \mod 31 \equiv q - n \mod q$.

Journal of Advances in Mathematics and Computer Science

Volume XXX, Issue XX, Page XX-XX, 2024; Article no.JAMCS.116921

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

JAMCS2.JPG

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

Consider $\mathbb{F}_{31}$ and $n = 5$. Since $5 \mid (31-1)$, we have
$y^5 - 1 = (y+30)(y+29)(y+27)(y+23)(y+15)$ in $\mathbb{F}_{31}$,
and the zeros α_i are $\{30, 29, 27, 23, 15\}$.
sum of the zeros $\sum_{i=1}^{n} \alpha_i = 124 \equiv 0 \mod 31$
and $\frac{\sum_{i=1}^{n} \alpha_i}{q} = \frac{124}{31} = 4$
$\implies \sum_{i=1}^{n} \alpha_i$ =k.q
$\prod_{i=1}^{n} \alpha_i = 30.29.27.23.15 = 8,104,050 \equiv -1 \mod 31$
$\frac{\prod_{i=1}^{n} \alpha_i}{n} = \frac{8,104,050}{5} = 1,620,810$ and $(\frac{\prod_{i=1}^{n} \alpha_i}{n})^{-1} = \frac{1}{1,620,810} \equiv 26 \mod 31 \equiv q - n \mod q$.

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

Consider $\mathbb{F}_{37}$ and $n = 4$. Since $4 \mid (37-1)$, we have
$y^4 - 1 = (y+36)(y+31)(y+6)(y+1)$ in $\mathbb{F}_{37}$,
and the zeros α_i are $\{36, 31, 6, 1\}$.
sum of the zeros $\sum_{i=1}^{n} \alpha_i = 124 \equiv 0 \mod 37$
and $\frac{\sum_{i=1}^{n} \alpha_i}{q} = \frac{74}{37} = 2$
$\implies \sum_{i=1}^{n} \alpha_i$ =k.q
$\prod_{i=1}^{n} \alpha_i = 36.31.6.1 = 6696 \equiv -1 \mod 37$
$\frac{\prod_{i=1}^{n} \alpha_i}{n} = \frac{6696}{4} = 1,674$ and $(\frac{\prod_{i=1}^{n} \alpha_i}{n})^{-1} = \frac{1}{1,674} \equiv 33 \mod 37 \equiv q - n \mod q$.

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

Consider $\mathbb{F}_{37}$ and $n = 6$. Since $6 \mid (37-1)$, we have
$y^6 - 1 = (y+36)(y+27)(y+26)(y+11)(y+10)(y+1)$ in $\mathbb{F}_{37}$,
and the zeros α_i are $\{36, 27, 26, 11, 10, 1\}$.
sum of the zeros $\sum_{i=1}^{n} \alpha_i = 111 \equiv 0 \mod 37$
and $\frac{\sum_{i=1}^{n} \alpha_i}{q} = \frac{111}{37} = 3$
$\implies \sum_{i=1}^{n} \alpha_i$ =k.q
$\prod_{i=1}^{n} \alpha_i = 36.27.26.11.10.1 = 2,779,920 \equiv -1 \mod 37$
$\frac{\prod_{i=1}^{n} \alpha_i}{n} = \frac{2,779,920}{6} = 463,320$ and $(\frac{\prod_{i=1}^{n} \alpha_i}{n})^{-1} = \frac{1}{463,320} \equiv 31 \mod 37 \equiv q - n \mod q$.

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

Consider $\mathbb{F}_{37}$ and $n = 9$. Since $9 \mid (37-1)$, we have
$y^9 - 1 = (y+36)(y+30)(y+28)(y+27)(y+25)(y+21)(y+11)(y+4)(y+3)$ in $\mathbb{F}_{37}$,
and the zeros α_i are $\{36, 30, 28, 27, 25, 21, 11, 4, 3\}$.
sum of the zeros $\sum_{i=1}^{n} \alpha_i = 221 \equiv 0 \mod 37$
and $\frac{\sum_{i=1}^{n} \alpha_i}{q} = \frac{74}{37} = 2$
$\implies \sum_{i=1}^{n} \alpha_i$ =k.q
$\prod_{i=1}^{n} \alpha_i = 36.30.28.27.25.21.11.4.3 = 56,582,064,000 \equiv -1 \mod 37$
$\frac{\prod_{i=1}^{n} \alpha_i}{n} = \frac{56,582,064,000}{9} = 6,286,896,000$ and $(\frac{\prod_{i=1}^{n} \alpha_i}{n})^{-1} = \frac{1}{6,286,896,000} \equiv 28 \mod 37 \equiv q - n \mod q$.

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

Journal of Advances in Mathematics and Computer Science

Volume XXX, Issue XX, Page XX-XX, 2024; Article no.JAMCS.116921

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

JAMCS2.JPG

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

Journal of Advances in Mathematics and Computer Science

Volume XXX, Issue XX, Page XX-XX, 2024; Article no.JAMCS.116921

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

These relations hold independently of the particular choice of primitive nth 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.

Competing Interests

Authors have declared that no competing interests exist.

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] Bierbrauer J. Introduction to Coding Theory. Chapman & Hall/CRC; 2004.

[6] Arnold A, Monagan M. Calculating cyclotomic polynomials. Mathematics of Computation. 2011;80(276):2359–2379.

[7] Bamunoba A. Cyclotomic Polynomials. London: Oxford; 2011.

[8] 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

[9] Lao H, Kivunge B, Muthoka G, Mwangi P. Enumeration of cyclic codes over GF [17]. nternational Journal of Scientific Research and Innovative Technology. May 2015;2(5).
ISSN: 2313-3759

[10] Manish G, Bhullar JS, Vinocha OP. On the Combination of five cyclic code. Int. J. Contemp. Math. Sciences. 2010;5(33:1627-1635.

[11] Runji FM. Enumeration of cyclic codes over $GF(5)$.International Journal of Multi Disciplinary Research. 2014;1(6):2348-2052.

[12] 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.

[13] Simatwo KB. Enumeration of cyclic codes over $GF(23)$. Journal of Advances in Mathematics and Computing Science 2023;38(9).
ISSN 2456-9968.

[14] Ondiany, J. J. O., Karieko, 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.

[15] 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).

[16] Lidl, R., Niederreiter, H. (1997). Finite Fields. Cambridge University Press.

[17] van Lint, J. H. (1999). Introduction to Coding Theory. Springer.

Journal of Advances in Mathematics and Computer Science

Volume XXX, Issue XX, Page XX-XX, 2024; Article no.JAMCS.116921

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

JAMCS2.JPG

[18] Ding, C., Niederreiter, H. (1999). Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory, 45(2), 760–765.

[19] Wan, Z. X. (2003). Lectures on Finite Fields and Galois Rings. World Scientific.