mathematics

MDPI

Article

A Note on Factorization and the Number of Irreducible Factors of $x^n - \lambda$ over Finite Fields

Jinle Liu and Hongfeng Wu *

College of Science, North China University of Technology, Beijing 100144, China; 2023312050128@mail.ncut.edu.cn
* Correspondence: whfmath@ncut.edu.cn

Abstract: Let $\mathbb{F}_q$ be a finite field, and let n be a positive integer such that $\gcd(q, n) = 1$. The irreducible factors of $x^n - 1$ and $x^n - \lambda$ are fundamental concepts with wide applications in cyclic codes and constacyclic codes. Furthermore, the number of irreducible factors of $x^n - 1$ and $x^n - \lambda$ is useful in many computational problems involving cyclic codes and constacyclic codes. In this paper, we give a more concrete irreducible factorization of $x^n - 1$ and $x^n - \lambda$. Based on this, the number of irreducible factors of $x^n - 1$ and $x^n - \lambda$ over $\mathbb{F}_q$, for any $\lambda \in \mathbb{F}_q^*$, is determined through research on the representatives and the sizes of the q-cyclotomic cosets. As applications, we present the necessary and sufficient conditions for $| \mathfrak{F}(x^n - 1) | = 6$ and a more concrete factorization of $x^n - 1$ in these cases.

Keywords: finite fields; irreducible factors; cyclotomic polynomial; cyclotomic cosets; constacyclic codes

MSC: 11T06; 11T71

1. Introduction

Let $\mathbb{F}_q$ be a finite field, and let n be a positive integer such that $\gcd(n, q) = 1$. For any $\gamma \in \mathbb{Z}/n\mathbb{Z}$, the q-cyclotomic coset modulo n containing γ is defined by the subset

$$c_{n/q}(\gamma) = \{\gamma, \gamma q, \cdots, \gamma q^{\tau-1}\},$$

where τ is the smallest positive integer such that $\gamma q^\tau \equiv \gamma \pmod{n}$. Each element in $c_{n/q}(\gamma)$ is called a representative of the coset $c_{n/q}(\gamma)$. The study of cyclotomic cosets plays a very important role in many computational problems. Since q-cyclotomic cosets completely determine the irreducible factorization of $x^n - 1, \Phi_n(x)$, and $x^n - \lambda$ over $\mathbb{F}_q$, cyclotomic cosets are also needed in coding theory, such as the classification of constacyclic codes and counting problems involving constacyclic codes. These problems all require the parameters of cyclotomic cosets, for example, leaders, sizes, or representatives.

In [1], the q-cyclotomic cosets modulo n contained in the subset $1 + r\mathbb{Z}/nr\mathbb{Z}$, such that $\gcd(nr, q) = 1$ and $r \mid q - 1$, were determined. Further, the authors enumerated the Euclidean self-dual codes. In [2,3], algorithms for calculating the leader of cyclotomic cosets were given based on the stream cipher m-sequences and problems in statistical physics, respectively. Determining the representatives and the sizes of q-cyclotomic cosets modulo n under certain conditions can help in studying problems involving constacyclic codes. Some research work can be seen in [4–11].

check for updates

Academic Editor: Askar Tuganbaev

Received: 26 November 2024
Revised: 24 December 2024
Accepted: 25 December 2024
Published: 31 January 2025

Citation: Liu, J.; Wu, H. A Note on Factorization and the Number of Irreducible Factors of $x^n - \lambda$ over Finite Fields. *Mathematics* **2025**, *13*, 473. https://doi.org/10.3390/math13030473

This paper was inspired by [12]. The purpose of this paper is to determine the number of irreducible factors of $x^n - \lambda$ over $\mathbb{F}_q$ for any $\lambda \in \mathbb{F}_q^*$. We know that we can calculate the number of irreducible factors of $x^n - 1$ using the equation

$$x^n - 1 = \prod_{d|n} \Phi_n(x),$$

where, for any $d \mid n$, $\Phi_d(x)$ can be factored into $\frac{\phi(d)}{\mathrm{ord}_d(q)}$ monic irreducible polynomials of the same degree $\mathrm{ord}_d(q)$ over $\mathbb{F}_q$. In [12], a necessary and sufficient condition for

$$| \mathfrak{F}(x^n - 1) | = s$$

was given, where $| \mathfrak{F}(x^n - 1) |$ denotes the number of distinct irreducible factors of $x^n - 1$ over $\mathbb{F}_q$. Suppose that $n_1, n_2, \cdots, n_t$ are t factors of n, and d_{n_i} denotes the order of q modulo n_i. Then,

$$| \mathfrak{F}(x^n - 1) | = s$$

if and only if

$$x_i = \frac{\phi(n_i)}{d_{n_i}} (i = 1, 2, \cdots, t)$$

is a solution to the Diophantine equation

$$x_1 + x_2 + \cdots + x_t = s.$$

As an application, [12] obtained the sufficient and necessary conditions for $| \mathfrak{F}(x^n - 1) | = 3, 4, 5$.

Through a careful study of the q-cyclotomic cosets, we give more concrete factorization of $x^n - 1$ and $x^n - \lambda$ than the factorization formula given in [13]. Then, based on the splitting or stability of cyclotomic cosets, we determine the number of irreducible factors of $x^n - \lambda$ and $x^n - 1$ over $\mathbb{F}_q$ for any $\lambda \in \mathbb{F}_q^*$; however, the method differs from that in [12]. As an application, we establish the necessary and sufficient conditions when

$$| \mathfrak{F}(x^n - 1) | = 6.$$

In addition, a more concrete factorization of $x^n - 1$ in these cases is given.

2. Preliminaries

Throughout this paper, we assume that n is a positive integer and that $\mathbb{F}_q$ denotes a finite field with q elements, where $q = p^e$ is a power of a prime p and $\gcd(p, n) = 1$. $\mathbb{F}_q^* = \mathbb{F}_q / \{0\}$ is the multiplicative group of $\mathbb{F}_q$ consisting of all non-zero elements of $\mathbb{F}_q$. We first review some basic results in number theory and finite fields, which we will use in the subsequent sections.

2.1. Basic Number Theory

Let ℓ be a prime number. We denote the ℓ-adic valuation of n as follows:

$$v_\ell(n) = \max\{k \in \mathbb{Z} : \ell^k \mid n\}.$$

Then we introduce the following lift-the-exponent lemmas in two cases.

Lemma 1 ([2]). *Let ℓ be an odd prime number, and let m be an integer such that $\ell \mid m-1$. Then, $v_\ell(m^d-1) = v_\ell(m-1) + v_\ell(d)$ for any positive integer d.*

Lemma 2 ([2]). *Let m be an odd integer, and d be a positive integer. Based on this, the following cases arise:*

(1) If $m \equiv 1 \pmod 4$, then

$$v_2(m^d-1) = v_2(m-1) + v_2(d),\ v_2(m^d+1) = 1.$$

(2) If $m \equiv 3 \pmod 4$ and d is odd, then

$$v_2(m^d-1) = 1,\ v_2(m^d+1) = v_2(m+1).$$

(3) If $m \equiv 3 \pmod 4$ and d is even, then

$$v_2(m^d-1) = v_2(m+1) + v_2(d),\ v_2(m^d+1) = 1.$$

2.2. Cyclotomic Cosets

If the decomposition of n is given by $n = p_1^{e_1} \cdots p_s^{e_s}$, where $p_1, \cdots, p_s$ are distinct prime numbers and $e_1, \cdots, e_s$ are positive integers, m is an integer coprime to n. We define $\mathrm{rad}(n)$ and $\mathrm{ord}_n(m)$ as follows:

$$\begin{aligned} \mathrm{rad}(n) &= p_1 \cdots p_s, \\ \mathrm{ord}_n(m) &= \min\{k \in \mathbb{Z} : m^k \equiv 1 \pmod n\}. \end{aligned}$$

If $(\mathbb{Z}/n\mathbb{Z})^*$ is a cyclic group, each generator of $(\mathbb{Z}/n\mathbb{Z})^*$ is called a primitive root modulo n. A well-known theorem about the existence of primitive roots is shown below.

Lemma 3 ([14]). *Let n be a positive integer. Then, n possesses primitive roots if and only if n is of the form $2, 4, p^\alpha$, or $2p^\alpha$, where p is an odd prime and α is a positive integer.*

We also review some familiar results below.

Lemma 4 ([15]). *Let η be a primitive root modulo an odd prime ℓ. If $\eta^{\ell-1}$ is not congruent to 1 modulo ℓ^2, then η is a primitive root modulo ℓ^d for all $d \geq 1$.*

Lemma 5 ([12]). *Let ℓ be an odd prime and η be a primitive root modulo ℓ^2, with $\gcd(\eta, \ell) = 1$. Then, η is a primitive root modulo ℓ^d for all $d \geq 1$.*

Lemma 6 ([12]). *Let η be a primitive root modulo ℓ^d. Then η is a primitive root modulo $2\ell^d$, where η, ℓ, and d are defined as above.*

Recently, a criterion for the primitive root system and a proof of the existence of the primitive root system modulo $p_1^{e_1} \cdots p_s^{e_s}$ were given in [16].

Lemma 7 ([16]). *Let $p_1, \cdots, p_s$ be distinct odd primes, and let $e_1, \cdots, e_s$ be positive integers. An s-tuple $(\eta_1, \cdots, \eta_s)$ of integers is said to be a primitive root system modulo $p_1^{e_1} \cdots p_s^{e_s}$ if, for any $1 \leq i \leq s$, the following conditions hold:*

(1) η_i is a primitive root modulo p_i^d for all $d \geq 1$;

(2) $\eta_i \equiv 1 \pmod{p_j^{e_j}}$ for any $j \neq i$.

For any odd primes $p_1, \cdots, p_s$ and positive integers $e_1, \cdots, e_s$, there exists a primitive root system modulo $p_1^{e_1} \cdots p_s^{e_s}$.

Further, the explicit representatives and sizes of q-cyclotomic cosets modulo an odd integer n are given. If $n = p_1^{e_1} \cdots p_s^{e_s}$ for distinct odd primes $p_1, \cdots, p_s$ different from p and positive integers $e_1, \cdots, e_s$, fix a system of primitive roots $(\eta_1, \cdots, \eta_s)$ modulo n. For any integers $y_1, \cdots, y_s$ such that $0 \le y_i \le e_i$, $i = 1, \cdots, s$, the notations are defined as follows:

(1) $f_{i,y_i} = \mathrm{ord}_{p_i^{e_i - y_i}}(q)$;

(2) $g_{i,y_i} = \phi(p_i^{e_i - y_i})/f_{i,y_i}$;

(3) $\tau_{y_1 \cdots y_s} = \mathrm{ord}_{p_1^{e_1 - y_1} \cdots p_s^{e_s - y_s}}(q) = \mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})$.

Lemma 8 ([16]). *Let $p_1, \cdots, p_s$ be distinct odd prime numbers different from p, and let $e_1, \cdots, e_s$ be positive integers. Then, all the distinct q-cyclotomic cosets modulo $n = p_1^{e_1} \cdots p_s^{e_s}$ are given by*

$$c_{n/q}(\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s}) = \{\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s}, \eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} q, \cdots, \eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} q^{\tau_{y_1 \cdots y_s} - 1}\}$$

for $0 \le y_i \le e_i$, $i = 1, \cdots, s$; $0 \le x_1 \le g_{1,y_1} - 1$; and $0 \le x_i \le g_{i,y_i} \cdot \gcd(\mathrm{lcm}(f_{1,y_1}, \cdots, f_{i-1,y_{i-1}}), f_{i,y_i}) - 1$, $i = 2, \cdots, s$.

By applying the lift-the-exponent lemma, a more concrete size of the q-cyclotomic cosets modulo n is given.

Lemma 9 ([16]). *Denote by $\Sigma = \Sigma(n; q)$ the set of all applicable $2s$-tuples $(y_1, \cdots, y_s, x_1, \cdots, x_s)$ that satisfy the inequality above. For any $2s$-tuple $(y_1, \cdots, y_s, x_1, \cdots, x_s) \in \Sigma$, the q-cyclotomic coset $c_{n/q}(\eta^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s})$ has a size of*

$$\tau_{y_1 \cdots y_s} = \mathrm{lcm}(\mathrm{ord}_{p_1^{m_1}}(q) \cdot p_1^{M_1}, \cdots, \mathrm{ord}_{p_s^{m_s}}(q) \cdot p_s^{M_s}),$$

where $m_i = \min\{e_i - y_i, 1\}$ and $M_i = \max\{e_i - y_i - v_{p_i}(q^{\mathrm{ord}_{p_i}(q)} - 1), 0\}$, $i = 1, \cdots, s$.

Based on the theories above, [16] considered the case where modulo n is even. Let $n = 2^{e_0} p_1^{e_1} \cdots p_s^{e_s}$, where $p_1, \cdots, p_s$ are different odd primes and $e_0, e_1, \cdots, e_s$ are positive integers. Since there is no primitive root of $\mathbb{Z}/2^{e_0}\mathbb{Z}$, where $e_0 \ge 3$, Lemma 8 does not apply in this case.

Lemma 10 ([16]). *Let n be an arbitrary positive integer, and let q be an odd prime power that is coprime to n. Let γ be an element in $\mathbb{Z}/n\mathbb{Z}$ with the associated q-cyclotomic coset modulo n given by*

$$c_{n/q}(\gamma) = \{\gamma, \gamma q, \cdots, \gamma q^{\tau - 1}\}.$$

(1) If $2n \mid \gamma q^\tau - \gamma$, that is, $v_2(q^\tau - 1) + v_2(\gamma) \ge v_2(n) + 1$, then by viewing γ as an element in $\mathbb{Z}/2n\mathbb{Z}$, the q-cyclotomic coset modulo $2n$ containing γ is

$$c_{2n/q}(\gamma) = \{\gamma, \gamma q, \cdots, \gamma q^{\tau - 1}\}.$$

Moreover, the q-cyclotomic coset

$$c_{2n/q}(n + \gamma) = \{n + \gamma, (n + \gamma)q, \cdots, (n + \gamma)q^{\tau - 1}\}$$

modulo $2n$ containing $n + \gamma$ is disjoint with $c_{2n/q}(\gamma)$, and the union $c_{2n/q}(\gamma) \sqcup c_{2n/q}(n + \gamma)$ is exactly the preimage of $c_{n/q}(\gamma)$ under the projection $\mathbb{Z}/2n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

(2) *If* $2n \nmid \gamma q^\tau - \gamma$, *that is,* $v_2(q^\tau - 1) + v_2(\gamma) < v_2(n) + 1$, *then by viewing* γ *as an element in* $\mathbb{Z}/2n\mathbb{Z}$, *the* q*-cyclotomic coset modulo* $2n$ *containing* γ *is*

$$c_{2n/q}(\gamma) = \{\gamma, \gamma q, \cdots, \gamma q^{2\tau-1}\}.$$

Moreover, the coset $c_{2n/q}(\gamma)$ *contains* $n + \gamma$ *and is exactly the preimage of* $c_{n/q}(\gamma)$ *under the projection* $\mathbb{Z}/2n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

If $\gamma \in \mathbb{Z}/n\mathbb{Z}$ fits the first condition in Lemma 10, we say that $c_{n/q}(\gamma)$ is splitting with respect to the extension $\mathbb{Z}/2n\mathbb{Z} : \mathbb{Z}/n\mathbb{Z}$. Otherwise, we say that $c_{n/q}(\gamma)$ is stable with respect to the extension $\mathbb{Z}/2n\mathbb{Z} : \mathbb{Z}/n\mathbb{Z}$. We define that an element $\overline{\gamma} \in \mathbb{Z}/n\mathbb{Z}$ is divisible by 2^{e_0} if any representative of γ in $\mathbb{Z}$ is divisible by 2^{e_0}. This definition is clearly well defined. Then, we give an explanation of q-cyclotomic cosets modulo n, where n is even.

For any $\gamma \in \mathbb{Z}/n'\mathbb{Z}$, where n' is the greatest odd factor of n, we denote the size of the q-cyclotomic coset modulo n' containing γ by τ, and it is easy to see that $2^0 \mid \gamma$. Since

$$v_2(\gamma) + v_2(q^\tau - 1) \geq v_2(2n'),$$

we have that the q-cyclotomic cosets modulo $2n'$ containing γ is

$$c_{2n'/q}(\gamma) = \{\gamma, \gamma q, \cdots, \gamma q^{\tau-1}\}$$

and

$$c_{2n'/q}(\gamma + n') = \{\gamma + n', (\gamma + n')q, \cdots, (\gamma + n')q^{\tau-1}\}.$$

If γ is odd, then we have $2 \mid \gamma + n'$; otherwise, we have $2 \mid \gamma$. We assume that $2 \mid \gamma$ (if $2 \mid n' + \gamma$, the proof is similar). Since

$$v_2(\gamma) + v_2(q^\tau - 1) \geq v_2(2^2 n'),$$

we have that the q-cyclotomic cosets modulo $2^2 n'$ containing γ is

$$c_{2^2 n'/q}(\gamma) = \{\gamma, \gamma q, \cdots, \gamma q^{\tau-1}\}$$

and

$$c_{2^2 n'/q}(\gamma + 2n') = \{\gamma + 2n', (\gamma + 2n')q, \cdots, (\gamma + 2n')q^{\tau-1}\}.$$

If $2^2 \nmid \gamma$, then we can easily see that $2^2 \mid 2n' + \gamma$. Conversely, if $2^2 \nmid 2n' + \gamma$, then we can easily see that $2^2 \mid \gamma$. So there must be one of γ and $2n' + \gamma$ that is divisible by 2^2. And so on, for $n = 2^{e_0} p_1^{e_1} \cdots p_s^{e_s}$, if $2^{e_0} \mid \gamma$, we can verify that there is exactly one among $c_{2n/q}(\gamma)$ and $c_{2n/q}(n + \gamma)$ that is divisible by 2^{e_0+1}. Furthermore, there is a q-cyclotomic coset that will keep splitting, while others will remain stable when

$$v_2(\gamma) + v_2(q^\tau - 1) < v_2(n).$$

2.3. The Factorization of $x^n - 1$, $\Phi_n(X)$, *and* $x^n - \lambda$

In this subsection, we review the formula in [13] for the factorization of $x^n - 1$, $\Phi_n(x)$, and $x^n - \lambda$. Here, n is a positive integer coprime to q.

Lemma 11 ([13]). *Let* $\omega = \mathrm{ord}_{\mathrm{rad}(n)}(q)$, *and set* $s = \omega$ *if* $4 \nmid n$ *or* $q^\omega \equiv 1 \pmod 4$; *otherwise, set* $s = 2\omega$. *Furthermore, for all positive integers* t, *we define* $d^{(t)} = \gcd(n, q^t - 1)$, *and for*

every $i \in CR_q(d^{(s)})$, where $CR_q(d^{(s)})$, denote a complete set of representatives of the q-cyclotomic cosets modulo $d^{(s)}$, we set $c_i = \min\{t \in \mathbb{N} | \frac{d^{(s)}}{d^{(t)}} \mid i\}$. Then, the factorization of $x^n - 1$ into monic irreducible factors over $\mathbb{F}_q$ is

$$\prod_{v|\frac{n}{d^{(s)}}} \prod_{\substack{i \in CR_q(d^{(s)}) \\ \gcd(i,v)=1}} \left[\sum_{l=0}^{c_i} x^{v \cdot l} \cdot (-1)^{c_i - l} \sum_{\substack{\mathcal{U} \subseteq \{0,\cdots,c_i-1\} \\ |\mathcal{U}| = c_i - l}} \prod_{u \in \mathcal{U}} \zeta_{d^{(s)}}^{1 \cdot q^u} \right],$$

where, for all $v \mid \frac{n}{d^{(s)}}$ and all $i \in CR_q(d^{(s)})$ such that $\gcd(i, v) = 1$, the monic irreducible factor belonging to (v, i) has degree vc_i and order $v \cdot \frac{d^{(s)}}{\gcd(i, d^{(s)})}$.

Lemma 12 ([13]). *Let $n \in \mathbb{N}$ such that $\gcd(n, q) = 1$. Let $\omega = \mathrm{ord}_{\mathrm{rad}(n)}(q)$, and set $s = \omega$ if $4 \nmid n$ or $q^\omega \equiv 1 \pmod 4$; otherwise, set $s = 2\omega$. Furthermore, we define $d^{(s)} = \gcd(n, q^s - 1)$. Then, the factorization of the cyclotomic polynomial $\Phi_n(x)$ into $\frac{\phi(d^{(s)})}{s}$ monic irreducible factors of degree $\frac{n}{d^{(s)}} \cdot s$ over $\mathbb{F}_q$ is*

$$\prod_{\substack{i \in \mathrm{CR}_q(d^{(s)}) \\ \gcd(i, d^{(s)})=1}} [\sum_{l=0}^{s} x^{\frac{n}{d^{(s)}} \cdot l} \cdot (-1)^{s-l} \sum_{\substack{\mathrm{U} \subseteq \{0,\cdots,s-1\} \\ |\mathrm{U}| = s-l}} \prod_{u \in \mathrm{U}} \zeta_{d^{(s)}}^{i \cdot q^u}].$$

Lemma 13 ([13]). *Let $\lambda \in \mathbb{F}_q^*$ and $n \in \mathbb{N}$ such that $\gcd(n, q) = 1$ and $n = n_1 \cdot n_2$, where $\mathrm{rad}(n_1) \mid \mathrm{ord}(\lambda)$ and $\gcd(n_2, \mathrm{ord}(\lambda)) = 1$. Let $\omega = \mathrm{ord}_{\mathrm{rad}(n)}(q)$, and set $s = \omega$ if $4 \nmid n$ or $q^\omega \equiv 1 (\pmod 4)$; otherwise, set $s = 2\omega$. For all positive integers t, we set $d_1^{(t)} = \gcd(n_1, \frac{q^t - 1}{\mathrm{ord}(\lambda)})$ and $d_2^{(t)} = \gcd(n_2, q^t - 1)$. If $4 \nmid d_1^{(s)}$ or $q \equiv 1 \pmod 4$, then $s_1 = \frac{d_1^{(s)}}{d_1^{(1)}}$; otherwise, $s_1 = \frac{2d_1^{(s)}}{d_1^{(2)}}$. For every $i \in CR_q(d_2^{(s)})$, where $CR_q(d_2^{(s)})$ denote a complete set of representatives of the q-cyclotomic cosets modulo $d_2^{(s)}$, we set $t_i = \min\{t \in \mathbb{N} \mid \frac{d_2^{(s)}}{d_2^{(t)}} \mid i\}$ and $c_i = \mathrm{lcm}(t_i, s_1)$. Then, there exists $b \in \mathbb{F}_{q^s}$ such that $b^{d_1^{(s)}} = a$, and the factorization of $x^n - \lambda$ over $\mathbb{F}_q$ is*

$$\prod_{j \in \{0,\cdots,d_1^{(s)}-1\}/\sim} \prod_{v|\frac{n_2}{d_2^{(s)}}} \prod_{\substack{i \in CR_q(d_2^{(s)}) \\ \gcd(i,v)=1}} \prod_{m=0}^{\gcd(t_i,s_1)-1} S_{(j,v,i,m)},$$

where, for all applicable (j, v, i, m), the monic irreducible polynomial $S_{(j,v,i,m)}$ of degree $\frac{n_1}{d_1^{(s)}} \cdot v \cdot c_i$ and order $\mathrm{ord}(a) \cdot n_1 \cdot v \cdot \frac{d_2^{(s)}}{\gcd(i, d_2^{(s)})}$ is defined as

$$S_{(j,v,i,m)} = \sum_{l=0}^{c_i} x^{\frac{n_1}{d_1^{(s)}} \cdot v \cdot l} \cdot (-1)^{c_i - l} \sum_{\substack{\mathcal{U} \subseteq \{0,\cdots,c_i-1\} \\ |\mathcal{U}| = c_i - l}} \prod_{u \in \mathcal{U}} (\zeta_{d_2^{(s)}}^{i \cdot q^m} (\zeta_{d_1^{(s)}}^{j} b)^{rv})^{q^u},$$

where r is a positive integer satisfying $r = 1$ if $a = 1$ or $rn_2 \equiv 1 (\pmod{\mathrm{ord}(a) \cdot d_1^{(s)}})$ otherwise. Furthermore, for all $j, \widetilde{j} \in \{0, \cdots, d_1^{(s)} - 1\}$, we have $j \sim \widetilde{j}$ if and only if $\zeta_{d_1^{(s)}}^{\widetilde{j}} = \zeta_{d_1^{(s)}}^{j \cdot q^m} b^{q^m - 1}$ for an integer $0 \le m \le s_1 - 1$.

It is not difficult to observe that, although [13] provided the explicit factorization of $x^n - 1, \Phi_n(x)$, and $x^n - \lambda$, we cannot calculate the number of irreducible factors for any

n, q such that $\gcd(n, q) = 1$ because the author did not provide the explicit representatives and sizes of the q-cyclotomic cosets modulo n in the formula.

3. Main Results

Let $\mathbb{F}_q$ be a finite field, and let $q = p^e$, n be a positive integer such that $\gcd(n, q) = 1$. Then, we give a different formula to calculate the number of irreducible factors of $x^n - 1$ and $x^n - \lambda$ over $\mathbb{F}_q$ for any $\lambda \in \mathbb{F}_q^*$.

3.1. The Number of Irreducible Factors of $x^n - 1$

Let $n = 2^{\widetilde{e_0}} p_1^{\widetilde{e_1}} \cdots p_s^{\widetilde{e_s}}$, and set

$$\omega = \begin{cases} \mathrm{ord}_{\mathrm{rad}(n)}(q), & \text{if } 4 \nmid n \text{ or } q^{\mathrm{ord}_{\mathrm{rad}(n)}(q)} \equiv 1 \pmod 4; \\ 2\mathrm{ord}_{\mathrm{rad}(n)}(q), & \text{otherwise.} \end{cases} \tag{1}$$

$d = \gcd(n, q^\omega - 1) = 2^{e_0} p_1^{e_1} \cdots p_s^{e_s}$, $d' = p_1^{e_1} \cdots p_s^{e_s}$.

Without loss of generality, we assume that the odd primes $p_1, \cdots, p_s$ are ranked in such a way that

$$\mathrm{ord}_{p_1}(q), \mathrm{ord}_{p_2}(q), \cdots, \mathrm{ord}_{p_{s'}}(q)$$

are even, and

$$\mathrm{ord}_{p_{s'+1}}(q), \mathrm{ord}_{p_{s'+2}}(q), \cdots, \mathrm{ord}_{p_s}(q)$$

are odd.

Fix a system of primitive roots $(\eta_1, \cdots, \eta_s)$ modulo $d' = p_1^{e_1} \cdots p_s^{e_s}$, and let $\Sigma = \Sigma(d'; q)$ be the set of applicable $2s$-tuples, i.e., the tuples $(y_1, \cdots, y_s, x_1, \cdots, x_s)$, such that $0 \le y_i \le e_i$ and that $0 \le x_1 \le g_{1,y_1} - 1$ and $0 \le x_i \le g_{i,y_i} \cdot \gcd(\mathrm{lcm}(f_{1,y_1}, \cdots, f_{i-1,y_{i-1}}), f_{i,y_i})$ for $i = 2, \cdots, m$.

For any $(y, x) = (y_1, \cdots, y_s, x_1, \cdots, x_s) \in \Sigma$, define $\Gamma(y) = \Gamma(y_1, \cdots, y_s)$ to be the set of all s-tuples $u = (u_1, \cdots, u_s)$ of integers satisfying $0 \le u_i \le \widetilde{e_i} - e_i$ and $u_i = 0$ given $y_i \ne 0$. For any $y = (y_1, \cdots, y_s)$, where $(y, x) \in \Sigma$, let $\{i_1, \cdots, i_{\alpha(y)}\}$ consisting of index i such that $y_i = 0$.

Now, we will calculate the number of irreducible factors of $x^n - 1$. We begin with the easier cases where, $\widetilde{e_0} = 0$ and $\widetilde{e_1} = 1$.

Proposition 1.

(1) If $\widetilde{e_0} = 0$, then $x^n - 1$ can be factored into the irreducible factors over $\mathbb{F}_q$ as

$$x^n - 1 = \prod_{(y,x) \in \Sigma} \prod_{u \in \Gamma(y)} S_{y,x,u},$$

where, for every $(y, x) = (y_1, \cdots, y_s, x_1, \cdots, x_s) \in \Sigma$ and $u = (u_1, \cdots, u_s) \in \Gamma(y)$, the irreducible polynomial $S_{y,x,u}$ is given by

$$S_{y,x,u} = \sum_{j=0}^{\tau_{y_1 \cdots y_s}} (-1)^{\tau_{y_1 \cdots y_s} - j} \left(\sum_{\substack{R \subseteq \{0, \cdots, \tau_{y_1 \cdots y_s} - 1\} \\ |R| = \tau_{y_1 \cdots y_s} - j}} \prod_{r \in R} \zeta_d^{\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} q^r} \right) x^j p_1^{u_1} \cdots p_s^{u_s}.$$

(2) The number of irreducible factors of $x^n - 1$ *is*

$$\kappa = \sum_{0 \le y_1 \le e_1} \cdots \sum_{0 \le y_s \le e_s} \frac{\prod_{i=1}^{s} [p_i^{e_i - y_i - 1}(p_i - 1)]}{\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})} \cdot \left(\prod_{j=1}^{\alpha(y)} (\widetilde{e_{i_j}} - e_{i_j} + 1) \right).$$

Proposition 2.

(1) If $\widetilde{e_0} = 1$, *then* $x^n - 1$ *can be factored into the irreducible factors over* $\mathbb{F}_q$ *as*

$$x^n - 1 = \prod_{(y,x) \in \Sigma} \prod_{u \in \Gamma(y)} S_{y,x,u} \cdot (S'_{y,x,u}),$$

where, for any $(y, x) \in \Sigma$ *and* $u \in \Gamma(y)$, *the irreducible polynomials* $S_{y,x,u}$ *and* $S'_{y,x,u}$ *are, respectively, given by*

$$S_{y,x,u} = \sum_{j=0}^{\tau_{y_1 \cdots y_s}} (-1)^{\tau_{y_1 \cdots y_s} - j} \left(\sum_{\substack{R \subseteq \{0, \cdots, \tau_{y_1 \cdots y_s} - 1\} \\ |R| = \tau_{y_1 \cdots y_s} - j}} \prod_{r \in R} \zeta_d^{\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} q^r} \right) x^j p_1^{u_1} \cdots p_s^{u_s}$$

and

$$S'_{y,x,u} = \sum_{j=0}^{\tau_{y_1 \cdots y_s}} (-1)^{\tau_{y_1 \cdots y_s} - j} \left(\sum_{\substack{R \subseteq \{0, \cdots, \tau_{y_1 \cdots y_s} - 1\} \\ |R| = \tau_{y_1 \cdots y_s} - j}} \prod_{r \in R} -\zeta_d^{\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} q^r} \right) x^j p_1^{u_1} \cdots p_s^{u_s}.$$

(2) The number of irreducible factors of $x^n - 1$ *is* 2κ, *where*

$$\kappa = \sum_{0 \le y_1 \le e_1} \cdots \sum_{0 \le y_s \le e_s} \frac{\prod_{i=1}^{s} [p_i^{e_i - y_i - 1}(p_i - 1)]}{\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})} \cdot \left(\prod_{j=1}^{\alpha(y)} (\widetilde{e_{i_j}} - e_{i_j} + 1) \right).$$

We still need to consider the case where $\widetilde{e_0} \ge 2$. Fix an applicable $2s$-tuple $(y, x) = (y_1, \cdots, y_s, x_1, \cdots, x_s) \in \Sigma$ and an s-tuple $u = (u_1, \cdots, u_s) \in \Gamma(y)$. Let $v^+_{y_1 \cdots y_s} = v_2(q^{\tau_{y_1 \cdots y_s}} - 1)$, $v^-_{y_1 \cdots y_s} = v_2(q^{\tau_{y_1 \cdots y_s}} + 1)$.

Proposition 3. *If* $q \equiv 3 \pmod 4$, *for any* s*-tuple* $y = (y_1, \cdots, y_s)$, *where* $(y, x) \in \Sigma$, $q^{\tau_{y_1 \cdots y_s}} \equiv 3 \pmod 4$ *if and only if*

$$y_i = e_i, \ for \ i = 1, \cdots, s',$$

where $\tau_{y_1 \cdots y_s}$ *is the size of the* q*-cyclotomic coset modulo* d'.

Proof. Since $q \equiv 3 \pmod 4$, $q^{\tau_{y_1 \cdots y_s}} \equiv 3 \pmod 4$ if and only if $\tau_{y_1 \cdots y_s}$ is odd. According to Lemma 9, we know that

$$\tau_{y_1 \cdots y_s} = \mathrm{lcm}(\mathrm{ord}_{p_1^{m_1}}(q) \cdot p_1^{M_1}, \cdots, \mathrm{ord}_{p_s^{m_s}}(q) \cdot p_s^{M_s}),$$

where $m_i = \min\{e_i - y_i, 1\}$ and $M_i = \max\{e_i - y_i - v_{p_i}(q^{\mathrm{ord}_{p_i}(q)} - 1), 0\}$, $i = 1, \cdots, s$. Noting that

$$\mathrm{ord}_{p_1}(q), \mathrm{ord}_{p_2}(q), \cdots, \mathrm{ord}_{p_{s'}}(q)$$

are even, $\tau_{y_1\cdots y_s}$ is odd if and only if $e_i = y_i$ for any $i = 1, \cdots, s'$. □

Proposition 4. *For any $y = (y_1, \cdots, y_s)$, where $(y, x) \in \Sigma$, if $q^{\tau_{y_1\cdots y_s}} \equiv 1 \pmod 4$, the number of irreducible factors of $x^n - 1$ associated with $y = (y_1, \cdots, y_s)$ is*

$$\kappa_y = \begin{cases} 2^{v_2(d)-1}(\widetilde{e_0} - e_0 + 1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)] + 2^{v_2(d)-1}[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)], 1 \le v_2(d) \le v^+_{y_1\cdots y_s}; \\ 2^{v^+_{y_1\cdots y_s}-1}(\widetilde{e_0} - e_0 + 1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)] \\ +[(v_2(d) - v^+_{y_1\cdots y_s} - 1)\cdot 2^{v^+_{y_1\cdots y_s}-1} + 2^{v^+_{y_1\cdots y_s}}][\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)], v_2(d) \ge v^+_{y_1\cdots y_s} + 1 \end{cases}$$

Proof. For any $(y, x) = (y_1, \cdots, y_s, x_1, \cdots, x_s) \in \Sigma$, when $v_2(d) = 1$, there will be two q-cyclotomic cosets modulo d

$$c_{d/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}), c_{n/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s} + d')$$

generated by $c_{d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s})$, and there is one among $c_{d/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s})$ and $c_{d/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s} + d')$ whose elements are all even, while the other has elements that are all odd. Suppose that $\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}$ is odd, then $\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s} + d'$ is even. Since

$$v_2(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}) + v_2(q^{\tau_{y_1\cdots y_s}} - 1) = v^+_{y_1\cdots y_s},$$

according to Lemma 10, we know it can split until $v_2(d) = v^+_{y_1\cdots y_s}$, i.e., when $1 \le v_2(d) \le v^+_{y_1\cdots y_s}$, there will be $2^{v_2(d)-1}$ q-cyclotomic cosets modulo d generated by $c_{2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s})$, and the length of them will be $\tau_{y_1\cdots y_s}$. On the other hand, since

$$v_2(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}) + v_2(q^{\tau_{y_1\cdots y_s}} - 1) > v^+_{y_1\cdots y_s},$$

according to Lemma 10, $c_{2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s} + d')$ can also split until $v_2(d) = v^+_{y_1\cdots y_s}$, i.e., when $1 \le v_2(d) \le v^+_{y_1\cdots y_s}$, there will be $2^{v_2(d)-1}$ q-cyclotomic cosets modulo d generated by $c_{2d'}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s} + d')$, and the elements in these q-cyclotomic cosets are all even. Noting that $\{i_1, \cdots, i_{\alpha(y)}\}$ is the subset of $\{1, \cdots, s\}$ such that $y_{i_j} = 0$ for $j = 1, \cdots, \alpha(y)$, we can easily see that when $1 \le v_2(d) \le v^+_{y_1\cdots y_s}$, there will be

$$2^{v_2(d)-1}(\widetilde{e_0} - e_0 + 1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)] + 2^{v_2(d)-1}[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)]$$

irreducible factors of $x^n - 1$ associated with $y = (y_1, \cdots, y_s)$.

When $v_2(d) = v^+_{y_1\cdots y_s} + 1$, the q-cyclotomic cosets modulo d generated by

$$c_{2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s})$$

are stable, and the q-cyclotomic cosets modulo d generated by $c_{2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s} + d')$ will split into $2^{v^+_{y_1\cdots y_s}}$ q-cyclotomic cosets. Now, we only need to consider the number of q-cyclotomic cosets modulo d generated by $c_{2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s} + d')$. When $v_2(d) = v^+_{y_1\cdots y_s} + 2$, there will be $\frac{1}{2}\cdot 2^{v^+_{y_1\cdots y_s}}$ stable q-cyclotomic cosets and the other $\frac{1}{2}\cdot v^+_{y_1\cdots y_s}$ q-cyclotomic cosets will split into $2^{v^+_{y_1\cdots y_s}}$ q-cyclotomic cosets modulo d. Continuing this process, when $v_2(d) \ge v^+_{y_1\cdots y_s} + 1$, there will be $(v_2(d) - v^+_{y_1\cdots y_s} - 1)\cdot 2^{v^+_{y_1\cdots y_s}-1} + 2^{v^+_{y_1\cdots y_s}}$

q-cyclotomic cosets modulo d. Furthermore, the number of irreducible factors of $x^n - 1$ associated with $y = (y_1 \cdots y_s)$ is

$$2^{v^+_{y_1\cdots y_s}-1}(\widetilde{e_0} - e_0 + 1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)] + [(v_2(d) - v^+_{y_1\cdots y_s} - 1) \cdot 2^{v^+_{y_1\cdots y_s}-1} + 2^{v^+_{y_1\cdots y_s}}][\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)].$$

If $\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s}$ is even and $\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} + d'$ is odd, the proof is similar. Now we conclude the proof of this proposition. □

Proposition 5. *For any $y = (y_1, \cdots, y_s)$, where $(y, x) \in \Sigma$, if $q^{\tau_{y_1\cdots y_s}} \equiv 3 \pmod 4$, the number of irreducible factors of $x^n - 1$ associated with $y = (y_1, \cdots, y_s)$ is*

$$\kappa'_y = \begin{cases} (\widetilde{e_0} - e_0 + 1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)] + \prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1), v_2(d) = 1; \\ (\widetilde{e_0} - e_0 + 1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)] + 2 \cdot \prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1), v_2(d) = 2; \\ 2^{v_2(d)-2}(\widetilde{e_0} - e_0 + 1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)] \\ +(2^{v_2(d)-2} + 1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)], 3 \le v_2(d) \le v^-_{y_1\cdots y_s} + 1; \\ 2^{v^-_{y_1\cdots y_s}-1}(\widetilde{e_0} - e_0 + 1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)] \\ +[(v_2(d) - v^-_{y_1\cdots y_s} - 2) \cdot 2^{v^-_{y_1\cdots y_s}-1} + 2^{v^-_{y_1\cdots y_s}} + 1][\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}} - e_{i_j} + 1)], v_2(d) \ge v^-_{y_1\cdots y_s} + 2. \end{cases}$$

Proof. For any $(y, x) = (y_1, \cdots, y_s, x_1, \cdots, x_s) \in \Sigma$, when $v_2(d) = 1$, there will be two q-cyclotomic cosets modulo d

$$c_{d/q}(\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s}), c_{n/q}(\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} + d')$$

generated by $c_{d'/q}(\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s})$, and there is one among $c_{d/q}(\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s})$ and $c_{d/q}(\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} + d')$ whose elements are all even, while the other has elements that are all odd. Suppose that $\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s}$ is odd and $\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} + d'$ is even. Since

$$v_2(\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s}) + v_2(q^{\tau_{y_1\cdots y_s}} - 1) = 1,$$

it will be stable when $v_2(d) = 2$, and the size of $c_{2^2d'}(\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s})$ is $2\tau_{y_1\cdots y_s}$. From the lift-the-exponent lemma,

$$\begin{aligned} &v_2(\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s}) + v_2(q^{2\tau_{y_1\cdots y_s}} - 1) \\ =&0 + v_2(q^{\tau_{y_1\cdots y_s}} + 1) + 1 \\ =&v^-_{y_1\cdots y_s} + 1, \end{aligned}$$

and we can easily see that the q-cyclotomic cosets $c_{2^2d'}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s})$ will split until $v_2(d)=v^-_{y_1\cdots y_s}+1$, i.e., when $3\le v_2(d)\le v^-_{y_1\cdots y_s}+1$, there will be $2^{v_2(d)-2}$ q-cyclotomic cosets modulo d generated by $c_{2^2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s})$. On the other hand, since

$$\begin{aligned}&v_2(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}+d')+v_2(q^{2\tau_{y_1\cdots y_s}}-1)\\=&1+v^-_{y_1\cdots y_s}+1\\=&2+v^-_{y_1\cdots y_s}.\\>&v^-_{y_1\cdots y_s}+1,\end{aligned}$$

for any $3\le v_2(d)\le v^-_{y_1\cdots y_s}+1$, there will be $1+2^{v_2(d)-2}$ q-cyclotomic cosets modulo d generated by $c_{2^2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}+d')$. If all elements in these q-cyclotomic cosets are even, we have that the number of the irreducible factors of x^n-1 is

$$2^{v_2(d)-2}(\widetilde{e_0}-e_0+1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}}-e_{i_j}+1)]+(2^{v_2(d)-2}+1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}}-e_{i_j}+1)].$$

When $v_2(d)=v^-_{y_1\cdots y_s}+2$, the q-cyclotomic cosets modulo d generated by

$$c_{2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s})$$

are stable, and the q-cyclotomic cosets modulo d generated by

$$c_{2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}+d')$$

will split into $1+2^{v^-_{y_1\cdots y_s}}$ q-cyclotomic cosets modulo d. When $v_2(d)\ge v^-_{y_1\cdots y_s}+3$, we only need to consider the q-cyclotomic cosets modulo d generated by

$$c_{2^2d'}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}+d'),$$

and when $v_2(d)=v^-_{y_1\cdots y_s}+3$, there will be $2^{v^-_{y_1\cdots y_s}-1}+1$ q-cyclotomic cosets that are stable, and the other $2^{v_{y_1\cdots y_s}-1}$ q-cyclotomic cosets will split into $2^{v_{y_1\cdots y_s}}$ q-cyclotomic cosets modulo $2d$, and so on. When $v_2(d)\ge v_{y_1\cdots y_s}+2$, there will be

$$[(v_2(d)-v^-_{y_1\cdots y_s}-2)\cdot 2^{v^-_{y_1\cdots y_s}-1}+2^{v^-_{y_1\cdots y_s}}+1][\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}}-e_{i_j}+1)]$$

q-cyclotomic cosets modulo d generated by

$$c_{2d'/q}(\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}+d').$$

Furthermore, the number of irreducible factors of x^n-1 associated with $y=(y_1\cdots,y_s)$ is

$$\begin{aligned}2^{v^-_{y_1\cdots y_s}-1}(\widetilde{e_0}-e_0+1)[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}}-e_{i_j}+1)]+[(v_2(d)-v^-_{y_1\cdots y_s}-2)\cdot 2^{v^-_{y_1\cdots y_s}-1}\\+2^{v^-_{y_1\cdots y_s}}+1][\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}}-e_{i_j}+1)].\end{aligned}$$

If $\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}$ is even and $\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}+d'$ is odd, the proof is similar. Now we conclude the proof of this proposition. □

Theorem 1. *The notations are defined above. When* $q \equiv 1 \pmod 4$, *the number of irreducible factors of* $x^n - 1$ *is*

$$\kappa = \sum_{0 \le y_1 \le e_1} \cdots \sum_{0 \le y_s \le e_s} \cdot \kappa_y \cdot \frac{\prod_{i=1}^{s} [p_i^{e_i - y_i - 1}(p_i - 1)]}{\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})}.$$

When $q \equiv 3 \pmod 4$, *the number of irreducible factors of* $x^n - 1$ *is*

$$\kappa = \sum_{y_1 = e_1} \cdots \sum_{y_{s'} = e_{s'}} \cdot \kappa'_y \cdot \frac{\prod_{i=s'+1}^{s} [p_i^{e_i - y_i - 1}(p_i - 1)]}{\mathrm{lcm}(f_{s'+1}, \cdots, f_{s,y_s})}$$
$$+ \sum_{0 \le y_1 \le e_1 - 1} \cdots \sum_{0 \le y_{s'} \le e_{s'} - 1} \sum_{0 \le y_{s'+1} \le e_{s'+1}} \cdots \sum_{0 \le y_s \le e_s} \cdot \kappa_y \cdot \frac{\prod_{i=1}^{s} [p_i^{e_i - y_i - 1}(p_i - 1)]}{\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})}.$$

Proof. If $q \equiv 1 \pmod 4$, for any $y = (y_1, \cdots, y_s)$, where $(y, x) \in \Sigma$, $q^{\tau_{y_1 \cdots y_s}} \equiv 1 \pmod 4$. Then, by applying Lemma 8, we have that the number of q-cyclotomic cosets modulo d are

$$\begin{aligned}
&\sum_{0 \le y_1 \le e_1} \cdots \sum_{0 \le y_s \le e_s} g_{1,y_1} \cdot g_{2,y_1} \gcd(f_{1,y_1}, f_{2,y_2}) \cdots g_{s-1,y_{s-1}} \cdot \gcd(\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s-1,y_{s-1}}), f_{s,y_s}) \\
&= \sum_{0 \le y_1 \le e_1} \cdots \sum_{0 \le y_s \le e_s} \frac{\phi(p_1^{e_1 - y_1})}{f_{1,y_1}} \cdot \frac{\phi(p_2^{e_2 - y_2})}{f_{2,y_2}} \\
&\quad \cdot \gcd(f_{1,y_1}, f_{2,y_2}) \cdots \frac{\phi(p_s^{e_s - y_s})}{f_{s,y_s}} \cdot \frac{f_{s,y_s} \cdot \mathrm{lcm}(f_{1,y_1}, \cdots, f_{s-1,y_{s-1}}, f_{s,y_s})}{\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})} \\
&= \sum_{0 \le y_1 \le e_1} \cdots \sum_{0 \le y_s \le e_s} \cdot \frac{\prod_{i=1}^{s} [p_i^{e_i - y_i - 1}(p_i - 1)]}{\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})}.
\end{aligned}$$

By applying Proposition 4, we can easily see that the irreducible factors of $x^n - 1$ when $q \equiv 1 \pmod 4$ are

$$\sum_{0 \le y_1 \le e_1} \cdots \sum_{0 \le y_s \le e_s} \cdot \kappa_y \cdot \frac{\prod_{i=1}^{s} [p_i^{e_i - y_i - 1}(p_i - 1)]}{\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})}.$$

When $q \equiv 3 \pmod 4$, for any $y = (y_1, \cdots, y_s)$, where $(y, x) \in \Sigma$, if $\tau_{y_1 \cdots y_s}$ is odd, then $q^{\tau_{y_1 \cdots y_s}} \equiv 3 \pmod 4$; if $\tau_{y_1 \cdots y_s}$ is even, then $q^{\tau_{y_1 \cdots y_s}} \equiv 1 \pmod 4$. From Proposition 3 and similar to $q \equiv 1 \pmod 4$, we have that the number of irreducible factors of $x^n - 1$ when $q \equiv 3 \pmod 4$ is

$$\sum_{y_1 = e_1} \cdots \sum_{y_{s'} = e_{s'}} \cdot \kappa'_y \cdot \frac{\prod_{i=s'+1}^{s} [p_i^{e_i - y_i - 1}(p_i - 1)]}{\mathrm{lcm}(f_{s'+1}, \cdots, f_{s,y_s})}$$
$$+ \sum_{0 \le y_1 \le e_1 - 1} \cdots \sum_{0 \le y_{s'} \le e_{s'} - 1} \sum_{0 \le y_{s'+1} \le e_{s'+1}} \cdots \sum_{0 \le y_s \le e_s} \cdot \kappa_y \cdot \frac{\prod_{i=1}^{s} [p_i^{e_i - y_i - 1}(p_i - 1)]}{\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})}.$$

□

3.2. The Number of Irreducible Factors of $x^n - \lambda$

Let $n = n_1 \cdot n_2$, where $\mathrm{rad}(n_1) \mid \mathrm{ord}(\lambda)$, $\gcd(n_2, \mathrm{ord}(\lambda)) = 1$, and let $n_2 = 2^{\widetilde{e_0}} p_1^{\widetilde{e_1}} \cdots p_s^{\widetilde{e_s}}$. Set

$$\omega = \begin{cases} \mathrm{ord}_{\mathrm{rad}(n)}(q), & \text{if } 4 \nmid n \text{ or } q^{\mathrm{ord}_{\mathrm{rad}(n)}(q)} \equiv 1 \pmod 4; \\ 2\mathrm{ord}_{\mathrm{rad}(n)}(q), & \text{otherwise.} \end{cases} \tag{2}$$

$d_1 = \gcd(n_1, \frac{q^\omega - 1}{\mathrm{ord}(\lambda)})$, $d_2 = \gcd(n_2, q^\omega - 1) = 2^{e_0} p_1^{e_1} \cdots p_s^{e_s}$, $d_2' = p_1^{e_1} \cdots p_s^{e_s}$. If $4 \nmid d_1$ or $q \equiv 1 \pmod 4$, then $s = \dfrac{\gcd(n_1, \frac{q^\omega - 1}{\mathrm{ord}(\lambda)})}{\gcd(n_1, \frac{q-1}{\mathrm{ord}(\lambda)})}$; otherwise, $s = \dfrac{2\gcd(n_1, \frac{q^\omega - 1}{\mathrm{ord}(\lambda)})}{\gcd(n_1, \frac{q-1}{\mathrm{ord}(\lambda)})}$. m is a positive integer satisfying $m = 1$ if $\lambda = 1$ or $mn_2 \equiv 1 \pmod{\mathrm{ord}(\lambda) \cdot d_1}$.

Without loss of generality, we also assume that the odd primes $p_1, \cdots, p_s$ are ranked in such a way that

$$\mathrm{ord}_{p_1}(q), \mathrm{ord}_{p_2}(q), \cdots, \mathrm{ord}_{p_{s'}}(q)$$

are even, and

$$\mathrm{ord}_{p_{s'+1}}(q), \mathrm{ord}_{p_{s'+2}}(q), \cdots, \mathrm{ord}_{p_s}(q)$$

are odd.

Fix a system of primitive roots $(\eta_1, \cdots, \eta_s)$ modulo $d' = p_1^{e_1} \cdots p_s^{e_s}$, Let $\Sigma = \Sigma(d'; q)$ be the set of applicable $2s$-tuples, i.e., the tuples $(y_1, \cdots, y_s, x_1, \cdots, x_s)$, such that $0 \le y_i \le e_i$ and $0 \le x_1 \le g_{1,y_1} - 1$ and $0 \le x_i \le g_{i,y_i} \cdot \gcd(\mathrm{lcm}(f_{1,y_1}, \cdots, f_{i-1,y_{i-1}}), f_{i,y_i})$ for $i = 2, \cdots, m$.

For any $(y, x) = (y_1, \cdots, y_s, x_1, \cdots, x_s) \in \Sigma$, define $\Gamma(y) = \Gamma(y_1, \cdots, y_s)$ as the set of all s-tuples $u = (u_1, \cdots, u_s)$ of integers satisfying $0 \le u_i \le \widetilde{e_i} - e_i$ and $u_i = 0$ when $y_i \ne 0$. For any $y = (y_1, \cdots, y_s)$, where $(y, x) \in \Sigma$, let $\{i_1, \cdots, i_{\alpha(y)}\}$ consist of indices i such that $y_i = 0$,

Now, we calculate the number of irreducible factors of $x^n - \lambda$. We begin with the easier cases where $\widetilde{e_0} = 0$ and $\widetilde{e_1} = 1$.

Proposition 6.

(1) If $\widetilde{e_0} = 0$, then $x^n - \lambda$ can be factored into the irreducible factors over $\mathbb{F}_q$ as

$$x^n - \lambda = \prod_{z \in \{0, \cdots, d_1 - 1\}/\sim} \prod_{(y,x) \in \Sigma} \prod_{u \in \Gamma(y)} \prod_{a=0}^{\gcd(\tau_{y_1 \cdots y_s}, s) - 1} S_{z,y,x,u,a},$$

where, for every $z \in \{0, \cdots, d_1 - 1\}/\sim$, $(y, x) = (y_1, \cdots, y_s, x_1, \cdots, x_s) \in \Sigma$, $u \in \Gamma(y)$, $0 \le a \le \gcd(\tau_{y_1 \cdots y_s}, s) - 1$, the irreducible polynomial $S_{z,y,x,u,a}$ is given by

$$S_{z,y,x,u,a} = \sum_{j=0}^{\mathrm{lcm}(\tau_{y_1 \cdots y_s}, s)} \cdot (-1)^{\mathrm{lcm}(\tau_{y_1 \cdots y_s}, s) - j} \sum_{\substack{R \subseteq \{0, \cdots \mathrm{lcm}(\tau_{y_1 \cdots y_s}, s) - 1\} \\ |R| = \mathrm{lcm}(\tau_{y_1 \cdots y_s}, s) - j}} \cdot \prod_{r \in R} \left(\zeta_{d_2}^{\eta_1^{x_1} \cdots \eta_s^{x_s} p_1^{y_1} \cdots p_s^{y_s} q^a} (\zeta_{d_1}^z b)^{m p_1^{u_1} \cdots p_s^{u_s}} \right)^{q^r} \cdot x^{\frac{n_1}{d_1} j p_1^{u_1} \cdots p_s^{u_s}}.$$

(2) The number of irreducible factors of $x^n - \lambda$ *is*

$$\kappa = \sum_{0\le y_1\le e_1} \cdots \sum_{0\le y_s\le e_s} \frac{\prod_{i=1}^{s}[p_i^{e_i-y_i-1}(p_i-1)]}{\mathrm{lcm}(f_{1,y_1},\cdots,f_{s,y_s})}[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}}-e_{i_j}+1)]\cdot\frac{d_1}{s}\cdot\gcd(\tau_{y_1\cdots y_s},s).$$

Proposition 7.

(1) If $\widetilde{e_0}=1$, *then* $x^n-\lambda$ *can be factored into the irreducible factors over* $\mathbb{F}_q$ *as*

$$x^n-\lambda=\prod_{z\in\{0,\cdots,d_1-1\}/\sim}\prod_{(y,x)\in\Sigma}\prod_{u\in\Gamma(y)}\prod_{a=0}^{\gcd(\tau_{y_1\cdots y_s},s)-1}S_{z,y,x,u,a}\cdot(S'_{z,y,x,u,a}),$$

where, for every $z\in\{0,\cdots,d_1-1\}/\sim$, $(y,x)=(y_1,\cdots,y_s,x_1,\cdots,x_s)\in\Sigma$, $u\in\Gamma(y)$, $0\le a\le\gcd(\tau_{y_1\cdots y_s},s)-1$, *the irreducible polynomial* $S_{z,y,x,u,a}$ *is given by*

$$S_{z,y,x,u,a}=\sum_{j=0}^{\mathrm{lcm}(\tau_{y_1\cdots y_s},s)}\cdot(-1)^{\mathrm{lcm}(\tau_{y_1\cdots y_s},s)-j}\sum_{\substack{R\subseteq\{0,\cdots\mathrm{lcm}(\tau_{y_1\cdots y_s},s)-1\}\\|R|=\mathrm{lcm}(\tau_{y_1\cdots y_s},s)-j}}$$
$$\cdot\prod_{r\in R}\left(\zeta_{d_2}^{\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}q^a}(\zeta_{d_1}^z b)^{mp_1^{u_1}\cdots p_s^{u_s}}\right)^{q^r}\cdot x^{\frac{n_1}{d_1}jp_1^{u_1}\cdots p_s^{u_s}}.$$

and

$$S'_{z,y,x,u,a}=\sum_{j=0}^{\mathrm{lcm}(\tau_{y_1\cdots y_s},s)}\cdot(-1)^{\mathrm{lcm}(\tau_{y_1\cdots y_s},s)-j}\sum_{\substack{R\subseteq\{0,\cdots\mathrm{lcm}(\tau_{y_1\cdots y_s},k)-1\}\\|R|=\mathrm{lcm}(\tau_{y_1\cdots y_s},k)-j}}$$
$$\cdot\prod_{r\in R}\left(-\zeta_{d_2}^{\eta_1^{x_1}\cdots\eta_s^{x_s}p_1^{y_1}\cdots p_s^{y_s}q^a}(\zeta_{d_1}^z b)^{mp_1^{u_1}\cdots p_s^{u_s}}\right)^{q^r}\cdot x^{\frac{n_1}{d_1}jp_1^{u_1}\cdots p_s^{u_s}}.$$

(2) The number of irreducible factors of $x^n-\lambda$ *is* 2κ, *where*

$$\kappa = \sum_{0\le y_1\le e_1} \cdots \sum_{0\le y_s\le e_s} \frac{\prod_{i=1}^{s}[p_i^{e_i-y_i-1}(p_i-1)]}{\mathrm{lcm}(f_{1,y_1},\cdots,f_{s,y_s})}[\prod_{j=1}^{\alpha(y)}(\widetilde{e_{i_j}}-e_{i_j}+1)]\cdot\frac{d_1}{s}\cdot\gcd(\tau_{y_1\cdots y_s},s).$$

We still need to consider the case where $\widetilde{e_0}\ge 2$. Fix an applicable $2s$-tuple $(y,x)=(y_1,\cdots,y_s,x_1,\cdots,x_s)\in\Sigma$ and an s-tuple $u=(u_1,\cdots,u_s)\in\Gamma(y)$. Let $v^+_{y_1\cdots y_s}=v_2(q^{\tau_{y_1\cdots y_s}}-1)$, $v^-_{y_1\cdots y_s}=v_2(q^{\tau_{y_1\cdots y_s}}+1)$. By combining Proposition 3, Proposition 4, Proposition 5, and Lemma 9, we can easily obtain the theorem below.

Theorem 2. *The notations are defined above. When* $q\equiv 1 \pmod 4$, *the number of irreducible factors of* $x^n-\lambda$ *is*

$$\kappa = \sum_{0\le y_1\le e_1} \cdots \sum_{0\le y_s\le e_s} \cdot\kappa_y\cdot\frac{\prod_{i=1}^{s}[p_i^{e_i-y_i-1}(p_i-1)]}{\mathrm{lcm}(f_{1,y_1},\cdots,f_{s,y_s})}\cdot\frac{d_1}{s}\cdot\gcd(\tau_{y_1,\cdots,y_s},s).$$

When $q \equiv 3 \pmod 4$, *the number of irreducible factors of* $x^n - \lambda$ *is*

$$\kappa = \sum_{y_1=e_1} \cdots \sum_{y_{s'}=e_{s'}} \cdot \kappa'_y \cdot \frac{\prod_{i=s'+1}^{s} [p_i^{e_i-y_i-1}(p_i-1)]}{\mathrm{lcm}(f_{s'+1}, \cdots, f_{s,y_s})} \cdot \frac{d_1}{s} \cdot \gcd(\tau_{y_1,\cdots,y_s}, s)$$
$$+ \sum_{0\le y_1\le e_1-1} \cdots \sum_{0\le y_{s'}\le e_{s'}-1} \sum_{0\le y_{s'+1}\le e_{s'+1}} \cdots \sum_{0\le y_s\le e_s} \cdot \kappa_y \cdot \frac{\prod_{i=1}^{s} [p_i^{e_i-y_i-1}(p_i-1)]}{\mathrm{lcm}(f_{1,y_1}, \cdots, f_{s,y_s})}$$
$$\cdot \frac{d_1}{s} \cdot \gcd(\tau_{y_1,\cdots,y_s}, s).$$

4. Application

Let $\mathbb{F}_q$ be a finite field, and let n be a positive integer such that $\gcd(n, q) = 1$. Denote by $\mathfrak{F}(x^n - 1)$ the set of all distinct monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$.

Based on the theories in [12], we now give the necessary and sufficient conditions for

$$| \mathfrak{F}(x^n - 1) | = 6$$

and the irreducible factorization of $x^n - 1$ in these cases.

(i) If the number of factors of n is 6, the possible values of n are p_1^5, 2^5, $p_1^2p_2$, 2^2p_1, $2p_1^2$. The unique positive integer solution of the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 6$$

is

$$x_1 = x_2 = x_3 = x_4 = x_5 = x_6 = 1.$$

Case 1: If $n = 2^5$,

$$x^n - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)\Phi_{16}(x)\Phi_{32}(x).$$

Since $8, 16, 32$ have no primitive roots, we have that $\Phi_8(x), \Phi_{16}(x), \Phi_{32}(x)$ are reducible over $\mathbb{F}_q$. Then,

$$| \mathfrak{F}(x^n - 1) | > 6.$$

Case 2: If $n = p_1^2p_2$,

$$x^n - 1 = \Phi_1(x)\Phi_{p_1}(x)\Phi_{p_2}(x)\Phi_{p_1p_2}(x)\Phi_{p_1^2}(x)\Phi_{p_1^2p_2}(x).$$

Since p_1p_2 and $p_1^2p_2$ have no primitive roots, we have that $\Phi_{p_1p_2}(x)$ and $\Phi_{p_1^2p_2}(x)$ are reducible over $\mathbb{F}_q$ and

$$| \mathfrak{F}(x^n - 1) | > 6.$$

Case 3: If $n = 2^2p_1$,

$$x^n - 1 = \Phi_1(x)\Phi_2(x)\Phi_{p_1}\Phi_{2^2}(x)\Phi_{2p_1}(x)\Phi_{2^2p_1}(x).$$

Since $2^2 p_1$ has no primitive root, we that have $\Phi_{2^2 p_1}$ is reducible over $\mathbb{F}_q$ and

$$| \mathfrak{F}(x^n - 1) | > 6.$$

Case 4: If $n = p_1^5$, we have

$$x^n - 1 = \Phi_1(x)\Phi_{p_1}(x)\Phi_{p_1^2}(x)\Phi_{p_1^3}(x)\Phi_{p_1^4}(x)\Phi_{p_1^5}(x)$$

and

$$\frac{\phi(p_1)}{d_{p_1}} = \frac{\phi(p_1^2)}{d_{p_1^2}} = \frac{\phi(p_1^3)}{d_{p_1^3}} = \frac{\phi(p_1^4)}{d_{p_1^4}} = \frac{\phi(p_1^5)}{d_{p_1^5}}.$$

Since

$$\mathrm{ord}_{\mathrm{rad}(n)}(q) = \mathrm{ord}_{p_1}(q) = \phi(p_1)$$

and

$$d = \gcd(n, q^{\phi(p_1)} - 1) = \gcd(p_1^5, q^{\phi(p_1)} - 1) = p_1.$$

According to Lemma 8, since

$$g_{1,0} = \frac{\phi(p_1)}{f_{1,0}} = \frac{\phi(p_1)}{\mathrm{ord}_{p_1}(q)} = 1,$$

we have that the q-cyclotomic cosets modulo d are

$$c_{d/q}(p_1^0), c_{d/q}(p_1).$$

Further, according to Lemma 11, we have that the irreducible factorization of $x^n - 1$ is

$$\begin{aligned} x^n - 1 =& \Phi_1(x)\Phi_{p_1}(x)\Phi_{p_1^2}(x)\Phi_{p_1^3}(x)\Phi_{p_1^4}(x)\Phi_{p_1^5}(x) \\ =& (x-1)\cdot[\prod_{j=0}^{\tau_0-1}(x-\zeta_d^{q^j})]\cdot[\prod_{j=0}^{\tau_0-1}(x^{p_1}-\zeta_d^{q^j})]\cdot[\prod_{j=0}^{\tau_0-1}(x^{p^2}-\zeta_d^{q^j})] \\ & \cdot[\prod_{j=0}^{\tau_0-1}(x^{p_3}-\zeta_d^{q^j})]\cdot[\prod_{j=0}^{\tau_0-1}(x^4-\zeta_d^{q^j})], \end{aligned}$$

where $\tau_0 = \phi(p_1)$, ζ_d is the d-th primitive root, and $d = p_1$.
Case 5: If $n = 2p_1^2$,

$$x^n - 1 = \Phi_1(x)\Phi_2(x)\Phi_{p_1}(x)\Phi_{2p_1}(x)\Phi_{p_1^2}(x)\Phi_{2p_1^2}(x)$$

and

$$\frac{\phi(p_1)}{d_{p_1}} = \frac{\phi(2p_1)}{d_{2p_1}} = \frac{\phi(p_1^2)}{d_{p_1^2}} = \frac{\phi(2p_1^2)}{d_{2p_1^2}} = 1.$$

Since

$$\mathrm{ord}_{\mathrm{rad}(n)}(q) = \mathrm{ord}_{2p_1}(q) = \phi(p_1)$$

and

$$d = \gcd(n, q^{\phi(p_1)} - 1) = \gcd(2p_1^2, q^{\phi(p_1)} - 1) = 2p_1.$$

According to Lemma 8, since

$$g_{1,0} = \frac{\phi(p_1)}{f_{1,0}} = \frac{\phi(p_1)}{\mathrm{ord}_{p_1}(q)} = 1,$$

we have that the q-cyclotomic cosets modulo p_1 are

$$c_{d/q}(p_1^0), c_{d/q}(p_1),$$

and according to Lemma 10, the q-cyclotomic cosets modulo d are

$$c_{d/q}(1), c_{d/q}(1+p_1), c_{d/q}(p_1), c_{d/q}(2p_1).$$

By applying Lemma 11, we have that the irreducible factorization of $x^n - 1$ is

$$\begin{aligned} x^n - 1 =& \Phi_1(x)\Phi_2(x)\Phi_{p_1}(x)\Phi_{2p_1}(x)\Phi_{p_1^2}(x)\Phi_{2p_1^2}(x) \\ =& (x-1)(x+1)\cdot[\prod_{j=0}^{\tau_0-1}(x-\zeta_d^{q^j})]\cdot[\prod_{j=0}^{\tau_0-1}(x-\zeta_d^{(1+p_1)q^j})]\cdot[\prod_{j=0}^{\tau_0-1}(x^{p_1}-\zeta_d^{q^j})] \\ & \cdot[\prod_{j=0}^{\tau_0-1}(x^{p_1}-\zeta_d^{(1+p_1)q^j})], \end{aligned}$$

where $\tau_0 = \phi(p_1)$, ζ_d is a d-th primitive root, and $d = 2p_1$.

(ii) If the number of factors of n is 5, then the possible values of n are $p_1^4, 2^4$. The unique positive integer solution of the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 6$$

is

$$x_1 = x_2 = x_3 = x_4 = 1, x_5 = 2.$$

Case 1: If $n = 2^4$,

$$x^n - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)\Phi_{16}(x).$$

Since 8 and 16 have no primitive roots, we have that at least one of $\Phi_8(x)$ and $\Phi_{16}(x)$ is reducible over $\mathbb{F}_q$ and

$$|\ \mathfrak{F}(x^n - 1)\ | > 6.$$

Case 2: If $n = p_1^4$,

$$x^n - 1 = \Phi_1(x)\Phi_{p_1}(x)\Phi_{p_1^2}(x)\Phi_{p_1^3}(x)\Phi_{p_1^4}(x)$$

and

$$\frac{\phi(p_1)}{d_{p_1}} = \frac{\phi(p_1^3)}{d_{p_1^3}} = \frac{\phi(p_1^4)}{d_{p_1^4}} = 1, \frac{\phi(p_1^2)}{d_{p_1^2}} = 2.$$

Since $\mathrm{ord}_{p_1^2}(q) = \frac{1}{2}\phi(p_1^2)$, $\mathrm{ord}_{p_1^3} = \phi(p_1^3)$, we have

$$\begin{aligned} & v_{p_1}(q^{\frac{1}{2}\phi(p_1)} - 1) \\ =& v_{p_1}(q^{\frac{1}{2}\phi(p_1^2)} - 1) - v_{p_1}(p_1) \geq 1, \end{aligned}$$

which contradicts $\mathrm{ord}_{p_1}(q) = \phi(p_1)$.

(iii) If the number of factors of n is 4, then the possible values of n are $p_1^3, 2p_1, p_1p_1, 8$. The positive integer solution of the equation

$$x_1 + x_2 + x_3 + x_4 = 6$$

is

$$x_1 = x_2 = x_3 = 1, x_4 = 3 \text{ or } x_1 = x_2 = 1, x_3 = x_4 = 2.$$

Case 1: If $n = p_1^3$, we have

$$x^n - 1 = \Phi_1(x)\Phi_{p_1}(x)\Phi_{p_1^2}(x)\Phi_{p_1^3}(x).$$

(1) When

$$\frac{\phi(p_1)}{d_{p_1}} = \frac{\phi(p_1^3)}{d_{p_1^3}} = 1, \frac{\phi(p_1^2)}{d_{p_1^2}} = 3,$$

we have

$$\begin{aligned} &v_{p_1}(q^{\frac{1}{3}\phi(p_1)} - 1) \\ =&v_{p_1}(q^{\frac{1}{3}\phi(p_1^2)} - 1) - v_{p_1}(p_1) \geq 1, \end{aligned}$$

which contradicts $\text{ord}_{p_1}(q) = \phi(p_1)$.

(2) When

$$\frac{\phi(p_1)}{d_{p_1}} = 1, \frac{\phi(p_1^2)}{d_{p_1^2}} = \phi(p_1^3)d_{p_1^3} = 2,$$

we have

$$\begin{aligned} &v_{p_1}(q^{\frac{1}{2}\phi(p_1)} - 1) \\ =&v_{p_1}(q^{\frac{1}{2}\phi(p_1^2)} - 1) - v_{p_1}(p_1) \geq 1, \end{aligned}$$

which contradicts $\text{ord}_{p_1}(q) = \phi(p_1)$.

Case 2: If $n = 2p_1$, we have

$$x^n - 1 = \Phi_1(x)\Phi_2(x)\Phi_{p_1}(x)\Phi_{2p_1}(x).$$

(1) When

$$\frac{\phi(p_1)}{d_{p_1}} = 1, \frac{\phi(2p_1)}{d_{2p_1}} = 3,$$

we have

$$\begin{aligned} &v_{p_1}(q^{\frac{1}{3}\phi(p_1)} - 1) \\ =&v_{p_1}(q^{\frac{1}{3}\phi(p_1^2)} - 1) - v_{p_1}(p_1) \geq 1, \end{aligned}$$

which contradicts $\text{ord}_{p_1}(q) = \phi(p_1)$.

(2) When

$$\frac{\phi(p_1)}{d_{p_1}} = 3, \frac{\phi(2p_1)}{d_{2p_1}} = 1,$$

and since $\gcd(n, q) = 1$, q is odd, we have

$$2p_1 \mid q^{\frac{1}{3}\phi(p_1)} - 1,$$

which contradicts $\mathrm{ord}_{2p_1}(q) = \phi(p_1)$.

(3) When

$$\frac{\phi(p_1)}{d_{p_1}} = \frac{\phi(2p_1)}{d_{2p_1}} = 2,$$

since

$$\mathrm{ord}_{\mathrm{rad}(n)}(q) = \mathrm{ord}_{2p_1}(q) = \frac{1}{2}\phi(p_1)$$

and

$$d = \gcd(n, q^{\frac{1}{2}\phi(p_1)} - 1) = \gcd(2p_1, q^{\frac{1}{2}\phi(p_1)} - 1) = 2p_1.$$

According to Lemma 8, since

$$g_{1,0} = \frac{\phi(p_1)}{f_{1,0}} = \frac{\phi(p_1)}{\mathrm{ord}_{p_1}(q)} = 2,$$

we have that the q-cyclotomic cosets modulo p_1 are

$$c_{p_1/q}(\eta_1^0 p_1^0), c_{p_1/q}(\eta_1 p_1^0), c_{p_1/q}(p_1),$$

where η_1 is a primitive root modulo p_1. Further, according to Lemma 10, the q-cyclotomic cosets modulo d are

$$c_{d/q}(1), c_{d/q}(1+p_1), c_{d/q}(\eta_1), c_{d/q}(\eta_1+p_1), c_{d/q}(p_1), c_{d/q}(2p_1).$$

By applying Lemma 11, we have that the irreducible factorization of $x^n - 1$ is

$$\begin{aligned} x^n - 1 =& (x-1)(x+1) \cdot [\prod_{j=0}^{\tau_0-1}(x - \zeta_d^{q^j})] \cdot [\prod_{j=0}^{\tau_0-1}(x - \zeta_d^{(1+p_1)q^j})] \cdot [\prod_{j=0}^{\tau_0-1}(x - \zeta_d^{\eta_1 q^j})] \\ & \cdot [\prod_{j=0}^{\tau_0-1}(x - \zeta_d^{(\eta_1+p_1)q^j})]. \end{aligned}$$

Case 3: If $n = p_1 p_2$, we have

$$x^n - 1 = \Phi_1(x)\Phi_{p_1}(x)\Phi_{p_2}(x)\Phi_{p_1p_2}(x),$$

and since $p_1 p_2$ have no primitive roots, we have the following cases:

(1) When

$$\frac{\phi(p_1)}{d_{p_1}} = \frac{\phi(p_2)}{d_{p_2}} = 1, \frac{\phi(p_1p_2)}{d_{p_1p_2}} = 3,$$

since

$$\mathrm{ord}_{p_1}(q) = \phi(p_1), \mathrm{ord}_{p_2}(q) = \phi(p_2),$$

we have

$$\begin{aligned} \mathrm{ord}_{p_1p_2}(q) &= \mathrm{lcm}(\phi(p_1), \phi(p_2)) \\ &= \frac{\phi(p_1)\phi(p_2)}{\gcd(\phi(p_1), \phi(p_2))}, \end{aligned}$$

and since

$$2 \mid \gcd(\phi(p_1), \phi(p_2)),$$

there exists a contradiction with $\mathrm{ord}_{p_1p_2}(q) = \frac{1}{3}\phi(p_1p_2)$.

(2) When

$$\frac{\phi(p_1)}{d_{p_1}}, \frac{\phi(p_2)}{d_{p_2}} = \frac{\phi(p_1p_2)}{d_{p_1p_2}} = 2,$$

since

$$\mathrm{ord}_{\mathrm{rad}(n)}(q) = \mathrm{ord}_{p_1p_2}(q) = \frac{1}{2}\phi(p_1p_2)$$

and

$$d = \gcd(n, q^{\frac{1}{2}\phi(p_1p_2)} - 1) = p_1p_2.$$

According to Lemma 8, since

$$g_{1,0} = \frac{\phi(p_1)}{f_{1,0}} = 1, g_{2,0} = \frac{\phi(p_2)}{f_{2,0}} = 2,$$

we have that the q-cyclotomic cosets modulo d are

$$c_{d/q}(\eta_1^0\eta_2^0p_1^0p_2^0), c_{d/q}(\eta_1^0\eta_2p_1^0p_2^0), c_{d/q}(\eta_1^0\eta_2^0p_1p_2^0), c_{d/q}(\eta_1^0\eta_2p_1p_2^0), c_{d/q}(\eta_1^0\eta_2^0p_1^0p_2), c_{d/q}(\eta_1^0\eta_2^0p_1p_2)$$

and

$$\tau_{00} = \frac{1}{2}\phi(p_1p_1), \tau_{01} = \phi(p_1), \tau_{10} = \frac{1}{2}\phi(p_2), \tau_{11} = 1,$$

where η_1, η_2 are primitive roots modulo p_1, p_2, respectively. By applying Lemma 11, we have that the irreducible factorization of $x^n - 1$ is

$$x^n - 1 = (x-1) \cdot [\prod_{j=0}^{\tau_{00}-1}(x - \zeta_d^{\eta_2q^j})] \cdot [\prod_{j=0}^{\tau_{00}-1}(x - \zeta_d^{q^j})] \cdot [\prod_{j=0}^{\tau_{10}-1}(x - \zeta_d^{p_1q^j})]$$
$$\cdot [\prod_{j=0}^{\tau_{10}-1}(x - \zeta_d^{\eta_2p_1q^j})] \cdot [\prod_{j=0}^{\tau_{01}-1}(x - \zeta_d^{p_2q^j})],$$

where ζ_d is a primitive d-th root and $d = p_1p_2$.
Case 4: If $n = 8$, then

$$x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x).$$

(1) When

$$\frac{\phi(2)}{d_2} = \frac{\phi(4)}{d_4} = 1, \frac{\phi(8)}{d_8} = 3,$$

it follows that

$$\mathrm{ord}_8(q) = \frac{1}{3}\phi(8),$$

which is not an integer. Hence, there exists a contradiction.

(2) When

$$\frac{\phi(4)}{d_4} = \frac{\phi(8)}{d_8} = 2,$$

it follows that

$$\mathrm{ord}_4(q) = \frac{1}{2}\phi(4) = 1,$$

$$\mathrm{ord}_8(q) = \frac{1}{2}\phi(8) = 2$$

and

$$d = \gcd(n, q-1) = 4.$$

Then, we have that the irreducible factorization of $x^n - 1$ is

$$x^n - 1 = (x-1)(x+1)(x-\zeta_4)(x-\zeta_4^3)(x^2-\zeta_4)(x^2-\zeta_4^3),$$

where ζ_4 is a primitive 4th root.

(iv) If the number of factors of n is 3, then the possible values of n are 4, p_1^2. The positive integer solution of the equation

$$x_1 + x_1 + x_3 = 6$$

is

$$x_1 = x_2 = 1, x_3 = 4 \; or \; x_1 = 1, x_2 = 2, x_3 = 3.$$

Case 1: If $n = 4$, the number of irreducible factors of $x^4 - 1$ is 4 at most.
Case 2: If $n = p_1^2$, then we have

$$x^n - 1 = \Phi_1(x)\Phi_{p_1}(x)\Phi_{p_1^2}(x)$$

(1) When

$$\frac{\phi(p_1)}{d_{p_1}} = 1, \frac{\phi_{p_1^2}}{d_{p_1^2}} = 4,$$

it follows that

$$\begin{aligned} & v_{p_1}(q^{\frac{1}{4}\phi(p_1)} - 1) \\ =& - v_{p_1}(p_1) + v_{p_1}(q^{\frac{1}{4}\phi(p_1^2)} - 1) \geq 1, \end{aligned}$$

which contradicts $\mathrm{ord}_{p_1}(q) = \phi(p_1)$.

(2) When

$$\frac{\phi(p_1)}{d_{p_1}} = 4, \frac{\phi(p_1^2)}{d_{p_1^2}} = 1,$$

it follows that

$$\begin{aligned} & v_{p_1}(q^{\frac{1}{4}\phi(p_1^2)} - 1) \\ =& v_{p_1}(p_1) + v_{p_1}(q^{\frac{1}{4}\phi(p_1)} - 1) \\ \geq& 2, \end{aligned}$$

which contradicts $\mathrm{ord}_{p_1^2}(q) = \phi(p_1^2)$.

(3) When

$$\frac{\phi(p_1)}{d_{p_1}} = 2, \frac{\phi(p_1^2)}{d_{p_1^2}} = 3,$$

it follows that

$$\begin{aligned} & v_{p_1}(q^{\frac{1}{3}\phi(p_1^2)} - 1) \\ =& v_{p_1}(p_1) + v_{p_1}(q^{\frac{1}{3}\phi(p_1)} - 1) \\ \geq& 2, \end{aligned}$$

which contradicts $\mathrm{ord}_{p_1}(q) = \frac{1}{2}\phi(p_1)$.

(4) When

$$\frac{\phi(p_1)}{d_{p_1}} = 3, \frac{\phi(p_1^2)}{d_{p_1^2}} = 2,$$

there is a contradiction in the same way.

(v) If the number of factors of n is 2, then the possible value of n is p_1. The unique solutions of the equation

$$x_1 + x_2 = 6$$

are

$$x_1 = 1, x_2 = 5,$$

and

$$\frac{\phi(p_1)}{d_{p_1}} = 5.$$

Further, we have

$$\mathrm{ord}_{p_1}(q) = \frac{1}{5}\phi(p_1),$$

$$d = \mathrm{n}, \mathrm{q}^{\frac{1}{5}\mathrm{\Phi}(\mathrm{p}_1)} - 1 = p_1$$

and

$$g_{1,0} = \frac{\phi(p_1)}{d_{f_{1,0}}} = 5, \tau_0 = \frac{1}{5}\phi(p_1).$$

Then, the q-cyclotomic cosets modulo p_1 are

$$c_{d/q}(\eta_1^0 p_1^0), c_{d/q}(\eta_1^1 p_1^0), c_{d/q}(\eta_1^2 p_1^0), c_{d/q}(\eta_1^3 p_1^0), c_{d/q}(\eta_1^4 p_1^0), c_{d/q}(\eta_1^0 p_1^1),$$

where η_1 is a primitive root modulo p_1. By applying Lemma 11, we have that the irreducible factorization of $x^n - 1$ is

$$x^n - 1 = (x-1) \cdot [\prod_{j=0}^{\tau_0 - 1}(x - \zeta_d^{q^j})] \cdot [\prod_{j=0}^{\tau_0 - 1}(x - \zeta_d^{\eta_1 q^j})] \cdot [\prod_{j=0}^{\tau_0 - 1}(x - \zeta_d^{\eta_1^2 q^j})]$$
$$\cdot [\prod_{j=0}^{\tau_0 - 1}(x - \zeta_d^{\eta_1^3 q^j})] \cdot [\prod_{j=0}^{\tau_0 - 1}(x - \zeta_d^{\eta_1^4 q^j})],$$

where ζ_d is the d-th primitive root.

Author Contributions: Two authors contributed equally. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Natural Science Foundation of Beijing Municipal (M23017).

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Chen, B.; Ling, S.; Zhang, G. Enumeration formulas for self-dual cyclic codes. *Finite Field Appl.* **2016**, *42*, 1–22. [CrossRef]
2. Ghazi Nezami, S.; Khat, L.D. (In English: Lifting The Exponent Lemma). Published on October 2009. Available online: http://imo09.blogfa.com/page/2khat.aspx (accessed on 25 November 2024)
3. Yue, D.; Hu, Z. A new method for the calculation of the leader elements of cyclotomic cosets. *Inf. Secur. Commun. Priv.* **1995**, *1*, 28–32.
4. Chen, B.; Dinh, H.; Liu, H. Repeated-root constacyclic codes of length ℓp^s and their duals. *Discret. Appl. Math.* **2014**, *177*, 60–70. [CrossRef]

5. Chen, B.; Dinh, H.; Liu, H. Repeated-root constacyclic codes of length $2\ell^m p^s$. *Finite Fields Their Appl.* **2015**, *33*, 137–159. [CrossRef]
6. Liu, L.; Li, L.; Kai, X.; Zhu, S. Reapeated-root constacylic codes of length $3\ell p^s$ and their dual codes. *Finite Fields Their Appl.* **2016**, *42*, 269–295. [CrossRef]
7. Liu, L.; Li, L.; Wang, L.; Zhu, S. Reapeated-root Constacylic Codes of Length $n\ell p^s$. *Discret. Math.* **2017**, *340*, 2250–2261. [CrossRef]
8. Sharma, A. Repeated-root constacyclic codes of length $\ell^t p^s$ and their dual codes. *Cryptogr. Commun.* **2015**, *7*, 229–255. [CrossRef]
9. Sharma, A.; Rani, S. Repeated-root constacyclic codes of length $4\ell^m p^n$. *Finite Fields Their Appl.* **2016**, *40*, 163–200. [CrossRef]
10. Wu, H.; Zhu, L. Repeated-root constacyclic codes of length $p_1 p_2^t p^s$ and their dual codes. *Aims Math.* **2023**, *8*, 12793–12818. [CrossRef]
11. Geraci, J.; Bussel, F.V. A Note on Cyclotomic Cosets, an Algorithm for finding Coset Representatives and Size, and a Theorem on the Quantum evaluation of Weight Enumerators for a Certain Class of Cyclic Codes. *arXiv* **2008**, arXiv:cs/0703129.
12. Xie, W.; Zhang, J.; Cao, W. On the number of the irreducible factors of over finite fields. *Aims Math.* **2024**, *9*, 23468–23488. [CrossRef]
13. Graner, A. Closed formulas for the factorization of $X^n - 1$, the n-th cyclotomic polynomials, $X^n - a$ and $f(X)$ over a finite field for arbitrary positive integer n. *arXiv* **2024**, arXiv:2306.11183v2.
14. Ireland, K.; Rosen, M. *A Classical Introduction to Modern Number Theory*; Springer: Berlin/Heidelberg, Germany, 1990.
15. Hardy, G.; Wright, E. *An Introduction to the Theory of Numbers*, 5th ed.; Clarendon Press: Oxford, UK, 1984.
16. Zhu, L.; Liu, J.; Wu, H. Explict representatives and sizes of cyclotomic cosets and their application to cyclic codes over finite fields. *arXiv* **2024**, arXiv:2410.12122v1.