Composed Product and Factorization of Cyclotomic Polynomials over Finite Fields

by

Zynab Alshareef

A Thesis Submitted to the Faculty of Graduate Student and Postdoctoral Affairs in partial fulfilment of the requirements for the degree of

Master of Science

in

Mathematics

Carleton University

Ottawa, Ontario

Abstract

Let $q = p^e$ be a power of prime number p and $\mathbb{F}_q$ be a finite field with q elements. Let Φ_n be the nth cyclotomic polynomial over $\mathbb{F}_q$ such that q is congruent to ± 1 modulo each prime divisor of n. We use composed products to obtain an explicit factorization of Φ_n over the finite field $\mathbb{F}_q$.

Acknowledgements

I especially would like to thank my professor Steven Wang for his great supervising, support, guidance, and all the help he has provided me during my study. He inspired me greatly to work in this project.

I would like to thank my husband Mohammad for his support and help.

I would like to thank my family and my friends for their love, support, and encouragement.

I would like to thank my classmates Kirsten Nelson and Aleksandr Tuxanidy for their help and support.

Finally, I would like to thank Carelton University and all the professors who taught me in the department of mathematics, and I would like to thank the Saudi Culture Bureau for their financial support during my study.

Dedication

I would like to dedicated my thesis to my lovely family: My grateful Mother and Father for their support, my wonderful husband for his care, and my lovely sisters and brothers for their love.

Contents

1 Introduction

Let $q = p^e$ be a power of prime number p and $\mathbb{F}_q$ be the finite field with q elements. It is well known that the factorization of $x^n - 1$ over the finite field $\mathbb{F}_q$ has an application in coding theory such as constructing BCH codes with designated distance [6, 7]. Indeed, each irreducible factor of $x^n - 1$ in $\mathbb{F}_q[x]$ determine a cyclic code of length n over $\mathbb{F}_q$; see [7, 8] and the references therein.

Let Φ_n denote the nth cyclotomic polynomial, where Φ_n is defined as

$$\Phi_n(x) = \prod_{\substack{0<k\leq n \\ gcd(n,k)=1}} (x - {\zeta_n}^k),$$

where ζ_n is a primitive nth root of unity.

The factorization of cyclotomic polynomial is related to the factorization of several classes of polynomials. For instance, factoring $x^n - 1$ is very related to $\Phi_n(x)$ as we know that

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \Phi_d(x) \\ &= \Phi_n(x) \prod_{d|n, d\neq n} \Phi_d(x). \end{aligned}$$

In addition, we can find the factorization of Dickson polynomial from the factorization of cyclotomic polynomial. In 2007, Fitzgerald and Yucas [5] obtained the factorization of $\Phi_{2^m r}$ over $\mathbb{F}_q$, where r is prime and $q \equiv \pm 1 \pmod{r}$. In particular, they found the complete factorization of the cyclotomic polynomial $\Phi_{2^m 3}$ and the Dickson polynomial $D_{2^m 3}$ over $\mathbb{F}_q$. Earlier in 1997, Lidl and Niederreiter [6] showed the explicit factorization of Φ_{2^m} over $\mathbb{F}_q$ when $q \equiv 1 \pmod 4$, and the case when $q \equiv 3 \pmod 4$ was performed in [10]. In 2012, Wang and Wang [13] gave the explicit factorization of $\Phi_{2^n 5}$ over $\mathbb{F}_q$. Assuming Φ_r are known, Wang and Tuxanidy [11] obtained the factorization of the cyclotomic polynomial of $\Phi_{2^m r}$ over $\mathbb{F}_q$ where $r \geq 3$ is an odd integer.

For cyclotomic polynomials of the order $2^m u^n$ such that $u \mid q-1$ is an odd prime , Chen, Li and Tuerhong gave the explicit factorization in [4]. More generally, Martinez, Vergara, and de Oliveira [8] studied the factorization of the polynomial $x^n - 1 \in \mathbb{F}_q[x]$ under the condition that $rad(n) \mid q-1$. In this case, all irreducible factors are either binomials or trinomials. Extending the results in [13], all irreducible factors of $u^n r$-th cyclotomic polynomials can be obtained from the irreducible factors of cyclotomic polynomials of small order, in particular, the factorization of 3^m, $3^m 5$, and $3^m 7$ has been achieved in [14].

The goal of this thesis is to study the factorization of Φ_n such that q is congruent to ± 1 modulo all prime divisors of n. This would generalize the results in [8] under the assumption $rad(n) \mid q-1$. Without loss of generality, we can assume that $n = r_0^{e_0} r_1^{e_1} \cdots r_{s+t}^{e_{s+t}}$ such that $r_0 = 2$, $e_0 \geq 0$, $q \equiv 1 \pmod{r_i}$ with $1 \leq i \leq t$, $q \equiv -1 \pmod{r_i}$ with $t+1 \leq i \leq t+s$, and $e_i > 0$ for $1 \leq i \leq t+s$. In particular, we can assume that $e_0 = 0$ if q is even. It is well known that Φ_n is a composed product of $\Phi_{r_i^{e_i}}$'s. Under the above assumptions, each $\Phi_{r_i^{e_i}}$ can be factorized into irreducbile binomials or trinomials. Through the study of the factorization of composed products of irreducibe binomials and trinomials of these special forms, we can obtain the explicit factorization of Φ_n such that q is congruent to ± 1 modulo all prime divisors of n. The number of all irreducible factors are also counted.

The rest of the thesis is organized as follows. In Chapter 2 we give basic information of finite fields, cyclotomic polynomials, and composed products. In Chapter 3, we present some technical lemmas and their proofs on the composed products of irreducible binomials and trinomials. This will help on the results of factorization of cyclotomic polynomial Φ_n. In Chapter 4, we obtain the main results of this thesis on the factorization of cyclotomic polynomials Φ_n over $\mathbb{F}_q$ such that q is congruent to ± 1 modulo each prime divisor of n. We first obtain the factorization of cyclotomic polynomials Φ_n such that $n = r_1^{e_1} \cdots r_{t+s}^{e_{t+s}}$ with $q \equiv 1 \pmod{r_i}$ for $1 \leq i \leq t$ and $q \equiv -1 \pmod{r_i}$ for $t+1 \leq i \leq t+s$ (see Theorem 17). When q is odd and n is even, the factorization of Φ_n are different under the different assumptions depending on $q \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$. These results can be found in Theorem 18 and

Theorem 19. Some concrete examples are also provided. In Chapter 5, we give a conclusion and some final thoughts.

2 Preliminaries

Throughout this chapter, we give a a brief background of finite fields. We present some important definitions and theorems of cyclotomic polynomials that it helps on the main result. Then, we give some information about composed product.

2.1 Finite fields

Definition 1. A finite field is a field with exactly p^n elements, where p is a prime power and n is a positive integers. We denote a finite field with q elements by $\mathbb{F}_q$.

Theorem 1. *Let F be a field, and f be a polynomial of degree n with integer coefficients, then f has at most n different roots in F.*

Definition 2. For any positive integer n, an nth root of unity is a complex number ζ such that $\zeta^n = 1$. There are n distinct nth roots of unity, which are given by $e^{\frac{2\pi i}{n}}, e^{\frac{2\pi i 2}{n}}, ..., e^{\frac{2\pi i n}{n}}$.

Definition 3. Let F be any field, the smallest positive integer e such that $a^e = 1$ is the order of a denoted by $ord_F(a)$.

Definition 4. A primitive nth root of unity is an nth root of unity whose order is n. Let n, k be positive integers such that $1 \leq k \leq n$, and ζ be a primitive nth root of unity, then ζ^n is a primitive root of unity if and only if $gcd(k, n) = 1$.

There are exactly $\phi(n)$ primitive nth root of unity, where ϕ is Euler's phi function.

Definition 5. For $n \in N$, the Mobius function μ is defined as

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1; \\ (-1)^r, & \text{if } n = p_1\ p_2\ ...\ p_k \textit{ a product of distinct primes}; \\ 0, & \text{if } p^2 | n \textit{ for some prime } p. \end{cases}$$

Proposition 1. The Mobius function satisfies the following identity

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & otherwise. \end{cases}$$

Definition 6. [11] Let f be an irreducible polynomial over $\mathbb{F}_q$ of degree m with $f(0) \neq 0$. Then the order $ord(f)$ of f is equal to the order of any root of f in the multiplicative group $\mathbb{F}_{q^m}$.

2.2 Cyclotomic polynomials

Definition 7. For any positive integer n, the nth cyclotomic polynomial is the unique monic polynomial having exactly the primitive nth root of unity as it zeros. Namely,

$$\Phi_n(x) = (x - \omega_1)(x - \omega_2) \cdots (x - \omega_k),$$

where $\omega_1, \omega_2, \ldots, \omega_k$ are the primitive nth roots of unity. In other words,

$$\Phi_n(x) = \prod_{\substack{0<k\leq n \\ gcd(n,k)=1}} (x - {\zeta_n}^k),$$

where ζ_n is primitive nth root of unity. Since there are exactly $\phi(n)$ primitive nth root of unity, the degree of nth cyclotomic polynomials is always $\phi(n)$.

The relation between the Mobius function and cyclotomic polynomial gives

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

More specifically,

$$
\begin{aligned}
x^n - 1 &= \prod_{1 \le k \le n} (x - e^{2\pi i \frac{k}{n}}) \\
&= \prod_{d|n} \prod_{\substack{0<k\le n \\ gcd(n,k)=1}} (x - e^{2\pi i \frac{k}{n}}) \\
&= \prod_{d|n} \prod_{\substack{0<k\le n \\ gcd(n,k)=1}} (x - {\zeta_n}^k) \\
&= \prod_{d|n} \Phi_n(x) \\
&= \Phi_n(x) \prod_{d|n, n\neq d} \Phi_d(x).
\end{aligned}
$$

In the sequel, we also need the next few important theorems on factorization of cyclotomic polynoamials. The proofs of them can be found in [6, 11, 13, 14].

Theorem 2. *[14] Let q be a power of a prime and n be a positive integer such that $gcd(q, n) = 1$. Then the cyclotomic polynomials $\Phi_n(x)$ can be factored into $\frac{\phi(n)}{m}$ distinct monic irreducible polynomials of the same degree m over $\mathbb{F}_q$, where m is the least positive integer such that $q^m \equiv 1 \pmod{n}$.*

Theorem 3. *[8] The following results of cyclotomic polynomials holds:*

(1) $\Phi_{2n}(x) = \Phi_n(-x)$ for $n \ge 3$ and n odd;

(2) $\Phi_{mt}(x) = \Phi_m(x^t)$ for all positive integers m which are divisible by the prime t;

(3) $\Phi_{mt^k}(x) = \Phi_{mt}(x^{t^{k-1}})$ if t is a prime and m, k are arbitrary positive integers.

Theorem 4. *[6] Let $f_1, f_2, \ldots, f_n$ be all distinct monic irreducible polynomials over $\mathbb{F}_q$ of degree m and order e, and let $t \ge 2$ be an integer whose prime factors divide e but do not divide $\frac{q^m-1}{e}$. Assume that $q^m \equiv 1 \pmod{4}$. If $t \equiv 0 \pmod{4}$, then $f_1(x^t), f_2(x^t), \ldots, f_n(x^t)$ are all distinct monic irreducible polynomials of degree mt and order et.*

Theorem 5. *[14] Let $q = r^e$ be a power of an odd prime p with $q \equiv 1 \pmod{r}$. Let $a = v_r(q - 1)$ be the maximum power of r dividing $q - 1$. For any $e \ge a$ and any*

irreducible factor f of Φ_{r^a} over $\mathbb{F}_q$, $f(x^{r^{e-a}})$ is also irreducible over $\mathbb{F}_q$. Moreover, all irreducible factors of Φ_{r^e} are obtained in this way.

Therefore, the following explicit factorization can be obtained in this way. Let U_e denote the set of primitive 2^e-th roots of unity.

Theorem 6. *[11] Let $q \equiv 1 \pmod 4$ be written as $q = 2^a m + 1$, $a \geq 2$, m odd. Let $e \geq 2$. Then,*

(1) if $e \leq a$, then Φ_{2^e} can be factored as

$$\Phi_{2^e}(x) = \prod_{u \in U_e} (x + u);$$

(2) if $e > a$, then Φ_{2^e} can be factored as

$$\Phi_{2^e}(x) = \prod_{u \in U_a} (x^{2^{e-a}} + u).$$

Theorem 7. *[11] Let $q \equiv 3 \pmod 4$ be written as $q = 2^a m - 1$, $a \geq 2$, m odd. Let $e \geq 2$. Then,*

(1) if $e \leq a$, then Φ_{2^e} can be factored as

$$\Phi_{2^e}(x) = \prod_{u \in U_e} (x^2 + (u + u^{-1})x + 1);$$

(2) if $e > a$, then Φ_{2^e} can be factored as

$$\Phi_{2^e}(x) = \prod_{u \in U_a} (x^{2^{e-a+1}} + (u + u^{-1})x^{2^{e-a}} - 1).$$

Theorem 8. *[14] Let p any odd prime, and $\mathbb{F}_q$ be finite field such that $q \equiv 1 \pmod p$. Then,*

(1) If $e \leq a$, then Φ_{p^e} can be factored as

$$\Phi_{p^e}(x) = \prod_{u \in U_e} (x - u);$$

(2) If $e > a$, then Φ_{p^e} can be factored as

$$\Phi_{p^e}(x) = \prod_{u \in U_a} (x^{p^{e-a}} - u).$$

Theorem 9. *[14] Let p any odd prime, and $\mathbb{F}_q$ be a finite field such that $q \equiv -1 \pmod{p}$. Then,*

(1) If $e \leq a$, then Φ_{p^e} can be factored as

$$\Phi_{p^e}(x) = \prod_{u \in U_e} (x^2 - (u + u^q)x + 1);$$

(2) If $e > a$, then Φ_{p^e} can be factored as

$$\Phi_{p^e}(x) = \prod_{u \in U_a} (x^{2p^{e-a}} - (u + u^q)x^{p^{e-a}} + 1).$$

We remark that all these irreducible factors are binomials or trinomials in the above theroems.

2.3 Composed product

Definition 8. [3] The composed product of two polynomials f and g over $\mathbb{F}_q$ is defined by $f(x) \odot g(x) = \prod_{\alpha} \prod_{\beta} (x - \alpha\beta)$, where the product $\prod_{\alpha} \prod_{\beta}$ runs over all roots α, β of f and g respectively.

It is easy to see that $\deg(f \odot g) = (\deg f) \cdot (\deg g)$.

Lemma 1. *[11] Let $f, g \in \mathbb{F}_q[x]$ be of degree m, n, respectively. Then*

$$(f \odot g)(x) = \prod_{\alpha} \alpha^n g(\alpha^{-1}x),$$

where the product $\prod_{\alpha}$ runs over all the roots of f.

Theorem 10. *[3] The composed product is a binary operation on $\mathbb{F}_q$. Moreover, $f \odot g = g \odot f$.*

Theorem 11. *[2] Let $f, g \in \mathbb{F}_q[x]$ of degrees m and n. Then, $f \odot g$ is irreducible over $\mathbb{F}_q$ if and only if f and g are irreducible over $\mathbb{F}_q$ and $gcd(m, n) = 1$.*

Corollary 1. *[9] Let $f, g \in \mathbb{F}_q[x]$ be irreducible polynomials of degrees m and n. Then, the number of distinct irreducible factors of $f \odot g$ which lie in $\mathbb{F}_q[x]$ is at most $d = gcd(m, n)$, and the degree of each factor divides $lcm(m, n)$.*

Theorem 12. *[11] let $n = {p_1}^{e_1}{p_1}^{e_1} \cdots {p_s}^{e_s}$ be the complete factorization of $n \in \mathbb{N}$. Let $\Phi_{{p_1}^{e_1}} = \prod_{i_1} f_{i_1}, \Phi_{{p_2}^{e_2}} = \prod_{i_2} f_{i_2}, \ldots, \Phi_{{p_s}^{e_s}} = \prod_{i_s} f_{i_s}$ be the corresponding factorization over $\mathbb{F}_q$. Then*

$$\begin{aligned} \Phi_n &= \Phi_{{p_1}^{e_1}} \odot \Phi_{{p_2}^{e_2}} \odot \cdots \odot \Phi_{{p_s}^{e_s}} \\ &= \prod_{i_1} \prod_{i_2} \cdots \prod_{i_s} (f_{i_1} \odot f_{i_2} \odot \cdots \odot f_{i_s}). \end{aligned}$$

Moreover, if the multiplicative orders of q modulo all these primes powers ${p_i}^{e^i}$ are pairwise coprime, then this is the complete factorization of $\Phi_n(x)$ over $\mathbb{F}_q$.

3 Composed product and factorization of cyclotomic polynomials over finite field $\mathbb{F}_q$

In this chapter, we give some technical lemmas and their proofs on composed products of certain irreducible binomials or trinomials over the finite field $\mathbb{F}_q$. These binomials and trinomials are irreducible factors of $\Phi_{r_i^{e_i}}$ such that $q \equiv \pm 1 \pmod{r_i}$ or irreducible factors of composed products of these cyclotomic polynomials. We denote ζ_L as a primitive L-th roots of unity.

Lemma 2. *Let L be a positive integer and $a, b \in \mathbb{F}_q$. Let $a = c^L$, for some c. Then,*

$$\prod_{i=0}^{L-1} \left(x - b(c\zeta_L^i)\right) = x^L - ab^L$$

Proof. Using Lemma 1, we have

$$\begin{aligned} (x^L - a) \odot (x - b) &= \prod_{i=0}^{L-1} \left(x - b(c\zeta_L^i)\right), \text{ and} \\ (x - b) \odot (x^L - a) &= x^L - ab^L \end{aligned}$$

Therefore, using Theorem 10 we have

$$\prod_{i=0}^{L-1} \left(x - b(c\zeta_L^i)\right) = x^L - ab^L$$

□

Lemma 3. *Let L and R be positive integers and $a, b \in \mathbb{F}_q$. Then*

$$\left(x^L - a\right) \odot \left(x^R - b\right) = x^{RL} - a^R b^L.$$

Furthermore, if both $x^L - a$ and $x^R - b$ are irreducible over $\mathbb{F}_q$ and $(L, R) = 1$, then $x^{RL} - a^R b^L$ is irreducible over $\mathbb{F}_q$.

Proof. Let $a = c^L$ for some c, then

$$\begin{aligned}\big(x^L - a\big) \odot \big(x^R - b\big) &= \prod_{i=0}^{L-1} \big(x - (c\ \zeta_L^i)\big) \odot \big(x^R - b\big) \\ &= \prod_{i=0}^{L-1} (c\ \zeta_L^i)^R \big(x^R (c\ \zeta_L^i)^{-R} - b\big) \\ &= \prod_{i=0}^{L-1} \big(x^R - b(c\ \zeta_L^i)^R\big) \\ &= x^{RL} - b^L a^R,\end{aligned}$$

the last equality is obtained using Lemma 2.

Moreover, since $(x^L - a)$ and $(x^R - b)$ are irreducible and $gcd(R, L) = 1$, then by Theorem 11, $x^{RL} - a^R b^L$ is irreducible over $\mathbb{F}_q$. □

Lemma 4. *Let L be a positive integer, $a \in \mathbb{F}_q$, u, $u^q \in \mathbb{F}_{q^2}$. Let $a = c^L$ for some c. Then,*

$$x^{2L} - (u^L + u^{qL})\ a\ x^L + a^2\ u^{(q+1)L} = \prod_{i=0}^{L-1} \big(x^2 - (u + u^q)(c\ \zeta_L^i)x + (c\ \zeta_L^i)^2 u^{q+1}\big),$$

Proof. Obviously, by using Lemma 1, we have

$$\begin{aligned}\big(x^2 - (u + u^q)x + u^{q+1}\big) \odot \big(x^L - a\big) &= u^L \big(x^L u^{-L} - a\big) u^{qL} \big(x^L u^{-qL} - a\big) \\ &= \big(x^L - a u^L\big)\big(x^L - a u^{qL}\big) \\ &= x^{2L} - (u^L + u^{qL}) a x^L + a^2 u^{(q+1)L}.\end{aligned}$$

On the other hand, we have

$$\begin{aligned}&\big(x^L - a\big) \odot \big(x^2 - (u + u^q)x + u^{q+1}\big) \\ = &\prod_{i=0}^{L-1} (c\zeta_L^i)^2 \big(x^2 (c\zeta_L^i)^{-2} - (u + u^q)(c\zeta_L^i)^{-1} x + u^{q+1}\big) \\ = &\prod_{i=0}^{L-1} \big(x^2 - (u + u^q)(c\zeta_L^i)x + u^{q+1}(c\zeta_L^i)^2\big).\end{aligned}$$

Therefore, by using Theorem 10 we have, $x^{2L} - (u^L + u^{qL})\ a\ x^L + a^2\ u^{(q+1)L} = \prod_{i=0}^{L-1} \big(x^2 - (u+u^q)(c\ \zeta_L^i)x + (c\ \zeta_L^i)^2 u^{q+1}\big)$.

□

Lemma 5. *Let L, R be odd positive integers, $a \in \mathbb{F}_q$, and $u, u^q \in \mathbb{F}_{q^2}$. Then*

$$\big(x^L - a\big) \odot \big(x^{2R} - (u+u^q)x + u^{q+1}\big) = x^{2LR} - (u^L + u^{qL})\ a^R\ x^{RL} + a^{2R}\ u^{(q+1)L}.$$

Furthermore, if both $(x^L - a)$ and $(x^{2R} - (u+u^q)x + u^{q+1})$ are irreducible over $\mathbb{F}_q$ and $(L, 2R) = 1$, then $x^{2LR} - (u^L + u^{qL})\ a^R\ x^{LR} + a^{2R}\ u^{(q+1)L}$ is irreducible over $\mathbb{F}_q$.

Proof. Let $a = c^L$ for some c, then

$$\begin{aligned}
& \big(x^L - a\big) \odot \big(x^{2R} - (u+u^q)x + u^{q+1}\big) \\
= & \prod_{i=0}^{L-1} \big(x - (c\zeta_L^i)\big) \odot \big(x^{2R} - (u+u^q)x + u^{q+1}\big) \\
= & \prod_{i=0}^{L-1} (c\zeta_L^i)^{2R} \big(x^{2R}(c\zeta_L^i)^{-2R} - (u+u^q)(c\zeta_L^i)^{-R}x^R + u^{q+1}\big) \\
= & \prod_{i=0}^{L-1} \big(x^{2R} - (u+u^q)(c\ \zeta_L^i)^R\ x^R + (c\ \zeta_L^i)^{2R})u^{q+1}\big) \\
= & \ x^{2RL} - (u^L + u^{qL})\ a^R\ x^{RL} + a^{2R}\ u^{(q+1)L},
\end{aligned}$$

the last equality is obtained by using Lemma 4. Moreover, since $gcd(L, 2R) = 1$, $x^L - a$ and $x^{2R} - (u+u^q)x^R + u^{q+1}$ are irreducible over $\mathbb{F}_q$. Then by Theorem 11, $x^{2RL} - (u^L + u^{qL})\ a^R\ x^{RL} + a^{2R}\ u^{(q+1)L}$ is irreducible over $\mathbb{F}_q$. □

Lemma 6. *Let $q \equiv 1 \pmod 4$ such that $q = 2^A m + 1$, $A \geq 2$, and m is odd. Let L and R be positive integers, and let c, $d \in \mathbb{F}_q$ such that $c = -d = -b^2$ and $d^{2^{A-1}} = -1$.*

Let $u, u^q \in \mathbb{F}_{q^2}$, *then*

$$\begin{aligned}
& \big(x^{2L}+c\big) \odot \big(x^{2R}-(u+u^q)x^R+u^{(q+1)R}\big) \\
= \; & \big(x^{2L}-d\big) \odot \big(x^{2R}-(u+u^q)x^R+u^{(q+1)R}\big) \\
= \; & \big(x^{2LR}-(b^R u^L+b^{qR}u^{qL})x^{LR}+b^{(q+1)R}u^{(q+1)L}\big) \\
& \big(x^{2LR}-(b^R u^{qL}+b^{qR}u^L)x^{LR}+b^{(q+1)R}u^{(q+1)L}\big).
\end{aligned}$$

Furthermore, if both $(x^{2L}-d)$ *and* $(x^{2R}-(u+u^q)x^R+u^{(q+1)R})$ *are irreducible over* $\mathbb{F}_q$ *and* $(2L,2R)=2$ *then both* $x^{2LR}-(b^R u+b^{qR}u^q)x^{LR}+b^{(q+1)R}u^{(q+1)L}$ *and* $x^{2LR}-(b^R u^q+b^{qR}u)x^{LR}+b^{(q+1)R}u^{(q+1)L}$ *are irreducible over* $\mathbb{F}_q$.

Proof. Since $d^{2^{A-1}}=-1$, then $b^{2^A}=-1$ and $b^q = b^{2^A m+1}=b^{2^A m}b=(b^{2^A})^m b=(-1)^m b=-b$. Hence $x^{2L}-d = \big(x^L-b\big)\big(x^L+b\big)=\big(x^L-b\big)\big(x^L-b^q\big)$. Assume $b=f^L$, we obtain

$$\begin{aligned}
& \big(x^{2L}-d\big) \odot \big(x^{2R}-(u+u^q)x^R+u^{(q+1)R}\big) \\
= \; & \big(x^L-b\big)\big(x^L-b^q\big) \odot \big(x^{2R}-(u+u^q)x^R+u^{(q+1)R}\big) \\
= \; & \Big(\big(x^L-b\big) \odot \big(x^{2R}-(u+u^q)x^R+u^{(q+1)R}\big)\Big) \\
& \Big(\big(x^L-b^q\big) \odot \big(x^{2R}-(u+u^q)x^R+u^{(q+1)R}\big)\Big) \\
= \; & \prod_{i=0}^{L-1} \big(x^{2R}-(u+u^q)(f\ \zeta_L^i)^R\ x^R+(f\zeta_L^i)^{2R})u^{q+1}\big) \\
& \prod_{i=0}^{L-1} \big(x^{2R}-(u+u^q)(f^q\zeta_L^i)^R\ x^R+(f^q\zeta_L^i)^{2R}u^{q+1}\big) \\
= \; & \big(x^{2LR}-(b^R u^L+b^R u^{qL})x^{LR}+b^{2R}u^{(q+1)L}\big) \\
& \big(x^{2LR}-(b^{qR}u^L+b^{qR}u^{qL})x^{LR}+b^{2qR}u^{(q+1)L}\big),
\end{aligned}$$

where the last equality holds by Lemma 5. Expanding the multiplication, we obtain

$$\begin{aligned}
& \big(x^{2L} - d\big) \odot \big(x^{2R} - (u + u^q)x^R + u^{(q+1)R}\big) \\
= \; & \big(x^{2LR} - (b^R u^L + b^R u^{qL})x^{LR} + b^{2R} u^{(q+1)L}\big) \\
& \big(x^{2LR} - (b^{qR} u^L + b^{qR} u^{qL})x^{LR} + b^{2qR} u^{(q+1)L}\big) \\
= \; & \Big(x^{4LR} - \big(b^R u^L + b^R u^{qL} + b^{qR} u^L + b^{qR} u^{qL}\big)x^{3L} + \\
& \big(b^{2qR} u^{(q+1)L} + b^{2R} u^{(q+1)L} + b^{(q+1)R} u^{2L} + b^{(q+1)R} u^{(q+1)L} + \\
& b^{(q+1)R} u^{(q+1)L} + b^{(q+1)R} u^{2qL}\big)x^{2L} - \big(b^{(2q+1)R} u^{(q+2)L} + b^{(2q+1)R} u^{(2q+1)L} + \\
& b^{(q+2)R} u^{(q+2)L} + b^{(q+2)R} u^{(2q+1)L}\big)x^L + b^{2R(q+1)} u^{2L(q+1)}\big) \\
= \; & \big(x^{2LR} - (b^R u^L + b^{qR} u^{qL})x^{LR} + b^{(q+1)R} u^{(q+1)L}\big) \\
& \big(x^{2LR} - (b^R u^{qL} + b^{qR} u^L)x^{LR} + b^{(q+1)R} u^{(q+1)L}\big),
\end{aligned}$$

where the last two polynomials belong to $\mathbb{F}_q[x]$. Moreover, since $gcd(2L, 2R) = 2$, $(x^{2L} + c)$ and $(x^{2R} - (u + u^q)x^R + u^{(q+1)R})$ are irreducible over $\mathbb{F}_q$, then by Corollary 1, both $x^{2LR} - (b^r u^L + b^{qR} u^{qL})x^{LR} + b^{(q+1)R})u^{(q+1)L}$ and $x^{2LR} - (b^r u^{qL} + d^{qR} u^L)x^{LR} + b^{(q+1)R})u^{(q+1)L} f$ are irreducible over $\mathbb{F}_q$. □

Lemma 7. *Let L be a positive integer, u, u^q, v, $v^q \in \mathbb{F}_{q^2}$. Let $(\bar{u}\zeta_L)^L = u$, $(\bar{u^q}\zeta_L)^L = u^q$ for some $\bar{u}, \bar{u^q}$, then*

$$\begin{aligned}
& \big(x^{2L} - (uv^L + u^q v^{qL})x^L + u^{q+1} v^{(q+1)L}\big) \\
& \big(x^{2L} - (u^q v^L + uv^{qL})x^L + u^{q+1} v^{(q+1)L}\big) \\
= \; & \prod_{i=0}^{L-1} \big(x^2 - (v + v^q)(\bar{u}\zeta_L^i)x + v^{q+1}\ (\bar{u}\zeta_L^i)^2\big) \\
& \big(x^2 - (v + v^q)(\bar{u^q}\zeta_L^i)x + v^{q+1}\ (\bar{u^q}\zeta_L^i)^2\big).
\end{aligned}$$

Proof. Obviously, by using Lemma 1, we have

$$\begin{aligned}
&\big(x^2-(v+v^q)x+v^{q+1}\big)\odot\big(x^{2L}-(u+u^q)x^L+u^{q+1}\big)\\
=\;& v^{2L}\big(x^{2L}v^{-2L}-(u+u^q)v^{-L}x^L+u^{q+1}\big)\\
&v^{2qL}\big(x^{2L}v^{-2L}-(u+u^q)v^{-qL}x^L+u^{q+1}\big)\\
=\;&\big(x^{2L}-(u+u^q)v^Lx^L+u^{q+1}v^{2L}\big)\big(x^{2L}-(u+u^q)v^{qL}x^L+u^{q+1}v^{q2L}\big)\\
=\;&\big(x^{2L}-(uv^L+u^qv^L)x^L+u^{q+1}v^{2L}\big)\big(x^{2L}-(uv^{qL}+u^qv^{qL})x^L+u^{q+1}v^{2qL}\big)\\
=\;&\Big(x^{4L}-\big(uv^{qL}+u^qv^{qL}+uv^L+u^qv^L\big)x^{3L}+\big(u^{q+1}v^{2qL}+u^{(q+1)}v^{2L}+\\
&u^2v^{(q+1)L}+u^{(q+1)}v^{(q+1)L}+u^{(q+1)}v^{(q+1)L}+u^{2q}v^{(q+1)L}\big)x^{2L}-\big(u^{(q+2)}v^{(2q+1)L}\\
&+u^{(2q+1)}v^{(2q+1)L}+u^{(q+2)}v^{(q+2)L}+u^{(2q+1)}v^{(q+2)L}\big)x^L+u^{2(q+1)}v^{2L(q+1)}\Big)\\
=\;&\big(x^{2L}-(uv^L+u^qv^{qL})x^L+u^{q+1}v^{(q+1)L}\big)\big(x^{2L}-(uv^{qL}+u^qv^L)x^L+u^{q+1}v^{(q+1)L}\big).
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
&\big(x^{2L}-(u+u^q)x^L+u^{q+1}\big)\odot\big(x^2-(v+v^q)x+v^{q+1}\big)\\
=\;&\prod_{i=0}^{L-1}(\bar{u}\zeta_L^i)^2\big(x^2(\bar{u}\zeta_L^i)^{-2}-(v+v^q)(\bar{u}\zeta_L^i)^{-1})x+v^{q+1}\big)\\
&(\bar{u^q}\zeta_L^i)^2\big(x^2(\bar{u^q}\zeta_L^i)^{-2}-(v+v^q)(\bar{u^q}\zeta_L^i)^{-1}x+v^{q+1}\big)\\
=\;&\prod_{i=0}^{L-1}\big(x^2-(v+v^q)(\bar{u}\zeta_L^i))x+v^{(q+1)}(\bar{u}\zeta_L^i)^2\big)\\
&\big(x^2-(v+v^q)(\bar{u^q}\zeta_L^i)x+v^{(q+1)}(\bar{u^q}\zeta_L^i)^2\big)
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\prod_{i=0}^{L-1}\big(x^2-(v+v^q)(\bar{u}\zeta_L^i)x+v^{(q+1)}\ (\bar{u}\zeta_L^i)^2\big)\\
&\big(x^2-(v+v^q)(\bar{u^q}\zeta_L^i)x+v^{(q+1)}\ (\bar{u^q}\zeta_L^i)^2\big)\\
=\;&\big(x^{2L}-(v^Lu+v^{qL}u^q)x^L+v^{(q+1)L}u^{q+1}\big)\\
&\big(x^{2L}-(v^Lu^q+v^{qL}u)x^L+v^{(q+1)L}u^{q+1}\big).
\end{aligned}$$

□

Lemma 8. *Let L and R be positive integers, u, u^q, v, v^q $\in \mathbb{F}_{q^2}$. Then*

$$\begin{aligned} & \big(x^{2L} - (u+u^q)x + u^{q+1}\big) \odot \big(x^{2R} - (v+v^q)x + v^{q+1}\big) \\ = \; & \big(x^{2LR} - (v^L u^R + u^{qL} v^{qR})x^{LR} + v^{(q+1)^L} u^{(q+1)^R}\big) \\ & \big(x^{2LR} - (v^L u^{qR} + v^{qL} u^R)x^{LR} + v^{(q+1)^L} u^{(q+1)^R}\big). \end{aligned}$$

Furthermore, if both $(x^{2L}-(u+u^q)x+u^{q+1})$ and $(x^{2R}-(v+v^q)x+v^{q+1})$ are irreducible over $\mathbb{F}_q$ and $(2L, 2R) = 2$, then both $(x^{2LR} - (v^L u^R + u^{qL} v^{qR})x^{LR} + v^{(q+1)^L} u^{(q+1)^R})$ and $(x^{2LR} - (v^L u^{qR} + v^{qL} u^R)x^{LR} + v^{(q+1)^L} u^{(q+1)R})$ are irreducible over $\mathbb{F}_q$.

Proof. Let $(\bar{u}\zeta_L)^L = u$, $(\bar{u^q}\zeta_L)^L = u^q$ for some $\bar{u}, \bar{u^q}$, we have

$$\begin{aligned} & \big(x^{2L} - (u+u^q)x + u^{q+1}\big) \odot \big(x^{2R} - (v+v^q)x + v^{q+1}\big) \\ = \; & \prod_{i=0}^{L-1} (\bar{u}\zeta_L^i)^{2R} \big(x^{2R}(\bar{u}\zeta_L^i)^{-2R} - (v+v^q)(\bar{u}\zeta_L^i)^{-R})x^R + v^{q+1}\big) \\ & (\bar{u^q}\zeta_L^i)^{2R} \big(x^{2R}(\bar{u^q}\zeta_L^i)^{-2R} - (v+v^q)(\bar{u^q}\zeta_L^i)^{-R}x^R + v^{q+1}\big) \\ = \; & \prod_{i=0}^{L-1} \big(x^{2R} - (v+v^q)(\bar{u}\zeta_L^i)^R x^R + v^{q+1}(\bar{u}\zeta_L^i)^{2R}\big) \\ & \big(x^{2R} - (v+v^q)(\bar{u^q}\zeta_L^i)^R x^R + v^{(q+1)}(\bar{u^q}\zeta_L^i)^{2R}\big) \\ = \; & \big(x^{2LR} - (v^L u^R + v^{qR} u^{qL})x^{LR} + v^{(q+1)^L} u^{(q+1)^R}\big) \\ & \big(x^{2LR} - (v^L u^{qR} + v^{qL} u^R)x^{LR} + v^{(q+1)^L} u^{(q+1)^R}\big), \end{aligned}$$

the last equality is obtained by Lemma 7. Moreover, since $x^{2L} - (u+u^q)x + u^{q+1}$ and $x^{2R} - (v+v^q)x + v^{(q+1)}$ are irreducible over $\mathbb{F}_q$, and $gcd(2L, 2R) = 2$, then by Corollary 1, both $x^{2LR} - (v^L u^R + v^{qR} u^{qL})x^{LR} + v^{(q+1)^L} u^{(q+1)^R}$ and $x^{2LR} - (v^L u^{qR} + v^{qL} u^R)x^{LR} + v^{(q+1)^L} u^{(q+1)^R}$ are irreducible over $\mathbb{F}_q$.

□

Lemma 9. *Let $q \equiv 3 \pmod 4$ such that $q = 2^a m - 1$, $a \geq 2$, and m is odd. Let L*

and R be positive integers. Let u, u^q, v, $v^q \in \mathbb{F}_{q^2}$. Let $(\bar{v}\zeta_L)^L = v$, $(\bar{v^q}\zeta_L)^L = v^q$, then

$$\begin{aligned}
& \big(x^{2L} + (vu^L + v^q u^{qL})x^L + v^{q+1}u^{(q+1)L}\big) \\
& \big(x^{2L} + (vu^{qL} + v^q u^L)x^L + v^{q+1}u^{(q+1)L}\big) \\
= & \prod_{i=0}^{L-1} \big(x^2 - (u+u^q)(-\bar{v}\zeta_L^i))x + u^{(q+1)}(\bar{v}\zeta_L^i)^2\big) \\
& \big(x^2 - (u+u^q)(-\bar{v^q}\zeta_L^i)x + u^{(q+1)}(\bar{v^q}\zeta_L^i)^2\big).
\end{aligned}$$

Proof. Obviously, by using Lemma 1, we have

$$\begin{aligned}
& \big(x^2 - (u+u^q)x + u^{q+1}\big) \odot \big(x^{2L} + (v+v^q)x^R + v^{q+1}\big) \\
= & u^{2L}\big(x^{2L}u^{-2L} + (v+v^q)u^{-L}x^L + v^{q+1}\big) \\
& u^{2qL}\big(x^{2L}u^{-2L} + (v+v^q)u^{-qL}x^L + v^{q+1}\big) \\
= & \big(x^{2L} + (v+v^q)(u)^L x^L + v^{q+1}u^{2L}\big)\big(x^{2L} + (v+v^q)(u^q)^L x^L + v^{q+1}u^{q2L}\big) \\
= & \big(x^{2L} + (vu^L + v^q u^L)x^L + v^{q+1}u^{2L}\big)\big(x^{2L} + (vu^{qL} + v^q u^{qL})x^L + v^{q+1}u^{2qL}\big) \\
= & \Big(x^{4L} + \big(vu^{qL} + v^q u^{qL} + vu^L + v^q u^L\big)x^{3L} + \big(v^{q+1}u^{2qL} + v^{(q+1)}u^{2L} + \\
& v^2 u^{(q+1)L} + v^{(q+1)}u^{(q+1)L} + v^{(q+1)}u^{(q+1)L} + v^{2q}u^{(q+1)L}\big)x^{2L} - \big(v^{(q+2)}u^{(2q+1)L} \\
& + v^{(2q+1)}u^{(2q+1)L} + v^{(q+2)}u^{(q+2)L} + v^{(2q+1)}u^{(q+2)L}\big)x^L + v^{2(q+1)}u^{2L(q+1)}\Big). \\
= & \big(x^{2L} + (vu^L + v^q u^{qL})x^L + v^{q+1}u^{(q+1)L}\big) \\
& \big(x^{2L} + (vu^{qL} + v^q u^L)x^L + v^{q+1}u^{(q+1)L}\big).
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
& \big(x^{2L} + (v+v^q)x^L + v^{(q+1)}\big) \odot \big(x^2 - (u+u^q)x + u^{q+1}\big) \\
= & \prod_{i=0}^{L-1} (-\bar{v}\zeta_L^i)^2\big(x^2(\bar{v}\zeta_L^i)^{-2} - (u+u^q)(-\bar{v}\zeta_L^i)^{-1})x + u^{q+1}\big) \\
& (-\bar{v^q}\zeta_L^i)^2\big(x^2(-\bar{u^q}\zeta_L^i)^{-2} - (u+u^q)(\bar{v^q}\zeta_L^i)^{-1}x + u^{q+1}\big) \\
= & \prod_{i=0}^{L-1} \big(x^2 - (u+u^q)(-\bar{v}\zeta_L^i))x + u^{(q+1)}(\bar{v}\zeta_L^i)^2\big) \\
& \big(x^2 - (u+u^q)(-\bar{v^q}\zeta_L^i)x + u^{(q+1)}(\bar{v^q}\zeta_L^i)^2\big)
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\prod_{i=0}^{L-1}\left(x^2-(u+u^q)(-\bar{v}\zeta_L^i)\right)x+u^{(q+1)}(\bar{v}\zeta_L^i)^2\big)\\
&\big(x^2-(u+u^q)(-\bar{v^q}\zeta_L^i)x+u^{(q+1)}(\bar{v^q}\zeta_L^i)^2\big).\\
=\ &\big(x^{2L}+(vu^L+v^qu^{qL})x^L+v^{q+1}u^{(q+1)L}\big)\\
&\big(x^{2L}+(vu^{qL}+v^qu^L)x^L+v^{q+1}u^{(q+1)L}\big).
\end{aligned}$$

□

Lemma 10. *Let $q\equiv 3 \pmod 4$ such that $q=2^am-1$, $a\geq 2$, and m is odd. Let L and R be positive integers. Let $u,u^q,v,v^q\in\mathbb{F}_{q^2}$, then*

$$\begin{aligned}
&\big(x^{2R}-(u+u^q)x^R+u^{q+1}\big)\odot\big(x^{2L}+(v-v^{-1})x^L-1\big)\\
=\ &\big(x^{2R}-(u+u^q)x^R+u^{q+1}\big)\odot\big(x^{2L}+(v+v^q)x^L+v^{q+1}\big)\\
=\ &\big(x^{2LR}+(v^Ru^L+v^{qR}u^{qL})x^{LR}+v^{(q+1)R}u^{(q+1)L}\big)\\
&\big(x^{2LR}+(v^Ru^{qL}+v^{qR}u^L)x^{LR}+v^{(q+1)R}u^{(q+1)L}\big).
\end{aligned}$$

Furthermore, if both $x^{2R}-(u+u^q)x^R+u^{q+1}$ and $x^{2L}+(v-v^{-1})x^L-1$ are irreducible over $\mathbb{F}_q$ and $(2L,2R)=2$, then both $x^{2RL}+(u^Lv^R+u^{qL}v^{qR})x^{RL}+u^{(q+1)L}v^{(q+1)R}$ and $x^{2LR}+(v^Lu^{qR}+v^{qL}u^R)x^{LR}+v^{(q+1)^L}$ are irreducible over $\mathbb{F}_q$.

Proof. Let $(\bar{u}\zeta_R)^R=u$, $(\bar{u^q}\zeta_R)^R=u^q$ for some $\bar{u},\bar{u^q}$, we have

$$\begin{aligned}
&\big(x^{2R}-(u+u^q)x^R+u^{q+1}\big)\odot\big(x^{2L}+(v+v^q)x^L+v^{q+1}\big)\\
=\ &\prod_{i=0}^{R-1}(\bar{u}\zeta_R^i)^{2L}\big(x^{2L}(\bar{u}\zeta_R^i)^{-2L}+(v+v^q)(\bar{u}\zeta_R^i)^{-L})x^L+v^{q+1}\big)\\
&(\bar{u^q}\zeta_R^i)^{2L}\big(x^{2L}(\bar{u^q}\zeta_R^i)^{-2L}+(v+v^q)(\bar{u^q}\zeta_R^i)^{-L}x^L+v^{q+1}\big)\\
=\ &\prod_{i=0}^{R-1}\Big(x^{2L}+(v+v^q)(\bar{u}\zeta_R^i)^Lx^L-(\bar{u}\zeta_R^i)^{2L}\big)\\
&\big(x^{2L}+(v+v^q)(\bar{u^q}\zeta_R^i)^Lx^L+(\bar{u^q}\zeta_R^i)^{2L}\big)
\end{aligned}$$

$$
\begin{aligned}
&= \left(x^{2LR} + (v^R + v^{qR})u^L x^{LR} + v^{(q+1)R}u^{2L}\right) \\
&\quad \left(x^{2LR} + (v^R + v^{qR})u^{qL} x^{LR} + v^{(q+1)R}u^{2qL}\right) \\
&= \left(x^{2LR} + (v^R u^L + v^{qR}u^{qL})x^{LR} + v^{(q+1)R}u^{(q+1)L}\right) \\
&\quad \left(x^{2LR} + (v^R u^{qL} + v^{qR}u^L)x^{LR} + v^{(q+1)R}u^{(q+1)L}\right),
\end{aligned}
$$

the last equality is obtained by Lemma 9. Moreover, since $x^{2R} - (u + u^q)x^R + u^{q+1}$ and $x^{2L} + (v + v^q)x^L + v^{(q+1)}$ are irreducible over $\mathbb{F}_q$, and $gcd(2L, 2R) = 2$, then by Corollary 1, both $x^{2LR} + (v^R u^L + v^{qR}u^{qL})x^{LR} + v^{(q+1)R}u^{(q+1)L}$ and $x^{2LR} + (v^R u^{qL} + v^{qR}u^L)x^{LR} + v^{(q+1)R}u^{(q+1)L}$, are irreducible over $\mathbb{F}_q$.

□

We have presented some technical lemmas and their proofs on the composed products of irreducible binomials and trinomials of special forms. This will help us derive the results of factorization of cyclotomic polynomial Φ_n over $\mathbb{F}_q$ such that q is congruent to ± 1 modulo each prime divisor of n in the next chapter.

4 Factorization of the cyclotomic polynomial $\Phi_n(x)$ when q is congruent to ± 1 modulo each prime divisor of n

In this chapter, we give theorems and their proofs for the factorization of $\Phi_{r_1{}^{e_1}} \odot \cdots \odot \Phi_{r_t{}^{e_t}}$ when $q \equiv 1 \pmod{r_i}$, where $1 \leq i \leq t$, the factorization of $\Phi_{r_{t+1}{}^{e_{t+1}}} \odot \cdots \odot \Phi_{r_{t+s}{}^{e_{t+s}}}$ when $q \equiv -1 \pmod{r_{t+i}}$, where $t+1 \leq i \leq t+s$, and then we give the factorization of $\Phi_{r_1{}^{e_1}} \odot \cdots \odot \Phi_{r_t{}^{e_t}} \odot \Phi_{r_{t+1}{}^{e_{t+1}}} \odot \cdots \odot \Phi_{r_{t+s}{}^{e_{t+s}}}$ when $q \equiv 1 \pmod{r_i}$ for $1 \leq i \leq t$, $q \equiv -1 \pmod{r_i}$ for $t+1 \leq i \leq t+s$, where r_i's are distinct odd primes. When q is odd and n is even, the factorization of Φ_n are considered separately under the different assumptions depending on $q \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$. Throughout the rest of the thesis, when $q \equiv 1 \pmod{r_i}$, then we let $a_i = v_r(q-1)$ denote the highest power of r dividing $q-1$. When $q \equiv -1 \pmod{r_i}$, then we let $a_i = v_r(q^2-1)$ denote the highest power of r dividing q^2-1.

4.1 Factorization of $\Phi_{r_1{}^{e_1}} \odot \cdots \odot \Phi_{r_t{}^{e_t}}$ when $q \equiv 1 \pmod{r_i}$

We first prove Theorem 8 (with different notations) because it is used in the factorization of $\Phi_{r_1{}^{e_1}} \odot \cdots \odot \Phi_{r_t{}^{e_t}}$ when $q \equiv 1 \pmod{r_i}$ for $1 \leq i \leq t$.

Theorem 13. *Let r_i be any odd prime, $\mathbb{F}_q$ be a finite field such that $q \equiv 1 \pmod{r_i}$, and $a_i = v_{r_i}(q-1)$. Then, the factorization of $\Phi_{r_i^{e_i}}(x)$ is given by*

$$\Phi_{r_i^{e_i}}(x) = \begin{cases} \displaystyle\prod_{\zeta_{r_i^{e_i}} \in \Omega(r_i^{e_i})} (x - \zeta_{r_i^{e_i}}), & \text{if } e_i \leq a_i; \\ \displaystyle\prod_{\zeta_{r_i^{a_i}} \in \Omega(r_i^{a_i})} (x^{r_i^{e_i - a_i}} - \zeta_{r_i^{a_i}}), & \text{if } e_i > a_i, \end{cases}$$

where $\Omega(r_i^{a_i})$ denotes the set of all $r_i^{a_i}$th primitive roots of unity.

Proof. When $e_i \leq a_i$, $q \equiv 1 \pmod{r_i}$ implies $r_i \mid q-1$ because $a_i = v_{r_i}(q-1)$. Then,

there exist a primitive $r_i^{e_i}$th root in $\mathbb{F}_q$ and the factorization of $\Phi_{r_i^{e_i}}(x)$ is

$$\Phi_{r_i^{e_i}}(x) = \prod_{\zeta_{r_i^{e_i}} \in \Omega(r_i^{e_i})} (x - \zeta_{r_i^{e_i}}).$$

When $e_i > a_i$, by Theorem 2, the number of distinct irreducible factor of $\Phi_{r_i^{a_i}}$ is $\phi(r_i^{a_i})/m$ where m is the least positive integer such that $q^m \equiv 1 \pmod{r_i^{a_i}}$. Here we have $m = 1$, and hence $r_i^{a_i+1} \nmid (q-1)$. In addition, each factor of $\Phi_{r_i^{a_i}}$ has order $e = {r_i}^{a_i}$ and $r_i \mid {r_i}^{a_i}$ but $r_i \nmid \frac{q-1}{{r_i}^{a_i}}$. Then, by Theorem 4, each irreducible factors f of $\Phi_{{r_i}^{a_i}}$ generates an irreducible factor $f(x^{{r_i}^{e_i-a_i}})$ for $\Phi_{{r_i}^{e_i}}$, which is of order ${r_i}^{e_i}$, and of degree ${r_i}^{e_i-a_i}$. Therefore, the factorization of $\Phi_{{r_i}^{a_i}}(x)$ is given as

$$\Phi_{{r_i}^{e_i}}(x) = \prod_{\zeta_{{r_i}^{a_i}} \in \Omega(r^a)} (x^{r_i^{e_i-a_i}} - \zeta_{r_i^{a_i}}).$$

□

Using composed products of irreducible binomials, we now give the factorization of $\Phi_{{r_1}^{e_1}} \odot \cdots \odot \Phi_{{r_t}^{e_t}}$ when $q \equiv 1 \pmod{r_i}$ where $1 \le i \le t$. Each irreducible factor is again a binomial.

Theorem 14. *Let r_i be any distinct odd prime, $\mathbb{F}_q$ be the finite field with q elements such that $q \equiv 1 \pmod{r_i}$, and $a_i = v_{r_i}(q-1)$ where $1 \le i \le t$, then the irreducible factorization of $\Phi_{{r_1}^{e_1}} \odot \cdots \odot \Phi_{{r_t}^{e_t}}$ is given as*

$$\begin{aligned}
\Phi_{{r_1}^{e_1}}(x) \odot \cdots \odot \Phi_{{r_t}^{e_t}}(x) &= \prod_{c_1} \ldots \prod_{c_t} (x^{A_1} - c_1) \odot \cdots \odot (x^{A_t} - c_t) \\
&= \prod_{c_1} \cdots \prod_{c_t} (x^{F_t} - \prod_{i=1}^{t} {c_i}^{F_t/A_i}), \text{ where } F_t = A_1\, A_2 \cdots A_t,
\end{aligned}$$

and

$$A_i = \begin{cases} 1, & \text{if } e_i \le a_i; \\ r_i^{e_i - a_i}, & \text{if } e_i > a_i. \end{cases}$$

In addition, $c_i \in \Omega({r_i}^{e_i})$ if $e_i \le a_i$ or $c_i \in \Omega({r_i}^{a_i})$ if $e_i > a_i$.

Proof. We use mathematical induction to prove this result.

Because $q \equiv 1 \pmod{r_i}$, by Theorem 13, we have

$$\Phi_{{r_i}^{e_i}}(x) = \prod_{c_i}(x^{A_i} - c_i).$$

First, we assume $t = 2$. We have,

$$\begin{aligned}
\Phi_{{r_1}^{e_1}}(x) \odot \Phi_{{r_2}^{e_2}}(x) &= \prod_{c_1}(x^{A_1} - c_1) \odot \prod_{c_2}(x^{A_2} - c_2) \\
&= \prod_{c_1}\prod_{c_2}(x^{A_1} - c_1) \odot (x^{A_2} - c_2) \\
&= \prod_{c_1}\prod_{c_2}(x^{A_1A_2} - c_2^{A_1}c_1^{A_2}),
\end{aligned}$$

the last equality is obtained by using Lemma 3. In addition, because r_i are distinct odd primes, then $gcd(A_1, A_2) = 1$ and thus $(x^{A_1A_2} - c_2^{A_1}c_1^{A_2})$ is irreducible over $\mathbb{F}_q$.

Second, we assume the result is true for t

$$\begin{aligned}
&\Phi_{{r_1}^{e_1}}(x) \odot \Phi_{{r_2}^{e_2}}(x) \odot \cdots \odot \Phi_{{r_t}^{e_t}}(x) \\
= &\prod_{c_1,c_2,\ldots,c_t}(x^{A_1A_2\cdots A_t} - c_t^{A_1A_2A_3\cdots/A_t} \ \cdots \ c_2^{A_1\cdots A_T/A_2}c_1^{A_2\cdots A_T/A_1}),
\end{aligned}$$

Now, we will prove the result for $t + 1$

$$\begin{aligned}
&(\Phi_{{r_1}^{e_1}}(x) \odot \Phi_{{r_2}^{e_2}}(x) \odot \cdots \odot \Phi_{{r_t}^{e_t}}(x)) \odot (\Phi_{{r_{t+1}}^{e_{t+1}}}(x)) \\
= &\prod_{c_1,\ldots,c_t}(x^{A_1A_2\cdots A_t} - c_t^{A_1A_2A_3\cdots/A_t} \ \cdots \ c_2^{A_1\cdots A_T/A_2}c_1^{A_2\cdots A_T/A_1}) \odot \prod_{c_{t+1}}(x^{A_{t+1}} - c_{t+1}) \\
= &\prod_{c_1,\ldots,c_t}\prod_{c_{t+1}}(x^{A_1A_2\cdots A_t} - c_t^{A_1A_2A_3\cdots/A_t} \ \cdots \ c_2^{A_1\cdots A_T/A_2}c_1^{A_2\cdots A_T/A_1}) \odot (x^{A_{t+1}} - c_{t+1}) \\
= &\prod_{c_1,\ldots,c_t}\prod_{c_{t+1}}(x^{A_1A_2\cdots A_{t+1}} - c_{t+1}^{A_1A_2A_3\cdots/A_{t+1}}c_t^{A_1A_2A_3\cdots/A_t}\cdots c_2^{A_1\cdots A_t/A_2}c_1^{A_2\cdots A_t/A_1}),
\end{aligned}$$

the last equality is obtained also by using Lemma 3. Moreover, because r_i are distinct odd primes, then $gcd(A_1 \cdots A_t, A_{t+1}) = 1$ and thus $(x^{A_1A_2\cdots A_{t+1}} - c_{t+1}^{A_1A_2A_3\cdots/A_{t+1}}c_t^{A_1A_2A_3\cdots/A_t}$.

$\cdot\cdot\, c_2^{A_1\cdots A_t/A_2} c_1^{A_2\cdots A_t/A_1})$ is irreducible over $\mathbb{F}_q$.

Therefore, by mathematical induction we prove that,

$$\begin{aligned}
&\Phi_{r_1{}^{e_1}}(x) \odot \cdots \odot \Phi_{r_t{}^{e_t}}(x) \\
= &\prod_{c_1} \cdots \prod_{c_t} (x^{A_1A_2\cdots A_t} - c_t^{A_1A_2A_3\cdots/A_t} \ \cdots\ c_3^{A_1A_2\cdots A_t/A_3} c_2^{A_1\cdots A_t/A_2} c_1^{A_2\cdots A_t/A_1}) \\
= &\prod_{c_1} \cdots \prod_{c_t} (x^{F_t} - \prod_{i-1}^{t} c_i{}^{F_t/A_i}).
\end{aligned}$$

□

4.2 Factorization of $\Phi_{r_{t+1}{}^{e_{t+1}}} \odot \cdots \odot \Phi_{r_{t+s}{}^{e_{t+s}}}$ when $q \equiv -1 \pmod{r_{t+i}}$

Similarly, we prove Theorem 9 (again with new notations that we prefer) before we obtain the factorization of $\Phi_{r_{t+1}{}^{e_{t+1}}} \odot \cdots \odot \Phi_{r_{t+s}{}^{e_{t+s}}}$ when $q \equiv -1 \pmod{r_{t+i}}$ where $1 \le i \le s$ and t is fixed. Without loss of generality, we present the following results with $t = 0$ for simplicity.

Theorem 15. *Let r_i be any distinct prime, $\mathbb{F}_q$ be a finite field such that $q \equiv -1 \pmod{r_i}$, and $a_i = v_{r_i}(q^2-1)$. Then, $\Phi_{r_i^{e_i}}(x)$ is given by*

$$\Phi_{r_i^{e_i}}(x) = \begin{cases} \displaystyle\prod_{\zeta_{r_i^{e_i}} \in \Omega(r_i^{e_i})} (x^2 - (\zeta_{r_i^{e_i}} + \zeta_{r_i^{e_i}}^{q})x + \zeta_{r_i^{e_i}}^{q+1}), & \text{if } e_i \le a_i; \\ \displaystyle\prod_{\zeta_{r_i^{e_i}} \in \Omega(r_i^{a_i})} (x^{2r_i^{e_i-a_i}} - (\zeta_{r_i^{a_i}} + \zeta_{r_i^{a_i}}^{q})x^{r_i^{e_i-a_i}} + \zeta_{r_i^{a_i}}^{q+1}). & \text{if } e_i > a_i, \end{cases}$$

Proof. When $e_i \le a_i$, $q \equiv -1 \pmod{r_i}$ implies $r_i \mid q^2 - 1$ because $a_i = v_r(q^2-1)$. Then, there exist a primitive $r_i{}^{e_i}th$ root in $\mathbb{F}_q^2$. Then, factorization of $\Phi_{r_i^{e_i}}(x)$ is given as

$$\begin{aligned}
\Phi_{r_i^{e_i}}(x) &= \prod_{\zeta_{r_i^{e_i}} \in \Omega(r_i^{e_i})} (x - \zeta_{r_i^{e_i}})(x - \zeta_{r_i^{e_i}}{}^{q}) \\
&= \prod_{\zeta_{r_i^{e_i}} \in \Omega(r_i^{e_i})} (x^2 - (\zeta_{r_i^{e_i}} + \zeta_{r_i^{e_i}}^{q})x + \zeta_{r_i^{e_i}}^{q+1}).
\end{aligned}$$

When $e_i > a_i$, by Theorem 2, the number of distinct irreducible factor of $\Phi_{{r_i}^{a_i}}$ is $\phi({r_i}^{a_i})/m$ where m is the least positive integer such that $q^m \equiv 1 \pmod{{r_i}^{a_i}}$. Here we have $m = 2$, and hence ${r_i}^{a_i+1} \nmid (q^2-1)$. In addition, each factor of $\Phi_{{r_i}^{a_i}}$ has order $e = r_i^{a_i}$ and $r_i \mid r_i^{a_i}$ but $r_i \nmid \frac{q^2-1}{{r_i}^{a_i}}$, then by Theorem 4, each irreducible factors $f(x)$ of $\Phi_{{r_i}^{a_i}}$ generates an irreducible factor $f(x^{r_i^{e_i-a_i}})$ for $\Phi_{{r_i}^{e_i}}$, which is of order ${r_i}^{e_i}$, and of degree $r_i^{e_i-a_i}$. Therefore, the factorization of $\Phi_{r_i^{a_i}}(x)$ is given as

$$\begin{aligned}\Phi_{r_i^{a_i}}(x) &= \prod_{\zeta_{r_i^{a_i}} \in \Omega(r_i^{a_i})} (x^{r_i^{e_i-a_i}} - \zeta_{r_i^{a_i}})(x^{r_i^{e_i-a_i}} - \zeta_{r_i^{a_i}}^q) \\ &= \prod_{\zeta_{r_i^{a_i}} \in \Omega(r_i^{a_i})} (x^{2{r_i}^{e_i-a_i}} - (\zeta_{r_i^{a_i}} + \zeta_{r_i^{a_i+1}}^q)x + \zeta_{{r_i}^{a_i+1}}^{q+1}).\end{aligned}$$

□

Notation 1. *For the rest of the thesis, we denote*

$$\prod_{i=1}^{s} {u_i}^{\prod_{\substack{j=1 \\ j\neq i}}^{s} B_j} = U_s, \quad \prod_{i=1}^{s} {u_i}^{q\prod_{\substack{j=1 \\ j\neq i}}^{s} B_j} = {U_s}^q,$$

$$\prod_{\substack{i=1 \\ i\notin\{i_1,\ldots,i_k\}}}^{s} {u_i}^{\prod_{\substack{j=1 \\ j\neq i}}^{s} B_j} \prod_{\substack{i=1 \\ i\in\{i_1,\ldots,i_k\}}}^{s} {u_i}^{q\prod_{\substack{j=1 \\ j\neq i}}^{s} B_j} = U_s(i_1,\ldots,i_k),$$

$$\prod_{\substack{i=1 \\ i\notin\{i_1,\ldots,i_k\}}}^{s} {u_i}^{q\prod_{\substack{j=1 \\ j\neq i}}^{s} B_j} \prod_{\substack{i=1 \\ i\in\{i_1,\ldots,i_k\}}}^{s} {u_i}^{\prod_{\substack{j=1 \\ j\neq i}}^{s} B_j} = {U_s}^q(i_1,\ldots,i_k).$$

where $i_1 \le i_2 \le \cdots \le i_k$ are some integers between 1 and s.

Theorem 16. *Let r_i be any distinct odd primes, $\mathbb{F}_q$ be a finite field such that $q \equiv -1 \pmod{r_i}$, and $a_i = v_{r_i}(q^2-1)$ where $1 \le i \le s$. Then, the irreducible factorization of $\Phi_{{r_1}^{e_1}} \odot \cdots \odot \Phi_{{r_s}^{e_s}}$ is given by*

$$
\begin{aligned}
&\Phi_{{r_1}^{e_1}}(x) \odot \cdots \odot \Phi_{{r_s}^{e_s}}(x) \\
= &\prod_{u_1} \cdots \prod_{u_s} \left(x^{2B_1} - (u_1 + {u_1}^q)x + {u_1}^{q+1} \right) \odot \cdots \odot \left(x^{2B_s} - (u_s + {u_s}^q)x + {u_s}^{(q+1)} \right) \\
= &\prod_{u_1} \cdots \prod_{u_s} \left(x^{2E_s} - \left(U_s + {U_s}^q\right)x^{E_s} + {U_s}^{(q+1)} \right) \\
&\left(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ 1 \le k < \frac{s}{2}}} x^{2E_s} - \left(U_s(i_1,\ldots,i_k) + U_s(i_1,\ldots,i_k)^q\right)x^{E_s} + U_s(i_1,\ldots,i_k)^{(q+1)} \right) \\
&\left(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ k = \frac{s}{2}, i_k = s}} x^{2E_s} - \left(U_s(i_1,\ldots,i_k) + U_s(i_1,\ldots,i_k)^q\right)x^{E_s} + U_s(i_1,\ldots,i_k)^{(q+1)} \right),
\end{aligned}
$$

where $E_s = \prod_{i=1}^{s} B_i$, *and*

$$
B_i = \begin{cases} 1, & \text{if } e_i \le a_i; \\ {r_i}^{e_i - a_i}, & \text{if } e_i > a_i. \end{cases}
$$

In addition, $u_i, {u_i}^q \in \Omega({r_i}^{e_i})$ *if* $e_i \le a_i$, *or* $u_i, {u_i}^q \in \Omega({r_i}^{a_i})$ *if* $e_i > a_i$.

Proof. We use mathematical induction to prove this result. Because $q \equiv -1 \pmod{r_i}$, by Theorem 15, we have

$$
\Phi_{{r_i}^{e_i}}(x) = \prod_{u_i} (x^{2B_i} - (u_i + {u_i}^q)x^{B_i} + {u_i}^{q+1}).
$$

First, we assume $s = 2$

$$
\begin{aligned}
&\Phi_{{r_1}^{e_1}}(x) \odot \Phi_{{r_2}^{e_2}}(x) \\
= &\prod_{u_1} \left(x^{2B_1} - \left(u_1 + {u_1}^q\right)x^{B_1} + {u_1}^{(q+1)} \right) \odot \prod_{u_2} \left(x^{2B_2} - \left(u_2 + {u_2}^q\right)x^{B_2} + {u_2}^{(q+1)} \right) \\
= &\prod_{u_1} \prod_{u_2} \left(x^{2B_1} - \left(u_1 + {u_1}^q\right)x^{B_1} + {u_1}^{(q+1)} \right) \odot \left(x^{2B_2} - \left(u_2 + {u_2}^q\right)x^{B_2} + {u_2}^{(q+1)} \right) \\
= &\prod_{u_1} \prod_{u_2} \left(x^{2B_1B_2} - \left({u_1}^{B_2}{u_2}^{B_1} + {u_1}^{qB_2}{u_2}^{qB_1}\right)x^{B_1B_2} + {u_1}^{(q+1)B_2}{u_2}^{(q+1)B_1} \right) \\
&\left(x^{2B_1B_2} - \left({u_1}^{qB_2}{u_2}^{B_1} + {u_1}^{B_2}{u_2}^{qB_1}\right)x^{B_1B_2} + {u_1}^{(q+1)B_2}{u_2}^{(q+1)B_1} \right)
\end{aligned}
$$

$$= \prod_{u_1}\prod_{u_2}\Big(x^{2B_1B_2} - \big(U_2 + {U_2}^q\big)x^{B_1B_2} + {U_2}^{(q+1)}\Big)$$
$$\Big(x^{2B_1B_2} - \big(U_2(i_1) + {U_2}^q(i_1)\big)x^{B_1B_2} + {U_2}^{(q+1)}\Big),$$

the second last equality is obtained by using Lemma 8. In the last equality, the two factors are irreducible over $\mathbb{F}_q$ since r_i are distinct odd primes and $gcd(2B_1, 2B_2) = 2$. Next, we assume the result is true for s

$$\begin{aligned}
&\Phi_{{r_1}^{e_1}}(x) \odot \cdots \odot \Phi_{{r_s}^{e_s}}(x) \\
= \;& \prod_{u_1}\cdots\prod_{u_s}\Big(x^{2E_s} - \big(U_s + {U_s}^q\big)x^{E_s} + {U_s}^{(q+1)}\Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\} \\ 1\le k<\frac{s}{2}}} x^{2E_s} - \big(U_s(i_1,\ldots,i_k) + U_s(i_1,\ldots,i_k)^q\big)x^{E_s} + U_s(i_1,\ldots,i_k)^{(q+1)}\Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\} \\ k=\frac{s}{2}, i_k=s}} x^{2E_s} - \big(U_s(i_1,\ldots,i_k) + U_s(i_1,\ldots,i_k)^q\big)x^{E_s} + U_s(i_1,\ldots,i_k)^{(q+1)}\Big),
\end{aligned}$$

Now, we will prove the result for $s+1$

$$\begin{aligned}
&\Big(\Phi_{{r_1}^{e_1}}(x) \odot \cdots \odot \Phi_{{r_s}^{e_s}}(x)\Big) \odot \Big(\Phi_{{r_{s+1}}^{e_{s+1}}}(x)\Big) \\
= \;& \prod_{u_1\cdots u_s}\prod_{u_{s+1}}\Big(\Phi_{{r_1}^{e_1}} \odot \cdots \odot \Phi_{{r_s}^{e_s}}\Big) \odot \Big(x^{2B_{s+1}} - \big(u_{s+1} + {u_{s+1}}^q\big)x^{B_{s+1}} + {u_{s+1}}^{q+1}\Big).
\end{aligned}$$

By using our assumpition for s, we need to do composed product for each factor of $(\Phi_{{r_1}^{e_1}}(x) \odot \cdots \odot \Phi_{{r_s}^{e_s}}(x))$ separately with each factor of $\Phi_{{r_{s+1}}^{e_{s+1}}}(x)$.

$$\prod_{u_1,\ldots,u_s}\Big(x^{2E_s} - \big(U_s + {U_s}^q\big)x^{E_s} + {U_s}^{q+1}\Big) \odot$$
$$\prod_{u_{s+1}}\Big(x^{2B_{s+1}} - \big(u_{s+1} + {u_{s+1}}^q\big)x^{B_{s+1}} + {u_{s+1}}^{q+1}\Big)$$

$$
\begin{aligned}
&= \prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}\Big(x^{2E_s}-\big(U_s+{U_s}^q\big)x^{E_s}+{U_s}^{q+1}\Big)\odot\\
&\quad\Big(x^{2B_{s+1}}-\big(u_{s+1}+{u_{s+1}}^q\big)x^{B_{s+1}}+{u_{s+1}}^{q+1}\Big)\\
&= \prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}\Big(x^{2E_sB_{s+1}}-\Big(\big(U_s\big)^{B_{s+1}}\big(u_{s+1}\big)^{E_s}+\big({U_s}^q\big)^{B_{s+1}}\big(u_{s+1}\big)^{qE_s}\Big)\\
&\quad x^{E_sB_{s+1}}+\big({U_s}^{q+1}\big)^{B_{s+1}}\big(u_{s+1}\big)^{(q+1)E_s}\Big)\\
&\quad\Big(x^{2E_sB_{s+1}}-\Big(\big(U_s\big)^{B_{s+1}}\big(u_{s+1}\big)^{qE_s}+\big({U_s}^q\big)^{B_{s+1}}\big(u_{s+1}\big)^{E_s}\Big)\\
&\quad x^{E_sB_{s+1}}+\Big(\big({U_s}^{(q+1)}\big)^{B_{s+1}}\big(u_{s+1}\big)^{(q+1)E_s}\Big)\\
&= \prod_{u_1,\ldots,u_s,u_{s+1}}\Big(x^{2E_{s+1}}-\big(U_{s+1}+{U_{s+1}}^q\big)x^{E_{s+1}}+{U_{s+1}}^{(q+1)}\Big)\\
&\quad\Big(x^{2E_{s+1}}-\big(U_{s+1}(s+1)+{U_{s+1}}^q(s+1)\big)x^{E_{s+1}}+{U_{s+1}}^{(q+1)}\Big),
\end{aligned}
$$

the third equality is obtained by using Lemma 8. In the last equality the two factors are irreducible over $\mathbb{F}_q$ since r_i are distinct odd primes and $gcd(2E_s, 2B_{s+1}) = 2$. Suppose s is odd, we have

$$
\begin{aligned}
&\prod_{u_1,\ldots,u_s}\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s\}\\1\le k<\frac{s}{2}}}x^{2E_s}-\Big(U_s(i_1,\ldots,i_k)+{U_s}^q(i_1,\ldots,i_k)\Big)x^{E_s}+\\
&\quad\big(U_s(i_1,\ldots,i_k)\big)^{(q+1)}\Big)\odot\prod_{u_{s+1}}\Big(x^{2B_{s+1}}-(u_{s+1}+{u_{s+1}}^q)x^{B_{s+1}}+{u_{s+1}}^{q+1}\Big)\\
=&\prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots s\}\\1\le k<\frac{s}{2}}}x^{2E_s}-\Big(U_s(i_1,\ldots,i_k)+{U_s}^q(i_1,\ldots,i_k)\Big)x^{E_s}+\\
&\quad\big(U_s(i_1,\ldots,i_k)\big)^{(q+1)}\Big)\odot\Big(x^{2B_{s+1}}-(u_{s+1}+{u_{s+1}}^q)x^{B_{s+1}}+{u_{s+1}}^{q+1}\Big)\\
=&\prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s\}\\1\le k<\frac{s}{2}}}\Big(x^{2E_sB_{s+1}}-\Big(\big(U_s(i_1,\ldots,i_k)\big)^{B_{s+1}}\big(u_{s+1}\big)^{E_s}+\\
&\quad\big(U_s(i_1,\ldots,i_k)\big)^{qB_{s+1}}\big(U_{s+1}\big)^{qE_s}\Big)x^{E_sB_{s+1}}+\Big(U_s(i_1,\ldots,i_k)\Big)^{(q+1)Bs+1}\Big(u_{s+1}\Big)^{(q+1)E_s}\Big)\\
&\quad\Big(x^{2E_sB_{s+1}}-\Big(\big(U_s(i_1,\ldots,i_k)\big)^{B_{s+1}}\big(u_{s+1}\big)^{qE_s}+\big(U_s(i_1,\ldots,i_k)\big)^{qB_{s+1}}\\
&\quad\big(U_{s+1}\big)^{E_s}\big)x^{E_sB_{s+1}}+\big(U_s(i_1,\ldots,i_k)\big)^{(q+1)Bs+1}\big(u_{s+1}\big)^{(q+1)E_s}\Big).
\end{aligned}
$$

$$= \prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s\}\\ 1\le k<\frac{s}{2}}}\Big(x^{2E_{s+1}}-\big(U_{s+1}(i_1,\ldots,i_k)+{U_{s+1}}^q(i_1,\ldots,i_k)\big)$$
$$x^{E_{s+1}}+{U_{s+1}}^{(q+1)}(i_1,\ldots,i_k)\Big)$$
$$\Big(x^{2E_{s+1}}-\Big(U_{s+1}(i_1,\ldots,i_k,s+1)+{U_{s+1}}^q(i_1,\ldots,i_k,s+1)\Big)x^{E_s}+$$
$${U_{s+1}}^{(q+1)}(i_1,\ldots,i_k,s+1)\Big).$$

the third equality is obtained by using Lemma 8. In the last equality the two factors are irreducible over $\mathbb{F}_q$ since $gcd(2E_s, 2B_{s+1}) = 2$ and r_i are distinct odd primes.

Hence

$$(\Phi_{{r_1}^{e_1}}(x)\odot\cdots\odot\Phi_{{r_s}^{e_s}}(x))\odot(\Phi_{{r_{s+1}}^{e_{s+1}}}(x))$$
$$= \prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}(\Phi_{{r_1}^{e_1}}(x)\odot\cdots\odot\Phi_{{r_s}^{e_s}}(x))\odot(x^{2B_{s+1}}-\big(u_{s+1}+{u_{s+1}}^q\big)x^{B_{s+1}}+{u_{s+1}}^{q+1})$$
$$= \prod_{u_1,\ldots,u_s,u_{s+1}}\Big(x^{2E_{s+1}}-\big(U_{s+1}+{U_{s+1}}^q\big)x^{E_{s+1}}+{U_{s+1}}^{(q+1)}\Big)$$
$$\Big(x^{2E_{s+1}}-\big(U_{s+1}(s+1)+{U_{s+1}}^q(s+1)\big)x^{E_{s+1}}+{U_{s+1}}^{(q+1)}\Big)$$
$$\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s\}\\ 1\le k<\frac{s}{2}}}\Big(x^{2E_{s+1}}-\big(\big(U_{s+1}(i_1,\ldots,i_k)+{U_{s+1}}^q(i_1,\ldots,i_k)\big)x^{E_{s+1}}+$$
$${U_{s+1}}^{q+1}(i_1,\ldots,i_k)\Big)\Big)$$
$$\Big(x^{2E_{s+1}}-\big(\big(U_{s+1}(i_1,\ldots,i_k,s+1)+{U_{s+1}}^q(i_1,\ldots,i_k,s+1)\Big)x^{E_{s+1}}+$$
$${U_{s+1}}^{(q+1)}(i_1,\ldots,i_k,s+1)\Big)\Big)$$
$$= \prod_{u_1,\ldots,u_s,u_{s+1}}\Big(x^{2E_{s+1}}-\big(U_{s+1}+{U_{s+1}}^q\big)x^{E_{s+1}}+{U_{s+1}}^{(q+1)}\Big)$$
$$\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s+1\}\\ 1\le k<\frac{s+1}{2}}}\Big(x^{2E_{s+1}}-\big(U_{s+1}(i_1,\ldots,i_k)+{U_{s+1}}^q(i_1,\ldots,i_k)\big)x^{E_{s+1}}$$
$$+\big(U_{s+1}(i_1,\ldots,i_k)\big)^{(q+1)}\Big)$$
$$\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s+1\}\\ k=\frac{s+1}{2}}}\Big(x^{2E_{s+1}}-\big(U_{s+1}(i_1,\ldots,i_k)+{U_{s+1}}^q(i_1,\ldots,i_k)\big)x^{E_{s+1}}$$
$$+\big(U_{s+1}(i_1,\ldots,i_k)\big)^{(q+1)}\Big)$$

By mathematical induction, we complete the proof for odd s.

Now, suppose s is even, we have

$$\begin{aligned}
&\prod_{u_1,\ldots,u_s}\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s\}\\ k=\frac{s}{2},i_k=s}} x^{2E_s}-\big(U_s(i_1,\ldots,i_k)+{U_s}^q(i_1,\ldots,i_k)\big)x^{E_s}\\
&+{U_s}^{q+1}(i_1,\ldots,i_k)\Big)\odot\prod_{u_{s+1}}\Big(x^{2B_{s+1}}-(u_{s+1}+{u_{s+1}}^q)x^{B_{s+1}}+{u_{s+1}}^{q+1}\Big)\\
=&\prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s\}\\ k=\frac{s}{2},i_k=s}} x^{2E_s}-\big(U_s(i_1,\ldots,i_k)+{U_s}^q(i_1,\ldots,i_k)\big)x^{E_s}\\
&\big(U_s(i_1,\ldots,i_k)\big)^{(q+1)}\Big)\odot\Big(x^{2B_{s+1}}-(u_{s+1}+{u_{s+1}}^q)x^{B_{s+1}}+{u_{s+1}}^{q+1}\Big)\\
=&\prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}\prod_{\substack{\{i_1,\ldots i_k\}\subset\{1,2,\ldots,s\}\\ k=\frac{s}{2},i_k=s}}\Big(x^{E_sB_{s+1}}-\Big(\big(U_s(i_1,\ldots,i_k)\big)^{B_{s+1}}\big(u_{s+1}\big)^{E_s}\\
&+\big(U_s(i_1,\ldots,i_k)\big)^{qB_{s+1}}\big(U_{s+1}\big)^{qE_s}\Big)x^{E_sB_{s+1}}+\Big(U_s(i_1,\ldots,i_k)\Big)^{(q+1)Bs+1}\Big(u_{s+1}\Big)^{(q+1)E_s}\Big)\\
&\Big(x^{2E_sB_{s+1}}-\Big(\big(U_s(i_1,\ldots,i_k)\big)^{B_{s+1}}\big(u_{s+1}\big)^{qE_s}+\big(U_s(i_1,\ldots,i_k)\big)^{qB_{s+1}}\big(u_{s+1}\big)^{E_s}\big)\\
&x^{E_sB_{s+1}}+\big(U_s(i_1,\ldots,i_k)\big)^{(q+1)Bs+1}\big(u_{s+1}\big)^{(q+1)E_s}\Big).\\
=&\prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s\}\\ k=\frac{s}{2},i_k=s}}\Big(x^{2E_{s+1}}-\Big(U_{s+1}(i_1,\ldots,i_k)+{U_{s+1}}^q(i_1,\ldots,i_k)\Big)x^{E_{s+1}}+\\
&{U_{s+1}}^{(q+1)}(i_1,\ldots,i_k)\Big)\Big(x^{2E_{s+1}}-\Big(U_{s+1}(i_1,\ldots,i_k,s+1)+{U_{s+1}}^q(i_1,\ldots,i_k,s+1)\Big)\\
&x^{E_{s+1}}+{U_{s+1}}^{(q+1)}(i_1,\ldots,i_k,s+1)\Big).\\
=&\prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots s\}\\ k=\frac{s}{2},i_k=s}}\Big(x^{2E_{s+1}}-\Big(U_{s+1}(i_1,\ldots,i_k)+{U_{s+1}}^q(i_1,\ldots,i_k)\Big)x^{E_{s+1}}+\\
&{U_{s+1}}^{(q+1)}(i_1,\ldots,i_k)\Big)\Big(x^{2E_{s+1}}-\Big({U_{s+1}}^q(j_1,\ldots,j_{s/2})+U_{s+1}(j_1,\ldots,j_{s/2})\Big)x^{E_{s+1}}+\\
&\Big({U_{s+1}}^{(q+1)}(j_1,\ldots,i_{s/2})\Big),
\end{aligned}$$

where $\{i_1,\ldots,i_{s/2-1},s\}\ \cup\ \{j_1,\ldots,j_{s/2}\}=\{1,\ldots,s\}$.

Therefore, the third equality is obtained by using Lemma 8. In the last two equality the two factors are irreducible over $\mathbb{F}_q$ since $gcd(2B_1\cdots B_s,2B_{s+1})=2$ and r_i are distinct odd primes.

Hence

$$
\begin{aligned}
&(\Phi_{r_1{}^{e_1}}(x)\odot\cdots\odot\Phi_{r_s{}^{e_s}}(x))\odot(\Phi_{r_{s+1}{}^{e_{s+1}}}(x))\\
=&\prod_{u_1,\ldots,u_s}\prod_{u_{s+1}}(\Phi_{r_1{}^{e_1}}(x)\odot\cdots\odot\Phi_{r_s{}^{e_s}}(x))\odot(x^{2B_{s+1}}-\big(u_{s+1}+{u_{s+1}}^q\big)x^{B_{s+1}}+{u_{s+1}}^{q+1})\\
=&\prod_{u_1,\ldots,u_s,u_{s+1}}\Big(x^{2E_{s+1}}-\big(U_{s+1}+{U_{s+1}}^q\big)x^{E_{s+1}}+{U_{s+1}}^{(q+1)}\Big)\\
&\Big(x^{2E_{s+1}}-\big(U_{s+1}(s+1)+{U_{s+1}}^q(s+1)\big)x^{E_{s+1}}+{U_{s+1}}^{(q+1)}\Big)\\
&\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s\}\\1\le k<\frac{s}{2}}}\Big(x^{2E_{s+1}}-\big(U_{s+1}(i_1,\ldots,i_k)+{U_{s+1}}^q(i_1,\ldots,i_k)\big)x^{E_{s+1}}+\\
&{U_{s+1}}^{q+1}(i_1,\ldots,i_k)\Big)\\
&\Big(x^{2E_{s+1}}-\big(U_{s+1}(i_1,\ldots,i_k,s+1)+{U_{s+1}}^q(i_1,\ldots,i_k,s+1)\big)x^{E_s}+\\
&{U_{s+1}}^{q+1}(i_1,\ldots,i_k,s+1)\Big)\\
&\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s\}\\k=\frac{s}{2},i_k=s}}\Big(x^{2E_{s+1}}-\big(U_{s+1}(i_1,\ldots,i_k)+{U_{s+1}}^q(i_1,\ldots,i_k)\big)x^{E_{s+1}}+\\
&{U_{s+1}}^{(q+1)}(i_1,\ldots,i_k)\Big)\\
&\Big(x^{2E_{s+1}}-\big({U_{s+1}}^q(j_1,\ldots,j_k)+U_{s+1}(j_1,\ldots,j_{s/2})\big)x^{E_{s+1}}+{U_{s+1}}^{(q+1)}(j_1,\ldots,i_k)\Big)\\
=&\prod_{u_1,\ldots,u_s,u_{s+1}}\Big(x^{2E_{s+1}}-\big(U_{s+1}+{U_{s+1}}^q\big)x^{E_{s+1}}+{U_{s+1}}^{(q+1)}\Big)\\
&\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,2,\ldots,s+1\}\\1\le k<\frac{s+1}{2}}}x^{2E_{s+1}}-\big(U_{s+1}(i_1,\ldots,i_k)+{U_{s+1}}^q(i_1,\ldots,i_k)\big)x^{E_{s+1}}+\\
&\big(U_{s+1}(i_1,\ldots,i_k)\big)^{(q+1)}\Big).
\end{aligned}
$$

By mathematical induction, we complete the proof for even s.

Therefore, we have proved that

$$
\begin{aligned}
& \Phi_{r_1{}^{e_1}}(x) \odot \cdots \odot \Phi_{r_s{}^{e_s}}(x) \\
= \; & \prod_{u_1} \cdots \prod_{u_s} \Big(x^{2B_1} - (u_1 + {u_1}^q)x + {u_1}^{q+1} \Big) \odot \cdots \odot \Big(x^{2B_s} - (u_s + {u_s}^q)x + {u_s}^{(q+1)} \Big) \\
= \; & \prod_{u_1} \cdots \prod_{u_s} \Big(x^{2E_s} - \big(U_s + {U_s}^q\big)x^{E_s} + {U_s}^{(q+1)} \Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ 1 \le k < \frac{s}{2}}} x^{2E_s} - \big(U_s(i_1,\ldots,i_k) + {U_s}^q(i_1,\ldots,i_k)\big)x^{E_s} + U_s(i_1,\ldots,i_k)^{(q+1)} \Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ k = \frac{s}{2}, i_k = s}} x^{2E_s} - \big(U_s(i_1,\ldots,i_k) + {U_s}^q(i_1,\ldots,i_k)\big)x^{E_s} + U_s(i_1,\ldots i_k)^{(q+1)} \Big),
\end{aligned}
$$

□

4.3 Factorization of $\Phi_{r_0^{e_0}} \odot \Phi_{r_1^{e_1}} \odot \cdots \odot \Phi_{r_{t+s}^{e_{t+s}}}$ when $q \equiv \pm 1 \pmod{r_i}$

In this subsection, we consider three cases: 1) when q is odd (i.e., $q \equiv \pm 1 \pmod{r_i}$, r_i's are odd, where $1 \le i \le t+s$); 2) $q \equiv 1 \pmod 4$; 3) $q \equiv 3 \pmod 4$. In the last two cases, the prime number $r_0 = 2$ must appear in the factorization of n.

Theorem 17. *Without loss of generality, assume that $q \equiv 1 \pmod{r_i}$ with $1 \le i \le t$ and $q \equiv -1 \pmod{r_i}$ with $t+1 \le i \le t+s$, where r_i are odd primes for $1 \le i \le t+s$. Then, the irreducible factorization of $\Phi_{r_1^{e_1} \cdots r_{t+s}^{e_{t+s}}}$ over $\mathbb{F}_q$ is*

$$
\begin{aligned}
&\Phi_{r_1^{e_1}}(x) \odot \cdots \odot \Phi_{r_{t+s}^{e_{t+s}}}(x) \\
= \; & \prod_{c_1} \cdots \prod_{c_t} \prod_{u_1} \cdots \prod_{u_s} \Bigg(x^{2E_sF_t} - \Big((U_s)^{F_t} + (U_s{}^q)^{F_t} \Big) \Big(\prod_{i=1}^{t} {c_i}^{F_t/c_i} \Big)^{E_s} x^{E_sF_t} + \\
& \Big({U_s}^{(q+1)} \Big)^{F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2E_s} \Bigg) \\
& \Bigg(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ 1 \le k < \frac{s}{2}}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k)\big)^{F_t} + \big(U_s{}^q(i_1,\ldots,i_k)\big)^{F_t} \Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k) \Big)^{F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2E_s} \Bigg) \\
& \Bigg(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ k = \frac{s}{2}, i_k = s}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k)\big)^{F_t} + \big(U_s{}^q(i_1,\ldots,i_k)\big)^{F_t} \Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k) \Big)^{F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2E_s} \Bigg),
\end{aligned}
$$

where $F_t = A_1A_2\cdots A_t$, $E_s = B_1B_2\cdots B_s$, and for $1 \le i \le t$ and $1 \le j \le s$,

$$
A_i = \begin{cases} 1, & \text{if } e_i \le a_i; \\ r_i^{e_i - a_i}, & \text{if } e_i > a_i, \end{cases} \qquad B_j = \begin{cases} 1, & \text{if } e_{t+j} \le a_{t+j}; \\ {r_{t+j}}^{e_{t+j} - a_{t+j}}, & \text{if } e_{t+j} > a_{t+j}. \end{cases}
$$

In addition,

$$c_i \in \begin{cases} \Omega({r_i}^{e_i}), & \text{if } e_i \le a_i; \\ \Omega({r_i}^{a_i}), & \text{if } e_i > a_i, \end{cases} \quad u_j \in \begin{cases} \Omega({r_{t+j}}^{e_{t+j}}), & \text{if } e_{t+j} \le a_{t+j}; \\ \Omega({r_{t+j}}^{a_{t+j}}), & \text{if } e_{t+j} > a_{t+j}, \end{cases}$$

Moreover, the number of irreducible factors of $\Phi_{{r_1}^{e_1}\cdots{r_{t+s}}^{e_{t+s}}}$ *in* $\mathbb{F}_q[x]$ *is*

$$\prod_{i=1}^{t} \phi({r_i}^{f_i}) \prod_{i=t+1}^{t+s} \frac{\phi({r_i}^{f_i})}{2} \cdot 2^{s-1},$$

where for $1 \le i \le t+s$,

$$f_i = \begin{cases} e_i, & \text{if } e_i \le a_i; \\ a_i, & \text{otherwise.} \end{cases}$$

Proof. First, since $q \equiv 1 \pmod{r_i}$ with $1 \le i \le t$, then by Theorem 14, we have the factorization of $\Phi_{r_1^{e_1}\cdots r_t^{e_t}}$ as

$$\Phi_{r_1^{e_1}\cdots r_t^{e_t}} = \prod_{c_1} \cdots \prod_{c_t} \Big(x^{F_t} - \prod_{i-1}^{t} {c_i}^{F_t/a_i} \Big), \text{where } F_t = A_1 \cdots A_t.$$

Second, since $q \equiv -1 \pmod{r_i}$ with $t+1 \le i \le s$, then by Theorem 16, we have the factorization of $\Phi_{r_{t+1}^{e_{t+1}}\cdots r_{t+s}^{e_{t+s}}}$ as

$$\begin{aligned}
& \Phi_{{r_{t+1}}^{e_{t+1}}}(x) \odot \cdots \odot \Phi_{{r_{t+s}}^{e_{t+s}}}(x) \\
= \; & \prod_{u_1} \cdots \prod_{u_s} \Big(x^{2B_1} - (u_1 + {u_1}^q)x + {u_1}^{q+1} \Big) \odot \cdots \odot \Big(x^{2B_s} - (u_s + {u_s}^q)x + {u_s}^{(q+1)} \Big) \\
= \; & \prod_{u_1} \cdots \prod_{u_s} \Big(x^{2E_s} - \Big(U_s + {U_s}^q \Big) x^{E_s} + {U_s}^{(q+1)} \Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ 1 \le k < \frac{s}{2}}} x^{2E_s} - \Big(U_s(i_1,\ldots,i_k) + U_s(i_1,\ldots,i_k)^q \Big) x^{E_s} + U_s(i_1,\ldots,i_k)^{(q+1)} \Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ k = \frac{s}{2}, i_k = s}} x^{2E_s} - \Big(U_s(i_1,\ldots,i_k) + U_s(i_1,\ldots,i_k)^q \Big) x^{E_s} + \\
& U_s(i_1,\ldots,i_k)^{(q+1)} \Big). \qquad (1)
\end{aligned}$$

Finally, by Lemma 5, we get the factorization of $\Phi_{r_1^{e_1}\dots r_{t+s}^{e_{t+s}}}$ when $q \equiv \pm 1 \ (mod\ r_i)$ by applying the composed product as

$$
\begin{aligned}
&\Phi_{r_1^{e_1}\dots r_t^{e_t}}(x) \odot \Phi_{r_{t+1}^{e_{t+1}}\dots r_{t+s}^{e_{t+s}}}(x) \\
= \ & \prod_{c_1}\cdots\prod_{c_t}\prod_{u_1}\cdots\prod_{u_s}\left(x^{F_t} - \prod_{i-1}^{t} {c_i}^{F_t/a_i}\right) \odot \left[\left(x^{2E_s} - \Big(U_s + {U_s}^q\Big)x^{E_s} + {U_s}^{(q+1)}\right)\right. \\
& \left(\prod_{\substack{\{i_1,\dots,i_k\}\subset\{1,\dots,s\} \\ 1\le k<\frac{s}{2}}} x^{2E_s} - \Big(U_s(i_1,\dots,i_k) + U_s(i_1,\dots,i_k)^q\Big)x^{E_s} + U_s(i_1,\dots,i_k)^{(q+1)}\right) \\
& \left.\left(\prod_{\substack{\{i_1,\dots,i_k\}\subset\{1,\dots,s\} \\ k=\frac{s}{2}, i_k=s}} x^{2E_s} - \Big(U_s(i_1,\dots,i_t) + U_s(i_1,\dots,i_k)^q\Big)x^{E_s} + U_s(i_1,\dots,i_k)^{(q+1)}\right)\right] \\
= \ & \prod_{c_1}\cdots\prod_{c_t}\prod_{u_{t+1}}\cdots\prod_{u_{t+s}}\left(x^{2E_sF_t} - \Big((U_s)^{F_t} + ({U_s}^q)^{F_t}\Big)\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{E_s} x^{E_sF_t} + \Big({U_s}^{(q+1)}\Big)^{F_t}\right. \\
& \left.\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2E_s}\right) \\
& \left(\prod_{\substack{\{i_1,\dots,i_k\}\subset\{1,\dots,s\} \\ 1\le k<\frac{s}{2}}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\dots,i_k)\big)^{F_t} + \big({U_s}^q(i_1,\dots,i_k)\big)^{F_t}\Big)\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{E_s}\right. \\
& \left. x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\dots,i_k)\Big)^{F_t}\Big(\prod_{i=1}^{t} {a_i}^{F_t/a_i}\Big)^{2E_s}\right) \\
& \left(\prod_{\substack{\{i_1,\dots,i_k\}\subset\{1,\dots,s\} \\ k=\frac{s}{2}, i_k=s}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\dots,i_k)\big)^{F_t} + \big({U_s}^q(i_1,\dots,i_k)\big)^{F_t}\Big)\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{E_s}\right. \\
& \left. x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\dots,i_k)\Big)^{F_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2E_s}\right).
\end{aligned}
$$

Since $(q,n)=1$, then we know by Theorem 2 that Φ_n can be factorized into ϕ_n/d distinct monic irreducible polynomial of the same degree d over $\mathbb{F}_q$, where d is the least positive integer such that $q^d \equiv 1 \pmod{n}$. Therefore, the number of irreducible polynomials $(x^{A_i} - c_i)$ is $\phi({r_i}^{e_i})$ when $e_i \le a_i$ and is $\phi({r_i}^{a_i})$ when $e_i > a_i$. In addition, since we have $gcd(A_1, A_2) = gcd(A_1A_2, A_3) = \cdots = gcd(A_1A_2\dots A_{t-1}, A_t) = 1$, and since $\Phi_{{r_1}^{e_1}\dots{r_t}^{e_t}} = \prod_{c_1}\cdots\prod_{c_t}(x^{A_1} - c_1) \odot \cdots \odot (x^{A_t} - c_t)$, then each of composed product

is an irreducible polynomial, and the number of factors is $\prod_{i=1}^{t}\phi({r_i}^{e_i})$ when $e_i \le a_i$ and is $\prod_{i=1}^{t}\phi({r_i}^{a_i})$ when $e_i > a_i$. Moreover, the number of irreducible polynomials $\left(x^{2B_i}-(u_i+{u_i}^q)x^{B_i}+{u_i}^{q+1}\right)$ is $\frac{\phi({r_i}^{e_i})}{2}$ when $e_i \le a_i$ and is $\frac{\phi({r_i}^{a_i})}{2}$ when $e_i > a_i$. Since $\Phi_{{r_1}^{e_1}\cdots{r_s}^{e_s}} = \prod_{u_1}\cdots\prod_{u_s}\left(x^{2B_1}-(u_1+{u_1}^q)x+{u_1}^{q+1}\right)\odot\cdots\odot\left(x^{2B_s}-(u_s+{u_s}^q)x+{u_s}^{(q+1)}\right)$, then the number of $\left(x^{2B_1}-(u_1+{u_1}^q)x+{u_1}^{q+1}\right)\odot\cdots\odot\left(x^{2B_s}-(u_s+{u_s}^q)x+{u_s}^{(q+1)}\right)$ is $\prod_{i=t+1}^{s}\frac{\phi({r_i}^{e_i})}{2}$ when $e_i \le a_i$, and the number is $\prod_{i=t+1}^{s}\frac{\phi({r_i}^{e_i})}{2}$ when $e_i > a_i$. In addition, since we have $gcd(B_1, B_2) = gcd(B_1B_2, B_3) = \cdots = gcd(B_1B_2\cdots B_{s-1}, B_s) = 2$, and from Equation (1), the number of irreducible factors for each $\left(x^{2B_1}-(u_1+{u_1}^q)x+{u_1}^{q+1}\right)\odot\cdots\odot\left(x^{2B_s}-(u_s+{u_s}^q)x+{u_s}^{(q+1)}\right)$ is 2^{s-1}. Therefore the number of irreducible factors of $\left(x^{2B_1}-(u_1+{u_1}^q)x+{u_1}^{q+1}\right)\odot\cdots\odot\left(x^{2B_s}-(u_s+{u_s}^q)x+{u_s}^{(q+1)}\right)$ is $\prod_{i=t+1}^{s}\frac{\phi({r_i}^{e_i})}{2}2^{s-1}$ when $e_i \le a_i$, and that number is $\prod_{i=t+1}^{s}\frac{\phi({r_i}^{e_i})}{2}2^{s-1}$ when $e_i > a_i$.

Because all r_i's are odd, the number of irreducible factors for each $\left(x^{2B_1}-(u_1+{u_1}^q)x+{u_1}^{q+1}\right)\odot\cdots\odot\left(x^{2B_s}-(u_s+{u_s}^q)x+{u_s}^{(q+1)}\right)$ gives the same number of irreducible factors of $(x^{A_1}-c_1)\odot\cdots\odot(x^{A_t}-c_t)\odot\left(x^{2B_1}-(u_1+{u_1}^q)x+{u_1}^{q+1}\right)\odot\cdots\odot\left(x^{2B_s}-(u_s+{u_s}^q)x+{u_s}^{(q+1)}\right)$. Hence the proof is complete. □

Theorem 18. *Without loss of generality, assume that* $q \equiv 1 \pmod 4$, *and let* $r_0 = 2$, $q \equiv 1 \pmod{r_i}$ *with* $1 \le i \le t$, *and* $q \equiv -1 \pmod{r_i}$ *with* $t+1 \le i \le t+s$, *where* r_i *are odd for* $1 \le i \le t+s$. *Then, the irreducible factorization of* $\Phi_{{r_0}^{e_0}}\odot\cdots\odot\Phi_{{r_{t+s}}^{e_{t+s}}}$ *when* $e_i \le a_i$ *is*

$$
\begin{aligned}
&\Phi_{{r_0}^{e_0}}(x)\odot\cdots\odot\Phi_{{r_{t+s}}^{e_{t+s}}}(x)\\
=\;&\prod_{c_0}\prod_{c_1}\cdots\prod_{c_t}\prod_{u_1}\cdots\prod_{u_s}\left(x^{2E_sF_t}-\left((U_s)^{F_t}+(U_s)^{qF_t}\right)\left(c_0\right)^{E_sF_t}\right.\\
&\left.\left(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\right)^{E_s}x^{E_sF_t}+\left({U_s}^{(q+1)}\right)^{F_t}\left(c_0\right)^{2E_sF_t}\left(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\right)^{2E_s}\right)\\
&\left(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\1\le k<\frac{s}{2}}}x^{2E_sF_t}-\left({U_s}^{F_t}(i_1,\ldots,i_k)+{U_s}^{qF_t}(i_1,\ldots,i_k)\right)\left(c_0\right)^{E_sF_t}\right.
\end{aligned}
$$

$$\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_s}x^{E_sF_t}+\Big({U_s}^{(q+1)F_t}(i_1,\dots,i_k)\Big)\Big(c_0\Big)^{2E_sF_t}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_s}\Big)$$
$$\Big(\prod_{\substack{\{i_1,\dots,i_k\}\subset\{1,\dots,s\}\\ k=\frac{s}{2},i_k=s}}x^{2E_sF_t}-\Big({U_s}^{F_t}(i_1,\dots,i_k)+{U_s}^{qF_t}(i_1,\dots,i_k)\Big)\Big(c_0\Big)^{E_sF_t}$$
$$\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_s}x^{E_sF_t}+\Big({U_s}^{(q+1)F_t}(i_1,\dots,i_k)\Big)\Big(c_0\Big)^{2E_sF_t}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_s}\Big).$$

When $e_i > a_i$, the irreducible factorization of $\Phi_{r_0^{e_0}}\odot\cdots\odot\Phi_{r_{t+s}^{e_{t+s}}}$ is

$$\begin{aligned}
&\Phi_{r_0^{e_0}}(x)\odot\cdots\odot\Phi_{r_{t+s}^{e_{t+s}}}(x)\\
=\;&\prod_{c_0}\prod_{c_1}\cdots\prod_{c_t}\prod_{u_1}\cdots\prod_{u_s}\Big(x^{2E_sF_tA_0}-\Big((U_s)^{F_tA_0}(c_0)^{E_sF_t}+(U_s{}^q)^{F_tA_0}(c_0)^{qE_sF_t}\Big)\\
&\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}x^{E_sF_tA_0}+\Big(U_s{}^{(q+1)}\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big)\\
&\Big(x^{2E_sF_tA_0}-\Big((U_s)^{qF_tA_0}(c_0)^{E_sF_t}+(U_s)^{F_tA_0}(c_0)^{qE_sF_t}\Big)\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}\\
&x^{E_sF_tA_0}+\Big(U_s{}^{(q+1)}\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big)\\
&\Big(\prod_{\substack{\{i_1,\dots,i_k\}\subset\{1,\dots,s\}\\ 1\le k<\frac{s}{2}}}x^{2E_sF_tA_0}-\Big(\big(U_s(i_1,\dots,i_k)\big)^{F_tA_0}(c_0)^{E_sF_t}+\big(U_s{}^q(i_1,\dots,i_k)\big)^{F_tA_0}(c_0)^{qE_sF_t}\Big)\\
&\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}x^{E_sF_tA_0}+\Big(U_s{}^{(q+1)}(i_1,\dots,i_k)\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big)\\
&\Big(x^{2E_sF_tA_0}-\Big(\big(U_s(i_1,\dots,i_k)\big)^{qF_tA_0}(c_0)^{E_sF_t}+\big(U_s(i_1,\dots,i_k)\big)^{F_tA_0}(c_0)^{qE_sF_t}\Big)\\
&\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}x^{E_sF_tA_0}+\Big(U_s{}^{(q+1)}(i_1,...,i_k)\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big)\\
&\Big(\prod_{\substack{\{i_1,\dots,i_k\}\subset\{1,\dots,s\}\\ k=\frac{s}{2},i_k=s}}x^{2E_sF_tA_0}-\Big(\big(U_s(i_1,\dots,i_k)\big)^{F_tA_0}(c_0)^{E_sF_t}+\big(U_s{}^q(i_1,\dots,i_k)\big)^{F_tA_0}(c_0)^{qE_sF_t}\Big)\\
&\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}x^{E_sF_tA_0}+\Big(U_s{}^{(q+1)}(i_1,\dots,i_k)\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big),
\end{aligned}$$

where $A_0 = 2^{e_0-a_0}$, c_0 is the set of all primitive A_0th roots of unity, and all the other

notations can be found in Theorem 17.

Moreover, the number of irreducible factors of $\Phi_{{r_0}^{e_0}r_1{}^{e_1}\dots r_{t+s}{}^{e_{t+s}}}$ *in* $\mathbb{F}_q[x]$ *when* $e_0 \le a_0$ *is*

$$\phi({r_0}^{e_0}) \cdot \prod_{i=1}^{t} \phi({r_i}^{f_i}) \cdot \prod_{i=t+1}^{t+s} \frac{\phi({r_i}^{f_i})}{2} \cdot 2^{s-1}.$$

When $e_0 > a_0$

$$2\phi({r_0}^{a_0}) \cdot \prod_{i=1}^{t} \phi({r_i}^{f_i}) \cdot \prod_{i=t+1}^{t+s} \frac{\phi({r_i}^{f_i})}{2} \cdot 2^{s-1}, \ \textit{where}$$

$$f_i = \begin{cases} e_i, & \textit{if } e_i \le a_i; \\ a_i, & \textit{otherwise.} \end{cases}$$

Proof. First, by Theorem 6, we have

$$\Phi_{{r_0}^{e_0}}(x) = \begin{cases} \prod\limits_{c_0 \in C_e} (x + c_0), & \text{if } e_0 \le a_0; \\ \prod\limits_{c_0 \in C_a} (x^{A_0} + c_0), & \text{if } e_0 > a_0, \end{cases}$$

Then, by Theorem 17, the factorization of $\Phi_{r_1^{e_1}\dots r_{t+s}^{e_{t+s}}}$ when $q \equiv \pm 1 \ (mod\ r_i)$ is

$$\begin{aligned} & \Phi_{r_1^{e_1}\dots r_{t+s}^{e_{t+s}}}(x) = \Phi_{r_1^{e_1}}(x) \odot \Phi_{{r_2}^{e_2}}(x) \odot \cdots \odot \Phi_{{r_{t+s}}^{e_{t+s}}}(x) \\ = \ & \prod_{c_1} \cdots \prod_{c_t} \prod_{u_1} \cdots \prod_{u_s} \Big(x^{2E_sF_t} - \Big((U_s)^{F_t} + (U_s{}^q)^{F_t} \Big) \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} \\ & x^{E_sF_t} + \Big(U_s{}^{(q+1)} \Big)^{F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2E_s} \Big) \\ & \Big(\prod_{\substack{\{i_1,\dots,i_k\} \subset \{1,\dots,s\} \\ 1 \le k < \frac{s}{2}}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\dots,i_k) \big)^{F_t} + \big(U_s{}^q(i_1,\dots,i_k) \big)^{F_t} \Big) \\ & \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} x^{E_sF_t} + \Big(U_s{}^{(q+1)}(i_1,\dots,i_k) \Big)^{F_t} \Big(\prod_{i=1}^{t} {a_i}^{F_t/a_i} \Big)^{2E_s} \Big) \end{aligned}$$

$$\Big(\prod_{\substack{\{1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ k=\frac{s}{2},i_k=s}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k)\big)^{F_t} + \big({U_s}^q(i_1,\ldots,i_k)\big)^{F_t}\Big)$$
$$\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{E_s} x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k)\Big)^{F_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2E_s}\Big).$$

Finally, we do the composed product using Lemma 5, and we get the final factorization for $e_0 \leq a_0$ as

$$\prod_{c_0}\prod_{c_1}\cdots\prod_{c_t}\prod_{u_1}\cdots\prod_{u_s}\big(x-c_0\big)\odot\Bigg[\Big(x^{2E_sF_t} - \Big((U_s)^{F_t} + ({U_s}^q)^{F_t}\Big)\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{E_s}$$
$$x^{E_sF_t} + \Big({U_s}^{(q+1)}\Big)^{F_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2E_s}\Big)$$
$$\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ 1\leq k<\frac{s}{2}}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k)\big)^{F_t} + \big({U_s}^q(i_1,\ldots,i_k)\big)^{F_t}\Big)\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{E_s}$$
$$x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_t)\Big)^{F_t}\Big(\prod_{i=1}^{t} {a_i}^{F_t/a_i}\Big)^{2E_s}\Big)$$
$$\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ k=\frac{s}{2},i_k=s}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k)\big)^{F_t} + \big({U_s}^q(i_1,\ldots,i_k)\big)^{F_t}\Big)\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{E_s}$$
$$x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k)\Big)^{F_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2E_s}\Big)\Bigg]$$
$$= \prod_{c_0}\prod_{c_1}\cdots\prod_{c_t}\prod_{u_1}\cdots\prod_{u_s}\Big(x^{2E_sF_t} - \Big((U_s)^{F_t} + ({U_s}^{qF_t}\Big)\Big(c_0\Big)^{E_sF_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{E_s}$$
$$x^{E_sF_t} + \Big({U_s}^{(q+1)}\Big)^{F_t}\Big(c_0\Big)^{2E_sF_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2E_s}\Big)$$
$$\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ 1\leq k<\frac{s}{2}}} x^{2E_sF_t} - \Big({U_s}^{F_t}(i_1,\ldots,i_k) + {U_s}^{qF_t}(i_1,\ldots,i_k)\Big)\Big(c_0\Big)^{E_sF_t}$$
$$\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{E_s} x^{E_sF_t} + \Big({U_s}^{(q+1)F_t}(i_1,\ldots,i_k)\Big)\Big(c_0\Big)^{2E_sF_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2E_s}\Big)$$

$$\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ k=\frac{s}{2},i_k=s}} x^{2E_sF_t} - \Big({U_s}^{F_t}(i_1,\ldots,i_k) + {U_s}^{qF_t}(i_1,\ldots,i_k)\Big)\Big(c_0\Big)^{E_sF_t}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_s}$$

$$x^{E_sF_t} + \Big({U_s}^{(q+1)F_t}(i_1,\ldots,i_k)\Big)\Big(c_0\Big)^{2E_sF_t}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_s}\Big).$$

For $e_0 > a_0$, since $gcd(A_0, 2EsF_t) = 2$ we use Lemma 6 to have the final factorization as,

$$\begin{aligned}
&\prod_{c_0}\prod_{c_1}\cdots\prod_{c_t}\prod_{u_1}\cdots\prod_{u_s}\Big(x^{A_0}-c_0\Big)\odot\Big(x^{2E_sF_t} - \Big((U_s)^{F_t} + ({U_s}^q)^{F_t}\Big)\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_s}\\
&x^{E_sF_t} + \Big({U_s}^{(q+1)}\Big)^{F_t}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_s}\Big)\\
&\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ 1\le k<\frac{s}{2}}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k)\big)^{F_t} + \big({U_s}^q(i_1,\ldots,i_k)\big)^{F_t}\Big)\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_s}\\
&x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_t)\Big)^{F_t}\Big(\prod_{i=1}^{t}{a_i}^{F_t/a_i}\Big)^{2E_s}\Big)\\
&\Big(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ k=\frac{s}{2},i_k=s}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k)\big)^{F_t} + \big({U_s}^q(i_1,\ldots,i_k)\big)^{F_t}\Big)\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_s}\\
&x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k)\Big)^{F_t}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_s}\Big)\\
=\ &\prod_{c_0}\prod_{c_1}\cdots\prod_{c_t}\prod_{u_1}\cdots\prod_{u_s}\Big(x^{2E_sF_tA_0} - \Big((U_s)^{F_tA_0}(c_0)^{E_sF_t} + ({U_s}^q)^{F_tA_0}(c_0)^{qE_sF_t}\Big)\\
&\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0} x^{E_sF_tA_0} + \Big({U_s}^{(q+1)}\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big)\\
&\Big(x^{2E_sF_tA_0} - \Big((U_s)^{qF_tA_0}(c_0)^{E_sF_t} + (U_s)^{F_tA_0}(c_0)^{qE_sF_t}\Big)\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}\\
&x^{E_sF_tA_0} + \Big({U_s}^{(q+1)}\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big)
\end{aligned}$$

$$\Bigg(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ 1\le k<\frac{s}{2}}} x^{2E_sF_tA_0}-\Big(\big(U_s(i_1,\ldots,i_k)\big)^{F_tA_0}(c_0)^{E_sF_t}+\big(U_s{}^q(i_1,\ldots,i_k)\big)^{F_tA_0}(c_0)^{qE_sF_t}\Big)$$
$$\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}x^{E_sF_tA_0}+\Big(U_s{}^{(q+1)}(i_1,\ldots,i_k)\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big)$$
$$\Big(x^{2E_sF_tA_0}-\Big(\big(U_s(i_1,\ldots,i_k)\big)^{qF_tA_0}(c_0)^{E_sF_t}+\big(U_s(i_1,\ldots,i_k)\big)^{F_tA_0}(c_0)^{qE_sF_t}\Big)$$
$$\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}x^{E_sF_tA_0}+\Big(U_s{}^{(q+1)}(i_1,\ldots,i_k)\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big)$$
$$\Bigg(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ k=\frac{s}{2},i_k=s}} x^{2E_sF_tA_0}-\Big(\big(U_s(i_1,\ldots,i_k)\big)^{F_tA_0}(c_0)^{E_sF_t}+\big(U_s{}^q(i_1,\ldots,i_k)\big)^{F_tA_0}(c_0)^{qE_sF_t}\Big)$$
$$\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}x^{E_sF_tA_0}+\Big(U_s{}^{(q+1)}(i_1,\ldots,i_k)\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big)$$
$$\Big(x^{2E_sF_tA_0}-\Big(\big(U_s(i_1,\ldots,i_k)\big)^{qF_tA_0}(c_0)^{E_sF_t}+\big(U_s(i_1,\ldots,i_k)\big)^{F_tA_0}(c_0)^{qE_sF_t}\Big)$$
$$\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{E_sA_0}x^{E_sF_tA_0}+\Big(U_s{}^{(q+1)}(i_1,\ldots,i_k)\Big)^{F_tA_0}\Big(\prod_{i=1}^{t}{c_i}^{F_t/a_i}\Big)^{2E_sA_0}(c_0)^{(q+1)E_sF_t}\Big).$$

Moreover, we know that the number of irreducible factors of $\Phi_{{r_1}^{e_1}\cdots{r_{t+s}}^{e_{t+s}}}$ is

$$\prod_{i=1}^{t}\phi({r_i}^{f_i})\cdot\prod_{i=t+1}^{t+s}\frac{\phi({r_i}^{f_i})}{2}\cdot 2^{s-1}.$$

Additionally, the number of irreducible factors for $r_0=2$ is $\phi({r_0}^{e_0})$ when $e_0\le a_0$ since $gcd(1,2E_sF_t)=1$ and there is no extra factors. Also, the number of irreducible factors is $2\phi({r_0}^{a_0})$ when $e_0>a_0$ since $gcd(A_0,2E_sF_t)=2$. Then, the total number of factors when $e_0\le a_0$ is

$$\phi({r_0}^{e_0})\cdot\prod_{i=1}^{t}\phi({r_i}^{f_i})\cdot\prod_{i=t+1}^{t+s}\frac{\phi({r_i}^{f_i})}{2}\cdot 2^{s-1}.$$

When $e_0>a_0$, we have

$$2\phi({r_0}^{a_0})\cdot\prod_{i=1}^{t}\phi({r_i}^{f_i})\cdot\prod_{i=t+1}^{t+s}\frac{\phi({r_i}^{f_i})}{2}\cdot 2^{s-1}.$$

□

Theorem 19. *Without loss of generality, assume that* $q \equiv 3 \pmod 4$, *and let* $r_0 = 2$, $q \equiv 1 \pmod{r_i}$ *with* $1 \le i \le t$, *and* $q \equiv -1 \pmod{r_i}$ *with* $t+1 \le i \le s$, *where* r_i *are odd for* $1 \le i \le s$. *Then, the irreducible factorization of* $\Phi_{r_0^{e_0}} \odot \cdots \odot \Phi_{r_{t+s}^{e_{t+s}}}$ *is*

$$
\begin{aligned}
&\Phi_{{r_0}^{e_0}}(x) \odot \cdots \odot \Phi_{{r_{t+s}}^{e_{t+s}}}(x) \\
= \;& \prod_{u_0} \prod_{c_1} \cdots \prod_{c_t} \prod_{u_1} \cdots \prod_{u_s} \Bigg(x^{2B_0E_sF_t} + \Big((U_s)^{B_0F_t} {u_0}^{E_sF_t} + {(U_s}^q)^{B_0F_t} {u_0}^{qE_sF_t} \Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/c_i} \Big)^{B_0E_s} x^{B_0E_sF_t} + \Big({U_s}^{(q+1)} \Big)^{2B_0F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2B_0E_s} {u_0}^{(q+1)E_sF_t} \Big) \\
& \Bigg(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ 1 \le k < \frac{s}{2}}} x^{2B_0E_sF_t} + \Big(\big(U_s(i_1,\ldots,i_k)\big)^{B_0F_t} {u_0}^{E_sF_t} + \big({U_s}^q(i_1,\ldots,i_k)\big)^{B_0F_t} {u_0}^{qE_sF_t} \Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{B_0E_s} x^{B_0E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k) \Big)^{2B_0F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2B_0E_s} {u_0}^{(q+1)E_sF_t} \Big) \\
& \Bigg(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ k = \frac{s}{2}, i_k = s}} x^{2B_0E_sF_t} + \Big(\big(U_s(i_1,\ldots,i_k)\big)^{B_0F_t} {u_0}^{E_sF_t} + \big({U_s}^q(i_1,\ldots,i_k)\big)^{B_0F_t} {u_0}^{qE_sF_t} \Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{B_0E_s} x^{B_0E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k) \Big)^{2B_0F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2B_0E_s} {u_0}^{(q+1)E_sF_t} \Big),
\end{aligned}
$$

where

$$
B_0 = \begin{cases} 1, & \text{if } e_0 \le a_0; \\ 2^{e_0 - a_0}, & \text{if } e_0 > a_0, \end{cases}
$$

and u_0 *is the set of all primitive* B_0*th root of unity, and all the other notations can be found in Theorem 17.*

Moreover, the number of irreducible factors of $\Phi_{{r_0}^{e_0} {r_1}^{e_1} \cdots {r_{t+s}}^{e_{t+s}}}$ *in* $\mathbb{F}_q[x]$ *is*

$$
\frac{\phi({r_0}^{f_0})}{2} \cdot \prod_{i=1}^{t} \phi({r_i}^{f_i}) \cdot \prod_{i=t+1}^{t+s} \frac{\phi({r_i}^{f_i})}{2} \cdot 2^s.
$$

$$f_i = \begin{cases} e_i, & \text{if } e_i \leq a_i; \\ a_i, & \text{if } e_i > a_i. \end{cases}$$

Proof. First, by Theorem 7, we have

(1) if $e \leq a$, then Φ_{2^e} can be factorized as

$$\Phi_{2^e}(x) = \prod_{u \in U_e} (x^2 + (u + u^{-1})x + 1).$$

In the prood of (Theorem 1 [10]), we have $u^{q+1} = 1$ because $ord(u) \leq 2^a$. So, $u^q = u^{-1}$ and we get

$$\Phi_{2^e}(x) = \prod_{u \in U_e} (x^2 + (u + u^q)x + u^{q+1}).$$

(2) if $e > a$, then Φ_{2^e} can be factorized as

$$\Phi_{2^e}(x) = \prod_{u \in U_a} (x^{2^{e-a+1}} + (u + u^{-1})x^{2e-a} - 1).$$

Also, in the prood of (Theorem 1 [10]), we have u^{q+1} because u is a primitive $2^{a+1}th$ root of unity. So, $u^q = u^{-1}$ and we get,

$$\Phi_{2^e}(x) = \prod_{u \in U_a} (x^{2^{e-a+1}} + (u + u^q)x^{2^{e-a}} + u^{q+1}),$$

Therefore, the factorization of $\Phi_{r_0^{e_0}}$ when $q \equiv 3 \pmod 4$ is

$$\Phi_{2^e}(x) = \prod_{u \in U_e or U_a} (x^{2B_0} + (u_0 + {u_0}^q)x^{B_0} + {u_0}^{q+1}).$$

Then, by Theorem 17, the factorization of $\Phi_{r_1^{e_1} \cdots r_{t+s}^{e_{t+s}}}$ when $q \equiv \pm 1 \ (mod\ r_i)$ is

$$
\begin{aligned}
&\Phi_{r_1^{e_1}}(x) \odot \cdots \Phi_{t+s^{e_{t+s}}}(x) \\
= \;& \prod_{c_1} \cdots \prod_{c_t} \prod_{u_1} \cdots \prod_{u_s} \Big(x^{2E_sF_t} - \Big((U_s)^{F_t} + (U_s{}^q)^{F_t} \Big) \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} \\
& x^{E_sF_t} + \Big({U_s}^{(q+1)} \Big)^{F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2E_s} \Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ 1 \le k < \frac{s}{2}}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k) \big)^{F_t} + \big(U_s{}^q(i_1,\ldots,i_k) \big)^{F_t} \Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k) \Big)^{F_t} \Big(\prod_{i=1}^{t} {a_i}^{F_t/a_i} \Big)^{2E_s} \Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ k = \frac{s}{2}, i_k = s}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k) \big)^{F_t} + \big(U_s{}^q(i_1,\ldots,i_k) \big)^{F_t} \Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k) \Big)^{F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2E_s} \Big),
\end{aligned}
$$

Finally, we do the composed product and we get the final factorization as

$$
\begin{aligned}
& \prod_{u_0} \prod_{c_1} \cdots \prod_{c_t} \prod_{u_1} \cdots \prod_{u_s} \Big(x^{2B_0} + (u_0 + {u_0}^q) x^{B_0} + {u_0}^{q+1} \Big) \odot \\
& \Big[\Big(x^{2E_sF_t} - \Big((U_s)^{F_t} + (U_s{}^q)^{F_t} \Big) \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} x^{E_sF_t} + \Big({U_s}^{(q+1)} \Big)^{F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2E_s} \Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ 1 \le k < \frac{s}{2}}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k) \big)^{F_t} + \big(U_s{}^q(i_1,\ldots,i_k) \big)^{F_t} \Big) \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} \\
& x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k) \Big)^{F_t} \Big(\prod_{i=1}^{t} {a_i}^{F_t/a_i} \Big)^{2E_s} \Big) \\
& \Big(\prod_{\substack{\{i_1,\ldots,i_k\} \subset \{1,\ldots,s\} \\ k = \frac{s}{2}, i_k = s}} x^{2E_sF_t} - \Big(\big(U_s(i_1,\ldots,i_k) \big)^{F_t} + \big(U_s{}^q(i_1,\ldots,i_k) \big)^{F_t} \Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{E_s} x^{E_sF_t} + \Big({U_s}^{(q+1)}(i_1,\ldots,i_k) \Big)^{F_t} \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i} \Big)^{2E_s} \Big) \Big]
\end{aligned}
$$

$$
\begin{aligned}
= \prod_{u_0}\prod_{c_1}\cdots\prod_{c_t}\prod_{u_1}\cdots\prod_{u_s}\Bigg(& x^{2B_0E_sF_t} + \Big((U_s)^{B_0F_t}{u_0}^{E_sF_t} + (U_s{}^q)^{B_0F_t}{u_0}^{qE_sF_t}\Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/c_i}\Big)^{B_0E_s} x^{B_0E_sF_t} + \Big(U_s{}^{(q+1)}\Big)^{2B_0F_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2B_0E_s}{u_0}^{(q+1)E_sF_t}\Big) \\
& \Bigg(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ 1\le k<\frac{s}{2}}} x^{2B_0E_sF_t} + \Big(\big(U_s(i_1,\ldots,i_k)\big)^{B_0F_t}{u_0}^{E_sF_t} + \big(U_s{}^q(i_1,\ldots,i_k)\big)^{B_0F_t}{u_0}^{qE_sF_t}\Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{B_0E_s} x^{B_0E_sF_t} + \Big(U_s{}^{(q+1)}(i_1,\ldots,i_k)\Big)^{2B_0F_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2B_0E_s}{u_0}^{(q+1)E_sF_t}\Big) \\
& \Bigg(\prod_{\substack{\{i_1,\ldots,i_k\}\subset\{1,\ldots,s\}\\ k=\frac{s}{2},i_k=s}} x^{2B_0E_sF_t} + \Big(\big(U_s(i_1,\ldots,i_k)\big)^{B_0F_t}{u_0}^{E_sF_t} + \big(U_s{}^q(i_1,\ldots,i_k)\big)^{B_0F_t}{u_0}^{qE_sF_t}\Big) \\
& \Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{B_0E_s} x^{B_0E_sF_t} + \Big(U_s{}^{(q+1)}(i_1,\ldots,i_k)\Big)^{2B_0F_t}\Big(\prod_{i=1}^{t} {c_i}^{F_t/a_i}\Big)^{2B_0E_s}{u_0}^{(q+1)E_sF_t}\Big),
\end{aligned}
$$

the last equality is obtained by Lemma 10. Moreover, we know that the number of irreducible factors of $\Phi_{{r_1}^{e_1}\cdots{r_{t+s}}^{e_{t+s}}}$ is

$$\prod_{i=1}^{t}\phi({r_i}^{f_i})\cdot\prod_{i=t+1}^{t+s}\frac{\phi({r_i}^{f_i})}{2}\cdot 2^{s-1}.$$

The number of irreducible factors for $r_0 = 2$ is $2^{\frac{\phi({r_0}^{a_0})}{2}}$ since $gcd(2B_0, 2E_sF_t) = 2$. Therefore, the total number of irreducible factors is

$$
\begin{aligned}
& 2\Big(\frac{\phi({r_0}^{a_0})}{2}\Big)\cdot\prod_{i=1}^{t}\phi({r_i}^{f_i})\cdot\prod_{i=t+1}^{t+s}\frac{\phi({r_i}^{f_i})}{2}\cdot 2^{s-1} \\
= \ & \frac{\phi({r_0}^{a_0})}{2}\cdot\prod_{i=1}^{t}\phi({r_i}^{f_i})\cdot\prod_{i=t+1}^{t+s}\frac{\phi({r_i}^{f_i})}{2}\cdot 2^{s}.
\end{aligned}
$$

□

Example 1. Let $q = 29$. Let $r_1 = 2$, with $q \equiv 1 \pmod 2$, $r_2 = 3$ with $q \equiv -1 \pmod 3$, $r_3 = 5$ with $q \equiv -1 \pmod 5$, and $r_4 = 7$ with $q \equiv 1 \pmod 7$. Therefore, $t = 1$ and $s = 2$, and $a_1 = 2,\ a_2 = a_3 = a_4 = 1$.

The number of factors of $\Phi_{2^2.3^1.5^1.7^1}$ when $e_i \leq a_i$ is

$$\begin{aligned}\phi({r_0}^{a_0}) \cdot \prod_{i=1}^{t} \phi({r_i}^{f_i}) \cdot \prod_{i=t+1}^{t+s} \frac{\phi(r_i{}^{f_i})}{2} \cdot 2^{s-1} &= \phi(2^2) \cdot \frac{\phi(3)}{2} \cdot \frac{\phi(5)}{2} \cdot \phi(7) \cdot 2 \\ &= 2 \cdot 2 \cdot 6 \cdot 2 = 48.\end{aligned}$$

since $e_1 \leq a_1$, and $q \equiv 1 \pmod 4$,we have $c_1 = 17$ or 12. Also, $e_4 \leq a_4$ and $q \equiv 1 \pmod 7$, we have $c_2 = 7,\ 16,\ 20,\ 23,\ 24$ or 25. Since $e_i \leq a_i$, we have $F_t = 1$.
Then, by Theorem 14, we have

$$\begin{aligned}\Phi_{2^2.7} &= (x-(17\cdot 7))(x-(17\cdot 16))(x-(17\cdot 20))(x-(17\cdot 23))(x-(17\cdot 24)) \\ &\quad (x-(17\cdot 25))(x-(12\cdot 7))(x-(12\cdot 16))(x-(12\cdot 20))(x-(12\cdot 23)) \\ &\quad (x-(12\cdot 24))(x-(12\cdot 25)) \\ &= (x-3)(x-11)(x-21)(x-14)(x-2)(x-19)(x-26)(x-18) \\ &\quad (x-8)(x-15)(x-27)(x-10).\end{aligned}$$

since $e_2 \leq a_2$ and $q \equiv -1 \pmod 3$, we have $u_1 = 14a+8$, ${u_1}^q = 15a+20$. Also, $e_3 \leq a_3$ and $q \equiv -1 \pmod 5$, we have $u_2 = 7a+14$ or $6a+11$, ${u_2}^q = 22a+20$ or $23a+12$. Since $e_i \leq a_i$, we have $E_s = 2$.
Then, by Theorem 15, we have

$$\begin{aligned}\Phi_{3\cdot 5} &= (x^2 - \big((14a+8)(7a+14)+(15a+20)(22a+20)\big)x+1)(x^2-\big((7a+14) \\ &\quad (15a+20)+(22a+20)(14a+8)\big)x+1)(x^2-\big((14a+8)(15a+20) \\ &\quad (23a+12)\big)x+1)(x^2-\big((6a+11)(15a+20)+(23a+12)(14a+8)\big)x+1) \\ &= (x^2-4x+1),(x^2-20x+1)(x^2-21x+1),(x^2-14x+1).\end{aligned}$$

Then, by Theorem 17, we have that $\Phi_{2^2.3\cdot 5\cdot 7}$ is

$$(x^2-(4)(3)x+(3)^2)(x^2-(4)(11)x+(11)^2)(x^2-(4)(21)x+(21)^2)$$

$$
\begin{aligned}
& (x^2-(4)(14)x+(14)^2)(x^2-(4)(2)x+(2)^2)(x^2-(4)(19)x+(19)^2) \\
& (x^2-(4)(26)x+(26)^2)(x^2-(4)(18)x+(18)^2)(x^2-(4)(8)x+(8)^2) \\
& (x^2-(4)(15)x+(15)^2)(x^2-(4)(27)x+(27)^2)(x^2-(4)(10)x+(10)^2) \\
& (x^2-(20)(3)x+(3)^2)(x^2-(20)11)x+(11)^2)(x^2-(20)(21)x+(21)^2) \\
& (x^2-(20)(14)x+(14)^2)(x^2-(20)(2)x+(2)^2)(x^2-(20)(19)x+(19)^2) \\
& (x^2-(20)(26)x+(26)^2)(x^2-(20)(18)x+(18)^2)(x^2-(20)(8)x+(8)^2) \\
& (x^2-(20)(15)x+(15)^2)(x^2-(20)(27)x+(27)^2)(x^2-(20)(10)x+(10)^2) \\
& (x^2-(21)(3)x+(3)^2)(x^2-(21)(11)x+(11)^2)(x^2-(21)(21)x+(21)^2) \\
& (x^2-(21)(14)x+(14)^2)(x^2-(21)(2)x+(2)^2)(x^2-(21)(19)x+(19)^2) \\
& (x^2-(21)(26)x+(26)^2)(x^2-(21)(18)x+(18)^2)(x^2-(21)(8)x+(8)^2) \\
& (x^2-(21)(15)x+(15)^2)(x^2-(21)(27)x+(27)^2)(x^2-(21)(10)x+(10)^2) \\
& (x^2-(14)(3)x+(3)^2)(x^2-(14)(11)x+(11)^2)(x^2-(14)(21)x+(21)^2) \\
& (x^2-(14)(14)x+(14)^2)(x^2-(14)(2)x+(2)^2)(x^2-(14)(19)x+(19)^2) \\
& (x^2-(14)(26)x+(26)^2)(x^2-(14)(18)x+(18)^2)(x^2-(14)(8)x+(8)^2) \\
& (x^2-(14)(15)x+(15)^2)(x^2-(14)(27)x+(27)^2)(x^2-(14)(10)x+(10)^2) \\
= \; & (x^2-12x+9)(x^2-15x+5)(x^2-26x+6)(x^2-27x+22)(x^2-8x+4) \\
& (x^2-18x+13)(x^2-17x+9)(x^2-14x+5)(x^2-3x+6)(x^2-2x+22) \\
& (x^2-21x+4)(x^2-11x+13)(x^2-2x+9)(x^2-17x+5)(x^2-14x+6) \\
& (x^2-19x+22)(x^2-11x+4)(x^2-3x+13)(x^2-27x+9)(x^2-12x+5) \\
& (x^2-15x+6)(x^2-10x+22)(x^2-18x+4)(x^2-26x+13)(x^2-5x+9) \\
& (x^2-28x+5)(x^2-6x+6)(x^2-4x+22)(x^2-13x+4)(x^2-22x+13) \\
& (x^2-24x+9)(x^2-x+5)(x^2-23x+6)(x^2-25x+22)(x^2-16x+4) \\
& (x^2-7x+13)(x^2-13x+9)(x^2-9x+5)(x^2-4x+6)(x^2-22x+22) \\
& (x^2-28x+4)(x^2-5x+13)(x^2-16x+9)(x^2-20x+5)(x^2-25x+6) \\
& (x^2-7x+22)(x^2-x+4)(x^2-24x+13).
\end{aligned}
$$

When $e_i > a_i$, the number of factors of $\Phi_{2^3 \cdot 3^2 \cdot 5^2 \cdot 7^2}$ is

$$\begin{aligned} 2\phi({r_0}^{a_0}) \cdot \prod_{i=1}^{t} \phi({r_i}^{f_i}) \cdot \prod_{i=t+1}^{t+s} \frac{\phi({r_i}^{f_i})}{2} \cdot 2^{s-1} &= 2 \cdot \phi(2^2) \cdot \frac{\phi(3)}{2} \cdot \frac{\phi(5)}{2} \cdot \phi(7) \cdot 2 \\ &= 4 \cdot 2 \cdot 6 \cdot 2 = 96. \end{aligned}$$

since $e_1 > a_1$, and $q \equiv 1 \pmod 4$, we have $c_1 = 17$ or 12. Also, $e_4 > a_4$ and $q \equiv 1 \pmod 7$, we have $c_2 = 7,\ 16,\ 20,\ 23,\ 24$, or 25. Since $e_i > a_i$, we have $F_t = 2^{3-2} \cdot 7^{2-1} = 14$. Then, by Theorem 14, we have that $\Phi_{2^3 \cdot 7^2}$ is

$$\begin{aligned} & \left(x^{14} - (17^7 \cdot 7^2)^{15}\right)\left(x^{14} - (17^7 \cdot 16^2)^{15}\right)\left(x^{14} - (17^7 \cdot 20^2)^{15}\right)\left(x^{14} - (17^7 \cdot 23^2)^{15}\right) \\ & \left(x^{14} - (17^7 \cdot 24^2)^{15}\right)\left(x^{14} - (17^7 \cdot 25^2)^{15}\right)\left(x^{14} - (12^7 \cdot 7^2)^{15}\right)\left(x^{14} - (12^7 \cdot 16^2)^{15}\right) \\ & \left(x^{14} - (12^7 \cdot 20^2)^{15}\right)\left(x^{14} - (12^7 \cdot 23^2)^{15}\right)\left(x^{14} - (12^7 \cdot 24^2)^{15}\right)\left(x^{14} - (12^7 \cdot 25^2)^{15}\right) \\ = \ & (x^{14} - 21)(x^{14} - 2)(x^{14} - 14)(x^{14} - 3)(x^{14} - 19)(x^{14} - 11)(x^{14} - 8) \\ & (x^{14} - 27)(x^{14} - 15)(x^{14} - 26)(x^{14} - 10)(x^{14} - 18). \end{aligned}$$

since $e_2 > a_2$ and $q \equiv -1 \pmod 3$, we have $u_1 = 14a + 8$, ${u_1}^q = 15a + 20$. Also, $e_3 > a_3$ and $q \equiv -1 \pmod 5$, we have $u_2 = 7a + 14$ or $6a + 11$, ${u_2}^q = 22a + 20$ or $23a + 12$. Since $e_i > a_i$, we have $E_s = 2 \cdot 3^{2-1} \cdot 5^{2-1} = 30$.
Then, by Theorem 15, we have

$$\begin{aligned} \Phi_{3^2 \cdot 5^2} &= (x^{30} - \left((14a+8)^5\ (7a+14)^3\right)^{14} + \left((15a+20)^5\ (22a+20)^3\right)^{14} x^{15} + 1) \\ & \quad (x^{30} - \left((14a+8)^5\ (6a+11)^3\right)^{14} + \left((15a+20)^5\ (23a+12)^3\right)^{14} x^{15} + 1) \\ & \quad (x^{30} - \left((7a+14)^3\ (15a+20)^5\right)^{14} + \left((22a+20)^3\ (14a+8)^5\right)^{14} x^{15} + 1) \\ & \quad (x^{30} - \left((6a+11)^3\ (15a+20)^5\right)^{14} + \left((23a+12)^3\ (14a+8)^5\right)^{14}) x^{15} + 1) \\ &= (x^{30} - 21x^{15} + 1), (x^{30} - 20x^{15} + 1)(x^{30} - 14x^{15} + 1), (x^{30} - 4x + 1). \end{aligned}$$

Finally, by Theorem 17, we have that $\Phi_{2^3.3^2.5^2.7^2}$ is

$$
\begin{aligned}
& (x^{420}-(21)(21)x^{210}+(21)^2)(x^{420}-(21)(2)x^{210}+(2)^2)(x^{420}-(21)(14)x^{210}+(14)^2) \\
& (x^{420}-(21)(3)x^{210}+(3)^2)(x^{420}-(21)(19)x^{210}+(19)^2)(x^{420}-(21)(11)x^{210}+(11)^2) \\
& (x^{420}-(21)(8)x^{210}+(8)^2)(x^{420}-(21)(27)x^{210}+(27)^2)(x^{420}-(21)(15)x^{210}+(15)^2) \\
& (x^{420}-(21)(26)x^{210}+(26)^2)(x^{420}-(21)(10)x^{210}+(10)^2)(x^{420}-(21)(18)x^{210}+(18)^2) \\
& (x^{420}-(20)(21)x^{210}+(21)^2)(x^{420}-(20)(2)x^{210}+(2)^2)(x^{420}-(20)(14)x^{210}+(14)^2) \\
& (x^{420}-(20)(3)x^{210}+(3)^2)(x^{420}-(20)(19)x^{210}+(19)^2)(x^{420}-(20)(11)x^{210}+(11)^2) \\
& (x^{420}-(20)(8)x^{210}+(8)^2)(x^{420}-(20)(27)x^{210}+(27)^2)(x^{420}-(20)(15)x^{210}+(15)^2) \\
& (x^{420}-(20)(26)x^{210}+(26)^2)(x^{420}-(20)(10)x^{210}+(10)^2)(x^{420}-(20)(18)x^{210}+(18)^2) \\
& (x^{420}-(14)(21)x^{210}+(21)^2)(x^{420}-(14)(2)x^{210}+(2)^2)(x^{420}-(14)(14)x^{210}+(14)^2) \\
& (x^{420}-(14)(3)x^{210}+(3)^2)(x^{420}-(14)(19)x^{210}+(19)^2)(x^{420}-(14)(11)x^{210}+(11)^2) \\
& (x^{420}-(14)(8)x^{210}+(8)^2)(x^{420}-(14)(27)x^{210}+(27)^2)(x^{420}-(14)(15)x^{210}+(15)^2) \\
& (x^{420}-(14)(26)x^{210}+(26)^2)(x^{420}-(14)(10)x^{210}+(10)^2)(x^{420}-(14)(18)x^{210}+(18)^2) \\
& (x^{420}-(4)(21)x^{210}+(21)^2)(x^{420}-(4)(2)x^{210}+(2)^2)(x^{420}-(4)(14)x^{210}+(14)^2) \\
& (x^{420}-(4)(3)x^{210}+(3)^2)(x^{420}-(4)(19)x^{210}+(19)^2)(x^{420}-(4)(11)x^{210}+(11)^2) \\
& (x^{420}-(4)(8)x^{210}+(8)^2)(x^{420}-(4)(27)x^{210}+(27)^2)(x^{420}-(4)(15)x^{210}+(15)^2) \\
& (x^{420}-(4)(26)x^{210}+(26)^2)(x^{420}-(4)(10)x^{210}+(10)^2)(x^{420}-(4)(18)x^{210}+(18)^2) \\
= \; & (x^{420}-6x^{210}+6)(x^{420}-13x^{210}+4)(x^{420}-4x^{210}+22)(x^{420}-5x^{210}+9) \\
& (x^{420}-22x^{210}+13)(x^{420}-28x^{210}+5)(x^{420}-23x^{210}+6)(x^{420}-16x^{210}+4) \\
& (x^{420}-25x^{210}+22)(x^{420}-24x^{210}+9)(x^{420}-7x^{210}+13)(x^{420}-x^{210}+5) \\
& (x^{420}-14x^{210}+6)(x^{420}-11x^{210}+4)(x^{420}-19x^{210}+22)(x^{420}-2x^{210}+9) \\
& (x^{420}-3x^{210}+13)(x^{420}-17x^{210}+5)(x^{420}-15x^{210}+6)(x^{420}-18x^{210}+4) \\
& (x^{420}-10x^{210}+22)(x^{420}-27x^{210}+9)(x^{420}-26x^{210}+13)(x^{420}-12x^{210}+5) \\
& (x^{420}-4x^{210}+6)(x^{420}-28x^{210}+4)(x^{420}-22x^{210}+22)(x^{420}-13x^{210}+9) \\
& (x^{420}-5x^{210}+13)(x^{420}-9x^{210}+5))(x^{420}-25x^{210}+6)(x^{420}-x^{210}+4)
\end{aligned}
$$

$$(x^{420} - 7x^{210} + 22)(x^{420} - 16x^{210} + 9)(x^{420} - 24x^{210} + 13)(x^{420} - 20x^{210} + 5)$$
$$(x^{420} - 26x^{210} + 6)(x^{420} - 8x^{210} + 4)(x^{420} - 27x^{210} + 22)(x^{420} - 12x^{210} + 9)$$
$$(x^{420} - 18x^{210} + 13)(x^{420} - 15x^{210} + 5)(x^{420} - 3x^{210} + 6)(x^{420} - 21x^{210} + 4)$$
$$(x^{420} - 2x^{210} + 22)(x^{420} - 17x^{210} + 9)(x^{420} - 11x^{210} + 13)(x^{420} - 14x^{210} + 5).$$

After that, the final factorization give as irreducible polynomials as

$$(x^{210} + 14x^{105} + 8)(x^{210} + 15x^{105} + 8)(x^{210} + 3x^{105} + 27)(x^{210} + 26x^{105} + 27)$$
$$(x^{210} + 11x^{105} + 15)(x^{210} + 18x^{105} + 15)(x^{210} + 12x^{105} + 26)(x^{210} + 17x^{105} + 26)$$
$$(x^{210} + 10x^{105} + 10)(x^{210} + 19x^{105} + 10)(x^{210} + 8x^{105} + 18)(x^{210} + 21x^{105} + 18)$$
$$(x^{210} + 6x^{105} + 21)(x^{210} + 23x^{105} + 21)(x^{210} + 7x^{105} + 2)(x^{210} + 22x^{105} + 2)$$
$$(x^{210} + 13x^{105} + 14)(x^{210} + 16x^{105} + 14)(x^{210} + x^{105} + 3)(x^{2}10 + 28x^{105} + 3)$$
$$(x^{210} + 4x^{105} + 19)(x^{210} + 25x^{105} + 19)(x^{2}10 + 9 * x^{1}05 + 11)(x^{210} + 20x^{105} + 11)$$
$$(x^{210} + x^{105} + 8)(x^{210} + 28x^{105} + 8)(x^{210} + 6x^{105} + 27)(x^{210} + 23x^{105} + 27)$$
$$(x^{210} + 7x^{105} + 15)(x^{210} + 22x^{105} + 15)(x^{210} + 5x^{105} + 26)(x^{210} + 24x^{105} + 26)$$
$$(x^{210} + 9x^{105} + 10)(x^{210} + 20x^{105} + 10)(x^{210} + 13x^{105} + 18)(x^{210} + 16x^{105} + 18)$$
$$(x^{210} + 12x^{105} + 21)(x^{210} + 17x^{105} + 21)(x^{210} + 14x^{105} + 2)(x^{210} + 15x^{105} + 2)$$
$$(x^{210} + 3x^{105} + 14)(x^{210} + 26x^{105} + 14)(x^{210} + 2x^{105} + 3)(x^{210} + 27x^{105} + 3)$$
$$(x^{210} + 8x^{105} + 19)(x^{210} + 21x^{105} + 19)(x^{210} + 11x^{105} + 11)(x^{210} + 18x^{105} + 11)$$
$$(x^{210} + 7x^{105} + 8)(x^{210} + 22x^{105} + 8)(x^{210} + 13x^{105} + 27)(x^{210} + 16x^{105} + 27)$$
$$(x^{210} + 9x^{105} + 15)(x^{210} + 20x^{105} + 15)(x^{210} + 6x^{105} + 26)(x^{210} + 23x^{105} + 26)$$
$$(x^{210} + 5x^{105} + 10)(x^{210} + 24x^{105} + 10)(x^{210} + 4x^{105} + 18)(x^{210} + 25x^{105} + 18)$$
$$(x^{210} + 3x^{105} + 21)(x^{210} + 26x^{105} + 21)(x^{210} + 11x^{105} + 2)(x^{210} + 18x^{105} + 2)$$
$$(x^{210} + 8x^{105} + 14)(x^{210} + 21x^{105} + 14)(x^{210} + 14x^{105} + 3)(x^{210} + 15x^{105} + 3)$$
$$(x^{210} + 2x^{105} + 19)(x^{210} + 27x^{105} + 19)(x^{210} + 10x^{105} + 11)(x^{210} + 19x^{105} + 11)$$
$$(x^{210} + 10x^{105} + 8)(x^{210} + 19x^{105} + 8)(x^{210} + 2x^{105} + 27)(x^{210} + 27x^{105} + 27)$$

$$(x^{210}+12x^{105}+15)(x^{210}+17x^{105}+15)x^{210}+8x^{105}+26)(x^{210}+21x^{105}+26)$$
$$(x^{210}+3x^{105}+10)(x^{210}+26x^{105}+10)(x^{210}+14x^{105}+18)(x^{210}+15x^{105}+18)$$
$$(x^{210}+4x^{105}+21)(x^{210}+25x^{105}+21)(x^{210}+5x^{105}+2)(x^{210}+24x^{105}+2)$$
$$(x^{210}+x^{105}+14)(x^{210}+28x^{105}+14)(x^{210}+9x^{105}+3)(x^{210}+20x^{105}+3)$$
$$(x^{210}+7x^{105}+19)(x^{210}+22x^{105}+19)(x^{210}+6x^{105}+11)(x^{210}+23x^{105}+11).$$

Example 2. Let $q = 41$. Let $r_1 = 2$ with $q \equiv -1 \pmod 2$, $r_2 = 3$ with $q \equiv 1 \pmod 3$, $r_3 = 7$ with $q \equiv 1 \pmod 7$, and $r_4 = 11$ with $q \equiv -1 \pmod{11}$. Therefore, $t = 2$ and $s = 1$ and since $a_i = v_r(q-1)$ when $q \equiv 1 \pmod{r_i}$ and $a_i = v_r(q^2-1)$ when $q \equiv -1 \pmod{r_i}$, we have $a_1 = 3,\ a_2 = a_3 = a_4 = 1$.
The number of factors of $\Phi_{2^2 \cdot 3^1 \cdot 7^1 \cdot 11^1}$ when $e_i \leq a_i$ is

$$\begin{aligned}\frac{\phi({r_0}^{a_0})}{2} \cdot \prod_{i=1}^{t} \phi({r_i}^{f_i}) \cdot \prod_{i=t+1}^{t+s} \frac{\phi({r_i}^{f_i})}{2} \cdot 2^s &= \frac{\phi(2^2)}{2} \cdot \phi(3) \cdot \phi(7) \cdot \frac{\phi(11)}{2} \cdot 2 \\ &= 2 \cdot 6 \cdot 5 \cdot 2 = 120.\end{aligned}$$

since $e_2 \leq a_2$ and $q \equiv 1 \pmod 3$, we have $c_1 = 36$ or 6. Also, $e_3 \leq e_3$ and $q \equiv 1 \pmod 7$, we have $c_2 = 4,\ 11,\ 16,\ 21,\ 35$, or 41. Since $e_i \leq a_i$, we have $F_t = 1$. Then, by Theorem 14, we have that $\Phi_{3\cdot 7}$ is

$$\begin{aligned}&(x-(36\cdot 4))(x-(36\cdot 11))(x-(36\cdot 16))(x-(36\cdot 21))(x-(36\cdot 35)) \\ &(x-(36\cdot 41))(x-(6\cdot 4))(x-(6\cdot 11))(x-(6\cdot 16))(x-(6\cdot 21))(x-(6\cdot 35)) \\ &(x-(6\cdot 41)) \\ = \ &(x-15)(x-9)(x-17)(x-25)(x-13)(x-14)(x-24)(x-23) \\ &(x-10)(x-40)(x-38)(x-31) \\ = \ &(x+28)(x+34)(x+26)(x+18)(x+30)(x+29)(x+19)(x+20) \\ &(x+33)(x+3)(x+5)(x+12).\end{aligned}$$

since $e_1 \leq a_1$ and $q \equiv -1 \pmod 2$, we have $u_1 = 4a+41$, ${u_1}^q = 39a+2$. Also, $e_4 \leq a_4$, and $q \equiv -1 \pmod 7$, we have $u_2 = 36a+32,\ 31a+17,\ 11a+43,\ 37a+29$

or $34a+28$, ${u_2}^q = 7a+25$, $12a+5$, $32a+2$, $6a+23$ or $9a+19$. Since $e_i \leq a_i$, we have $E_s = 2$. Then, by Theorem 15, we have that $\Phi_{2^2 \cdot 11}$ is

$$
\begin{aligned}
& \Big(x^2 - \big((4a+41)(36a+32) + (39a+2)(7a+25)\big)x + 1\Big) \\
& \Big(x^2 - \big((4a+41)(31a+17) + (39a+2)(12a+5)\big)x + 1\Big) \\
& \Big(x^2 - \big((4a+41)(11a+34) + (39a+2)(32a+2)\big)x + 1\Big) \\
& \Big(x^2 - \big((4a+41)(37a+29) + (39a+2)(6a+23)\big)x + 1\Big) \\
& \Big(x^2 - \big((4a+41)(34a+28) + (39a+2)(9a+19)\big)x + 1\Big) \\
& \Big(x^2 - \big((36a+32)(39a+2) + (7a+25)(4a+41)\big)x + 1\Big) \\
& \Big(x^2 - \big((31a+17)(39a+2) + (12a+5)(4a+41)\big)x + 1\Big) \\
& \Big(x^2 - \big((11a+34)(39a+2) + (32a+2)(4a+41)\big)x + 1\Big) \\
& \Big(x^2 - \big((37a+29)(39a+2) + (6a+23)(4a+41)\big)x + 1\Big) \\
& \Big(x^2 - \big((34a+28)(39a+2) + (9a+19)(4a+41)\big)x + 1\Big) \\
= \; & (x^2 - 25x + 1)(x^2 - 6x + 1)(x^2 - 16x + 1)(x^2 - 3x + 1)(x^2 - 26x + 1) \\
& (x^2 - 18x + 1)(x^2 - 37x + 1)(x^2 - 27x + 1)(x^2 - 40x + 1)(x^2 - 17x + 1) \\
= \; & (x^2 + 18x + 1)(x^2 + 37x + 1)(x^2 + 27x + 1)(x^2 + 40x + 1)(x^2 + 17x + 1) \\
& (x^2 + 25x + 1)(x^2 + 6x + 1)(x^2 + 16x + 1)(x^2 + 3x + 1)(x^2 + 26x + 1).
\end{aligned}
$$

Then, by Theorem 17, we have that $\Phi_{2^2 \cdot 3 \cdot 7 \cdot 11}$ is

$$
\begin{aligned}
& (x^2 - (29)(18)x + (29)^2)(x^2 - (29)(37)x + (29)^2)(x^2 - (29)(27)x + (29)^2) \\
& (x^2 - (29)(40)x + (29)^2)(x^2 - (29)(17)x + (29)^2)(x^2 - (29)(25)x + (29)^2) \\
& (x^2 - (29)(6)x + (29)^2)(x^2 - (29)(16)x + (29)^2)(x^2 - (29)(3)x + (29)^2) \\
& (x^2 - (29)(26)x + (29)^2)(x^2 - (28)(18)x + (28)^2)(x^2 - (28)(37)x + (28)^2) \\
& (x^2 - (28)(27)x + (28)^2)(x^2 - (28)(40)x + (28)^2)(x^2 - (28)(17)x + (28)^2) \\
& (x^2 - (28)(25)x + (28)^2)(x^2 - (28)(6)x + (28)^2)(x^2 - (28)(16)x + (28)^2)
\end{aligned}
$$

$(x^2-(28)(3)x+(28)^2)(x^2-(28)(26)x+(28)^2)(x^2-(30)(18)x+(30)^2)$

$(x^2-(30)(37)x+(30)^2)(x^2-(30)(27)x+(30)^2)(x^2-(30)(40)x+(30)^2)$

$(x^2-(30)(17)x+(30)^2)(x^2-(30)(25)x+(30)^2)(x^2-(30)(6)x+(30)^2)$

$(x^2-(30)(16)x+(30)^2)(x^2-(30)(3)x+(30)^2)(x^2-(30)(26)x+(30)^2)$

$(x^2-(26)(18)x+(26)^2)(x^2-(26)(37)x+(26)^2)(x^2-(26)(27)x+(26)^2)$

$(x^2-(26)(40)x+(26)^2)(x^2-(26)(17)x+(26)^2)(x^2-(26)(25)x+(26)^2)$

$(x^2-(26)(6)x+(26)^2)(x^2-(26)(16)x+(26)^2)(x^2-(26)(3)x+(30)^2)$

$(x^2-(26)(26)x+(26)^2)(x^2-(34)(18)x+(34)^2)(x^2-(34)(37)x+(34)^2)$

$(x^2-(34)(27)x+(34)^2)(x^2-(34)(40)x+(34)^2)(x^2-(34)(17)x+(34)^2)$

$(x^2-(34)(25)x+(34)^2)(x^2-(34)(6)x+(34)^2)(x^2-(34)(16)x+(34)^2)$

$(x^2-(34)(3)x+(34)^2)(x^2-(34)(26)x+(34)^2)(x^2-(18)(18)x+(18)^2)$

$(x^2-(18)(37)x+(18)^2)(x^2-(18)(27)x+(18)^2)(x^2-(18)(40)x+(18)^2)$

$(x^2-(18)(17)x+(18)^2)(x^2-(18)(25)x+(18)^2)(x^2-(18)(6)x+(18)^2)$

$(x^2-(18)(16)x+(18)^2)(x^2-(18)(3)x+(18)^2)(x^2-(18)(26)x+(18)^2)$

$(x^2-(12)(18)x+(12)^2)(x^2-(12)(37)x+(12)^2)(x^2-(12)(27)x+(12)^2)$

$(x^2-(12)(40)x+(12)^2)(x^2-(12)(17)x+(12)^2)(x^2-(12)(25)x+(12)^2)$

$(x^2-(12)(6)x+(12)^2)(x^2-(12)(16)x+(12)^2)(x^2-(12)(3)x+(12)^2)$

$(x^2-(12)(26)x+(12)^2)(x^2-(19)(18)x+(19)^2)(x^2-(19)(37)x+(19)^2)$

$(x^2-(19)(27)x+(19)^2)(x^2-(19)(40)x+(19)^2)(x^2-(19)(17)x+(19)^2)$

$(x^2-(19)(25)x+(19)^2)(x^2-(19)(6)x+(19)^2)(x^2-(19)(16)x+(19)^2)$

$(x^2-(19)(3)x+(19)^2)(x^2-(19)(26)x+(19)^2)(x^2-(5)(18)x+(5)^2)$

$(x^2-(5)(37)x+(5)^2)(x^2-(5)(27)x+(5)^2)(x^2-(5)(40)x+(5)^2)$

$(x^2-(5)(17)x+(5)^2)(x^2-(5)(25)x+(5)^2)(x^2-(5)(6)x+(5)^2)$

$(x^2-(5)(16)x+(5)^2)(x^2-(5)(3)x+(5)^2)(x^2-(5)(26)x+(5)^2)$

$(x^2-(33)(18)x+(33)^2)(x^2-(33)(37)x+(33)^2)(x^2-(33)(27)x+(33)^2)$

$$
\begin{aligned}
& (x^2-(33)(40)x+(33)^2)(x^2-(33)(17)x+(33)^2)(x^2-(33)(25)x+(33)^2) \\
& (x^2-(33)(6)x+(33)^2)(x^2-(33)(16)x+(33)^2)(x^2-(33)(3)x+(33)^2) \\
& (x^2-(33)(26)x+(33)^2)(x^2-(20)(18)x+(20)^2)(x^2-(20)(37)x+(20)^2) \\
& (x^2-(20)(27)x+(20)^2)(x^2-(20)(40)x+(28)^2)(x^2-(20)(17)x+(20)^2) \\
& (x^2-(20)(25)x+(20)^2)(x^2-(20)(6)x+(20)^2)(x^2-(20)(16)x+(20)^2) \\
& (x^2-(20)(3)x+(20)^2)(x^2-(20)(26)x+(20)^2)(x^2-(3)(18)x+(3)^2) \\
& (x^2-(3)(37)x+(3)^2)(x^2-(3)(27)x+(3)^2)(x^2-(3)(40)x+(3)^2) \\
& (x^2-(3)(17)x+(3)^2)(x^2-(3)(25)x+(3)^2)(x^2-(3)(6)x+(3)^2) \\
& (x^2-(3)(16)x+(3)^2)(x^2-(3)(3)x+(3)^2)(x^2-(3)(26)x+(3)^2) \\
= \; & (x^2+6x+24)(x^2+41x+24)(x^2+9x+24)(x^2+42x+24)(x^2+20x+24) \\
& (x^2+37x+24)(x^2+2x+24)(x^2+34x+24)(x^2+x+24)(x^2+23x+24) \\
& (x^2+31x+10)(x^2+4x+10)(x^2+25x+10)(x^2+2x+10)(x^2+3x+10) \\
& (x^2+12x+10)(x^2+39x+10)(x^2+18x+10)(x^2+41x+10)(x^2+40x+10) \\
& (x^2+24x+40)(x^2+35x+40)(x^2+36x+40)(x^2+39x+40)(x^2+37x+40) \\
& (x^2+19x+40)(x^2+8x+40)(x^2+7x+40)(x^2+4x+40)(x^2+6x+40) \\
& (x^2+38x+31)(x^2+16x+31)(x^2+14x+31)(x^2+8x+31)(x^2+12x+31) \\
& (x^2+5x+31)(x^2+27x+31)(x^2+29x+31)(x^2+35x+31)(x^2+31x+31) \\
& (x^2+10x+38)(x^2+11x+38)(x^2+15x+38)(x^2+27x+38)(x^2+19x+38) \\
& (x^2+33x+38)(x^2+32x+38)(x^2+28x+38)(x^2+16x+38)(x^2+24x+38) \\
& (x^2+23x+23)(x^2+21x+23)(x^2+13x+23)(x^2+32x+23)(x^2+5x+23) \\
& (x^2+20x+23)(x^2+22x+23)(x^2+30x+23)(x^2+11x+23)(x^2+38x+23) \\
& (x^2+x+15)(x^2+14x+15)(x^2+23x+15)(x^2+7x+15)(x^2+32x+15) \\
& (x^2+42x+15)(x^2+29x+15)(x^2+20x+15)(x^2+36x+15)(x^2+11x+15) \\
& (x^2+41x+17)(x^2+15x+17)(x^2+40x+17)(x^2+29x+17)(x^2+22x+17) \\
& (x^2+2x+17)(x^2+28x+17)(x^2+3x+17)(x^2+14x+17)(x^2+21x+17)
\end{aligned}
$$

$$(x^2+4x+25)(x^2+13x+25)(x^2+6x+25)(x^2+28x+25)(x^2+42x+25)$$
$$(x^2+39x+25)(x^2+30x+25)(x^2+37x+25)(x^2+15x+25)(x^2+x+25)$$
$$(x^2+35x+14)(x^2+17x+14)(x^2+31x+14)(x^2+30x+14)(x^2+2x+14)$$
$$(x^2+8x+14)(x^2+26x+14)(x^2+12x+14)(x^2+13x+14)(x^2+41x+14)$$
$$(x^2+16x+13)(x^2+9x+13)(x^2+24x+13)(x^2+26x+13)(x^2+39x+13)$$
$$(x^2+27x+13)(x^2+34x+13)(x^2+19x+13)(x^2+17x+13)(x^2+4x+13)$$
$$(x^2+11x+9)(x^2+25x+9)(x^2+38x+9)(x^2+34x+9)(x^2+8x+9)$$
$$(x^2+32x+9)(x^2+18x+9)(x^2+5x+9)(x^2+9x+9)(x^2+35x+9).$$

When $e_i > a_i$, the number of factors of $\Phi_{2^4.3^2.7^2.11^2}$ will be

$$\begin{aligned}\frac{\phi({r_0}^{a_0})}{2}\cdot\prod_{i=1}^{t}\phi({r_i}^{f_i})\cdot\prod_{i=t+1}^{t+s}\frac{\phi({r_i}^{f_i})}{2}\cdot 2^s &= \frac{\phi(2^3)}{2}\cdot\phi(3)\cdot\phi(7)\cdot\frac{\phi(11)}{2}\cdot 2\\ &= 2\cdot 2\cdot 6\cdot 5\cdot 2 = 240.\end{aligned}$$

since $e_2 > a_2$ and $q \equiv 1 \pmod 3$, we have $c_1 = 36$ or 6. Also, $e_3 > a_3$ and $q \equiv 1 \pmod 7$, we have $c_2 =$ 4, 11, 16, 21, 35, or 41. Since $e_i > a_i$, we have $F_t = 3^{2-1}7^{2-1} = 21$. Then by Theorem 14, we have

$$\begin{aligned}\Phi_{3^2.7^2} &= (x^{21}-((36)^7(4)^3))(x^{21}-(36)^7(11)^3)(x^{21}-(36)^7(16)^3)(x^{21}-(36)^7(21)^3)\\ &\quad (x^{21}-(36)^7(35)^3)(x^{21}-(36)^7(4)^3)(x^{21}-(6)^7(41)^3)(x^{21}-(6)^7(11)^3)\\ &\quad (x^{21}-(6)^7(16)^3)(x^{21}-(6)^7(21)^3)(x^{21}-(6)^7(35)^3)(x^{21}-(6)^7(4)^3)\\ &= (x^{21}-13)(x^{21}-14)(x^{21}-9)(x^{21}-17)(x^{21}-15)(x^{21}-25)(x^{21}-38)\\ &\quad (x^{21}-31)(x^{21}-23)(x^{21}-10)(x^{21}-24)(x^{21}-40)\\ &= (x^{21}+30)(x^{21}+29)(x^{21}+34)(x^{21}+26)(x^{21}+28)(x^{21}+18)(x^{21}+5)\\ &\quad (x^{21}+12)(x^{21}+20)(x^{21}+33)(x^{21}+19)(x^{21}+3).\end{aligned}$$

since $e_1 \le a_1$ and $q \equiv -1 \pmod 4$, we have $u_1 = 32a+19$ or $11a+24$, ${u_1}^q = 11a+8$ or $32a+35$. Also, $e_4 > a_4$ and $q \equiv -1 \pmod{11}$, we have $u_2 = 36a+32$, $31a+17$, $11a+43$, $37a+29$ or $34a+28$, ${u_2}^q = 7a+25$, $12a+5$, $32a+2$, $6a+23$ or $9a+19$.

Since $e_i > a_i$, we have $E_s = 2 \cdot 2^{3-2} \cdot 11^{2-1} = 44$.

Then, by Theorem 15, we have that $\Phi_{2^3.11^2}$ is

$$\Big(x^{44} - \Big((11a+8)^{11}(31a+17)^2 + (32a+19)^{11}(12*a+5)^2\Big)x^{22} +$$
$$\Big((11a+8)^{(11q+11)}(31a+17)^{(2q+2)}\Big)\Big)\Big(x^{44} - \Big((11a+8)^{11}(11a+34)^2$$
$$+(32a+19)^{11}(32a+2)^2\Big)x^{22} + \Big((11a+8)^{(11q+11)}(11a+34)^{(2q+2)}\Big)\Big)$$
$$\Big(x^{44} - \Big((11a+8)^{11}(37a+29)^2 + (32a+19)^{11}(6a+23)^2\Big)x^{22}$$
$$+\Big((11a+8)^{(11q+11)}(37a+29)^{(2q+2)}\Big)\Big)\Big(x^{44} - \Big((11a+8)^{11}$$
$$(34a+28)^2(32a+19)^{11}(9a+19)^2\Big)x^{22} + \Big((11a+8)^{(11q+11)}(34a+28)^{(2q+2)}\Big)\Big)$$
$$\Big(x^{44} - \Big((11a+24)^{11}(36a+32)^2 + (32a+35)^{11}(7a+25)^2\Big)x^{22}$$
$$+\Big((11a+8)^{(11q+11)}(36a+32)^{(2q+2)}\Big)\Big)\Big(x^{44} - \Big((11a+24)^{11}(31a+17)^2$$
$$+(32a+35)^{11}(12a+5)^2\Big)x^{22} + \Big((11a+24)^{(11q+11)}(31a+17)^{(2q+2)}\Big)\Big)$$
$$\Big(x^{44} - \Big((11a+24)^{11}(11a+34)^2 + (32a+35)^{11}(32a+2)^2\Big)x^{22} +$$
$$\Big((11a+24)^{(11q+11)}(11a+34)^{(2q+2)}\Big)\Big)\Big(x^{44} - \Big((11+24)^{11}(37a+29)^2$$
$$+(32a+35)^{11}(6a+23)^2\Big)x^{22} + \Big((11a+24)^{(11q+11)}(37a+29)^{(2q+2)}\Big)\Big)$$
$$\Big(x^{44} - \Big((11a+24)^{11}(34a+28)^2 + (32a+35)^{11}(9a+19)^2\Big)x^{22} +$$
$$\Big((11a+24)^{(11q+11)}(34a+28)^{(2q+2)}\Big)\Big)\Big(x^{44} - \Big((36a+32)^2(32a+19)^{11}$$
$$+(7a+25)^2(11a+8)^{11}\Big)x^{22} + \Big((36a+32)^{(11q+11)}(11a+8)^{(2q+2)}\Big)\Big)$$
$$\Big(x^{44} - \Big((31a+17)^2(32a+19)^{11} + (12a+5)^2(11a+8)^{11}\Big)x^{22} + \Big((31a+17)^{(2q+2)}$$

$$
\begin{aligned}
& (11a+8)^{(11q+11)}\Big)\Big)\Big(x^{44}-\Big((11a+34)^2(32a+19)^{11}+(32a+2)^2\\
& (11a+8)^{11})\Big)x^{22}+\Big((11a+34)^{(2q+2)}(11a+8)^{(11q+11)}\Big)\Big)\Big(x^{44}-\Big((37a+29)^2\\
& (32a+19)^{11}+(6a+23)^2(11a+8)^{11}\Big)x^{22}+\Big((37a+29)^{(2q+2)}(11a+8)^{(11q+11)}\Big)\Big)\\
& \Big(x^{44}-\Big((34a+28)^2(32a+19)^{11}+(9a+19)^2(11a+8)^{11})\Big)x^{22}+\Big((34a+28)^{(2q+2)}\\
& (11a+8)^{(11q+11)}\Big)\Big)\Big(x^{44}-\Big((36a+32)^2(32a+35)^{11}+(7a+25)^2(11a+24)^{11}\Big)x^{22}\\
& +\Big((36a+32)^{(2q+2)}(11a+24)^{(11q+11)}\Big)\Big)\Big(x^{44}-\Big((31a+17)^2(32a+35)^{11}+(12a+5)^2\\
& (11a+24)^{11})\Big)x^{22}+\Big((31a+17)^{(2q+2)}(11a+24)^{(11q+11)}\Big)\Big)\Big(x^{44}-\Big((11a+34)^2\\
& (32a+35)^{11}+(32a+2)^2(11a+24)^{11}\Big)x^{22}+\Big((11a+34)^{(2q+2)}(11a+24)^{(11q+11)}\Big)\Big)\\
& \Big(x^{44}-\Big((37a+29)^2(32a+35)^{11}+(6a+23)^2(11a+24)^{11}\Big)x^{22}+\Big((37a+29)^{(2q+2)}\\
& (11a+24)^{(11q+11)}\Big)\Big)\Big(x^{44}-\Big((34a+28)^2(32a+35)^{11}+(9a+19)^2\\
& (11a+24)^{11}\Big)x^{22}+\Big((34a+28)^{(2q+2)}(11a+24)^{(11q+11)}\Big)\Big)\\
= \;& (x^{44}+42x^{22}+42)(x^{44}+5x^{22}+42)(x^{44}+25x^{22}+42)(x^{44}+29x^{22}+42)\\
& (x^{44}+11x^{22}+42)(x^{44}+34x^{22}+42)(x^{44}+33x^{22}+42)(x^{44}+4x^{22}+42)\\
& (x^{44}+12x^{22}+42)(x^{44}+2x^{22}+42)(x^{44}+9x^{22}+42)(x^{44}+10x^{22}+42)\\
& (x^{44}+39x^{22}+42)(x^{44}+31x^{22}+42)(x^{44}+41x^{22}+42)(x^{44}+x^{22}+42)\\
& (x^{44}+38x^{22}+42)(x^{44}+18x^{22}+42)(x^{44}+14x^{22}+42)(x^{44}+32x^{22}+42).
\end{aligned}
$$

Finally, by Theorem 17, we have

$$
\begin{aligned}
& \Phi_{2^3\cdot 3^2\cdot 7^2\cdot 11^2}\\
= \;& (x^{924}-(29)(1)x^{462}+(29)^{44}42^{21})(x^{924}-(29)(2)x^{462}+(29)^{44}42^{21})\\
& (x^{924}-(29)(4)x^{462}+(29)^{44}42^{21})(x^{924}-(29)(5)x^{462}+(29)^{44}42^{21})\\
& (x^{924}-(29)(9)x^{462}+(29)^{44}42^{21})(x^{924}-(29)(10)x^{462}+(29)^{44}42^{21})
\end{aligned}
$$

$(x^{924} - (29)(11)x^{462} + (29)^{44}42^{21})(x^{924} - (29)(12)x^{462} + (29)^{44}42^{21})$

$(x^{924} - (29)(14)x^{462} + (29)^{44}42^{21})(x^{924} - (29)(18)x^{462} + (29)^{44}42^{21})$

$(x^{924} - (29)(25)x^{462} + (29)^{44}42^{21})(x^{924} - (29)(29)x^{462} + (29)^{44}42^{21})$

$(x^{924} - (29)(31)x^{462} + (29)^{44}42^{21})(x^{924} - (29)(32)x^{462} + (29)^{44}42^{21})$

$(x^{924} - (29)(33)x^{462} + (29)^{44}42^{21})(x^{924} - (29)(34)x^{462} + (29)^{44}42^{21})$

$(x^{924} - (29)(38)x^{462} + (29)^{44}42^{21})(x^{924} - (29)(39)x^{462} + (29)^{44}42^{21})$

$(x^{924} - (29)(41)x^{462} + (29)^{44}42^{21})(x^{924} - (29)(42)x^{462} + (29)^{44}42^{21})$

$(x^{924} - (28)(1)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(2)x^{462} + (28)^{44}42^{21})$

$(x^{924} - (28)(4)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(5)x^{462} + (28)^{44}42^{21})$

$(x^{924} - (28)(9)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(10)x^{462} + (28)^{44}42^{21})$

$(x^{924} - (28)(11)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(12)x^{462} + (28)^{44}42^{21}$

$(x^{924} - (28)(14)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(18)x^{462} + (28)^{44}42^{21})$

$(x^{924} - (28)(25)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(29)x^{462} + (28)^{44}42^{21})$

$(x^{924} - (28)(31)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(32)x^{462} + (28)^{44}42^{21})$

$(x^{924} - (28)(33)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(34)x^{462} + (28)^{44}42^{21})$

$(x^{924} - (28)(38)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(39)x^{462} + (28)^{44}42^{21})$

$(x^{924} - (28)(41)x^{462} + (28)^{44}42^{21})(x^{924} - (28)(42)x^{462} + (28)^{44}42^{21})$

$(x^{924} - (30)(1)x^{462} + (30)^{44}42^{21})(x^{2} - (30)(2)x + (30)^{44}42^{21})$

$(x^{924} - (30)(4)x + (30)^{44}42^{21})(x^{924} - (30)(5)x + (30)^{44}42^{21})$

$(x^{924} - (30)(9)x^{462} + (30)^{44}42^{21})(x^{924} - (30)(10)x^{462} + (30)^{44}42^{21})$

$(x^{924} - (30)(11)x^{462} + (30)^{44}42^{21})(x^{924} - (30)(12)x^{462} + (30)^{44}42^{21})$

$(x^{924} - (30)(14)x^{462} + (30)^{44}42^{21})(x^{924} - (30)(18)x^{462} + (30)^{44}42^{21})$

$(x^{924} - (30)(25)x^{462} + (30)^{44}42^{21})(x^{924} - (30)(29)x^{462} + (30)^{44}42^{21})$

$(x^{924} - (30)(31)x^{462} + (30)^{44}42^{21})(x^{924} - (30)(32)x^{462} + (30)^{44}42^{21})$

$(x^{924} - (30)(33)x^{462} + (30)^{44}42^{21})(x^{924} - (30)(34)x^{462} + (30)^{44}42^{21})$

$(x^{924} - (30)(38)x^{462} + (30)^{44}42^{21})(x^{924} - (30)(39)x^{462} + (30)^{44}42^{21})$

$(x^{924} - (30)(41)x^{462} + (30)^{44}42^{21})(x^{924} - (30)(42)x^{462} + (30)^{44}42^{21})$

$(x^{924} - (26)(1)x^{462} + (26)^{44}42^{21})(x^{924} - (26)(2)x^{462} + (26)^{44}42^{21})$

$(x^{924} - (26)(4)x^{462} + (26)^{44}42^{21})(x^{924} - (26)(5)x^{462} + (26)^{44}42^{21})$

$(x^{924} - (26)(9)x^{462} + (26)^{44}42^{21})(x^{924} - (26)(10)x^{462} + (26)^{44} * 42^{21})$

$(x^{924} - (26)(11)x^{462} + (26)^{44}42^{21})(x^{924} - (26)(12)x^{462} + (26)^{44}42^{21})$

$(x^{924} - (26)(14)x^{462} + (26)^{44}42^{21})(x^{924} - (26)(18)x^{462} + (26)^{44}42^{21})$

$(x^{924} - (26)(25)x^{462} + (26)^{44}42^{21})(x^{924} - (26)(29)x^{462} + (26)^{44}42^{21})$

$(x^{924} - (26)(31)x^{462} + (26)^{44}42^{21})(x^{924} - (26)(32)x^{462} + (26)^{44}42^{21})$

$(x^{924} - (26)(33)x^{462} + (26)^{44}42^{21})(x^{924} - (26)(34)x^{462} + (26)^{44}42^{21})$

$(x^{924} - (26)(38)x + (26)^{44}42^{21})(x^{924} - (26)(39)x^{462} + (26)^{44}42^{21})$

$(x^{924} - (26)(41)x^{462} + (26)^{44}42^{21})(x^{924} - (26)(42)x^{462} + (26)^{44}42^{21})$

$(x^{924} - (34)(1)x^{462} + (34)^{44}42^{21})(x^{924} - (34)(2)x^{462} + (34)^{44}42^{21})$

$(x^{924} - (34)(4)x^{462} + (34)^{44}42^{21})(x^{924} - (34)(5)x^{462} + (34)^{44}42^{21})$

$(x^{924} - (34)(9)x^{462} + (34)^{44}42^{21})(x^{924} - (34)(10)x^{462} + (34)^{44}42^{21})$

$(x^{924} - (34)(11)x^{462} + (34)^{44}42^{21})(x^{924} - (34)(12)x^{462} + (34)^{44}42^{21})$

$(x^{924} - (34)(14)x^{462} + (34)^{44}42^{21})(x^{924} - (34)(18)x^{462} + (34)^{44}42^{21})$

$(x^{924} - (34)(25)x^{462} + (34)^{44}42^{21})(x^{924} - (34)(29)x^{462} + (34)^{44}42^{21})$

$(x^{924} - (34)(31)x^{462} + (34)^{44}42^{21})(x^{924} - (34)(32)x^{462} + (34)^{44}42^{21})$

$(x^{924} - (34)(33)x^{462} + (34)^{44}42^{21})(x^{924} - (34)(34)x^{462} + (34)^{44}42^{21})$

$(x^{924} - (34)(38)x^{462} + (34)^{44}42^{21})(x^{924} - (34)(39)x + (34)^{44}42^{21})$

$(x^{924} - (34)(41)x + (34)^{44}42^{21})(x^{924} - (34)(42)x^{462} + (34)^{44}42^{21})$

$(x^{924} - (18)(1)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(2)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (18)(4)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(5)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (18)(9)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(10)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (18)(11)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(12)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (18)(14)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(18)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (18)(25)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(29)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (18)(31)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(32)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (18)(33)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(34)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (18)(38)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(39)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (18)(41)x^{462} + (18)^{44}42^{21})(x^{924} - (18)(42)x^{462} + (18)^{44}42^{21})$

$(x^{924} - (12)(1)x^{462} + (12)^{44}42^{21})(x^{924} - (12)(2)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (12)(4)x^{462} + (12)^{44}42^{21})(x^{924} - (12)(5)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (12)(9)x^{462} + (12)^{44}42^{21})(x^{924} - (12)(10)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (12)(11)x^{462} + (12)^{44}42^{21})(x^{924} - (12)(12)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (12)(14)x^{462} + (12)^{44}42^{21})(x^{924} - (12)(18)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (12)(25)x^{462} + (12)^{44}42^{21})(x^{924} - (12)(29)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (12)(31)x^{462} + (12)^{44}42^{21})(x9242 - (12)(32)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (12)(33)x^{462} + (12)^{44}42^{21})(x^{924} - (12)(34)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (12)(38)x^{462} + (12)^{44}42^{21})(x^{924} - (12)(39)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (12)(41)x^{462} + (12)^{44} * 42^{21})(x^{924} - (12)(42)x^{462} + (12)^{44}42^{21})$

$(x^{924} - (19)(1)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(2)x^{462} + (19)^{44}42^{21})$

$(x^{924} - (19)(4)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(5)x^{462} + (19)^{44}42^{21})$

$(x^{924} - (19)(9)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(10)x^{462} + (19)^{44}42^{21})$

$(x^{924} - (19)(11)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(12))x^{462} + (19)^{44}42^{21})$

$(x^{924} - (19)(14)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(18)x^{462} + (19)^{44}42^{21})$

$(x^{924} - (19)(25)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(29)x^{462} + (19)^{44}42^{21})$

$(x^{924} - (19)(31)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(32)x^{462} + (19)^{44}42^{21})$

$(x^{924} - (19)(33)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(34)x^{462} + (19)^{44}42^{21})$

$(x^{924} - (19)(38)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(39)x^{462} + (19)^{44}42^{21})$

$(x^{924} - (19)(41)x^{462} + (19)^{44}42^{21})(x^{924} - (19)(42)x^{462} + (19)^{44}42^{21})$

$(x^{924} - (5)(1)x^{462} + (5)^{44}42^{21})(x^{924} - (5)(2)x^{462} + (5)^{44}42^{21})$

$(x^{924} - (5)(4)x^{462} + (5)^{44} * 42^{21})(x^{924} - (5)(5)x^{462} + (5)^{44}42^{21})$

$(x^{924} - (5)(9)x^{462} + (5)^{44}42^{21})(x^{924} - (5)(10)x^{462} + (5)^{44}42^{21})$

$(x^{924} - (5)(11)x^{462} + (5)^{44}42^{21})(x^{924} - (5)(12))x^{462} + (5)^{44}42^{21})$

$(x^{924} - (5)(14)x^{462} + (5)^{44}42^{21})(x^{924} - (5)(18)x^{462} + (5)^{44}42^{21})$

$(x^{924} - (5)(25)x^{462} + (5)^{44}42^{21})(x^{924} - (5)(29)x^{462} + (5)^{44}42^{21})$

$(x^{924} - (5)(31)x^{462} + (5)^{44}42^{21})(x^{924} - (5)(32)x^{462} + (5)^{44}42^{21})$

$(x^{924} - (5)(33)x^{462} + (5)^{44}42^{21})(x^{924} - (5)(34)x^{462} + (5)^{44}42^{21})$

$(x^{924} - (5)(38)x^{462} + (5)^{44}42^{21})(x^{924} - (5)(39)x^{462} + (5)^{44}42^{21})$

$(x^{924} - (5)(41)x^{462} + (5)^{44}42^{21})(x^{924} - (5)(42)x^{462} + (5)^{44}42^{21})$

$(x^{924} - (33)(1)x^{462} + (33)^{44}42^{21})(x^{924} - (33)(2)x^{462} + (33)^{44}42^{21})$

$(x^{924} - (33)(4)x^{462} + (33)^{44} * 42^{21})(x^{924} - (33)(5)x^{462} + (33)^{44}42^{21})$

$(x^{924} - (33)(9)x^{462} + (33)^{44}42^{21})(x^{924} - (33)(10)x^{462} + (33)^{44}42^{21})$

$(x^{924} - (33)(11)x^{462} + (33)^{44}42^{21})(x^{924} - (33)(12))x^{462} + (33)^{44}42^{21})$

$(x^{924} - (33)(14)x^{462} + (33)^{44}42^{21})(x^{924} - (33)(18)x^{462} + (33)^{44}42^{21})$

$(x^{924} - (33)(25)x^{462} + (33)^{44}42^{21})(x^{924} - (33)(29)x^{462} + (33)^{44}42^{21})$

$(x^{924} - (33)(31)x^{462} + (33)^{44} * 42^{21})(x^{924} - (33)(32)x^{462} + (33)^{44}42^{21})$

$(x^{924} - (33)(33)x^{462} + (33)^{44}42^{21})(x^{924} - (33)(34)x^{462} + (33)^{44}42^{21})$

$(x^{924} - (33)(38)x^{462} + (33)^{44}42^{21})(x^{924} - (33)(39)x^{462} + (33)^{44}42^{21})$

$(x^{924} - (33)(41)x^{462} + (33)^{44}42^{21})(x^{924} - (33)(42)x^{462} + (33)^{44}42^{21})$

$(x^{924} - (20)(1)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(2)x^{462} + (20)^{44}42^{21})$

$(x^{924} - (20)(4)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(5)x^{462} + (20)^{44}42^{21})$

$(x^{924} - (20)(9)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(10)x^{462} + (20)^{44}42^{21})$

$(x^{924} - (20)(11)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(12))x^{462} + (20)^{44}42^{21})$

$(x^{924} - (20)(14)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(18)x^{462} + (20)^{44}42^{21})$

$(x^{924} - (20)(25)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(29)x^{462} + (20)^{44}42^{21})$

$(x^{2} - (20)(31)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(32)x^{462} + (20)^{44}42^{21})$

$$
\begin{aligned}
& (x^{924} - (20)(33)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(34)x^{462} + (20)^{44}42^{21}) \\
& (x^{924} - (20)(38)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(39)x^{462} + (20)^{44}42^{21}) \\
& (x^{924} - (20)(41)x^{462} + (20)^{44}42^{21})(x^{924} - (20)(42)x^{462} + (20)^{44}42^{21}) \\
& (x^{924} - (3)(1)x^{462} + (3)^{44}42^{21})(x^{924} - (3)(2)x^{462} + (3)^{44}42^{21}) \\
& (x^{924} - (3)(4)x^{462} + (3)^{44}42^{21})(x^{924} - (3)(5)x^{462} + (3)^{44}42^{21}) \\
& (x^{924} - (3)(9)x^{462} + (3)^{44}42^{21})(x^{924} - (3)(10)x^{462} + (3)^{44}42^{21}) \\
& (x^{924} - (3)(11)x^{462} + (3)^{44}42^{21})(x^{924} - (3)(12))x^{462} + (3)^{44}42^{21}) \\
& (x^{924} - (3)(14)x^{462} + (3)^{44}42^{21})(x^{924} - (3)(18)x^{462} + (3)^{44}42^{21}) \\
& (x^{924} - (3)(25)x^{462} + (3)^{44} * 42^{21})(x^{924} - (3)(29)x^{462} + (3)^{44}42^{21}) \\
& (x^{924} - (3)(31)x^{462} + (3)^{44}42^{21})(x^{924} - (3)(32)x^{462} + (3)^{44}42^{21}) \\
& (x^{924} - (3)(33)x^{462} + (3)^{44}42^{21})(x^{924} - (3)(34)x^{462} + (3)^{44}42^{21}) \\
& (x^{924} - (3)(38)x^{462} + (3)^{44}42^{21})(x^{924} - (3)(39)x^{462} + (3)^{44}42^{21}) \\
& (x^{924} - (3)(41)x^{462} + (3)^{44}42^{21})(x^{924} - (3)(42)x^{462} + (3)^{44}42^{21}) \\
= \; & (x^{924} + 29x^{462} + 19)(x^{924} + 15x^{462} + 19)(x^{924} + 30x^{462} + 19)(x^{924} + 16x^{462} + 19) \\
& (x^{924} + 3x^{462} + 19)(x^{924} + 32x^{462} + 19)(x^{924} + 18x^{462} + 19)(x^{924} + 4x^{462} + 19) \\
& (x^{924} + 19x^{462} + 19)(x^{924} + 6x^{462} + 19)(x^{924} + 37x^{462} + 19)(x^{924} + 24x^{462} + 19) \\
& (x^{924} + 39x^{462} + 19)(x^{924} + 25x^{462} + 19)(x^{924} + 11x^{462} + 19)(x^{924} + 40x^{462} + 19) \\
& (x^{924} + 27x^{462} + 19)(x^{924} + 13x^{462} + 19)(x^{924} + 28x^{462} + 19)(x^{924} + 14x^{462} + 19) \\
& (x^{924} + 28x^{462} + 33)(x^{924} + 13x^{462} + 33)(x^{924} + 26x^{462} + 33)(x^{924} + 11x^{462} + 33) \\
& (x^{924} + 37x^{462} + 33)(x^{924} + 22x^{462} + 33)(x^{924} + 7x^{462} + 33)(x^{924} + 35x^{462} + 33) \\
& (x^{924} + 5x^{462} + 33)(x^{924} + 31x^{462} + 33)(x^{924} + 12x^{462} + 33)(x^{924} + 38x^{462} + 33) \\
& (x^{924} + 8x^{462} + 33)(x^{924} + 36x^{462} + 33)(x^{924} + 21x^{462} + 33)(x^{924} + 6x^{462} + 33) \\
& (x^{924} + 32x^{462} + 33)(x^{924} + 17x^{462} + 33)(x^{924} + 30x^{462} + 33)(x^{924} + 15x^{462} + 33) \\
& (x^{924} + 30x^{462} + 3)(x^{924} + 17x^{462} + 3)(x^{924} + 34x^{462} + 3)(x^{924} + 21x^{462} + 3) \\
& (x^{924} + 12x^{462} + 3)(x^{924} + 42x^{462} + 3)(x^{924} + 29x^{462} + 3)(x^{924} + 16x^{462} + 3) \\
& (x^{924} + 33x^{462} + 3)(x^{924} + 24x^{462} + 3)(x^{924} + 19x^{462} + 3)(x^{924} + 10x^{462} + 3)
\end{aligned}
$$

$(x^{924} + 27x^{462} + 3)(x^{924} + 14x^{462} + 3)(x^{924} + x^{462} + 3)(x^{924} + 31x^{462} + 3)$

$(x^{924} + 22x^{462} + 3)(x^{924} + 9x^{462} + 3)(x^{924} + 26x^{462} + 3)(x^{924} + 13x^{462} + 3)$

$(x^{924} + 26x^{462} + 12)(x^{924} + 9x^{462} + 12)(x^{924} + 18x^{462} + 12)(x^{924} + x^{462} + 12)$

$(x^{924} + 19x^{462} + 12)(x^{924} + 2x^{462} + 12)(x^{924} + 28x^{462} + 12)(x^{924} + 11x^{462} + 12)$

$(x^{924} + 20x^{462} + 12)(x^{924} + 38x^{462} + 12)(x^{924} + 5x^{462} + 12)(x^{924} + 23x^{462} + 12)$

$(x^{924} + 32x^{462} + 12)(x^{924} + 15x^{462} + 12)(x^{924} + 41x^{462} + 12)(x^{924} + 24x^{462} + 12)$

$(x^{924} + 42x^{462} + 12)(x^{924} + 25x^{462} + 12)(x^{924} + 34x^{462} + 12)(x^{924} + 17x^{462} + 12)$

$(x^{924} + 34x^{462} + 5)(x^{4}62 + 25x^{462} + 5)(x^{924} + 7x^{462} + 5)(x^{924} + 41x^{462} + 5)$

$(x^{924} + 5x^{462} + 5)(x^{924} + 39x^{462} + 5)(x^{924} + 30x^{462} + 5)(x^{924} + 21x^{462} + 5)$

$(x^{924} + 3x^{462} + 5)(x^{924} + 10x^{462} + 5)(x^{924} + 33x^{462} + 5)(x^{924} + 40x^{462} + 5)$

$(x^{924} + 22x^{462} + 5)(x^{924} + 13x^{462} + 5)(x^{924} + 4x^{462} + 5)(x^{924} + 38x^{462} + 5)$

$(x^{924} + 2x^{462} + 5)(x^{924} + 36x^{462} + 5)(x^{924} + 18x^{462} + 5)(x^{924} + 9x^{462} + 5)$

$(x^{924} + 18x^{462} + 20)(x^{924} + 36x^{462} + 20)(x^{924} + 29x^{462} + 20), (x^{924} + 4x^{462} + 20)$

$(x^{924} + 33x^{462} + 20)(x^{924} + 8x^{462} + 20)(x^{924} + 26x^{462} + 20)(x^{924} + x^{462} + 20)$

$(x^{924} + 37x^{462} + 20)(x^{924} + 23x^{462} + 20)(x^{924} + 20x^{462} + 20)(x^{924} + 6x^{462}$

$+20)(x^{924} + 42x^{462} + 20)(x^{924} + 17x^{462} + 20)(x^{924} + 35x^{462} + 20)(x^{924} + 10x^{462} + 20)$

$(x^{924} + 39x^{462} + 20)(x^{924} + 14x^{462} + 20)(x^{924} + 7x^{462} + 20)(x^{924} + 25x^{462} + 20)$

$(x^{924} + 12x^{462} + 28)(x^{924} + 24x^{462} + 28)(x^{924} + 5x^{462} + 28)(x^{924} + 17x^{462} + 28)$

$(x^{924} + 22x^{462} + 28)(x^{924} + 34x^{462} + 28)(x^{924} + 3x^{462} + 28)(x^{924} + 15x^{462} + 28)$

$(x^{924} + 39x^{462} + 28)(x^{924} + x^{462} + 28)(x^{924} + 42x^{462} + 28), (x^{924} + 4x^{462} + 28)$

$(x^{924} + 28x^{462} + 28)(x^{924} + 40x^{462} + 28)(x^{924} + 9x^{462} + 28)(x^{924} + 21x^{462} + 28)$

$(x^{924} + 26x^{462} + 28)(x^{924} + 38x^{462} + 28)(x^{924} + 19x^{462} + 28)(x^{924} + 31x^{462} + 28)$

$(x^{924} + 19x^{462} + 26)(x^{924} + 38x^{462} + 26)(x^{924} + 33x^{462} + 26)(x^{924} + 9x^{462} + 26)$

$(x^{924} + 42x^{462} + 26)(x^{924} + 18x^{462} + 26)(x^{924} + 37x^{462} + 26)(x^{924} + 13x^{462} + 26)$

$(x^{924} + 8x^{462} + 26)(x^{924} + 41x^{462} + 26)(x^{924} + 2x^{462} + 26)(x^{924} + 35x^{462} + 26)$

$(x^{924} + 30x^{462} + 26)(x^{924} + 6x^{462} + 26)(x^{924} + 25x^{462} + 26)(x^{924} + x^{462} + 26)$

$(x^{924} + 34x^{462} + 26)(x^{924} + 10x^{462} + 26)(x^{924} + 5x^{462} + 26)(x^{924} + 24x^{462} + 26)$

$$(x^{924}+5x^{462}+18)(x^{924}+10x^{462}+18(x^{924}+20x^{462}+18)(x^{924}+25x^{462}+18)$$
$$(x^{924}+2x^{462}+18)(x^{924}+7x^{462}+18)(x^{924}+12x^{462}+18)(x^{924}+17x^{462}+18)$$
$$(x^{924}+27x^{462}+18)(x^{924}+4x^{462}+18)(x^{924}+39x^{462}+18)(x^{924}+16x^{462}+18)$$
$$(x^{924}+26x^{462}+18)(x^{924}+31x^{462}+18)(x^{924}+36x^{462}+18)(x^{924}+41x^{462}+18)$$
$$(x^{924}+18x^{462}+18)(x^{924}+23x^{462}+18)(x^{924}+33x^{462}+18)(x^{924}+38x^{462}+18)$$
$$(x^{924}+33x^{462}+29)(x^{924}+23x^{462}+29)(x^{924}+3x^{462}+29)(x^{924}+36x^{462}+29)$$
$$(x^{924}+39x^{462}+29)(x^{924}+29x^{462}+29)(x^{924}+19x^{462}+29)(x^{924}+9x^{462}+29)$$
$$(x^{924}+32x^{462}+29)(x^{924}+35x^{462}+29)(x^{924}+8x^{462}+29)(x^{924}+11x^{462}+29)$$
$$(x^{924}+34x^{462}+29)(x^{924}+24x^{462}+29)(x^{924}+14x^{462}+29)(x^{924}+4x^{462}+29)$$
$$(x^{924}+7x^{462}+29)(x^{924}+40x^{462}+29)(x^{924}+20x^{462}+29)(x^{924}+10x^{462}+29)$$
$$(x^{924}+20x^{462}+30)(x^{924}+40x^{462}+30)(x^{924}+37x^{462}+30)(x^{924}+14x^{462}+30)$$
$$(x^{924}+8x^{462}+30)(x^{924}+28x^{462}+30)(x^{924}+5x^{462}+30)(x^{924}+25x^{462}+30)$$
$$(x^{924}+22x^{462}+30)(x^{924}+16x^{462}+30)(x^{924}+27x^{462}+30)(x^{924}+21x^{462}+30)$$
$$(x^{924}+18x^{462}+30)(x^{924}+38x^{462}+30)(x^{924}+15x^{462}+30)(x^{924}+35x^{462}+30)$$
$$(x^{924}+29x^{462}+30)(x^{924}+6x^{462}+30)(x^{924}+3x^{462}+30)(x^{924}+23x^{462}+30)$$
$$(x^{924}+3x^{462}+34)(x^{924}+6x^{462}+34)(x^{924}+12x^{462}+34)(x^{924}+15x^{462}+34)$$
$$(x^{924}+27x^{462}+34)(x^{924}+30x^{462}+34)(x^{924}+33x^{462}+34)(x^{924}+36x^{462}+34)$$
$$(x^{924}+42x^{462}+34)(x^{924}+11x^{462}+34)(x^{924}+32x^{462}+34)(x^{924}+x^{462}+34)$$
$$(x^{924}+7x^{462}+34)(x^{924}+10x^{462}+34)(x^{924}+13x^{462}+34)(x^{924}+16x^{462}+34)$$
$$(x^{924}+28x^{462}+34)(x^{924}+31x^{462}+34)(x^{924}+37x^{462}+34)(x^{924}+40x^{462}+34).$$

Those examples demonstrate the results of factorization of cyclotomic polynomials Φ_n over $\mathbb{F}_q$ such that q is congruent to ± 1 modulo each prime divisor of n.

5 Conclusion

Let $\mathbb{F}_q$ be a finite field with q elements, and let $q = p^e$ be a power of prime number p.Let $n = {r_0}^{e_0}{r_1}^{e_1}\cdots{r_{t+s}}^{e_{t+s}}$ be the prime factorization such that $r_0 = 2$ and all other r_i are distinct odd primes for $1 \leq i \leq t+s$. Let $\Phi_n(x)$ denote the nth cyclotomic polynomial. The main focus of this thesis is to give the irreducible factorization of cyclotomic polynomial Φ_n over finite field $\mathbb{F}_q$ when $q \equiv \pm 1 \pmod{r_i}$ for all $0 \leq i \leq t+s$. Under our assumptions, each $\Phi_{r_i^{e_i}}$ can be factorized into irreducbile binomials or trinomials. Through the factorization of composed products of irreducible binomials and trinomials, we obtain the explicit irreducible factorizaton of Φ_n. The main results are summerized in three cases: 1) n is odd; 2) n is even and $q \equiv 1 \pmod 4$; 3) n is even and $q \equiv 3 \pmod 4$. Some concrete examples are also provided to demonstrate our results. We also notice that there is a recent paper [15] to appear in Finite Fields Appl. In [15], Wu, Yue and Fan obtained the explicit factorization of $x^n - 1$ such that $rad(n) \nmid q-1$ and $rad(n) \mid q^w - 1$ where w is a prime number. They achieved this goal by combining irreducible factors of $x^n - 1$ over $\mathbb{F}_{q^w}$. Our focus is on the factorization of n-th cyclotomic polynomials and our approach is to use composed products of irreducible binomials and trinomials. In conclusion, we have advanced on the problem of factoring cyclotomic polynomials for some choices of n's even though the problem still open for general n.

References

[1] Blacke, I. F., Gao, S., Mullin, R. C. (1993), Explicit factorization of $x^{2^k}+1$ over $\mathbb{F}_p$ with prime $p \equiv 3 \pmod 4$ *University of Waterloo*, 89-94

[2] Brawley, J. F., Brown, D. (1993), Composed products and module polynomials over finite fields *Discrete Mathematics*, **117**, 41-56

[3] Brawley, J. F., Carlitz, L. (1987), Irreducible and the composed product for polynomials over finite field. *Discrete Mathematics*, **65**, 115-139

[4] Chen, B., Li, L., Tuerhong, R. (2013), Explicit factorization of $X^{2^m p^n}-1$ over finite fields. *Finite Fields and Their Applications*, **24**, 95-104

[5] Fitzgerald, R., W., Yucas, J. L. (2007). Explicit factorization of cyclotomic and Dickson polynomials over finite fields. *J. Southern Illinois University Carbondale*, 01-10.

[6] Lidl, R., Niederreiter, H. (1997). Finite Fields, 2nd edn. *Cambridge University Press.*

[7] Van Lint J.H. (1998), Introduction to Coding Theory, 3rd edn. *Graduate Texts in Mathematics*, **86**. Springer, New York.

[8] Martinez, F. E. B., Vergara, C. R. G., de Oliveira, L. B. (2015), Explicit factorization of $x^n-1 \in \mathbb{F}_q[x]$, *Des Codes Cryptography* **77** 277-286.

[9] Mills, D. (2001), Factorization of root-based polynomial composition *Discrete Mathematics* **240**, 161-173.

[10] Meyn, H. (1996), Factorization of cyclotomic polynomial $x^{2n}+1$ over finite fields. *Finite Field and Their Applications* **2**, 439-442

[11] Tuxanidy, A., Wang, Q. (2013), Composed product and factors of cylcotomic polynomials over finite fields. *Des. Codes Cryptography* **69**, 203-231.

[12] Wang, Z. (2003), Lectures on Finite Fields and Galois Rings. *World Scientific Publishing Co.*

[13] Wang, L., Wang, Q. (2012), On explicit factors of cyclotomic polynomials over finite fields *Des. Codes Cryptography* **63**, 87-104.

[14] Wu, Y., Yue, Q., Fan, S. (2018), Further factorization of $x^n - 1$ over a finite field, *Finite Fields Appl.* **54**, 197-215.

[15] Wu, H., Zhu, L., Feng, R., Yang, S. (2017), Explicit factorization of cyclotomic polynomials over finite fields *Des. Codes Cryptography* **63**, 197-217.