Modified Cyclotomic Polynomial and Its Irreducibility

Ki-Suk Lee, Sung-Mo Yang and Soon-Mo Jung

1 Department of Mathematics Education, Korea National University of Education, Cheongju 28173, Korea; smyang@knue.ac.kr
2 College of Science and Technology, Hongik University, Sejong 30016, Korea; smjung@hongik.ac.kr
* Correspondence: ksleeknue@gmail.com; Tel.: +82-43-230-3753
† These authors contributed equally to this work.

Received: 28 January 2020; Accepted: 1 March 2020; Published: 4 March 2020

Abstract: Finding irreducible polynomials over \( \mathbb{Q} \) (or over \( \mathbb{Z} \)) is not always easy. However, it is well-known that the \( m \)th cyclotomic polynomials are irreducible over \( \mathbb{Q} \). In this paper, we define the \( m \)th modified cyclotomic polynomials and we get more irreducible polynomials over \( \mathbb{Q} \) systematically by using the modified cyclotomic polynomials. Since not all modified cyclotomic polynomials are irreducible, a criterion to decide the irreducibility of those polynomials is studied. Also, we count the number of irreducible \( m \)th modified cyclotomic polynomials when \( m = p^a \) with \( p \) a prime number and \( a \) a positive integer.

Keywords: irreducible polynomial; cyclotomic polynomial; modified cyclotomic polynomial; semi-cyclotomic polynomial; multiplicative group

1. Introduction

For each \( m \in \mathbb{N} \), the \( m \)th cyclotomic polynomial is the unique irreducible polynomial with integer coefficients which is a divisor of \( x^m - 1 \) and is not a divisor of \( x^k - 1 \) for all \( k < m \). Its roots are all \( m \)th primitive roots of unity \( e^{2\pi i k / m} \), where \( 0 < k \leq m \) and \( k \) is relatively prime to \( m \). More precisely, the \( m \)th cyclotomic polynomial \( \Phi_m(x) = \prod_{k \in \mathbb{Z}_m^{*}} (x - e^{2\pi i k / m}) \) is always irreducible over \( \mathbb{Q} \). However, there are more irreducible polynomials over \( \mathbb{Q} \), which are not the cyclotomic polynomials.

In this paper, we generalize the definition of cyclotomic polynomials to introduce a new kind of polynomials in \( \mathbb{Z}[x] \), which is related to subgroups of the multiplicative group \( \mathbb{Z}_m^{*} \).

Let \( m \geq 2 \) be an integer. A positive integer \( g \) is called a primitive root modulo \( m \) if each positive integer \( a \) that is relatively prime to \( m \) is congruent to a power of \( g \) modulo \( m \). In other words, \( g \) is called a primitive root modulo \( m \) if for any integer \( a \) relatively prime to \( m \), there exists a positive integer \( k \) such that \( g^k \equiv a \pmod{m} \). Such a \( k \) is said to be the index of \( a \), denoted by \( k = \text{ind}_g a \).

Denote by \( e \) the identity element of a group \( G \). If \( a \in G \) and there exists the smallest positive integer \( k \) such that \( a^k = e \), \( a \) is said to be of order \( k \) in \( G \). We denote the order of \( a \in G \) by \( |a| \). Notice that if \( a \in G \), there is a subgroup of \( G \), \( \langle a \rangle = \{a^k : k \in \mathbb{Z} \} \). This subgroup is said to be cyclic, and \( a \) is called a generator of this cyclic (sub)group.

It is well-known that a positive integer \( m \) has a primitive root if and only if \( m \) is one of the following forms: \( 2, 4, p^a, 2p^a \), where \( p \) is an odd prime and \( a \) is a positive integer (see [1], Theorem 20.4). That is, the multiplicative group \( \mathbb{Z}_m^{*} = \{a \in \mathbb{Z}_m : (a, m) = 1 \} \) is cyclic if and only if \( m \) is one of \( 2, 4, p^a, \) and \( 2p^a \). Here \( (a, m) \) denotes the greatest common divisor of \( a \) and \( m \). Likewise, we denote by \( |a, m| \) the least common multiple of \( a \) and \( m \).

Throughout this paper, we give following notations for the convenience.
(a) If $G$ is a finite cyclic group where one of its generators is $a \in G$, we get the following formula for the order of $a^i \in G$ (see [2], Theorem 7.9):

$$|a^i| = \frac{|a|}{(|a|, i)}.$$

(b) Let $\tau(m)$ denote the total number of positive factors of an integer $m$ and let $\varphi(m)$ be the Euler's phi function, which is the order of $\mathbb{Z}_m^*$.

We notice that there is no primitive root modulo $2^a$ with $a \geq 3$. In Section 3, we introduce the structure of $\mathbb{Z}_m^*$ when $a \geq 3$.

The goals of our paper are

(i) to study a criterion to check the irreducibility of modified cyclotomic polynomials;
(ii) to count the number of irreducible $m$th modified cyclotomic polynomials.

The main results of this paper are Theorems 6 and 9 and Corollary 1. We prove in Theorem 6 that if $m = 2^a$ for some integer $a \geq 3$, then there are only 4 irreducible $m$th modified cyclotomic polynomials. And Theorem 9 states that if $p$ is an odd prime and $m = p^a$ for some integer $a \geq 2$, then there are exactly $\tau(p - 1) + 1$ irreducible $m$th modified cyclotomic polynomials. On the other hand, we can also induce Theorems 7 and 8 from Theorem 9.

2. Modified Cyclotomic Polynomials

It is well-known that every cyclotomic polynomial is irreducible over $\mathbb{Q}$ and all of its coefficients are integral (see [3], Theorem 3.1, Chapter IV and [4], Theorem 1.2). The authors of [4] defined the $m$th 'semi-cyclotomic polynomial' from the notion of the cyclotomic polynomial, which is denoted by $\Psi_m(x)$ throughout this paper. We give the definition of a semi-cyclotomic polynomial as follows.

**Definition 1.** We assume that $m \geq 3$ is an integer. Let $\zeta = e^{2\pi i/m} = \cos \left(\frac{2\pi}{m}\right) + is\left(\frac{2\pi}{m}\right)$, $s = \frac{\varphi(m)}{2}$, and let $\{\pm r_1, \ldots, \pm r_s\}$ denote a reduced residue system modulo $m$. The $m$th semi-cyclotomic polynomial $\Psi_m(x)$ is defined as

$$\Psi_m(x) = \prod_{j=1}^{s} \left(x - (\zeta^j + \zeta^{-j})\right).$$

**Example 1.** There are a few examples of $m$th semi-cyclotomic polynomials as we see below.

| $m$ | $\zeta$ | $\Psi_m(x)$ |
|-----|---------|-------------|
| 3   | $e^{2\pi i/3}$ | $x - (\zeta + \zeta^2) = x + 1$ |
| 4   | $e^{2\pi i/4}$ | $x - (\zeta + \zeta^3) = x$ |
| 5   | $e^{2\pi i/5}$ | $(x - (\zeta + \zeta^4))(x - (\zeta^2 + \zeta^3)) = x^2 + x - 1$ |
| 6   | $e^{2\pi i/6}$ | $x - (\zeta + \zeta^5) = x - 1$ |
| 7   | $e^{2\pi i/7}$ | $(x - (\zeta + \zeta^6))(x - (\zeta^2 + \zeta^5))(x - (\zeta^3 + \zeta^4)) = x^3 + x^2 - 2x + 1$ |
| 8   | $e^{2\pi i/8}$ | $(x - (\zeta + \zeta^7))(x - (\zeta^3 + \zeta^5)) = x^2 - 2$ |

For instance, we calculate $\Psi_8(x)$ with $\zeta = e^{2\pi i/8}$. Since $\zeta$ is a root of the 8th cyclotomic polynomial $\Phi_8(x) = x^4 + 1$, we have $\zeta^4 = -1$. The rest of the calculation is

$$\Psi_8(x) = \left(x - (\zeta + \zeta^7)\right)\left(x - (\zeta^3 + \zeta^5)\right)$$

$$= x^2 - (\zeta + \zeta^7 + \zeta^3 + \zeta^5)x + (\zeta + \zeta^7)(\zeta^3 + \zeta^5)$$

$$= x^2 - (\zeta - \zeta^3 + \zeta^5 - \zeta)x + (-1 - \zeta^2 + \zeta^2 - 1)$$

$$= x^2 - 2.$$
All six semi-cyclotomic polynomials listed in the table above are in \( \mathbb{Z}[x] \). Further, they are all irreducible over \( \mathbb{Q} \), because \( \Psi_5(x) \), \( \Psi_7(x) \), and \( \Psi_8(x) \) have degrees 2 or 3, and they have no rational roots ([2], Corollary 4.19 and Theorem 4.21).

In general, every \( \Psi_m(x) \) is irreducible over \( \mathbb{Q} \), and each coefficient of \( \Psi_m(x) \) is integral (see [4], Theorems 2.2 and 2.4). In a continuing study, another kind of polynomial was defined with a motivation from the notion of semi-cyclotomic polynomial. The author of [5] defined \( n \)th ‘modified semi-cyclotomic polynomial’ for specific motivation from the notion of semi-cyclotomic polynomial. The author of [5] defined \( n \)th modified semi-cyclotomic polynomial \( \Psi_m(x) \) is defined as

\[
\Psi_m(x) = \prod_{j=1}^s \left( x^2 - \zeta^{2j} - \zeta^{-2j} + 2 \right).
\]

**Example 2.** From Definition 2, the \( n \)th modified semi-cyclotomic polynomial is the product of quadratic polynomials. Furthermore, if we compare Definitions 1 and 2, it follows that \( \Psi_m(x) \) has a factor \( x^2 - 4 \cos^2 \left( \frac{\phi(m)}{2m} \right) + 4 \) while \( \Psi_m(x) \) has a factor \( x^2 - 4 \cos^2 \left( \frac{\phi(m)}{2m} \right) \), where those factors belong to \( \mathbb{R}[x] \).

For instance, let \( \zeta \) be a primitive 16th root of unity. We can decompose \( \Psi_{16}(x) = x^4 - 4x^2 + 2 = (x^2 - 2 - \sqrt{2})(x^2 - 2 + \sqrt{2}) \) in \( \mathbb{R}[x] \). Then the 16th modified semi-cyclotomic polynomial is calculated by

\[
\Psi_{16}(x) = \left((x^2 - 2 - \sqrt{2}) + 4\right)\left((x^2 - 2 + \sqrt{2}) + 4\right) = (x^2 + 2 - \sqrt{2})(x^2 + 2 + \sqrt{2}) = x^4 + 4x^2 + 2.
\]

The following theorem states about a property of subgroups of the cyclic group \( \mathbb{Z}_m^* \) when \( m \) has a primitive root.

**Lemma 1.** Let \( m \) be a positive integer which has a primitive root \( g \), \( d \) be a positive divisor of \( \phi(m) \), and \( a \in \mathbb{Z}_m^* \). Then the congruence \( t^d \equiv a \pmod{m} \) has a solution if and only if

\[
\frac{\phi(m)}{d} \equiv 1 \pmod{m}.
\]

If the congruence has a solution, it has exactly \( d \) distinct solutions.

**Proof.** Since \( m \) has a primitive root \( g \) modulo \( m \), the congruence \( t^d \equiv a \pmod{m} \) is equivalent to the congruence \( dX \equiv A \pmod{\phi(m)} \) with \( X = \text{ind}_g a \) and \( A = \text{ind}_g a \). Note that \( d = (d, \phi(m)) \). Then \( dX \equiv A \pmod{\phi(m)} \) has a solution if and only if \( d \mid A \) ([11], Theorem 3.1).

We denote \( \frac{\phi(m)}{d} \equiv e \). Then it follows that \( d \mid A \) if and only if \( de \mid eA \). By ([11], Definition 17.1), we obtain \( eA \equiv \text{ind}_e a^e \pmod{\phi(m)} \). That is, \( d \mid A \) holds if and only if \( \phi(m) \mid eA \), which is equivalent to \( a^e \equiv 1 \pmod{\phi(m)} \). Consequently, the congruence \( t^d \equiv a \pmod{m} \) has a solution if and only if \( a^e \equiv 1 \pmod{\phi(m)} \), and it has \( d \) distinct solutions if they exist. \( \square \)
Like the semi-cyclotomic polynomial, for every \( m = 4n \) \((n > 1)\), \( \Psi_m(x) \) is in \( \mathbb{Z}[x] \) and it is irreducible over \( \mathbb{Q} \) ([5], Theorems 1.4.5 and 1.4.6). The following lemma has been proved in [5], so we guide the reader to refer to the proof of ([5], Lemma 1.4.3).

**Lemma 2.** ([5], Lemma 1.4.3) Assume that \( m = 4n \) for some integer \( n > 1 \). Let \( \zeta = e^{\frac{2\pi i}{m}} = \cos\left(\frac{2\pi}{m}\right) + i\sin\left(\frac{2\pi}{m}\right) \), \( u_j = \zeta^j - \zeta^{-j} \), and \( v_j = -u_j \) for \( j \in \{1, \ldots, s\} \) with \( s = \frac{q(m)}{4} \). Then \( u_j \) and \( v_k \) are all distinct complex numbers for every distinct \( j \) and \( k \).

In terms of Lemma 2, \( \Psi_m(x) = \prod_{j=1}^{s} (x - u_j)(x - v_j) \). The following theorems show that all the coefficients of modified semi-cyclotomic polynomials are integral and the modified semi-cyclotomic polynomials are irreducible over \( \mathbb{Q} \).

**Theorem 1.** ([5], Theorems 1.4.4 and 1.4.5) For any positive integer \( m = 4n \) with \( n > 1 \), \( \Psi_m(x) \in \mathbb{Z}[x] \).

**Proof.** Let us denote by \( \zeta \) a primitive \( m \)-th root of unity. And let \( K = \mathbb{Q}(\zeta) \).

First we show that \( \Psi_m(x) \) belongs to \( \mathbb{Q}[x] \). Assume that \( r \) is an arbitrary element of \( \mathbb{Z}_m^* \) and we define a \( \mathbb{Q} \)-isomorphism \( \phi_r \) in Galois group \( G(K/\mathbb{Q}) \) by \( \phi_r(\zeta) = \zeta^r \) and \( \phi_r(q) = q \) for all \( q \in \mathbb{Q} \). We use the same definitions of \( s, r, u_j, \) and \( v_j \) from Definition 2 and Lemma 2.

Assume that \( \phi_r(u_j) = \phi_r(u_k) \) holds for all \( j, k \in \{1, \ldots, s\} \). The calculation \( \phi_r(u_j) = \phi_r(\zeta^j - \zeta^{-j}) = \zeta^{rj} - \zeta^{-rj} \) deduces to \( \zeta^{rj} - \zeta^{-rj} = \zeta^{rk} - \zeta^{-rk} \).

Suppose that \( rr_j \equiv r_{j_2} \pmod{m} \) and \( rr_k \equiv r_{k_2} \pmod{m} \) for some \( j_2, k_2 \in \{1, \ldots, s\} \) without loss of generality. Then

\[
\phi_r(u_j) = \phi_r(u_k) \iff \zeta^{rj} - \zeta^{-rj} = \zeta^{rk} - \zeta^{-rk}
\]

But this is contrary to Lemma 2, so we obtain \( rr_j \equiv r_{j_2} \pmod{m} \) and \( rr_k \equiv r_{k_2} \pmod{m} \) for some \( j_1, k_1 \in \{1, \ldots, s\} \). Therefore, we get either \( u_j = u_{k_1} \) or \( v_j = v_{k_1} \), and it follows that \( r_j \equiv r_{k_1} \pmod{m} \) by Lemma 2.

\[
\phi_r(u_j) = \phi_r(u_k) \iff \zeta^{rj} - \zeta^{-rj} = \zeta^{rk} - \zeta^{-rk}
\]

Hence, \( u_j = u_k \) and \( v_j = v_k \), which implies that \( \phi_r \) is one-to-one on \( S = \bigcup_{j=1}^{s} \{u_j, v_j\} \). This proves that \( \phi_r \mid \mathbb{Z} : S \rightarrow S \) is a permutation on \( S \) for arbitrary \( r \). Since we have \( \Psi_m(x) = \prod_{j=1}^{s} (x - u_j)(x - v_j) \), every coefficient of \( \Psi_m(x) \) is fixed by any \( \phi_r \). In other words, all coefficients of \( \Psi_m(x) \) belong to the fixed field of \( G(K/\mathbb{Q}) \) and the fixed field is obviously \( \mathbb{Q} \) by ([2], Theorem 12.9).

We proved that \( \Psi_m(x) \in \mathbb{Q}[x] \), but in fact, \( \Psi_m(x) \in \mathbb{Z}[x] \). Note that \( \phi_r(x) \) is the irreducible monic polynomial with the minimal degree of \( \zeta \) over \( \mathbb{Q} \) and \( K \) is a vector space over \( \mathbb{Q} \), whose basis is \( B = \{1, \zeta, \ldots, \zeta^{q(m)-1}\} \) (see [2], Theorem 11.7). When \( \Phi_m(x) = x^{q(m)} + a_{q(m)-1}x^{q(m)-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x] \), then we get \( \zeta^{q(m)} = -a_{q(m)-1}\zeta^{q(m)-1} - \cdots - a_1\zeta - a_0 \) since \( \zeta \) is a root of \( \Phi_m(x) \). Then if \( y \) is an arbitrary coefficient of \( \Psi_m(x) \), \( y \) can be expressed as \( b_0 + b_1\zeta + \cdots + b_{q(m)-1}\zeta^{q(m)-1} \in \mathbb{Z}[x] \), because \( y \) is the sum of products of \( \pm u_j's \) for some \( j's \) and \( \zeta^{q(m)} = -a_{q(m)-1}\zeta^{q(m)-1} - \cdots - a_1\zeta - a_0 \). Hence, \( (y - b_0) + b_1\zeta + \cdots + b_{q(m)-1}\zeta^{q(m)-1} = 0 \) implies \( y - b_0 = b_1 = \cdots = b_{q(m)-1} = 0 \) because of
the linear independence of $B$. In particular, $y = b_0$ is an integer. Thus every coefficient of $\Psi_m^*(x)$ is integral. □

The following theorem has been proved in [5], so we guide the reader to refer to the proof of ([5], Theorem 1.4.6).

**Theorem 2.** ([5], Theorem 1.4.6) For any positive integer $m = 4n$ with $n > 1$, $\Psi_m^*(x)$ is irreducible over $\mathbb{Q}$.

Later, a more general notion came out from the notions of $\Phi_m(x)$, $\Psi_m(x)$, and $\Psi_m^*(x)$. This notion is a new kind of polynomial through prior researches [5–7], which is initially defined and named by ‘Galois polynomial’ in [6]. We rename this notion (Galois polynomial) to ‘modified cyclotomic polynomial’.

**Definition 3.** $\zeta = e^{2\pi i} = \cos \left(\frac{2\pi}{m}\right) + i \sin \left(\frac{2\pi}{m}\right)$. Suppose that $H$ is a subgroup of $\mathbb{Z}_m^*$. And let $\ell = [\mathbb{Z}_m^* : H]$, $\mathbb{Z}_m^*/H = \{h_1H, \ldots, h_lH\}$, and $a_j = \sum_{h \in H} \zeta^{hj} (j \in \{1, \ldots, \ell\})$. The $m$th modified cyclotomic polynomial of $H$ is denoted by $\Lambda_{m,H}(x)$, and it is defined as $\Lambda_{m,H}(x) = \prod_{j=1}^{\ell} (x - a_j)$.

**Example 4.** We deal with an example of $7$th modified cyclotomic polynomials. There are $4$ subgroups of $\mathbb{Z}_7^*$: $H_1 = \{1\}$, $H_2 = \{6\}$, $H_3 = \{2\}$, and $H_4 = \mathbb{Z}_7^*$. If $\zeta$ is a primitive $7$th root of unity, we obtain $\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$ and $\zeta^7 = 1$.

(i) The corresponding quotient group is $\mathbb{Z}_7^*/H_1 = \{1H_1, 2H_1, \ldots, 6H_1\}$.

Then we have $\Lambda_{7,H_1}(x) = \prod_{j=1}^{6} (x - \zeta^j) = \Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

(ii) $\mathbb{Z}_7^*/H_2 = \{1H_2, 2H_2, 3H_2\}$, where $2H_2 = \{2, 5\}$ and $3H_2 = \{3, 4\}$.

So, we get $\Lambda_{7,H_2}(x) = \prod_{j=1}^{3} (x - (\zeta^j + \zeta^{-j})) = \Psi_7(x) = x^3 + x^2 - 2x - 1$.

(iii) It follows that $\mathbb{Z}_7^*/H_3 = \{1H_3, 3H_3\}$, where $3H_3 = \{3, 5, 6\}$.

Subsequently, $\Lambda_{7,H_3}(x) = (x - (\zeta + \zeta^2 + \zeta^4))(x - (\zeta^3 + \zeta^5 + \zeta^6)) = x^2 + x + 2$.

(iv) Note that $\mathbb{Z}_7^*/H_4$ is the trivial group. It follows from the fact $\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta = -1$ that $\Lambda_{7,H_4}(x) = x - \sum_{j=1}^{6} \zeta^j = x + 1$.

In general, $\Lambda_{m,H}(x)$ is a polynomial of degree $\ell = [\mathbb{Z}_m^*: H]$ and all of its coefficients are integral (see [6], Theorems 2.2 and 2.3). By Definition 3, we know that $\Phi_m(x) = \Lambda_{m,(1)}(x)$ and $\Psi_m^*(x) = \Lambda_{m,(1)}(x)$. When we denote the subgroup $\hat{H} = \{1, 2n - 1\}$ of $\mathbb{Z}_m^*$ where $m = 4n$ ($n > 1$), it follows that $\Psi_m^*(x) = \Lambda_{m,\hat{H}}(x)$.

If $H$ equals the whole group $\mathbb{Z}_m^*$, the corresponding polynomial $\Lambda_{m,H}(x)$ is $x - q$ with $q = \sum_{h \in H} \zeta^h$ where $\zeta$ is a primitive $m$th root of unity. We give examples of $\Lambda_{m,\mathbb{Z}_m^*}(x)$ when $m$ is a power of a prime number as follows.

**Example 4.** When $\alpha \geq 3$ and $\zeta = e^{2\pi i/\alpha}$, we obtain the formula of $\Phi_{2^\alpha}(x)$ inductively:

$$\Phi_{2^\alpha}(x) = \frac{x^{2^\alpha} - 1}{\Phi_2(x)\Phi_2(x) \cdots \Phi_{2^{\alpha-1}}(x)} = \frac{(x^{2^{\alpha-1}})^2 - 1}{x^{2^{\alpha-1}} - 1} = x^{2^{\alpha-1}} + 1.$$ We get $\sum_{k \in \mathbb{Z}_{2^\alpha}^*} \zeta^k = 0$ by definition of the $2\alpha$th cyclotomic polynomial and $\Lambda_{2^\alpha,\mathbb{Z}_{2^\alpha}^*}(x) = x$.

We also give the form of $\Lambda_{m,\mathbb{Z}_m^*}(x)$, when $\alpha$ is a positive integer and $m = p^\alpha$ for some odd prime $p$. We denote a primitive $m$th root of unity by $\zeta$. 


Theorem 3. Let $\alpha = 1$. Then we have

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

by the definition of the $m$th cyclotomic polynomial. So, according to Definition 3, we get

$$\sum_{k \in \mathbb{Z}_m} \zeta^k = \zeta + \cdots + \zeta^{p(m)-1} = -1.$$ 

And it follows that $\Lambda_{m, \mathbb{Z}_m} = x + 1$.

(ii) Let $\alpha \geq 2$. We obtain a following formula by the inductive process:

$$\Phi_p(x) = \Phi_1(x) \Phi_p(x) \cdots \Phi_{p-1}(x) = \frac{(x^{p-1} - 1)}{(x^{p-1} - 1)} = \Phi_p(x^{p-1})$$

Note that $p^{p-1}(p-1) > p^{1}(p-1) - 1 > p^{1}(p-1) - p^{1}(p-2)$. So, we obtain $\sum_{k \in \mathbb{Z}_m} \zeta^k = \zeta + \cdots + \zeta^{p(m)-1} = 0$ and $\Lambda_{m, \mathbb{Z}_m} = x$.

On the other hand, [5] shows the comparison of the coefficients of both $m$th and $2m$th modified cyclotomic polynomials for odd $m$. Hence, we guide the reader to refer to ([5], Theorem 2.3.1) for the proof of the following theorem.

**Theorem 3.** ([5], Theorem 2.3.1) For every odd positive integer $m$ and every subgroup $H = \{h_1, \ldots, h_s\}$ of $\mathbb{Z}_m^*$, let $\Lambda_{m, H}(x)$ be expressed as $\sum_{j=0}^{\ell} c_j x^j = c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \cdots + c_1 x + c_0$, where $\ell = \left[ \mathbb{Z}_m^* : H \right]$ and $\mathbb{Z}_m^* / H = \{k_1 H, \ldots, k_\ell H\}$. Then

$$\Lambda_{2m, \hat{H}}(x) = \sum_{j=0}^{\ell} (-1)^j c_{\ell-j} x^j = c_\ell x^\ell - c_{\ell-1} x^{\ell-1} + \cdots + (-1)^{\ell-1} c_1 x + (-1) \ell c_0,$$

where $f : \mathbb{Z}_m^* \rightarrow \mathbb{Z}_{2m}^*$ is defined by $f(kh_j) = 2kh_j + m$ for $k \in \{k_1, \ldots, k_\ell\}$ and $j \in \{1, \ldots, s\}$, and $\hat{H} = f(k^* H)$ for $k^* \in \{k_1, \ldots, k_\ell\}$ with $1 \in f(k^* H)$.

**Example 5.** We use the notations $k^*$ and $\hat{H}$, which are given in the proof of Theorem 3. Let $m = 9$ and let $H_j$ be a subgroup of $\mathbb{Z}_9^*$ for each $j$ as below. Each corresponding $\hat{H}$ is given by

| Subgroup of $\mathbb{Z}_9^*$ | Subgroup of $\mathbb{Z}_{18}^*$ | $k^*$ |
|-----------------------------|-------------------------------|------|
| $H_1 = \{1\}$              | $\hat{H}_1 = \{1\}$          | $k^* = 5$ |
| $H_2 = \langle 8 \rangle$   | $\hat{H}_2 = \langle 17 \rangle$ | $k^* = 1$ |
| $H_3 = \langle 4 \rangle$   | $\hat{H}_3 = \langle 7 \rangle$ | $k^* = 2$ |
| $H_4 = \mathbb{Z}_9^*$      | $\hat{H}_4 = \mathbb{Z}_{18}^*$ | $k^* = 8$ |

Then $\Lambda_{9, H_j}(x)$ and $\Lambda_{18, \hat{H}_j}(x)$ corresponding to $j$ are calculated as follows:

| $j$ | $\Lambda_{9, H_j}(x)$ | $\Lambda_{18, \hat{H}_j}(x)$ |
|-----|------------------------|------------------------------|
| 1   | $x^6 + x^3 + 1$        | $x^6 - x^3 + 1$             |
| 2   | $x^3 - 3x + 1$         | $x^3 - 3x - 1$              |
| 3   | $x^2$                  | $x^2$                       |
| 4   | $x$                    | $x$                         |

It is shown that each two coefficients of both $\Lambda_{9, H_j}(x)$ and $\Lambda_{18, \hat{H}_j}(x)$ in the same degree has the same absolute value. However, as the degree decreases by 1, the sign of ‘ratio’ of corresponding coefficients changes in the alternating manner, starting from the situation that both leading coefficients coincide.
3. Irreducibility of Modified Cyclotomic Polynomial

In general, there are a number of reducible modified cyclotomic polynomials. For instance, see Example 5: If we have \( H = \{4\} \), the corresponding modified cyclotomic polynomial is \( \Lambda_{2,H}(x) = x^2 \), which is not irreducible. The previous researches \cite{7-9} give a crucial criterion in this section, to determine whether an \( m \)th modified cyclotomic polynomial is irreducible or not.

First, we define \( r(m) \), \( L(m) \), and \( U(m) \) as below.

**Definition 4.** Let \( m \geq 2 \) be an integer, and its prime decomposition be \( p_1^{a_1} \cdots p_t^{a_t} \), with prime factors \( p_1 < \cdots < p_t \) and integers \( e_1, \ldots, e_t \geq 1 \).

(i) We define \( r(m) \) by

\[
    r(m) = \begin{cases} 
        2p_1 \cdots p_t & \text{(for } 8 \mid m), \\
        p_1 \cdots p_t & \text{(for } 8 \nmid m) 
    \end{cases}
\]

(ii) A subset \( U(m) \) of \( \mathbb{Z}_m^\ast \) is defined as \( U(m) = \{ a \in \mathbb{Z}_m^\ast : a \equiv 1 \pmod{r(m)} \} \).

(iii) When \( m = p^a \) with \( p \) a prime number and \( \alpha \) a positive integer, we define a subset \( L(m) \) of \( \mathbb{Z}_m^\ast \) as a cyclic subgroup of order \( p - 1 \).

Indeed, \( U(m) \) is a subgroup of \( \mathbb{Z}_m^\ast \), whose order equals \( \frac{m}{r(m)} \) \((\text{see } [9], \text{Lemma 6})\). In particular, if \( m = p^a \) where \( p \) is an odd prime and \( \alpha \geq 1 \), \( U(m) \) is of order \( p^a - 1 \). Note that if \( m = p^a \), two subgroups \( L(m) \) and \( U(m) \) are relatively prime, because of the fact \( (p - 1, p^a - 1) = 1 \). Then we conclude that \( \mathbb{Z}_p^\ast \) is group isomorphic to \( L(p^a) \otimes U(p^a) \) by \((2), \text{Theorem 9.3})\).

We need a theorem as below. For the definition of the Gauss sum, we refer the reader to \([10]\).

**Theorem 4.** \((8), \text{p} \, 218 \text{ and } [9], \text{Theorem 2})\) For \( m \geq 2 \), let \( H \) be a subgroup of \( \mathbb{Z}_m^\ast \). Then the Gauss sum \( \sum_{\eta \in H} \zeta^{\eta} \) is not zero if and only if \( H \cap U(m) = \{1\} \).

We give a criterion to determine whether or not a modified cyclotomic polynomial is irreducible. This has been proved in \([7]\).

**Theorem 5.** \((7), \text{Theorem 3.7})\) Let \( m \geq 2 \) be an integer, \( \zeta \) be a primitive \( m \)th root of unity, and \( \sum_{\eta \in H} \zeta^{\eta} \neq 0 \) for a subgroup \( H \) of \( \mathbb{Z}_m^\ast \). Then \( \Lambda_{m,H}(x) \) is irreducible.

Note that the converse of Theorem 5 is not true, see Example 4 for instances. With the criterion above, we could decide whether a modified cyclotomic polynomial is irreducible over \( \mathbb{Q} \). The following example shows how many irreducible \( p \)th modified cyclotomic polynomials exist for an odd prime \( p \).

**Example 6.** Let \( p \) be an odd prime. We have \( U(p) = \{1\} \) and we easily find that every subgroup \( H \) of \( \mathbb{Z}_p^\ast \) satisfies \( H \cap U(p) = \{1\} \). Alternatively, if \( \zeta \) is a primitive \( p \)th root of unity, \( \sum_{k \in \mathbb{Z}_p^\ast} \zeta^k = -1 \) by the case (i) of Example 4. So, every \( p \)th modified cyclotomic polynomial is irreducible over \( \mathbb{Q} \) by Theorem 5. Also, there are exactly \( r(p - 1) \) irreducible \( p \)th modified cyclotomic polynomials, since cyclic group \( \mathbb{Z}_p^\ast \) has the unique subgroup of the order which divides \( p - 1 \).

We suggest Theorem 6 for figuring out which \( m \)th modified cyclotomic polynomial is irreducible, where \( m = 2^a \) \((a \geq 3)\). It is known that if \( m = 2^a \) \((a \geq 3)\), \( \mathbb{Z}_m^\ast \) has an element \( h \) of order \( \frac{\varphi(m)}{2} = 2^{a-2} \), though it has no primitive root (see \([11], \text{Theorem 2})\). We call this element \( h \) as ‘semi-primitive root’ modulo \( m \). It follows that \( \mathbb{Z}_m^\ast \) is isomorphic to \( \langle -1 \rangle \otimes \langle h \rangle \), where \( h \) is a semi-primitive root modulo \( m \) by \(([11], \text{Lemma 1 and Theorem 3})\). That is, any element of \( \mathbb{Z}_m^\ast \) is \( \pm h^i \pmod{m} \) for some \( i \in \{0, 1, \ldots, 2^{a-2} - 1\} \).
Before proving Theorem 6, we will prove the following lemma for predicting the number of elements in $\mathbb{Z}_{2^a}$ of order 2 when $\alpha \geq 3$.

**Lemma 3.** When $\alpha \geq 3$, $\mathbb{Z}_{2^a}$ has exactly 3 elements of order 2.

**Proof.** If $\alpha = 3$, then $\mathbb{Z}_{2^a}^* = \{1, 3, 5, 7\}$. And it is obvious that 3, 5, and 7 are 3 elements of order 2. Assume that $\alpha \geq 4$. Note that there exists a semi-primitive root $h$ modulo $2^\alpha$, then $\mathbb{Z}_{2^a}$ is group isomorphic to $(-1) \otimes \langle h \rangle$.

Let $u \in \mathbb{Z}_{2^a}^*$ be of order 2. There exists nonzero $i < 2^{\alpha-2} = \frac{\varphi(m)}{2}$ such that $u \equiv \pm h^i \pmod{2^\alpha}$. We consider two cases (i) and (ii) as below.

(i) Assume that $u \equiv h^i \pmod{2^\alpha}$. Since $|h| = \frac{\varphi(m)}{2} = 2^{\alpha-2}$, by (b) in Introduction, the following holds.

$$|u| = |h^i| = 2 \iff \frac{|h|}{(|h|, i)} = 2 \iff (|h|, i) = 2^{\alpha-3} \iff i = 2^{\alpha-3}$$

In this case, we get $u \equiv h^{2^{\alpha-3}} \pmod{m}$ and $u^2 \equiv h^{2^{\alpha-2}} \equiv 1 \pmod{m}$. But $u \in \langle h \rangle$ and $\langle h \rangle \cap \langle -1 \rangle = \{1\}$ imply $u \equiv -1 \pmod{2^\alpha}$.

(ii) Assume that $u \equiv -h^i \pmod{2^\alpha}$. Remark that $2 = | - h^i | = |1 - h^i| = [2, |h^i|]$. Either $|h^i| = 1$ or $|h^i| = 2$ holds. By the result of (i), $u \equiv -1 \pmod{2^\alpha}$ or $u \equiv -h^{2^{\alpha-3}} \pmod{2^\alpha}$.

So, the element $u$ of order 2 belongs to $\{\pm h^{2^{\alpha-3}}, -1\}$. □

The following theorem is one of main results of this paper.

**Theorem 6.** Assume that $m = 2^\alpha$ for some integer $\alpha \geq 3$. There are only 4 irreducible $m$th modified cyclotomic polynomials such as $x$, $\Psi_m(x)$, $\Psi_m^*(x)$, and $\Phi_m(x)$.

**Proof.** Let $\zeta$ be a primitive $2^\alpha$th root of unity and let $H$ be a subgroup of $\mathbb{Z}_{m}^*$.

We assume that $H \cap U(m) = \{1\}$. Then $\sum_{h \in H} \zeta^h \neq 0$ by Theorem 4, and $\Lambda_{m,H}(x)$ is irreducible over $\mathbb{Q}$ by Theorem 5. If $H$ is the trivial group $\{1\}$, we have $\Lambda_{m,H}(x) = \Phi_m(x)$.

Suppose that $H \neq \{1\}$, and let $a$ and $b$ be arbitrary elements of $H - \{1\}$. We get $r(m) = 4$ by Definition 4, since $8|m$. Then $H \cap U(m) = \{1\}$ implies $a \equiv b \equiv 3 \pmod{4}$. Since we have $a^2 \equiv ab \equiv 1 \pmod{4}$ for $a^2, ab \in H$, it follows that $a^2 \equiv ab \equiv 1 \pmod{m}$. We get $a \equiv b \pmod{m}$ since $(a, m) = 1$. Also, $a$ is of order 2. This shows that $H = \{1, a\}$ for some $a \equiv 3 \pmod{4}$.

Note that $-1$ is clearly of order 2 and

$$(2^a - 1)^2 \equiv 2^{2a-2} + 2a + 1 \equiv 1 \pmod{m}$$

because $2a - 2 \geq a$. Then there are only 3 elements of order 2 by Lemma 3: $-1, 2^a - 1 \pmod{m}$. Since $2^a - 1 + 1 \equiv 1 \pmod{4}$ is the nontrivial element, $a$ is either $-1$ or $2^a - 1 - 1$ modulo $m$. So, if $H = \langle -1 \rangle$, we have $\Lambda_{m,H}(x) = \Psi_m(x)$. If $H = \langle 2^a - 1 \rangle$, this leads to $\Lambda_{m,H}(x) = \Psi_m^*(x)$.

Suppose that $\Lambda_{m,H}(x)$ is irreducible but $H \cap U(m) \neq \{1\}$. Thus we obtain $\sum_{h \in H} \zeta^h = 0$ by Theorem 4. By Definition 3, $\Lambda_{m,H}(x)$ has a factor $x - \sum_{h \in H} \zeta^h = x$. Hence, $\Lambda_{m,H}(x)$ is an irreducible polynomial over $\mathbb{Q}$ having a factor $x$, we conclude $\Lambda_{m,H}(x) = x$ (And $H$ equals $\mathbb{Z}_m^*$ in this case).

In conclusion, there are exactly 4 irreducible $m$th modified cyclotomic polynomials such as $x$, $\Psi_m(x)$, $\Psi_m^*(x)$, and $\Phi_m(x)$. □

**Example 7.** We find all the 16th modified cyclotomic polynomials as below:
Theorem 7. Let \( m = 3^a \) (\( a \geq 2 \)). Then there are only 3 irreducible \( m \)th modified cyclotomic polynomials such as \( x, \Psi_m(x), \) and \( \Phi_m(x) \).

**Proof.** Let \( \zeta \) be a primitive \( m \)th root of unity and let \( H \) be a subgroup of \( \mathbb{Z}_m^* \).

We assume that \( H \cap U(m) = \{1\} \). Then \( \sum_{h \in H} \zeta^{mh} \neq 0 \) by Theorem 4, and \( \Lambda_{m,H}(x) \) is irreducible over \( \mathbb{Q} \) by Theorem 5. If \( H \) is the trivial group \( \{1\} \), we have \( \Lambda_{m,H}(x) = \Phi_m(x) \).

We assume that \( H \neq \{1\} \) and \( a \) and \( b \) are arbitrary elements of \( H - \{1\} \). According to Definition 4, we have \( r(m) = 3 \). Then \( H \cap U(m) = \{1\} \) implies \( a \equiv b \equiv 2 \pmod{3} \). Since we have \( a^2 \equiv ab \equiv 1 \pmod{3} \) for \( a, b \in H \), it follows that \( a^2 \equiv ab \equiv 1 \pmod{3} \). We get \( a \equiv b \pmod{3} \) since \( (a,m) = 1 \). Also, \( a \) is of order 2. This shows that \( H = \{1,a\} \) for some \( a \equiv 2 \pmod{3} \). Note that \( m \) has a primitive root. Hence, \( a \equiv 1 \pmod{3} \), and it follows that \( a \equiv -1 \pmod{3} \) by Lemma 1. In this case, \( H = \langle -1 \rangle \) and \( \Lambda_{m,H}(x) = \Psi_m(x) \).

If \( H \cap U(m) \neq \{1\} \), we obtain \( \Lambda_{m,H}(x) = x \) as in the proof of Theorem 6. Thus there are 3 irreducible \( m \)th modified cyclotomic polynomials: \( x, \Psi_m(x), \) and \( \Phi_m(x) \). \( \square \)

Theorem 8. Let \( m = 5^a \) (\( a \geq 2 \)). Then there are exactly 4 irreducible \( m \)th modified cyclotomic polynomials.

**Proof.** Let \( \zeta \) be a primitive \( m \)th root of unity and let \( H \) be a subgroup of \( \mathbb{Z}_m^* \).

We assume that \( H \cap U(m) = \{1\} \). Then \( \sum_{h \in H} \zeta^{mh} \neq 0 \) by Theorem 4, and \( \Lambda_{m,H}(x) \) is irreducible over \( \mathbb{Q} \) by Theorem 5. If \( H \) is the trivial group \( \{1\} \), we have \( \Lambda_{m,H}(x) = \Phi_m(x) \).

We assume that \( H \neq \{1\} \). By Definition 4, we get \( r(m) = 5 \) and every nontrivial element of \( H \) is congruent to either 2, 3, or 4 modulo 5. We figure out \( H \) for following cases.

(i) Assume that we have \( a \equiv b \equiv 4 \pmod{5} \) for every \( a, b \in H - \{1\} \). Since we have \( a^2 \equiv b^2 \equiv 1 \pmod{5} \), the fact \( H \cap U(m) = \{1\} \). Both \( a^2 \equiv b^2 \pmod{5} \) and \( a + b \equiv 3 \pmod{5} \) imply \( a \equiv b \pmod{5} \). So, we have \( H = \{1,a\} \). By Lemma 1, we get \( a \equiv -1 \pmod{5} \) and \( \Lambda_{m,H}(x) = \Psi_m(x) \).

(ii) Assume that there is a nontrivial element \( u \) in \( H \) with either \( u \equiv 2 \pmod{5} \) or \( u \equiv 3 \pmod{5} \). If \( u \equiv 2 \pmod{5} \), we get \( u^3 \equiv 3 \pmod{5} \) with \( u^3 \in H \). Likewise, if \( u \equiv 3 \pmod{5} \), we have \( u^3 \equiv 2 \pmod{5} \) with \( u^3 \in H \). So, there are \( a, b \in H - \{1\} \) where \( a \equiv 2 \pmod{5} \) and \( b \equiv 3 \pmod{5} \).

Then we obtain \( ab \equiv c^2 \equiv 1 \pmod{5} \) and \( a^2c \equiv b^2c \equiv 1 \pmod{5} \), which leads to \( ab \equiv c^2 \equiv 1 \pmod{5} \) and \( a^2c \equiv b^2c \equiv 1 \pmod{5} \) by \( H \cap U(m) = \{1\} \). Hence, \((a-b)(a+b) \equiv a^2c-b^2c \equiv 0 \pmod{5} \), \((c,m) = 1 \), and \( a-b \equiv 4 \pmod{5} \) imply \( b \equiv -a \pmod{5} \).

Suppose that there exists \( a_1, b_1, c_1 \in H - \{1\} \) such that \( a_1 \equiv 2 \pmod{5} \), \( b_1 \equiv 3 \pmod{5} \), and \( c_1 \equiv 4 \pmod{5} \). A similar calculation yields the following congruences, because of the fact \( H \cap U(m) = \{1\} \).

- \(-a_1^2 \equiv -a^2 \equiv 1 \pmod{5} \implies a_1^2 \equiv a^2 \pmod{5} \)
- \(a_1^2c_1 \equiv b_1^2c_1 \equiv 1 \pmod{5} \implies a_1^2c_1 \equiv b_1^2c_1 \equiv 1 \pmod{5} \)
- \(c_1^2 \equiv 1 \equiv c^2 \pmod{5} \implies c_1^2 \equiv 1 \equiv c^2 \pmod{5} \)
And we have
\[ a_1^2 \equiv a^2 \pmod{m} \quad \Rightarrow \quad (a_1 + a)(a_1 - a) \equiv 0 \pmod{m} \]
\[ a_1 \equiv a \pmod{m} \quad (\text{because } a_1 + a \equiv 4 \pmod{5}) \]
\[ a_1^2 c_1 \equiv b_1^2 \cdot c_1 \equiv 1 \pmod{m} \quad \Rightarrow \quad c_1(a_1 - b_1)(a_1 + b_1) \equiv 0 \pmod{m} \]
\[ b_1 \equiv -a_1 \pmod{m} \quad (\text{because } a_1 - b_1 \equiv 4 \pmod{5} \text{ and } c_1, m = 1) \]
\[ c_1^2 \equiv 1 \equiv c^2 \pmod{m} \quad \Rightarrow \quad (c_1 + c)(c_1 - c) \equiv 0 \pmod{m} \]
\[ c_1 \equiv c \pmod{m} \quad (\text{because } c_1 + c \equiv 3 \pmod{5}). \]

In consequence, we get \( a_1 \equiv a \pmod{m}, b_1 \equiv b \pmod{m}, \) and \( c_1 \equiv c \pmod{m}. \) These show that \( H = \{1, a, -a, -1\} \) holds for some \( a \equiv 2 \pmod{5}. \) We denote this \( H \) by \( \bar{H}. \) Then \( \bar{H} \) is the unique subgroup of order 4, because \( \mathbb{Z}_m^* \) is cyclic.

And if \( H \cap U(m) \neq \{1\}, \) we obtain \( \Lambda_{m,H}(x) = x \) as in the proof of Theorem 6. Thus there are 4 irreducible \( m \)th modified cyclotomic polynomials like \( x, \Lambda_{m,H}(x), \Psi_m(x), \) and \( \Phi_m(x). \)

The following main theorem predicts the number of irreducible \( m \)th modified cyclotomic polynomials, where \( p \) is an odd prime and \( m = p^a \) for some integer \( a \geq 2.\)

**Theorem 9.** If \( p \) is an odd prime and \( m = p^a \) for some integer \( a \geq 2, \) there are exactly \( \tau(p - 1) + 1 \) irreducible \( m \)th modified cyclotomic polynomials.

**Proof.** Assume that \( \zeta \) is a primitive \( m \)th root of unity and \( H \) is a subgroup of \( \mathbb{Z}_m^*. \)

We assume that \( H \cap U(m) = \{1\}. \) Then \( \Lambda_{m,H}(x) \) is irreducible over \( \mathbb{Q} \) by Theorems 4 and 5. Note that \( \mathbb{Z}_m^* \) is isomorphic to \( L(m) \cap U(m), \) and \( \mathbb{Z}_m^*/U(m) \) is isomorphic to \( L(m) \) (see [2], Theorem 9.3). Let \( \phi : \mathbb{Z}_m^* \to \mathbb{Z}_m^*/U(m) \) be the canonical map, which is defined as \( \phi(k) = kU(m). \) Then the kernel of \( \phi \) is \( U(m), \) and the restriction map \( \phi|_H : H \to \phi(H) \) has the kernel \( H \cap U(m) = \{1\}. \) That is, \( \phi|_H \) is the isomorphism because \( \phi \) is onto.

In particular, \( H \) is isomorphic to \( \phi(H), \) and so \( H \) is regarded as a subgroup of \( \mathbb{Z}_m^*/U(m). \) Further, \( H \) is isomorphic to a subgroup of \( L.m. \) Since \( L(m) \) is cyclic of order \( p - 1, \) there are exactly \( \tau(p - 1) \) choices of \( H \) satisfying \( H \cap U(m) = \{1\}. \) In other words, there are \( \tau(p - 1) \) irreducible \( m \)th modified cyclotomic polynomials for proper subgroups \( H. \) Also, we have \( \Lambda_{m,H}(x) = x \) as in the proof of Theorem 6. So, there are exactly \( \tau(p - 1) + 1 \) irreducible \( m \)th modified cyclotomic polynomials.

**Example 8.** There are all the 49th modified cyclotomic polynomials as below:

| \( H \) | \( \Lambda_{49,H}(x) \) |
|---|---|
| \( H_1 = \{1\} \) | \( \Lambda_{49,H_1}(x) = x^{42} + x^{35} + x^{28} + x^{21} + x^{14} + x^7 + 1 = \Phi_{49}(x) \) |
| \( H_2 = \{49\} \) | \( \Lambda_{49,H_2}(x) = x^{21} - 21x^{19} + 189x^{17} - 952x^{15} + x^{14} + 2940x^{13} - 14x^{12} - 573x^{11} + 77x^{10} + 7007x^9 - 210x^8 - 5147x^7 + 294x^6 + 2072x^5 - 196x^4 - 371x^3 + 49x^2 + 14x - 1 = \Psi_{49}(x) \) |
| \( H_3 = \{18\} \) | \( \Lambda_{49,H_3}(x) = x^{14} - 28x^{11} + 7x^{10} + 14x^9 + 189x^8 - 90x^7 - 98x^6 - 196x^5 + 427x^4 - 217x^3 - 140x^2 + 119x + 79 \) |
| \( H_4 = \{19\} \) | \( \Lambda_{49,H_4}(x) = x^7 - 21x^5 - 21x^4 + 91x^3 + 112x^2 - 84x - 97 \) |
| \( H_5 = \{8\} \) | \( \Lambda_{49,H_5}(x) = x^6 \) |
| \( H_6 = \{6\} \) | \( \Lambda_{49,H_6}(x) = x^3 \) |
| \( H_7 = \{2\} \) | \( \Lambda_{49,H_7}(x) = x^2 \) |
| \( H_8 = \mathbb{Z}_{49} \) | \( \Lambda_{49,H_8}(x) = x \) |

By Theorem 5, we have \( r(49) = 7. \) So, if \( H \) is a subgroup of \( \mathbb{Z}_{49}^* \) with \( H \cap \{1, 8, 15, 22, 29, 36, 43\} = \{1\}, \) corresponding \( \Lambda_{49,H}(x) \) is irreducible over \( \mathbb{Q}. \) Thus there are \( 5 = \tau(7 - 1) + 1 \) irreducible 49th modified cyclotomic polynomials: \( \Lambda_{49,H_1}(x) = \Phi_{49}(x), \Lambda_{49,H_2}(x) = \Psi_{49}(x), \Lambda_{49,H_3}(x), \Lambda_{49,H_4}(x), \Lambda_{49,H_6}(x), \Lambda_{49,H_8}(x) = x. \)

**Corollary 1.** If \( p \) is an odd prime and \( m = p^a \) for some integer \( a \geq 2, \) there are exactly \( \tau(p - 1) + 1 \) irreducible \( 2m \)th modified cyclotomic polynomials.
Proof. Let $H$ be a subgroup of $\mathbb{Z}_m^*$. We use the same definition of $\hat{H}$ of Theorem 3. According to the proof of Theorem 3, $\Lambda_{m,H}(x)$ is one-to-one correspondent to $\Lambda_{2m,\hat{H}}(x)$. We denote the polynomial $\Lambda_{m,H}(x) = \sum_{\ell=0}^{\ell} a_\ell x^\ell =: f(x)$ with $\ell = [\mathbb{Z}_m^* : H]$.

Let $f^*(x)$ be the reciprocal polynomial of $f(x)$:

$$f^*(x) = x^f \left( \frac{1}{x} \right) = a_0 x^f + a_1 x^{f-1} + \cdots + a_{f-1} x + a_f = \sum_{j=0}^{\ell} a_{\ell-j} x^j.$$ 

Then $f^*(x)$ is irreducible if and only if $f(x)$ is irreducible (see [12], Theorem 39). Let $g(x) = f^*(-x)$, then $g(x)$ is irreducible if and only if $f^*(x)$ is irreducible. Let $g^*(x)$ be the reciprocal polynomial of $g(x)$. It follows that

$$g^*(x) = x^f g \left( \frac{1}{x} \right) = x^f f^* \left( \frac{1}{x} \right) = x^f \left( \sum_{j=0}^{\ell} a_{\ell-j} \left( -\frac{1}{x} \right)^j \right)$$

$$= x^f \left( \frac{a_\ell}{x^\ell} - \frac{a_{\ell-1}}{x^{\ell-1}} + \frac{a_{\ell-2}}{x^{\ell-2}} - \cdots + (-1)^{\ell-1} \frac{a_1}{x} + (-1)^\ell \cdot a_0 \right)$$

$$= \sum_{j=0}^{\ell} (-1)^j \cdot a_{\ell-j} x^{f-j}.$$ 

So, we have $g^*(x) = \Lambda_{2m,\hat{H}}(x)$ by Theorem 3. This shows that $g^*(x) = \Lambda_{2m,\hat{H}}(x)$ is irreducible if and only if $f(x) = \Lambda_{m,H}(x)$ is irreducible. Therefore, there are exactly $\tau(p-1) + 1$ irreducible $2m$th modified cyclotomic polynomials due to Theorem 9. 

4. Discussion

In this paper, we defined and studied the modified cyclotomic polynomials mainly for the cases when $m$ is $p^e$ or $2p^e$, with $p$ a prime number.

One of the main results is the irreducibility of modified cyclotomic polynomial if $H \cap U(m) = \{1\}$, when $\mathbb{Z}_m^* = U(m) \otimes L(m)$. However, this result can be generalized in the case when $m = p_1^{e_1} \cdots p_r^{e_r}$, i.e., $m$ has more than one prime factor. So, we may get more irreducible modified cyclotomic polynomials.

Another result of this paper is finding the number of the irreducible modified cyclotomic polynomials when $m = 2^{e_1}, 3^{e_2}, 5^{e_3}, p^{e_4},$ or $2p^e$ for general prime number $p$. This result can also be generalized to arbitrary positive number $m$ when $m$ has more than one prime factor. We may use the fact that the irreducibility of modified cyclotomic polynomial is obtained when $H \cap U(m) = \{1\}$, and this condition implies that $H \subseteq L(m)$, i.e., $H$ is isomorphic to a subgroup of $L(m)$.

It is difficult to find examples of the application of modified cyclotomic polynomials among known references. The doctoral thesis [13] briefly mentioned the application of modified cyclotomic polynomials. Indeed, the author of [13] used the terminology “cyclotomic subgroup-polynomials” instead of “modified cyclotomic polynomials.” To the best of our knowledge, this is the only paper that mentioned examples of using modified cyclotomic polynomials.

However, examples of the application of cyclotomic polynomials have been found in a few papers. Readers interested in applications of cyclotomic polynomials should refer to [13–15].

In earlier researches like [8], the terminology “period polynomial” was used and its related topics were studied. Later in [6], the terminology “Galois polynomial” was chosen for the special case of the period polynomial, and this terminology has been used throughout researches including [5–7]. The motivation of this terminology is based on the use of Galois theory although we renamed the notion by our new terminology “modified cyclotomic polynomial” in the present paper, because we noticed that the notion is a modified concept of the cyclotomic polynomial. At a similar period, the author
of [13] used the terminology “cyclotomic subgroup-polynomial”, whose corresponding notion is the same as ours.

5. Conclusions

As a generalization of cyclotomic polynomials, modified cyclotomic polynomials are defined. Main results of this paper are as follows:

(i) A criterion to decide the irreducibility of a modified cyclotomic polynomial \( \Lambda_{m,H}(x) \) is studied when \( H \cap U(m) = \{1\} \).

(ii) The number of irreducible cyclotomic polynomials are calculated for the cases, \( m = 2^a \), \( m = 3^a \), \( m = 2 \cdot 3^a \), and \( m = 5^a \) respectively.

(iii) More generally, the number of irreducible cyclotomic polynomials are obtained when \( m = p^a \), with \( p \) a prime number. If \( p \geq 3 \) is prime, then the number of \( 2p^a \)th irreducible modified cyclotomic polynomials is the same as the number of \( p^a \)th ones.

Author Contributions: All authors contributed equally to the writing of this paper. All authors read and approved the final manuscript. Writing original draft, K.-S.L., S.-M.Y. and S.-M.J.; Writing review & editing, K.-S.L., S.-M.Y. and S.-M.J. All authors have read and agreed to the published version of the manuscript.

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

References

1. Bolker, E.D. Elementary Number Theory: An Algebraic Approach; W.A. Benjamin: New York, NY, USA, 1970.
2. Hungerford, T.W. Abstract Algebra: An Introduction, 3rd ed.; Brooks/Cole, Cengage Learning: Boston, MA, USA 2014.
3. Lang, S. Algebra; Addison-Wesley: Boston, MA, USA 1984.
4. Lee, K.-S., Lee, J.-E., Kim, J.-H. Semi-cyclotomic polynomials. Honam Math. J. 2015, 37, 469–472.
5. Lim, S.-A. A Note on the Properties of the Coefficients of Galois Polynomials. Master’s Thesis, Korea National University of Education, Cheongju, South Korea, 2018.
6. Kwon, M.-Y.; Lee, J.-E.; Lee, K.-S. Galois irreducible polynomials. Commun. Korean Math. Soc. 2017, 32, 1–6.
7. Shin, G.-C.; Bae, J.-Y.; Lee, K.-S. Irreducibility of Galois polynomials. Honam Math. J. 2018 40, 281–291.
8. Evans, R.J. Period polynomials for generalized cyclotomic periods. Manuscr. Math. 1982, 40, 217–243.
9. Diamond, H.G.; Gerth, F.; Vaaler, J.D. Gauss sums and Fourier analysis on multiplicative subgroups of \( \mathbb{Z}_q \). Trans. Am. Math. Soc. 1983, 227, 711–726.
10. Jung, S.-M.; Lee, K.-S. Concise Number Theory with Applications: Introductory Theorems and Problems; Lambert Academic Publishing, Saarbrücken, Germany, 2011.
11. Lee, K.-S.; Kwon, M.-Y.; Kang, M.-K.; Shin, G.-C. Semi-primitive root modulo \( n \). Honam Math. J. 2011 33, 181–186.
12. Pless, V. Introduction to the Theory of Error-Correcting Codes; John Wiley & Sons: Hoboken, NJ, USA: 1998; Volume 48.
13. Al-Shaghay, A. Some Classes of Generalized Cyclotomic Polynomials. Ph.D. Thesis, Dalhousie University, Halifax, NS, Canada, 2019.
14. Bach, E.; Shallit, J. Factoring with cyclotomic polynomials. Math. Comput. 1989, 52, 201–219.
15. Duke, W.; Nguyen, H.N. Infinite products of cyclotomic polynomials. Bull. Aust. Math. Soc. 2015, 91, 400–411.