Factorizations of Cyclotomic Polynomials over $\mathbb{Q}(\zeta_m)$ with Applications

Xiaoyu Liu* and Daniel Slilaty†

November 8, 2023

Abstract

Cyclotomic polynomials are a well-studied class of polynomials in algebraic number theory. The n^{th} cyclotomic polynomial, denoted as $\Phi_n(x)$, is a polynomial with integer coefficients that has precisely all primitive n^{th} roots of unity as its roots. Cyclotomic polynomials are known to be irreducible over the rational numbers. In this paper, we propose a factorization of $\Phi_{mp}(x)$ in which p is prime and $p \nmid m$ over the cyclotomic extension field $\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m^{th} root of unity, and show that the proposed factorization is irreducible over this extension field. Moreover, all coefficients of these irreducible factors are powers of ζ_m. With this factorization, we provide new proofs for the coefficients of cyclotomic polynomials $\Phi_{3p}(x)$ and $\Phi_{6p}(x)$ for any prime $p \geq 5$ and prove a new explicit identity for $\Phi_{5p}(x)$ and $\Phi_{10p}(x)$ for any prime $p \geq 7$.

1 Introduction

Research on cyclotomic polynomials has a long and rich history that spans centuries. The concept of roots of unity traces back to ancient Greek mathematics. In the 1730's Euler formally introduced the concept of cyclotomic polynomials. He defined the n^{th} cyclotomic polynomial, denoted by $\Phi_n(x)$, as the polynomial whose roots are precisely the primitive n^{th} roots of unity. Gauss made significant contributions to the study of cyclotomic polynomials. In his work "Disquisitiones Arithmeticae" (1801) he proved irreducibility of $\Phi_p(x)$ over rational numbers when p is prime, derived the cyclotomic identity $x^n - 1 = \prod_{d|n} \Phi_d(x)$, and developed the theory of cyclotomy that studies the properties of cyclotomic fields. In the mid-19^{th} century, Kronecker expanded upon Gauss' ideas and further developed the theory of cyclotomic polynomials. The study of cyclotomic polynomials gained further momentum in the 20^{th} century with the work of Kummer in which he established deep connections between cyclotomic polynomials and algebraic number theory.

*Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA. Email xiaoyu.liu@wright.edu.

†Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA. Email daniel.slilaty@wright.edu.

For any positive integer n, the n^{th} *cyclotomic polynomial* in $\mathbb{Q}[x]$ is the unique irreducible polynomial with integer coefficients that is a divisor of $x^n - 1$ and has as its roots all n^{th} primitive roots of unity. In other words, the n^{th} cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ (k,n)=1}} (x - \zeta_n^k),$$

where ζ_n is any primitive n^{th} root of unity. The irreducibility of $\Phi_p(x)$ for prime p was first proved by Gauss [1], and the irreducibility of $\Phi_n(x)$ for general integer n was first proved by Kronecker [2].

The prime factorization of n plays an important role in the study of $\Phi_n(x)$. Two of the most straightforward results are: $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ for any prime p; and $\Phi_{2p}(x) = 1 - x + x^2 - \cdots + x^{p-1}$ for any odd prime p. Explicit formulae for Φ_{3p}, Φ_{6p} (p an odd prime) and other results for $\Phi_{pq}(x)$ (where p and q distinct odd primes) can be found in [3, 4, 5].

In this paper, we are interested in $\Phi_n(x)$ for $n = mp$, where p is an odd prime and $(m, p) = 1$. Note that we focus on the situation that $(m, p) = 1$ because of this well-known fact: if $n = mp^r$ with $(m, p) = 1$, then $\Phi_n(x) = \Phi_{mp}(x^{p^{r-1}})$ [6]. Instead of restricting ourselves to $\mathbb{Q}[x]$, we examine the factorization of $\Phi_{mp}(x)$ over the simple extension field $\mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m^{th} root of unity.

The field $\mathbb{Q}(\zeta_n)$ is called the n^{th} *cyclotomic field* and it is the splitting field of $x^n - 1$ and of $\Phi_n(x)$ over $\mathbb{Q}$. Therefore $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where φ is Euler's totient function. The Galois group $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is naturally isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, which consists of the invertible residues modulo n. The isomorphism sends each $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ to $a \mod n$, where a is an integer such that $\sigma(\zeta_n) = \zeta_n^a$.

2 Main Results

The main result of this paper gives a factorization of $\Phi_{mp}(x)$ over the cyclotomic field $\mathbb{Q}(\zeta_m)$ where p is prime and $(m, p) = 1$.

Theorem 2.1. *Suppose $n = mp$, where p is a prime and $(m, p) = 1$. Let ζ_n be a primitive n^{th} root of unity and $\zeta_m = \zeta_n^p$ be a primitive m^{th} root of unity. Define $\Phi_{n,i}(x) = \sum_{t=0}^{p-1} \zeta_m^{it} x^{p-1-t}$. Then*

$$\Phi_n(x) = \prod_{\substack{1 \le i \le m \\ (i,m)=1}} \Phi_{n,i}(x).$$

Proof. Note that the cyclotomic polynomial

$$\Phi_n(x) = \prod_{\substack{1 \le j \le n \\ (j,n)=1}} (x - \zeta_n^j).$$

For each $1 \le i \le m$ with $(i, m) = 1$, the set $\{j \mid 1 \le j \le n,\ (j, n) = 1,\ j \equiv ip \mod m\}$ has order $p - 1$, by the Chinese Remainder Theorem. All these sets are disjoint, partitioning

the numbers in $\{1 \le j \le n |\ (j,n) = 1\}$ into $\varphi(m)$ subsets of equal size. So

$$\Phi_n(x) = \prod_{\substack{1 \le i \le m \\ (i,m)=1}} \psi_{n,i}(x),$$

where each

$$\psi_{n,i}(x) = \prod_{\substack{1 \le j \le n,\ (j,n)=1 \\ j \equiv ip \mod m}} (x - \zeta_n^j)$$

is a polynomial of degree $p-1$, which equals the degree of $\Phi_{n,i}(x) = \sum_{t=0}^{p-1} \zeta_m^{it} x^{p-1-t}$. Therefore, it is sufficient to show that each ζ_n^j, where $1 \le j \le n$, $(j,n) = 1$, $j \equiv ip \mod m$, is a root of $\Phi_{n,i}(x)$. Note that

$$\Phi_{n,i}(\zeta_n^j) = \sum_{t=0}^{p-1} \zeta_m^{it} (\zeta_n^j)^{p-1-t} = \sum_{t=0}^{p-1} \zeta_n^{ipt} \zeta_n^{j(p-1-t)} = \zeta_n^{j(p-1)} \sum_{t=0}^{p-1} \zeta_n^{(ip-j)t}.$$

Since $j \equiv ip \mod m$ and $(j,n) = 1$, ζ_n^{ip-j} is a primitive p^{th} root of unity. So $\sum_{t=0}^{p-1} \zeta_n^{(ip-j)t} = 0$. □

For example, if $n = 105 = 15 \cdot 7$ (i.e., $m = 15$ and $p = 7$) then

$$\Phi_{105}(x) = \Phi_{105,1}(x) \cdot \Phi_{105,2}(x) \cdot \Phi_{105,4}(x) \cdot \Phi_{105,7}(x) \cdot \Phi_{105,8}(x) \cdot \Phi_{105,11}(x) \cdot \Phi_{105,13}(x) \cdot \Phi_{105,14}(x).$$

Each of the above eight $\Phi_{105,i}(x) = x^6 + \zeta_{15}^i x^5 + \cdots + \zeta_{15}^{5i} x + \zeta_{15}^{6i}$, where $\zeta_{15} = \zeta_{105}^7$. Moreover, each $\Phi_{105,i}(x)$ has six roots. For instance, the roots of $\Phi_{105,1}(x)$ are ζ_{105}^j, $j = 22, 37, 52, 67, 82, 97$.

The next result shows that each factor $\Phi_{mp,i}(x)$ in the Theorem 2.1 is irreducible over $\mathbb{Q}(\zeta_m)[x]$.

Theorem 2.2. *Let $\Phi_{n,i}(x)$ be as defined in Theorem 2.1, and ζ_m be any primitive m^{th} root of unity. Then $\Phi_{n,i}(x)$ is an irreducible polynomial in $\mathbb{Q}(\zeta_m)[x]$.*

Proof. By way of contradiction, assume that $\Phi_{n,i}(x)$ is reducible. Say $\Phi_{n,i}(x) = f(x)g(x)$ for polynomials $f(x), g(x) \in \mathbb{Q}(\zeta_m)[x]$

Consider the Galois group $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/mp\mathbb{Z})^\times$. The element of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ corresponding to $a \in (\mathbb{Z}/mp\mathbb{Z})^\times$ will be denoted by σ_a which is the automorphism defined by $\sigma_a(\zeta_n) = \zeta_n^a$. Consider the subgroup $\{km + 1 : 0 \le k \le (p-1) \text{ and } (p, km+1) = 1\}$ of $(\mathbb{Z}/mp\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$. This corresponds to the cyclic subgroup $\langle 1 \rangle \times (\mathbb{Z}/p\mathbb{Z})^\times$ of $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ which has order $p-1$. Thus $P = \{\sigma_{km+1} : 0 \le k \le (p-1) \text{ and } (p, km+1) = 1\}$ forms the subgroup of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ which fixes the m^{th} roots of unity $\langle \zeta_n^p \rangle = \langle \zeta_m \rangle$; that is, $P = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))$. Now the roots of $\Phi_{n,i}(x)$ are all ζ_n^j for which $1 \le j \le n-1$, $(j,n) = 1$, and $j = i \pmod m$. Note that for each such j, $\zeta_n^j \notin \mathbb{Q}(\zeta_m)$ because p does not divide j and $\zeta_n^p = \zeta_m$.

Now suppose without loss of generality that $j = i \pmod m$, ζ_n^i is a root of $f(x)$, and ζ_n^j is a root of $g(x)$. Since $f(x)$ and $g(x)$ are polynomials over $\mathbb{Q}(\zeta_m)$, they are both fixed under

the action of P. However, we will conclude the proof by showing that there is $\sigma_{km+1} \in P$ such that $\sigma_{km+1}(\zeta_n^i) = \zeta_n^j$, which contradicts the fact that P fixes $f(x)$ and $g(x)$.

The elements $i, j \in (\mathbb{Z}/mp\mathbb{Z})^\times$ are congruent modulo m and so correspond to pairs $([i]_m, [i]_p)$ and $([j]_m, [j]_p) = ([i]_m, [j]_p)$ in $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times \cong (\mathbb{Z}/mp\mathbb{Z})^\times$. Let $km+1$ be the element of $(\mathbb{Z}/mp\mathbb{Z})^\times$ which corresponds to the pair $(1, [j]_p[i]_p^{-1})$ in $\langle 1 \rangle \times (\mathbb{Z}/p\mathbb{Z})^\times$. Thus $\sigma_{km+1} \in P$ and takes ζ_n^i to ζ_n^j, as required. □

3 Applications

One application of the factorization in Theorem 2.1 is to compute the coefficients of $\Phi_{mp}(x)$ when $\varphi(m)$ is small. For $m = 3$ or 6, $\varphi(m) = 2$ and we have that $\Phi_n(x) = \Phi_{n,1}(x)\Phi_{n,n-1}(x)$. With this factorization, we are able to provide a new and straightforward proof of Theorem 3.1 which was first proven in [4].

Theorem 3.1. *[4] Let p be any odd prime.*

- *If $p \equiv 1 \mod 3$, then*

$$\Phi_{3p}(x) = 1 - x + x^3 - x^4 + \cdots - x^{p-3} + x^{p-1} - x^{p+1} + \cdots - x^{2p-6} - x^{2p-5} + x^{2p-3} + x^{2p-2}.$$

- *If $p \equiv 2 \mod 3$, then*

$$\Phi_{3p}(x) = 1 - x + x^3 - x^4 + \cdots - x^{p-2} - x^{p-1} - x^p + \cdots - x^{2p-6} - x^{2p-5} + x^{2p-3} + x^{2p-2}.$$

Proof. Let c_k denote the coefficient of x^k in the polynomial $\Phi_{3p}(x)$. For each $0 \leq k \leq p-1$ write $k = 3t + r$ for $r \in \{0, 1, 2\}$. Now

$$c_{2p-2-k} = \sum_{i=0}^{3t+r} \zeta_3^i \zeta_3^{i+2r} = \zeta_3^{2r} \sum_{i=0}^{3t+r} \zeta_3^{2i} = \zeta_3^{2r} \sum_{i=0}^{r} \zeta_3^{2i}.$$

When $r = 0$ this sum is 1, when $r = 1$ this sum is $\zeta_3^2(1 + \zeta_3^2) = \zeta_3^2(-\zeta_3) = -1$, and when $r = 2$ this sum is $\zeta_3(1 + \zeta_3^2 + \zeta_3) = 0$. This gives us the $p-1$ coefficients of the highest powers of x, the lower-order coefficients follow from the fact that $\Phi_{3p}(x)$ is a palindrome. □

The known identity $\Phi_{2n}(x) = (-1)^{\Phi(n)}\Phi_n(-x)$ from [6] for any odd value of n yields $\Phi_{6p}(x) = \Phi_{3p}(-x)$ for an odd prime p and so we also have Theorem 3.2.

Theorem 3.2. *Let p be any odd prime.*

- *If $p \equiv 1 \mod 3$, then*

$$\Phi_{6p}(x) = 1 + x - x^3 - x^4 + \cdots - x^{p-3} + x^{p-1} - x^{p+1} + \cdots - x^{2p-6} - x^{2p-5} + x^{2p-3} + x^{2p-2}.$$

- *If $p \equiv 2 \mod 3$, then*

$$\Phi_{6p}(x) = 1 + x - x^3 - x^4 + \cdots + x^{p-2} - x^{p-1} + x^p + \cdots - x^{2p-6} - x^{2p-5} + x^{2p-3} + x^{2p-2}.$$

The factorization in Theorem 2.1 even allows us to calculate $\Phi_{5p}(x)$ and $\Phi_{10p}(x)$. Because $\Phi_n(x)$ is a palindrome, Theorems 3.3 and 3.7 yield explicit formulae.

Theorem 3.3. *Let $p > 5$ be prime and let c_k be the coefficient of x^k in the cyclotomic polynomial $\Phi_{5p}(x)$ which has degree $4(p-1)$. Then for $0 \le k \le p-1$,*

$$c_{4p-4-k} = \begin{cases} 1 & \text{if } k = 0 \mod 5 \\ -1 & \text{if } k = 1 \mod 5 \\ 0 & \text{if } k = 2,3,4 \mod 5 \end{cases}$$

Furthermore,

- *if $p = 1 \mod 5$, then*

$$c_{3p-3-k} = \begin{cases} 1 & \text{if } k = 0 \mod 5 \\ -1 & \text{if } k = 2 \mod 5 \\ 0 & \text{if } k = 1,3,4 \mod 5 \end{cases}$$

- *if $p = 2 \mod 5$, then*

$$c_{3p-3-k} = \begin{cases} 1 & \text{if } k = 1,4 \mod 5 \\ -1 & \text{if } k = 0,2 \mod 5 \\ 0 & \text{if } k = 3 \mod 5 \end{cases}$$

- *if $p = 3 \mod 5$, then*

$$c_{3p-3-k} = \begin{cases} 1 & \text{if } k = 1,3 \mod 5 \\ -1 & \text{if } k = 2,4 \mod 5 \\ 0 & \text{if } k = 0 \mod 5 \end{cases}$$

- *if $p = 4 \mod 5$, then*

$$c_{3p-3-k} = \begin{cases} 1 & \text{if } k = 1 \mod 5 \\ -1 & \text{if } k = 3 \mod 5 \\ 0 & \text{if } k = 0,2,4 \mod 5 \end{cases}$$

Here are two examples calculated with Theorem 3.3.

$p = 11$ $\Phi_{55}(x)$ has degree 40 and since $11 = 1 \mod 5$ its sequence of coefficients is as follows. The circled entry is the coefficient of the middle term, x^{20}.

$$\begin{array}{cccccccccccc} 1 & -1 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & & \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & \textcircled{1} & \\ 0 & 0 & -1 & 0 & 1 & 0 & 0 & -1 & 0 & 1 & & \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & & \end{array}$$

$p = 17$ $\Phi_{85}(x)$ has degree 64 and since $17 = 2 \mod 5$ its sequence of coefficients is as follows. The circled entry is the coefficient of the middle term, x^{32}.

$$\begin{array}{cccccccccccccccc}
1 & -1 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1 & \\
-1 & 1 & -1 & 0 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & \textcircled{1} \\
-1 & 1 & 0 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & \\
1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & -1 & 1 &
\end{array}$$

Before proving Theorem 3.3 we present the following propositions which we use repeatedly without further mention. Let g denote the golden ratio $\frac{1+\sqrt{5}}{2}$ and $\bar{g} = \frac{1-\sqrt{5}}{2}$. These are the roots of polynomial $x^2 - x - 1$. They also satisfy the relation $g\bar{g} = -1$.

Proposition 3.4. *Let c_k denote the coefficient of x^k in $\Phi_{5p,1}(x)\Phi_{5p,4}(x)$. If $0 \le k \le p-1$, then*

$$c_{2p-2-k} = \begin{cases} 1 \text{ if } k = 0 \mod 5 \\ -\bar{g} \text{ if } k = 1 \mod 5 \\ \bar{g} \text{ if } k = 2 \mod 5 \\ -1 \text{ if } k = 3 \mod 5 \\ 0 \text{ if } k = 4 \mod 5 \end{cases}$$

Furthermore, $\Phi_{5p,1}(x)\Phi_{5p,4}(x)$ is a palindrome and so $c_k = c_{2(p-1)-k}$ for $0 \le k < p-1$.

Proof. Recall that $\cos(\frac{\pi}{5}) = \frac{g}{2}$. Thus $\zeta_5^2 + \zeta_5^3 = -g$ and $\zeta_5 + \zeta_5^4 = -\bar{g}$. Now, for each $0 \le k \le p-1$ write $k = 5t + r$ for $r \in \{0, 1, 2, 3, 4\}$. Now

$$c_{2p-2-k} = \sum_{i=0}^{5t+r} \zeta_5^i \zeta_5^{i+4r} = \zeta_5^{4r} \sum_{i=0}^{5t+r} \zeta_5^{2i} = \zeta_5^{4r} \sum_{i=0}^{r} \zeta_5^{2i}.$$

For $r = 0 \mod 5$ this sum is 1, for $r = 1 \mod 5$ this sum is $\zeta_5^4(1 + \zeta_5^2) = \zeta_5^4 + \zeta_5 = -\bar{g}$, for $r = 2 \mod 5$ this sum is $\zeta_5^3(1 + \zeta_5^2 + \zeta_5^4) = \zeta_5^3 + 1 + \zeta_5^2 = \bar{g}$, for $r = 3 \mod 5$ this sum is $\zeta_5^2(1 + \zeta_5^2 + \zeta_5^4 + \zeta_5) = \zeta_5^2(-\zeta_5^3) = -1$, and for $r = 4 \mod 5$ this sum is $\zeta_5(1 + \zeta_5^2 + \zeta_5^4 + \zeta_5 + \zeta_5^3) = 0$.

The roots of $\Phi_{5p,1}(x)\Phi_{5p,4}(x)$ are all ζ_5^t for which $(t, 5) = 1$ and $t = 1$ or $4 \mod 5$. This set of roots is closed under multiplicative inverses. Therefore $f(x) = \Phi_{5p,1}(x)\Phi_{5p,4}(x)$ and its reciprocal polynomial $x^{2p-2}f(1/x)$ have the same roots which makes $f(x)$ a palindrome. Thus the calculation above for c_k with $k \ge p-1$ suffices to find c_k for $k < p-1$ as stated. □

Proposition 3.5. *Let c_k denote the coefficient of x^k in $\Phi_{5p,2}(x)\Phi_{5p,3}(x)$. Let g denote the golden ratio $\frac{1+\sqrt{5}}{2}$. If $0 \le k \le p-1$, then*

$$c_{2p-2-k} = \begin{cases} 1 \text{ if } k = 0 \mod 5 \\ -g \text{ if } k = 1 \mod 5 \\ g \text{ if } k = 2 \mod 5 \\ -1 \text{ if } k = 3 \mod 5 \\ 0 \text{ if } k = 4 \mod 5 \end{cases}$$

Furthermore, $\Phi_{5p,2}(x)\Phi_{5p,3}(x)$ is a palindrome and so $c_k = c_{2(p-1)-k}$ for $0 \le k < p-1$.

Proof. Similar to the previous proof. □

Proposition 3.6. *Let* $\gamma_g = (1, -g, g, -1, 0)$ *and* $\gamma_{\bar{g}} = (1, -\bar{g}, \bar{g}, -1, 0)$. *If* u *and* v *are obtained respectively from* γ_g *and* $\gamma_{\bar{g}}$ *by cyclic shift, reversal, and/or negation, then* $u \cdot v = 0$.

Proof. First note that the vector obtained from reversal of γ_g is equal to the negation of a cyclic shift of γ_g; similarly for the reversal of $\gamma_{\bar{g}}$. So we need only check that γ_g is orthogonal to every cyclic shift of $\gamma_{\bar{g}}$ and this will complete the proof.

- $(1, -g, g, -1, 0) \cdot (1, -\bar{g}, \bar{g}, -1, 0) = 1 - 1 - 1 + 1 = 0$
- $(1, -g, g, -1, 0) \cdot (-\bar{g}, \bar{g}, -1, 0, 1) = -\bar{g} + 1 - g = 0$
- $(1, -g, g, -1, 0) \cdot (\bar{g}, -1, 0, 1, -\bar{g}) = \bar{g} + g - 1 = 0$
- $(1, -g, g, -1, 0) \cdot (-1, 0, 1, -\bar{g}, \bar{g}) = -1 + g + \bar{g} = 0$
- $(1, -g, g, -1, 0) \cdot (0, 1, -\bar{g}, \bar{g}, -1) = -g + 1 - \bar{g} = 0$

□

Proof of Theorem 3.3. Let $f(x) = \Phi_{5p,2}(x)\Phi_{5p,3}(x)$ and $f(x) = \Phi_{5p,1}(x)\Phi_{5p,4}(x)$. Thus $\Phi_{5p}(x) = f(x)h(x)$. Now let c_k denote the coefficient of x^k in $\Phi_{5p}(x)$ which has degree $4(p-1)$. Thus

$$c_{4p-4} = 1,$$

$$c_{4p-5} = (1, -g) \cdot (-\bar{g}, 1) = -1,$$

$$c_{4p-6} = (1, -g, g) \cdot (\bar{g}, -\bar{g}, 1) = 0,$$

$$c_{4p-7} = (1, -g, g, -1) \cdot (-1, \bar{g}, -\bar{g}, 1) = 0, \text{ and}$$

$$c_{4p-8} = (1, -g, g, -1, 0) \cdot (0, -1, \bar{g}, -\bar{g}, 1) = 0$$

These together with the orthogonality of cyclic shifts, reversals, and/or negations of γ_g and $\gamma_{\bar{g}}$ imply that imply that c_{4p-4-k} has the required value for $0 \leq k \leq p-1$.

It remains only to prove the statement of our theorem for coefficients c_{3p-3-k} for $0 \leq p \leq k-1$. In Case 1 we will assume $p = 3 \mod 5$ and in Case 2 we assume $p = 1 \mod 5$. The remaining two cases are done similarly.

Case 1 Assume that $p = 3 \mod 5$. First, we directly calculate $c_{2p-2}, c_{2p-1}, c_{2p}, c_{2p+1}, c_{2p+2}$. As an aid to the reader, the coefficient of the middle terms of the palindromes $f(x)$ and $h(x)$ are circled. Thus

$$\begin{array}{rcl} c_{2p-2} & = & (\gamma_g \ \ldots \ \gamma_g \ 1 \ -g \ \textcircled{g} \ -g \ 1 \ J\gamma_g \ \ldots \ J\gamma_g) \cdot \\ & & (\gamma_{\bar{g}} \ \ldots \ \gamma_{\bar{g}} \ 1 \ -\bar{g} \ \textcircled{\bar{g}} \ -\bar{g} \ 1 \ J\gamma_{\bar{g}} \ \ldots \ J\gamma_{\bar{g}}) \end{array}$$

in which Jv is the vector obtained from vector v by reversing its entries. Therefore $c_{2p-2} = (1, -g, g, -g, 1) \cdot (1, -\bar{g}, \bar{g}, -\bar{g}, 1) = -1$. Next,

$$c_{2p-1} = \begin{matrix}(\gamma_g & \dots & \gamma_g & 1 & -g & \textcircled{g} & -g & \gamma' & \dots & \gamma') \cdot \\ (\gamma'' & \dots & \gamma'' & -\bar{g} & \textcircled{\bar{g}} & -\bar{g} & 1 & J\gamma_{\bar{g}} & \dots & J\gamma_{\bar{g}})\end{matrix}$$

in which γ' is a cyclic shift of $J\gamma_g$ and γ'' is a cyclic shift of $\gamma_{\bar{g}}$. Therefore $c_{2p-1} = (1, -g, g, -g) \cdot (-\bar{g}, \bar{g}, -\bar{g}, 1) = 1$. Next,

$$c_{2p} = \begin{matrix}(\gamma_g & \dots & \gamma_g & 1 & -g & \textcircled{g} & \gamma' & \dots & \gamma') \cdot \\ (\gamma'' & \dots & \gamma'' & \textcircled{\bar{g}} & -\bar{g} & 1 & J\gamma_{\bar{g}} & \dots & J\gamma_{\bar{g}})\end{matrix}$$

in which γ' is a cyclic shift of $J\gamma_g$ and γ'' is a cyclic shift of $\gamma_{\bar{g}}$. Therefore $c_{2p} = (1, -g, g) \cdot (\bar{g} - \bar{g}, 1) = 0$. Next,

$$c_{2p+1} = \begin{matrix}(\gamma_g & \dots & \gamma_g & 1 & -g & \gamma' & \dots & \gamma') \cdot \\ (\gamma'' & \dots & \gamma'' & -\bar{g} & 1 & J\gamma_{\bar{g}} & \dots & J\gamma_{\bar{g}})\end{matrix}$$

in which γ' is a cyclic shift of $J\gamma_g$ and γ'' is a cyclic shift of $\gamma_{\bar{g}}$. Therefore $c_{2p+1} = (1, -g) \cdot (-\bar{g}, 1) = -1$. Lastly,

$$c_{2p+2} = \begin{matrix}(\gamma_g & \dots & \gamma_g & 1 & \gamma' & \dots & \gamma') \cdot \\ (\gamma'' & \dots & \gamma'' & 1 & J\gamma_{\bar{g}} & \dots & J\gamma_{\bar{g}})\end{matrix}$$

in which γ' is a cyclic shift of $J\gamma_g$ and γ'' is a cyclic shift of $\gamma_{\bar{g}}$. Therefore $c_{2p+2} = 1$.

Now for $0 \le t \le 4$ and $0 \le t + 5k \le p - 1$ we must have $c_{2p-2+t+5k} = c_{2p-2+t}$ because the form of the dot product for $c_{2p-2+t+5k}$ is given by the form of dot product for c_{2p-2+t} with k copies of an appropriate cyclic shift γ_g and of $\gamma_{\bar{g}}$ inserted between the circled entries as shown.

$$c_{2p-2+5k} = \begin{matrix}(\gamma_g & \dots & \gamma_g & 1 & -g & g & \dots & \delta' & -g & 1 & J\gamma_g & \dots & J\gamma_g) \cdot \\ (\gamma_{\bar{g}} & \dots & \gamma_{\bar{g}} & 1 & -\bar{g} & \textcircled{\bar{g}} & \dots & \delta'' & -\bar{g} & 1 & J\gamma_{\bar{g}} & \dots & J\gamma_{\bar{g}})\end{matrix} = c_{2p-2}$$

$$c_{2p-1+5k} = \begin{matrix}(\gamma_g & \dots & \gamma_g & 1 & -g & \dots & \delta' & \textcircled{g} & -g & \gamma' & \dots & \gamma') \cdot \\ (\gamma'' & \dots & \gamma'' & -\bar{g} & \textcircled{\bar{g}} & \dots & \delta'' & -\bar{g} & 1 & J\gamma_{\bar{g}} & \dots & J\gamma_{\bar{g}})\end{matrix} = c_{2p-1}$$

$$c_{2p+5k} = \begin{matrix}(\gamma_g & \dots & \gamma_g & 1 & -g & \dots & \delta' & \textcircled{g} & \gamma' & \dots & \gamma') \cdot \\ (\gamma'' & \dots & \gamma'' & \textcircled{\bar{g}} & -\bar{g} & \dots & \delta'' & 1 & J\gamma_{\bar{g}} & \dots & J\gamma_{\bar{g}})\end{matrix} = c_{2p}$$

$$c_{2p+1+5k} = \begin{matrix}(\gamma_g & \dots & \gamma_g & 1 & -g & \dots & \gamma' & \gamma' & \dots & \gamma') \cdot \\ (\gamma'' & \dots & \gamma'' & -\bar{g} & 1 & \dots & J\gamma_{\bar{g}} & J\gamma_{\bar{g}} & \dots & J\gamma_{\bar{g}})\end{matrix} = c_{2p+1}$$

$$c_{2p+2+5k} = \begin{matrix}(\gamma_g & \dots & \gamma_g & 1 & \dots & \gamma' & \gamma' & \dots & \gamma') \cdot \\ (\gamma'' & \dots & \gamma'' & 1 & \dots & J\gamma_{\bar{g}} & J\gamma_{\bar{g}} & \dots & J\gamma_{\bar{g}})\end{matrix} = c_{2p+2}$$

Now because $p = 3 \mod 5$, we have that $3p - 3 = 2p \pmod 5$. This yields the desired result for c_{3p-3-k} in the statement of our proposition.

Case 2 Assume that $p = 1 \mod 5$. So

$$\begin{array}{rcl} c_{2p-2} & = & (\gamma_g \ \ldots \ \gamma_g \ \textcircled{1} \ J\gamma_g \ \ldots \ J\gamma_g)\cdot \\ & & (\gamma_{\bar{g}} \ \ldots \ \gamma_{\bar{g}} \ \textcircled{1} \ J\gamma_{\bar{g}} \ \ldots \ J\gamma_{\bar{g}}) \ = \ 1 \end{array}$$

and

$$\begin{array}{rcl} c_{2p-1} & = & (\gamma_g \ \ldots \ \gamma_g \ \gamma' \ \ldots \ \gamma')\cdot \\ & & (\gamma'' \ \ldots \ \gamma'' \ J\gamma_{\bar{g}} \ \ldots \ J\gamma_{\bar{g}}) \ = \ 0 \end{array}$$

and

$$\begin{array}{rcl} c_{2p} & = & (\gamma_g \ \ldots \ \gamma_g \ 1 \ -g \ g \ -1 \ 0 \ \textcircled{1} \ 0 \ -1 \ g \ \gamma' \ \ldots \ \gamma')\cdot \\ & & (\gamma'' \ \ldots \ \gamma'' \ \bar{g} \ -1 \ 0 \ \textcircled{1} \ 0 \ -1 \ \bar{g} \ -\bar{g} \ 1 \ J\gamma_{\bar{g}} \ \ldots \ J\gamma_{\bar{g}}) \ = \ 0 \end{array}$$

and

$$\begin{array}{rcl} c_{2p+1} & = & (\gamma_g \ \ldots \ \gamma_g \ 1 \ -g \ g \ -1 \ 0 \ \textcircled{1} \ 0 \ -1 \ \gamma' \ \ldots \ \gamma')\cdot \\ & & (\gamma'' \ \ldots \ \gamma'' \ -1 \ 0 \ \textcircled{1} \ 0 \ -1 \ \bar{g} \ -\bar{g} \ 1 \ J\gamma_{\bar{g}} \ \ldots \ J\gamma_{\bar{g}}) \ = \ -1 \end{array}$$

and

$$\begin{array}{rcl} c_{2p+2} & = & (\gamma_g \ \ldots \ \gamma_g \ 1 \ -g \ g \ -1 \ 0 \ \textcircled{1} \ 0 \ \gamma' \ \ldots \ \gamma')\cdot \\ & & (\gamma'' \ \ldots \ \gamma'' \ 0 \ \textcircled{1} \ 0 \ -1 \ \bar{g} \ -\bar{g} \ 1 \ J\gamma_{\bar{g}} \ \ldots \ J\gamma_{\bar{g}}) \ = \ 0. \end{array}$$

Now for $0 \leq t \leq 4$ and $0 \leq t + 5k \leq p - 1$ we must have $c_{2p-2+t+5k} = c_{2p-2+t}$ is proven in a manner analogous to that of Case 1. Finally, because $p = 1 \mod 5$, we have that $3p - 3 = 2p - 2 \pmod 5$. This yields the desired result for c_{3p-3-k} in the statement of our proposition. □

Again we can apply $\Phi_{2n}(x) = (-1)^{\Phi(n)}\Phi_n(-x)$ for odd n to obtain $\Phi_{10p}(x) = \Phi_{5p}(-x)$ and Theorem 3.7.

Theorem 3.7. *Let $p > 5$ be prime and let c_k be the coefficient of x^k in the cyclotomic polynomial $\Phi_{10p}(x)$ which has degree $4(p-1)$. Then for $0 \leq k \leq p-1$,*

$$c_{4p-4-k} = \begin{cases} 1 & \text{if } k = 0, 1 \mod 10 \\ -1 & \text{if } k = 5, 6 \mod 10 \\ 0 & \text{if } k = 2, 3, 4, 7, 8, 9 \mod 10 \end{cases}$$

Furthermore,

- *if $p = 1 \mod 5$, then*

$$c_{3p-3-k} = \begin{cases} 1 & \text{if } k = 0, 7 \mod 10 \\ -1 & \text{if } k = 2, 5 \mod 10 \\ 0 & \text{if } k = 1, 3, 4, 6, 8, 9 \mod 10 \end{cases}$$

- *if* $p = 2 \mod 5$, *then*

$$c_{3p-3-k} = \begin{cases} 1 & \text{if } k = 4, 5, 6, 7 \mod 10 \\ -1 & \text{if } k = 0, 1, 2, 9 \mod 10 \\ 0 & \text{if } k = 3, 8 \mod 10 \end{cases}$$

- *if* $p = 3 \mod 5$, *then*

$$c_{3p-3-k} = \begin{cases} 1 & \text{if } k = 6, 7, 8, 9 \mod 5 \\ -1 & \text{if } k = 1, 2, 3, 4 \mod 5 \\ 0 & \text{if } k = 0, 5 \mod 5 \end{cases}$$

- *if* $p = 4 \mod 5$, *then*

$$c_{3p-3-k} = \begin{cases} 1 & \text{if } k = 3, 6 \mod 10 \\ -1 & \text{if } k = 1, 8 \mod 10 \\ 0 & \text{if } k = 0, 2, 4, 5, 7, 9 \mod 10 \end{cases}$$

References

[1] C. F. Gauss: Disquisitiones Arithmeticae. Lipsiae, 1801 (Latin), Available in English translation in Springer-Verlag, New York, 1986. Translation by A. A. Clarke. Revised by W. C. Waterhouse, C. Greither and A. W. Grootendorst and with a preface by Waterhouse.

[2] L. Kronecker: Memoire sur les facteures irreductibles de 'lexpression $x^n - 1$. J. Math. Pures et Appls. 19, 177-192 (1854)

[3] M. Beiter: The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$, Amer. Math. Monthly 71, 769-770 (1964)

[4] H. Habermehl, S. Richardson and M. A. Szwajkos: A Note on Coefficients of Cyclotomic Polynomials. Math. Magazine 37, 183-185 (1964)

[5] T. Y. Lam and K. H. Leung: On the Cyclotomic Polynomial $\Phi_{pq}(X)$. Amer. Math. Monthly, 103, 562-564 (1996)

[6] C. Sanna: A Survey on Coefficients of Cyclotomic Polynomials. Expositiones Mathematicae, 40, 469-494 (2022)