Polynomial Form of Binary Cyclotomic Polynomials

Aaron Elliot
College of Information and Computer Science
University of Massachusetts Amherst
Computer Science Building, Amherst MA, 01002
E-mail: aelliot@cs.umass.edu

September 6, 2018

Abstract

This paper presents a closed form polynomial expression for the cyclotomic polynomial \( \Phi_{pq}(X) \), where \( p, q \) are distinct primes. We contrast this against expressions for binary cyclotomic polynomials in (Lam and Leung 1996) and (Lenstra 1979). In addition, we present a related result on factoring \( X^{ab} - 1 \), where \( a, b \) are coprime natural numbers.

1 Introduction

This paper presents two theorems. Theorem 2.3 is a closed form polynomial expression for the cyclotomic polynomial \( \Phi_{pq}(X) \), where \( p \) and \( q \) are distinct primes. Related to that result, theorem 2.4 is a factorization of \( X^{ab} - 1 \), where \( a \) and \( b \) are coprime natural numbers.

There exists a rich body of literature exploring the cyclotomic polynomial \( \Phi_{pq}(X) \). To my knowledge, the exploration of \( \Phi_{pq}(X) \) began with Miggotti in 1883, when he showed that the coefficients of \( \Phi_{pq}(X) \) are within \( \{1, -1, 0\} \).[Mig83]

Similarly to this paper, a multitude of authors have proposed explicit expressions for \( \Phi_{pq}(X) \). We contrast our expression for \( \Phi_{pq}(X) \) against the expressions proposed by Lenstra in 1979[HWL79] and Lam and Leung in 1996[LL96].
Lenstra demonstrated in 1979 that
\[
\Phi_{pq} = \sum_{i=0}^{\lambda-1} \sum_{j=0}^{\mu-1} X^{ip+jq} - \sum_{i=\lambda}^{\mu} \sum_{j=\mu}^{p-1} X^{ip+jq-pq},
\]

where \(\lambda, \mu \in \mathbb{N}\) such that \(\lambda < q, \mu < p, \lambda p \equiv q \pmod{1}\) and \(\mu p \equiv q \pmod{1}\.\)[HWL79]

Lam and Leung demonstrated in 1996 the conditions under which the coefficients of \(\Phi_{pq}(X)\) are 1, -1, or 0. Using a result from Boot and Greenberg[BG64] that there exists non-negative integers \(r, s\) such that \(rp + sq = (p-1)(q-1)\), Lam and Leung showed for \(\Phi_{pq}(X) = \sum_{i=0}^{(p-1)(q-1)} a_k X^k\), \(a_k = 1\) if and only if there exists a solution to \(k = ip + jq\) for some \(i \in [0, r]\) and \(j \in [0, s]\); \(a_k = -1\) if and only if there exists a solution to \(k + pq = ip + jq\) for some \(i \in [r+1, q-1]\) and \(j \in [s+1, p-1]\); lastly, \(a_k = 0\) otherwise.[LL96]

The main result of this paper, in theorem 2.3, stands at contrast against the results of Lam, Leung and Lenstra cited above. An advantage of the above expressions is that they lend themselves to some analysis tasks well. However, the main disadvantage of both the above expressions is that they require solving for integer solutions of \(\mu, \lambda\) and \(r, s\) respectively. A possible route for further research is investigating the full repercussions of the expression we present equalling the above expressions for \(\Phi_{pq}(X)\).

\section{Theorems}

\textbf{Definition 2.1.} For our purposes, we will use \(a \% b := \begin{cases} a - b \left\lfloor \frac{a}{b} \right\rfloor & : b \neq 0 \\ a & : b = 0 \end{cases}\)

\textbf{Remark 2.2.} Originally, I simply used lemma 2.7 and the Môbiüs-Dedekind formula to derive theorem 2.3. This meant reducing the division \(\Phi_{pq}(X) = \frac{\Phi_q(X^p)}{\Phi_q(X)}\). However, making this a rigorous proof meant contorting my argument to avoid division by 0. The below proof allowed me to avoid that problem entirely, and yielded theorem 2.4 as an intermediate result.

\textbf{Theorem 2.3.} Given distinct primes \(p\) and \(q\) such that \(p > q\),

\[
\Phi_{pq}(X) = (1 + (X - 1) \sum_{i=0}^{q-1} \sum_{j=1}^{q} X^{pi+qj}).
\]
**Polynomial Form of Binary Cyclotomic Polynomials**

**Proof.** Given distinct primes \( p, q \) such that \( p > q \), consider the following:

\[
X^{pq} - 1 = \prod_{k \in \{k \in \mathbb{N} : k \mid pq\}} \Phi_k(X)
\]

\[
= \prod_{k \in \{1, p, q, pq\}} \Phi_k(X)
\]

\[
= (X - 1)\left(\sum_{i=0}^{p-1} X^i\right)\left(\sum_{i=0}^{q-1} X^i\right)\Phi_{pq}(X)
\]

By Theorem 2.4, this implies,

\[
(X - 1)\left(\sum_{i=0}^{p} X^i\right)\left(\sum_{i=0}^{q} X^i\right)\Phi_{pq}(X) = (X - 1)\left(\sum_{i=0}^{p-1} X^i\right)\left(\sum_{i=0}^{q-1} X^i\right)(1 + (X - 1) \sum_{i=0}^{q-1} \sum_{j=1}^{\frac{pi-(pi)\%q}{q}} X^{pi-qj})
\]

\[
\Phi_{pq}(X) = (1 + (X - 1) \sum_{i=0}^{q-1} \sum_{j=1}^{\frac{pi-(pi)\%q}{q}} X^{pi-qj})
\]

\[
\square
\]

**Theorem 2.4.** Given \( a, b \in \mathbb{N} \) such that \( a \) is coprime to \( b \) and \( a > b \).

\[
X^{ab} - 1 = (X^a - 1)\left(\sum_{i=0}^{b-1} X^i\right)(1 + (X - 1) \sum_{i=0}^{b-1} \sum_{j=1}^{\frac{ai-(ai)\%b}{b}} X^{ai-bj})
\]

**Proof.** Given \( a, b \in \mathbb{N} \) such that \( a, b \) are coprime and \( a > b \), let \( U = \{(ai)\%b : \}

\[ i \in \{0, 1, 2, \ldots, b - 1\} \] and \( V = \{0, 1, 2, \ldots, b - 1\} \).

By lemmas 2.6, it follows that,

\[
X^{ab} - 1 = (X^a - 1) \sum_{i=0}^{b-1} X^{ia} \\
= (X^a - 1) \sum_{i=0}^{b-1} (X^{(ai)\%b}) + (X^b - 1) \sum_{j=1}^{ai\%b} X^{ai-bj} \\
= (X^a - 1) \sum_{i=0}^{b-1} (X^{(ai)\%b}) + (X^b - 1) \sum_{i=0}^{ai\%b} \sum_{j=1}^{b-1} X^{ai-bj} \\
= (X^a - 1) \sum_{u \in U} X^u + (X^b - 1) \sum_{i=0}^{b-1} \sum_{j=1}^{ai\%b} X^{ai-bj} \\
\]

By lemmas 2.7, it follows that,

\[
= (X^a - 1) \sum_{v \in V} X^v + (X^b - 1) \sum_{i=0}^{b-1} \sum_{j=1}^{ai\%b} X^{ai-bj} \\
= (X^a - 1) \sum_{i=0}^{b-1} X^i(1 + (X - 1) \sum_{j=1}^{ai\%b} X^{ai-bj}) \\
X^{ab} - 1 = (X - 1) \sum_{i=0}^{a-1} X^i(1 + (X - 1) \sum_{j=1}^{ai\%b} X^{ai-bj}) \\
\]

**Lemma 2.5.** Given \( a, b \in \mathbb{N} \) and \( c \in \{0, 1, \ldots, b - 1\} \) such that \( a \equiv_b c \), \( a\%b = c \).

**Proof.** Consider \( a, b \in \mathbb{N} \) and \( c \in \{0, 1, \ldots, b - 1\} \) such that \( a \equiv_b c \), in this lemma, we intend to prove \( a\%b = c \).

As \( a \equiv_b c \), it follows that there exists \( k \in \mathbb{Z} \) such that \( a = c + kb \). Thus,

\[
a\%b = (c + kb)\%b \\
= c + kb - b\lfloor \frac{c + kb}{b} \rfloor \\
= c + kb - kb - b\lfloor \frac{c}{b} \rfloor \\
= c + 0 - b(0) \\
= c
\]
Lemma 2.6. Given $a, b, i \in \mathbb{N}$ such that $a$ is coprime to $b$ and $a > b$,

$$X^{(ai)\%b} + (X^b - 1)(\sum_{j=1}^{\frac{ai-(ai)\%b}{b}} X^{ai-bj}) = X^{ai}$$

Proof. Consider $a, b \in \mathbb{N}$ such that $a$ is coprime to $b$ and $a > b$.

$$X^{(ai)\%b} + (X^b - 1)(\sum_{j=1}^{\frac{ai-(ai)\%b}{b}} X^{ai-bj}) = X^{(ai)\%b} + \left(\sum_{j=1}^{\frac{ai-(ai)\%b}{b}} X^{ai-bj}\right) - \left(\sum_{j=1}^{\frac{ai-(ai)\%b}{b}} X^{ai-bj}\right)$$

$$= X^{(ai)\%b} + \left(\sum_{j=0}^{\frac{ai-(ai)\%b}{b}-1} X^{ai-bj}\right) - \left(\sum_{j=1}^{\frac{ai-(ai)\%b}{b}} X^{ai-bj}\right)$$

$$= X^{(ai)\%b} + X^{ai} - X^{ai-b(\frac{ai-(ai)\%b}{b})}$$

$$= X^{(ai)\%b} + X^{ai} - X^{(ai)\%b}$$

$$= X^{ai}$$

Lemma 2.7. Given $a, b \in \mathbb{N}$ such that $a$ is coprime to $b$ and $a > b$,

$$\{(ai)\%b : i \in \{0, ..., b-1\}\} = \{0, ..., b-1\}$$

Proof. Given $a, b \in \mathbb{N}$ such that $a$ is coprime to $b$ and $a > b$, let $U = \{(ai)\%b : i \in \{0, ..., b-1\}\}$, $V = \{0, ..., b-1\}$ and $W = \{ai : i \in \{0, ..., b-1\}\}$. We intend to prove that $U = V$. We will prove this in two steps, (1) and (2). Together statements (1) and (2) imply $U = V$.

Given $a, b \in \mathbb{N}$ such that $a$ is coprime to $b$ and $a > b$, let $U = \{(ai)\%b : i \in \{0, ..., b-1\}\}$, $V = \{0, ..., b-1\}$ and $W = \{ai : i \in \{0, ..., b-1\}\}$. In this lemma, we intend to prove that $U = V$. We will prove this in two steps, (1) and (2). Together statements (1) and (2) imply $U = V$.

First we prove statement (1). By the definition of complete residue systems, $V$ is a complete residue system modulo $b$ [Apo76]. Consider some $u \in U$. It follows there exists $i \in V$ such that $ai\%b = u$. It follows that there exists $v \in V$ such that $ai \equiv_b v$. By lemma 2.5, it follows that $ai\%b = v$ and therefore $u \in V$. Which suffices to show statement (1).
Second we prove statement (2). As \(a, b\) are coprime, it follows that \(\gcd(a, b) = 1\). From Apostol 1976 theorem 5.11[Apo76], this implies that \(W\) is a complete residue system modulo \(b\). Consider some \(v \in V\). It follows there exists \(w \in W\) such that \(v \equiv_b w\). By lemma 2.5, this implies \(v = w \% b\). By our definition of \(U\), \(w \% b \in U\), and therefore \(v \in U\). Which suffices to show statement (2).

\[\square\]

Acknowledgement

I would like to thank Dr. Mark Kon carefully going over my first draft and indicating where it needed improvement. As well as Dr. Thomas Enkosky for mentoring me during my time at Boston University.

References


