SOME CLASSES OF GENERALIZED CYCLOTOMIC POLYNOMIALS

by

Abdullah Al-Shaghay

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

at

Dalhousie University
Halifax, Nova Scotia
December 2019

Table of Contents

List of Tables

List of Figures

Abstract

For a positive integer n the n^{th} cyclotomic polynomial can be written as

$$\Phi_n(x) = \prod_{\substack{k=1 \\ k\in(\mathbb{Z}/n\mathbb{Z})^\times}}^{n} (x - e^{\frac{2\pi ik}{n}}).$$

When $n = p$ is an odd prime, the n^{th} cyclotomic polynomial has the special form

$$\Phi_p(x) = \sum_{k=0}^{p-1} x^k = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

These two representations of the cyclotomic polynomials highlight the roots of $\Phi_n(x)$ and the coefficients of $\Phi_n(x)$, respectively. Continuing with the work of Kwon, J. Lee, and K. Lee and Harrington we investigate the generalization of the cyclotomic polynomials in two distinct ways; one affecting the roots of $\Phi_n(x)$ and the other affecting the coefficients of $\Phi_n(x)$.

In the final chapter of the thesis we discuss congruences for particular binomial sums and use those congruences to prove results concerning two special cases of Jacobi polynomials, the Chebyshev polynomials and the Legendre polynomials.

List of Abbreviations and Symbols Used

Notation	Description
$a \equiv b \pmod{n}$	a is congruent to b modulo n; that is, $b - a = kn$ for some integer k.
$a \mid b$	a divides b; that is, $b = ak$ for some integer k.
(a, b)	Greatest common divisor of a and b.
$\left(\frac{a}{p}\right)$	Legendre symbol of a and p defined for integers a and odd primes p for which $p \nmid a$ to be 1 if $x^2 \equiv a \pmod{p}$ for some x and -1 otherwise.
$\binom{n}{k}$	Binomial coefficient defined by $\frac{n!}{(n-k)!k!}$.
$\Phi_n(x)$	The n^{th} cyclotomic polynomial.
$T_n(x)$	The n^{th} Chebyshev polynomial of the first kind.
$U_n(x)$	The n^{th} Chebyshev polynomial of the second kind.
$P_n(x)$	The n^{th} Legendre polynomial.
$\varphi(n)$	The Euler totient function.
$\mu(n)$	The Möbius function.
$H \leq G$	H is a subgroup of G.
$H \trianglelefteq G$	H is a normal subgroup of G.
$< x >$	The cyclic group generated by the element x.
$\|G\|$	The order of the group G.
$\mathbb{Z}/n\mathbb{Z}$	Ring of integers modulo n.
$\mathbb{Q}_p$	Field of p-adic numbers.
$\mathbb{Z}_p$	Ring of p-adic integers in $\mathbb{Q}_p$.
$R^\times$	Group of units in R.
$R[x]$	Ring of polynomials in x with coefficients in R.
$\mathbb{F}(\alpha_1, \ldots, \alpha_n)$	The smallest subfield of $\mathbb{C}$ containing $\mathbb{F}$ and $\alpha_1, \ldots, \alpha_n$.
$R[\alpha_1, \ldots, \alpha_n]$	The smallest subring of $\mathbb{C}$ containing R and $\alpha_1, \ldots, \alpha_n$.
$\rho(f(x), g(x))$	The resultant of the two polynomials $f(x)$ and $g(x)$.
$D(f(x))$	The discriminant of the polynomial $f(x)$.

Acknowledgements

I would like to especially acknowledge and thank my supervisor, Dr. Karl Dilcher, for everything he has done for me. Karl was my first year calculus professor and over the past decade he has been and continues to be a wonderful teacher, supervisor, and mentor. My academic pursuits would not have been possible without his assistance, generosity, patience, and understanding. I will forever be grateful for his kindness.

I would like to thank my thesis committee and my external examiner, Dr. Keith Johnson, Dr. Rob Noble, and Dr. Michael Filaseta. Thank you for taking the time to read and comment on my thesis. I really value and respect your opinions and suggestions. All of your help is greatly appreciated and this thesis is undoubtedly improved because of your inputs.

I would like to thank the Department of Mathematics and Statistics at Dalhousie University for all of their support. The faculty, administrative staff, and other students have made my experience very enjoyable and memorable.

Chapter 1

Introduction

The study of polynomials goes back to as early as 250 A.D with Diophantus. Determining the roots of polynomials and solving algebraic equations is one of the oldest problems in mathematics. The theory of polynomials is closely linked to the theory of fields and derives from the solution of algebraic equations and the geometric construction problems to which they were equivalent [25, ppg. 49–51]. Babylonian and Greek mathematicians had success solving quadratic and certain quartic equations. Italian mathematicians, working on cubic equations and the general quartic solution began to notice a connection between the roots of a polynomial and its coefficients. Cardano had the initial idea of the notion of the multiplicity of a root and began calculations with the square roots of negative numbers. Cardano's pupils began formalizing the rules for calculation with complex numbers and in 1545 L. Ferrari succeeded in solving the general quartic. Viète explicitly described the relationship between the roots and the coefficients of an algebraic equation. Descartes studied and managed to distinguish between algebraic and transcendental functions. Due to work by Leibniz and Johann Bernoulli, the calculus of complex numbers began to be formalized more and the question of the decomposition of a polynomial into linear factors was pursued until the fundamental theorem of algebra was proved in 1806 by Argand [44].

Related to the study of polynomials, the study of binomial coefficients goes back to as early as the 2nd Century BC with Pingala, although the notation we use today was introduced in 1826 by von Ettingshausen. One of the avenues pursued in this history has been the study of congruences of binomial coefficients modulo a prime p.

For a more detailed discussion regarding the history of polynomials, or mathematics in general, the reader is referred to [21], [25], and [44].

Of particular historical interest to this thesis, in the late seventeenth century and early eighteenth century Cotes and deMoivre reduced the solution of the equation $x^n - 1 = 0$ to the division of the circle into n equal parts. The n^{th} cyclotomic polynomial can also be thought of as the unique irreducible polynomial with integer coefficients that divides $x^n - 1$ but does not divide $x^k - 1$ for any $k < n$. A well known formula for the n^{th} cyclotomic polynomial is given in the proposition below.

Proposition 1.1. *For any positive integer n, the n^{th} cyclotomic polynomial may be calculated as*

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ (k,n)=1}} (x - e^{\frac{2\pi i k}{n}}).$$

There is an inherent link between cyclotomic polynomials and primitive roots of unity given by the following formula.

Proposition 1.2.

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

This shows us that x is a root of $x^n - 1$ if and only if it is a d^{th} primitive root of unity for some $d|n$.

In the next two chapters of this thesis we study two separate generalizations of the cyclotomic polynomial. The first generalization will be achieved by altering the *roots* of the cyclotomic polynomials to arrive at a family of polynomials we have named the Cyclotomic Subgroup-Polynomials. On the other hand, the second generalization will be achieved by altering the *coefficients* of the cyclotomic polynomials. We then present some binomial coefficient congruences that lead to polynomial congruences for a special family of polynomials (the Jacobi polynomials) in the following chapter.

Chapter 2

Cyclotomic Subgroup-Polynomials

2.1 Preliminaries

In this chapter, we discuss a generalization of cyclotomic polynomials. In the next chapter, we will alter the coefficients of a given cyclotomic polynomial to obtain one possible generalization. Here, the roots of the cyclotomic polynomial will be altered instead.

As we know, $\Phi_n(x)$ can be written as

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - w^k), \quad (w = e^{\frac{2\pi i k}{n}}),$$

where $(\mathbb{Z}/n\mathbb{Z})^\times$ is the group of units modulo n. In [35], M. Kwon, J. Lee, and K.S. Lee used the fundamental theorem of Galois theory to generalize the idea of cyclotomic polynomials and discussed irreducible polynomials associated with primitive n^{th} roots of unity.

While the motivation for this chapter comes from the work of Kwon, J. Lee, and K.S. Lee, this type of polynomial construction appears in the literature in at least two earlier instances: Wójcik's paper of 1969 [57] and Stauduhar's paper of 1973 [55]. In [55] Stauduhar gives a technique for the determination of the Galois groups of irreducible polynomials with integer coefficients while in [57] Wójcik gives completely algebraic proofs of special cases of Dirichlet's theorem on primes in arithmetic progression.

2.2 Algebraic Background

In this section we will introduce only those results from Algebra that are required to discuss the generalization of Kwon, Lee, and Lee in [35]. All of the results presented here, as well as additional related ones, can be found in standard introductory textbooks in Algebra, such as [20] or [30].

Of importance to this chapter are the concepts of cyclic groups, normal subgroups, quotient groups, and Galois groups. We now recall these below.

Definition 2.1. *A group H is cyclic if H can be generated by a single element. That is, there is some element $x \in H$ such that $H = \{x^n | n \in \mathbb{Z}\}$, where the operation is multiplication. The cyclic group generated by x is denoted by $< x >$.*

A cyclic group is then completely determined by its generator. Therefore we have:

Theorem 2.2. *Any two cyclic groups of the same order are isomorphic.*

The number of subgroups of a finite cyclic group and the order of the subgroups of a finite cyclic group are discussed with examples in [10], [51], and [56]. The structure of cyclic groups can be completely determined as follows.

Theorem 2.3. *Let $H =< x >$ be a cyclic group.*

(i) Every subgroup of H is cyclic.

(ii) If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of order a. This subgroup is the cyclic group $< x^d >$, where $d = \frac{n}{a}$. Furthermore, for every integer m, $< x^m >=< x^{(n,m)} >$, so that the subgroups of H correspond bijectively with the positive divisors of n.

A normal subgroup $N \trianglelefteq G$ is a subgroup that is invariant under conjugation by elements of the group G. That is, $gng^{-1} \in N$ for all $g \in G, n \in N$. Normal subgroups N are also the subgroups such that left and right congruence modulo N coincide. That is, left and right congruence define the same equivalence relation on the group G. We formalize this equivalence relation below:

Theorem 2.4. *If N is a normal subgroup of a group G and G/N is the set of all (left) cosets of N in G, then G/N is a group under the binary operation given by $(aN)(bN) = (ab)N$. Further, if G is finite then G/N has order $|G|/|N|$.*

This construction defines an important group which is closely tied to homomorphisms on the larger group G.

Definition 2.5. *The group G/N in Theorem 2.4 is called the quotient group or factor group of G by N.*

The set of all field automorphisms $F \to F$ that fix a given subfield K forms a group under composition of functions, denoted by Gal (F/K) and referred to as the Galois group of F/K. It was Galois who discovered that many of the group-theoretical properties of this automorphism group correspond to properties of roots of polynomials over the subfield K. This vast area of study is referred to as Galois Theory. We only require the following small lemma:

Lemma 2.6. *Let $w = e^{\frac{2\pi ik}{n}}$ with $(k, n) = 1$ be a primitive n^{th} root of unity and let $\mathbb{Q}(w)$ be the simple extension field of $\mathbb{Q}$ generated by w. Then the Galois group $Gal(\mathbb{Q}(w)/\mathbb{Q})$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$ via the mapping $\theta : (\mathbb{Z}/n\mathbb{Z})^\times \to Gal(\mathbb{Q}(w)/\mathbb{Q})$, defined by $\theta[s](w) = w^s$, $s \in (\mathbb{Z}/n\mathbb{Z})^\times$.*

2.3 Galois Irreducible Polynomials

We are now ready to define the main object of study in [35] and the related papers [37], [38]. Let $w = e^{\frac{2\pi i}{n}}$ be a primitive n^{th} root of unity, H be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and $(\mathbb{Z}/n\mathbb{Z})^\times/H = \{h_1H, h_2H, \ldots, h_lH\}$ be the corresponding quotient group. For each $1 \leq k \leq l$, let

$$a_k = \sum_{h \in H} w^{h_k h}. \tag{2.1}$$

The monic square-free polynomial having $a_1, \ldots, a_l$ as its roots will be denoted by $J_{n,H}(x)$. That is,

$$J_{n,H}(x) = (x - a_1)(x - a_2) \cdots (x - a_l). \tag{2.2}$$

For a fixed positive integer n, $J_{n,H}(x)$ only depends on the subgroup H and not the choice of coset representatives h_k. Choosing different coset representatives $h'_k \in (\mathbb{Z}/n\mathbb{Z})^\times$ would only permute the sum that defines a_k in (2.1) and therefore keep $J_{n,H}(x)$ unchanged. Irreducible polynomials with integer coefficients of the form of $J_{n,H}(x)$ were called *Galois Irreducible Polynomials* by the authors of [35] and [38].

Definition 2.7. *In the general case, we will refer to $J_{n,H}(x)$ as a Cyclotomic Subgroup-Polynomial.*

Example 2.8. If we take the trivial subgroup, $\{1\}$, which is obviously a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ for all n, we recover the cyclotomic polynomials. Indeed, let n be a positive integer and let $G = (\mathbb{Z}/n\mathbb{Z})^\times$. Since $H = \{1\}$, we have

$$G/H \cong G = \{g_1, g_2, \ldots, g_{\varphi(n)}\}.$$

Then,

$$a_k = w^{g_k}, \quad (w = e^{\frac{2\pi i}{n}}),$$

for $k = 1, 2, \ldots, \varphi(n)$ and we have

$$\begin{aligned} J_{n,\{1\}}(x) &= (x - a_1)(x - a_2)\cdots(x - a_{\varphi(n)}) \\ &= (x - w^{g_1})(x - w^{g_2})\cdots(x - w^{g_{\varphi(n)}}) \\ &= \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - w^k) \\ &= \Phi_n(x). \end{aligned}$$

Since $J_{n,\{1\}} = \Phi_n(x)$, we see that these polynomials are indeed generalizations of the cyclotomic polynomials. We now calculate some examples that do not only result in a cyclotomic polynomial.

Example 2.9. If we consider the entire group, $(\mathbb{Z}/n\mathbb{Z})^\times$, which is trivially a subgroup of itself for all n, we obtain one of only three possible monic square-free polynomials depending on the prime decomposition of the integer n. Specifically, if n is a square-free positive integer with an odd number of prime factors we get $x + 1$; if n is

a square-free positive integer with an even number of prime factors we get $x-1$, and if n has a squared prime factor, we get x, as we will now show.

Let n be a positive integer and $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$. Since $H = \{g_1, g_2, \ldots, g_{\varphi(n)}\} = G$, we have

$$G/H \cong \{1\}.$$

Then,

$$a_1 = a = w^{g_1} + w^{g_2} + \ldots + w^{g_{\varphi(n)}} = \mu(n), \quad (w = e^{\frac{2\pi i}{n}}),$$

where

$$\mu(n) = \begin{cases} 1 & \text{when } n \text{ square-free and has an odd number of prime factors,} \\ -1 & \text{when } n \text{ square-free and has an even number of prime factors,} \\ 0 & \text{when } n \text{ has a squared prime factor.} \end{cases}$$

is the Möbius function evaluated at n and the last equality is obtained using Theorem A.21 in Appendix A. Hence we have

$$J_{n,G}(x) = \begin{cases} x+1 & \text{when } n \text{ square-free and has an odd number of prime factors,} \\ x-1 & \text{when } n \text{ square-free and has an even number of prime factors,} \\ x & \text{when } n \text{ has a squared prime factor.} \end{cases}$$

Example 2.10. If we take $n = 7$, then $G = (\mathbb{Z}/7\mathbb{Z})^{\times} = \{1, 2, 3, 4, 5, 6\}$ and $w = e^{\frac{2\pi i}{7}}$. G has the four subgroups

$$\begin{aligned} H_1 &= \{1\}, \\ H_2 &= \{1, 6\}, \\ H_3 &= \{1, 2, 4\}, \\ H_4 &= \{1, 2, 3, 4, 5, 6\} = G, \end{aligned}$$

with corresponding quotients

$$\begin{aligned} G/H_1 &= \{\{1\},\{2\},\{3\},\{4\},\{5\},\{6\}\}, \\ G/H_2 &= \{\{1,6\},\{2,5\},\{3,4\}\}, \\ G/H_3 &= \{\{1,2,4\},\{3,5,6\}\}, \\ G/H_4 &= \{1,2,3,4,5,6\}\}. \end{aligned}$$

We then have:

$$\begin{aligned} J_{7,H_1}(x) &= (x-w)(x-w^2)(x-w^3)(x-w^4)(x-w^5)(x-w^6) \\ &= x^6+x^5+x^4+x^3+x^2+x+1 = \Phi_7(x). \\ J_{7,H_2}(x) &= (x-(w+w^6))(x-(w^2+w^5))(x-(w^3+w^4)) \\ &= x^3+x^2-2x-1. \\ J_{7,H_3}(x) &= (x-(w+w^2+w^4))(x-(w^3+w^5+w^6)) \\ &= x^2+x+2. \\ J_{7,H_4}(x) &= (x-(w+w^2+w^3+w^4+w^5+w^6)) \\ &= x+1. \end{aligned}$$

It is of note that, in this example, each $J_{n,H_j}(x)$ is an irreducible polynomial. We will see later in this chapter that this is not a coincidence and $J_{p,H}(x)$ is irreducible for all H when $p > 2$ is a prime number.

We close this section by summarizing our observations from Example 2.8 and Example 2.9 with the following lemma.

Lemma 2.11. *Let n be a positive integer and $J_{n,H}(x)$ be the Cyclotomic Subgroup-Polynomial corresponding to n and the subgroup $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$. Then we have*

(i) $J_{n,\{1\}}(x) = \Phi_n(x)$ *for all* n.

(ii) $$J_{n,(\mathbb{Z}/n\mathbb{Z})^\times}(x) = \begin{cases} x-1 & n \text{ square-free and has an even number of prime factors,} \\ x & n \text{ has a square prime factor,} \\ x+1 & n \text{ square-free and has an odd number of prime factors.} \end{cases}$$

2.4 Known Results

Kwon, Lee, Lee, and Kim presented a number of interesting results regarding these Galois Irreducible Polynomials in [35] and [38]. This section is meant to serve as a collection of their results. For proofs, the reader is referred to the original papers [35] and [38]. In this section, unless otherwise stated, we shall take n to be a positive integer, $p > 2$ a prime number, and $w = e^{\frac{2\pi i}{n}}$ a primitive n^{th} root of unity.

The first result shows us that the coefficients of the Cyclotomic Subgroup-Polynomials are elements of the field $\mathbb{Q}$:

Theorem 2.12 ([35], Theorem 2.2)**.** *For any subgroup H of $(\mathbb{Z}/n\mathbb{Z})^\times$, $J_{n,H}(x) \in \mathbb{Q}[x]$.*

It is of note that, in a remark in their paper [35], Kwon, J.E Lee, K.S Lee, and Kim actually provide a proof of the stronger result that the coefficients of these polynomials are indeed integers. That is, we have $J_{n,H}(x) \in \mathbb{Z}[x]$ for all integers n.

Kwon, Lee, and Lee then answer the question of when $J_{n,H}(x)$ is a monomial:

Theorem 2.13 ([35], Corollary 2.4)**.** *Let H be a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. If $\zeta = \sum_{h\in H} w^h \in \mathbb{Q}$, then $\zeta = 0$ and hence $J_{n,H}(x) = x^l$, where $l = |(\mathbb{Z}/n\mathbb{Z})^\times/H|$.*

Example 2.14. Let us consider the case $n = 8$ and $w = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}}$. Then $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ and we look at the case $H = \{1, 5\}$. We calculate:

$$\begin{aligned} a_1 &= w + w^5 = e^{\frac{\pi i}{4}} + e^{\frac{5\pi i}{4}} = 0, \\ a_2 &= w^3 + w^7 = e^{\frac{3\pi i}{4}} + e^{\frac{7\pi i}{4}} = 0, \\ J_{8,\{1,5\}}(x) &= (x-0)(x-0) = x^2, \end{aligned}$$

as expected.

In the following two results, the authors of [35] then consider the special case when $n = p$ is an odd prime:

Theorem 2.15 ([35], Theorem 2.5)**.** *If p is an odd prime number, then for any subgroup H of $(\mathbb{Z}/p\mathbb{Z})^\times$ the polynomial $J_{p,H}(x)$ is the minimal polynomial of $\zeta = \sum_{h\in H} w^h$ over $\mathbb{Q}$.*

Since the minimal polynomial of an element is an irreducible polynomial, this theorem confirms what was observed in Example 2.10, namely that $J_{7,H}(x)$ was irreducible for all subgroups $H \leq (\mathbb{Z}/7\mathbb{Z})^\times$. Related to this observation, we have the following theorem:

Theorem 2.16 ([35], Corollary 3.2)**.** *Let p be an odd prime number and $w = e^{2\pi i/p}$. Then any subfield F of $\mathbb{Q}(w)$ over $\mathbb{Q}$ can be expressed as $F = \mathbb{Q}(\zeta)$, where $\zeta = \sum_{h\in H} w^h$ for some subgroup H of $(\mathbb{Z}/n\mathbb{Z})^\times$.*

The irreducibility of $J_{n,H}(x)$ for different integers n is addressed in these next three theorems:

Theorem 2.17 ([35], Theorem 3.6)**.** *Let n be a square-free integer. Then $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$ for any subgroup H of $(\mathbb{Z}/n\mathbb{Z})^\times$.*

We note that Theorem 2.16 is a special case of Theorem 2.17 since all primes are square-free integers.

If we have certain information about the structure of the subgroup H of the group G, the following two theorems allow us to conclude the irreducibility of $J_{n,H}(x)$. More specifically:

Theorem 2.18 ([35], Corollary 3.3)**.** *If H is a maximal proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\zeta = \sum_{h\in H} w^h \notin \mathbb{Q}$, then $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$.*

Example 2.19. If we take $n = 12$, then $G = (\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$ and $w = e^{\frac{\pi i}{6}}$. G has the five subgroups

$$\begin{aligned}
H_1 &= \{1\}, \quad \zeta = \frac{\sqrt{3}+i}{2},\\
H_2 &= \{1, 5\}, \quad \zeta = i,\\
H_3 &= \{1, 7\}, \quad \zeta = 0,\\
H_4 &= \{1, 11\}, \quad \zeta = \sqrt{3},\\
H_5 &= \{1, 5, 7, 11\}, \quad \zeta = 0.
\end{aligned}$$

We then have:

$$\begin{aligned}
J_{12,H_1}(x) &= (x-w)(x-w^5)(x-w^7)(x-w^{11}) \\
&= x^4 - x^2 + 1 = \Phi_{12}(x). \\
J_{12,H_2}(x) &= (x-(w+w^5))(x-(w^7+w^{11}) \\
&= x^2 + 1. \\
J_{12,H_3}(x) &= (x-(w+w^7))(x-(w^5+w^{11})) \\
&= x^2. \\
J_{12,H_4}(x) &= (x-(w+w^{11}))(x-(w^5+w^7)) \\
&= x^2 - 3. \\
J_{12,H_5}(x) &= (x-(w+w^5+w^7+w^{11})) \\
&= x.
\end{aligned}$$

It is of note that, in this example, not every $J_{n,H_j}(x)$ is an irreducible polynomial.

Theorem 2.20 ([35], Theorem 3.1)**.** *Let H be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and*

$$(\mathbb{Z}/n\mathbb{Z})^\times/H = \{h_1H, \ldots, h_lH\}.$$

Let $a_k = \sum_{h\in H} w^{h_k h}$, $k = 1, \ldots, l$ and $\mathbb{Q}(w)_H$ be the subfield of $\mathbb{Q}(w)$ fixed by $\{\theta[h] : h \in H\}$. Then $J_{n,H}(x) = (x-a_1)\cdots(x-a_l)$ is irreducible over $\mathbb{Q}$ if and only if $\mathbb{Q}(\zeta) = \mathbb{Q}(w)_H$, where $\zeta = \sum_{h\in H} w^h$.

As an application of the irreducibility of $J_{n,H}(x)$ presented in both [35] and [38], the authors provide an alternate proof of the following previously known theorem. For an interesting discussion on this theorem the reader is referred to [8].

Theorem 2.21 ([35], Theorem 3.5)**.** *If $n > 2$ and $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ then $\cos(\frac{2\pi}{n}k) \notin \mathbb{Q}$.*

Theorem 2.21 is the result of a corollary found in [35]:

Lemma 2.22 ([35], Corollary 3.4)**.** *For any positive integer $n > 2$,*

$$p(x) = \prod_{\substack{k\in(\mathbb{Z}/n\mathbb{Z})^\times, \\ k\le\varphi(n)/2.}} (x - (w^k - w^{-k}))$$

is irreducible over $\mathbb{Q}$.

Proof. Let $H = \{-1, 1\}$ and $\zeta = w + w^{-1}$. Then we have that $p(x) = J_{n,H}(x)$. We will now argue that $\mathbb{Q}(w)_H$, the fixed field of the set $\{\sigma \in Gal(\mathbb{Q}(w)/\mathbb{Q}) : \sigma(w) = w \text{ or } \sigma(w) = w^{-1}\}$, is equal to $\mathbb{Q}(\zeta)$.

Consider $\alpha = \sum_{k=0}^{m} c_k w^k \in \mathbb{Q}(w)_H$. Then, by the definition of the fixed field, we have $\sum_{k=0}^{m} c_k w^{-k} = \alpha$ also, which implies

$$2\alpha = \sum_{k=0}^{m} c_k (w^k + w^{-k}).$$

Using mathematical induction, and the identity

$$w^{k+1} + w^{-(k+1)} = (w^k + w^{-k})(w + w^{-1}) - (w^{k-1} + w^{-(k-1)}),$$

we know that $w^k + w^{-k} \in \mathbb{Q}(\zeta)$ for all k. This implies $\mathbb{Q}(w)_H \subseteq \mathbb{Q}(\zeta)$. This, combined with $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(w)_H$, shows that $\mathbb{Q}(\zeta) = \mathbb{Q}(w)_H$. Hence, by Theorem 2.20, we see that $p(x) = J_{n,H}(x)$ is irreducible, as required. □

We are now ready to prove Theorem 2.21.

Proof of Theorem 2.21. Let $n > 2$ be a positive integer and let k be relatively prime to n. Then we have that $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $w = e^{\frac{2\pi i}{n}}$ is a primitive n^{th} root of unity. Taking $H = \{-1, 1\}$, we see that $J_{n,H}(x) = p(x)$ from the statement of Lemma 2.22. Moreover, $a_k = w^k + w^{-k} = e^{\frac{2\pi ik}{n}} + e^{-\frac{2\pi ik}{n}} = 2\cos\left(\frac{2\pi ik}{n}\right)$. We have now shown that $2\cos\left(\frac{2\pi ik}{n}\right)$ is the root of a polynomial of degree ≥ 2 which is irreducible over $\mathbb{Q}$, and this in turn shows that $\cos\left(\frac{2\pi ik}{n}\right) \notin \mathbb{Q}$, as required. □

Having presented the concepts of Galois Irreducible Polynomials / Cyclotomic Subgroup-Polynomials, we now turn the discussion to new results for the remainder of this chapter. It has been established for which values of n $J_{n,H}(x)$ is irreducible; we now turn our attention to the study of the coefficients and roots of $J_{n,H}(x)$.

2.5 Cases of Interest

To help focus our efforts, we will restrict the values of n to consider. Of special interest to us will be the study of the Cyclotomic Subgroup-Polynomials corresponding to those integers n for which $G = (\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group. Since this choice means that there exists a unique subgroup $H \leq G$ of order $|H| = d$ for each $d \,|\, |G|$, we have an expectation of the number of polynomials $J_{n,H}(x)$ and their degrees for each choice of n. The integers of interest are precisely those having primitive roots, and so we restrict our attention to numbers of the form $n = 2, 4, p^\alpha$, and $2p^\alpha$, where α is a positive integer and p is an odd prime.

Moreover, of particular interest to us will be the cases when n is equal to a prime that is congruent to 1 modulo 3 and when n is equal to a prime congruent to 1 modulo 4. In these cases, we are guaranteed a subgroup $H \leq G$ of index three and of index four, respectively, as well as a cubic Cyclotomic Subgroup-Polynomial and a quartic Cyclotomic Subgroup-Polynomial, respectively.

2.6 Coefficients

In this section, we will investigate the coefficients of different Cyclotomic Subgroup-Polynomials. We will consider cases by one of two ways: we either restrict the degree of the polynomial $J_{n,H}(x)$ by picking a subgroup H of appropriate index, or we restrict the order of the subgroup H, itself.

2.6.1 The Case $J_{p,H}(x)$ Where p is an Odd Prime

We begin by studying the case $n = p$, for an arbitrary odd prime p, before specializing to particular congruence classes.

We start this subsection by calculating all of the Cyclotomic Subgroup-Polynomials for the prime $p = 11$ in the following example:

Example 2.23. For $n = p = 11$. we have

$$\begin{aligned} H_1 &= \{1\}, & J_{11,H_1}(x) &= \Phi_{11}(x), \\ H_2 &= \{1, 10\}, & J_{11,H_2}(x) &= x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1, \\ H_3 &= \{1, 3, 4, 5, 9\}, & J_{11,H_3}(x) &= x^2 + x + 3, \\ H_4 &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}, & J_{11,H_4}(x) &= x + 1. \end{aligned}$$

From the polynomials in this example, as well as the polynomials in Example 2.10, it seems that the leading and the next-to-leading coefficients are 1.

We formally state our observation as the following lemma:

Lemma 2.24. *Let p be an odd prime. Then the leading and next-to-leading coefficients of $J_{p,H}(x)$ are all 1.*

Proof. We will make use of Viète's formulas, which relate the coefficients of a polynomial to its roots, to prove the lemma. By their construction, it is clear that these polynomials are monic. For the next-to-leading coefficient, we consider Viète's formula to see that our coefficient is equal to

$$\begin{aligned} (-1) \cdot \sum_{k=1}^{\frac{p-1}{|H|}} a_k &= - \sum_{k=1}^{\frac{p-1}{|H|}} \sum_{h \in H} w^{h_k h} \\ &= - \sum_{j \in (\mathbb{Z}/p\mathbb{Z})^\times} w^j = -(-1) \\ &= 1, \end{aligned}$$

as required. □

In our proof of Lemma 2.24, the fact that $n = p$ was an odd prime was only used in the second last line. A completely analogous argument allows us to state the more general result:

Lemma 2.25. *Let n be a positive integer. Then the leading and next-to-leading coefficients of $J_{n,H}(x)$ are 1 and $-\mu(n)$ respectively.*

Proof. The proof of this lemma is analogous to that of Lemma 2.24 except for the second last equality which is obtained using the identity

$$\sum_{j\in(\mathbb{Z}/n\mathbb{Z})^\times} w^j = \mu(n);$$

see again Theorem A.21 in the appendix. □

From Example 2.10 and Example 2.23, as well as more numerical experimentation, we find the following:

Lemma 2.26. *Let* $J_{p,H}(x) = x^m + x^{m-1} + b_{m-2}x^{m-2} + \ldots + b_0$. *Then*

$$b_{m-2} = \begin{cases} \frac{p-1}{2} - \frac{|H|}{2}, & \text{if } |H| \text{ is even,} \\ \frac{|H|+1}{2}, & \text{if } |H| \text{ is odd.} \end{cases}$$

Proof. Using Viète's formula, we know that the coefficient of interest is the sum over all possible 2-products of the roots of $J_{p,H}(x)$. We begin by calculating the total number of terms in our "Viéte sum":

$$N := |H|^2 \cdot \binom{\frac{p-1}{|H|}}{2} = |H|^2 \cdot \frac{\frac{p-1}{|H|}\left(\frac{p-1}{|H|} - 1\right)}{2} = \frac{(p-1)(p-1-|H|)}{2}.$$

Case 1 (The index of H is even): Because of the group structure of the quotient group $(\mathbb{Z}/p\mathbb{Z})^\times / H \cong \mathbb{Z}/2k\mathbb{Z}$ for an integer k, as well as the group structure of $(\mathbb{Z}/p\mathbb{Z})^\times$, we know that we will have no terms that equal 1 in our sum; each element and its inverse are in the same coset. All of the terms will be in groups of $(p-1)$ terms that equal -1, namely $(w + w^2 + \ldots + w^{p-1})$. Therefore,

$$b_{m-2} = \frac{N}{(p-1)} = \frac{p-1-|H|}{2} = \frac{p-1}{2} - \frac{|H|}{2},$$

as required.

Case 2 (The index of H is odd): Because of the group structure of the quotient group $(\mathbb{Z}/p\mathbb{Z})^\times / H \cong \mathbb{Z}/(2k+1)\mathbb{Z}$ for an integer k, as well as the group structure of $(\mathbb{Z}/p\mathbb{Z})^\times$, we know that we will have $\frac{p-1}{2}$ terms that equal 1 in our sum; each

element and its inverse are in different cosets and will be multiplied together. The remainder of the terms will be in groups of $(p-1)$ that once again equal -1, namely $(w + w^2 + \ldots + w^{p-1})$. Therefore,

$$b_{m-2} = \frac{p-1}{2} - \frac{N - \frac{p-1}{2}}{p-1} = \frac{|H|+1}{2},$$

as required. □

2.6.2 The Case $J_{p,\{1,-1\}}(x)$

We now turn our attention to subgroups $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ of order 2, where p is an odd prime. This is a particular case of interest because not only does every group $(\mathbb{Z}/p\mathbb{Z})^\times$ have a subgroup H of order 2, but we also know the two elements in H for all p. Since p is an odd prime, we know that $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$ will be even. Then we have a cyclic group of even order, which must have a unique subgroup of order 2, namely $H = \{-1, 1\}$. The polynomials $J_{p,\{-1,1\}}(x)$ are the focus of this subsection. We begin our discussion by listing the first few examples of these polynomials.

Example 2.27. The polynomials $J_{p,\{-1,1\}}(x)$ for the primes $p = 3, 5, 7, 11, 13$, and 17 are as follows:

$$\begin{aligned}
J_{3,\{-1,1\}}(x) &= x + 1, \\
J_{5,\{-1,1\}}(x) &= x^2 + x - 1, \\
J_{7,\{-1,1\}}(x) &= x^3 + x^2 - 2x - 1, \\
J_{11,\{-1,1\}}(x) &= x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1, \\
J_{13,\{-1,1\}}(x) &= x^6 + x^5 - 5x^4 - 4x^3 + 6x^2 + 3x - 1, \\
J_{17,\{-1,1\}}(x) &= x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1.
\end{aligned}$$

As seen in Example 2.27, we notice an interesting pattern when considering these polynomials for various primes p; their coefficients follow a "ladder" pattern in Pascal's triangle. The pattern depends on the congruence class of p modulo 4 as formalized below:

(a) If $p \equiv 1 \pmod 4$, then the coefficients follow the pattern

$\binom{\frac{p-1}{2}}{0}; \binom{\frac{p-1}{2}}{0}, \binom{\frac{p-1}{2}-1}{1}; \binom{\frac{p-1}{2}-1}{1}, \binom{\frac{p-1}{2}-2}{2}; \binom{\frac{p-1}{2}-2}{2}, \binom{\frac{p-1}{2}-3}{3}; \ldots; \binom{\frac{p-1}{4}}{\frac{p-1}{4}-1}, \binom{\frac{p-1}{4}}{\frac{p-1}{4}}$.

(b) If $p \equiv 3 \pmod 4$, then the coefficients follow the pattern
$\binom{\frac{p-1}{2}}{0}; \binom{\frac{p-1}{2}-1}{0}, \binom{\frac{p-1}{2}-1}{1}; \binom{\frac{p-1}{2}-2}{1}, \binom{\frac{p-1}{2}-2}{2}; \binom{\frac{p-1}{2}-3}{2}, \binom{\frac{p-1}{2}-3}{3}; \ldots; \binom{\lfloor\frac{p-1}{4}\rfloor}{\lfloor\frac{p-1}{4}\rfloor}$.

If we split the odd-degree polynomials from the even-degree polynomials, a connection with the Chebyshev polynomials becomes evident. Some basic properties of the Chebyshev polynomials are summarized in the Appendix.

Theorem 2.28. *For any prime $p > 2$, we have*

$$\begin{aligned} J_{p,\{1,-1\}}(x) &= \prod_{k=1}^{\frac{p-1}{2}} \left(x - 2\cos\left(\tfrac{2\pi k}{p}\right)\right) \\ &= U_{\frac{p-1}{2}}\left(\frac{x}{2}\right) + U_{\frac{p-1}{2}-1}\left(\frac{x}{2}\right) \\ &= \frac{(-1)^{\frac{p-1}{2}}}{\sqrt{\frac{1}{2}-\frac{x}{4}}} T_p\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}\right), \end{aligned}$$

where $T_n(x)$ denotes the n^{th} Chebyshev polynomial of the first kind and $U_n(x)$ denotes the n^{th} Chebyshev polynomial of the second kind.

Proof. We have

$$\begin{aligned} &\frac{(-1)^{\frac{p-1}{2}}}{\sqrt{\frac{1}{2}-\frac{x}{4}}} T_p\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}\right) = \frac{(-1)^{\frac{p-1}{2}}}{2\left(\sqrt{\frac{1}{2}-\frac{x}{4}}\right)} \left(U_p\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}\right) - U_{p-2}\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}\right)\right) \\ &= \frac{(-1)^{\frac{p-1}{2}}}{2\left(\sqrt{\frac{1}{2}-\frac{x}{4}}\right)} U_p\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}\right) + \frac{(-1)^{\frac{p-1}{2}}}{2\left(\sqrt{\frac{1}{2}-\frac{x}{4}}\right)} U_{p-2}\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}\right) \\ &= U_{\frac{p-1}{2}}\left(\frac{x}{2}\right) + U_{\frac{p-1}{2}-1}\left(\frac{x}{2}\right), \end{aligned}$$

where we have applied both parts of Lemma A.7 to get the first and last equalities.

Now, knowing the roots of $T_n(x)$ explicitly, we can write

$$\begin{aligned}\frac{(-1)^{\frac{p-1}{2}}}{\sqrt{\frac{1}{2}-\frac{x}{4}}}T_p\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}\right) &= \frac{(-1)^{\frac{p-1}{2}}}{\sqrt{\frac{1}{2}-\frac{x}{4}}}\prod_{k=1}^{p}\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}-\cos\left(\tfrac{2k-1}{4n+2}\pi\right)\right)\\ &= (-1)^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}-\cos\left(\tfrac{2k-1}{2p}\pi\right)\right)\\ &\quad\prod_{k=\frac{p-1}{2}+2}^{p}\left(\sqrt{\tfrac{1}{2}-\tfrac{x}{4}}-\cos\left(\tfrac{2k-1}{2p}\pi\right)\right).\end{aligned}$$

To complete the proof, we need to observe two things. First, the transformations $x \to \frac{x}{2} \to \sqrt{\frac{1}{2}-\frac{x}{4}}$ have doubled the number of roots (the original roots of $T_n(x)$ and their negatives). Second, the identity $\cos(\theta) = -\cos(\theta+\pi)$ needs to be applied p times, once for each root, which eliminates the extra factor of $(-1)^{\frac{p-1}{2}}$ found above and will leave us the desired roots and their negatives, as required. □

Remark: In this proof, all instances of $\sqrt{\frac{1}{2}-\frac{x}{4}}$ *could have been replaced with* $-\sqrt{\frac{1}{2}-\frac{x}{4}}$ *as well.*

We conclude this subsection with a corollary of Theorem 2.28. To prove this corollary, we will require the following identity from [27].

Lemma 2.29 ([27], Identity 91.2.9, pg. 499)**.** *When n is an odd integer, we have*

$$\prod_{k=1}^{\frac{n-1}{2}}\left[\cos(y)-\cos\left(\tfrac{2\pi k}{n}\right)\right] = 2^{\frac{1-n}{2}}\sin\left(\tfrac{ny}{2}\right)\csc\left(\tfrac{y}{2}\right).$$

A more complete form of this lemma will be given in Section 2.11.

Corollary 2.30. *For any prime $p > 2$, the constant coefficient of $J_{p,\{-1,1\}}(x)$ is ± 1. Furthermore, the sign may be determined by the congruence class of p modulo 8. Namely, if $p \equiv 1, 3 \pmod 8$ then the constant coefficient will be 1 and if $p \equiv 5, 7 \pmod 8$ then the constant coefficient will be -1.*

Proof. From Theorem 2.28, we know that the constant coefficient will be equal to $(-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} 2\cos\left(\frac{2\pi k}{p}\right)$. Applying Lemma 2.29, we have

$$\begin{aligned}(-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} 2\cos\left(\frac{2\pi k}{p}\right) &= (-1)^{\frac{p-1}{2}} 2^{\frac{p-1}{2}} \left(2^{\frac{1-p}{2}} \sin\left(\tfrac{p\pi}{4}\right) \csc\left(\tfrac{\pi}{4}\right)\right) \\ &= (-1)^{\frac{p-1}{2}} \sin\left(\tfrac{p\pi}{4}\right) \csc\left(\tfrac{\pi}{4}\right) = \pm 1.\end{aligned}$$

If we consider $\frac{p\pi}{4}$, we see that if $p \equiv 1, 3 \pmod 8$, then the argument of $\frac{p\pi}{4}$ lies in quadrant 1 or quadrant 2, respectively, and $(-1)^{\frac{p-1}{2}} \sin\left(\frac{p\pi}{4}\right) \csc\left(\frac{\pi}{4}\right) = 1$, as required. Similarly, if $p \equiv 5, 7 \pmod 8$, then the argument of $\frac{p\pi}{4}$ lies in quadrant 3 or quadrant 4, respectively, and $(-1)^{\frac{p-1}{2}} \sin\left(\frac{p\pi}{4}\right) \csc\left(\frac{\pi}{4}\right) = -1$, as required. □

2.6.3 The Case $J_{p,H}(x)$ When $p \equiv 1 \pmod 3$ and $|H| = 3$

In this subsection, we will study another subset of the Cyclotomic Subgroup-Polynomials $J_{p,H}(x)$. We focus on primes $p \equiv 1 \pmod 3$ and the subgroup $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ of order 3. We begin by listing the first few such examples.

Example 2.31.

$$\begin{aligned}J_{7,\{1,2,4\}}(x) &= x^2 + x + 2, \\ J_{13,\{1,3,9\}}(x) &= x^4 + x^3 + 2x^2 - 4x + 3, \\ J_{19,\{1,7,11\}}(x) &= x^6 + x^5 + 2x^4 - 8x^3 - x^2 + 5x + 7, \\ J_{31,\{1,5,25\}}(x) &= x^{10} + x^9 + 2x^8 - 16x^7 - 9x^6 - 11x^5 + 43x^4 + 6x^3 + 63x^2 + 20x + 25.\end{aligned}$$

Lemma 2.32. *Let $p \equiv 1 \pmod 3$ and $|H| = 3$, and write $J_{p,H}(x) = x^m + x^{m-1} + b_{m-2}x^{m-2} + \ldots + b_0$. Then $b_{m-2} = 2$.*

Proof. This is a direct corollary of Lemma 2.26. However, to illuminate the proof through the use of a specific example, we present the following stand-alone proof.

Using Viète's formula, we know that the coefficient in question is the sum over all possible 2-products of the roots of $J_{p,H}(x)$. Because we know that $|H| = 3$, the total number of terms in the sum is $9 \cdot \binom{\frac{p-1}{3}}{2}$. Because of the group structure of the

quotient group $(\mathbb{Z}/p\mathbb{Z})^\times/H$ and the group structure of the group $\mathbb{Z}/p\mathbb{Z}^\times$, we know that we will have $\frac{p-1}{2}$ products that equal 1, namely $(w^n \cdot w^{p-n})$ for $n = 1, \ldots, \frac{p-1}{2}$. The remaining terms can then be organized in groups of $(p-1)$ summands that equal -1, namely $(w + w^2 + \ldots + w^{p-1}) = -1$. Putting all of this together, we get

$$b_{m-2} = \frac{p-1}{2} - \frac{9 \cdot \binom{\frac{p-1}{3}}{2} - \frac{p-1}{2}}{p-1} = \frac{p-1}{2} - \frac{p-5}{2} = 2.$$

Thus we have shown that $b_{m-2} = 2$, as required. □

Conjecture 2.33. *Let $p \equiv 1 \pmod 3$ and $|H| = 3$, and write $J_{p,H}(x) = x^m + x^{m-1} + b_{m-2}x^{m-2} + \ldots + b_0$. Then*

$$b_{m-3} = 2\left(\frac{p-1}{3}\right) - 4 = \frac{2p-14}{3}.$$

Through numerical experimentation this conjecture has been verified for all odd primes $p \equiv 1 \pmod 3$, $p < 10000$. When attempting to prove this conjecture, the major obstacle was determining the behaviour of sums of the form

$$\sum_{i,j,k} g_i g_j g_k \qquad g_i, g_j, g_k \in (\mathbb{Z}/p\mathbb{Z})^\times/H$$

for a given prime p and subgroup H as in the statement of the conjecture.

2.6.4 The Case $J_{p,H}(x)$ When $p \equiv 1 \pmod 4$ and $|H| = 4$

In this subsection, we will study a third subset of the Cyclotomic Subgroup-Polynomials $J_{p,H}(x)$. This time we focus on primes $p \equiv 1 \pmod 4$ and the subgroup $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ of order 4. We begin by listing the first few such examples.

Example 2.34.

$$J_{5,\{1,2,3,4\}}(x) = x + 1,$$
$$J_{13,\{1,5,8,12\}}(x) = x^3 + x^2 - 4x + 1,$$
$$J_{17,\{1,4,13,16\}}(x) = x^4 + x^3 - 6x^2 - x + 1,$$
$$J_{29,\{1,12,17,28\}}(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1.$$

Lemma 2.35. *Let $p \equiv 1 \pmod 4$ and $|H| = 4$. Then the constant coefficient of $J_{p,H}(x)$ is equal to 1.*

Proof. Since $p \equiv 1 \pmod 4$, we know that each root of $J_{p,H}(x)$ in this case is of the form

$$a_k = w^{g_{1_k}} + w^{g_{2_k}} + w^{g_{3_k}} + w^{g_{4_k}}$$

for $k = 1, 2, \ldots, \frac{p-1}{4}$. Because $H \cong \mathbb{Z}/4\mathbb{Z}$, we know that $g_{1_k} = -g_{4_k}$ and $g_{2_k} = -g_{3_k}$ for each value of k; this means that every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is inside the same coset as its inverse. The constant coefficient is the product of all of the a_k and since each $w^{g_{i_k}}$ is in the same coset as $w^{-g_{i_k}}$ there will be no cancellation in the product defining a_k and every element of $(\mathbb{Z}/p\mathbb{Z})$ will appear an equal number of times as an exponent of w. The $w^{g_{i_k}}$ will cancel each other out in groups of p elements because $w + w^2 + \ldots + w^{p-1} = -1$ and $w^0 = 1$. Since the total number of terms in the product $\prod_{k=1}^{\frac{p-1}{4}} a_k$ will be $4^{\frac{p-1}{4}}$, we look to write this quantity in the form $A \cdot p + B$ for integers A and B:

$$4^{\frac{p-1}{4}} = 2^{\frac{p-1}{2}} = \frac{1}{p}\left(2^{\frac{p-1}{2}} - \left(\frac{2}{p}\right)\right) \cdot p + \left(\frac{2}{p}\right).$$

This means that the product of the roots of $J_{p,H}(x)$ is equal to the Legendre symbol $\left(\frac{2}{p}\right)$. Using Viète's formula, the constant coefficient is equal to $(-1)^n \left(\frac{2}{p}\right) = 1$, as required. □

We conclude this section with a small table that summarizes our results, where the one entry for b_{m-3} is only conjectured.

p	Index of H	b_{m-2}	b_{m-3}	b_0
$\equiv 1 \pmod 2$	2	$\frac{p-3}{2}$		± 1
$\equiv 1 \pmod 3$	3	2	$\frac{2p-14}{3}$	
$\equiv 1 \pmod 4$	4	$\frac{p-5}{2}$		1
$\equiv 1 \pmod 2$	odd	$\frac{\lvert H\rvert+1}{2}$		
$\equiv 1 \pmod 2$	even	$\frac{p-1-\lvert H\rvert}{2}$		

Table 2.1: Some Coefficients of $J_{n,H}(x)$

2.7 Studying the Sets $\{J_{n,H}(x) \mid H \leq (\mathbb{Z}/n\mathbb{Z})^\times\}$

In this section, we investigate the relationship between sets of Cyclotomic Subgroup-Polynomials $\{J_{n_1,H}(x) \mid H \leq (\mathbb{Z}/n_1\mathbb{Z})^\times\}$ and $\{J_{n_2,H}(x) \mid H \leq (\mathbb{Z}/n_2\mathbb{Z})^\times\}$ for different positive integers n_1 and n_2.

2.7.1 The Case $n_1 = p$ Compared to the Case $n_2 = 2p$

We first consider the case with $n_1 = p$ an odd prime and $n_2 = 2p$. In this case, $(\mathbb{Z}/p\mathbb{Z})^\times$ and $(\mathbb{Z}/2p\mathbb{Z})^\times$ are both cyclic, and $\varphi(n_1) = \varphi(n_2) = p-1$. So we know that the two sets will be of equal cardinality, i.e., contain the same number of polynomials with the same degrees. We calculate such an example with $n_1 = 7$ and $n_2 = 14$:

Example 2.36. With $n_1 = 7$ and $n_2 = 14$, we display the two sets of polynomials using the following table for easier comparison.

n	H	$J_{n,H}(x)$
7	$\{1\}$	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
7	$\{1, 6\}$	$x^3 + x^2 - 2x - 1$
7	$\{1, 9, 11\}$	$x^2 - x + 2$
7	$\{1, 3, 5, 9, 11, 13\}$	$x - 1$
14	$\{1\}$	$x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$
14	$\{1, 13\}$	$x^3 - x^2 - 2x + 1$
14	$\{1, 2, 4\}$	$x^2 + x + 2$
14	$\{1, 2, 3, 4, 5, 6\}$	$x + 1$

Table 2.2: $\{J_{7,H}(x)\}_{H\leq(\mathbb{Z}/7\mathbb{Z})^\times}$ Compared to $\{J_{14,H}(x)\}_{H\leq(\mathbb{Z}/14\mathbb{Z})^\times}$

Just as n_1 and n_2 are closely related positive integers, we observe that these two sets of polynomials are also themselves quite similar. It turns out that this is the case when $n_1 = p^k$ and $n_2 = 2p^k$ for an odd prime p and positive integer k.

Theorem 2.37. *The sets of irreducible polynomials* $\{J_{p^k,H}(x) : H \leq (\mathbb{Z}/p^k\mathbb{Z})^\times\}$ *and* $\{J_{2p^k,H}(x) : H \leq (\mathbb{Z}/2p^k\mathbb{Z})^\times\}$ *are identical up to the signs of the coefficients of the individual polynomials.*

To prove Theorem 2.37, we will make use of Theorem 2.2 and the following lemma which may be found in many Algebra and/or Number Theory books, such as [15]:

Lemma 2.38 ([15], Lemma 1.4.5)**.** *Let p be an odd prime, and let g be a primitive root modulo p^k. Then either g or $(g+p^k)$ (whichever is odd) is a primitive root modulo $2p^k$ for all positive integers k.*

Proof of Theorem 2.37. We begin by noting that since $(\mathbb{Z}/p^k\mathbb{Z})^\times$ and $(\mathbb{Z}/2p^k\mathbb{Z})^\times$ are both cyclic groups and $\varphi(p^k) = \varphi(2p^k)$, Theorem 2.2 tells us that these two groups are actually isomorphic. Moreover, Lemma 2.38 tells that if g generates $(\mathbb{Z}/p^k\mathbb{Z})^\times$, then g or $g+p^k$ generates $(\mathbb{Z}/2p^k\mathbb{Z})^\times$. Now let $w_1 = e^{\frac{2\pi i}{p^k}}$ and $w_2 = e^{\frac{2\pi i}{2p^k}} = e^{\frac{\pi i}{p^k}}$. Note that $w_1 = w_2^2$. When comparing the roots of $J_{p^k,H}(x)$ to the roots of $J_{2p^k,H'}(x)$ (where $H \cong H'$ by Theorem 2.2), we have one of the following two scenarios:

Case 1: g generates both cyclic groups: Using the notation of (2.1), a root of $J_{p^k,H}$ looks like

$$\sum_{h\in H} w_1^{g^d h} = \sum_{h\in H} w_2^{2g^d h} = \sum_{h'\in H'} w_2^{2\cdot g^d h'},$$

which is a root of $J_{2p^k,H'}$, as required.

Case 2: g generates $(\mathbb{Z}/p^k\mathbb{Z})^\times$ and $(g+p^k)$ generates $(\mathbb{Z}/2p^k\mathbb{Z})^\times$: Using the notation of (2.1), a root of $J_{p^k,H}$ looks like

$$\begin{aligned}\sum_{h\in H} w_1^{g^d h} &= \sum_{h\in H} w_1^{(g+p^k)^d h} \quad \text{since } w_1^{p^k} = 1\\ &= \sum_{h\in H} w_2^{2(g+p^k)^d h}\\ &= \sum_{h'\in H'} w_2^{2\cdot(g+p^k)^d h},\end{aligned}$$

which is a root of $J_{2p^k,H'}$, as required. The variation in the sign of the coefficients of $J_{p^k,H}(x)$ and $J_{2p^k,H'}(x)$ comes from the fact that w_1^g may be in a different quadrant than w_2^g or $w_2^{g+p^k}$ with the same reference angle for their arguments. That is, $\operatorname{Re}(w_1^g) = \pm\operatorname{Re}(w_2^g)$ or $\operatorname{Re}(w_1^g) = \pm\operatorname{Re}(w_2^{g+p^k})$ and similarly $\operatorname{Im}(w_1^g) = \pm\operatorname{Im}(w_2^g)$ or $\operatorname{Im}(w_1^g) = \pm\operatorname{Im}(w_2^{g+p^k})$. □

2.7.2 The Case $n_1 = p$ Compared to the Cases $n_2 = 3p, 4p, \ldots$

The goal of this subsection is to investigate and compare the following sets of Cyclotomic Subgroup-Polynomials for these values of n_1 and n_2 and compare them with each other. This is a natural extension of the situation of the previous subsection.

Unfortunately, there is a nice comparison only between the sets $\{J_{p^k,H}(x)\}$ and $\{J_{2p^k,H}(x)\}$ discussed in the previous subsection. Suppose $n_1 = p^k$ and $n_2 = A \cdot p^k$ with $(A, p) = 1$ are the two positive integers that we wish to compare. The structure theorem of finite abelian groups tells us that

$$(\mathbb{Z}/Ap^k\mathbb{Z}) \cong (\mathbb{Z}A\mathbb{Z}) \times (\mathbb{Z}/p^k\mathbb{Z}),$$

and we know that $\varphi(Ap^k) = \varphi(A)\varphi(p^k)$.

If $A \neq 2$ and $(A, p) = 1$, then $(\mathbb{Z}/Ap^k\mathbb{Z})^\times$ is not cyclic and we know less about the group structure in general. Moreover, for $A \geq 3$, $\varphi(n_1) \neq \varphi(n_2)$ and we won't have the same number of polynomials in both sets. These two observations together show that it will be difficult to compare the case $n_1 = p$ with the cases $n_2 = 3p, 4p, \ldots$.

However, this discussion has not yet covered the case when A is a power of the prime p. That is, $A = p^s$ for some positive integer s. We calculate a few different sets $\{J_{n,H}(x)\}$ for integers n in the following example:

Example 2.39. For a few given integers of the form $n = A \cdot p^k$ with $p > 2$ we consider the sets of all $J_{n,H}(x)$ for subgroups $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$.

$$\{J_{3,H}(x)\}_H = \{x + 1,\ x^2 + x + 1\}$$
$$\{J_{5,H}(x)\}_H = \{x + 1,\ x^2 + x - 1,\ x^4 + x^3 + x^2 + x + 1\}$$
$$\{J_{9,H}(x)\}_H = \{x,\ x^2,\ x^3 - 3x + 1,\ x^6 + x^3 + 1\}$$

$$\{J_{15,H}(x)\}_H = \{x-1,\ x^2-x-1,\ x^2-x+4,\ x^2-x+1,\ x^4-x^3+x^2-x+1,$$
$$x^4-x^3-4x^2+4x+1,\ x^4-x^3+2x^2+x+1,$$
$$x^8-x^7+x^5-x^4+x^3-x+1\}$$
$$\{J_{27,H}(x)\}_H = \{x,\ x^2,\ x^3,\ x^6,\ x^9-9x^7+27x^5-30x^3+9x+1,\ x^{18}+x^9+1\}$$

We observe that the sets $\{J_{3,H}(x)\}_H$, $\{J_{5,H}(x)\}_H$, and $\{J_{15,H}(x)\}_H$ are not comparable in any meaningful way. However, the sets $\{J_{3,H}(x)\}_H$, $\{J_{9,H}(x)\}_H$, and $\{J_{27,H}(x)\}_H$ seem to be.

For the purpose of studying relationships between sets $\{J_{n_1,H}(x)\}_H$ and $\{J_{n_2,H}(x)\}_H$ in a systematic way and comparing these sets to one another, we seek values of n such that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group.

The values $n = 2, 4, p^k$, and $2p^k$ are specifically the integers n where either $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic or n has a primitive root. The group of units modulo n in these instances is cyclic so that the entire group structure is well determined. The case $n = 2$ produces the single element set $\{x+1\}$. The case $n = p$, as we have seen, produces an irreducible polynomial corresponding to every divisor $d|(p-1)$ that has degree $\frac{p-1}{d}$. We know what happens in the two extreme cases when $H = \{1\}$ and $H = (\mathbb{Z}/p\mathbb{Z})^\times$ and we also know some of the coefficients of these Cyclotomic Subgroup-Polynomials for certain congruence classes of p and particular values for the order $|H|$.

In the previous subsection, we studied the case $n_1 = p^k$ and $n_2 = 2p^k$. We saw that these two sets are essentially the same (up to sign of the coefficients). We now wish to study how the cases $n = p, p^2, p^3, \ldots$ are related to one another for a fixed odd prime p. In Example 2.39, we observed that the set of polynomials for $n = p^{k+1}$ contains the monomials x^s where s ranges through the degrees of the polynomials found in the set associated to $n = p^k$. Because of the embedding of $\mathbb{Z}/p^k\mathbb{Z}$ in $\mathbb{Z}/p^{k+1}\mathbb{Z}$, it is clear why polynomials of those degrees are present but it is not immediately obvious why zero is their only root. We now show that this fact is explained by a theorem of Sivek [54].

2.8 Vanishing Roots of Unity

We saw in Example 2.39 that the monomial x^s, for specific values of the positive integer s, is present as a Cyclotomic Subgroup-Polynomial in certain cases, namely in the sets $\{J_{9,H}(x)\}_H$ and $\{J_{27,H}(x)\}_H$. In this section, we characterize when this occurs.

2.8.1 k-Balancing Numbers

A number theoretic problem that has been studied is the following: For a given natural number n, what are the possible integers k for which there exist n^{th} roots of unity $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$ such that $\alpha_1 + \ldots + \alpha_k = 0$? If such a sum with k summands of n^{th} roots of unity exists, then n is called *k-balancing*.

Two papers, [36] and [54], approach this question of k-balancing with one major difference in their initial restrictions. In [36], the authors allow repetition in the summands of n^{th} roots of unity, while in [54] the author does not allow for any repetition in the summands of n^{th} roots of unity. It is this latter approach that we are interested in, and which applies to the study of Cyclotomic Subgroup-Polynomials. Because the roots of $J_{n,H}(x)$ are sums of elements determined from quotient groups and the elements in a group are distinct, we will never encounter repetition. In [54], Sivek presents the following theorem:

Theorem 2.40 (Sivek)**.** *Write $m = p_1^{e_1} \cdots p_r^{e_r}$, with each p_i prime and each e_i positive. Then m is k-balancing if and only if both k and $m-k$ are in $\mathbb{N}_0 p_1 + \ldots + \mathbb{N}_0 p_r$, where $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.*

This theorem allows us to determine exactly which polynomials $J_{n,H}(x)$ are of the form x^s for some positive integer s.

Example 2.41. Let $n = 27 = 3^3$. Since $|H|$ divides $|(\mathbb{Z}/27\mathbb{Z})^\times|$, we are interested in knowing which divisors k of $\varphi(27) = 18 = 2 \cdot 3^2$ are such that k and $27-k$ are multiples of 3. There are four such divisors k, namely $k = 3, 6, 9$ and 18. These correspond to the polynomials of degree $6, 3, 2$, and 1, respectively, as we saw in Example 2.39.

We demonstrate Theorem 2.40 with another example, this time an example where there are no monomials in our set $\{J_{n,H}(x)\}_H$.

Example 2.42. Let $n = 15 = 3 \cdot 5$. From Example 2.39, we know that the set $\{J_{15,H}(x)\}_H$ contains no monomials and we will now illustrate why. We seek positive integers k, such that $k|\varphi(15) = 8 = 2^3$ and both k and $15 - k$ can be written as a linear combination $A \cdot 3 + B \cdot 5$ for non-negative integers A and B. The set of all possible divisors k that we seek is $\{1, 2, 4, 8\}$. We exhaust each possible case and collect the information in a table. For each k, we seek a solution for $k = A \cdot 3 + B \cdot 5$ and $n - k = C \cdot 3 + D \cdot 5$ for non-negative integers A, B, C, and D.

k	$15 - k$	(A, B)	(C, D)
1	14	no solution	(3,1)
2	13	no solution	(1,2)
4	11	no solution	(2,1)
8	7	(1,1)	no solution

Table 2.3: k-Balancing When $n = 15$

We have therefore confirmed what we saw to be the case in Example 2.39; $\{J_{15,H}(x)\}$ contains no monomials x^s.

2.8.2 Reciprocal Polynomials

Given a polynomial $p(x) = a_0 + a_1x + \ldots + a_nx^n$ with real coefficients, the associated reciprocal polynomial is defined by $p^*(x) = a_n + a_{n-1}x + \ldots + a_0x^n = x^n p(x^{-1})$. We call a polynomial $p \in \mathbb{R}[x]$ a self-reciprocal polynomial if $p(x) = p^*(x)$. We have come across examples of self-reciprocal polynomials in this chapter, namely the cyclotomic polynomials $\Phi_n(x), n \geq 3$. Because the Cyclotomic Subgroup-Polynomials are a generalization of the cyclotomic polynomials, it is reasonable to explore which Cyclotomic Subgroup-Polynomials are self-reciprocal.

If we let $p(x) = x^s$ for a positive integer s, then $p(x) \neq p^*(x)$ and it does not satisfy the definition of a self-reciprocal polynomial. However, the coefficient sequence of a monomial x^s reads the same forwards and backwards trivially. For this reason, we will highlight monomials as well as self-reciprocal polynomials in this subsection.

In [12], Cafure and Cesaratto give a useful characterization of self-reciprocal polynomials in terms of their roots.

Theorem 2.43 (Cafure and Cesaratto)**.** *A polynomial $f \in \mathbb{Q}[x]$ is self-reciprocal if and only if it satisfies the following two properties:*

If 1 is a root of f, then its multiplicity is even.

If α is a root of f of multiplicity r, then $\frac{1}{\alpha}$ is a root of multiplicity r.

This characterization, based on the roots of a self-reciprocal polynomial, proves to be the most useful characterization when discussing the Cyclotomic Subgroup-Polynomials $J_{n,H}(x)$ since they are generated by first calculating their roots. Theorem 2.43 allows us to state and prove the following result.

Every family of Cyclotomic Subgroup-Polynomials contains the self-reciprocal polynomial $J_{n,\{1\}}(x) = \Phi_n(x)$. In certain cases, depending on the prime decomposition of n, we can enumerate the exact number of self-reciprocal polynomials and/or monomials found in the set $\{J_{n,H}(x)\}_H$.

Theorem 2.44. *(i) When $n = p$, we have the unique additional self-reciprocal polynomial $J_{p,(\mathbb{Z}/p\mathbb{Z})^\times}(x) = x + 1$.*

(ii) When $n = p^\alpha, \alpha > 1$, we have the additional $[d(p-1) \cdot (\alpha - 1)]$ monomials, where $d(p-1)$ is the number of divisors of $(p-1)$, and there are are no more.

(iii) When $n = p_1 \cdot p_2 \cdots p_k$, we have an additional $2^k - 2$ self-reciprocal polynomials for a total of exactly $(2^k - 1)$ self-reciprocal polynomials, and there are no more.

Proof. We begin by making a general remark regarding the conditions of Theorem 2.43. From (2.1), we see that the roots of the Cyclotomic Subgroup-Polynomials will never be equal to 1 and therefore vacuously satisfy the condition that 1 is a root of even multiplicity. Also from (2.1), we see that for a_k and $\frac{1}{a_k}$ to both be roots of the polynomial, a_k will need to itself be a root of unity since $\sum_{h\in H} w^{h_k h}$ and $\frac{1}{\sum_{h\in H} w^{h_k h}}$ would both have to be of the form $a_{k'} = \sum_{h\in H} w^{h'_k h}$ for some k'. If a_k is a root of unity for some k, then every a_k is a root of unity since they are all defined in terms of coset representatives of the subgroup H. We now prove the theorem by addressing

each case individually and in order.

Let $n = p$ and let $H = (\mathbb{Z}/p\mathbb{Z})^\times$. From (2.1) we then have $a_1 = \sum_{j=1}^{p-1} w^j = -1$ and from (2.2), we get $J_{p,(\mathbb{Z}/p\mathbb{Z})^\times}(x) = x + 1$ as stated. To show that we do not have any other self-reciprocal polynomials we use Theorem 2.43, and the fundamental theorem of finite abelian groups that tells us there is no subgroup $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ such that $H \cong (\mathbb{Z}/m\mathbb{Z})^\times$ for some integer m since p has no non-trivial proper divisors.

Now let $n = p^\alpha, \alpha > 1$. We will use Theorem 2.40 to help resolve this case. Since $\varphi(n) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$, we see that if k is a divisor of $\varphi(n)$, then $k = 1, p, p^2, \ldots, p^{\alpha-1}$ or $k|(p-1)$ and all possible products are from both of these sets. We then seek the cases where k and $n-k$ are both multiples of p. We see that this eliminates $k = 1$. The divisors $k = p, p^2, \ldots, p^{\alpha-1}$ all satisfy the conditions of Theorem 2.40 and correspond to $(\alpha - 1)$ different monomials in our set of Cyclotomic Subgroup-Polynomials. For any divisor $s|(p-1), s \neq 1$, the product $k = sp, sp^2, \ldots, sp^{\alpha-1}$ also satisfy the conditions of Theorem 2.40. Moreover, the fundamental theorem of finite abelian groups tells us that there are no other subgroups $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\sum_{h\in H} w^{h_k h}$ would be isomorphic to an m^{th} root of unity for some integer m since there are no other divisors of n.

Lastly, we now let $n = p_1 \cdot p_2 \cdots p_k$. The fundamental theorem of finite abelian groups tells us that

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times (\mathbb{Z}/p_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times.$$

We can quotient the group $(\mathbb{Z}/n\mathbb{Z})^\times$ by any combination of the subgroups $(\mathbb{Z}/p_j\mathbb{Z})^\times$ and the resulting quotient group will be isomorphic to the group of roots of unity of order $n/\prod_j p_j$. There are 2^k total combinations of these p_j, and we exclude the two extreme cases corresponding to choosing none of the p_j and choosing all of the p_j. This gives us the required $(2^k - 2)$ self-reciprocal polynomials we seek.

We have exhausted all three cases and thus have proved the theorem. □

We now conclude this section with three examples.

Example 2.45. Recall that in the case $n = 7$, by Example 2.10, we have a total of 2 self-reciprocal polynomials.

$$\begin{aligned}\{J_{7,H}(x)\} = \{&\underline{x+1},\\ &x^2+x+2,\\ &x^3+x^2-2x-1,\\ &\underline{x^6+x^5+x^4+x^3+x^2+x+1}\}.\end{aligned}$$

The self-reciprocal polynomials have been underlined for emphasis.

Example 2.46. Recall that in the case $n = 15 = 3 \cdot 5$, by Example 2.39, we have a total of $2^2 - 1 = 3$ self-reciprocal polynomials.

$$\begin{aligned}\{J_{15,H}(x)\} = \{&x-1,\\ &x^2-x-1,\\ &x^2-x+4,\\ &\underline{x^2-x+1},\\ &\underline{x^4-x^3+x^2-x+1},\\ &x^4-x^3-4x^2+4x+1,\\ &x^4-x^3+2x^2+x+1,\\ &\underline{x^8-x^7+x^5-x^4+x^3-x+1}\}.\end{aligned}$$

The self-reciprocal polynomials have again been underlined for emphasis.

Example 2.47. If we take $n = 105 = 3 \cdot 5 \cdot 7$, then the set $\{J_{105,H}(x)\}$ will contain exactly $2^3 - 1 = 7$ self-reciprocal polynomials. The degrees of these self-reciprocal polynomials will be, in descending order, $48, 24, 12, 8, 6, 4$, and 2. Due to its size, we refrain from listing the entire set of Cyclotomic Subgroup-Polynomials in this example.

For the integers that do not conform to one of the three specific cases of Theorem 2.44, the values presented in the theorem represent a lower bound. For example, if

$n = Ap^\alpha$ with $(A, p) = 1$ then we would have at least an additional $[d(p-1)\cdot(\alpha-1)]$ monomials and/or self-reciprocal polynomials.

2.9 Gauss Period Sums

Let $\mathbb{F}_{p^\alpha}$ be the finite field with p^α elements for an odd prime p and let g be a primitive root modulo p^α, i.e., g generates the cyclic group $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. For any divisor $d|(p-1)$, we write $p-1 = dm$; then Barcanescu [6] defines the *Gauss d-periods* to be

$$\eta_j = \sum_{x\in\{g^{kd+j}:k=0,1,\ldots,m-1\}} \zeta^x, \qquad j = 0, 1, 2, \ldots, d-1,$$

where ζ is a fixed primitive root of unity of order p. In [47], the author calls these η_j, "Gauss sums" as a convenient terminology but warns that the term doesn't agree with others in the literature.

In certain cases, namely when when $\alpha = 1$ and we are considering sums over $\mathbb{F}_p$, these η_j's are the roots of the Cyclotomic Subgroup-Polynomials, a_k from (2.1). In some cases of small degree, this allows us to calculate the coefficients of some of the Cyclotomic Subgroup-Polynomials. Specifically these cases occur when $n = p$ is an odd prime and the polynomial is of degree two, three, and four.

To properly state the results regarding the Gauss Period Sums, we must discuss the ability to write a prime number as a linear combination of two square integers. These results, due to Fermat and proven by Euler, can be found, with proof, in [7] and [17].

Theorem 2.48 (Fermat)**.** *(i) An odd prime p can be written as a sum of two integer squares if and only if $p \equiv 1 \pmod 4$.*

(ii) An odd prime p can be written as $p = x^2 + 2y^2$, where $x, y \in \mathbb{Z}$, if and only if $p \equiv 1, 3 \pmod 8$.

(iii) An odd prime p can be written as $p = x^2 + 3y^2$, where $x, y \in \mathbb{Z}$, if and only if $p \not\equiv 2 \pmod 3$.

We note that when we write $p = x^2 + y^2$, $p = x^2 + 2y^2$, or $p = x^2 + 3y^2$ for integers x and y, these representations are unique up to the sign of x and y. For proofs of this, see [48, pp. 167–174], and in particular, Corollary 3.23 and Theorem 3.27 with $d = -12$ and $d = -8$, respectively.

Let $p \equiv 1 \pmod 3$ be prime. By Theorem 2.48 we know that such primes p admit a representation as a sum of an integer square and 3 times an integer square. But if we consider such a representation $p = x^2 + 3y^2$ for integers x and y modulo 3, and use the fact that the only squares modulo 3 are 0 and 1, we can conclude that x^2 is congruent to 1 modulo 3. The congruence $x^2 \equiv 1 \pmod 3$ then implies that $x \equiv \pm 1 \pmod 3$. Finally, by switching the sign of x if necessary, we can assume that $x \equiv 1 \pmod 3$. It follows that, with $r = 2x$, $s = 2y$ we can represent $4p = r^2 + 3s^2$ with $r \equiv 1 \pmod 3$. The notation that will be used in Theorems 2.52–2.54 therefore makes sense.

When considering the general case given by $p = x^2 + ny^2$ for integers x and y and an arbitrary positive integer n one should be careful, the fact that a prime dividing an integer of this form need not imply that the prime is of the same form. For example, consider $n = 5$: $3 \mid 21 = 1^2 + 5 \cdot 2^2$ but $3 \neq x^2 + 5y^2$ for integers x and y.

To completely answer the question of when a prime can be written as $p = x^2 + ny^2$ for integers x, y and a given positive integer n, is beyond the scope of this thesis, and we have listed only the results that will be needed for our use. We refer the interested reader to [17] for a complete and thorough discussion of the subject.

We now list the first few examples of the specific Cyclotomic Subgroup-Polynomials that will be the focus of this section, grouped by their degrees.

Example 2.49. For an odd prime p, the order $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ is even and therefore will have a Cyclotomic Subgroup-Polynomial of degree 2. In this example, H denotes the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index 2 in each case. The first few examples of

these quadratics are:

$$J_{3,H}(x) = x^2 + x + 1, \qquad J_{5,H}(x) = x^2 + x - 1,$$
$$J_{7,H}(x) = x^2 + x + 2, \qquad J_{11,H}(x) = x^2 + x + 3,$$
$$J_{13,H}(x) = x^2 + x - 3, \qquad J_{17,H}(x) = x^2 + x - 4.$$

Example 2.50. For an odd prime $p \equiv 1 \pmod 3$, the order $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ is divisible by 3 and therefore will have a Cyclotomic Subgroup-Polynomial of degree 3. In this example, H denotes the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index 3 in each case. The first few examples of these cubics are:

$$J_{7,H}(x) = x^3 + x^2 - 2x - 1, \qquad J_{13,H}(x) = x^3 + x^2 - 4x + 1,$$
$$J_{19,H}(x) = x^3 + x^2 - 6x - 7, \qquad J_{31,H}(x) = x^3 + x^2 - 10x - 8,$$
$$J_{37,H}(x) = x^3 + x^2 - 12x + 11, \qquad J_{43,H}(x) = x^3 + x^2 - 14x + 8.$$

Example 2.51. For an odd prime $p \equiv 1 \pmod 4$, the order $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ is divisible by 4 and therefore will have a Cyclotomic Subgroup-Polynomial of degree 4. In this example, H denotes the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index 4 in each case.The first few examples of these quartics are:

$$J_{5,H}(x) = x^4 + x^3 + x^2 + x + 1, \qquad J_{13,H}(x) = x^4 + x^3 + 2x^2 - 4x + 3,$$
$$J_{17,H}(x) = x^4 + x^3 - 6x^2 - x + 1, \qquad J_{29,H}(x) = x^4 + x^3 + 4x^2 + 20x + 23,$$
$$J_{37,H}(x) = x^4 + x^3 + 5x^2 + 7x + 49, \qquad J_{41,H}(x) = x^4 + x^3 - 15x^2 + 18x - 4.$$

In papers by Barcanescu [6] and Myerson [47], methods are given to calculate the coefficients of the polynomial having special cases of Gauss Period Sums, η_j, as its roots. We will introduce a small piece of notation to help list the next few theorems neatly. Once a prime p is fixed, we take H_2 to be the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index 2. Analogously we shall use the notation H_3 and H_4 as well.

Theorem 2.52 ([6] and [47]). *For an odd prime p we have*

$$J_{p,H_2}(x) = x^2 + x + \frac{1-(-1)^{\frac{p-1}{2}}p}{4}.$$

Theorem 2.53 ([6] and [47]). *Let $p \equiv 1 \pmod 3$ be a prime, and the integer c be such that $4p = c^2 + 27b^2$ and $c \equiv 1 \pmod 3$. Then*

$$J_{p,H_3}(x) = x^3 + x^2 - \frac{p-1}{3}x - \frac{1}{27}(p(c+3)-1).$$

Theorem 2.54 ([6] and [47]). *Let $p \equiv 1 \pmod 8$ be a prime, and the integer s be such that $p = s^2 + 4t^2$ and $s \equiv 1 \pmod 4$. Then*

$$J_{p,H_4}(x) = x^4 + x^3 - \frac{3(p-1)}{8}x^2 + \frac{1}{16}\Big((2s-3)p+1\Big)x + \frac{1}{256}\Big(p^2 - (4s^2-8s+6)p + 1\Big).$$

Let $p \equiv 5 \pmod 8$ be a prime, and the integer s be such that $p = s^2 + 4t^2$ and $s \equiv 1 \pmod 4$.
Then

$$J_{p,H_4}(x) = x^4 + x^3 + \frac{1}{8}(p+3)x^2 + \frac{1}{16}\Big((2s+1)p+1\Big)x + \frac{1}{256}\Big(9p^2 - (4s^2-8s-2)p + 1\Big).$$

Using Theorems 2.52–2.54, along with computer algebra software, we can solve for the roots of these polynomials to obtain closed form formulas for the a_k found in (2.1) in terms of parameters that only depend on the prime p. Instead of using computer algebra software, one may directly apply the classical quadratic formula, cubic formulas of Cardano and Tartaglia, and the quartic equations of Cardano and L. Ferrari.

Theorem 2.55. *For an odd prime p, the roots of the Cyclotomic Subgroup-Polynomial* $J_{p,H_2}(x)$ *are*

$$x_{1,2} = -\frac{1}{2} \pm \frac{\sqrt{i(-1)^{\frac{p}{2}+1}}}{2},$$

where $\sqrt{i} = e^{\frac{\pi i}{4}} = \sqrt{2}\left(\frac{1+i}{2}\right)$ *and* $\sqrt{-i} = e^{\frac{-\pi i}{4}} = \sqrt{2}\left(\frac{1-i}{2}\right)$.

Theorem 2.56. *Let* $p \equiv 1 \pmod 3$ *be a prime, and the integer c be such that* $4p = c^2 + 27b^2$ *and* $c \equiv 1 \pmod 3$. *Then the roots of* $J_{p,H_3}(x)$ *are*

$$x_1 = \frac{1}{6}d^{\frac{1}{3}} + \frac{2p}{3d^{\frac{1}{3}}} - \frac{1}{3},$$
$$x_{2,3} = -\frac{1}{12}d^{\frac{1}{3}} - \frac{p}{3d^{\frac{1}{3}}} - \frac{1}{3} \pm \frac{i\sqrt{3}}{2}\left(\frac{d^{\frac{1}{3}}}{6} - \frac{2p}{3d^{\frac{1}{3}}}\right),$$

where $d := 4pc + 4\sqrt{p^2c^2 - 4p^3}$.

Theorem 2.57. *Let* $p \equiv 1 \pmod 8$ *be a prime, and the integer s be such that* $p = s^2 + 4t^2$ *and* $s \equiv 1 \pmod 4$. *Then the roots of* $J_{p,H_4}(x)$ *are*

$$x_{1,2} = -\frac{1}{4} + \frac{\sqrt{p}}{4} \pm \frac{\sqrt{2p - 2s\sqrt{p}}}{4},$$

$$x_{3,4} = -\frac{1}{4} - \frac{\sqrt{p}}{4} \pm \frac{\sqrt{2p + 2s\sqrt{p}}}{4}.$$

Let $p \equiv 5 \pmod 8$ *be a prime, and the integer s be such that* $p = s^2 + 4t^2$ *and* $s \equiv 1 \pmod 4$. *Then the roots of* $J_{p,H_4}(x)$ *are*

$$x_{1,2} = -\frac{1}{4} + \frac{\sqrt{p}}{4} \pm \frac{\sqrt{-2p - 2s\sqrt{p}}}{4},$$

$$x_{3,4} = -\frac{1}{4} - \frac{\sqrt{p}}{4} \pm \frac{\sqrt{-2p + 2s\sqrt{p}}}{4}.$$

2.10 Integral Formula for the Constant Coefficient of the Cyclotomic Subgroup-Polynomial

In [1] and [2], Andrica and Bagdasar present the *polygonal polynomials*, $P_n(x)$, which they define as follows:

Definition 2.58. *For a positive integer n,*

$$P_n(z) = (z-1)(z^2-1)\cdots(z^n-1).$$

The polygonal polynomials are a special case of a more general family of polynomials, also introduced in [1] and [2], defined as follows.

Definition 2.59. *For positive integers $n, m_1, m_2, \ldots, m_n$, and complex numbers $z_1, z_2, \ldots, z_n$ which satisfy $|z_k| = 1$ for $k = 1, \ldots, n$, we define*

$$F^{z_1,z_2,\ldots,z_n}_{m_1,m_2,\ldots,m_n}(z) = \prod_{k=1}^{n}(z^{m_k} - z_k).$$

Motivated by the results of Andrica and Bagdasar, in this section we apply the methodology found in [2] to provide an integral formula for calculating the constant coefficient of the Cyclotomic Subgroup-Polynomial $J_{n,H}(x)$.

Theorem 2.60. *The constant coefficient b_0 of the Cyclotomic Subgroup-Polynomial $J_{n,H}(x)$ is given by the integral formula*

$$b_0 = |a_1| \cdot |a_2| \cdots |a_N| \frac{(2i)^N}{\pi} \int_0^{\pi} \prod_{k=1}^{N} \sin\left(t - \tfrac{\alpha_k}{N}\right) e^{i\left(Nt + \frac{\alpha}{2}\right)} dt,$$

where N is the degree of $J_{n,H}(x)$, and $\alpha = \alpha_1 + \alpha_2 + \ldots + \alpha_N$ with $\arg(a_k) = \alpha_k$, and $a_1, \ldots, a_N$ given by (2.1).

Proof. The proof is based on a combination of two proofs found in [1] and [2]. We begin by scaling the roots a_k found in (2.1) to be on the unit circle. We will account for this change in the final step of the proof. Set $A_k = \frac{a_k}{|a_k|}$. Given equation (2.2), we want to re-write the difference $(x - A_k)$. We let $x = \cos(2t) + i\sin(2t)$ for $t \in [0, \pi]$.

We then have

$$\begin{aligned} x - A_k &= \Big(\cos(2t) - \cos(\alpha_k)\Big) + i\Big(\sin(2t) - \sin(\alpha_k)\Big) \\ &= -2\sin\left(t - \tfrac{\alpha_k}{2}\right)\sin\left(t + \tfrac{\alpha_k}{2}\right) + 2i\sin\left(t - \tfrac{\alpha_k}{2}\right)\cos\left(t + \tfrac{\alpha_k}{2}\right) \\ &= 2i\sin\left(t - \tfrac{\alpha_k}{2}\right)\Big(\cos\left(t + \tfrac{\alpha_k}{2}\right) + i\sin\left(t + \tfrac{\alpha_k}{2}\right)\Big) \\ &= 2i\sin\left(t - \tfrac{\alpha_k}{2}\right)e^{i\left(t + \frac{\alpha_k}{2}\right)}. \end{aligned}$$

We write $\widetilde{J}_{n,H}(x)$ to indicate that we have manipulated the original roots of the Cyclotomic Subgroup-Polynomial $J_{n,H}(x)$. Then

$$\begin{aligned} \widetilde{J}_{n,H}(x) = \sum_{j=0}^{N} c_j x^j &= \prod_{k=1}^{N}(x - A_k), \\ &= (2i)^N \prod_{k=1}^{N} \sin\left(t - \tfrac{\alpha_k}{2}\right) \cdot e^{i\left(t + \frac{\alpha_k}{2}\right)}, \\ &= (2i)^N \prod_{k=1}^{N} \sin\left(t - \tfrac{\alpha_k}{2}\right) \cdot e^{i\left(Nt + \frac{\alpha}{2}\right)}. \end{aligned}$$

Separating the constant coefficient, we now have the following:

$$\begin{aligned} c_0 + \sum_{k=1}^{N} c_k x^k &= \prod_{k=1}^{N}(x - A_k), \\ &= (2i)^N \prod_{k=1}^{N} \sin\left(t - \tfrac{\alpha_k}{2}\right) \cdot e^{i\left(Nt + \frac{\alpha}{2}\right)}, \\ &= (2i)^N \prod_{k=1}^{N} \sin\left(t - \tfrac{\alpha_k}{2}\right) \cdot e^{i\left(Nt + \frac{\alpha}{2}\right)}. \end{aligned}$$

Since $x = \cos(2t) + i\sin(2t), t \in [0, \pi]$, we observe that $t = 0$ and $t = \pi$ return the same value for x. Therefore:

$$\begin{aligned} \int_0^{\pi} \left(c_0 + \sum_{k=1}^{N} c_k x^k\right) dt &= \int_0^{\pi} c_0 \, dt + \int_0^{\pi} \sum_{k=1}^{n} c_k x^k dt \\ &= \int_0^{\pi} c_0 \, dt. \end{aligned}$$

Then, adjusting for our scaled roots as well as integrating a constant function over an interval of length π, the constant coefficient of the Cyclotomic Subgroup-Polynomial $J_{n,H}(x)$ is

$$b_0 = (|a_1| \cdot |a_2| \cdots |a_N|) \frac{(2i)^N}{\pi} \int_0^{\pi} \prod_{k=1}^{N} \sin\left(t - \tfrac{\alpha_k}{2}\right) \cdot e^{i\left(Nt + \frac{\alpha}{2}\right)} dt,$$

as required, and the proof is now complete. □

We now demonstrate an application of this theorem with an example.

Example 2.61. We saw in an earlier example that $J_{17,\{1,4,13,16\}}(x) = x^4 + x^3 - 6x^2 - x + 1$. We now use Theorem 2.60 to calculate the coefficients of this polynomial. We set $w = e^{\frac{2\pi i}{17}}$, and we calculate

$$\begin{aligned} a_1 &= w + w^4 + w^{13} + w^{16} & \arg(a_1) &= 0 \\ a_2 &= w^2 + w^8 + w^9 + w^{15} & \arg(a_2) &= \pi \\ a_3 &= w^3 + w^5 + w^{12} + w^{14} & \arg(a_3) &= 0 \\ a_4 &= w^6 + w^7 + w^{10} + w^{11} & \arg(a_4) &= \pi. \end{aligned}$$

We also calculate:

$$\begin{aligned} |a_1| &\approx 2.049481178 & |a_2| &\approx 0.4879283651 \\ |a_3| &\approx 0.3441507315 & |a_4| &\approx 2.905703545, \end{aligned}$$

so that

$$|a_1| \cdot |a_2| \cdot |a_3| \cdot |a_4| = 1.$$

Applying Theorem 2.60, we get that the constant coefficient is equal to

$$|a_1| \cdot |a_2| \cdot |a_3| \cdot |a_4| \frac{(2i)^4}{\pi} \int_0^{\pi} \sin^2(t) \sin^2\left(t - \tfrac{\pi}{2}\right) e^{i(4t+\pi)} dt = 1,$$

as expected. We note that the final integral was evaluated to be $\frac{\pi}{16}$, using the computer algebra system Maple.

2.11 Resultants of Pairs of Certain Cyclotomic Subgroup-Polynomials

In this section we study the resultant of pairs of Cyclotomic Subgroup-Polynomials of the form $J_{n,\{-1,1\}}(x)$. The resultant of two polynomials over a commutative ring is defined to be the determinant of their Sylvester matrix (see, for example, [49, pg. 21]). If the coefficients of the polynomials belong to an integral domain, such as is the case with the Cyclotomic Subgroup-Polynomials, then we can calculate the resultant as follows:

Definition 2.62. *Let* $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, a_n \neq 0$ *with roots* $\mu_1, \mu_2, \ldots, \mu_n$ *and* $g(x) = b_m x^m + a_{m-1} x^{m-1} + \ldots + b_1 x + b_0, b_m \neq 0$ *with roots* $\lambda_1, \lambda_2, \ldots, \lambda_m$. *Then the resultant of* $f(x)$ *and* $g(x)$ *can be calculated as*

$$\rho(f, g) = a_n^m b_m^n \prod_{\substack{1 \leq j \leq n \\ 1 \leq i \leq m}} (\mu_j - \lambda_i).$$

The resultants of pairs of cyclotomic polynomials was studied in [3] by Apostol, and Dresden [18] presented a new proof of Apostol's result, as well as a related theorem regarding linear combinations of cyclotomic polynomials. The main result concerning the resultant of cyclotomic polynomials is the following:

Theorem 2.63 (Apostol)**.** *For* $0 < m < n$ *integers, we have*

$$\rho(\Phi_m, \Phi_n) = \begin{cases} p^{\varphi(m)} & \text{if } n/m \text{ is a power of a prime } p, \\ 1 & \text{otherwise.} \end{cases}$$

We will now calculate a few resultants of pairs of Cyclotomic Subgroup-Polynomials, $J_{n,\{-1,1\}}(x)$, in the following example.

Example 2.64. The following resultants were calculated using the computer algebra system Maple using the built-in Resultant function.

$$\rho(J_{3,\{-1,1\}}, J_{5,\{-1,1\}}) = -1, \qquad \rho(J_{3,\{-1,1\}}, J_{6,\{-1,1\}}) = -2,$$
$$\rho(J_{3,\{-1,1\}}, J_{7,\{-1,1\}}) = 1, \qquad \rho(J_{5,\{-1,1\}}, J_{10,\{-1,1\}}) = -4,$$
$$\rho(J_{5,\{-1,1\}}, J_{25,\{-1,1\}}) = 25, \qquad \rho(J_{5,\{-1,1\}}, J_{49,\{-1,1\}}) = -1.$$

It seems that the calculated resultants are of the form $\pm 1, \pm p^k$ for a prime p.

We are now ready to state the main result of this section:

Theorem 2.65. *For $0 < m < n$ integers, we have*

$$\rho(J_{m,\{-1,1\}}, J_{n,\{-1,1\}}) = \begin{cases} \pm p^{\frac{\varphi(m)}{2}} & \text{if } n/m \text{ is a power of a prime } p, \\ \pm 1 & \text{otherwise,} \end{cases}$$

where the signs can be specified in some cases.

To prove this result, we will require a number of identities. To allow for an uninterrupted proof, we have collected all of these identities, in the order in which they are used, in the following section preceding the proof.

2.11.1 Useful Results

Throughout this section we will use the Legendre symbol $\left(\frac{a}{p}\right)$ of a and p, defined for integers a and odd primes p for which $p \nmid a$ to be 1 if $x^2 \equiv a \pmod{p}$ for some x and -1 otherwise. We begin with a famous result of Gauss; see, e.g., [48, pg. 132].

Theorem 2.66 (Lemma of Gauss)**.** *For any odd prime p let $(a, p) = 1$. Consider the integers $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ and their least positive residues modulo p. If n denotes the number of these residues that exceed $\frac{p}{2}$, then*

$$\left(\frac{a}{p}\right) = (-1)^n,$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol of a modulo p.

Next, we quote [48, pg. 142].

Theorem 2.67. *We call $\mathcal{H}$ a one-half set of reduced residues modulo p if $\mathcal{H}$ has the property that $h \in \mathcal{H}$ if and only if $-h \notin \mathcal{H}$. Let $\mathcal{H}$ and $\mathfrak{H}$ be two complementary one-half sets. Suppose that $(a,p) = 1$. Let v be the number of $h \in \mathcal{H}$ for which $ah \in \mathfrak{H}$. Then*

$$(-1)^v = \left(\frac{a}{p}\right),$$

$a\mathcal{H}$ and $a\mathfrak{H}$ are complementary one-half sets, and

$$\left(\frac{a}{p}\right) = \prod_{h\in\mathcal{H}} \frac{\sin\left(\frac{2\pi ah}{p}\right)}{\sin\left(\frac{2\pi h}{p}\right)}.$$

The following product involving differences of the cosine function can be found in [27, pg. 499, Identity (91.2.9)].

Theorem 2.68. *For positive integers n, we have*

$$\prod_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left(\cos(y) - \cos\left(\frac{2\pi k}{n}\right)\right) = \begin{cases} 2^{\frac{1}{2}-\frac{n}{2}}\sin\left(\frac{ny}{2}\right)\csc\left(\frac{y}{2}\right) & n \text{ odd}, \\ 2^{1-\frac{n}{2}}\sin\left(\frac{ny}{2}\right)\csc(y) & n \text{ even}, \end{cases}$$

where $\lfloor x\rfloor$ represents the floor of x.

The following product of the sine function can be found in [50, pg. 753, Identity 3].

Theorem 2.69. *For positive integers n, we have*

$$\prod_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\sin\left(\frac{k\pi}{n}\right) = 2^{\frac{1-n}{2}}n^{\frac{1}{2}}.$$

In this section we will also make use of the Möbius function $\mu(x)$ defined on the positive integers. For the definition of the Möbius function and some of its properties, see e.g. [48, Section 4.3]. We quote the following from [48, Section 4.3]:

Lemma 2.70. *For positive integers n and divisors d of n, we have*

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

and

$$\sum_{d|n} \mu(d) \frac{n}{d} = \varphi(n).$$

Lemma 2.71. *For positive integers n and divisors $d|n$, we have*

$$\prod_{d|n} \begin{cases} \left(2^{\frac{1}{2}-\frac{n}{2d}}\right)^{\mu(d)} & \text{if} \quad \frac{n}{d} \quad \text{odd}, \\ \left(2^{1-\frac{n}{2d}}\right)^{\mu(d)} & \text{if} \quad \frac{n}{d} \quad \text{even} \end{cases} = 2^{\frac{-\varphi(n)}{2}}.$$

Proof. Due to the common base 2 in both of these products, we can combine them into a single exponent: If we set

$$P := \prod_{d|n} \begin{cases} \left(2^{\frac{1}{2}-\frac{n}{2d}}\right)^{\mu(d)} & \text{if} \quad \frac{n}{d} \quad \text{odd}, \\ \left(2^{1-\frac{n}{2d}}\right)^{\mu(d)} & \text{if} \quad \frac{n}{d} \quad \text{even}, \end{cases}$$

then

$$P = \left(2^{\sum_{\frac{n}{d}\text{odd}} \frac{1}{2} - \frac{n}{2d} + \sum_{\frac{n}{d}\text{even}} 1 - \frac{n}{2d}}\right)^{\mu(d)}.$$

Now we use the fact that as d ranges through the divisors of n, the value $\frac{n}{d}$ also ranges through the divisors of n. We also clear the denominator in the exponent by multiplying the exponent by 2 and adjust by taking the square root:

$$\begin{aligned} P &= \left(\left(2^{\sum_{d\text{odd}} 1 - \frac{n}{d} + \sum_{d\text{even}} 2 - \frac{n}{d}}\right)^{\mu(d)}\right)^{\frac{1}{2}} \\ &= \left(2^{\sum_d -\mu(d)\frac{m}{d} + \sum_d \mu(d)}\right)^{\frac{1}{2}} \\ &= 2^{-\frac{\varphi(n)}{2}}, \end{aligned}$$

where we have used Lemma 2.70. This completes the proof of Lemma 2.71. □

Lemma 2.72. *For positive integers n, we have*

$$G(n) = \prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \sin\left(\frac{\pi k}{n}\right) = \begin{cases} \frac{\sqrt{p}}{2^{\frac{\varphi(n)}{2}}} & \text{if} \quad n = p^\alpha, \\ \frac{1}{2^{\frac{\varphi(n)}{2}}} & \text{if} \quad n \neq p^\alpha. \end{cases}$$

Proof. We begin by applying a multiplicative version of the Möbius inversion formula to Theorem 2.69, as given in [41]:

$$\prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \sin\left(\frac{\pi k}{n}\right) = \prod_{d|n} \left(2^{\frac{1-\frac{n}{d}}{2}} \sqrt{\frac{n}{d}}\right)^{\mu(d)}.$$

To prove the lemma, we need to consider the product

$$\prod_{d|n} \left(\sqrt{\frac{n}{d}}\right)^{\mu(d)} \tag{2.3}$$

for the two cases $n = p^\alpha$ and $n \neq p^\alpha$. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ and consider the set $S = \{p_1, p_2, \ldots, p_s\}$. As we apply the Möbius function to the divisors of n, we are applying it to every non-empty subset of S as well as the case $d = 1$. If the given subset is of odd order, then $\mu(d) = -1$ and it will contribute to the denominator of our product. If the given subset is of even order, then $\mu(d) = 1$ and it will contribute to the numerator of the product. We also note that, as the index ranges over the divisors of n, we can replace $\frac{n}{d}$ with d.

Case 1 ($n = p^\alpha$): In this case, $S = \{p\}$ and the product in (2.3) has two factors:

$$\prod_{d|n} \left(\sqrt{\frac{n}{d}}\right)^{\mu(d)} = \frac{\sqrt{p^\alpha}}{\sqrt{p^{\alpha-1}}} = \sqrt{p},$$

as required.

Case 2 ($n \neq p^\alpha$): In this case, $|S| > 1$ and we consider two cases separately, based on the parity of $|S|$.

Sub-case 1 ($|S|$ is even): Let $[j]$ denote the set of all possible quotients $\frac{n}{d}$ by subsets

of S of order j. Then the product (2.3) becomes

$$\sqrt{\frac{(n)[2][4]\cdots[s]}{[1][3]\cdots[s-1]}}.$$

We pair the quotient (n) which corresponds to the case $d = 1$ and the quotient $[s]$ to get $\frac{n^2}{p_1\cdots p_s}$, then we pair the $\binom{s}{2}$ quotients in the set $[2]$ with their matching quotients in the set $[s-2]$ to get $\binom{s}{2}$ copies of $\frac{n^2}{p_1\cdots p_s}$, and we continue this way in the numerator and denominator. To verify that the number of copies of $\frac{n^2}{p_1\cdots p_s}$ in the numerator and denominator are equal, we use the binomial formula

$$(1-1)^s = 1 - \binom{s}{1} + \cdots - \binom{s}{s-1} + \binom{s}{s} = 0.$$

Therefore

$$\prod_{d|n}\left(\sqrt{\frac{n}{d}}\right)^{\mu(d)} = 1,$$

as required.

Sub-case 2 ($|S|$ is odd): Then the product becomes

$$\sqrt{\frac{(n)[2][4]\cdots[s-1]}{[1][3]\cdots[s]}}.$$

We proceed in a similar fashion to the above sub-case, but this time we count the number of times any given p_r is in each $[k]$. Let p_r be fixed; then there are $\binom{s-1}{k-1}$ quotients in $[k]$ that contain p_r for each k. To verify that the number of copies of $\frac{n^2}{p_1\cdots p_s}$ in the numerator and denominator are equal we use the binomial formula

$$(1-1)^{s-1} = 1 - \binom{s-1}{1} + \cdots - \binom{s}{s-1} + \binom{s-1}{s-1} = 0.$$

Therefore

$$\prod_{d|n}\left(\sqrt{\frac{n}{d}}\right)^{\mu(d)} = 1,$$

as required. We have thus dealt with all cases, and the proof is complete. □

2.11.2 Proof of Theorem 2.65

We begin by considering the following resultant for arbitrary positive numbers m and n with $n > m$:

$$\begin{aligned}
\rho(J_{m,\{-1,1\}}, J_{n,\{-1,1\}}) &= \prod_{k=1,(k,n)=1}^{\lfloor\frac{n-1}{2}\rfloor}\prod_{j=1,(j,m)=1}^{\lfloor\frac{m-1}{2}\rfloor}\left(e^{\frac{2\pi ik}{n}} - e^{\frac{2\pi ij}{m}}\right)\\
&= \prod_{k=1,(k,n)=1}^{\lfloor\frac{n-1}{2}\rfloor}\prod_{j=1,(j,m)=1}^{\lfloor\frac{m-1}{2}\rfloor}\left(2\cos\left(\frac{2\pi k}{n}\right) - 2\cos\left(\frac{2\pi j}{m}\right)\right)\\
&= 2^{\frac{\phi(n)\phi(m)}{4}}\prod_{k=1,(k,n)=1}^{\lfloor\frac{n-1}{2}\rfloor}\prod_{j=1,(j,m)=1}^{\lfloor\frac{m-1}{2}\rfloor}\left(\cos\left(\frac{2\pi k}{n}\right) - \cos\left(\frac{2\pi j}{m}\right)\right).
\end{aligned}$$

From here, we will consider separate cases of the values of m and n to prove our result in general.

In the special case when $n = p$, $m = q$, are distinct odd primes we have

$$\begin{aligned}
\rho(J_{p,\{-1,1\}}, J_{q,\{-1,1\}}) &= 2^{\frac{(p-1)(q-1)}{4}}\prod_{k=1}^{\frac{p-1}{2}}\prod_{j=1}^{\frac{q-1}{2}}\left(\cos\left(\frac{2\pi k}{p}\right) - \cos\left(\frac{2\pi j}{q}\right)\right)\\
&= 2^{\frac{(p-1)(q-1)}{4}}\prod_{k=1}^{\frac{p-1}{2}} 2^{\frac{1}{2}-\frac{q}{2}}\sin\left(q\frac{\pi k}{p}\right)\csc\left(\frac{\pi k}{p}\right), \qquad (2.4)
\end{aligned}$$

by Theorem 2.68. Next, we simplify the terms of (2.4) to get

$$\rho(J_{p,\{-1,1\}}, J_{q,\{-1,1\}}) = \prod_{k=1}^{\frac{p-1}{2}}\frac{\sin\left(q\frac{\pi k}{p}\right)}{\sin\left(\frac{\pi k}{p}\right)} = \left(\frac{p}{q}\right) = \pm 1,$$

by Theorem 2.67, as required. In the special case when $m = p$ and $n > 1$, we have

$$\begin{aligned}\rho(J_{n,\{-1,1\}}, J_{p,\{-1,1\}}) &= 2^{\frac{\phi(n)(p-1)}{4}} \prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \prod_{j=1}^{\frac{p-1}{2}} \left(\cos\left(\frac{2\pi k}{n}\right) - \cos\left(\frac{2\pi j}{p}\right)\right) \\ &= 2^{\frac{\phi(n)(p-1)}{4}} \prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} 2^{\frac{1}{2}-\frac{p}{2}} \sin\left(p\frac{\pi k}{n}\right) \csc\left(\frac{\pi k}{n}\right), \qquad (2.5)\end{aligned}$$

by Theorem 2.68. Next, we simplify the terms of the product (2.5) and consider the three possible relationships between the integers m and n:

$$\begin{aligned}\rho(J_{n,\{-1,1\}}, J_{p,\{-1,1\}}) &= \prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \frac{\sin\left(p\frac{\pi k}{n}\right)}{\sin\left(\frac{\pi k}{n}\right)} \\ &= \begin{cases} \left(\frac{p}{n}\right) & \text{if } (n,p) = 1 \text{ by Theorem 2.67,} \\ \frac{\prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \sin\left(p\frac{\pi k}{n}\right)}{G(n)} & \text{if } (n,p) > 1 \end{cases} \\ &= \begin{cases} \pm 1 & \text{if } (n,p) = 1, \\ \pm q^{\frac{\varphi(n)}{2}} \frac{G(n)}{G(n)} = \pm q^{\frac{\varphi(n)}{2}} & \text{if } (n,p) > 1 \text{ and } \frac{n}{p} = q^{\alpha}, \\ \pm 1 & \text{if } (n,p) > 1 \text{ and } \frac{n}{p} \text{ is not a} \\ & \text{prime power by Lemma 2.72,} \end{cases}\end{aligned}$$

as required.

Now that we have considered these special cases of positive integers m and n, we return our attention to the general case. We have

$$\begin{aligned}\rho(J_{n,\{-1,1\}}, J_{m,\{-1,1\}}) &= 2^{\frac{\phi(n)\phi(m)}{4}} \prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \prod_{j=1,(j,m)=1}^{\lfloor \frac{m-1}{2} \rfloor} \left(\cos\left(\frac{2\pi k}{n}\right) - \cos\left(\frac{2\pi j}{m}\right)\right) \\ &= 2^{\frac{\phi(n)\phi(m)}{4}} \prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \prod_{d|m} \begin{cases} \left(2^{\frac{1}{2}-\frac{m}{2d}} \sin\left(\frac{m}{d}\cdot\frac{\pi k}{n}\right) \csc\left(\frac{\pi k}{n}\right)\right)^{\mu(d)}, \\ \left(2^{1-\frac{m}{2d}} \sin\left(\frac{m}{d}\cdot\frac{\pi k}{n}\right) \csc\left(\frac{2\pi k}{n}\right)\right)^{\mu(d)}, \end{cases} \qquad (2.6)\end{aligned}$$

where on the right-hand side the two terms hold for $\frac{m}{d}$ odd, respectively even, and

where we have applied the multiplicative version of the Möbius inversion formula found in [41] and Theorem 2.68. Simplifying the terms in the product (2.6) we get

$$\rho(J_{n,\{-1,1\}}, J_{m,\{-1,1\}}) = \prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \prod_{d|m} \begin{cases} \left(\sin\left(\frac{m}{d} \cdot \frac{\pi k}{n}\right) \csc\left(\frac{\pi k}{n}\right)\right)^{\mu(d)}, & \frac{m}{d} \quad \text{odd} \\ \left(\sin\left(\frac{m}{2d} \cdot \frac{2\pi k}{n}\right) \csc\left(\frac{2\pi k}{n}\right)\right)^{\mu(d)}, & \frac{m}{d} \quad \text{even} \end{cases}$$

$$= \prod_{d|m} \begin{cases} 1 \quad \text{if} \quad (\frac{m}{d}, n) = 1, \quad \frac{m}{d} \quad \text{odd}, \\ 1 \quad \text{if} \quad (\frac{m}{2d}, n) = 1, \quad \frac{m}{d} \quad \text{even}, \\ (G\left(\frac{nd}{m}\right)^2 / G(n))^{\mu(d)} \quad \text{if} \quad (\frac{m}{d}, n) > 1, \quad \frac{m}{d} \quad \text{odd}, \\ (G\left(\frac{2nd}{m}\right)^2 / G(n))^{\mu(d)} \quad \text{if} \quad (\frac{m}{2d}, n) > 1, \quad \frac{m}{d} \quad \text{even}, \end{cases}$$

where $G(n)$ is defined in Lemma 2.72. Hence

$$\rho(J_{n,\{-1,1\}}, J_{m,\{-1,1\}}) = \begin{cases} 1 \quad \text{if} \quad (n.m) = 1, \\ \pm p^{\frac{\phi(n)}{2}} \quad \text{if} \quad (n.m) > 1, \frac{n}{m} = p^{\alpha}, \\ \pm 1 \quad \text{if} \quad (n.m) > 1, \frac{n}{m} \neq p^{\alpha}, \end{cases}$$

as required. The proof of Theorem 2.65 is now complete. □

We conclude this section by noting that we found no results similar to Theorems 2.63 and 2.65 for the resultants of Cyclotomic Subgroup-Polynomials when the order of the subgroup $H \leq (\mathbb{Z}/n\mathbb{Z})^{\times}$ is $|H| \geq 3$. We demonstrate this with the following example.

Example 2.73. For varying values of positive integers n such that $3 \,|\, |(\mathbb{Z}/n\mathbb{Z})^{\times}|$, we calculate the following resultants:

$$\rho(J_{7,\{1,2,4\}}(x), J_{9,\{1,4,7\}}(x)) = 4, \qquad \rho(J_{7,\{1,2,4\}}(x), J_{13,\{1,3,9\}}(x)) = 53,$$
$$\rho(J_{7,\{1,2,4\}}(x), J_{14,\{1,9,11\}}(x)) = 8, \qquad \rho(J_{7,\{1,2,4\}}(x), J_{19,\{1,7,11\}}(x)) = 539,$$
$$\rho(J_{13,\{1,3,9\}}(x), J_{14,\{1,9,11\}}(x)) = 79, \qquad \rho(J_{14,\{1,9,11\}}(x), J_{19,\{1,7,11\}}(x)) = 1939,$$

with no apparent pattern and/or result.

Remark: The resultant in Theorem 2.65 can be re-written in two ways that may

be useful in studying identities involving the Chebyshev polynomials, and which was interesting to the author.

$$\rho(J_{m,\{-1,1\}}, J_{n,\{-1,1\}}) = 2^{\frac{\phi(n)\phi(m)}{4}} \prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \prod_{d|m} \begin{cases} \left(2^{\frac{1}{2}-\frac{m}{2d}} U_{\frac{m}{d}-1}\left(\cos\left(\frac{\pi k}{n}\right)\right)\right)^{\mu(d)}, & 2 \not| \frac{m}{d}, \\ \left(2^{1-\frac{m}{2d}} U_{\frac{m}{2d}-1}\left(\cos\left(\frac{2\pi k}{n}\right)\right)\right)^{\mu(d)}, & 2 | \frac{m}{d}. \end{cases}$$

$$= 2^{\frac{\phi(n)\phi(m)}{2}} (-1)^{\frac{\phi(n)\phi(m)}{4}} \prod_{k=1,(k,n)=1}^{\lfloor \frac{n-1}{2} \rfloor} \prod_{j=1,(j,m)=1}^{\lfloor \frac{m-1}{2} \rfloor} \sin\left(\frac{\pi k}{n} - \frac{\pi j}{m}\right) \sin\left(\frac{\pi k}{n} + \frac{\pi j}{m}\right).$$

2.12 The Irreducibility of $J_{p,H}(x)$ Revisited

In this section, we will provide an alternative proof that the Cyclotomic Subgroup-Polynomials are irreducible when $n = p$ is an odd prime and $H < (\mathbb{Z}/p\mathbb{Z})^{\times}$. Similarly to the cyclotomic polynomials $\Phi_p(x)$, we will show that $J_{p,H}(x)$ satisfies the Eisenstein criterion for an odd prime p.

We will adopt the same notation as was used in the Section 2.9. That is, we write $p - 1 = md$, with $d \geq 2$. We also write $J_{p,H}(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. We apply two transformations to our polynomials $J_{p,H}(x)$: first we replace x with $\frac{x-1}{n}$ and then we multiply the polynomial by the constant n^n. We illustrate these transformations by applying them to the polynomials of Example 2.23 in the following example.

Example 2.74.

$$J_{11,H_1}(x) = \Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\to x^{10} + 55x^8 + 440x^7 + 5170x^6 + 56408x^5 + 620950x^4 +$$
$$6830120x^3 + 75131485x^2 + 826446280x + 9090909091.$$

$$J_{11,H_2}(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$$
$$\to x^5 - 110x^3 - 55x^2 + 2310x + 979.$$

$$J_{11,H_3}(x) = x^2 + x + 3$$
$$\to x^2 + 11$$

We note that all the modified polynomials in this example are 11-Eisenstein. This is no coincidence:

Theorem 2.75. *If p is an odd prime, then the polynomials $J_{p,H}(x)$ become p-Eisenstein polynomials for all proper subgroups $H < (\mathbb{Z}/p\mathbb{Z})^\times$ when x is replaced by $\frac{x-1}{n}$ and the polynomial is multiplied by the constant n^n, where $n = \deg(J_{p,H}(x)) = [(\mathbb{Z}/p\mathbb{Z})^\times : H]$.*

Proof. We break this proof into two parts. We begin by showing that p divides all but the leading coefficient. Then we show that p^2 does not divide the constant coefficient.

Part 1. We transform $J_{p,H}(x)$ by defining $g(x) = n^n J_{p,H}\left(\frac{x-1}{n}\right)$. Then

$$\begin{aligned} g(x) &= n^n J_{p,H}(x)\left(\tfrac{x-1}{n}\right) \\ &= n^n\left(a_n\left(\tfrac{x-1}{n}\right)^n + \ldots + a_2\left(\tfrac{x-1}{n}\right)^2 + a_1\left(\tfrac{x-1}{n}\right) + a_0\right) \\ &= \sum_{j=0}^{n} n^{n-j} a_j (x-1)^j. \end{aligned}$$

Now write $g(x) = b_n x^n + \ldots + b_2 x^2 + b_1 x + b_0$. Then

$$\begin{aligned} b_i &= \sum_{k=i}^{n} n^{n-k}\binom{k}{i}(-1)^{k-i}a_k \\ &\equiv \sum_{k=i}^{d} d^{d-k-1}\binom{k}{i}(-1)^{k-i}\left[(-1)^{d-k+1}\binom{d}{d-k}m^{d-k-1}d^{-1}\right] \pmod{p}, \end{aligned}$$

since $d = \frac{p-1}{m}$. Then we have:

$$\begin{aligned} b_i &\equiv \sum_{k=i}^{d} d^{d-k-1}(-1)^{d+1-i}m^{d-k-1}\binom{k}{i}\binom{d}{d-k} \\ &= d^{d-1}m^{d-1}(-1)^{d+1-i}\sum_{k=i}^{d}(md)^{-k}\binom{k}{i}\binom{d}{d-k} \\ &= d^{d-1}m^{d-1}(-1)^{d+1-i}\sum_{k=i}^{d}(md)^{-k}\binom{d}{i}\binom{d-i}{d-k} \pmod{p}, \end{aligned}$$

where we have used the binomial coefficient formula $\binom{k}{i}\binom{d}{d-k} = \binom{d}{i}\binom{d-i}{d-k}$. Continuing, we get:

$$\begin{aligned} b_i &\equiv (-1)^i \binom{d}{i} \sum_{k=0}^{d-i} (-1)^{k+d} \binom{d-i}{k} \\ &= (-1)^{d-i} \binom{d}{i} \sum_{k=0}^{d-i} (-1)^{k} \binom{d-i}{k} \\ &= (-1)^{d-i} \binom{d}{i} (1+(-1))^{d-i} \\ &= 0 \pmod{p}, \end{aligned}$$

for $i \neq d$, as required. Note that the case $i = d$ corresponds to the leading coefficient which is 1.

Part 2. In this part of the proof, we will make use of a result of Barcanescu found in [6].

Lemma 2.76 (Barcanescu)**.** *For an odd prime p and non-empty subsets $M_1, M_2, \ldots, M_n \subseteq \mathbb{F}_p$, define*

$$\{1, C_1, \ldots, C_{d-1}\} := \#\{(x_1, \ldots, x_n) | x_j \in M_j \text{ and } \sum x_j = 0\}.$$

Then, with $p - 1 = md, d > 2$ we have

$$a_0(p,d) = \frac{1}{d}\left(p \cdot \{1, C_1, \ldots, C_{d-1}\} - m^{d-1}\right).$$

The important aspect of this lemma for us is: For a fixed odd prime p and proper subgroup $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$, the constant coefficient of $J_{p,H}(x)$ satisfies

$$a_0 = \frac{1}{d}\left(p \cdot A - m^{d-1}\right),$$

where $p - 1 = dm$ and A is a positive integer $0 \leq A \leq m \cdot (d-1)$.

Suppose, towards a contradiction, that $a_0 \equiv 0 \pmod{p^2}$. Then

$$\begin{aligned} & p \cdot A - m^{d-1} \equiv 0 \pmod{p^2}, \\ & \Rightarrow p \cdot A = m^{d-1} + Bp^2, \\ & \Rightarrow m^{d-1} = p \cdot A - Bp^2, \\ & \Rightarrow p | m^{d-1}. \end{aligned}$$

This is a contradiction since $p - 1 = md$ and $p \not| m$. This implies, in turn, that $b_0 \not\equiv 0 \pmod{p^2}$ and combined with part 1 we have shown that $g(x)$ is Eisenstein for the odd prime p, as required. □

2.13 Congruence Property

One of the properties of the cyclotomic polynomial is the fact that if $n = p^m$, then $\Phi_n(x) = \Phi_p(x^{p^{m-1}})$. This is not true for every Cyclotomic Subgroup-Polynomial, as we will see with the following example:

Example 2.77. We set $p = 5$ and take $n = p^2 = 25$. If we choose $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ to be $H = \{1, 4\}$, then $J_{5,H}(x) = x^2 + x - 1$. The associated subgroup having the same order $H' \leq (\mathbb{Z}/25\mathbb{Z})^\times$ such that $|H'| = |H|$ is $H' = \{1, 24\}$ and we have

$$J_{25,H'}(x) = x^{10} - 10x^8 + 35x^6 + x^5 - 50x^4 - 5x^3 + 25x^2 + 5x - 1.$$

We observe that

$$J_{5,H}(x^5) = x^{10} + x^5 - 1 \neq J_{25,H'}(x).$$

However, we do note that

$$J_{25,H'}(x) \equiv x^{10} + x^5 - 1 \pmod{5}.$$

As it turns out, this is not a coincidence.

As we just saw, we do not have the direct equality that we desired; however, we have the following analogue:

Theorem 2.78. *If $n = p^m$, then for each subgroup $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ and associated subgroup $H' \leq (\mathbb{Z}/p^m\mathbb{Z})^\times$ such that $|H'| = |H|$, we have*

$$J_{p^m,H'}(x) \equiv J_{p,H}(x^{p^{m-1}}) \pmod{p}.$$

To prove Theorem 2.78, we will make use of the following theorem (this theorem adds only a small variation to Theorem 2.3), which can be found in an Abstract Algebra reference such as [30, pg. 35], for example.

Theorem 2.79. *All subgroups of a cyclic group are cyclic. If $G =< g >$ is a cyclic group of order n, then for each divisor $d|n$ there exists exactly one subgroup of order d and it can be generated by the element $g^{\frac{n}{d}}$.*

We now return to our proof.

Proof of Theorem 2.78. Let us denote $w := e^{\frac{2\pi i}{p}}$ and $a := e^{2\pi i/p^m}$. We begin by noting that if the element h generates the subgroup $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$, then $h' = h^{p^{m-1}} \pmod{p^m}$ generates $H' \leq (\mathbb{Z}/p^m\mathbb{Z})^\times$. That is,

$$\begin{aligned} a^{h'} &\equiv a^{h^{p^{m-1}}} \pmod{p^m} \\ &= a^{hp(m-1)} = a^{(p^{m-1})^h} \equiv w^h \pmod{p}. \end{aligned}$$

The roots of $J_{p,H}$ and $J_{p^m,H'}$ are of the form $w^{\sum_{h\in H} h}$ and of the form $a^{\sum_{h'\in H'}}$, where the index runs through the coset representatives of H and H', respectively. If we then apply the congruence $a^{h'} \equiv w^h \pmod{p}$ to each term in the summand defining the roots, we get the required polynomial congruence. □

Let us illustrate this theorem with our recurring example from this subsection:

Example 2.80. We set $p = 5, n = 5^2 = 25, w = e^{\frac{2\pi i}{5}}$, and $a = e^{\frac{2\pi i}{25}}$. We take $H \leq (\mathbb{Z}/5\mathbb{Z})^\times$ to be $H = \{1, 4\}$. The unique subgroup of order 2 $H' \leq (\mathbb{Z}/25\mathbb{Z})^\times$ is

$H' = \{1, 24\}$. We then calculate:

$$\begin{aligned}
1^5 &= 1 \equiv 1 \pmod{25},\\
2^5 &= 32 \equiv 7 \pmod{25},\\
3^5 &= 243 \equiv 18 \pmod{25},\\
4^5 &= 1024 \equiv 24 \pmod{25};\\
w^1 + w^4 &= 2\cos(\frac{2\pi}{25}), \quad w^2 + w^3 = -2\cos(\frac{\pi}{5});\\
a^1 + a^{24} &= 2\cos(\frac{2\pi}{25}), \quad a^7 + a^{18} = -2\cos(\frac{11\pi}{25}), \ldots
\end{aligned}$$

Then

$$\begin{aligned}
J_{5,\{1,4\}}(x) &= x^2 + x - 1,\\
J_{25,\{1,24\}}(x) &= x^{10} - 10x^8 + 35x^6 + x^5 - 50x^4 - 5x^3 + 25x^2 + 5x - 1\\
&\equiv x^{10} + x^5 - 1 \pmod{5}\\
&= J_{5,\{1,4\}}(x^5),
\end{aligned}$$

as required.

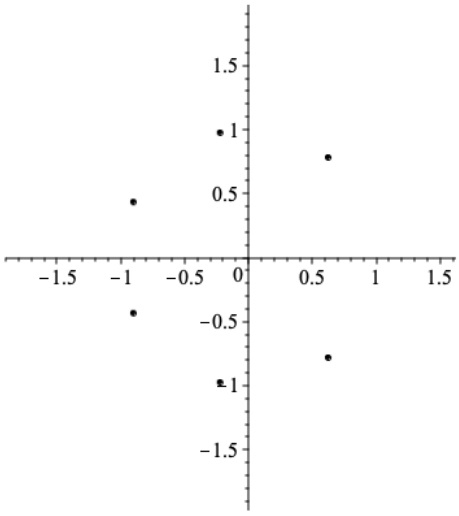
2.14 Roots

The aim of this section is to discuss the roots of the Cyclotomic Subgroup-Polynomials for different values of n and subgroups $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$. We start by considering the roots of of the polynomials calculated in Example 2.10.

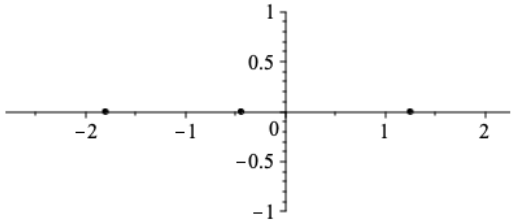
Example 2.81. As was calculated in Example 2.10, we have:

$$\begin{aligned}
J_{7,H_1}(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.\\
J_{7,H_2}(x) &= x^3 + x^2 - 2x - 1.\\
J_{7,H_3}(x) &= x^2 + x + 2.\\
J_{7,H_4}(x) &= x - 1.
\end{aligned}$$

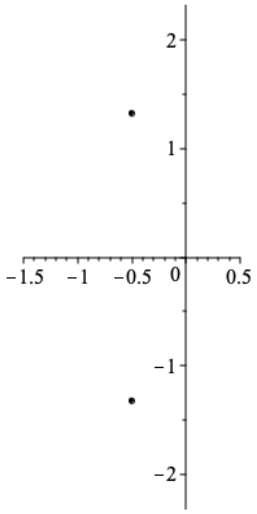
Plotting the roots of $J_{n,H_j}(x)$, we have:



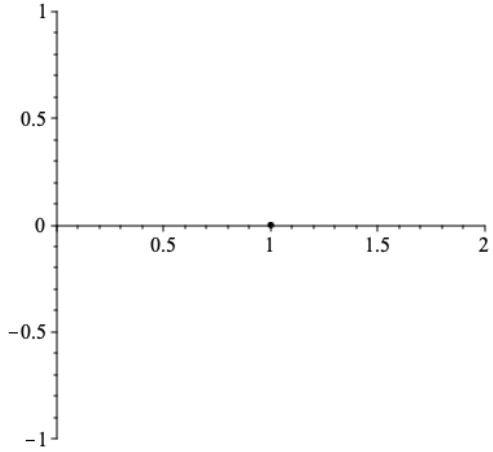
(a) Roots of J_{7,H_1}



(b) Roots of J_{7,H_2}



(c) Roots of J_{7,H_3}



(d) Roots of J_{7,H_4}

Figure 2.1: The Roots of $\{J_{7,H}(x)\}_{H\leq(\mathbb{Z}/7\mathbb{Z})^\times}$

We note from this example that $J_{7,H_j}(x)$ seems to have either all real roots or no real roots. This particular behaviour of the roots of $J_{n,H_j}(x)$ seems to depend entirely on the parity of the order of the subgroup $H_j \leq G, j = 1, 2, 3, 4$. We now formally state these observations for a general odd prime p.

Theorem 2.82. *When $|H|$ is even, $J_{p,H}(x)$ has only real roots.*

Proof. H is a finite cyclic subgroup of even order and is therefore isomorphic to $(\mathbb{Z}/2m\mathbb{Z})$ for some integer m. Then every coset of H is a scalar multiple of the

underlying set of $(\mathbb{Z}/2m\mathbb{Z})$ and we can consider a general root a_k. Writing $w = e^{\frac{2\pi i}{p}} = \left(\cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right)\right)$, we see that each root a_k, as defined in (2.1) and appearing in the product (2.2), will have imaginary part equal to 0 since $\sin(-\theta) = -\sin(\theta)$. Indeed,

$$\begin{aligned} a_k &= \sum_{h\in H} w^{h_k h} \\ &= \sum_{j=1}^{m} \left[\left(\cos\left(\frac{2\pi j}{p}\right) + i\sin\left(\frac{2\pi j}{p}\right)\right) + \left(\cos\left(-\frac{2\pi j}{p}\right) + i\sin\left(-\frac{2\pi j}{p}\right)\right)\right] \\ &= \sum_{j=1}^{m} 2\cos\left(\frac{2\pi j}{p}\right). \end{aligned}$$

This shows that $a_k \in \mathbb{R}$ for all k, as required. □

Analogously, we also have:

Theorem 2.83. *When $|H|$ is odd, $J_{p,H}(x)$ has no real roots.*

Proof. H is a finite cyclic subgroup of odd order and is therefore isomorphic to $(\mathbb{Z}/(2m+1)\mathbb{Z})$ for some integer m. Then every coset of H is a scalar multiple of the underlying set of $(\mathbb{Z}/(2m+1)\mathbb{Z})$ and we can consider a general root a_k. As we did in the previous proof, we write $w = e^{\frac{2\pi i}{p}} = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right)$ and see that each root a_k, as defined in (2.1) and appearing in the product (2.2), will have at least one non-zero imaginary part since the "pairing" that occurred in the previous proof will not occur in $(\mathbb{Z}/(2m+1)\mathbb{Z})$.

$$\begin{aligned} a_k &= \sum_{h\in H} w^{h_k h} \\ &= \sum_{j=1}^{2m+1} \left(\cos\left(\frac{2\pi j}{p}\right) + i\sin\left(\frac{2\pi j}{p}\right)\right) \\ &= \left[\cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right)\right] + \sum_{j=2}^{2m+1} \left(\cos\left(\frac{2\pi j}{p}\right) + i\sin\left(\frac{2\pi j}{p}\right)\right). \end{aligned}$$

We have separated the first term from the remainder of the that defines a_k just to emphasize the presence of at least one imaginary term. This shows that $a_k \notin \mathbb{R}$ for all k, as required. □

We plotted the roots of $J_{p,H}(x)$ for various values of primes p and different subgroups H related to the congruence class of the prime p. When we have nonreal roots, it appears that the roots of these polynomials are filling out a distinct pattern but no limiting curve is apparent. Whether $J_{n,H}(x)$ has real roots or nonreal roots, it appears that the roots of these polynomials are bounded in modulus by a bound depending on the order of H.

Example 2.84. Let the subgroup $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$ be such that $|H| = 2$. Then we know each root in $J_{n,H}(x)$ is of the form $a_k = 2\cos(\alpha)$ for some real number α, so that $|a_k| \leq 2$. Recall from Example 2.10 that $H_2 = \{1, 6\} < (\mathbb{Z}/7\mathbb{Z})^\times$ with $w = e^{\frac{2\pi i}{7}}$. For $J_{7,H_2}(x)$, we have

$$\begin{aligned} a_1 &= w + w^6 = 2\cos\left(\frac{2\pi}{7}\right), \\ a_2 &= w^2 + w^5 = 2\cos\left(\frac{4\pi}{7}\right), \\ a_3 &= w^3 + w^4 = 2\cos\left(\frac{6\pi}{7}\right). \end{aligned}$$

This example can be generalized to give a rough bound for the modulus of the roots in the general case based on the parity of the order of the subgroup $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$:

Theorem 2.85. *(i) Let $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ be of even order, $|H| = 2m$. Then the roots of $J_{p,H}(x)$ all lie in the interval $(-2m, 2m)$ on the real line.*

(ii) Let $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ be of odd order, $|H| = 2m + 1$. Then the roots of $J_{p,H}(x)$ all lie inside the circle $|z| < 2m + 1$ on the plane.

Proof. (i) As in the proof of Theorem 2.82, for each $k = 1, 2, \ldots, \frac{p-1}{2m}$, we have

$$\begin{aligned} a_k &= \sum_{j=1}^{m} \left[\left(\cos\left(\frac{2\pi j}{p}\right) + i\sin\left(\frac{2\pi j}{p}\right) \right) + \left(\cos\left(-\frac{2\pi j}{p}\right) + i\sin\left(-\frac{2\pi j}{p}\right) \right) \right], \\ &= \sum_{j=1}^{m} 2\cos\left(\frac{2\pi j}{p}\right). \end{aligned}$$

Since $|\cos(\beta)| \leq 1$ for all $\beta \in \mathbb{R}$, we see that $|a_k| \leq 2m$, as required.

(ii) As in the proof of Theorem 2.83, for each $k = 1, 2, \ldots, \frac{p-1}{2m+1}$, we have

$$\begin{aligned}
|a_k| &= \left| \sum_{h \in H} w^{h_k h} \right| \\
&\leq \sum_{j=1}^{2m+1} \left| \left(\cos\left(\tfrac{2\pi j}{p}\right) + i \sin\left(\tfrac{2\pi j}{p}\right) \right) \right| \\
&\leq \left| \left(\cos\left(\tfrac{2\pi}{p}\right) + i \sin\left(\tfrac{2\pi}{p}\right) \right) \right| + \ldots + \left| \left(\cos\left(\tfrac{2\pi(2m+1)}{p}\right) + i \sin\left(\tfrac{2\pi(2m+1)}{p}\right) \right) \right|
\end{aligned}$$

Since $\left| \left(\cos\left(\tfrac{2\pi j}{p}\right) + i \sin\left(\tfrac{2\pi j}{p}\right) \right) \right| \leq 1$ for all j, we see that $|a_k| \leq 2m + 1$, as required.

□

The bound on $|a_k|$ is sharp in the sense that there are roots a_k that get arbitrarily close to the values $\pm 2m$ on the real line in the even order case and arbitrarily close in modulus to $\pm(2m + 1)$ in the odd order case. To see this, consider the function $\cos\left(\frac{2\pi k}{p}\right)$, which tends to 1 as p tends to infinity when k is bounded and $\sin\left(\frac{2\pi k}{p}\right)$ which tends to 0 as p tends to infinity when k is bounded.

We now turn our discussion to the location of the roots of $J_{p,H}(x)$ when $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ is of odd order. In this case, the roots do not appear to be contained in any particular region. We illustrate these observations with our next example.

Example 2.86. If we take $p = 31$ and calculate $J_{31,H}(x)$ for subgroups $H \leq (\mathbb{Z}/31\mathbb{Z})^\times$ of odd order, we get:

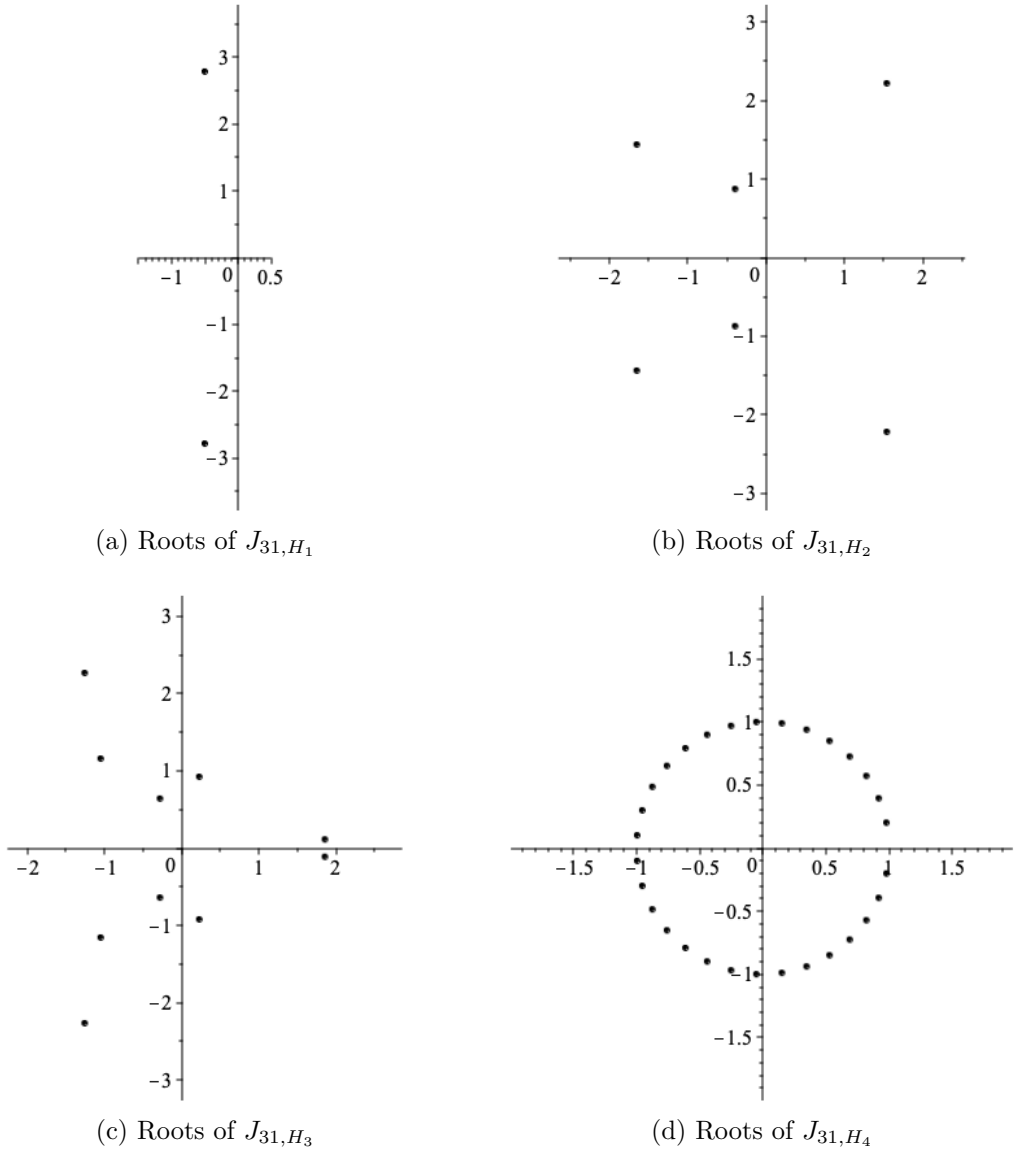
$$\begin{aligned}
H_1 &= \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}, \\
J_{31,H_1}(x) &= x^2 + x + 8,
\end{aligned}$$

$$\begin{aligned}
H_2 &= \{1, 2, 4, 8, 16\}, \\
J_{31,H_2}(x) &= x^6 + x^5 + 3x^4 + 11x^3 + 44x^2 + 36x + 32,
\end{aligned}$$

$$H_3 = \{1, 5, 25\},$$
$$J_{31,H_3}(x) = x^{10} + x^9 + 2x^8 - 16x^7 - 9x^6 - 11x^5 + 43x^4 + 6x^3 + 63x^2 + 20x + 25,$$

$$H_4 = \{1\}, \quad J_{31,H_4}(x) = \Phi_{31}(x).$$

The zeros of these polynomials are plotted in the following figure:



(a) Roots of J_{31,H_1}

(b) Roots of J_{31,H_2}

(c) Roots of J_{31,H_3}

(d) Roots of J_{31,H_4}

Figure 2.2: Roots of $\{J_{31,H}(x)\}_{H \leq (\mathbb{Z}/31\mathbb{Z})^\times}$

Chapter 3

Certain Classes of Quadrinomials

3.1 Background

For a positive integer n, the n^{th} cyclotomic polynomial, denoted by $\Phi_n(x)$, is the unique irreducible polynomial in $\mathbb{Z}[x]$ that divides $x^n - 1$ but not $x^m - 1$ for $m < n$. In the special case that p is an odd prime, the cyclotomic polynomial takes the form

$$\Phi_p(x) = \sum_{k=0}^{p-1} x^k = 1 + x + x^2 + \cdots + x^{p-1}, \tag{3.1}$$

and the roots of this polynomial are the primitive p^{th} roots of unity (equally spaced around the unit circle without $x = 1$). One variation on the general n^{th} cyclotomic polynomial is obtained by keeping the leading coefficient equal to 1, but replacing the remaining coefficients with an arbitrary positive integer c. In his investigation into the factorization of such polynomials

$$f_n(x) := x^n + cx^{n-1} + cx^{n-2} + \cdots + cx + c \in \mathbb{Z}[x], \tag{3.2}$$

Harrington [28] posed two main questions:

(1) For what positive integers n and c is $f_n(x)$ irreducible?

(2) If $f_n(x)$ is reducible, then how does it factor?

For particular values of c, these questions have been answered. Indeed, if there exists a prime p such that $p|c$ but $p^2 \not| c$, then the Eisenstein criterion applies and we conclude that $f_n(x)$ is irreducible. If $c = 1$, the two questions become questions related to cyclotomic polynomials and their answers are known. Harrington [28] answers these questions in general for values of c satisfying $c > 1$. His main results are as follows:

Theorem 3.1 (Harrington)**.** *Let n, c, and d be positive integers with $n \geq 3, d \neq c, d \leq 2(c-1)$, and $(n,c) \neq (3,3)$. If the trinomial $h(x) = x^n \pm cx^{n-1} \pm d$ is reducible in $\mathbb{Z}[x]$, then $h(x) = (x \pm 1)g(x)$ for some irreducible $g(x) \in \mathbb{Z}[x]$.*

This theorem is then used to answer the two initial questions with the following theorem below.

Theorem 3.2 (Harrington)**.** *Let n and c be positive integers with $c \geq 2$. Then the polynomials*

$$f(x) = x^n + \sum_{j=0}^{n-1} cx^j, \qquad g(x) = x^n + \sum_{j=0}^{n-1} (-1)^{n-j} cx^j,$$
$$h(x) = x^n - \sum_{j=0}^{n-1} cx^j, \qquad k(x) = x^n - \sum_{j=0}^{n-1} (-1)^{n-j} cx^j,$$

are irreducible in $\mathbb{Z}[x]$ with the exceptions of $f(x) = x^2 + 4x + 4 = (x+2)^2$ and $g(x) = x^2 - 4x + 4 = (x-2)^2$.

It is the purpose of this chapter to obtain analogous results for the modified case concerning polynomials of the form

$$x^n + cx^{n-a-1} + cx^{n-a-2} + \cdots + cx + c \in \mathbb{Z}[x], \tag{3.3}$$

where a and c are positive integers. In other words, we will investigate analogues to (3.2) with a gap after the leading coefficients. To align our notation with the original notation found in [28], we make the following definition.

Definition 3.3. *Let n, c and a be positive integers with $c \geq 2$ and $a < n$. Then denote:*

$$f_n^{a,c}(x) = x^n + \sum_{j=0}^{n-a-1} cx^j, \qquad g_n^{a,c}(x) = x^n + \sum_{j=0}^{n-a-1} (-1)^{n-j} cx^j,$$
$$h_n^{a,c}(x) = x^n - \sum_{j=0}^{n-a-1} cx^j, \qquad k_n^{a,c}(x) = x^n - \sum_{j=0}^{n-a-1} (-1)^{n-j} cx^j.$$

3.2 Irreducibility

In pursuit of an analogue to Theorem 3.1, we can multiply (3.3) by a linear factor $(x \pm 1)$. However, in this case, instead of the resulting polynomial being a trinomial we actually get a quadrinomial. More specifically, our resulting quadrinomials are of the form:

$$(x-1)f_n^{a,c}(x) = x^{n+1} - x^n + cx^{n-a} - c,$$

$$(x+1)g_n^{a,c}(x) = \begin{cases} x^{n+1} + x^n - cx^{n-a} + c & \text{if} \quad n-a \equiv 0 \pmod 2, \\ x^{n+1} + x^n + cx^{n-a} + c & \text{if} \quad n-a \equiv 1 \pmod 2, \end{cases}$$

$$(x-1)h_n^{a,c}(x) = x^{n+1} - x^n - cx^{n-a} + c,$$

$$(x+1)k_n^{a,c}(x) = \begin{cases} x^{n+1} + x^n + cx^{n-a} - c & \text{if} \quad n-a \equiv 0 \pmod 2, \\ x^{n+1} + x^n - cx^{n-a} - c & \text{if} \quad n-a \equiv 1 \pmod 2. \end{cases}$$

Unlike the case with Theorem 3.1, we are unable to determine the factorizations of these quadrinomials in the most general case. We will make an additional comment regarding an analogue to Theorem 3.1 in the conclusion of the thesis.

Similar to the case with Theorem 3.2, there are special factorizations of $f_n^{a,c}, g_n^{a,c}, h_n^{a,c}$, and $k_n^{a,c}$ that are known. For example, when $c = s^n$ is a perfect n^{th} power, we have:

$$x^n - c = (x-s)(x^{n-1} + sx^{n-2} + s^2x^{n-3} + \ldots + s^{n-1}), \tag{3.4}$$

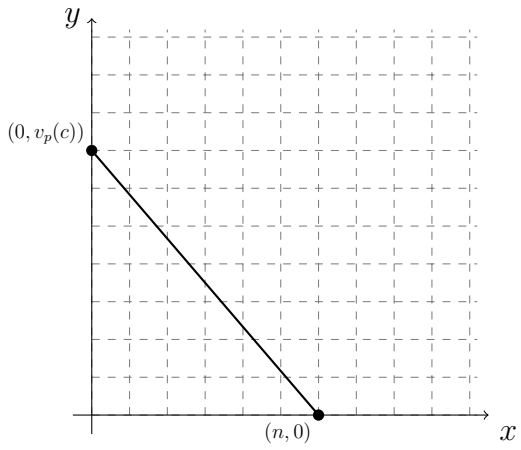
$$x^n + c = (x+s)(x^{n-1} - sx^{n-2} + s^2x^{n-3} - \ldots + s^{n-1}) \quad \text{if } n \text{ is odd.} \tag{3.5}$$

Already this contrasts with Theorem 3.1 in the sense that we have infinitely many exceptional cases. These are not the only reducible cases of $f_n^{a,c}, g_n^{a,c}, h_n^{a,c}$, and $k_n^{a,c}$ as we will see in the following example.

Example 3.4. We have the following factorizations of $f_6^{3,8}(x)$ and $h_8^{6,81}(x)$ respectively:

$$f_6^{3,8}(x) = x^6 + 8x^2 + 8x + 8 = (x^2 + 2x + 2)(x^4 - 2x^3 + 2x^2 + 4),$$
$$h_8^{6,81}(x) = x^8 - 81x - 81 = (x^2 + 3x + 3)(x^6 - 3x^5 + 6x^4 - 9x^3 + 9x^2 - 27).$$

This begs the question of whether we can say anything about the irreducibility of $f_n^{a,c}, g_n^{a,c}, h_n^{a,c}$, and $k_n^{a,c}$. If we fix an odd prime p that divides c and we consider the Newton polygon for either of these polynomials, we see that it is comprised of the line segment connecting $(0, v_p(c))$ to $(n, 0)$:



If we have $\gcd(v_p(c), n) = 1$ then there are no integer lattice points inside the line segment and by using Theorem A.12 and Corollary A.13 we conclude that the polynomial is irreducible. This gives rise to the following lemma.

Lemma 3.5. *Let $f_n^{a,c}(x), g_n^{a,c}(x), h_n^{a,c}(x)$, and $k_n^{a,c}(x)$ be as in Definition 3.3. If there exists a prime p such that $p|c$ and $\gcd(n, v_p(c)) = 1$, then the polynomials $f_n^{a,c}(x), g_n^{a,c}(x), h_n^{a,c}(x)$, and $k_n^{a,c}(x)$ are irreducible.*

It is important to note that this lemma is not an if and only if statement. That is, there exists irreducible polynomials of the form of $f_n^{a,c}, g_n^{a,c}, h_n^{a,c}$, and $k_n^{a,c}$ such that for every prime $p|c$, $\gcd(n, v_p(c)) > 1$. One such example is the irreducible polynomial $f_6^{4,27}(x) = x^6 + 27x + 27$.

In the case that $\gcd(v_p(c), n) > 1$ for all primes $p|c$, we cannot use Corollary A.13 since the line segment in question will contain integer lattice points. However, Theorem A.12 and the Newton polygon can give us some information and shed light on possible factors of these polynomials and help determine reducibility. We demonstrate this in the following example.

Example 3.6. Let p be a prime and consider the polynomial $f_6^{4,p^4}(x) = x^6 + p^4x + p^4$. We then have $\gcd(n, v_p(c)) = \gcd(6, 4) = 2$ and the Newton polygon is the line segment joining the points $(0, 4)$ and $(6, 0)$ which contains the integer lattice point $(3, 2)$. This tells us that if this polynomial factors, it factors as two cubic polynomials where p^2 divides the constant coefficient and the coefficient of x and p divides the coefficient of x^2 in each one. That is,

$$f_6^{4,p^4}(x) = \left(x^3 + Apx^2 + Bp^2x + Cp^2\right)\left(x^3 + A'px^2 + B'p^2x + C'p^2\right). \tag{3.6}$$

Comparing the constant coefficient on both sides of (3.6), we see that $C = C' = 1$. We then have

$$f_6^{4,p^4}(x) = \left(x^3 + Apx^2 + Bp^2x + p^2\right)\left(x^3 + A'px^2 + B'p^2x + p^2\right). \tag{3.7}$$

Comparing the coefficient of x^5 on both sides of (3.7), we see that $A'p + Ap = 0$ or $A' = -A$. We then have

$$f_6^{4,p^4}(x) = \left(x^3 + Apx^2 + Bp^2x + p^2\right)\left(x^3 - Apx^2 + B'p^2x + p^2\right). \tag{3.8}$$

Comparing the coefficient of x^4 on both sides of (3.8), we see that $B'p^2 + Bp^2 - A^2p^2 = 0$ or $B' + B - A^2 = 0$. Comparing the coefficient of x^3 on both sides of (3.8), we see that $2p^2 + AB'p^3 - ABp^3 = 0$ or $-Ap(B' - B) = 2$. This last equation indicates to us that if our system of equations has a solution (i.e., $f_6^{4,p^4}(x)$ is possibly reducible), the only option is p must be equal to 2. We substitute $p = 2$ and see that indeed:

$$f_6^{4,16}(x) = x^6 + 16x + 16 = (x^3 - 2x^2 + 4)(x^3 + 2x^2 + 4x + 4).$$

This example allows us to state the following lemma:

Lemma 3.7. *Let p be a prime and $f_6^{4,p^4}(x) = x^6 + p^4x + p^4$. Then f_6^{4,p^4} is irreducible for all odd primes p and reducible for the prime $p = 2$.*

To illustrate that this type of argument will not work in the most general case, consider the polynomial $f_{14}^{12,3^7}(x) = x^{14} + 2187x + 2187$ which is reducible and factors as a product of an irreducible quadratic and an irreducible polynomial of degree 12.

We will now consider another example illustrating the use of Newton polygons to help determine the irreducibility of $f_6^{4,q^3\cdot p^4}(x)$.

Example 3.8. Let p and q be distinct primes and consider the polynomial $f_6^{4,q^3\cdot p^4}(x) = x^6 + q^3p^4x + q^3p^4$. If we consider the Newton Polygon for this polynomial with respect to q we see that it is comprised of the line segment joining the points $(0,3)$ and $(6,0)$. This line segment contains the integer lattice points $(2,2)$ and $(4,1)$ which indicates that if this polynomial does factor, it will do so as a product of an irreducible quadratic and an irreducible quartic or as the product of three irreducible quadratics. If we consider the Newton Polygon for this polynomial with respect to p we see that is comprised of the line segment joining the points $(0,4)$ and $(6,0)$. This line segment contains the integer lattice point $(3,2)$ which indicates that if this polynomial does factor, it will do so as a product of two irreducible cubics. Since there is no way to reconcile these possible factorizations, we conclude that this polynomial must be irreducible.

The argument presented in this example was actually independent of the parameter a and allows us to state the following lemma.

Lemma 3.9. *For distinct primes p and q and integer $0 \leq a \leq 5$ the polynomial $f_6^{a,q^3\cdot p^4}(x) = x^6 + q^3p^4x^{n-a-1} + \ldots + q^3p^4x + q^3p^4$ is irreducible.*

We now generalize the previous example for a special form of the integer c.

Example 3.10. Consider the polynomial $f_{30}^{a,c}(x)$ where $c = p_1^6 \cdot p_2^{10} \cdot p_3^{15}$ for distinct primes p_1, p_2, and p_3. We have $n = 30 = 2 \cdot 3 \cdot 5$ and $\gcd(6,10,15) = \gcd(2,15) = 1$. If we consider the Newton polygon of p_1, p_2, and p_3 respectively we see that if $f_{30}^{a,c}$ was to be reducible:

(i) $f_{30}^{a,c}$ must factor as a product of at most 6 irreducible factors and the degree of each factor needs to be a multiple of 5,

(ii) $f_{30}^{a,c}$ must factor as a product of at most 10 irreducible factors and the degree of each factor needs to be a multiple of 3,

(iii) $f_{30}^{a,c}$ must factor as a product of at most 15 irreducible factors and the degree of each factor needs to be a multiple of 2.

It is not possible to reconcile the conditions $(i) - (iii)$ simultaneously and $f_{30}^{a,c}(x)$ must be irreducible. However, considering any two of the prime powers comprising c, we cannot conclude that the polynomial must be irreducible.

We conclude this section by formalizing the argument presented in the previous example.

Theorem 3.11. *Let n and a be positive integers such that $0 \leq a \leq n-1$ and let $c = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ for distinct primes $p_1, p_2, \ldots, p_r$, $\gcd(\alpha_1, \alpha_2, \ldots, \alpha_r) = 1$. Then $f_n^{a,c}(x) = x^n + cx^{n-a-1} + \ldots + cx + c$ is irreducible.*

Proof. If there exists a prime $p|c$ such that $\gcd(n, v_p(c)) = 1$, then $f_n^{a,c}(x)$ is irreducible by Lemma 3.5. Suppose $\gcd(n, v_{p_i}(c)) > 1$ for $i = 1, 2, \ldots, r$. If we consider the Newton polygon for a fixed p_i it consists of the line segment joining the point $(0, \alpha_i)$ to the point $(n, 0)$. This line segment contains $\gcd(n, \alpha_i) = a_i$-many integer lattice points. This tells us that if $f_n^{a,c}(x)$ is reducible, it will factor as a product of up to a_i-many irreducible factors each with degree that is a multiple of n/a_i. To reconcile these factorizations for every p_i simultaneously, we would at least need to have a factor that divides each α_i. Since $\gcd(\alpha_1, \alpha_2, \ldots, \alpha_r) = 1$, there is no way to reconcile these factorizations for each p_i and therefore we conclude that $f_n^{a,c}(x)$ is irreducible, as required. □

We note that Theorem 3.11 also holds for the polynomials $g_n^{a,c}(x)$, $h_n^{a,c}(x)$, and $k_n^{a,c}(x)$ under the same conditions; the proof is identical to the one above.

3.3 Roots

While initially studying and plotting the roots of $f_n^{a,c}(x)$, we noticed that the roots appear to be sitting on what at first sight appear to be two concentric circles around the origin: A first "(inner) circle" that looks to be the unit circle and a second (outer) "larger circle". We demonstrate this behaviour with an example:

Example 3.12. Consider $f_{25}^{7,12}(x) = x^{25} + 12 \cdot \sum_{n=0}^{17} x^n$. The following diagram is an illustration of the roots of $f_{25}^{7,12}(x)$ in the plane:

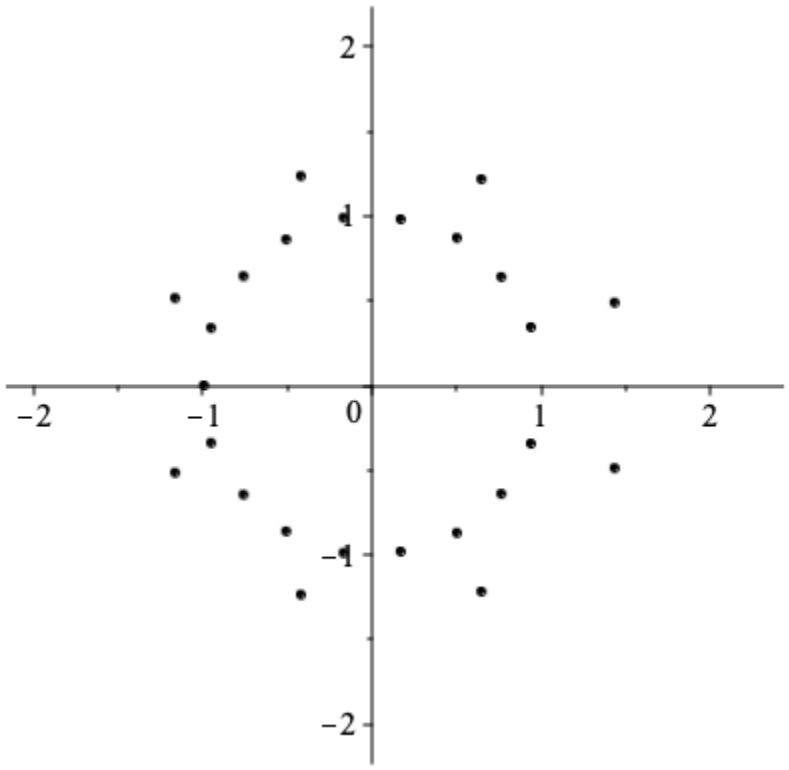


Figure 3.1: Roots of $f_{25}^{7,12}(x)$

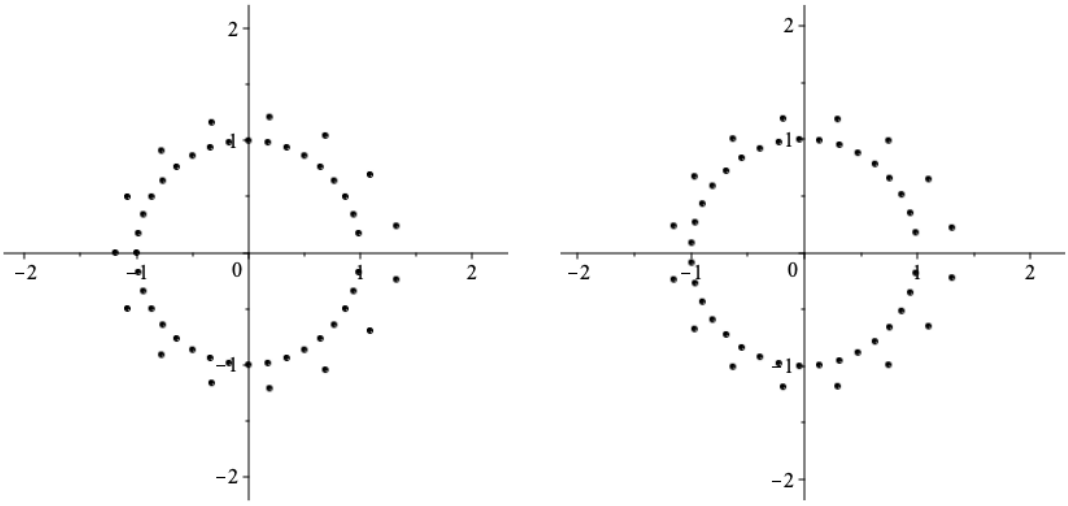
Varying one parameter while keeping the other two parameters fixed affects the roots in the following manner:

- Fixing the parameters a and c while increasing n fills more roots on the the inner "circle".
- Fixing the parameters n and c while increasing a fills more roots on the outer "circle".
- Fixing the parameters n and a while increasing c increases the diameter of the outer "circle".

As we will see, the inner "circle" and the outer "circle" are not actually circles, as is easy to verify numerically, but will converge to circles for large values of the parameter n. The roots of $f_n^{a,c}(x)$ are converging to these two regions, and because the set $|x| \leq R$ is a compact set for a real number R, we are facing a question of convergence of polynomial roots on a compact set. The following theorem of Hurwitz gives the conditions for convergence in this case; see, e.g. , [40, pg. 4].

Theorem 3.13 (Hurwitz)**.** *Let $f_n(z)$ $(n = 1, 2, \ldots)$ be a sequence of functions which are analytic in a region D and which converge uniformly to a function $f(z) \not\equiv 0$ in every closed subregion of D. Let ζ be an interior point of D. If ζ is a limit point of the zeros of the $f_n(z)$, then ζ is a zero of $f(z)$. Conversely, if ζ is an m-fold zero of $f(z)$, every sufficiently small neighbourhood K of ζ contains exactly m zeros (counted with their multiplicities) of each $f_n(z)$, $n \geq N(K)$.*

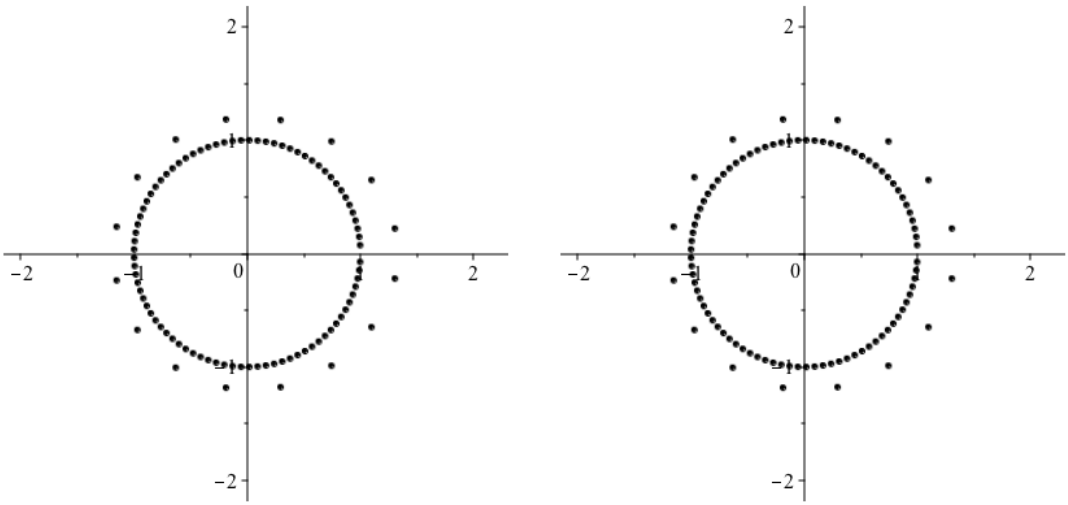
Thus, if we can find a function $Q(x)$ such that the roots of $f_n^{a,c}(x)$ are converging to the roots of $Q(x)$ uniformly on a compact subset, we can exactly describe the limiting curve of the roots of $f_n^{a,c}(x)$. Through computational experimentation we find the visual comparison below.



(a) Roots of $(x^{15} - x^{14} + 25)(\sum_{j=0}^{35} x^j)$ (b) Roots of $f_{50}^{15,25}(x)$

Figure 3.2: Comparison of Roots of Degree 50

If the parameter n (degree) is increased, that is, if we add more roots to the polynomials $f_n^{a,c}(x)$ and compare them to one another, we observe that the comparison strengthens.



(a) $(x^{15} - x^{14} + 25)(\sum_{j=0}^{85} x^j)$ (b) $f_{100}^{15,25}(x)$

Figure 3.3: Comparison of Roots of Degree 100

We now turn to the discussion of the roots of the polynomial $Q_n^{a,c}(x) = (x^{a+1} - x^a + c)(\sum_{j=0}^{n-a-1} x^j)$.

Lemma 3.14. *The roots of the polynomial* $Q_n^{a,c}(x) = (x^{a+1} - x^a + c)(\sum_{j=0}^{n-a-1} x^j)$ *can be described as* $(n-a-1)$ *equally spaced roots of unity as well as* $(a+1)$ *points inside the disk* $|x| = R$ *for* $R > 1$ *depending on* c.

Proof. We address the two factors of $Q_n^{a,c}(x)$ separately. The roots of $\sum_{j=0}^{n-a-1} x^j$ are the $(n-a-1)$ equally spaced $(n-a)th$ roots of unity. For the roots of the trinomial $x^{a+1} - x^a + c$, we will use the following three results regarding polynomials with real coefficients found in [40], pg. 123, 126, 165, respectively:

Theorem 3.15 (Cauchy)**.** *All the roots of* $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$, $a_n \neq 0$, *lie in the disk*

$$|z| < 1 + \max \frac{|a_k|}{|a_n|}, \quad k = 0, 1, 2, \ldots, n-1.$$

Theorem 3.16 (Birkhoff, Cohn, and Berwald)**.** *The root of smallest modulus of* $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$, $a_0 \neq 0$, *lies in the ring* $R \leq |z| \leq \frac{R}{2^{\frac{1}{n}} - 1}$,

where R is the positive root of of the equation

$$|a_0| - |a_1|z - |a_2|z^2 - \ldots - |a_n|z^n = 0.$$

Theorem 3.17 (Nekrasoff, Kempner, Herglotz, and Biernacki)**.** *The trinomial $\alpha z^n + z^p + 1$ for $\alpha \in \mathbb{R}$, $n, p \in \mathbb{N}$ with $0 < p < n$, has at least one root in each of the sectors*

$$\left|\mathrm{Arg}\,(z) - \frac{(2k+1)p}{\pi}\right| \leq \frac{\pi}{n}, \quad k = 0, 1, \ldots, p-1.$$

We apply Theorem 3.15 to conclude that the roots of $x^{a+1} - x^a + c$ lie inside the circle $|x| < 1 + |c|$. We then apply Theorem 3.16 to conclude that all of the roots of $x^{a+1} - x^a + c$ satisfy $|x| > 1$. Lastly, to apply Theorem 3.17, we note the following transformation:

$$\begin{aligned} q(z) &= bz^{a+1} + z^a + 1, \\ q\left(-\frac{z}{b}\right) &= b\left(-\frac{z}{b}\right)^{a+1} + \left(-\frac{z}{b}\right)^a + 1, \\ &= (-1)^{a+1}\frac{1}{b^a}(z^{a+1} - z^a) + 1. \end{aligned}$$

This implies that

$$-(-b)^a q\left(-\frac{z}{b}\right) = z^{a+1} - z^a - (-b)^a.$$

If we set $c = |-(-b)^a|$ (replacing b with $-b$ if necessary) we can now apply Theorem 3.17 to the trinomial $x^{a+1} - x^a + c$.

Putting it all together, we have shown that the roots of $Q_n^{a,c}$ are made up of $(n - a - 1)$ roots of unity and an additional $(a + 1)$ roots that lie in the disk $1 < |x| < 1 + c$ and have angular distribution as described in Theorem 3.17. We have now demonstrated all of the required properties and have proven Lemma 3.14. □

We are now in a position to apply Theorem 3.13 to $f_n^{a,c}(x)$.

Theorem 3.18. *For fixed natural numbers a, n, c with $0 < a < n$, the roots of the*

polynomial $f_n^{a,c}(x) = x^n + cx^{n-a-1} + cx^{n-a-2} + cx^{n-a-3} + \cdots + cx + c$ *converge to the roots of the polynomial* $(x^{a+1} - x^a + c)$ *and to the unit circle as* $n \to \infty$.

Proof. We begin by noting the identity

$$\begin{aligned} f_n^{a,c}(x) &= x^n + cx^{n-a-1} + cx^{n-a-2} + \cdots + cx + c \\ &= (x^{a+1} - x^a + c)\left(\sum_{j=0}^{n-a-1} x^j\right) + x^a. \end{aligned} \tag{3.9}$$

We set $N = n - a - 1$ and note that as $n \to \infty$, $N \to \infty$. We re-write (3.9) as

$$f_n^{a,c}(x) = (x^{a+1} - x^a + c)\left(\sum_{j=0}^{N} x^j\right) + x^a \tag{3.10}$$

and we consider the following two cases based on $|x|$. Let $\epsilon > 0$ be arbitrary.

(i) Case 1: $|x| \leq 1 - \epsilon$. As $N \to \infty$, the geometric series $\sum_{j=0}^{N} x^j$, converges to $\frac{1}{1-x}$ and the difference between the two sides of (3.10) is equal to x^n which converges uniformly to zero as $n \to \infty$ for $|x| \leq 1 - \epsilon$.

(ii) Case 2: $|x| \geq 1 + \epsilon$. We replace x with $\frac{1}{x}$ and proceed as in the previous case. This time, as $N \to \infty$, the difference between the two sides of (3.10) is equal to $\left(\frac{1}{x}\right)^n$ which converges uniformly to zero as $n \to \infty$ for $|x| \geq 1 + \epsilon$.

Since ϵ is arbitrary and can be made as small as we like, we see that as $n \to \infty$, $f_n^{a,c}(x)$ converges to the function $(x^{a+1} - x^a + c)(\sum_{j=0}^{N} x^j)$ where N is an arbitrarily large positive integer. Then the conditions of Theorem 3.13 are met and we can apply this theorem to conclude our desired result, Theorem 3.18. □

Although we used $f_n^{a,c}(x)$ explicitly in the statement and proof of Theorem 3.18, the result also applies to $g_n^{a,c}(x), k_n^{a,c}(x)$, and $h_n^{a,c}(x)$. To see this, note the following relationships between our polynomials:

$$\begin{aligned} h_n^{a,c}(x) &= (x^{a+1} - x^a - c)\left(\sum_{j=0}^{n-a-1} x^j\right) + x^a, \\ g_n^{a,c}(x) &= f_n^{a,c}(x), \\ k_n^{a,c}(x) &= h_n^{a,c}(-x). \end{aligned}$$

3.4 Discriminants

In this section we will introduce the very basics of the concept of the discriminant of a polynomial, just enough for our use. For a detailed and thorough treatment of the topic, the reader is referred to [49, ppg. 23–28].

Let f and g be two polynomials with real coefficients, given by

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \quad b_m \neq 0.$$

The resultant of $f(x)$ and $g(x)$ is defined by the determinant of a certain $(m+n) \times (m+n)$ matrix which has the coefficients of $f(x)$ and $g(x)$ or 0 as entries; we denote it by $\rho(f, g)$. The resultant was discussed in further detail earlier in this thesis in Subsection 2.11. The discriminant of a polynomial $f(x)$ is then defined as

$$D(f) = \frac{(-1)^{\frac{n(n+1)}{2}}}{a_n}\rho(f, f'),$$

where f' denotes the derivative of $f(x)$.

The discriminant of a polynomial is a polynomial function of the coefficients a_i, which provides some insight into the roots of the polynomials without requiring their computation. The canonical example is the quadratic polynomial $ax^2 + bx + c \in \mathbb{R}[x]$ which has discriminant $b^2 - 4ac$. If $b^2 - 4ac < 0$ then the quadratic has no real roots, if $b^2 - 4ac > 0$ then the quadratic has two distinct real roots, and if $b^2 - 4ac = 0$ then the quadratic has a single real root with multiplicity two. In general, a polynomial with real coefficients has a multiple root if and only if the discriminant is zero. If the roots of the polynomial are known, the discriminant can be calculated in terms of the roots as well.

Lemma 3.19. *The discriminants of $f_n^{a,c}(x), g_n^{a,c}(x), h_n^{a,c}(x)$, and $k_n^{a,c}(x)$ are congruent to zero modulo c for $n \geq 2$.*

Proof. Since the discriminant is a polynomial function in the coefficients of our polynomials and reduction modulo c is a ring homomorphism on $\mathbb{Z}$, we have

$$\begin{aligned} D(f_n^{a,c}(x)) \equiv D(g_n^{a,c}(x)) \equiv D(h_n^{a,c}(x)) \equiv D(k_n^{a,c}(x)) \pmod{c}, \\ \equiv D(x^n) \pmod{c}, \\ = 0 \quad \text{for} \quad n \geq 2, \end{aligned}$$

as required. □

When calculating the discriminants of $f_n^{a,c}(x), g_n^{a,c}(x), h_n^{a,c}(x)$, and $k_n^{a,c}(x)$, we notice that not only are they congruent to 0 modulo c, but that a higher power of c divides the discriminant. We demonstrate this with an example using $f_n^{a,c}(x)$.

Example 3.20.

$$\begin{aligned} D(f_3^{1,c}(x)) &= -3c^4 + 14c^3 - 27c^2, \\ D(f_4^{1,c}(x)) &= -12c^5 - 11c^4 + 256c^3, \\ D(f_5^{1,c}(x)) &= 64c^7 - 48c^6 - 84c^5 + 3125c^4, \\ D(f_3^{2,c}(x)) &= -27c^2, \\ D(f_4^{2,c}(x)) &= -27c^4 + 256c^3, \\ D(f_5^{2,c}(x)) &= 81c^6 + 906c^5 + 3125c^4. \end{aligned}$$

This leads us to the following stronger result:

Theorem 3.21. *For $f_n^{a,c}(x), g_n^{a,c}(x), h_n^{a,c}(x)$, and $k_n^{a,c}(x)$, we have*

$$D(f_n^{a,c}(x)) \equiv D(g_n^{a,c}(x)) \equiv D(h_n^{a,c}(x)) \equiv D(k_n^{a,c}(x)) \equiv 0 \pmod{c^{n-1}},$$

for all $n \geq 2$ and all values of a and c.

Proof. To prove Theorem 3.21, we will make use of the following result regarding discriminants of polynomials, which can be found in [32], for example.

Theorem 3.22 (Theorem 1.4 [32])**.** *(i) The discriminant of a polynomial f is homogenous of degree $(2n-2)$ in the coefficients $a_0, a_1, \ldots, a_n$.*

(ii) If a_i is regarded as having degree i in the discriminant, then the discriminant of f is homogenous of degree $n(n-1)$.

Since the coefficients of $f_n^{a,c}(x), g_n^{a,c}(x), h_n^{a,c}(x)$, and $k_n^{a,c}(x)$ all share the structure: $a_n = 1$ and $a_i = c$ for $i = 0, 1, 2, \ldots, (n-a-1)$, parts (i) and (ii) combine to allow us to conclude that the discriminants of $f_n^{a,c}(x), g_n^{a,c}(x), h_n^{a,c}(x)$, and $k_n^{a,c}(x)$ are homogenous in the term $1^n \cdot c^{n-1} = c^{n-1}$ as required. □

Remark: The author was made aware of a more direct approach to proving Theorem 3.21. One of the examiners notes that Theorem 3.21 follows directly by looking at the Sylvester matrix associated with the polynomials; they will have $n-1$ columns on the right where each element of the column is divisible by c and so the determinant is divisible by c^{n-1}.

3.5 Results About Related Trinomials and Quadrinomials

Although not applicable to the trinomials studied by Harrington in [28] or the quadrinomials mentioned in this chapter, we came across similar and interesting results in the literature for certain special cases of these polynomials.

The authors of [19] study the following three types of polynomials:

Definition 3.23. *A polynomial $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ with $a_k \in \{0, 1\}$ for all $1 \leq k \leq n-1$ and $a_0 = 1$ is called a Newman polynomial.*

Definition 3.24. *A polynomial $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ with $a_k \in \{-1, 1\}$ for all k is called a Littlewood polynomial.*

Definition 3.25. *A polynomial $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ with $a_k \in \{-1, 0, 1\}$ for all k and $a_0 \neq 0$ is called a Borwein polynomial.*

In [22], the author considers many interesting results on the geometry of the roots of trinomials. For results on the irreducibility of trinomials and quadrinomials with coefficients restricted to some subset of the set $\{-p, -1, 0, 1, p\}$ where p is an odd prime, the reader is referred to [23], [39], [45], and [46].

The books [5], [11], [40], and [49] contain many useful and interesting results on the reducibility and roots of polynomials in general.

Chapter 4

Binomial Congruences and Honda's Congruences

4.1 Background

Wilson's theorem and its converse due to Lagrange combine to give a criterion for identifying the prime numbers:

Theorem 4.1 (Wilson and Lagrange)**.** *A positive integer $p > 1$ is a prime if and only if $(p-1)! \equiv -1 \pmod{p}$.*

A famous binomial coefficient congruence, due to J. Wolstenholme, states

Theorem 4.2 (Wolstenholme)**.** *For any prime, $p \geq 5$,*

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

Unlike Wilson's theorem, a converse to Wolstenholme's theorem has not been established. But Theorem 4.2 has no composite solutions, $n < 10^9$, such that $\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}$. It has been conjectured that no composite solutions exist and that Wolstenholme's theorem, like Wilson's theorem, also gives a criterion for identifying the prime numbers. For a more detailed and complete presentation of Theorem 4.2, the reader is referred to [31] or [43].

Theorem 4.2 may be rewritten as

Theorem 4.3. *For any prime, $p \geq 5$,*

$$\binom{2p}{p} \equiv 2 \pmod{p^3}.$$

Wolstenholme's theorem was generalized by W. Ljunggren [26] to

Theorem 4.4 (Ljunggren)**.** *For any prime, $p \geq 5$, and nonnegative integers n, m we have*

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3}.$$

In two of their joint papers [13] and [14], M. Chamberland and K. Dilcher studied a class of binomial sums,

$$u^{\epsilon}_{a,b}(n) := \sum_{k=0}^{n} (-1)^{\epsilon k} \binom{n}{k}^a \binom{2n}{k}^b, \tag{4.1}$$

and their divisibility properties. In particular, when $a = b = \epsilon = 1$, they proved the following analogue of Ljunggren's theorem.

Theorem 4.5 ([14], Theorem 2.1)**.** *For all primes $p \geq 5$ and integers $m \geq 1$ we have*

$$u(mp) \equiv u(m) \pmod{p^3},$$

where $u(n) := u^1_{1,1}(n)$.

4.2 Parameter Introduced

In a paper by D.F. Bailey [4] the following parameterized version of Ljunggren's theorem is presented.

Theorem 4.6 (Bailey)**.** *For any prime $p \geq 5$ and nonnegative integers m, n, s we have*

$$\binom{mp^{s+1}}{np^{s+1}} \equiv \binom{mp^s}{np^s} \pmod{p^{s+3}}.$$

Of particular interest to us is an identity that appears on page 124 of [4] during the proof of Theorem 4.6:

Lemma 4.7 (Bailey)**.** *For any prime $p \geq 5$ and nonnegative integers m, n, s we have*

$$\binom{mp^{s+1}}{lp} \equiv \binom{mp^s}{l} \pmod{p^{s+3}}. \tag{4.2}$$

Following in the footsteps of Chamberland and Dilcher [14], we present the following new result.

Theorem 4.8. *For any prime $p \geq 5$ and nonnegative integers m, s we have*

$$u(mp^{s+1}) \equiv u(mp^s) \pmod{p^{s+3}}.$$

To prove this result we first note that the case $s = 0$ is the case proved in [14]; we will therefore assume that $s \geq 1$. We express the sum (4.1) for $a = b = \epsilon = 1$ as

$$\begin{aligned} u(mp^{s+1}) &:= \sum_{k=0}^{mp^{s+1}} (-1)^k \binom{mp^{s+1}}{k} \binom{2mp^{s+1}}{k} \\ &= \sum_{k=0}^{mp^s-1} \sum_{j=1}^{p-1} (-1)^{pk+j} \binom{mp^{s+1}}{pk+j} \binom{2mp^{s+1}}{pk+j} \\ &\qquad + \sum_{k=0}^{mp^s} (-1)^{pk} \binom{mp^{s+1}}{pk} \binom{2mp^{s+1}}{pk}. \end{aligned} \tag{4.3}$$

The proof is made up of two parts: first we show that the double sum is congruent to 0 modulo p^{s+3}, and then we use the fact that p is odd and apply Lemma 4.7 term by term to second sum of (4.3).

Lemma 4.9. *Let $m, s,$ and j be positive integers with $1 \leq j \leq p-1$. Then the power of the odd prime p dividing $\binom{mp^{s+1}}{pk+j}$ and $\binom{2mp^{s+1}}{pk+j}$ is at least $v_p(mp^{s+1})$.*

Proof. We will consider the first binomial coefficient and note that the case of the second follows in an analogous manner, since $v_p(mp^{s+1}) = v_p(2mp^{s+1})$. We have

$$\begin{aligned} \binom{mp^{s+1}}{pk+j} &= \frac{(mp^{s+1})!}{(pk+j)!(mp^{s+1}-pk-j)!} \\ &= \frac{(mp^{s+1}) \cdots (mp^{s+1}-pk-j+1)}{(pk+j) \cdots (2)(1)}. \end{aligned} \tag{4.4}$$

To ensure that the p-adic valuation of the binomial coefficient is indeed at least the p-adic valuation of mp^{s+1}, we need to show that the p-adic valuation of the denominator of (4.4) is less than or equal to the p-adic valuation of $(mp^{s+1}-1)!$. After some simplification, we need to show that, for fixed $p, k,$ and j as in the statement of

Lemma 4.9, we have:

$$v_p\left(\prod_{i=1}^{pk+j} i\right) \leq v_p\left(\prod_{i=mp^{s+1}-pk-j+1}^{mp^{s+1}-1} i\right). \tag{4.5}$$

The product on the left-hand side of the inequality (4.5) contains $(pk+j)$ consecutive terms with an initial term equal to 1 while the product on the right-hand side of the inequality (4.5) contains $(pk+j-1)$ consecutive terms with an initial term greater than 1. Since p is an odd prime, we know that the first two terms of the product on the left-hand side satisfy $v_p(i) = 0$, and therefore our inequality holds, as required. □

Proof of Theorem 4.8. Applying Lemma 4.9, we see that the double sum

$$\sum_{k=0}^{mp^s-1} \sum_{j=1}^{p-1} (-1)^{pk+j} \binom{mp^{s+1}}{pk+j} \binom{2mp^{s+1}}{pk+j}$$

is divisible by

$$v_p(mp^{s+1}) + v_p(2mp^{s+1}) = 2 \cdot (v_p(mp^{s+1})) \geq 2s+2 \geq s+3,$$

when $s \geq 1$. We have therefore proven the desired result. □

4.3 Extended Search Space and an Observation

In [14], the authors were interested in finding counterexamples to their analogue of the converse of Wolstenholme's Theorem 4.2. Namely, they were looking for composite solutions to the congruence

$$u(n) \equiv -1 \pmod{n^3}. \tag{4.6}$$

They found that the composite integers satisfying (4.6) all have exactly two prime factors, one of which is 2 or 5. Also in [14], the authors completely characterize the primes p such that $2p$ is a solution to (4.6). The paper [14] ends with some open problems, two of which are:

(i) Do any solutions of (4.6) have three or more prime factors? In [14], there were none found for $n \leq 4 \cdot 10^6$.

(ii) Can the primes p such that $5p$ satisfies (4.6) be completely characterized?

While we do not have definitive answers to either of these two questions, we can say something about both of these open problems.

Using Maple, we were able to verify the conjecture in [14] that no solution of (4.6) has three or more prime factors up to the new search limit of $n \leq 8 \cdot 10^6$.

The characterization of the primes p such that $2p$ satisfies (4.6) has to do with their binary expansion. Naturally, the authors of [14] considered the 5-ary expansion of the primes such that $5p$ satisfied (4.6) but no such characterization was found.

4.4 Honda's Congruences

A congruence is referred to as a supercongruence if the congruence also holds modulo a higher modulus than one would expect. The term first appeared in the work of F. Beukers in 1985 [9] and was the title of M. Coster's 1988 Ph.D. thesis [16].

Supercongruences in the literature have been motivated by a range of different areas in mathematics, including Apéry numbers, Bernoulli numbers/polynomials, binomial coefficients, Euler numbers/polynomials, Legendre polynomials, and certain infinite series of special interest.

In their paper [53], A. Robert and M. Zuber introduced a new proof for two known supercongruences involving binomial coefficients:

Theorem 4.10 (Kazandzidis)**.** *Let p be an odd prime and n, k, nonnegative integers. Then*

$$\binom{np}{kp} \equiv \binom{n}{k} \pmod{p^3 \cdot n \cdot k \cdot (n-k) \cdot \binom{n}{k} \mathbb{Z}_p} \quad p \geq 5, \tag{4.7}$$

$$\binom{3n}{3k} \equiv \binom{n}{k} \pmod{3^2 \cdot n \cdot k \cdot (n-k) \cdot \binom{n}{k} \mathbb{Z}_3} \quad p = 3. \tag{4.8}$$

The notation $A \equiv B \pmod{C\mathbb{Z}_p}$ is taken to mean that $(A - B) \in C\mathbb{Z}_p$ and $\mathbb{Z}_p$ denotes the p-adic integers. Robert and Zuber apply these two supercongruences to obtain a new supercongruence for the Legendre polynomials.

The new proof of Kazandzidis' congruences presented by Robert and Zuber uses the p-adic logarithm of the p-adic gamma function Γ_p. By considering the series expansion of $\log \Gamma_p(x)$ and bounding the absolute value of the coefficients, the authors obtain the desired result.

The Legendre polynomial $P_n(x)$ satisfies the explicit formula

$$P_n(1+2t) = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} t^k, \tag{4.9}$$

and satisfy the following congruences of Honda [29]:

$$P_{np-1}(1+2t) \equiv P_{n-1}(1+2t^p) \pmod{np\mathbb{Z}_p[t]} \quad n \geq 1, \tag{4.10}$$

$$P_{np}(1+2t) \equiv P_n(1+2t^p) \pmod{np\mathbb{Z}_p[t]} \quad n \geq 0. \tag{4.11}$$

Here, in analogy to before, the notation $A \equiv B \pmod{C\mathbb{Z}_p[t]}$ for polynomials $A, B \in \mathbb{Z}_p[t]$ is taken to mean that $(A - B) \in C\mathbb{Z}_p[t]$. If we define

$$Q_n(t) := P_n(1+2t) + P_{n-1}(1+2t),\ n \geq 1, \tag{4.12}$$

then as a direct corollary of Honda's congruences (4.10), (4.11) we have

$$Q_{np}(t) \equiv Q_n(t^p) \pmod{np\mathbb{Z}_p[t]}.$$

As a corollary of the Kazandzidis congruences (4.7), (4.8), Robert and Zuber present the following polynomial supercongruence:

Theorem 4.11 (Robert and Zuber)**.** *For p odd and for all integers $n \geq 1$ we have*

$$Q_{np}(t) \equiv Q_n(t^p) \pmod{n^2p^2\mathbb{Z}_p[t]}.$$

This raises the question regarding the necessity of $\mathbb{Z}_p$ and $\mathbb{Z}_p[t]$. That is, given that all of the elements involved are integers or have integer coefficients, do these same congruences hold over $\mathbb{Z}$ or $\mathbb{Z}[t]$? If not, do similar ones hold? Why or why not? This led us to some experimentation using the computer algebra system Maple, and we are able to discuss the following.

With regards to the supercongruences of Kazandzidis (4.7),(4.8), we did not consider them as congruences over the integers for two main reasons. If $n \leq k$, Theorem 4.10 is trivially true. Moreover, the explicit use of the congruences (4.7),(4.8) was not necessary in this approach over the integers without the machinery of the p-adic integers.

In analogy to the congruences of Honda (4.10),(4.11), we have the following theorem over the integers, that is, we are considering the congruence of the coefficients for the polynomials:

Theorem 4.12. *With the prime $p \geq 5$ fixed and $P_n(1+2t)$ defined as in (4.9), we have*

$$P_{np-1}(1+2t) \equiv P_{n-1}(1+2t^p) \pmod{np}, \tag{4.13}$$

$$P_{np}(1+2t) \equiv P_n(1+2t^p) \pmod{np}, \tag{4.14}$$

where $n = 1, 2, p, 2p, p^2, 2p^2, \ldots$.

To prove Theorem 4.12 we will require the following theorem of Kummer [34] and the associated corollary.

Theorem 4.13 (Kummer)**.** *Given integers m and n such that $n \geq m \geq 0$ and a prime number p, $v_p\left(\binom{n}{m}\right)$ is equal to the number of carries when m is added to $n-m$ in base p.*

This leads to the following corollary:

Corollary 4.14. *For positive integers n and k such that $1 \leq k \leq n$, we have*

$$\binom{n}{k}\binom{n+k}{k} \equiv 0 \pmod{2}.$$

Proof. If we consider the rightmost digit 1 of k in base 2 then either n or $n-k$ has a 1 in this position. We note that there will be at least one carry in either $(n-k)+k$ or $n+k$ and thus $2|\binom{n}{n+k}\binom{n+k}{k}$ as required. □

We now return to the proof of Theorem 4.12.

Proof of Theorem 4.12. We will prove the first part (4.13) of the theorem and note that the second part (4.14) is proved in an analogous manner. To prove (4.13), we will look at two separate cases, namely when $n = 2p^m$ and when $n = p^m$.

Using the explicit evaluation for the Legendre polynomials (4.9), we see that it suffices to show

$$\binom{np-1}{k}\binom{np-1+k}{k} \equiv 0 \pmod{np} \tag{4.15}$$

when $k \neq 0, p, 2p, \ldots, (n-1)p$, and

$$\binom{np-1}{kp}\binom{np-1+kp}{kp} \equiv \binom{n-1}{k}\binom{n-1+k}{k} \pmod{np} \tag{4.16}$$

when $k = 0, 1, 2, 3, \ldots, n-1$.

We first consider the congruence (4.15). We have:

$$\begin{aligned}
&\binom{np-1}{k}\binom{np-1+k}{k} = \frac{(np-1)!}{k!(np-1-k)!}\frac{(np-1+k)!}{k!(np-1)!} \\
&= \frac{(np-1+k)!}{k!^2(np-1-k)!} \\
&= \frac{(np+k-1)(np+k-2)\cdots(np+1)}{(k-1)!} \cdot \frac{np}{k} \cdot \frac{(np-1)(np-2)(np-k)}{k!}.
\end{aligned} \tag{4.17}$$

Since both expressions on either side of the equality in (4.17) are integers, we have

$$v_p\left(\tfrac{(np-1+k)!}{k!^2(np-1-k)!}\right) \geq v_p\left(\frac{np}{k}\right) = v_p(np).$$

This establishes (4.15) modulo the highest power of p dividing np, and Corollary 4.14 establishes (4.15) modulo 2 which ends the proof of (4.15).

It now remains to prove the congruence (4.16). We begin by noting that for integers $0 \leq l \leq m$

$$\binom{m}{l} = \frac{m}{m-l}\binom{m-1}{l} \quad \text{and} \quad \binom{m+l}{l} = \frac{m+l}{m}\binom{m-1+l}{l}.$$

We then have

$$\binom{m-1}{l}\binom{m-1+l}{l} = \frac{m-l}{m+l}\binom{m}{l}\binom{m+l}{l}.$$

By taking $(m,l) = (np, kp)$ and $(m.l) = (n,k)$ respectively, (4.16) becomes

$$\frac{n-k}{n+k} \cdot \binom{np}{kp}\binom{np+kp}{kp} \equiv \frac{n-k}{n+k} \cdot \binom{n}{k}\binom{n+k}{k} \pmod{np}.$$

To complete the proof of (4.16), we will use the following theorem of Gessel [24]:

Theorem 4.15 ([24], Theorem 2.2)**.** *Let a and b be nonnegative integers divisible by a prime p. Then unless $p = 2$ and $b \equiv a - b \equiv 2 \pmod 4$,*

$$\binom{a}{b} \equiv \binom{a/p}{b/p} \pmod{p^{\alpha+\beta+\gamma+\delta-\mu}},$$

where $\alpha = v_p(a), \beta = v_p(b), \gamma = v_p(a-b), \delta = v_p\left(\binom{a/p}{b/p}\right)$, and μ is $2, 1$, or 0 depending on whether p is $2, 3$ or greater than 3 respectively.

By Theorem 4.15, we have

$$\binom{np}{kp} \equiv \binom{n}{k} \quad \text{and} \quad \binom{np+kp}{kp}\binom{n+k}{k} \pmod{p^e},$$

where we can take

$$e = v_p(np) + v_p(kp) + \min\{v_p((n+k)p), v_p((n-k)p)\}.$$

Therefore it would suffice to show $v_p(kp) + \min\{v_p((n+k)p), v_p((n-k)p)\} \geq v_p\left(\frac{n-k}{n+k}\right)$. For our conditions on n and k, we have $v_p(kp) > v_p((n-k))$ and so (4.16) has been proven for the highest power of p dividing np. We again use Corollary 4.14 to establish (4.16) modulo 2 which ends the proof of (4.16). This completes the proof

of Theorem 4.12. □

Remark: While the author did have a proof of Theorem 4.12, suggestions from an external examiner have made the above proof more concise.

In regards to the Legendre polynomial supercongruence, we recall the definition of the polynomials $Q_n(t)$ from (4.12):

$$Q_n(t) := P_n(1+2t) + P_{n-1}(1+2t),$$

for $n \geq 1$. By the Honda-type congruences (4.13) and (4.14), for $p \geq 5$ fixed, we have

$$Q_{np}(t) \equiv Q_n(t^p) \pmod{np},$$

where $n = 1, p, p^2, p^3, \ldots$. In fact, we will show that the following stronger result holds true.

Theorem 4.16. *With $p \geq 5$ fixed and $Q_n(t)$ defined as above, we have*

$$Q_{np}(t) \equiv Q_n(t^p) \pmod{n^2p^2}, \tag{4.18}$$

for $n = 1, p, p^2, p^3, \ldots$.

Proof. Using the explicit formula (4.9) for $P_n(1+2t)$, we have

$$\begin{aligned} Q_{np}(t) - Q_n(t^p) = &\sum_{k=0}^{np} \binom{np}{k}\binom{np+k}{k} t^k + \sum_{k=0}^{np-1} \binom{np-1}{k}\binom{np-1+k}{k} t^k \\ &- \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} t^{pk} - \sum_{k=0}^{n-1} \binom{n-1}{k}\binom{n-1+k}{k} t^{pk}. \end{aligned}$$

Set $Q_{np}(t) - Q_n(t^p) = \sum_{k=0}^{np} q_k t^k$. Then we have:

(a) $q_0 = 0$.

(b) If $k \geq 1$, $(k,p) = 1$, then

$$\begin{aligned} q_k &= \binom{np}{k}\binom{np+k}{k} + \binom{np-1}{k}\binom{np+k-1}{k} \\ &= \frac{np}{k}\binom{np-1}{k-1}\left(\binom{np+k-1}{k-1} + \binom{np+k-1}{k}\right) \\ &\quad + \left(\binom{np}{k} - \binom{np-a}{k-1}\right)\frac{np}{k}\binom{np+k-1}{k-1} \\ &= \frac{np}{k}\binom{np-1}{k-1}\binom{np+k}{k} + \frac{np}{k}\binom{np-1}{k}\binom{np+k-1}{k-1} \\ &= 2\frac{n^2p^2}{k^2}\binom{np-1}{k-1}\binom{np+k-1}{k-1} \\ &\equiv 0 \pmod{n^2p^2}, \end{aligned}$$

since $(k,p) = 1$ and $n = p^i$.

(c) If $k < n$, then

$$\begin{aligned} q_{pk} &= \binom{np}{kp}\binom{np+kp}{kp} - \binom{n}{k}\binom{n+k}{k} + \binom{np-1}{kp}\binom{np+kp-1}{kp} \\ &\quad - \binom{n-1}{k}\binom{n+k-1}{k} \\ &= \frac{2n}{n+k}\left(\binom{np}{kp}\binom{np+kp}{kp} - \binom{n}{k}\binom{n+k}{k}\right) \\ &= \frac{2p^{m-1}}{p^{m-1}+k}\left(\binom{p^m}{kp}\binom{p^m+kp}{kp} - \binom{p^{m-1}}{k}\binom{p^{m-1}+k}{k}\right). \end{aligned}$$

So we must show that

$$\binom{p^m}{kp}\binom{p^m+kp}{kp} \equiv \binom{p^{m-1}}{k}\binom{p^{m-1}+k}{k} \pmod{p^{m+1}}.$$

However, from our proof of (4.13) and (4.14), we know that this congruence is true modulo p^{2m}. So we have that $q_{pk} \equiv 0 \pmod{n^2p^2}$ as required.

(d) We lastly consider q_{np}, namely

$$\begin{aligned} q_{np} &= \binom{2np}{np} - \binom{2n}{n} \\ &= \binom{2p^m}{p^m} - \binom{2p^{m-1}}{p^{m-1}}. \end{aligned}$$

To prove that $q_{p^m} \equiv 0 \pmod{p^{2m}}$ as required, we will invoke the following theorem of Jacobsthal which can be found in [26].

Theorem 4.17 (Jacobsthal)**.** *For any integers $\nu > \mu > 0$ and prime $p \geq 5$,*

$$\frac{\binom{\nu p}{\mu p}}{\binom{\nu}{\mu}} \equiv 1 \pmod{p^q},$$

where q is the power of p dividing $p^3\nu\mu(\nu - \mu)$.

In our case, $\nu = 2p^{m-1}$, $\mu = p^{m-1}$, and $q = 3m$. This gives us the congruence $q_{np} \equiv 0 \pmod{p^{3m}}$ which is actually stronger than the congruence we required. This completes the proof of Theorem 4.16 □

We finish this section by clarifying that Theorem 4.12, and by extension Theorem 4.16, are not new results but rather new arguments for (4.10) and (4.11) considered over the integers.

4.5 Other Polynomials

Given that Legendre polynomials are special cases of Jacobi polynomials, our work in Section 2.4 leads to the question whether Honda-type congruences also hold for Jacobi polynomials in general. That is, are there congruences of the form

$$P_n^{(\alpha,\beta)}(1 + 2t^p) \equiv P_{np}^{(\alpha,\beta)}(1 + 2t) \pmod{np}?$$

Supported by computer experimentation, it appears that, with the exception of $\alpha = \beta = 0$ (the Legendre case) and $\alpha = \beta = -\frac{1}{2}$, no such congruences exist. There is an issue with the coefficients of the polynomials not being invertible modulo np.

The case $\alpha = \beta = -\frac{1}{2}$ is the case of the Chebyshev polynomials of the first kind. We will use the following explicit formula for the Chebyshev polynomials of the first kind which can be found in [52]:

$$T_n(x) = \frac{n}{2}\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor}(-1)^k \frac{(n-k-1)!}{k!(n-2k)!}(2x)^{n-2k}.$$

For a fixed prime p, we have the following congruence:

Theorem 4.18. *For any prime p, we have*

$$T_{np}(x) \equiv T_n(x^p) \pmod{np},$$

where $n = 2^i p^j$, $i, j \geq 0$.

Proof. We need to show that

$$\frac{np}{2}\sum_{k=0}^{\lfloor \frac{np}{2} \rfloor}(-1)^k \frac{(np-k-1)!}{k!(np-2k)!}(2x)^{np-2k} \equiv \frac{n}{2}\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor}(-1)^k \frac{(n-k-1)!}{k!(n-2k)!}(2x^p)^{n-2k} \pmod{np}.$$

We are done if we can show that the following two congruences hold for $k = 0, 1, 2, \ldots$:

$$\frac{np}{2}2^{np-2k}(-1)^k \frac{(np-k-1)!}{k!(np-2k)!} \equiv 0 \pmod{np}, \quad k \neq 0, p, 2p, \ldots, \tag{4.19}$$

$$\frac{np}{2}2^{np-2k}(-1)^k \frac{(np-k-1)!}{k!(np-2k)!} \equiv \frac{n}{2}2^{n-2k}(-1)^k \frac{(n-k-1)!}{k!(n-2k)!} \pmod{np}, \quad \text{all other } k. \tag{4.20}$$

We begin by showing the first congruence (4.19):

$$\begin{aligned}\frac{np}{2}2^{np-2k}(-1)^k \frac{(np-k-1)!}{k!(np-2k)!} &= \frac{np}{2}2^{np-2k}(-1)^k \frac{(np-k-1)\cdots(np-2k+1)}{k!} \\ &\equiv 0 \pmod{np}\end{aligned}$$

since $k \neq mp$ for $m \in \mathbb{Z}$ and $n = 2^i p$, so the factor of np out front will not cancel. We now prove the second congruence (4.20). We begin by simplifying the left-hand

side of (4.20):

$$\begin{aligned}
&\frac{np}{2}2^{np-2k}(-1)^{kp}\frac{(np-k-1)!}{k!(np-2k)!} \\
&\qquad = \frac{2^i p^{j+1}}{2}2^{np-2kp}(-1)^{kp}\frac{(2^i p^{j+1}-kp-1)\cdots(2^i p^{j+1}-2kp+1)}{(kp)!} \\
&\qquad = 2^{np-2kp+i-1}p^{j+1}(-1)^{kp}\frac{(2^i p^{j+1}-kp-1)\cdots(2^i p^{j+1}-2kp+1)}{(kp)!}.
\end{aligned}$$

For simplifying the right-hand side of (4.20), we note

$$\begin{aligned}
\frac{n}{2}2^{n-2k}(-1)^{k}\frac{(n-k-1)!}{k!(n-2k)!} &= \frac{2^i p^j}{2}2^{n-2k}(-1)^{k}\frac{(2^i p^j-k-1)\cdots(2^i p^j-2k+1)}{k!} \\
&= 2^{n-2k+i-1}p^j(-1)^{k}\frac{(2^i p^j-k-1)\cdots(2^i p^j-2k+1)}{k!}.
\end{aligned}$$

It is clear that modulo 2^i, both the left-hand side and the right-hand side of (4.20) are congruent to 0. Now we only need to consider both sides modulo p^{j+1}. Furthermore, since both sides have a factor of p^j, we will divide it out and consider everything modulo p. We again begin with the left-hand side of (4.20):

$$\begin{aligned}
&(2^p)^{n-2k}2^{i-1}p(-1)^{kp}\frac{(2^i p^{j+1}-kp-1)\cdots(2^i p^{j+1}-2kp+1)}{(kp)!} \\
&\qquad \equiv 2^{n-2k}2^{i-1}\frac{(-1)^{kp}}{k}\frac{(-kp-1)\cdots(-2kp+1)}{(kp-1)!} \pmod{p} \\
&\qquad \equiv 2^{n-2k}2^{i-1}\frac{(-1)^{k}}{k}(-1)^{kp-1}\binom{2kp-1}{kp} \pmod{p} \\
&\qquad \equiv 2^{n-2k+i-1}\frac{(-1)^{2k-1}}{k}\binom{2kp-1}{kp} \pmod{p}.
\end{aligned}$$

We now look at the right-hand side of (4.20):

$$\begin{aligned}
&2^{n-2k}2^{i-1}(-1)^k\frac{(2^ip^j-k-1)\cdots(2^ip^j-2k+1)}{k!}\\
&\qquad\equiv 2^{n-2k}2^{i-1}\frac{(-1)^k}{k}\frac{(-k-1)\cdots(-2k+1)}{(k-1)!} \pmod p\\
&\qquad\equiv 2^{n-2k}2^{i-1}\frac{(-1)^k}{k}(-1)^{k-1}\binom{2k-1}{k} \pmod p\\
&\qquad\equiv 2^{n-2k+i-1}\frac{(-1)^{2k-1}}{k}\binom{2k-1}{k} \pmod p.
\end{aligned}$$

To complete the proof and show that the two sides are indeed congruent modulo p, we use the following theorem of Lucas which can be found in [26]:

Theorem 4.19 (Lucas)**.** *Let m_0 and n_0 be the least non-negative residues of m and n modulo p, respectively. Then*

$$\binom{n}{m}\equiv\binom{\lfloor\frac{n}{p}\rfloor}{\lfloor\frac{m}{p}\rfloor}\binom{n_0}{m_0} \pmod p.$$

Using this theorem, we have $\binom{2kp-1}{kp}\equiv\binom{2k-1}{k} \pmod p$ and the proof of Theorem 4.18 is complete. □

We now illustrate Theorem 4.18 with an example:

Example 4.20. Let us set $p=3, i=1$, and $j=1$. Then $n=2\cdot 3=6$ and we calculate

$$\begin{aligned}
T_{np}(x)=T_{18}(x)=131072x^{18}-589824x^{16}+1105920x^{14}-1118208x^{12}+658944x^{10}\\
-228096x^8+44352x^6-4320x^4+162x^2-1,
\end{aligned}$$

$$T_n(x^p)=T_6(x^3)=32x^{18}-48x^{12}+18x^6-1.$$

Reducing modulo $np=6\cdot 3=18$, we get

$$T_{18}(x)=14x^{18}+6x^{12}+17 \pmod{18}$$

and

$$T_6(x^3) = 14x^{18} + 6x^{12} + 17 \pmod{18},$$

as expected.

The Chebyshev polynomials of the second kind, $U_x(x)$, can be expressed in terms of the Chebyshev polynomials of the first kind, $T_n(x)$. For more information regarding the relationship between $T_n(x)$ and $U_n(x)$ as well as an explicit formula for $U_n(x)$ the reader is referred to Theorem A.6 in the appendices, and to [52]. As an immediate consequence of Theorem 4.18 we have the following two corollaries:

Corollary 4.21. *For p an odd prime, we have*

$$U_{np}(x) - U_{np-2}(x) \equiv U_n(x^p) - U_{n-2}(x^p) \pmod{np}$$

for $n = 2^i p^j$, $i, j \geq 0$.

Corollary 4.22. *For $p = 2$, we have*

$$U_{2^{k+1}}(x) - U_{2^{k+1}-2}(x) \equiv U_{2^k}(x^2) - U_{2^k-2}(x^2) \pmod{2^{k+1}}$$

for $k \geq 0$.

4.6 Comments

Further commentary on Theorem 4.19 as well as a generalized version of Theorem 4.19 may be found in [42].

We continued to do some Maple experimentation with more Jacobi polynomials and Hermite polynomials. While no results analogous to Honda's congruences (4.13) and (4.14) were found in these cases, it has led us to investigate other related results for these polynomials and make the following observations.

There are some differences between the work of Robert and Zuber (Theorem 4.11) and our work that are worth mentioning. Despite being similar to the results

in the paper [53], our results are obtained without the use of p-adic numbers. The congruences in [53] are modulo a multiple of $\mathbb{Z}_p$ while ours are over $\mathbb{Z}$. However, the congruences in [53] hold for any value of n, while ours only hold for specific values of n.

We have considered the difference of the two sides of Honda's congruences (4.13), (4.14) and tried to see if we get recognizable polynomial sequences when they do not equal 0. No recognizable sequences or patterns were found.

We have also considered the divisibility of the denominators of the coefficients of these Jacobi polynomials. Since they are not invertible, they are sharing a non-trivial factor with np. The power of this factor showing up in the denominator of each Jacobi polynomial forms a non-monotonic sequence that has relatively large values for some indices in the sequence.

The congruences for $Q_n(t)$ found in Theorem 4.16 no longer hold in the cases $n = 2p^m$. The problem arises modulo 2 and modulo 2^2. We will demonstrate this with an example.

Example 4.23. If we take $p = 7$ and $n = 1$, we get:

$$Q_7(t) = 2t^7 + 2 \pmod{7^2} \qquad Q_1(t) = 2t + 2 \pmod{7^2}$$

and Theorem 4.16 holds as desired. However,

$$Q_7(t) = 2t^7 + 2 \pmod{2^2} \qquad Q_1(t) = 2t + 2 \pmod{2^2}$$

and here Theorem 4.16 fails to hold since $2t^7 + 2 \not\equiv 2t + 2 \pmod{2^2}$.

For the Legendre polynomials, unfortunately, the parallel ends here because a congruence of the form

$$T_{n-1}(x^p) \equiv T_{np-1}(x) \pmod{np}$$

does not hold. This means that we cannot define the analogue of $Q_n(x)$ from the Legendre case.

The congruence in Theorem 4.18 we found resembles a result by Dilcher and Chamberland [14, Theorem 2.1], specifically regarding the values of n for which it holds. Maybe there is a connection deeper than just "shape".

No such congruence was found for the Chebyshev polynomials of the second kind, but given the close relationship they share with those of the first kind, I believe that there would be an analogue of some sort for the polynomials of the second kind.

Chapter 5

Conclusion

We begin this chapter with final comments on some of the results in the thesis. This is followed by natural questions related to the work in Chapters 2–4 and by some remarks on possible further work. Any background material referenced in the thesis as well as a few elementary examples of the objects studied are collected in the appendices.

5.1 Comments

5.1.1 The case $a = 0$ in Chapter 3

Unless explicitly stated otherwise, the results presented in Chapter 3 concerning the polynomials $f_n^{a,c}(x), g_n^{a,c}(x), h_n^{a,c}(x)$, and $k_n^{a,c}(x)$ also apply to the polynomials $f(x), g(x), h(x)$, and $k(x)$ studied by Harrington in [28] if you take $a = 0$.

5.1.2 Height of $J_{n,H}(x)$

If $P(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$ is a polynomial of degree m, then the height of $P(x)$ is defined as $\max\{a_i\}_{i=0}^m$. For a given integer n, we wondered for which subgroup $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$ did $J_{n,H}(x)$ have the largest height. This is a question that is of interest for all of the varying special cases of n studied in Chapter 2. Although not true in general, it appears to be the case that the polynomial $J_{n,\{1,-1\}}(x)$ is the one with largest height in each family for certain cases on the integer n.

5.1.3 Potential Applications

In their joint paper [33], Joyner and Shaska discuss the applications of self-inverse or self-reciprocal polynomials to coding theory and reduction theory. They credit the behaviour of the roots of self-reciprocal polynomials and their location in the complex plane for their utility in the subject. It would be of interest to study the

potential relationship between the self-reciprocal polynomials of the form $J_{n,H}(x)$ for some integers n and subgroup $H \leq (\mathbb{Z}/n\mathbb{Z})^{\times}$ and such applications.

5.2 Further Directions

While studying congruences of the form of (4.13),(4.14) in Chapter 4, differences of Jacobi polynomials were considered modulo powers of an odd prime p. There seem to be "spikes" of divisibility as the integer n ranges with no currently discernible pattern. Studying the divisibility of these differences may lead to new congruences for Jacobi polynomials.

In Chapter 4, we mentioned that the authors of [13] considered the base-5 expansion of the primes such that 5p satisfied (2.2) but no such characterization was found. Through numerical experimentation, an interesting observation was made: taking the primes p such that $5p$ satisfied (4.6) and plugging them into the function $f(x) = 5x + 4$ resulted in $f(p)$ not being prime or $f(p)$ remaining prime for an odd number of iterations of $f(x)$.

Although they were not applied in this thesis, it is of interest to revisit the approach of Robert and Zuber [53] in an attempt to apply those methods to the more general Jacobi polynomials in hope of obtaining modulo p congruences or congruences in $\mathbb{Z}_p$ for primes p.

In Chapter 3, we proved a result regarding the discriminants of the polynomials studied in [28] by Harrington and their variation introduced in Chapter 3. We would like to study these discriminants in more depth, as well as study the resultants of pairs of these polynomials.

Despite not being able to get a direct analogue to Theorem 3.1 in this thesis, that is not to say it is an impossible task. We would like to investigate this matter further and potentially classify more examples of reducible and/or irreducible families of polynomials.

In Chapter 2 we studied the coefficients of Cyclotomic Subgroup-Polynomials $J_{n,H}(x)$ for fixed orders of the subgroup H. Namely, the cases discussed were $|H| = 1, 2, 3$, and 4. We would like to study the cases $J_{n,H}(x)$ when H is of order 5 and higher.

At the very beginning of Chapter 2 we restricted our attention to integers n that resulted in cyclic groups $(\mathbb{Z}/n\mathbb{Z})^\times$. This choice was made because of the nice structure of cyclic groups and the nice structure of their subgroups. We would like to study the set of Cyclotomic Subgroup-Polynomials for integers n when $(\mathbb{Z}/n\mathbb{Z})^\times$ is not necessarily a cyclic group.

While we were not able to find the limiting curve for the roots of the Galois Subgroup-Polynomials, there does seem to be some pattern in the behaviour of these roots. We would like to study these roots in more detail in attempt to find a limiting curve or some long-term behaviour.

Theorem 2.65 can be considered the "order 2" analogue of Apostol's famous result on the resultant of cyclotomic polynomials. In Chapter 2 we mention that we couldn't find evidence of an "order 3" analogue of Apostol's result; we would like to study this further in hopes of finding an "order 3" analogue or explaining the non-existence of one. It is also of interest to study the discriminants of the Cyclotomic Subgroup-Polynomials for different values of the positive integers n, a, and c.

As mentioned in Chapter 2, if the integer n is free of any square prime factors then $J_{n,H}(x)$ will be irreducible for all subgroups $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$. That isn't to say that it is not possible for $J_{n,H}(x)$ to be irreducible when n has a squared prime factor. An area of interest would be to try to enumerate the number of irreducible polynomials for any given integer n.

Appendices

Appendix A

Some Mathematical Background

Let x be an indeterminate and R a commutative ring with unity. The formal sum, $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, with $n \geq 0$ and $a_i \in R$ for each i is called a polynomial in x with coefficients in R. Given $a_n \neq 0$, we say that the polynomial is of degree n and we call a_n the leading coefficient. In the special case $a_n = 1$, we refer to the polynomial as a monic polynomial of degree n. The set of all such polynomials forms the ring of polynomials in x with coefficients in R, denoted $R[x]$, along with the two familiar operation of addition and multiplication.

Definition A.1. *Let n be a positive integer, K a field such that $char(K)$ does not divide n, and F a cyclotomic extension of order n of K. The n^{th} cyclotomic polynomial over K is the monic polynomial $\Phi_n(x) = (x - \zeta_1)(x - \zeta_2)\cdots(x - \zeta_r)$ where $\zeta_1, \ldots, \zeta_r$ are all the distinct primitive n^{th} roots of unity in F.*

A.0.1 Properties of the Cyclotomic Polynomials

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})}, \tag{A.1}$$

where μ is the Möbius function. Special cases:

$$\Phi_p(x) = \sum_{k=0}^{p-1} x^k = 1 + x + x^2 + \ldots + x^{p-2} + x^{p-1}. \tag{A.2}$$

$$\Phi_{2p}(x) = \sum_{k=0}^{p-1}(-x)^k = 1 - x + x^2 - x^3 + \ldots - x^{p-2} + x^{p-1}. \tag{A.3}$$

In the case $n = p^m r$, with $(p, r) = 1$, we have

$$\Phi_n(x) = \Phi_{pr}(x^{p^{m-1}}). \tag{A.4}$$

A.0.2 Properties of Binomial Coefficients

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

A.0.3 Chebyshev Polynomials

Definition A.2. *The Chebyshev Polynomials of the first kind are defined by the recurrence relation*

$$\begin{aligned} T_0(x) &= 1, \\ T_1(x) &= x, \\ T_{n+1}(x) &= 2xT_n(x) - T_{n-1}(x), \quad n \geq 2. \end{aligned}$$

Definition A.3. *The Chebyshev Polynomials of the second kind are defined by the recurrence relation*

$$\begin{aligned} U_0(x) &= 1, \\ U_1(x) &= 2x, \\ U_{n+1}(x) &= 2xU_n(x) - U_{n-1}(x), \quad n \geq 2. \end{aligned}$$

Lemma A.4. *The Chebyshev polynomials have the following generating functions:*

$$\sum_{n=0}^{\infty} T_n(x)t^n = \frac{1-tx}{1-2tx+t^2}, \tag{A.5}$$

$$\sum_{n=0}^{\infty} U_n(x)t^n = \frac{1}{1-2tx+t^2}. \tag{A.6}$$

Lemma A.5. *The Chebyshev polynomials satisfy the following identities:*

$$T_n(\cos(\theta)) = \cos(n\theta), \tag{A.7}$$

$$U_n(\cos(\theta)) = \frac{\sin((n+1)\theta)}{\sin(\theta)}. \tag{A.8}$$

Theorem A.6. *The Chebyshev polynomials of the second kind have the following explicit expressions:*

$$U_n(x) = \frac{(x+\sqrt{x^2-1})^{n+1} - (x-\sqrt{x^2-1})^{n+1}}{2\sqrt{x^2-1}}, \tag{A.9}$$

$$= \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n+1}{2k+1} (x^2-1)^k x^{n-2k}, \tag{A.10}$$

$$= x^n \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n+1}{2k+1} (1-x^2)^k x^k, \tag{A.11}$$

$$= \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{2k-(n+1)}{k} (2x)^{n-2k}, \quad n > 0, \tag{A.12}$$

$$= \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \binom{n-k}{k} (2x)^{n-2k}, \quad n > 0, \tag{A.13}$$

$$= \sum_{k=0}^{n} (-2)^k \frac{(n+k+1)!}{(n-k)!(2k+1)!} (1-x)^k, \quad n > 0. \tag{A.14}$$

Lemma A.7. *The Chebyshev polynomials satisfy the following identities:*

$$T_n(x) = \frac{1}{2}\left(U_n(x) - U_{n-2}(x)\right), \tag{A.15}$$

$$2xU_n(1-2x^2) = (-1)^n U_{2n+1}(x). \tag{A.16}$$

A.0.4 General Polynomial Results

Suppose we have the following polynomial with integer coefficients:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0.$$

We begin with some important irreducibility criteria.

Theorem A.8 (Eisenstein Criterion)**.** *If there exists a prime number p such that the following three conditions all apply:*

(i) p divides each a_i for $i \neq n$,

(ii) p does not divide a_n,

(iii) p^2 does not divide a_0,

then $P(x)$ is irreducible over the rationals.

Definition A.9. *Let $P(x)$ be as above with $a_i \in K$ for K a local field with discrete valuation and with $a_0 a_n \neq 0$. Then the Newton polygon of $P(x)$ is defined to be the lower convex hull of the set of points $\{Q_i = (i, v_K(a_i)\}$, ignoring the points where $a_i = 0$.*

Theorem A.10 (Schönemann's Criterion)**.** *Suppose that a polynomial $f(x) \in \mathbb{Z}[x]$ has the form $f(x) = \phi(x)^e + pM(x)$, where p is a prime number, $\phi(x)$ is an irreducible polynomial modulo p, and $M(x)$ is a polynomial relatively prime to $\phi(x)$ modulo p, with $deg(M) < deg(f)$. Then f is irreducible over $\mathbb{Q}$.*

Definition A.11. *Let p be a fixed prime, and let $f(x) = \sum_{i=0}^{n} A_i x^i$ be a polynomial with integer coefficients such that $A_0 A_n \neq 0$. Let us represent the nonzero coefficients of f in the form $A_i = a_i p^{\alpha_i}$, where a_i is an integer not divisible by p. To every nonzero coefficient $a_i p^{\alpha_i}$ we assign a point in the plane with coordinated (i, α_i). These points give rise to the Newton Diagram of the polynomial f (corresponding to p). The construction of the diagram is as follows. Let $P_0 = (0, \alpha_0)$ and $P_1 = (i_1, \alpha_{i_1})$, where i_1 is the largest integer for which there are no points (i, α_i) below the line $P_0 P_1$. Further let $P_2 = (i_2, \alpha_{i_2})$, where I_2 is the largest integer for which there are no points (i, α_i) below the line $P_1 P_2$, etc. The very last segment is of the form $P_{r-1} P_r$ where*

$P_r = (n, \alpha_n)$. If some segments of the broken line $P_0, \ldots, P_r$ pass through points with integer coordinates, then such points will be also considered as vertices of the broken line.

Theorem A.12 (Dumas)**.** *Let $f = gh$, where f, g, and h are polynomials with integer coefficients. Then the system of vectors of the segments for f is the union of the systems of vectors of the segments for g and h (provided that p is the same for all polynomials).*

Corollary A.13. *If, for a prime p, the Newton diagram for f consists of precisely one segment, i.e., consists of a segment containing no points with integer coefficients, then f is irreducible.*

Lemma A.14. *The Legendre polynomials, $P_n(\zeta)$, can be defined as coefficients of the generating function*

$$\frac{1}{\sqrt{1 - 2\zeta x + x^2}} = \sum_{n=0}^{\infty} P_n(\zeta) x^n.$$

Carrying out the substitution $\zeta = 1 + 2t$, we obtain the following explicit formula for $P_n(1 + 2t)$

$$P_n(1 + 2t) = \sum_{k=0}^{n} \binom{n}{k} \binom{n+k}{k} t^k.$$

Theorem A.15 (Viète's Formulas)**.** *Given the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, with $a_n \neq 0$, with its (not necessarily distinct) zeros $x_1, x_2, \ldots, x_n$, we have the following formulas:*

$$\begin{cases} x_1 + x_2 + \ldots + x_{n-1} + x_n = -\frac{a_{n-1}}{a_n}, \\ (x_1x_2 + x_1x_3 + \ldots + x_1x_n) + (x_2x_3 + x_2x_4 + \ldots + x_2x_n) + \ldots + x_{n-1}x_n = \frac{a_{n-2}}{a_n}, \\ \vdots \\ x_1x_2x_3 \cdots x_n = (-1)^n \frac{a_0}{a_n}. \end{cases}$$

A.0.5 Algebra Results

Theorem A.16. *If $\mathcal{R}$ is a unique factorization domain, then $\mathcal{R}[x]$ is a unique factorization domain.*

Theorem A.17. *A finite field $\mathbb{F}$ with n elements exists if and only if $n = p^k$ for some odd prime p and some non-negative integer k. Moreover, this field is unique up to isomorphism.*

Theorem A.18 (Structure Theorem for Finite Abelian Groups)**.** *Every finite Abelian group is isomorphic to a direct product of cyclic groups of orders that are powers of prime numbers. That is, if G is a finite Abelian group, then*

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}},$$

where $|G| = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$.

A.0.6 Number Theory Results

Theorem A.19 (Wilson's Theorem)**.** *For an odd prime, p,*

$$(p-1)! \equiv -1 \pmod{p}.$$

Theorem A.20. *There exists a primitive root modulo m if and only if $m = 1, 2, 4, p^\alpha$, and $2p^\alpha$ in which p is an odd prime and α is a natural number.*

Theorem A.21. *For a positive integer n, we have*

$$\mu(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} \exp\left(\frac{2\pi i k}{n}\right).$$

Appendix B

SAGE Code

The computer algebra system SAGE was used to generate a list of all subgroups of the group of multiplicative integers $(\mathbb{Z}/n\mathbb{Z})^\times$ for a given integer n. The computer algebra system Maple is capable of doing these calculations as well but SAGE was preferred in this case due to its speed.

The author used some advice and suggestions from different discussion posts found at the website https://ask.sagemath.org/questions/ .

Attached is a small example of how SAGE was used.

```
def list_elts(G):
    exps = [range(g.multiplicative_order()) for g in G]
    return [prod(g^e for g, e in zip(G, exp)) for exp in \
   CartesianProduct(*exps)]
```

```
R = Integers(3); map(list_elts, R.multiplicative_subgroups())
```
[[1, 2], [1]]

```
R = Integers(4); map(list_elts, R.multiplicative_subgroups())
```
[[1, 3], [1]]

```
R = Integers(5); map(list_elts, R.multiplicative_subgroups())
```
[[1, 2, 4, 3], [1, 4], [1]]

```
R = Integers(6); map(list_elts, R.multiplicative_subgroups())
```
[[1, 5], [1]]

```
R = Integers(7); map(list_elts, R.multiplicative_subgroups())
```
[[1, 3, 2, 6, 4, 5], [1, 2, 4], [1, 6], [1]]

Appendix C

Maple Code

The computer algebra system Maple was used to generate lists of the Galois Subgroup-Polynomials for a given integer n. The computer algebra system SAGE is capable of doing these calculations as well but Maple was preferred in this case due to its speed.

The author used some advice and suggestions from different discussion posts found at the website https://www.mapleprimes.com, and modified some of the functions found in found in the following master's thesis to suit this task:

Cooper, III, Thomas Edmond, "Using the Maple Computer Algebra System as a Tool for Studying Group Theory." Master's Thesis, University of Tennessee, 2002.

Attached is a small example of how Maple was used.

```
> with(GroupTheory) : Digits := 10^5 :
> Integers :=proc(n, f)
  ### Group of integers modulo n ###
  local A, i :
  A := [seq(i - 1, i = 1 ..n)] :
  f := (a, b) → (a + b) mod n :
  RETURN(A, f)
  end proc:
> MultInt :=proc(n, f)
  ### Group of multiplicative integers modulo n ###
  local i, j, H, A :
  H := {seq(i, i = 0 ..n - 1)} :
  A := [ ] :
  for j from 1 to n do
  if gcd(H[j], n) = 1 then A := [op(A), H[j]] :
  fi:
  od:
  f := (a, b) → (a·b) mod n :
  RETURN(A, f)
  end proc:
> Closed :=proc(G, f, x)
  ### Determines whether or not a list or set, G, with a given operation, f, is closed ###
  local i, j, m, n, y, z :
  y := nops(G) :
  for i from 1 to y do
  for j from 1 to y do
  z := member(f(G[i], G[j]), G) :
  if z = false then
  if nargs = 3 then
  printf(`this set with this operation is not closed since\n`);
  printf(`%a(%a,%a)=%a\n`, f, G[i], G[j], f(G[i], G[j]));
  RETURN( );
  fi:
  RETURN(`not closed`);
  fi:
  od:
  od:
  if nargs = 2 then RETURN(`closed`); fi:
  RETURN(`This set with this operation is closed`);
  end proc:
> Identity :=proc(G, f)
  ### Find the identity element of a set G under the operation f or returns noid ###
  local ct, i, j, x, y, n, id :
  id := noid :
  n := nops(G) :
  for i from 1 to n do
  ct := 0 :
  for j from 1 to n do
  x := f(G[i], G[j]) :
  if x ≠ G[j] then break fi:
  x := f(G[j], G[i]) :
```

```
    if x ≠ G[j] then break fi:
    ct := ct + 1 :
    od:
    if ct = n then id := G[i] : break fi:
    od:
    RETURN(id)
    end proc:
> SubGps := proc(G, f)
    ### Finds all subgroups of G ###
    local c, i, j, k, DiV, X, y, id :
    DiV := numtheory[divisors](nops(G)) :
    id := Identity(G, f) :
    for i from 1 to nops(DiV) do
    y := [ ] :
    X := combinat[choose](G, DiV[i]) :
    for j from 1 to nops(X) do
    k := member(id, X[j]) :
    if k = true then
    c := Closed(X[j], f) :
    if c = closed then
    y := [op(y), X[j]] :
    fi:
    fi:
    od:
    print(y)
    od:
    end proc:
> Lcoset := proc(x, H, G, f)
    ### Finds xH ###
    local i, y, z, m, xH:
    m := member(x, G) :
    if m = false then RETURN( `ERROR: not in group`); fi:
    xH := { } :
    for i from 1 to nops(H) do
    y := f(x, H[i]) :
    z := member(y, xH) :
    if z = false then
    xH := {op(xH), y} :
    fi:
    od:
    RETURN(xH);
    end proc:
> GmodH := proc(H, G, f, g)
    ### Forms the quotient group G modulo H with operation g ###
    local i, y, z, j, xH, X, GMODH :
    X := { } :
    for j from 1 to nops(G) do
    xH := { } :
    for i from 1 to nops(H) do
    y := f(G[j], H[i]) :
    xH := {op(xH), y} :
    od:
```

```
    X := {op(X), xH} :
    od:
    GMODH := X :
    g := (a, b) → Lcoset(f(a[1], b[1]), H, G, f) :
    return(GMODH)
    end proc:
> GIP := proc(G, n)
    ### Creates the family of Galois irreducible polynomials ###
    local A, Z, h, i, j, b, a, F, m, B, C, Y :
    A := [ ] :
    for i from 1 to nops(G) do
    A := [op(A), GmodH(G[i], MultInt(n, f), f, f) ] :
    od:
    Z := [ ] : h := 1 : Y := [ ] : B := 0 : F := [ ] :
    for i from 1 to nops(A) do
    for j from 1 to nops(A[i]) do
    h := h·(x − sum(w^A[i][j][k], k = 1 ..nops(A[i][j]))) ;
    od:
    Z := [op(Z), h]; h := 1 :
    od:
    for b from 1 to nops(Z) do
    Z[b] :
    expand(%) :
    simplify(%, {w^n = 1}) :
    collect(%, x) :
    simplify(%, {w = exp(2·Pi·I / n)}) :
    convert(%, exp) :
    evalf[10^5](%) :
    collect(%, x) :
    a := [coeffs(%, x, 't')] :
    for j from 1 to nops(a) do
    F := [op(F), round(a[j])] :
    od:
    for m from 1 to nops(F) do
    B := B + F[m]·t[m] :
    od:
    C := collect(B, x) :
    F := [ ] : B := 0 :
    Y := [op(Y), C] :
    od:
    end proc:

> GIP([[1, 2], [1]], 3) :
> for n from 1 to nops(%) do
    print(%[n])
    od:
```

$$x + 1 \tag{1}$$

$$x^2 + x + 1 \tag{1}$$

```
> GIP([[1, 3], [1]], 4):
> for n from 1 to nops(%) do
  print(%[n])
  od:
```

$$x_1$$

$$x^2 + 1 \tag{2}$$

```
> GIP([[1, 2, 4, 3], [1, 4], [1]], 5):
> for n from 1 to nops(%) do
  print(%[n])
  od:
```

$$x + 1$$

$$x^2 + x - 1$$

$$x^4 + x^3 + x^2 + x + 1 \tag{3}$$

```
> GIP([[1, 5], [1]], 6):
> for n from 1 to nops(%) do
  print(%[n])
  od:
```

$$x - 1$$

$$x^2 - x + 1 \tag{4}$$

```
> GIP([[1, 3, 2, 6, 4, 5], [1, 2, 4], [1, 6], [1]], 7):
> for n from 1 to nops(%) do
  print(%[n])
  od:
```

$$x + 1$$

$$x^2 + x + 2$$

$$x^3 + x^2 - 2x - 1$$

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \tag{5}$$

```
>
```

Appendix D

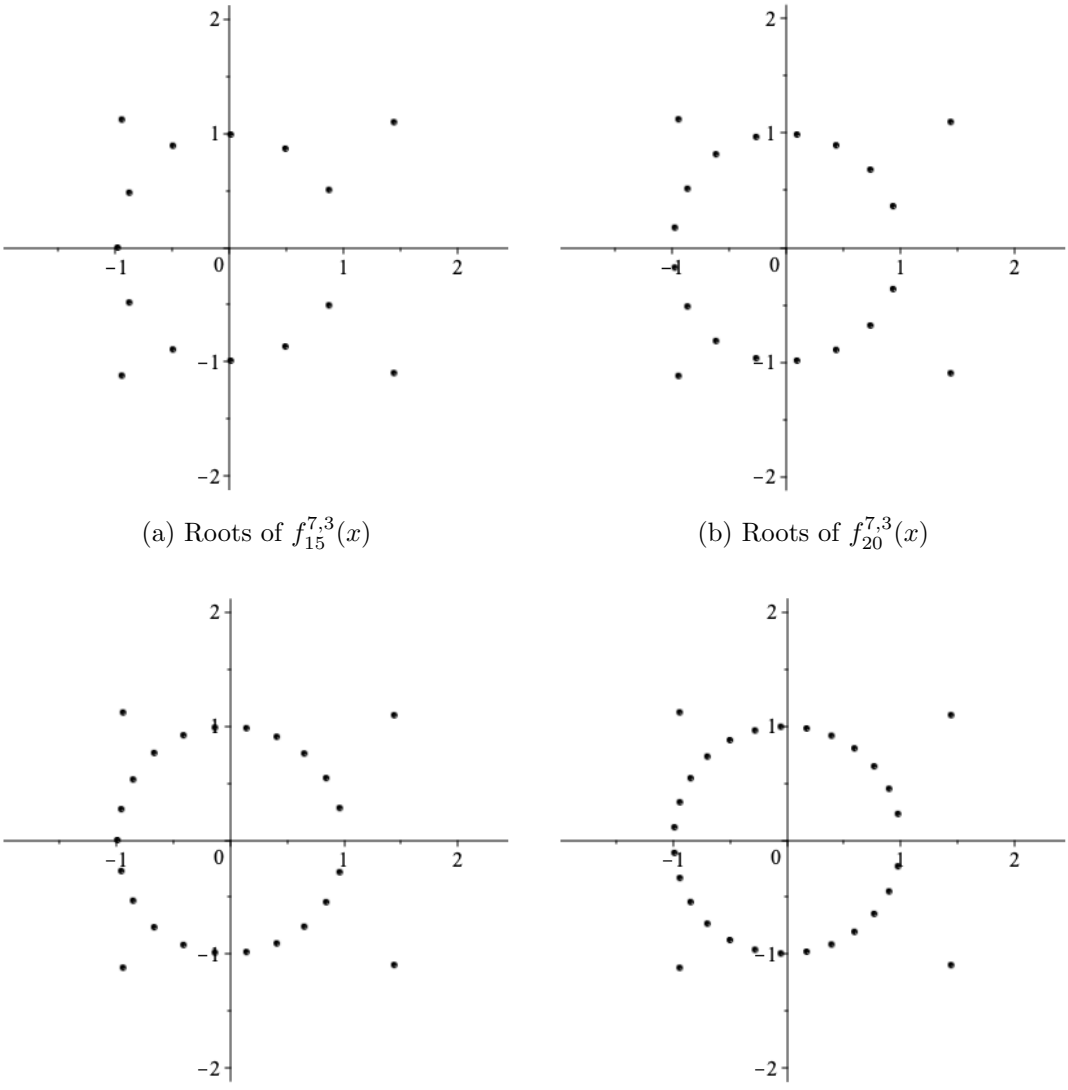
Table of Cyclotomic Subgroup-Polynomials

n	H	$J_{n,H}(x)$
3	$\{1,2\}$	$x+1$
3	$\{1\}$	x^2+x+1
4	$\{1,3\}$	x
4	$\{1\}$	x^2+1
5	$\{1,2,3,4\}$	$x+1$
5	$\{1,4\}$	x^2+x-1
5	$\{1\}$	$x^4+x^3+x^2+x+1$
6	$\{1,5\}$	$x-1$
6	$\{1\}$	x^2-x+1
7	$\{1,2,3,4,5,6\}$	$x+1$
7	$\{1,2,4\}$	x^2+x+2
7	$\{1,6\}$	x^3+x^2-2x-1
7	$\{1\}$	$x^6+x^5+x^4+x^3+x^2+x+1$
8	$\{1,3,5,7\}$	x
8	$\{1,7\}$	x^2-2
8	$\{1,5\}$	x^2
8	$\{1,3\}$	x^2+2
8	$\{1\}$	x^4+1
9	$\{1,2,4,5,7,8\}$	x
9	$\{1,4,7\}$	x^2
9	$\{1,8\}$	x^3-3x+1
9	$\{1\}$	x^6+x^3+1
10	$\{1,3,7,9\}$	$x-1$
10	$\{1,9\}$	x^2-x-1
10	$\{1\}$	$x^4-x^3+x^2-x+1$

Table D.1: Cyclotomic Subgroup-Polynomials

Appendix E

Plots of the Roots of $f_n^{a,c}(x)$



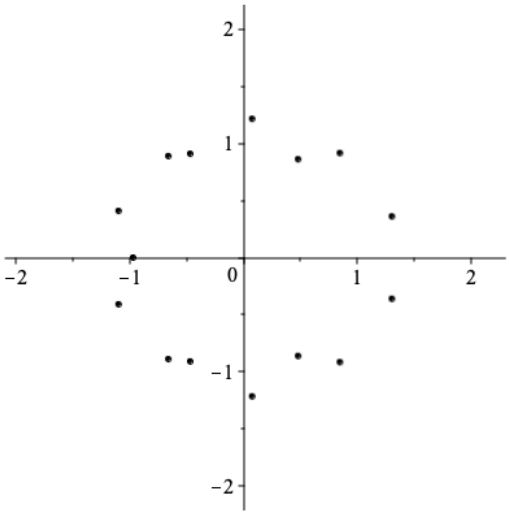
(a) Roots of $f_{15}^{7,3}(x)$

(b) Roots of $f_{20}^{7,3}(x)$

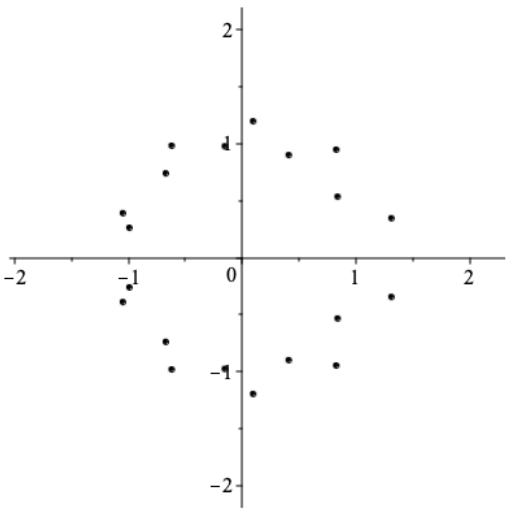
(c) Roots of $f_{25}^{7,3}(x)$

(d) Roots of $f_{30}^{7,3}(x)$

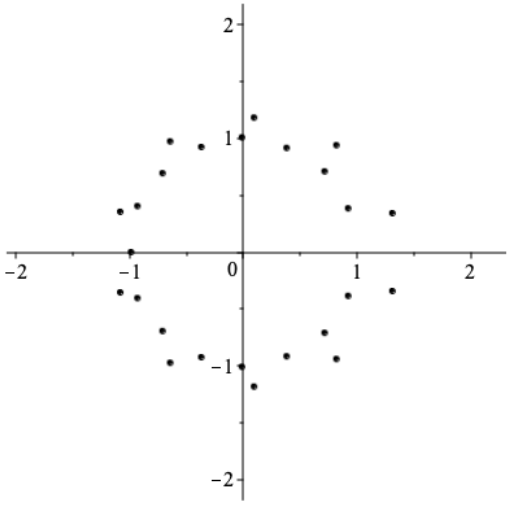
Figure E.1: Comparison of Roots of $f_n^{7,3}(x)$ when $n = 15, 20, 25, 30$.



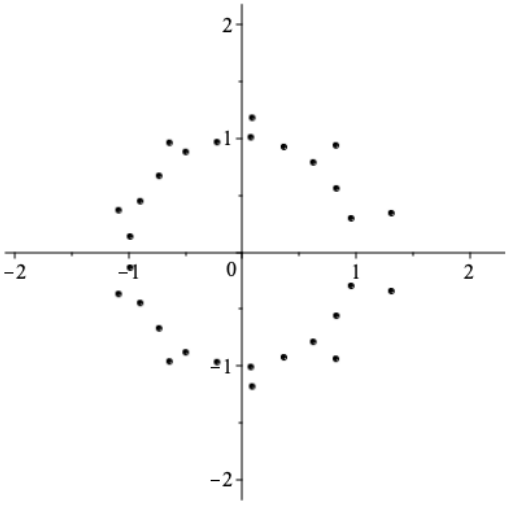
(a) Roots of $f_{15}^{7,9}(x)$



(b) Roots of $f_{20}^{7,9}(x)$

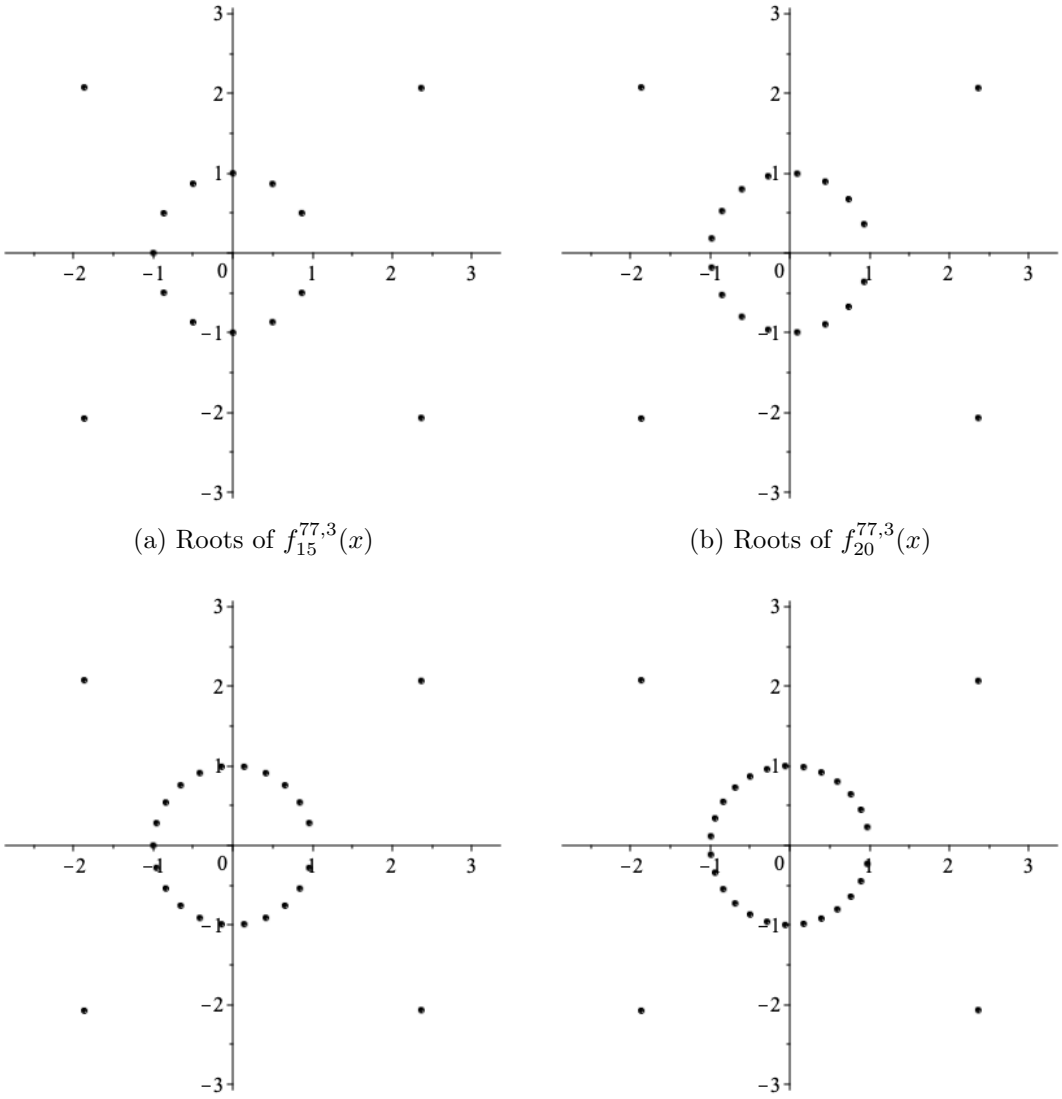


(c) Roots of $f_{25}^{7,9}(x)$



(d) Roots of $f_{30}^{7,9}(x)$

Figure E.2: Comparison of Roots of $f_n^{7,9}(x)$ when $n = 15, 20, 25, 30$.



(a) Roots of $f_{15}^{77,3}(x)$

(b) Roots of $f_{20}^{77,3}(x)$

(c) Roots of $f_{25}^{77,3}(x)$

(d) Roots of $f_{30}^{77,3}(x)$

Figure E.3: Comparison of Roots of $f_n^{77,3}(x)$ when $n = 15, 20, 25, 30$.

Bibliography

[1] Dorin Andrica and Ovidiu Bagdasar. On some results concerning the polygonal polynomials. *Carpathian Journal of Mathematics.*, 2019.

[2] Dorin Andrica and Ovidiu Bagdisar. Some remarks on a general family of complex polynomials. Submitted for Publication, 2018.

[3] Tom M. Apostol. Resultants of cyclotomic polynomials. *Proc. Amer. Math. Soc.*, 24:457–462, 1970.

[4] D. F. Bailey. More binomial coefficient congruences. *Fibonacci Quart.*, 30(2):121–125, 1992.

[5] E. J. Barbeau. *Polynomials*. Problem Books in Mathematics. Springer New York, 2003.

[6] Serban Barcanescu. The coefficients of the period polynomials. *arXiv e-prints*, page arXiv:1402.3833, Feb 2014.

[7] Bruce C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society series of monographs and advanced texts. Wiley, 1998.

[8] Scott Beslin and Valerio De Angelis. The minimal polynomials of $\sin(\frac{2\pi}{p})$ and $\cos(\frac{2\pi}{p})$. *Math. Mag.*, 77(2):146–149, 2004.

[9] F. Beukers. Some congruences for the Apéry numbers. *J. Number Theory*, 21(2):141–155, 1985.

[10] F. Rudolf Beyl. Cyclic subgroups of the prime residue group. *Amer. Math. Monthly*, 84(1):46–48, 1977.

[11] P. Borwein and T. Erdelyi. *Polynomials and Polynomial Inequalities*. Graduate Texts in Mathematics. Springer New York, 1995.

[12] Antonio Cafure and Eda Cesaratto. Irreducibility criteria for reciprocal polynomials and applications. *Amer. Math. Monthly*, 124(1):37–53, 2017.

[13] Marc Chamberland and Karl Dilcher. Divisibility properties of a class of binomial sums. *J. Number Theory*, 120(2):349–371, 2006.

[14] Marc Chamberland and Karl Dilcher. A binomial sum related to Wolstenholme's theorem. *J. Number Theory*, 129(11):2659–2672, 2009.

[15] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2013.

[16] Matthijs Coster. *Supercongruences*. PhD thesis, Universiteit Leiden, 1988.

[17] David A. Cox. *Primes of the Form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[18] Gregory Dresden. Resultants of cyclotomic polynomials. *Rocky Mountain J. Math.*, 42(5):1461–1469, 2012.

[19] Paulius Drungilas, Jonas Jankauskas, and Jonas Šiurys. On Newman and Littlewood multiples of Borwein polynomials. *arXiv e-prints*, Sep 2016.

[20] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2004.

[21] A.W.F. Edwards. *Pascal's Arithmetical Triangle: The Story of a Mathematical Idea*. Johns Hopkins Paperback. Johns Hopkins University Press, 2002.

[22] Harriet Fell. The geometry of zeros of trinomial equations. *Rendiconti del Circolo Matematico di Palermo*, 29(2):303–336, May 1980.

[23] Michael Filaseta and Ikhalfani Solan. An extension of a theorem of Ljunggren. *Math. Scand.*, 84(1):5–10, 1999.

[24] Ira M. Gessel. Some congruences for generalized Euler numbers. *Canad. J. Math.*, 35(4):687–709, 1983.

[25] T. Gowers, J. Barrow-Green, and I. Leader. *The Princeton Companion to Mathematics*. Princeton University Press, 2010.

[26] Andrew Granville. Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. In *Organic mathematics (Burnaby, BC, 1995)*, volume 20 of *CMS Conf. Proc.*, pages 253–276. Amer. Math. Soc., Providence, RI, 1997.

[27] E. R. Hansen. *A Table of Series and Products*. Prentice-Hall series in automatic computation. Prentice-Hall, 1975.

[28] Joshua Harrington. On the factorization of the trinomials $x^n + cx^{n-1} + d$. *Int. J. Number Theory*, 8(6):1513–1518, 2012.

[29] Taira Honda. Two congruence properties of Legendre polynomials. *Osaka J. Math.*, 13(1):131–133, 1976.

[30] T. W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2003.

[31] Saud Hussein. New conjecture related to a conjecture of McIntosh. *arXiv e-prints*, Feb 2018.

[32] Svante Janson. Resultant and discriminant of polynomials. 2007.

[33] David Joyner and Tony Shaska. Self-inversive polynomials, curves, and codes. *arXiv e-prints*, Jun 2016.

[34] E. E. Kummer. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. *J. Reine Angew. Math.*, 44:93–146, 1852.

[35] Miyeon Kwon, Ji-Eun Lee, and Ki-Suk Lee. Galois irreducible polynomials. *Commun. Korean Math. Soc.*, 32(1):1–6, 2017.

[36] T. Y. Lam and K. H. Leung. On vanishing sums of roots of unity. *J. Algebra*, 224(1):91–109, 2000.

[37] Ki-Suk Lee and Ji-Eun Lee. Classification of Galois polynomials. *Honam Math. J.*, 39(2):259–265, 2017.

[38] Ki-Suk Lee, Ji-Eun Lee, and Ji-Hye Kim. Semi-cyclotomic polynomials. *Honam Math. J.*, 37(4):469–472, 2015.

[39] Wilhelm Ljunggren. On the irreducibility of certain trinomials and quadrinomials. *Math. Scand.*, 8:65–70, 1960.

[40] M. Marden. *Geometry of Polynomials*. Number no. 3 in Geometry of Polynomials. American Mathematical Society, 1949.

[41] Greg Martin. A product of Gamma function values at fractions with the same denominator. *arXiv e-prints*, Jul 2009.

[42] Richard J. McIntosh. A generalization of a congruential property of Lucas. *Amer. Math. Monthly*, 99(3):231–238, 1992.

[43] Richard J. McIntosh. On the converse of Wolstenholme's theorem. *Acta Arith.*, 71(4):381–389, 1995.

[44] J. Meldrum and N. Bourbaki. *Elements of the History of Mathematics*. Springer Berlin Heidelberg, 1998.

[45] Idris Mercer. Newman polynomials, reducibility, and roots on the unit circle. *Integers*, 12(4):503–519, 2012.

[46] W. H. Mills. The factorization of certain quadrinomials. *Math. Scand.*, 57(1):44–50, 1985.

[47] Gerald Myerson. Period polynomials and Gauss sums for finite fields. *Acta Arith.*, 39(3):251–264, 1981.

[48] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[49] V. V. Prasolov and D. Leites. *Polynomials*. Number v. 13 in Algorithms and Computation in Mathematics. Springer, 2004.

[50] A. P. Prudnikov. *Integrals and Series: Volume 1: Elementary Functions; Volume 2: Special Functions*. Taylor & Francis, 1986.

[51] I. M. Richards. A remark on the number of cyclic subgroups of a finite group. *Amer. Math. Monthly*, 91(9):571–572, 1984.

[52] T.J. Rivlin. *Chebyshev Polynomials: From Approximation Theory to Algebra and Number Theory*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 1990.

[53] Alain Robert and Maxime Zuber. The Kazandzidis supercongruences. A simple proof and an application. *Rend. Sem. Mat. Univ. Padova*, 94:235–243, 1995.

[54] Gary Sivek. On vanishing sums of distinct roots of unity. *Integers*, 10:A31, 365–368, 2010.

[55] Richard P. Stauduhar. The determination of Galois groups. *Math. Comp.*, 27:981–996, 1973.

[56] Marius Tărnăuceanu. Finite groups with a certain number of cyclic subgroups. *Amer. Math. Monthly*, 122(3):275–276, 2015.

[57] J. Wójcik. A refinement of a theorem of Schur on primes in arithmetic progressions. III. *Acta Arith*, 15:193–197, 1968/1969.