5-2010

On the Irreducibility of the Cauchy-Mirimanoff Polynomials

Brian C. Irick
University of Tennessee - Knoxville, birick@utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Brian C. Irick entitled "On the Irreducibility of the Cauchy-Mirimanoff Polynomials." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Pavlos Tzermias, Major Professor

We have read this dissertation and recommend its acceptance:

David Dobbs, Shashikant Mulay, Soren Sorensen

Accepted for the Council:
Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:
I am submitting herewith a dissertation written by Brian Christopher Irick entitled "On the Irreducibility of the Cauchy-Mirimanoff Polynomials". I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Pavlos Tzermias
Major Professor

We have read this dissertation
and recommend its acceptance:

David Dobbs

Shashikant Mulay

Soren Sorensen

Accepted for the Council:

Carolyn Hodges
Vice Provost and Dean of
the Graduate School

(Original signatures are on file with offical student records.)

On the Irreducibility of the Cauchy-Mirimanoff Polynomials

A Dissertation
Presented for the
Doctor of Philosophy
Degree
The University of Tennessee, Knoxville

Brian Christopher Irick
May 2010

Acknowledgments

First and foremost, I would like to thank my advisor, Pavlos Tzermias, for suggesting the topic of this dissertation and for all his help during my research. I am particularly grateful for the freedom I had to pursue this in my own way. His thoughtful suggestions and personal encouragement were always what I needed to move forward. I very much appreciate his efforts, and this dissertation is better because of it.

I would also like to thank my doctoral committee members David Dobbs, Shashikant Mulay, and Soren Sorensen for their time and interest in this topic. I am particularly indebted to each for my education, and I am grateful to be able to call each a friend.

Abstract

The Cauchy-Mirimanoff Polynomials are a class of polynomials that naturally arise in various classical studies of Fermat's Last Theorem. Originally conjectured to be irreducible over 100 years ago, the irreducibility of the Cauchy-Mirimanoff polynomials is still an open conjecture. Recently, there has been renewed interest in this conjecture including Helou (1997), Beukers (1997), Tzermias (2007) and (2009), and Nanninga (2009).

This dissertation takes a new approach to the study of the Cauchy-Mirimanoff Polynomials. The reciprocal transform of a self-reciprocal polynomial is defined, and the reciprocal transforms of the Cauchy-Mirimanoff Polynomials are found and studied. Particular attention is given to the Cauchy-Mirimanoff Polynomials with index three times a power of a prime, and it is shown that the Cauchy-Mirimanoff Polynomials of index three times a prime are irreducible.

Contents

List of Tables

Chapter 1

Introduction

In this dissertation, the factorization of a class of polynomials that originally arose in the first proof of Fermat's Last Theorem for the special case $n = 7$ is studied. This class of polynomials has come to be known as the *Cauchy-Mirimanoff Polynomials*, and it is a long standing conjecture that every Cauchy-Mirimanoff polynomial is irreducible.

1.1 Background

In 1839, Gabriel Lamé proved the special case of Fermat's Last Theorem for exponent $n = 7$. In the proof, Lamé used the polynomial identity:

$$(X + Y)^7 - X^7 - Y^7 = 7XY(X + Y)(X^2 + XY + Y^2)^2$$

In examining Lamé's proof, Augustin-Louis Cauchy and Joseph Liouville indicated a more general identity of which the following is a special case (set $Y = 1$):

$$P_n(X) := (X + 1)^n - X^n - 1 = X(X + 1)^{\epsilon_n}(X^2 + X + 1)^{e_n}E_n(X) \tag{1.1}$$

where for even n, $\epsilon_n = e_n = 0$; for odd n, $\epsilon_n = 1$ and $e_n = 0$, 1, or 2 according as $n \equiv 0$, 2, or 1 (mod 3). The remaining factor $E_n(X)$ of $P_n(X)$ is called the n^{th} *Cauchy-Mirimanoff Polynomial*. Dimitry Mirimanoff studied $E_n(X)$ extensively for prime n, and conjectured its irreducibility over $\mathbb{Q}[X]$ (Mirimanoff, 1903). Indeed, this conjecture seems to hold for all $n \geq 2$. The interested reader may find a more extensive account of the historical connection of the Cauchy-Mirimanoff Polynomials to Fermat's Last Theorem in Ribenboim (1979).

Little progress was made on the conjecture until the mid 1990's. Helou (1997) studied the Galois group of the Cauchy-Mirimanoff Polynomials and included a proof, attributed to Michael Filaseta, that $E_{2p}(x)$ is irreducible for all primes p. Many of the results from Helou (1997) will be of use in this dissertation and are stated in Sections 2.2.3, 2.3.1, and 2.3.2. Independently, in an application to the Korteweg-de Vries equation, Beukers (1997) proved that the Cauchy-Mirimanoff Polynomials are relatively prime to each other.

Tzermias (2007) studied the Cauchy-Mirimanoff polynomials of prime index and obtained lower bounds for the degrees of some factors of the Cauchy-Mirimanoff polynomials of prime index p with $p \equiv 2 \pmod 3$. Recently, Tzermias (2009) obtained bounds for the degrees of some factors of the Cauchy-Mirimanoff polynomials of prime index p with $p \equiv 1 \pmod 3$. The main results of both papers are stated in Section 2.3.3.

In a submitted Ph.D. thesis, Nanninga (2009) has announced a proof that $E_n(X)$ is irreducible when $n = 2^k m$ where m is an odd integer and $k \in \{1, 2, 3, 4, 5\}$. The thesis is under revision, but the results would seem to indicate a generalization of Michael Filaseta's proof of the irreducibility of $E_{2p}(X)$.

1.2 Contributions

This dissertation begins with a broad overview of the known results regarding the Cauchy-Mirimanoff Polynomials. Then the reciprocal transform of a self-reciprocal polynomial is defined, and the reciprocal transforms of the Cauchy-Mirimanoff Polynomials are found (Theorem 4.2.1). It is worth noting that the reciprocal transforms of the Cauchy-Mirimanoff polynomials are closely related to a problem of minimization in Approximation Theory (Chebyshev Approximation), and are also related to Dickson Polynomials. In other words, the Cauchy-Mirimanoff Polynomials could have applications to cryptography, coding theory, and applied mathematics (in addition to the Korteweg-de Vries equation).

After applying Dickson's Theorem to the Cauchy-Mirimanoff Polynomials (Theorem 4.3.2), we specialize to the polynomials $E_{3p^i}(X)$ for primes p and $i \in \mathbb{N}$. In particular, it is shown that $E_{3p}(X)$ is irreducible over $\mathbb{Q}$, and in fact, three distinct proofs are provided (see Section 5.2.3, Corollary 6.2.9, and Corollary 6.3.5). It is also shown that for any $i \in \mathbb{N}$, $E_{3p^i}(X)$ is a product of no more than i irreducible polynomials (Corollary 6.2.8), every irreducible factor of $E_{3p^i}(X)$ has degree $d \geq 3(p-1)$ (Corollary 6.3.7), and $E_{3p^i}(X)$ has an irreducible factor of degree $d \geq 3(p-1)p^{i-1}$ (Corollary 6.3.6). It is also shown that $E_{3p^2}(X)$ is either irreducible, or a product of two irreducible factors of degree $3(p-1)$ and $3(p-1)p$ (Corollary 6.3.8).

1.3 Arrangement

Chapter 2 defines the Cauchy-Mirimanoff Polynomials, and contains many of the known results regarding these polynomials including results from Mirimanoff (1903), Helou (1997), Beukers (1997), Tzermias (2007, 2009), and Nanninga (2009). Reciprocal and self-reciprocal polynomials are defined and studied.

Chapter 3 defines the Fractional, Half-Fractional, and Modified Half-Fractional Chebyshev Polynomials. These functions, which are not necessarily polynomials, are closely related to the classic Chebyshev Polynomials and have a number of analogous properties. These properties will be useful in applications to the Cauchy-Mirimanoff Polynomials, and do not seem to appear in the literature.

Chapter 4 defines the concept of the reciprocal transform of a self-reciprocal polynomial. This is not a new idea, but there is no universal agreement to name or notation. Dickson's Theorem, which relates factorization of a self-reciprocal polynomial to the factorization of the reciprocal transform, is stated and applied to the Cauchy-Mirimanoff Polynomials. An explicit formula for the reciprocal transform of the Cauchy-Mirimanoff Polynomials is found and the roots are studied.

Chapter 5 begins with a new proof that $E_{2p}(X)$ is irreducible over $\mathbb{Q}$. Then, the Newton Polygon of the reciprocal transform of $E_{3p}(X)$ is studied. Subsequently combining many of the results from Chapters 2 and 4, a proof that $E_{3p}(X)$ is irreducible is given.

Chapter 6 generalizes the results of Chapter 5 to the Cauchy-Mirimanoff Polynomials $E_{3p^i}(X)$. Two additional proofs of the irreducibility of $E_{3p}(X)$ are obtained as corollaries to more general theorems. It is shown that for any $i \in \mathbb{N}$, $E_{3p^i}(X)$ is a product of no more than i irreducible polynomials, every irreducible factor of $E_{3p^i}(X)$ has degree $d \geq 3(p-1)$, and $E_{3p^i}(X)$ has an irreducible factor of degree $d \geq 3(p-1)p^{i-1}$. It is also shown that $E_{3p^2}(X)$ is either irreducible, or a product of two irreducible factors of degree $3(p-1)$ and $3(p-1)p$.

Chapter 2

The Cauchy-Mirimanoff Polynomials

In this chapter, the Cauchy-Mirimanoff Polynomials are defined and many of the known facts regarding these polynomials are presented.

2.1 Definition of the Cauchy-Mirimanoff Polynomials

Proposition 2.1.1. *Let $n \geq 2$ be an integer, ω a primitive third root of unity, and define $P_n(X) \in \mathbb{Z}[X]$ as*

$$P_n(X) \coloneqq (X+1)^n - X^n - 1$$

Then

1. *0 is a simple root of $P_n(X)$.*
2. *If n is even, then -1 is not a root of $P_n(X)$; if n is odd, then -1 is a simple root of $P_n(X)$.*
3. *If n is even, then ω is not a root of $P_n(X)$; if n is odd, then ω is a root of $P_n(X)$ of multiplicity $0,\ 1$, or 2 according as $n \equiv 0,\ 2$, or $1 \pmod 3$.*

Proof. Proceed by examining cases.
For all $n \geq 2$:

- $X \mid P_n(X) : P_n(0) = 0$.
- $X^2 \nmid P_n(X)$: If $X^2 \mid P_n(X)$, then 0 is a root of $\frac{dP_n}{dx}$. However $\frac{dP_n(0)}{dx} = n \neq 0$.

Suppose $n \geq 2$ is even:

- $(X+1) \nmid P_n(X) : P_n(-1) = -2 \neq 0$.
- $(X^2 + X + 1) \nmid P_n(X) : P_n(\omega) = -2\mathbb{i} \sin(\frac{2\pi n}{3}) - 1$. So either $P_n(\omega)$ has a nonzero imaginary part or equals -1. In either case $P_n(\omega) \neq 0$.

Suppose $n \geq 2$ is odd:

- $(X+1) \mid P_n(X) : P_n(-1) = 0$.
- $(X+1)^2 \nmid P_n(X)$: If $(X+1)^2 \mid P_n(X)$, then -1 is a root of $\frac{dP_n}{dx}$. However, $\frac{dP_n(-1)}{dx} = -n \neq 0$.

Suppose $n \geq 2$ is odd and $n \equiv 0 \pmod 3$:

- $(X^2 + X + 1) \nmid P_n(X) : P_n(\omega) = -3 \neq 0$.

Suppose $n \geq 2$ is odd and $n \equiv 1 \pmod 3$:

- $(X^2 + X + 1)^2 \mid P_n(X)$: It is enough to check that ω is a root of both $P_n(X)$ and $\frac{dP_n}{dx}$. Both are easily verified.
- $(X^2 + X + 1)^3 \nmid P_n(X)$: If $(X^2 + X + 1)^3 \mid P_n(X)$, then ω is a root of $\frac{d^2P_n}{dx^2}$. However, in this case, $\frac{d^2P_n(\omega)}{dx^2} = n(n-1) \neq 0$.

Finally, suppose $n \geq 2$ is odd and $n \equiv 2 \pmod 3$:

- $(X^2 + X + 1) \mid P_n(X) : P_n(\omega) = 0$.
- $(X^2+X+1)^2 \nmid P_n(X)$: If $(X^2+X+1)^2 \mid P_n(X)$, then ω is a root of $\frac{dP_n}{dx}$. However, $\frac{dP_n(\omega)}{dx} = -\sqrt{3}\mathbb{i}n \neq 0$.

□

Often Proposition 2.1.1 is stated more succinctly in terms of the factorization of $P_n(X)$. This leads to the definition of the Cauchy-Mirimanoff Polynomials.

Definition 2.1.2 (Cauchy-Mirimanoff Polynomials)**.** Let $n \geq 2$ be an integer. The n^{th} *Cauchy-Mirimanoff Polynomial* is the remaining factor $E_n(X)$ of $P_n(X)$, in $\mathbb{Q}[X]$, after removing X and the cyclotomic factors. Specifically,

$$P_n(X) = X(X+1)^{\epsilon_n}(X^2 + X + 1)^{e_n} E_n(X) \tag{2.1}$$

where for even n, $\epsilon_n = e_n = 0$; for odd n, $\epsilon_n = 1$ and $e_n = 0$, 1, or 2 according as $n \equiv 0$, 2, or 1 $\pmod 3$.

Corollary 2.1.3. *If n is even, then* $\deg(E_n) = n - 2$. *If n is odd, then* $\deg(E_n) = n - 3 - 2e_n$.

Proof. By inspection, $\deg(P_n) = n - 1$. By Proposition 2.1.1, if n is even, then X is a factor of $P_n(X)$ $\therefore$ $\deg(E_n) = n - 2$. Similarly, if n is odd, then X and $X + 1$ are factors of $P_n(X)$ of degree 1, and $X^2 + X + 1$ is a factor of degree $2e_n$ $\therefore$ $\deg(E_n) = n - 3 - 2e_n$. □

2.2 The Roots of $P_n(X)$ and $E_n(X)$

This section collects many of the known facts about the roots of both $P_n(X)$ and $E_n(X)$.

2.2.1 Elementary Facts

Theorem 2.2.1. *Let $n \geq 2$. Then*

1. *$P_n(X)$ has no roots that are roots of unity beside -1 and ω in the cases already handled.*
2. *$P_n(X)$ has no real roots except 0 and -1 (n odd).*
3. *$E_n(X)$ has no roots that are roots of unity.*
4. *$E_n(X)$ has no real roots.*
5. *$E_n(X)$ has no repeated roots in any splitting field over $\mathbb{Q}$.*

Proof.

1. Let $\zeta_m = e^{\frac{2\pi\mathrm{i}}{m}}$, $m \geq 4$, and $n \geq 3$. Then $|P_n(\zeta_m)| = |(\zeta_m + 1)^n - \zeta_m^n - 1| \geq ||(\zeta_m + 1)^n| - |\zeta_m^n + 1|| = ||\zeta_m^{\frac{n}{2}}(\zeta_m^{\frac{1}{2}} + \zeta_m^{\frac{-1}{2}})^n| - |\zeta_m^n + 1|| = ||(2\cos(\frac{\pi}{m}))^n| - |\zeta_m^n + 1||$. As $|(2\cos(\frac{\pi}{m}))^n| > 2 \geq |\zeta_m^n + 1|$, it follows $|(2\cos(\frac{\pi}{m}))^n| \neq |\zeta_m^n + 1| \therefore |(2\cos(\frac{\pi}{m}))^n| - |\zeta_m^n + 1| \neq 0 \therefore ||(2\cos(\frac{\pi}{m}))^n| - |\zeta_m^n + 1|| > 0 \therefore |P_n(\zeta_m)| > 0$.

2. Observe $\frac{dP_n}{dX} = n(X + 1)^{n-1} - nX^{n-1}$. If $\alpha \in \mathbb{R}$ such that $\frac{dP_n(\alpha)}{dX} = 0$ then $n(\alpha + 1)^{n-1} = n\alpha^{n-1}$. If n is even, no solution exists; if n is odd, then $\alpha = -\frac{1}{2}$ is the only solution. Consequently, if n is even, then $P_n(X)$ can have at most one real root; if n is odd, then $P_n(X)$ can have at most two roots. From Proposition 2.1.1, $P_n(X)$ has 0 as a root if n is even, and 0 and -1 as roots if n is odd, and so these are the only real roots of $P_n(X)$.

3. Consequence of 1 above.

4. Consequence of 2 above.

5. Suppose $\alpha \in \mathbb{C}$ is a multiple root of $P_n(X)$. Then both $P_n(\alpha)$ and $\frac{dP_n(\alpha)}{dx}$ equal 0. This implies that $(\alpha + 1)^n - \alpha^n - 1 = 0$ and $(\alpha + 1)^{n-1} = \alpha^{n-1} \therefore (\alpha + 1)^n - \alpha(\alpha + 1)^{n-1} = 1 \therefore (\alpha + 1)^{n-1} = 1 \therefore \alpha^{n-1} = 1$. Therefore, α must be a root of unity. The only roots of unity of $P_n(X)$ are -1 and ω, from 1 above, and the multiplicity of those roots was handled in Proposition 2.1.1. Therefore, ω and $\overline{\omega}$ (:= complex conjugate of z) are the only possible multiple roots of $P_n(X)$ (which do occur in certain cases) $\therefore E_n(X)$ has no multiple roots.

□

2.2.2 Reciprocal and Self-Reciprocal Polynomials

Definition 2.2.2 (Reciprocal and Self-Reciprocal Polynomials)**.** Let $\mathbb{D}$ be an integral domain, $0 \neq p(x) \in \mathbb{D}[x]$, and let $d := \deg(p)$. The *reciprocal polynomial of* $p(x)$ is defined to be the polynomial $p^{\dashv}(x) := x^d p(\frac{1}{x})$. A polynomial is said to be *self-reciprocal* if it equals its reciprocal, that is, $p(x) = p^{\dashv}(x)$.

There is no universally agreed upon definition or notation for reciprocal and self-reciprocal polynomials in the literature. The reciprocal of a polynomial is sometimes called the "reversal"; self-reciprocal polynomials are sometimes simply called "reciprocals" or "palindromes".

Proposition 2.2.3. *Let $\mathbb{D}$ be an integral domain, $p(x) \in \mathbb{D}[x]$, and $d := \deg(p)$.*

1. *If $x \nmid p(x)$, then $d = \deg(p^{\dashv})$.*

2. *If $x \mid p(x)$, then $d > \deg(p^{\dashv})$*

3. *If $p(x)$ is self-reciprocal, then $x \nmid p(x)$.*

Proof.

1. Let $p(x) = c_d x^d + \cdots + c_0$. Then $p^{\dashv}(x) = x^d \left(c_d \frac{1}{x^d} + \cdots + c_0\right) = c_d + \cdots + c_0 x^d$.

2. Let $p(x) = c_d x^d + \cdots + c_\alpha x^\alpha$ with $d \geq \alpha > 0$. Then $p^{\dashv}(x) = x^d \left(c_d \frac{1}{x^d} + \cdots + c_\alpha \frac{1}{x^\alpha}\right) = c_d + \cdots + c_\alpha x^{d-\alpha}$.

3. Assume $x \mid p(x)$. Then, by 2, $d > \deg(p^{\dashv})$, yet $d = \deg(p^{\dashv}) \because p(x) = p^{\dashv}(x)$, a contradiction. □

An alternative way to characterize reciprocal and self-reciprocal polynomials is by their roots.

Theorem 2.2.4. *Let $\mathbb{D}$ be an integral domain, $\mathbb{F}$ the quotient field of $\mathbb{D}$, and $p(x) \in \mathbb{D}[x]$ with nonzero constant coefficient c_0. Let $f(x) \in \mathbb{F}[x]$ be the monic polynomial whose roots are precisely the multiplicative inverses of the roots of $p(x)$ (counting multiplicity). Then $c_0 f(x) = p^{\dashv}(x)$.*

Proof. Let $\overline{\mathbb{F}}$ be the splitting field of $p(x)$ over $\mathbb{F}$. In $\overline{\mathbb{F}}[x]$, suppose $p(x) = c_n(x - z_1)^{\alpha_1} \cdots (x - z_n)^{\alpha_n}$ with the $z_i{}'s$ unique roots of $p(x)$, and α_i the multiplicity of the root z_i for $i = 1 \cdots n$. Let $d \coloneqq \deg(p) = \alpha_1 + \cdots + \alpha_n$. By the definition of f,

$$\begin{aligned}
f(x) &= \left(x - \frac{1}{z_1}\right)^{\alpha_1} \cdots \left(x - \frac{1}{z_n}\right)^{\alpha_n} \\
&= \frac{x^d}{z_1^{\alpha_1} \cdots z_n^{\alpha_n}} \left(z_1 - \frac{1}{x}\right)^{\alpha_1} \cdots \left(z_n - \frac{1}{x}\right)^{\alpha_n} \\
&= \frac{(-1)^d x^d}{z_1^{\alpha_1} \cdots z_n^{\alpha_n}} \left(\frac{1}{x} - z_1\right)^{\alpha_1} \cdots \left(\frac{1}{x} - z_n\right)^{\alpha_n} \\
&= \frac{x^d}{(-1)^d z_1^{\alpha_1} \cdots z_n^{\alpha_n}} \frac{p\left(\frac{1}{x}\right)}{c_n} \\
&= \frac{p^{\dashv}(x)}{c_0}
\end{aligned}$$

□

Theorem 2.2.5. *Let $\mathbb{D}$ be an integral domain and $p(x) \in \mathbb{D}[x]$ such that ± 1 are not roots of $p(x)$. Then $p(x)$ is self-reciprocal if and only if when z is a root of $p(x)$ of multiplicity α, then $\frac{1}{z}$ is also a root of $p(x)$ of multiplicity α.*

Proof. Let $\mathbb{F}$ be the quotient field of $\mathbb{D}$, and let $\overline{\mathbb{F}}$ be the splitting field of $p(x)$ over $\mathbb{F}$.

($\Rightarrow$) Suppose $p(x)$ is self-reciprocal with $d \coloneqq \deg(p)$. By Proposition 2.2.3, all roots of $p(x)$ are nonzero, so the multiplicative inverse of each root of $p(x)$ exists in $\overline{\mathbb{F}}$. Factoring over $\overline{\mathbb{F}}[x]$, say
$p(x) = c(x - z_1)^{\alpha_1} \cdots (x - z_n)^{\alpha_n}$ with the $z_i{}'s$ distinct roots of $p(x)$ each with multiplicity α_i. Consequently,

$$\begin{aligned}
p(x) &= p^{\dashv}(x) \\
&= x^d p\left(\frac{1}{x}\right) \\
&= x^d c \left(\frac{1}{x} - z_1\right)^{\alpha_1} \cdots \left(\frac{1}{x} - z_n\right)^{\alpha_n} \\
&= (-1)^d c z_1^{\alpha_1} \cdots z_n^{\alpha_n} \left(x - \frac{1}{z_1}\right)^{\alpha_1} \cdots \left(x - \frac{1}{z_n}\right)^{\alpha_n}
\end{aligned}$$

So for each root z_i with multiplicity α_i of $p(x)$, it is clear that $\frac{1}{z_i}$ is also a root of $p(x)$ with multiplicity α_i.

($\Leftarrow$) Suppose that when z is a root of $p(x)$ of multiplicity α then $\frac{1}{z}$ is also a root $p(x)$ of multiplicity α, and note z and $\frac{1}{z}$ are distinct since $z \neq \pm 1$. Let c_d be the leading coefficient of $p(x)$, c_0 the constant coeffient of $p(x)$, and let $f(x)$ be the monic polynomial whose roots are precisely the multiplicative inverses of the roots of $p(x)$ (counting multiplicity). Consequently, $c_d f(x) = p(x)$. By Theorem 2.2.4, $f(x) = \frac{p^{\dashv}(x)}{c_0}$ so

$\frac{c_d}{c_0} p^{\dashv}(x) = p(x)$. The fraction $\frac{c_d}{c_0}$ is up to sign the product of the roots of $p(x)$. Therefore, by hypothesis, $\frac{c_d}{c_0} = (-1)^{\deg(p)}$. Also by hypothesis, it is clear that the number of roots, counting multiplicity, of $p(x)$ is even, so $\deg(p)$ is even $\therefore \frac{c_d}{c_0} = 1 \therefore p^{\dashv}(x) = p(x) \therefore p(x)$ is self-reciprocal. □

Theorem 2.2.6 (Cauchy-Mirimanoff Polynomials are self-reciprocal)**.**
Let $n \geq 2$. Then

1. *$\frac{P_n(X)}{X}$ is a self-reciprocal polynomial.*
2. *$E_n(X)$ is a self-reciprocal polynomial.*

Proof.

1. Fix $n \geq 2$. Then

$$\begin{aligned}
\left(\frac{P_n(X)}{X}\right)^{\dashv} &= X^{n-2} \frac{P_n\left(\frac{1}{X}\right)}{\frac{1}{X}} \\
&= X^{n-1}\left(\left(\frac{1}{X}+1\right)^n - \frac{1}{X^n} - 1\right) \\
&= \frac{1}{X}((X+1)^n - 1 - X^n) \\
&= \frac{P_n(X)}{X}
\end{aligned}$$

2. Fix $n \geq 2$, and let z be a root of $E_n(X)$. By Theorem 2.2.1, z is a root of multiplicity one, so by Theorem 2.2.5 it is enough to show $\frac{1}{z}$ is also a root of $E_n(X)$. As z is a root of $E_n(X)$, it is also a root of $P_n(X)$. Clearly, $z \neq 0 \because E_n(X)$ has no real roots, so z is a root of $\frac{P_n(X)}{X}$. Since $\frac{P_n(X)}{X}$ is a self-reciprocal polynomial, $\frac{1}{z}$ is a root of $\frac{P_n(X)}{X}$. As $z \neq -1, \omega$, or ω^2 it follows $\frac{1}{z} \neq -1, \omega$ or $\omega^2 \therefore \frac{1}{z}$ is not a root of $X+1$ or $X^2+X+1 \therefore \frac{1}{z}$ must be a root of $E_n(X)$.

□

2.2.3 Root Orbits of the Cauchy-Mirimanoff Polynomials

Since the Cauchy-Mirimanoff polynomials are self-reciprocal, if z is a root of $E_n(X)$ then $\frac{1}{z}$ is also a root of $E_n(X)$. While this is true for all $n \geq 2$, even more can be said when $n \geq 9$ is odd.

Definition 2.2.7. Let $n \geq 9$ be odd, and let z be a root of $E_n(X)$. The orbit of z, denoted $Orb(z)$, is the set

$$Orb(z) := \left\{z, \frac{1}{z}, -z-1, -\frac{1}{z+1}, -1-\frac{1}{z}, -\frac{z}{z+1}\right\}$$

Theorem 2.2.8. *Let $n \geq 9$ be odd, and let z be a root of $E_n(X)$. Then the elements of $Orb(z)$ are distinct roots of $E_n(X)$.*

Proof. Observe that $P_n(-X-1) = (-X)^n - (-X-1)^n - 1 = P_n(X) \therefore$ if $P_n(z) = 0$ then $P_n(-z-1) = 0$. Consequently, if $E_n(z) = 0$ then $-z-1$ is a root of $P_n(X)$. Since z is not real, $-z-1$ is not real $\therefore -z-1$ is not a root of X or $X+1$. If $-z-1$ were a root of X^2+X+1, then $(-z-1)^2+(-z-1)+1 = z^2+z+1 = 0 \therefore z = \omega$

or ω^2, which is impossible. Therefore, $-z-1$ must be a root of $E_n(X)$. Since $E_n(X)$ is self-reciprocal, $-\frac{1}{z+1}$ is also a root of $E_n(X)$. Similarly, since $\frac{1}{z}$ is a root of $E_n(X)$, the same reasoning shows $-1-\frac{1}{z}$ and $-\frac{z}{z+1}$ are roots of $E_n(X)$.

As $z \neq 1, -2, -\frac{1}{2}, \omega$ or ω^2, a brute force comparison of the elements of $Orb(z)$ verifies that the elements are distinct. □

The set $Orb(z)$ is the orbit of z under the action of the group of unimodular transformations $\mathcal{T} = \{X, \frac{1}{X}, -X-1, -\frac{1}{X+1}, -\frac{X+1}{X}, -\frac{X}{X+1}\}$ on $\mathbb{C} - \{0, -1\}$. The group $\mathcal{T}$ is isomorphic to $\mathfrak{S}_3$, the symmetric group on three elements. By Corollary 2.1.3, for odd $n \geq 9$, the roots of $E_n(X)$ are partitioned into $r_n := \frac{n-3-2e_n}{6}$ orbits. This leads to an important observation in Helou (1997).

Theorem 2.2.9 (Helou (1997) - Lemma 2)**.** *For odd $n \geq 9$, the roots of $E_n(X)$ in $\mathbb{C}$ are partitioned into r_n orbits; and $E_n(X)$ has exactly $2r_n$ roots of absolute value 1, two conjugates in each orbit.*

It is natural to consider whether the elements of a root orbit of $E_n(X)$ are $\mathbb{Q}$-conjugates. So for every root z of $E_n(X)$ in $\mathbb{C}$, let $g_z(X)$ be the monic polynomial with roots the elements of $Orb(z)$.

Definition 2.2.10. Let $J(X) \in \mathbb{Q}(X)$ be the rational function

$$J(X) := \frac{(X^2+X+1)^3}{X^2(X+1)^2}$$

Proposition 2.2.11 (Helou (1997))**.** *Let $n \geq 9$ be odd. For z a root of $E_n(X)$ in $\mathbb{C}$,*

$$g_z(X) = X^6 + 3X^5 + (6 - J(z))X^4 + (7 - 2J(z))X^3 + (6 - J(z))X^2 + 3X + 1$$

All elements of $Orb(z)$ have the same image under J. In particular, if $\theta \not\equiv \pi \pmod{2\pi}$ in $\mathbb{R}$, then $J(e^{\mathrm{i}\theta}) = \frac{(2\cos\theta+1)^3}{2(\cos\theta+1)}$. So, if z is a root of $E_n(X)$, then $J(z) \in \mathbb{R}$ and $g_z \in \mathbb{R}[X]$. In fact, more can be said of $J(z)$.

Proposition 2.2.12 (Helou (1997) - Lemma 3)**.** *For odd $n \geq 9$ and z a root of $E_n(X)$, $J(z)$ is a real algebraic number. If n is a prime, then $J(z)$ is a real algebraic integer.*

Lastly, Helou (1997) gives a lemma which will be used to give a partial answer to whether the elements of $Orb(z)$, for a root z of $E_n(X)$, are $\mathbb{Q}$-conjugates.

Theorem 2.2.13 (Helou (1997) - Lemma 4)**.** *Let $n \geq 9$ be odd, z a root of $E_n(X)$ in $\mathbb{C}$, and $K := \mathbb{Q}(J(z_1), \cdots, J(z_{r_n}))$ where $z_j = e^{\mathrm{i}\theta_j}$ $(1 \leq j \leq r_n)$ are representatives of the root orbits of $E_n(X)$ in $\mathbb{C}$.*

1. *We have $\mathbb{Q}(z) \cap K = \mathbb{Q}(J(z))$ and $Gal(K(z)|K) \simeq Gal(\mathbb{Q}(z)|\mathbb{Q}(J(z))) \simeq \mathcal{T}_z$, where $\mathcal{T}_z$ is a subgroup of $\mathcal{T}$ of order $|\mathcal{T}_z| \in \{2, 6\}$.*
2. *For a $\mathbb{Q}$-conjugate z' of z, $\mathcal{T}_{z'} = \mathcal{T}_z$. The minimal polynomial of z over $\mathbb{Q}$ is the product of $[\mathbb{Q}(J(z)) : \mathbb{Q}]$ minimal polynomials over K of such z' in different orbits.*
3. *If $|\mathcal{T}_z| = 2$ then, for any $z'' \in Orb(z)$, $|\mathcal{T}_{z''}| = 2$; and, if $|z| = 1$ then all the roots of the minimal polynomial of z over $\mathbb{Q}$ have absolute value 1.*

It is not immediately obvious to see how Theorem 2.2.13 gives a partial answer to whether elements of $Orb(z)$ are $\mathbb{Q}$-conjugates of each other. This connection will be made clear through the next results.

Lemma 2.2.14. *Let $n \geq 9$ be odd, and $z \in \mathbb{C}$ a root of $E_n(X)$. Then for any $z' \in Orb(z)$, we have $z' \in \mathbb{Q}(z)$.*

Proof. Straightforward observation. □

Lemma 2.2.15. *Let $n \geq 9$ be odd, and $z \in \mathbb{C}$ a root of $E_n(X)$. Then*

$$\mathbb{Q}(z) = \mathbb{Q}\left(\frac{1}{z}\right) = \mathbb{Q}(-z-1) = \mathbb{Q}\left(-\frac{1}{z+1}\right) = \mathbb{Q}\left(-1-\frac{1}{z}\right) = \mathbb{Q}\left(-\frac{z}{z+1}\right)$$

Proof. Consequence of Lemma 2.2.14. □

Lemma 2.2.16. *Let $n \geq 9$ be odd, and $z \in \mathbb{C}$ a root of $E_n(X)$. Let $z' \in Orb(z)$ be such that there exists $\sigma \in Aut(\mathbb{Q}(z))$ with $\sigma(z) = z'$. Then $\sigma \in Gal(\mathbb{Q}(z)/\mathbb{Q}(J(z)))$.*

Proof. It is enough to show $\sigma(J(z)) = J(z)$. Observe $\sigma(J(z)) = J(\sigma(z)) = J(z')$. As $z' \in Orb(z)$, both z and z' have the same image under J, i.e. $J(z') = J(z) \therefore \sigma(J(z)) = J(z)$. □

Corollary 2.2.17. *Let $n \geq 9$ be odd, $z \in \mathbb{C}$ a root of $E_n(X)$, and $z' \in Orb(z)$ such that $z' \neq z, \overline{z}$. If z and z' are $\mathbb{Q}$-conjugates, then $|\mathcal{T}_z| = 6$.*

Proof. Let $f(x)$ be the minimal polynomial of z over $\mathbb{Q}$, and let K be the splitting field of f. Since z and z' are $\mathbb{Q}$-conjugates, there exists $\sigma \in Gal(K/\mathbb{Q})$ such that $\sigma(z) = z'$. Define $\phi : \mathbb{Q}(z) \to \mathbb{Q}(z') = \mathbb{Q}(z)$ by $\phi := \sigma|_{\mathbb{Q}(z)}$, and note $\phi \in Aut(\mathbb{Q}(z))$. It follows from Lemma 2.2.16 that $\phi \in Gal(\mathbb{Q}(z)/\mathbb{Q}(J(z)))$.

The complex conjugate root theorem guarantees that z and $\overline{z}$ are $\mathbb{Q}$-conjugates, so as in the previous paragraph, there also exists $\gamma \in Gal(\mathbb{Q}(z)/\mathbb{Q}(J(z)))$ such that $\gamma(z) = \overline{z}$. As id, σ, and γ are three distinct elements of $Gal(\mathbb{Q}(z)/\mathbb{Q}(J(z)))$, it follows that $|\mathcal{T}_z| \geq 3$. Consequently, by Theorem 2.2.13 (1), $|\mathcal{T}_z| = 6$. □

Finally, Theorem 2.2.18 and Corollary 2.2.19 make explicit how to use Theorem 2.2.13 to determine if the elements of $Orb(z)$ are $\mathbb{Q}$-conjugates.

Theorem 2.2.18. *Let $n \geq 9$ be odd, and $z := e^{\mathbb{i}\theta}$ be a root of $E_n(X)$. Then the following are equivalent:*

1. $|\mathcal{T}_z| = 2$
2. *The only $\mathbb{Q}$-conjugate of z in $Orb(z)$ is $\frac{1}{z}$.*
3. *The only $\mathbb{Q}$-conjugate of $-z-1$ in $Orb(z)$ is $-1-\frac{1}{z}$.*
4. *The only $\mathbb{Q}$-conjugate of $-\frac{1}{z+1}$ in $Orb(z)$ is $-\frac{z}{z+1}$.*

Proof. $(1 \Rightarrow 2, 3, 4)$ Suppose $|\mathcal{T}_z| = 2$. By the complex conjugate root theorem, z and $\frac{1}{z}$ are $\mathbb{Q}$-conjugates, $-z-1$ and $-1-\frac{1}{z}$ are $\mathbb{Q}$-conjugates, and $-\frac{1}{z+1}$ and $-\frac{z}{z+1}$ are $\mathbb{Q}$-conjugates. By 2.2.13 (3), all $\mathbb{Q}$-conjugates of z have absolute value 1, so the only possible $\mathbb{Q}$-conjugate of z in $Orb(z)$ is $\frac{1}{z}$, which establishes (2).

To establish (3), suppose $-z-1$ had a $\mathbb{Q}$-conjugate other than itself or $-1-\frac{1}{z}$ in $Orb(z)$. Then by Corollary 2.2.17, $|\mathcal{T}_{-z-1}| = 6$, which contradicts Theorem 2.2.13 (3). Similar reasoning establishes (4).
$(1 \Leftarrow 2, 3, 4)$ By Theorem 2.2.13 (1), if $|\mathcal{T}_z| \neq 2$, then $|\mathcal{T}_z| = 6$. So suppose $|\mathcal{T}_z| = 6$. As $Gal(\mathbb{Q}(z)/\mathbb{Q}(J(z))) \subseteq Aut(\mathbb{Q}(z))$, it follows by the Isomorphism Extension Theorem that the elements of $Orb(z)$ are $\mathbb{Q}$-conjugates of each other. As this is prohibited by (2), (3), or (4), it follows $|\mathcal{T}_z| \neq 6 \therefore |\mathcal{T}_z| = 2$. □

Corollary 2.2.19. *Let $n \geq 9$ be odd, and $z \in \mathbb{C}$ be a root of $E_n(X)$. Then $|\mathcal{T}_z| = 6$ if and only if the elements of $Orb(z)$ are $\mathbb{Q}$-conjugates.*

Proof. $(\Rightarrow)$ Established in the proof of Theorem 2.2.18 for the $(\Leftarrow)$-direction.
$(\Leftarrow)$ Consequence of Corollary 2.2.17. □

2.3 Factors of $E_n(X)$

2.3.1 Self-Reciprocal Polynomials Revisited

Theorem 2.3.1. *Suppose $\pm 1 \neq z \in \mathbb{C}$ such that $|z| = 1$. If z is algebraic over $\mathbb{Q}$, then the minimal polynomial of z over $\mathbb{Q}$ is a self-reciprocal polynomial of even degree.*

Proof. Since $z \neq \pm 1$ and $|z| = 1$, it follows that $z \neq \overline{z}$ and $\overline{z} = \frac{1}{z}$. Let $f(x)$ be the minimal polynomial of z over $\mathbb{Q}$, and define $d \coloneqq \deg(f)$. Observe $f^{\dashv}(z) = z^d f(\frac{1}{z}) = z^d f(\overline{z}) = z^d \overline{f(z)} = 0 \therefore z$ is a root of $f^{\dashv}(x)$. If $f(0) = 0$, then $x \mid f(x) \therefore f(x) = x$ because $f(x)$ is monic and irreducible. The only root of $f(x) = x$ is 0, which contradicts the hypothesis that $f(x)$ is the minimal polynomial of z with $|z| = 1$. So $f(0) \neq 0 \therefore \deg(f) = \deg(f^{\dashv})$ by Proposition 2.2.3.

Because $f(x)$ is the minimal polynomial of z, it follows $f(x) \mid f^{\dashv}(x) \therefore f(x)h(x) = f^{\dashv}(x)$ for some $h(x) \in \mathbb{Q}[x]$. As $\deg(f) = \deg(f^{\dashv})$, it follows $\deg(h) = 0 \therefore h(x) = q$ for some $0 \neq q \in \mathbb{Q} \therefore qf(x) = f^{\dashv}(x)$.

Let z' be any root of $f(x)$. Then $\frac{1}{z'} \in \mathbb{C}$ ($\because z' \neq 0$), $z' \neq \frac{1}{z'}$ ($\because z' \neq \pm 1$), and $\frac{1}{z'}$ is a root of $f(x)$ ($\because f(\frac{1}{z'}) = q^{-1}(\frac{1}{z'})^d f(z') = 0$). Therefore, the roots of $f(x)$ may be partitioned into sets of order 2 consisting of a complex number and its multiplicative inverse. In particular, the degree, d, of $f(x)$ is even and the product of the roots is 1. Consequently, $f(0) = 1$.

The leading coefficient of $qf(x)$ is q because $f(x)$ is monic. As $f(0) \neq 0$, the leading coefficient of $f^{\dashv}(x)$ equals the constant coefficient of $f(x) \therefore$ the leading coefficient of $f^{\dashv}(x)$ is 1. Because $qf(x) = f^{\dashv}(x)$ and the leading coefficients must be equal, $q = 1 \therefore f(x) = f^{\dashv}(x) \therefore f(x)$ is self-reciprocal. □

This theorem provides information about any possible factors of the Cauchy-Mirimanoff Polynomials. Indeed, a necessary condition that the Cauchy-Mirimanoff polynomials be irreducible is that all the elements in $Orb(z)$ for any root z of $E_n(X)$ are $\mathbb{Q}$-conjugates of each other. As the next two corollaries show, this condition is equivalent to checking that factors of $E_n(X)$ are self-reciprocal.

Corollary 2.3.2. *Let $n \geq 9$ be odd. Then at least one irreducible factor of $E_n(X)$ over $\mathbb{Q}$ (or $\mathbb{Z}$) is self-reciprocal.*

Proof. By Theorem 2.2.9, there exists at least one root z of $E_n(X)$ such that $|z| = 1$. Let $f(x)$ be the minimal polynomial of z, and note that $f(x)$ is an irreducible factor of $E_n(X)$. By Theorem 2.3.1, $f(x)$ is self-reciprocal. □

Corollary 2.3.3. *Let $n \geq 9$ be odd. If $|\mathcal{T}_z| = 6$ for all roots z of $E_n(X)$, then all irreducible factors of $E_n(X)$ over $\mathbb{Q}$ (or $\mathbb{Z}$) are self-reciprocal polynomials.*

Proof. Suppose $|\mathcal{T}_z| = 6$ for all roots of $E_n(X)$. Let z be a root of $E_n(X)$. By Corollary 2.2.19, every element of $Orb(z)$ is a $\mathbb{Q}$-conjugate of z. Consequently, by Theorem 2.2.9, there are at least two $\mathbb{Q}$-conjugates of z with absolute value 1. Therefore, the minimal polynomial of z, which is an irreducible factor of $E_n(X)$ over $\mathbb{Q}$, is a self-reciprocal polynomial by Theorem 2.3.1. □

This shows that techniques used to study self-reciprocal polynomials could be helpful in determining the irrreducibility or reducibility of the Cauchy-Mirimanoff polynomials.

Theorem 2.3.4 (Helou (1997) - Proposition 2)**.** *For prime $n \geq 11$ and any root z of $E_n(X)$ in $\mathbb{C}$, $g_z(x)$ is irreducible over $\mathbb{Q}(J(z))$ and $Gal(\mathbb{Q}(z) \mid \mathbb{Q}(J(z))) \simeq \mathfrak{G}_3$. Any irreducible factor of $E_n(X)$ over $\mathbb{Q}$ is a product of some of the g_z's.*

Corollary 2.3.5. *Let $p \geq 11$ be prime. All irreducible factors of $E_p(X)$ are self-reciprocal.*

Proof. From Theorem 2.3.4, for any root z of $E_n(X)$ it follows that $|\mathcal{T}_z| = 6$. The result is immediate from Corollary 2.3.3. □

2.3.2 Reduction Modulo a Prime

Often, to test the irreducibility of a polynomial, it is useful to consider the polynomial over $\mathbb{F}_p$ for a prime p. It is well-known that if a primitive polynomial (:= a polynomial such that the greatest common denominator of the coefficients is 1) over $\mathbb{Z}[X]$ is irreducible over $\mathbb{F}_p[X]$ for some prime p, then the polynomial is irreducible over $\mathbb{Z}[X]$. Of course, the converse isn't true. In other words, there exist primitive polynomials that are irreducible over $\mathbb{Z}[X]$, yet are reducible modulo every prime (the cyclotomic polynomials are such a class of polynomials). Helou (1997) considered the Cauchy-Mirimanoff polynomials modulo a prime.

Theorem 2.3.6 (Helou (1997) - Lemma 6)**.** *Let $f \in \mathbb{Z}[X]$ be a self-reciprocal polynomial such that there exists z in $\mathbb{C} - \{0, -1\}$ for which Orb(z) consists of six distinct roots of f. Then f is reducible modulo every prime p.*

Definition 2.3.7. Let $f(x) \in \mathbb{Z}[x]$ and p a prime. The reduction of $f(x)$ modulo p, denoted $\underline{f(x)}$, is the polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$ whose coefficients equal the coefficients of $f(x)$ reduced modulo p.

Helou applied Theorem 2.3.6 to obtain the next two results.

Corollary 2.3.8 (Helou (1997) - Lemma 6)**.** *For odd $n \geq 9$ and any prime number p, E_n is reducible modulo p.*

Corollary 2.3.9 (Helou (1997) - Proposition 3)**.** *Let n be a prime ≥ 11. If, for some prime p, $\underline{E_n}$ has at most 3 irreducible factors in $\mathbb{F}_p[X]$, then E_n is irreducible in $\mathbb{Q}[X]$.*

One might wonder how relevant Corollary 2.3.9 is to testing the irreducibility of the Cauchy-Mirimanoff polynomials. If the hypothesis of Corollary 2.3.9 is satisfied frequently, then Corollary 2.3.9 provides a compelling way to try to prove that the Cauchy-Mirimanoff polynomials are irreducible. After performing a series of numerical calculations on the Cauchy-Mirimanoff polynomials, summarized in Table A.1 in Appendix A, the following conjecture seems reasonable.

Conjecture 2.3.10. *Let $n \geq 9$ be odd. Then there exists a prime p such that $\underline{E_n}$ is a product of exactly two irreducible polynomials over $\mathbb{F}_p$.*

Of course, there is no reason to expect a theorem such as this to hold when n is even. In fact, the numerical evidence, summarized in Table A.2 also in Appendix A, would suggest the following conjecture when n is even.

Conjecture 2.3.11. *Let $n \geq 8$ be even. Then there exists a prime p such that $\underline{E_n}$ is irreducible over $\mathbb{F}_p$.*

The above, if true, would also provide structure information on the Galois groups of the Cauchy-Mirimanoff polynomials via Chebotarev's Density Theorem.

2.3.3 Bounds on the Degrees of Factors of the Cauchy-Mirimanoff Polynomials

If n is a prime, then Theorem 2.3.4 implies that every irreducible factor of $E_n(X)$ has degree ≥ 6. Tzermias (2007) improves this result for certain primes.

Theorem 2.3.12 (Tzermias (2007) - Theorem 1.1)**.** *Let p be a prime such that $p \equiv 2 \pmod 3$ and $p \geq 17$.*

1. *Every irreducible factor of $E_p(X)$ over $\mathbb{Q}$ is of degree at least 12.*
2. *For $p \geq 23$, $E_p(X)$ has an irreducible factor of degree $d \geq 18$.*

In a recent paper, Tzermias (2009), similar results are found for primes $p \equiv 1 \pmod 3$.

Theorem 2.3.13 (Tzermias (2009))**.** *Let S be the set of primes greater than or equal to 19 and congruent to 1 (mod 3). There exists an effectively computable subset S_0 of S with S_0 having at most 6 elements and such that, for any p in $S \setminus S_0$, the polynomial $E_p(X)$ has no irreducible factor of degree $d \leq 11$ over $\mathbb{Q}$.*

Theorem 2.3.14 (Tzermias (2009))**.** *Let p be a prime congruent to 1 (mod 3). Suppose that there exists a prime $q \geq 11$ such that $p \equiv 1 \pmod q$ and $p \not\equiv 1 \pmod{q^2}$. Then $E_p(X)$ has an irreducible factor of degree $d \geq 6\left\lfloor \frac{q}{3} \right\rfloor$ over $\mathbb{Q}$.*

2.4 Other Results

A couple of results remain that are certainly worth note. While these results will not be directly used in this dissertation, they are nonetheless important in the study of the Cauchy-Mirimanoff polynomials.

2.4.1 The Cauchy-Mirimanoff polynomials are relatively prime

In an application to the Korteweg-de Vries equation, Beukers (1997) proved the following theorem:

Theorem 2.4.1 (Beukers (1997) - Theorem 4.1)**.** *For all $1 < m < n$, $(E_n(X), E_m(X)) = 1$.*

An additional result of interest from Beukers (1997) relates to the location of the zeros of $P_n(X)$.

Theorem 2.4.2 (Beukers (1997) - Lemma 2.1)**.** *The number of distinct zeros z of $P_k(X)$ on the unit circle such that $z^2 + z + 1 \neq 0$ is at least $[\frac{2k}{3}] - [\frac{k}{3}] - 1$. In particular, if $k \neq 2, 3, 5, 7$ there exists a zero z on the unit circle such that $|z + 1| < 0.5$.*

2.4.2 $E_{2p}(X)$ is irreducible for all primes p

While numerical tests have shown that the Cauchy-Mirimanoff polynomials $E_n(X)$ are irreducible for at least all $n \leq 100$, almost no general irreducibility results are known. The first exception, attributed to Michael Filaseta, was proved in Helou (1997).

Theorem 2.4.3 (Helou (1997) - Proposition 4)**.** *For any odd prime p, E_{2p} is irreducible over $\mathbb{Q}$.*

The proof of this theorem used Newton Polygons to establish the form of any possible factorization of E_{2p}, and then a number-theoretic calculation to show that no factorization was possible.

2.4.3 A Generalization of the Irreducibility of $E_{2p}(X)$

In a thesis under revision, Nanninga (2009) announced a proof that $E_n(X)$ is irreducible when $n = 2^k m$ where m is an odd integer and $k \in \{1, 2, 3, 4, 5\}$. The proof has not yet been made available.

Chapter 3

Chebyshev Polynomials

While there are many excellent resources and even entire books devoted to the Chebyshev Polynomials, the results needed do not appear in the literature. All standard results on Chebyshev polynomials will simply be quoted and can be found in either of the excellent books Mason and Handscomb (2003) or Rivlin (1990).

3.1 The Fractional, Half-Fractional, and Modified Half-Fractional Chebyshev Polynomials

Recall the classic definition of the Chebyshev Polynomials (of the first kind):

Definition 3.1.1 (Chebyshev Polynomial)**.** The n^{th}*-Chebyshev Polynomial*, $T_n(X)$, is defined as

$$T_n(x) := \cos n\theta$$

where n is a nonnegative integer, $x = \cos\theta$, and $0 \leq \theta \leq \pi$.

The definition is often abbreviated by $T_n(X) = \cos(n \arccos(X))$. By de Moivre's Theorem, $\cos(n\theta)$ is a polynomial of degree n in $\cos(\theta)$, and making the substitution $x = \cos(\theta)$ gives the polynomial form of $T_n(X)$. The first six Chebyshev Polynomials are as follows:

$$\begin{aligned} T_0(x) &= 1 \\ T_1(x) &= x \\ T_2(x) &= 2x^2 - 1 \\ T_3(x) &= 4x^3 - 3x \\ T_4(x) &= 8x^4 - 8x^2 + 1 \\ T_5(x) &= 16x^5 - 20x^3 + 5x \end{aligned}$$

The choice of n as a nonnegative integer guarantees $T_n(X)$ is a polynomial in X. However, if one is willing to forgo the guarantee that $T_n(X)$ be a polynomial, then it is reasonable to consider any $n \in \mathbb{R}$. This leads to the definition of Fractional Chebyshev Polynomials.

Definition 3.1.2 (Fractional Chebyshev Polynomial)**.** The *q^{th}-Fractional Chebyshev Polynomial*, $T_q(X)$, is defined as

$$T_q(x) \coloneqq \cos(q \arccos x)$$

where $q \in \mathbb{Q}$, and $x \in [-1, 1]$.

It is unusual to call functions "polynomials" when they are not actually polynomials. This strange naming convention is meant to highlight the close relationship of these functions to the Chebyshev Polynomials, rather than indicate a specific form of the function. Additionally, for the sake of clarity, the standard Chebyshev Polynomials will sometimes be called the *Integral Chebyshev Polynomials*.

For the purposes at hand, it will be enough to consider a particular subclass of the Fractional Chebyshev Polynomials, called the Half-Fractional Chebyshev Polynomials.

Definition 3.1.3 (Half-Fractional Chebyshev Polynomial)**.** The *n^{th} Half-Fractional Chebyshev Polynomial*, $T_{\frac{n}{2}}(X)$, is defined as

$$T_{\frac{n}{2}}(x) \coloneqq \cos\left(\frac{n}{2} \arccos x\right)$$

where n is a nonnegative integer, and $x \in [-1, 1]$.

It should be clear that if n is even, then the Half-Fractional Chebyshev Polynomial is an Integral Chebyshev Polynomial; and if n is odd, then the Half-Fractional Chebyshev Polynomial is not a polynomial.

There is one last modification to consider. On the surface, Definition 3.1.4 appears to be a trivial modification to Half-Fractional Chebyshev Polynomials, but the change will be important later.

Definition 3.1.4 (Modified Half-Fractional Chebyshev Polynomial)**.** The *n^{th} Modified Half-Fractional Chebyshev Polynomial*, $C_{\frac{n}{2}}(X)$, is defined as

$$C_{\frac{n}{2}}(x) \coloneqq 2T_{\frac{n}{2}}\left(\frac{x}{2}\right)$$

where n is a nonnegative integer, and $x \in [-2, 2]$.

Of course, the *Modified Integral Chebyshev Polynomials*, and the *Modified Fractional Chebyshev Polynomials* are similarly defined. It also worth mention that $C_n(x) \coloneqq 2T_n\left(\frac{x}{2}\right)$ is the Dickson polynomial $D_n(x, 1)$ for nonnegative integers n.

3.2 Properties of the Half-Fractional and Modified Half-Fractional Chebyshev Polynomials

The modification to the definition of the Integral Chebyshev Polynomials yielding the Half-Fractional Chebyshev Polynomials makes it clear that the two collections of functions are related, yet the relationship is even closer than apparent at first blush.

Theorem 3.2.1. *For any nonnegative integer n, and $x \in [-1, 1]$*

$$T_{\frac{n}{2}}(x) = T_n\left(\frac{\sqrt{2x+2}}{2}\right)$$

Proof. Let $\theta := \arccos \frac{\sqrt{2x+2}}{2}$. Then

$$\theta = \arccos \frac{\sqrt{2x+2}}{2} \Leftrightarrow \cos\theta = \frac{\sqrt{2x+2}}{2} \Leftrightarrow 2\cos^2\theta - 1 = x \Leftrightarrow \cos(2\theta) = x \Leftrightarrow \theta = \frac{\arccos x}{2}$$

Consequently,

$$\begin{aligned} \arccos \frac{\sqrt{2x+2}}{2} &= \frac{\arccos x}{2} \\ \Rightarrow \cos\left(n \arccos \frac{\sqrt{2x+2}}{2}\right) &= \cos\left(\frac{n}{2} \arccos x\right) \\ \Rightarrow T_n\left(\frac{\sqrt{2x+2}}{2}\right) &= T_{\frac{n}{2}}(x) \end{aligned}$$

□

Some ambiguity in Theorem 3.2.1 may be perceived if n is even. However, let $n = 2k$. Using the "Nesting Property" of Chebyshev Polynomials, $T_{\frac{2k}{2}}(x) = T_{2k}\left(\frac{\sqrt{2x+2}}{2}\right) = T_k\left(T_2\left(\frac{\sqrt{2x+2}}{2}\right)\right) = T_k(x)$ as expected.

Corollary 3.2.2. *For any nonnegative integer n, and $x \in [-2, 2]$*

$$C_{\frac{n}{2}}(x) = 2T_n\left(\frac{\sqrt{x+2}}{2}\right)$$

Proof. Immediate from Definition 3.1.4 and Theorem 3.2.1. □

In the case of odd n, Theorem 3.2.1 gives an effective way to generate the Half-Fractional Chebyshev Polynomials. The first five odd Half-Fractional Chebyshev Polynomials are

$$\begin{aligned} T_{\frac{1}{2}}(x) &= \frac{\sqrt{2x+2}}{2} \\ T_{\frac{3}{2}}(x) &= \frac{\sqrt{2x+2}}{2}(2x-1) \\ T_{\frac{5}{2}}(x) &= \frac{\sqrt{2x+2}}{2}(4x^2-2x-1) \\ T_{\frac{7}{2}}(x) &= \frac{\sqrt{2x+2}}{2}(8x^3-4x^2-4x+1) \\ T_{\frac{9}{2}}(x) &= \frac{\sqrt{2x+2}}{2}(16x^4-8x^3-12x^2+4x+1) \end{aligned}$$

This suggests that the Half-Fractional Chebyshev Polynomials are always of the form $\frac{\sqrt{2x+2}}{2}$ times a polynomial. This is, in fact, true.

Theorem 3.2.3. *Let n be an odd nonnegative integer. Then*

$$T_{\frac{n}{2}}(x) = \frac{\sqrt{2x+2}}{2} f_n(x)$$

with $f_n(x) \in \mathbb{Z}[x]$.

Proof. By Theorem 3.2.1, $T_{\frac{n}{2}}(x) = T_n\left(\frac{\sqrt{2x+2}}{2}\right)$. By Definition 3.1.4, $T_{\frac{n}{2}}(x) = \frac{1}{2}C_n\left(\sqrt{2x+2}\right)$. It is known that $C_n(X) \in \mathbb{Z}[X]$ (see Rivlin (1990) - Theorem 5.5 and Lemma 5.2.2), and $C_n(X)$ is an odd function (see Rivlin (1990) - Equation 1.13). Consequently, $C_n(X) = X\tau(X^2)$ for some $\tau \in \mathbb{Z}[X]$. Therefore, $T_{\frac{n}{2}}(x) = \frac{1}{2}C_n\left(\sqrt{2x+2}\right) = \frac{\sqrt{2x+2}}{2}\tau(2x+2)$, where clearly $\tau(2x+2) \in \mathbb{Z}[x]$. Define $f(x) \coloneqq \tau(2x+2)$ to obtain the desired result. □

Once the polynomial form is known for the Integral Chebyshev Polynomials, the domain of the Integral Chebyshev Polynomials is extended to all of $\mathbb{R}$ or even all of $\mathbb{C}$, as these are valid for polynomials. The same now will be done for the Half-Fractional Chebyshev Polynomials. With this consideration, the domain for the Integral and Half-Fractional Chebyshev Polynomials will no longer be explicitly mentioned.

A known result for nonnegative integers n, is $C_n(X + X^{-1}) = X^n + X^{-n}$ (see Rivlin (1990) - Exercise 5.2.22). This is now generalized to Modified Half-Fractional Chebyshev Polynomials.

Theorem 3.2.4. *For any nonnegative integer n,*

$$C_{\frac{n}{2}}(x + x^{-1}) = x^{\frac{n}{2}} + x^{-\frac{n}{2}}$$

Proof. By Corollary 3.2.2,

$$C_{\frac{n}{2}}(x + x^{-1}) = 2T_n\left(\frac{\sqrt{x + x^{-1} + 2}}{2}\right)$$

For all nonnegative integers n, a well-known identity for Integral Chebyshev Polynomials is (see Rivlin (1990) - Exercise 1.1.1)

$$T_n(x) = \frac{(x - \sqrt{x^2-1})^n + (x + \sqrt{x^2-1})^n}{2}$$

Consequently,

$$\begin{aligned}
C_{\frac{n}{2}}(x + x^{-1}) &= 2T_n\left(\frac{\sqrt{x + x^{-1} + 2}}{2}\right) \\
&= \left(\frac{\sqrt{x + x^{-1} + 2}}{2} - \sqrt{\left(\frac{\sqrt{x + x^{-1} + 2}}{2}\right)^2 - 1}\right)^n + \left(\frac{\sqrt{x + x^{-1} + 2}}{2} + \sqrt{\left(\frac{\sqrt{x + x^{-1} + 2}}{2}\right)^2 - 1}\right)^n \\
&= \left(\frac{\sqrt{x + x^{-1} + 2}}{2} - \sqrt{\frac{x + x^{-1} + 2}{4} - 1}\right)^n + \left(\frac{\sqrt{x + x^{-1} + 2}}{2} + \sqrt{\frac{x + x^{-1} + 2}{4} - 1}\right)^n \\
&= \left(\frac{\sqrt{x + x^{-1} + 2}}{2} - \sqrt{\frac{x + x^{-1} - 2}{4}}\right)^n + \left(\frac{\sqrt{x + x^{-1} + 2}}{2} + \sqrt{\frac{x + x^{-1} - 2}{4}}\right)^n
\end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{\sqrt{x+x^{-1}+2}}{2} - \frac{\sqrt{x+x^{-1}-2}}{2}\right)^n + \left(\frac{\sqrt{x+x^{-1}+2}}{2} + \frac{\sqrt{x+x^{-1}-2}}{2}\right)^n \\
&= \left(\frac{\sqrt{\left(x^{\frac{1}{2}}+x^{-\frac{1}{2}}\right)^2}}{2} - \frac{\sqrt{\left(x^{\frac{1}{2}}-x^{-\frac{1}{2}}\right)^2}}{2}\right)^n + \left(\frac{\sqrt{\left(x^{\frac{1}{2}}+x^{-\frac{1}{2}}\right)^2}}{2} + \frac{\sqrt{\left(x^{\frac{1}{2}}-x^{-\frac{1}{2}}\right)^2}}{2}\right)^n \\
&= \left(\frac{x^{\frac{1}{2}}+x^{-\frac{1}{2}}}{2} - \frac{x^{\frac{1}{2}}-x^{-\frac{1}{2}}}{2}\right)^n + \left(\frac{x^{\frac{1}{2}}+x^{-\frac{1}{2}}}{2} + \frac{x^{\frac{1}{2}}-x^{-\frac{1}{2}}}{2}\right)^n \\
&= x^{\frac{n}{2}} + x^{-\frac{n}{2}}
\end{aligned}
$$

□

Chapter 4

The Reciprocal Transform of the Cauchy-Mirimanoff Polynomials

Over the last two hundred years, there have been many papers and results giving tests to apply to a polynomial to determine irreducibility. The difficulty in testing the irreducibility of the Cauchy-Mirimanoff Polynomials is that these polynomials, and their translates, seem to satisfy none of the hypotheses of any known tests. So instead of studying the Cauchy-Mirimanoff Polynomials directly, the reciprocal transform is defined and studied.

4.1 The Reciprocal Transform of a Self-Reciprocal Polynomial

4.1.1 Definition of the Reciprocal Transform of a Self-Reciprocal Polynomial

Theorem 4.1.1. *Let $\mathbb{D}$ be an integral domain and $f(x) \in \mathbb{D}[x]$ a self-reciprocal polynomial with* $\deg(f) = 2k$ *for some $k \in \mathbb{Z}$. Then there exists a unique polynomial $f^*(x) \in \mathbb{D}[x]$ such that*

$$f(x) = x^k f^*(x + x^{-1})$$

Proof. Uniqueness is straightforward. For existence, suppose

$$f(x) = a_{2k}x^{2k} + a_{2k-1}x^{2k-1} + \cdots + a_1 x + a_0 \tag{4.1}$$

with each $a_i \in \mathbb{D}$. Since $a_{2k-j} = a_j$ for each $j = 0, 1, \cdots, k$, Equation 4.1 may be rearranged as

$$\begin{aligned} f(x) &= \sum_{j=0}^{k-1} a_j(x^{2k-j} + x^j) + a_k x^k && (4.2)\\ &= x^k\left(\sum_{j=0}^{k-1} a_j(x^{k-j} + \frac{1}{x^{k-j}}) + a_k\right) && (4.3)\\ &= x^k\left(\sum_{j=0}^{k-1} a_j C_{k-j}\left(x + \frac{1}{x}\right) + a_k\right) && (4.4) \end{aligned}$$

As mentioned in the proof of Theorem 3.2.3, it is known that $C_n(x) \in \mathbb{Z}[x]$, so the coefficients of C_n in Equation 4.4 may be interpreted appropriately in $\mathbb{D}$ (i.e. as a sum of ± 1's). Thus, define

$$f^*(x) \coloneqq \sum_{j=0}^{k-1} a_j C_{k-j}(x) + a_k$$

where $\deg(f^*) = k$. □

The existence of f^* has been known for at least a century, but there is no universal agreement to notation or name.

Definition 4.1.2 (Reciprocal Transform of a Self-Reciprocal Polynomial)**.** Let $\mathbb{D}$ be an integral domain, $f(x) \in \mathbb{D}[x]$ a self-reciprocal polynomial of even degree, and $d \coloneqq \deg(f)$. The *reciprocal transform of* f is the unique polynomial $f^*(x) \in \mathbb{D}[x]$ with $\deg(f^*) = \frac{d}{2}$ such that

$$f(x) = x^{\frac{d}{2}} f^*(x + x^{-1})$$

4.1.2 Dickson's Theorem

It is natural to consider how the factorization of a polynomial is related to the factorization of its reciprocal transform.

Theorem 4.1.3 (Dickson (1908))**.** *Let $\mathbb{F}$ be a field, and $f(x) \in \mathbb{F}[x]$ a self-reciprocal polynomial such that $f(\pm 1) \neq 0$ and $\deg(f) = 2k$ for some $k \in \mathbb{Z}$. Then f(x) is irreducible over $\mathbb{F}$ if and only if*

1. *$f^*(x)$ is irreducible over $\mathbb{F}$, and*
2. *$f(x)$ is not a product of two distinct irreducible polynomials, each of degree k.*

Further commenting on Condition 2, if $f^*(x)$ is irreducible over $\mathbb{F}$ and $f(x) = g(x)h(x)$ is a product of two distinct irreducible polynomials, then the roots of h are the reciprocals of the roots of g. In other words, there exists a $\lambda \in \mathbb{F}$ and $g(x) \in \mathbb{F}[x]$ such that $f(x) = \lambda g(x) g^{\dashv}(x)$.

Moreover, $g(x)$ and $g^{\dashv}(x)$ are not self-reciprocal polynomials. On the contrary, if $g(x)$ is a self-reciprocal polynomial, then $g^{\dashv}(x)$ is also a self-reciprocal polynomial and both $\deg(g)$ and $\deg(g^{\dashv})$ are even integers (consequently the reciprocal transforms exist giving a factorization to $f^*(x)$). That the degrees are even follows from the hypothesis that $g(\pm 1) \neq 0$ and $g^{\dashv}(\pm 1) \neq 0$, and the fact that every irreducible self-reciprocal polynomial over $\mathbb{F}$, except $X + 1$, has even degree. For if z is a root of a self-reciprocal polynomial, then $\frac{1}{z}$ is also a root, so the roots of a self-reciprocal polynomial come in pairs unless $z = \frac{1}{z}$. This condition occurs if and only if $z = \pm 1$ is a root of the polynomial; the minimal polynomial of 1 is $X - 1$ and is not self-reciprocal unless $char(\mathbb{F}) = 2$, and the minimal polynomial of -1 is $X + 1$. Thus, the only irreducible self-reciprocal polynomial of odd degree is $X + 1$.

If the hypothesis that $f(\pm 1) \neq 0$ is dropped in Theorem 4.1.3, then the statement remains true if the word "distinct" is dropped in Condition 2. Moreover, in this case, there is no guarantee that the two polynomials of Condition 2 are non-self-reciprocal. For an example, consider $f(x) = x^2 + 2x + 1 = (x + 1)^2$ over $\mathbb{Q}$ with $f^*(x) = x + 2$.

After Dickson (1908), a number of papers have appeared on the topic including Kleiman (1974) and Meyn (1990).

4.2 The Reciprocal Transforms of the Cauchy-Mirimanoff Polynomials

By Theorem 2.2.6, the Cauchy-Mirimanoff Polynomials are self-reciprocal, so their reciprocal transform exists. In this section, an equation for this reciprocal transform is found and studied.

4.2.1 An Equation for the Reciprocal Transform of the Cauchy-Mirimanoff Polynomials

Theorem 4.2.1 (The Reciprocal Transform of the Cauchy-Mirimanoff Polynomials)**.** *For any integer $n \geq 2$, the reciprocal transform of $E_n(x)$ is given by*

$$E_n^*(x) = \frac{(x+2)^{\frac{n}{2}} - 2T_n\left(\frac{\sqrt{x+2}}{2}\right)}{\left(\sqrt{x+2}\right)^{\epsilon_n}(x+1)^{e_n}} \tag{4.5}$$

where for even n, $\epsilon_n = e_n = 0$; for odd n, $\epsilon_n = 1$ and $e_n = 0$, 1, or 2 according as $n \equiv 0$, 2, or 1 (mod 3).

Proof. Consider the function f_n^* defined by

$$f_n^*(x) \coloneqq \frac{(x+2)^{\frac{n}{2}} - C_{\frac{n}{2}}(x)}{\left(\sqrt{x+2}\right)^{\epsilon_n}(x+1)^{e_n}}$$

Now using Corollary 2.1.3, Definition 4.1.2, and Theorem 3.2.4, if n is even, then

$$\begin{aligned} x^{\frac{n-2}{2}} f_n^*\left(x+\frac{1}{x}\right) &= x^{\frac{n-2}{2}}\left(\left(x+\frac{1}{x}+2\right)^{\frac{n}{2}} - C_{\frac{n}{2}}\left(x+\frac{1}{x}\right)\right) \\ &= x^{\frac{n-2}{2}}\left(x^{-\frac{n}{2}}(x^2+2x+1)^{\frac{n}{2}} - x^{\frac{n}{2}} - x^{-\frac{n}{2}}\right) \\ &= x^{-1}((x+1)^n - x^n - 1) \\ &= E_n(x) \end{aligned}$$

On the other hand, if n is odd, then

$$\begin{aligned} x^{\frac{n-3-2e_n}{2}} f_n^*\left(x+\frac{1}{x}\right) &= x^{\frac{n-3-2e_n}{2}}\left(\frac{\left(x+\frac{1}{x}+2\right)^{\frac{n}{2}} - C_{\frac{n}{2}}\left(x+\frac{1}{x}\right)}{\sqrt{x+\frac{1}{x}+2}\left(x+\frac{1}{x}+1\right)^{e_n}}\right) \\ &= x^{\frac{n-3-2e_n}{2}}\left(\frac{x^{-\frac{n}{2}}\left(x^2+2x+1\right)^{\frac{n}{2}} - x^{\frac{n}{2}} - x^{-\frac{n}{2}}}{x^{-\frac{1}{2}-e_n}\sqrt{x^2+2x+1}\,(x^2+x+1)^{e_n}}\right) \\ &= x^{-1}\left(\frac{\left(x^2+2x+1\right)^{\frac{n}{2}} - x^n - 1}{\sqrt{x^2+2x+1}\,(x^2+x+1)^{e_n}}\right) \\ &= x^{-1}\left(\frac{(x+1)^n - x^n - 1}{(x+1)\,(x^2+x+1)^{e_n}}\right) \\ &= E_n(x) \end{aligned}$$

In either case, f_n^* is a reciprocal transform of E_n $\therefore$ E_n^* is the reciprocal transform of E_n. □

Corollary 4.2.2. *Let $n \geq 2$ be an integer.*

1. *If n is even, then* $\deg(E_n^*) = \frac{n-2}{2}$
2. *If n is odd, then* $\deg(E_n^*) = \frac{n-3-2e_n}{2}$

Proof. Immediate from Corollary 2.1.3. □

4.2.2 Roots of $E_n^*(x)$ and its Translates

Everything known about the roots of the Cauchy-Mirimanoff Polynomials may be translated to information about the roots of the reciprocal transform.

Proposition 4.2.3. *Let $n \geq 9$ be an odd integer. If $e^{\mathbb{i}\theta}$ is a root of $E_n(x)$, then $r \coloneqq 2\cos\theta$ is a real root of $E_n^*(x)$ such that $-2 \leq r \leq -1$.*

Proof. Suppose $e^{\mathbb{i}\theta}$ is a root of $E_n(x)$. This implies, by Defintion 4.1.2, that $r \coloneqq 2\cos\theta = e^{\mathbb{i}\theta} + e^{-\mathbb{i}\theta}$ is a root of $E_n^*(x)$. In Helou (1997), it was shown $\frac{\theta}{2} \in \left(\frac{\pi}{3}, \frac{\pi}{2}\right)$. Consequently, $\theta \in \left(\frac{2\pi}{3}, \pi\right) \therefore \cos\theta \in \left(-1, -\frac{1}{2}\right) \therefore 2\cos\theta \in (-2, -1)$. □

In Section 2.2.3, it is shown for odd n that the roots of $E_n(x)$ can be partitioned into orbits, each of which contains two roots of $E_n(x)$ of absolute value 1. The partitioning of the roots of $E_n(x)$ induces a partition of roots of $E_n^*(x)$. The "parts" of the induced partition of the roots of $E_n^*(x)$ will be called the *root orbits of* $E_n^*(x)$ to emphasize the relationship with the orbits of roots of $E_n(x)$.

Definition 4.2.4. Let $n \geq 9$ be an odd integer, and $z \coloneqq e^{\mathbb{i}\theta}$ be a root of $E_n(x)$. Then $Orb^*(z)$ is the set

$$Orb^*(z) \coloneqq \left\{2\cos\theta, -e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta} - 1}, -e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta} - 1}\right\}$$

Theorem 4.2.5. *Let $n \geq 9$ be an odd integer, and $z \coloneqq e^{\mathbb{i}\theta}$ be a root of $E_n(x)$. Then the root orbit of $E_n^*(x)$ induced by $Orb(z)$ is $Orb^*(z)$, and $Orb^*(z)$ consists of three distinct roots, one real and two complex conjugates, of $E_n^*(x)$.*

Proof. Considering each root of $Orb(z)$ separately, we find the corresponding root of $E_n^*(x)$.

1. $e^{\mathbb{i}\theta} \in Orb(z)$: Then $e^{\mathbb{i}\theta} + e^{-\mathbb{i}\theta} = 2\cos\theta$ is a root of $E_n^*(x)$.
2. $e^{-\mathbb{i}\theta} \in Orb(z)$: Then $e^{-\mathbb{i}\theta} + e^{\mathbb{i}\theta} = 2\cos\theta$ is a root of $E_n^*(x)$.
3. $-e^{\mathbb{i}\theta} - 1 \in Orb(z)$: Then $-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1}$ is a root of $E_n^*(x)$.
4. $\frac{1}{-e^{\mathbb{i}\theta}-1} \in Orb(z)$: Then $\frac{1}{-e^{\mathbb{i}\theta}-1} - e^{\mathbb{i}\theta} - 1$ is a root of $E_n^*(x)$.
5. $-1 - \frac{1}{e^{\mathbb{i}\theta}} \in Orb(z)$: Then $-1 - \frac{1}{e^{\mathbb{i}\theta}} + \frac{1}{-1-\frac{1}{e^{\mathbb{i}\theta}}} = -e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1}$ is a root of $E_n^*(x)$.
6. $-\frac{e^{\mathbb{i}\theta}}{e^{\mathbb{i}\theta}+1} \in Orb(z)$: Then $-\frac{e^{\mathbb{i}\theta}}{e^{\mathbb{i}\theta}+1} + \frac{1}{-\frac{e^{\mathbb{i}\theta}}{e^{\mathbb{i}\theta}+1}} = -e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1}$ is a root of $E_n^*(x)$.

So $Orb(z)$ induces a partition of the roots of $E_n^*(x)$ with parts $\left\{2\cos\theta, -e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1}, -e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1}\right\}$. It remains to show that these roots are distinct. As $2\cos\theta$ is real, it is enough to show $-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1}$ and $-e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1}$ are two distinct nonreal roots.

A complex number is real if and only if it equals its complex conjugate. Clearly, the complex conjugate of $-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1}$ is $-e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1}$, and vice versa, so suppose they are equal:

$$-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta} - 1} = -e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta} - 1}$$

Let $x \coloneqq e^{\mathbb{i}\theta}$, and solve for x:

$$\begin{gathered} -x - 1 + \tfrac{1}{-x-1} = -x^{-1} - 1 + \tfrac{1}{-x^{-1}-1} \\ \Rightarrow (x-1)(x^2 + x + 1) = 0 \end{gathered}$$

So x must be a root of unity, a contradiction since $E_n(x)$ has no roots that are roots of unity by Theorem 2.2.1. Thus, $-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1}$ and $-e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1}$ are two distinct nonreal numbers. □

In Section 2.2.3, conditions are given to show when the elements of $Orb(z)$ are $\mathbb{Q}$-conjugates. That work can be used to give conditions for when the elements of $Orb^*(z)$ are $\mathbb{Q}$-conjugates.

Lemma 4.2.6. *Let $n \geq 9$ be an odd integer, and $z \coloneqq e^{\mathbb{i}\theta}$ be a root of $E_n(x)$.*

1. *$|\mathcal{T}_z| = 6$ if and only if the elements of $Orb^*(z)$ are $\mathbb{Q}$-conjugates.*
2. *$|\mathcal{T}_z| = 2$ if and only if the only $\mathbb{Q}$-conjugate of $2\cos\theta$ in $Orb^*(z)$ is itself.*

Proof.

1. ($\Rightarrow$) Suppose $|\mathcal{T}_z| = 6$. Let $f(x)$ be the minimal polynomial of z over $\mathbb{Q}$. Then $f(x)$ is a self-reciprocal polynomial of even degree by Theorem 2.3.1, so the reciprocal transform $f^*(x) \in \mathbb{Q}[x]$ exists. Every element of $Orb(z)$ is a root of $f(x)$ by Corollary 2.2.19, so every element of $Orb^*(z)$ is a root of $f^*(x)$. By Dickson's Theorem (Theorem 4.1.3), $f^*(x)$ is irreducible over $\mathbb{Q}$ $\therefore$ the elements of $Orb^*(z)$ are $\mathbb{Q}$-conjugates.

   ($\Leftarrow$) Suppose the elements of $Orb^*(z)$ are $\mathbb{Q}$-conjugates, but $|\mathcal{T}_z| = 2$ (the only possibility if $|\mathcal{T}_z| \neq 6$ by Theorem 2.2.13). Let $f(x)$ be the minimal polynomial of z over $\mathbb{Q}$. Then $f(x)$ is a self-reciprocal polynomial by Theorem 2.3.1, so the reciprocal transform $f^*(x) \in \mathbb{Q}[x]$ exists. By Dickson's Theorem (Theorem 4.1.3), $f^*(x)$ is irreducible over $\mathbb{Q}$. So, by hypothesis, the elements of $Orb^*(z)$ are all roots of $f^*(x)$. In particular, $-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1}$ is a root of $f^*(x)$. Consequently,

   $$f(-e^{\mathbb{i}\theta} - 1) = x^{\frac{\deg(f)}{2}} f^*(-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta} - 1}) = 0$$

   Therefore, $-e^{\mathbb{i}\theta} - 1$ is a root of $f(x)$ $\therefore$ $-e^{\mathbb{i}\theta} - 1 \in Orb(z)$ is a $\mathbb{Q}$-conjugate of z. This contradicts Theorem 2.2.18 $\therefore$ $|\mathcal{T}_z| = 6$.

2. ($\Rightarrow$) Suppose $|\mathcal{T}_z| = 2$. Then by 1, the elements of $Orb^*(z)$ cannot all be $\mathbb{Q}$-conjugates. Since $-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1} \in Orb^*(z)$ and $-e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1} \in Orb^*(z)$ are complex conjugates, they are necessarily $\mathbb{Q}$-conjugates by the complex conjugate root theorem. So if $2\cos\theta$ were a $\mathbb{Q}$-conjugate to either

$-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1}$ or $-e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1}$, then all the elements of $Orb^*(z)$ would be $\mathbb{Q}$-conjugates, which is impossible. Therefore, the only $\mathbb{Q}$-conjugate of $2\cos\theta$ in $Orb^*(z)$ is itself.

($\Leftarrow$) Suppose the only $\mathbb{Q}$-conjugate of $2\cos\theta$ in $Orb^*(z)$ is itself. By 1, $|\mathcal{T}_z| \neq 6 \therefore |\mathcal{T}_z| = 2$. □

Corollary 4.2.7. *Let $n \geq 9$ be an odd integer, and $z \coloneqq e^{\mathbb{i}\theta}$ be a root of $E_n(x)$. Then the elements of $Orb(z)$ are $\mathbb{Q}$-conjugates if and only if the elements of $Orb^*(z)$ are $\mathbb{Q}$-conjugates.*

Proof. Apply Corollary 2.2.19 and Lemma 4.2.6. □

It is also useful to consider translates of $E_n^*(x)$. There is a natural partitioning of the roots of a translate of $E_n^*(x)$ induced by the orbits of roots of $E_n^*(x)$. To be precise, if $z := e^{\mathbb{i}\theta}$ is a root of $E_n(x)$, then *the root orbit of z of $E_n^*(x-j)$*, denoted by $Orb_j^*(z)$, is defined to be

$$Orb_j^*(z) \coloneqq \left\{2\cos\theta + j, -e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1} + j, -e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1} + j\right\}$$

Clearly, $Orb^*(z) = Orb_0^*(z)$. The elements of $Orb_j^*(z)$ satisfy a number of nice arithmetic properties.

Lemma 4.2.8. *Let $n \geq 9$ be an odd integer, and $z \coloneqq e^{\mathbb{i}\theta}$ be a root of $E_n(x)$.*

1. *The sum of the elements of $Orb_j^*(z)$ is $3(j-1)$ for any $j \in \mathbb{R}$.*
2. *The product of the elements of $Orb_1^*(z)$ is $J(z)$, with $J(z)$ as in Definition 2.2.10.*
3. *The product of the elements of $Orb_2^*(z)$ is 1.*

Proof. Each proof is an exercise in simplification.

1.
$$2\cos\theta + j - e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1} + j - e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1} + j = 3(j-1)$$

2.
$$(2\cos\theta+1)\left(-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1} + 1\right)\left(-e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1} + 1\right) = \frac{(2\cos\theta+1)^3}{2(\cos\theta+1)} = J(z)$$

3.
$$(2\cos\theta+2)\left(-e^{\mathbb{i}\theta} - 1 + \frac{1}{-e^{\mathbb{i}\theta}-1} + 2\right)\left(-e^{-\mathbb{i}\theta} - 1 + \frac{1}{-e^{-\mathbb{i}\theta}-1} + 2\right) = 1$$

□

Proposition 4.2.9. *Let $k \geq 1$ be odd. Then*

$$(x + x^{-1} + 2)^k + \left(-x - 1 + \frac{1}{-x-1} + 2\right)^k + \left(-x^{-1} - 1 + \frac{1}{-x^{-1}-1} + 2\right)^k = \frac{E_{3k}(x)}{(x^2+x)^{k-1}}$$

Proof. Multiply both sides by $(x^2+x)^k$ and simplify. □

Corollary 4.2.10. *Let $n \geq 9$ and $k \geq 1$ both be odd integers, and $z \coloneqq e^{\mathbb{i}\theta}$ a root of $E_n(X)$. The k^{th} power sum of the elements of $Orb_2^*(z)$ is $(z^2+z)^{1-k}E_{3k}(z)$.*

Proof. In Proposition 4.2.9, set $x := z$. □

4.3 Dickson's Theorem for the Cauchy-Mirimanoff Polynomials

Dickson's Theorem (Theorem 4.1.3) applies to general self-reciprocal polynomials. One might wonder what additional hypotheses are needed to make Condition 2 redundant.

Theorem 4.3.1. *Let $f(x) \in \mathbb{Q}[x]$ be a self-reciprocal polynomial with a complex root of absolute value 1, $f(\pm 1) \neq 0$, and $\deg(f)$ an even integer. Then $f(x)$ is irreducible if and only if $f^*(x)$ is irreducible.*

Proof. As $f(x)$ is self-reciprocal of even degree, the reciprocal transform $f^*(x)$ exists.
($\Rightarrow$) By Dickson's Theorem, $f^*(x)$ is irreducible.
($\Leftarrow$) Suppose $f^*(x)$ is irreducible. By Dickson's Theorem, $f(x)$ is either irreducible or a product of two irreducible (non-self-reciprocal) polynomials. However, as $f(x)$ has a root of absolute value 1, it must have at least one irreducible self-reciprocal factor. Consequently by Dickson's Theorem, this is possible only if $f(x)$ is irreducible. □

Corollary 4.3.2 (Dickson's Theorem for the Cauchy-Mirimanoff Polynomials)**.** *Let $n \geq 8$ be an integer. Then $E_n(x)$ is irreducible if and only if $E_n^*(x)$ is irreducible.*

Proof. From Theorem 2.4.2 (a similar result can be found in Helou (1997) - Lemma 1), if $n \geq 8$ then $E_n(x)$ has at least one nonreal root of absolute value 1. Apply Theorem 4.3.1. □

More can be said when the index of the Cauchy-Mirimanoff Polynomials is odd.

Corollary 4.3.3. *Let $n \geq 9$ be an odd integer, and let $f(x) \in \mathbb{Q}[x]$ be a factor of $E_n(x)$ such that $|\mathcal{T}_z| = 6$ for all roots z of $f(x)$. Then $f(x)$ is irreducible over $\mathbb{Q}$ if and only if $f^*(x)$ is irreducible over $\mathbb{Q}$.*

Proof. The condition that $|\mathcal{T}_z| = 6$ for all roots z of $f(x)$ guarantees that $f(x)$ will have at least one nonreal root of absolute value 1. Apply Theorem 4.3.1. □

Corollary 4.3.4. *Let $n \geq 9$ be an odd integer, and $|\mathcal{T}_z| = 6$ for all roots z of $E_n(x)$. Then the number of irreducible factors of $E_n(x)$ is equal to the number of irreducible factors of $E_n^*(x)$.*

Proof. The condition that $|\mathcal{T}_z| = 6$ for all roots z of $E_n(x)$ guarantees that every irreducible factor of $E_n(x)$ has at least one nonreal root of absolute value 1. By Theorem 4.3.1, there is a one-to-one correspondence between the factors of $E_n(x)$ and $E_n^*(x)$ yielding the result. □

The following corollary could also be obtained from results in Helou (1997).

Corollary 4.3.5. *Let $p \geq 11$ be a prime integer. Then the number of irreducible factors of $E_p(x)$ equals the number of irreducible factors of $E_p^*(x)$.*

Proof. Apply Corollary 4.3.4 to Theorem 2.3.4. □

Chapter 5

The Irreducibility of $E_{2p}(x)$ and $E_{3p}(x)$

5.1 The Irreducibility of $E_{2p}(x)$ - A New Proof

Visually inspecting $E^*_{2p}(x)$ for small primes p leads to the observation that the reciprocals $(E^*_{2p})^{\dashv}$ are irreducible by Eisenstein's criteria with respect to p.

Theorem 5.1.1. *Let p be an odd prime. Then $E^*_{2p}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. By Theorem 4.2.1,

$$E^*_{2p}(x) = (x+2)^p - 2T_{2p}\left(\frac{\sqrt{x+2}}{2}\right) = (x+2)^p - 2T_p\left(\frac{x}{2}\right)$$

It is convenient to consider the polynomial $f_{2p}(x) \in \mathbb{Z}[x]$ defined as

$$f_{2p}(x) \coloneqq 2^{p-1}(x+1)^p - T_p(x)$$

If $f_{2p}(x)$ is irreducible over $\mathbb{Q}$, then $E^*_{2p}(x)$ is irreducible $\because$ a factorization of $E^*_{2p}(x)$ yields a factorization of $E^*_{2p}(2x)$, which yields a factorization of $\frac{E^*_{2p}(2x)}{2} = f_{2p}(x)$ over $\mathbb{Q}$, a contradiction.

It is known that the leading coefficient of $T_p(x)$ is 2^{p-1}. So, the x^p-terms in $f_{2p}(x)$ cancel. Moreover, the powers of x in $T_p(x)$ differ by 2 (Rivlin (1990) - Exercise 1.2.1). Therefore, the leading coefficient of $f_{2p}(x)$ is $2^{p-1}px^{p-1}$.

The constant coefficient of $f_{2p}(x)$ is $f_{2p}(0) = 2^{p-1} - T_p(0) = 2^{p-1}$ (again apply Rivlin (1990) - Exercise 1.2.1 to find $T_p(0) = 0$). Every coefficient of $(x+1)^p$ beside the leading and constant coefficient is divisible by p. It is known (Rivlin (1990) - Equation (5.32)) that every coefficient beside the leading coefficient of $T_p(x)$ is divisible by p $\therefore$ all coefficients of $f_{2p}(x)$ are divisible by p except the constant coefficient.

By the previous two paragraphs, $f^{\dashv}_{2p}(x)$ is irreducible by Eisenstein's Criteria with respect to p. Consequently $f_{2p}(x)$ is irreducible $\therefore$ $E^*_{2p}(x)$ is irreducible. □

Corollary 5.1.2. *Let p be an odd prime. Then $E_{2p}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Verify directly for $p = 3$. If $p \geq 5$, apply Corollary 4.3.2 and Theorem 5.1.1. □

5.2 The Irreducibility of $E_{3p}(x)$ - First Proof

Rather than study $E^*_{3p}(x)$ directly, the translate $E^*_{3p}(x-2)$ is studied. Unfortunately, nothing as easy as Eisenstein's Irreducibility Criteria may be applied, yet the irreducibility of $E^*_{3p}(x)$ can still be proven.

5.2.1 The Newton Polygon of $E^*_{3p}(x-2)$

Newton Polygons are the main tool of this section; we follow the terminology in Mott (1995).

Theorem 5.2.1 (Dumas' Theorem - cf. Mott (1995))**.** *Let $f(x)$, $g(x)$, $h(x) \in \mathbb{Q}[x]$ and p a prime integer. If $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are nonconstant polynomials, then the Newton Polygon of $f(x)$ with respect to p is composed of segments that have the same width and slope as the segments of the Newton Polygons of $g(x)$ and $h(x)$ with respect to p. Moreover, the degree of a factor of $f(x)$ is the sum of the widths of some of the segments of the Newton Polygon of $f(x)$ with respect to p.*

Theorem 5.2.2. *Let $p \geq 5$ be prime. Then the Newton Polygon of $E^*_{3p}(x-2)$ has precisely three vertices - $(0,1)$, $(\frac{p-1}{2}, 0)$, $(\frac{3p-3}{2}, 1)$.*

Proof. The following three claims and their proofs are enough to establish the form of the Newton Polygon.

- *Claim*: All coefficients of $E^*_{3p}(x-2)$, except of $x^{\frac{p-1}{2}}$, are divisible by p.

  It is enough to show $E^*_{3p}(x-2) = 3x^{\frac{p-1}{2}}$, with $\overline{E^*_{3p}(x-2)}$ the image of $E^*_{3p}(x-2)$ in $\mathbb{F}_p(\sqrt{x})$. Before beginning, note $\overline{T_p(x) \equiv x^p \pmod{p}}$ (see Rivlin (1990) - Equation (5.32)). So using Theorem 4.2.1,

$$\begin{aligned}
\overline{E^*_{3p}(x-2)} &= \frac{x^{\frac{3p}{2}} - 2T_{3p}\left(\frac{\sqrt{x}}{2}\right)}{\sqrt{x}} \\
&= \frac{x^{\frac{3p}{2}} - 2T_p\left(T_3\left(\frac{\sqrt{x}}{2}\right)\right)}{\sqrt{x}} \\
&= \frac{x^{\frac{3p}{2}} - 2T_p\left(\frac{\sqrt{x}}{2}(x-3)\right)}{\sqrt{x}} \\
&= \frac{x^{\frac{3p}{2}} - 2\left(\frac{\sqrt{x}}{2}(x-3)\right)^p}{\sqrt{x}} \\
&= \frac{x^{\frac{3p}{2}} - x^{\frac{p}{2}}(x-3)^p}{\sqrt{x}} \\
&= x^{\frac{3p-1}{2}} - x^{\frac{p-1}{2}}(x-3)^p \\
&= x^{\frac{3p-1}{2}} - x^{\frac{p-1}{2}}(x^p - 3) \\
&= x^{\frac{3p-1}{2}} - x^{\frac{3p-1}{2}} + 3x^{\frac{p-1}{2}} \\
&= 3x^{\frac{p-1}{2}}
\end{aligned}$$

- *Claim*: The leading coefficient of $E^*_{3p}(x-2)$ is $3p$.

  It is known that a general formula for the Chebyshev Polynomials is

$$T_n(x) = \frac{n}{2}\sum_{r=0}^{\lfloor \frac{n}{2} \rfloor} \frac{(-1)^r}{n-r}\binom{n-r}{r}(2x)^{n-2r} \tag{5.1}$$

  Consequently,

$$\begin{aligned} E^*_{3p}(x-2) &= \frac{x^{\frac{3p}{2}} - 2T_{3p}\left(\frac{\sqrt{x}}{2}\right)}{\sqrt{x}} && (5.2)\\ &= \frac{x^{\frac{3p}{2}} - 3p\sum_{r=0}^{\lfloor \frac{3p}{2} \rfloor} \frac{(-1)^r}{3p-r}\binom{3p-r}{r}x^{\frac{3p-2r}{2}}}{\sqrt{x}} && (5.3)\\ &= -3p\sum_{r=1}^{\lfloor \frac{3p}{2} \rfloor} \frac{(-1)^r}{3p-r}\binom{3p-r}{r}x^{\frac{3p-2r-1}{2}} && (5.4) \end{aligned}$$

  The largest power of x occurs when $r = 1$ $\therefore$ the leading term is $-3p\frac{-1}{3p-1}\binom{3p-1}{1}x^{\frac{3p-3}{2}} = 3px^{\frac{3p-3}{2}}$.

- *Claim*: The constant coefficient of $E^*_{3p}(x-2)$ is $(-1)^{\frac{3p+1}{2}}(3p)$.

  From Equation 5.4, the constant coefficient comes when $r = \lfloor \frac{3p}{2} \rfloor = \frac{3p-1}{2}$. So the constant coefficient is $-3p\frac{(-1)^{\frac{3p-1}{2}}}{3p-\frac{3p-1}{2}}\binom{3p-\frac{3p-1}{2}}{\frac{3p-1}{2}} = -3p\frac{(-1)^{\frac{3p-1}{2}}}{\frac{3p+1}{2}}\binom{\frac{3p+1}{2}}{\frac{3p-1}{2}} = (-1)^{\frac{3p+1}{2}}(3p)$.

□

Corollary 5.2.3. *Let $p \geq 5$ be prime. Then $E^*_{3p}(x-2)$ is either irreducible or a product of two irreducible polynomials, one of degree $\frac{p-1}{2}$ and the other of degree $p-1$.*

Proof. By Theorem 5.2.2, the Newton Polygon of $E^*_{3p}(x-2)$ consists of precisely two segments, one of width $\frac{p-1}{2}$ and the other of width $p-1$. The result follows from Dumas' Theorem. □

5.2.2 Root Orbits of $E_{3p}(x)$ and $E^*_{3p}(x)$

Theorem 5.2.4. *Let $p \geq 5$ be prime. Then $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p}(x)$.*

Proof. On the contrary, suppose $E_n(x)$ has a root z so that $|\mathcal{T}_z| = 2$. By Theorem 2.2.13, there exists a $z' \in Orb(z)$ such that $|\mathcal{T}_{z'}| = 2$ and the absolute value of z' is 1. Define $f(x) \in \mathbb{Z}[x]$ to be the irreducible factor of $E_n(x)$ such that $f(z') = 0$. Additionally by Theorem 2.2.13, every root of $f(x)$ has absolute value 1. In particular, $f(x)$ is a self-reciprocal polynomial of even degree by Theorem 2.3.1 $\therefore$ $f^*(x) \in \mathbb{Z}[x]$ exists. By Dickson's Theorem, $f^*(x)$ is irreducible, and clearly $f^*(x) \mid E^*_{3p}(x)$.

By Proposition 4.2.3, each root of $f^*(x)$ is real and between -2 and -1. Hence, $f^*(x-2) \in \mathbb{Z}[x]$ is an irreducible factor of $E^*_{3p}(x-2)$ with all real roots between 0 and 1. As $E^*_{3p}(x)$ has exactly $\frac{p-1}{2}$ real roots, it follows $\deg(f^*(x)) \leq \frac{p-1}{2}$ $\therefore$ $\deg(f^*(x-2)) \leq \frac{p-1}{2}$. On the other hand, Corollary 5.2.3 requires $\deg(f^*(x-2)) \geq \frac{p-1}{2}$ $\therefore$ $\deg(f^*(x-2)) = \frac{p-1}{2}$.

From Theorem 5.2.2, the segment of the Newton Polygon of width $\frac{p-1}{2}$ has vertices $(0,1)$ and $(\frac{p-1}{2},0)$. Thus, by Dumas' Theorem, the Newton Polygon of $f^*(x-2)$ also consists of precisely one segment with vertices $(0,1)$ and $(\frac{p-1}{2},0)$. Consequently, all coefficients, except for the leading coefficient, of $f^*(x-2)$ are divisible by p (in fact, $f^*(x-2)$ is irreducible by Eisenstein's Criteria with respect to p).

For convenience, explicitly write $f^*(x-2)$ as a polynomial:

$$f^*(x-2) = a_{\frac{p-1}{2}} x^{\frac{p-1}{2}} + \cdots + a_1 x + a_0 \tag{5.5}$$

Restate the conclusions of the previous paragraph in the notation of Equation 5.5, $gcd(a_{\frac{p-1}{2}}, p) = 1$ and $p \mid a_0$ (but $p^2 \nmid a_0$). By the second claim in the proof of Theorem 5.2.2, the leading coefficient of $E^*_{3p}(x-2)$ is $3p$ $\therefore$ the leading coefficient, $a_{\frac{p-1}{2}}$, of $f^*(x-2)$ is 1, 3, p, or $3p$. That $gcd(a_{\frac{p-1}{2}}, p) = 1$ forces $a_{\frac{p-1}{2}} = 1$, or 3, and both yield contradictions.

- Suppose $a_{\frac{p-1}{2}} = 1$.

  Then the leading coefficient of $f^*(x)$ is 1, which forces the leading coefficient of $f(x)$ to be 1. In other words, $f(x) \in \mathbb{Z}[x]$ is a monic polynomial with every root on the unit circle. By Kronecker's Theorem (Kronecker (1857)), the roots of $f(x)$ are roots of unity contradicting Theorem 2.2.1.

- Suppose $a_{\frac{p-1}{2}} = 3$.

  The absolute value of the product of the roots of $f^*(x-2)$ is $\frac{|a_0|}{\left|a_{\frac{p-1}{2}}\right|} = \frac{|a_0|}{3}$. Because $p \mid |a_0|$, it immediately follows that $1 < \frac{p}{3} \leq \frac{|a_0|}{3}$ $\therefore$ the absolute value of the product of the roots of $f^*(x-2)$ is greater than 1. However, as already noted, each root of $f^*(x-2)$ is real and between 0 and 1 $\therefore$ the absolute value of the product of the roots is less than 1, a contradiction.

□

Corollary 5.2.5. *Let $p \geq 5$ be prime. The degree of any factor of $E^*_{3p}(x)$ is divisible by* 3.

Proof. By Theorem 5.2.4, $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p}(x)$. By Lemma 4.2.6, for each root $z := e^{\mathbb{i}\theta}$ of $E_{3p}(x)$, the elements of $Orb^*(z)$ are $\mathbb{Q}$-conjugates. Consequently, the number of roots of any irreducible factor of $E^*_{3p}(x)$ is divisible by 3 $\therefore$ the degree of any factor of $E^*_{3p}(x)$ is divisible by 3. □

5.2.3 The Irreducibility of $E^*_{3p}(x)$ and $E_{3p}(x)$

Lemma 5.2.6. *Let $p \equiv 2 \pmod 3$ be an odd prime. Then $E^*_{3p}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. By Corollary 5.2.3, $E^*_{3p}(x-2)$ is either irreducible or a product of two irreducible polynomials, one of degree $\frac{p-1}{2}$ and the other of degree $p-1$. The same holds true for any translate, so in particular, $E^*_{3p}(x)$ is either irreducible or a product of two irreducible polynomials, one of degree $\frac{p-1}{2}$ and the other of degree $p-1$. Suppose $E^*_{3p}(x)$ is a product of two irreducible polynomials. Then $p-1 \equiv 1 \pmod 3$, so $E^*_{3p}(x)$ has an irreducible factor of degree $p-1$, which is not divisible by 3, contradicting Corollary 5.2.5. Thus, $E^*_{3p}(x)$ must be irreducible. □

Lemma 5.2.7. *Let $p \equiv 1 \pmod 3$ be an odd prime. Then $E^*_{3p}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. By Corollary 5.2.3, $E^*_{3p}(x-2)$ is either irreducible or a product of two irreducible polynomials, one of degree $\frac{p-1}{2}$ and the other of degree $p-1$. Suppose $E^*_{3p}(x-2)$ is a product of two irreducible polynomials in $\mathbb{Z}[x]$, and let $f^*(x-2)$ be the irreducible factor of degree $\frac{p-1}{2}$. By Dumas' Theorem and Theorem 5.2.2, the Newton Polygon of $f^*(x-2)$ has precisely two vertices, $(0,1)$ and $(\frac{p-1}{2}, 0)$. For convenience, consider $f^*(x-2)$ as in Equation 5.5. Then $gcd(a_{\frac{p-1}{2}}, p) = 1$ and $a_{\frac{p-3}{2}} = p \cdot n$ for some $n \in \mathbb{Z}$. Consequently, the sum of the roots of $f^*(x-2)$ is $-\frac{a_{\frac{p-3}{2}}}{a_{\frac{p-1}{2}}} = -\frac{p \cdot n}{a_{\frac{p-1}{2}}}$.

By Theorem 5.2.4, $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p}(x)$. Therefore, by Lemma 4.2.6, for each root $z := e^{i\theta}$ of $E_{3p}(x)$ the elements of $Orb^*(z)$ are $\mathbb{Q}$-conjugates $\therefore$ the elements of $Orb^*_2(z)$ are also $\mathbb{Q}$-conjugates. As $p - 1 \equiv 0 \pmod 3$, there exist $\frac{p-1}{6}$ roots $z_1, \cdots, z_{\frac{p-1}{6}}$ of $E_{3p}(x)$ of absolute value 1 such that the roots of $f^*(x-2)$ can be partitioned into $Orb^*_2(z_1), \cdots, Orb^*_2(z_{\frac{p-1}{6}})$. By Lemma 4.2.8, the sum of the elements of each $Orb^*_2(z_i)$ is 3 $\therefore$ the sum of the roots of $f^*(x-2)$ is $3 \cdot \frac{p-1}{6} = \frac{p-1}{2}$.

Consequently, there are two expressions for the sum of the roots of $f^*(x-2)$ which must be equal:

$$-\frac{p \cdot n}{a_{\frac{p-1}{2}}} = \frac{p-1}{2} \Rightarrow -2pn = a_{\frac{p-1}{2}}(p-1)$$

As $p \mid -2pn$, it holds that $p \mid a_{\frac{p-1}{2}}(p-1)$ $\therefore$ $p \mid a_{\frac{p-1}{2}}$ or $p \mid p-1$. However, $p \nmid a_{\frac{p-1}{2}}$ $\because$ $gcd(a_{\frac{p-1}{2}}, p) = 1$, and clearly $p \nmid p-1$, which yields a contradiction. Therefore, $E^*_{3p}(x-2)$ is irreducible $\therefore$ $E^*_{3p}(x)$ is irreducible. □

Corollary 5.2.8. *Let $p \geq 5$ be prime. Then $E^*_{3p}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Combine Lemmas 5.2.6 and 5.2.7. □

Theorem 5.2.9. *Let $p \geq 5$ be prime. Then $E_{3p}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Apply Dickson's Theorem for the Cauchy-Mirimanoff Polynomials (Corollary 4.3.2) to Corollary 5.2.8. □

Corollary 5.2.10. *$E_{3p}(x)$ is irreducible over $\mathbb{Q}$ for all primes p.*

Proof. The only primes not included in Theorem 5.2.9 are $p = 2, 3$. If $p = 2$, then $E_{3p}(x)$ is irreducible by Corollary 5.1.2. It isn't hard to check the case $p = 3$ numerically. Alternatively, $E^*_9(x)$ is a polynomial of degree 3 - apply the rational root test to prove it is irreducible and then apply Dickson's Theorem. □

Chapter 6

A Study of $E_{3p^i}(x)$

The results of Chapter 5 are now generalized to the Cauchy-Mirimanoff polynomials $E_{3p^i}(X)$. The main result of this chapter is $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p^i}(X)$. A number of corollaries are obtained, including lower bounds on the degrees of possible factors of $E_{3p^i}(X)$, and two new proofs that $E_{3p}(X)$ is irreducible.

6.1 The Newton Polygon of $E^*_{3p^i}(x-2)$

Theorem 6.1.1. *Let $p \geq 5$ be prime, and $i \in \mathbb{N}$. The Newton Polygon of $E^*_{3p^i}(x-2)$ with respect to p has vertices:*

$$\left(\frac{p^0-1}{2}, i\right), \left(\frac{p^1-1}{2}, i-1\right), \quad \cdots \quad, \left(\frac{p^i-1}{2}, 0\right) =$$
$$\left(\frac{3p^i-3}{2} - (p^i-1), 0\right), \quad \cdots \quad, \left(\frac{3p^i-3}{2} - (p^1-1), i-1\right), \left(\frac{3p^i-3}{2} - (p^0-1), i\right)$$

Proof. Using Equation 4.5 and Equation 5.1, find

$$E^*_{3p^i}(x-2) = \sum_{k=0}^{\frac{3p^i-3}{2}} (-1)^{\frac{3p^i-3}{2}-k} \frac{3p^i}{\frac{3p^i-1}{2}-k} \binom{\frac{3p^i-1}{2}+k}{\frac{3p^i-3}{2}-k} x^k$$

For fixed p and i, define $a_k := (-1)^{\frac{3p^i-3}{2}-k} \frac{3p^i}{\frac{3p^i-1}{2}-k} \binom{\frac{3p^i-1}{2}+k}{\frac{3p^i-3}{2}-k}$. The following four claims and their proofs are enough to prove the Newton Polygon of $E^*_{3p^i}(x-2)$ is as asserted.

- *Claim*: Fix j so that $1 \leq j \leq i$. If k is such that $\frac{p^{j-1}-1}{2} \leq k < \frac{p^j-1}{2}$, then $p^{i-j+1} \mid a_k$.

  It is enough to show that $p^j \nmid \left(\frac{3p^i-1}{2} - k\right)$. On the contrary, suppose that $p^j \mid \left(\frac{3p^i-1}{2} - k\right) \therefore$

  $p^j z = \frac{3p^i-1}{2} - k$ for some $z \in \mathbb{Z}$. By the bound on k, there exists a $\kappa \in \mathbb{Z}$ with $1 \leq \kappa \leq \left(\frac{p-1}{2}\right) p^{j-1}$ such

that $k = \frac{p^j-1}{2} - \kappa$. Consequently,

$$\begin{aligned} p^j z &= \frac{3p^i-1}{2} - k \\ &= \frac{3p^i-1}{2} - (\frac{p^j-1}{2} - \kappa) \\ &= p^j\left(\frac{3p^{i-j}-1}{2}\right) + \kappa \end{aligned}$$

Thus, $\kappa = p^j z - p^j\left(\frac{3p^{i-j}-1}{2}\right) \therefore p^j \mid \kappa$. However, $\kappa \leq \left(\frac{p-1}{2}\right)p^{j-1} < p^j$, a contradiction.

- *Claim*: Fix j so that $0 \leq j \leq i$. If $k = \frac{p^j-1}{2}$, then $p^{i-j+1} \nmid a_k$.
  In this case, a_k may be simplified to

$$a_k = (-1)^{\frac{3p^i-3}{2}-k}\frac{3p^{i-j}}{\left(\frac{3p^{i-j}-1}{2}\right)}\binom{\frac{3p^i+p^j-2}{2}}{\frac{3p^i-p^j-2}{2}}$$

  So it is enough to show $p \nmid \binom{\frac{3p^i+p^j-2}{2}}{\frac{3p^i-p^j-2}{2}}$. Begin by rewriting the binomial coefficient as

$$\binom{\frac{3p^i+p^j-2}{2}}{\frac{3p^i-p^j-2}{2}} = \binom{\frac{3p^i+p^j-2}{2}}{p^j} = \frac{\left(\frac{3p^i+p^j}{2}-1\right)}{1}\frac{\left(\frac{3p^i+p^j}{2}-2\right)}{2}\cdots\frac{\left(\frac{3p^i+p^j}{2}-p^j\right)}{p^j}$$

  Consequently, it is enough to show $ord_p\left(\frac{\frac{3p^i+p^j}{2}-\alpha}{\alpha}\right) = 0$ for each $1 \leq \alpha \leq p^j$. Let $ord_p(\alpha) = \beta$, and note $\beta \leq j \because \alpha \leq p^j$. So $\alpha = p^\beta z$ for some $z \in \mathbb{Z}$ with $gcd(p, z) = 1$. Four cases must be considered:

  - $\beta < j < i$

$$ord_p\left(\frac{\frac{3p^i+p^j}{2}-\alpha}{\alpha}\right) = ord_p\left(\frac{\frac{3p^i+p^j}{2}-p^\beta z}{p^\beta z}\right) = ord_p\left(\frac{3p^{i-\beta}+p^{j-\beta}}{2} - z\right) = 0$$

  - $\beta = j < i$
    If $\beta = j$, then $\alpha = p^j$. So

$$ord_p\left(\frac{\frac{3p^i+p^j}{2}-\alpha}{\alpha}\right) = ord_p\left(\frac{\frac{3p^i+p^j}{2}-p^j}{p^j}\right) = ord_p(3p^{i-j}-1) = 0$$

  - $\beta < j = i$

$$ord_p\left(\frac{\frac{3p^i+p^j}{2}-\alpha}{\alpha}\right) = ord_p\left(\frac{2p^i-p^\beta z}{p^\beta z}\right) = ord_p(2p^{i-\beta}-z) = 0$$

– $\beta = j = i$

As noted before, $\alpha = p^j$. So

$$ord_p\left(\frac{\frac{3p^i+p^j}{2} - \alpha}{\alpha}\right) = ord_p(1) = 0$$

- *Claim*: Fix j so that $1 \leq j \leq i$. If k is such that $\frac{3p^i-3}{2} - (p^j - 1) < k \leq \frac{3p^i-3}{2} - (p^{j-1} - 1)$, then $p^{i-j+1} \mid a_k$.
  It is enough to show that $p^j \nmid \left(\frac{3p^i-1}{2} - k\right)$. On the contrary, suppose that $p^j \mid \left(\frac{3p^i-1}{2} - k\right) \therefore$
  $p^j z = \frac{3p^i-1}{2} - k$ for some $z \in \mathbb{Z}$. By the bound on k, there exists a $\kappa \in \mathbb{Z}$ with $1 \leq \kappa \leq (p-1)\,p^{j-1}$ such that $k = \frac{3p^i-3}{2} - (p^j - 1) + \kappa$. Consequently

$$\begin{aligned} p^j z &= \frac{3p^i - 1}{2} - k \\ &= \frac{3p^i - 1}{2} - (\frac{3p^i - 3}{2} - (p^j - 1) + \kappa) \\ &= p^j - \kappa \end{aligned}$$

  Clearly then $p^j \mid \kappa$. However, $\kappa \leq (p-1)p^{j-1} < p^j$, a contradiction.

- *Claim*: Fix j so that $0 \leq j \leq i$. If $k = \frac{3p^i-3}{2} - (p^j - 1)$, then $p^{i-j+1} \nmid a_k$.
  In this case, a_k may be simplified to

$$a_k = (-1)^{\frac{3p^i-3}{2}-k}(3p^{i-j})\binom{3p^i - p^j - 1}{p^j - 1}$$

  So it is enough to show $p \nmid \binom{3p^i-p^j-1}{p^j-1}$. Begin by rewriting the binomial coefficient as

$$\binom{3p^i - p^j - 1}{p^j - 1} = \frac{(3p^i - p^j - 1)}{1}\frac{(3p^i - p^j - 2)}{2}\cdots\frac{(3p^i - p^j - (p^j - 1))}{p^j - 1}$$

  So it is enough to show $ord_p\left(\frac{3p^i-p^j-\alpha}{\alpha}\right) = 0$ for $1 \leq \alpha \leq p^j - 1$. Let $ord_p(\alpha) = \beta$, and as $\alpha \leq p^j - 1$ note that $\beta < j$. So $\alpha = p^\beta z$ for some $z \in \mathbb{Z}$ with $gcd(p, z) = 1$. Thus

$$ord_p\left(\frac{3p^i - p^j - \alpha}{\alpha}\right) = ord_p\left(\frac{3p^i - p^j - p^\beta z}{p^\beta z}\right) = ord_p(3p^{i-\beta} - p^{j-\beta} - z) = 0$$

□

Corollary 6.1.2. *Let $p \geq 5$ be prime, and $i \in \mathbb{N}$. There are exactly $2i$ segments in the Newton Polygon of $E^*_{3p^i}(x-2)$ with respect to p, and the segments have widths (in order from left to right):*

$$\left(\frac{p-1}{2}\right)p^0, \left(\frac{p-1}{2}\right)p^1, \cdots, \left(\frac{p-1}{2}\right)p^{i-1}, (p-1)p^{i-1}, \cdots, (p-1)p^1, (p-1)p^0$$

Proof. Immediate from Theorem 6.1.1. □

6.2 The Root Orbits of $E_{3p^i}(x)$

The main result of this section is $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p^i}(x)$. While the basic idea is the same as that in Theorem 5.2.4, there are a number of technicalities that must be resolved.

6.2.1 Technical Results

Lemma 6.2.1. *Let $0 \leq i, j \in \mathbb{Z}$, and $5 \leq p \in \mathbb{Z}$. Then $\left(\frac{p-1}{2}\right) p^i \neq (p-1)p^j$.*

Proof. On the contrary, suppose $\left(\frac{p-1}{2}\right) p^i = (p-1)p^j$ for some $i, j \in \mathbb{Z}$. Then $p^i = 2p^j \therefore p^{i-j} = 2$. The only way this could happen is for $p = 2$, which is prohibited by the hypothesis, so a contradiction is reached. □

Theorem 6.2.2. *Let $0 \leq j \in \mathbb{Z}$, and $7 \leq p \in \mathbb{Z}$. Define sets $\mathcal{A} \coloneqq \left\{\left(\frac{p-1}{2}\right) p^i \mid 0 \leq i \leq j\right\}$,*
$\mathcal{B} \coloneqq \left\{(p-1)\, p^i \mid 0 \leq i \leq j\right\}$, and $\mathcal{S} \coloneqq \mathcal{A} \cup \mathcal{B}$. If $\varnothing \neq \mathcal{D}, \mathcal{E} \subseteq \mathcal{S}$ such that $\sum_{d\in\mathcal{D}} 2d = \sum_{e\in\mathcal{E}} e$, then

1. *$\mathcal{D} \subseteq \mathcal{A}$*
2. *$\mathcal{E} \subseteq \mathcal{B}$*
3. *For each $0 \leq i \leq j$ such that $\left(\frac{p-1}{2}\right) p^i \in \mathcal{D}$, it follows $(p-1)p^i \in \mathcal{E}$*

Proof. Proceed by induction on j. Let $j = 0 \therefore \mathcal{A} = \left\{\frac{p-1}{2}\right\}$, $\mathcal{B} = \{p-1\}$, and $\mathcal{S} = \left\{\frac{p-1}{2}, p-1\right\}$. By inspection, it is clear that the only choice of $\varnothing \neq \mathcal{D}, \mathcal{E} \subseteq \mathcal{S}$ so that $\sum_{d\in\mathcal{D}} 2d = \sum_{e\in\mathcal{E}} e$ is $\mathcal{D} = \left\{\frac{p-1}{2}\right\}$ and $\mathcal{E} = \{p-1\}$. The three conclusions follow trivially.

Let $j \geq 1$, and assume the inductive hypothesis for all nonnegative integers less than j. As $\mathcal{S} = \mathcal{A} \cup \mathcal{B}$, any sum of elements from $\mathcal{S}$ is of the form

$$\sum_{i=0}^{j} \alpha_i \left(\frac{p-1}{2}\right) p^i + \sum_{i=0}^{j} \beta_i (p-1)p^i \tag{6.1}$$

where $\alpha_i, \beta_i \in \{0, 1\}$ for all $0 \leq i \leq j$.

Let $\varnothing \neq \mathcal{D}, \mathcal{E} \subseteq \mathcal{S}$ such that $\sum_{d\in\mathcal{D}} 2d = \sum_{e\in\mathcal{E}} e$. Applying Equation 6.1, let

$$\sum_{d\in\mathcal{D}} d = \sum_{i=0}^{j} a_i \left(\frac{p-1}{2}\right) p^i + \sum_{i=0}^{j} b_i (p-1)p^i \tag{6.2}$$

$$\sum_{e\in\mathcal{E}} e = \sum_{i=0}^{j} c_i \left(\frac{p-1}{2}\right) p^i + \sum_{i=0}^{j} d_i (p-1)p^i \tag{6.3}$$

where $a_i, b_i, c_i, d_i \in \{0, 1\}$ for all $0 \leq i \leq j$. Then

$$0 = \sum_{e\in\mathcal{E}} e - 2\sum_{d\in\mathcal{D}} d \tag{6.4}$$

$$0 = \sum_{i=0}^{j} c_i \left(\frac{p-1}{2}\right) p^i + \sum_{i=0}^{j} d_i (p-1)p^i - 2\left(\sum_{i=0}^{j} a_i \left(\frac{p-1}{2}\right) p^i + \sum_{i=0}^{j} b_i (p-1)p^i\right) \tag{6.5}$$

Moving the j^{th}-term from each sum on the right of Equation 6.5 to the left of Equation 6.5 yields the formula

$$(a_j+2b_j-\frac{c_j}{2}-d_j)(p-1)p^j = \sum_{i=0}^{j-1} c_i\left(\frac{p-1}{2}\right)p^i+\sum_{i=0}^{j-1} d_i(p-1)p^i-2\left(\sum_{i=0}^{j-1} a_i\left(\frac{p-1}{2}\right)p^i+\sum_{i=0}^{j-1} b_i(p-1)p^i\right) \quad (6.6)$$

Two cases are considered based on whether the left of Equation 6.6 equals 0.

- *Case 1*: $(a_j + 2b_j - \frac{c_j}{2} - d_j)(p-1)p^j \neq 0$

  Consider the absolute values of the two sides of Equation 6.6.

$$\begin{aligned}
&\left|\sum_{i=0}^{j-1} c_i\left(\frac{p-1}{2}\right)p^i + \sum_{i=0}^{j-1} d_i(p-1)p^i - 2\left(\sum_{i=0}^{j-1} a_i\left(\frac{p-1}{2}\right)p^i + \sum_{i=0}^{j-1} b_i(p-1)p^i\right)\right| \\
= \;& (p-1)\left|\sum_{i=0}^{j-1}(\frac{c_i}{2} - a_i + d_i - 2b_i)p^i\right| \\
\leq \;& (p-1)\sum_{i=0}^{j-1}\left|\frac{c_i}{2} - a_i + d_i - 2b_i\right|p^i \\
\leq \;& (p-1)\sum_{i=0}^{j-1} 3p^i \\
= \;& 3(p^j-1) \\
< \;& 3p^j \\
\leq \;& \frac{p-1}{2}p^j \quad (\because p \geq 7) \\
\leq \;& \left|a_j + 2b_j - \frac{c_j}{2} - d_j\right|(p-1)p^j
\end{aligned}$$

  Of course, the conclusion is that the absolute value of the left side of Equation 6.6 is strictly greater than the absolute value of the right side of Equation 6.6, a contradiction. This case is impossible.

- *Case 2*: $(a_j + 2b_j - \frac{c_j}{2} - d_j)(p-1)p^j = 0$

  Then $a_j + 2b_j - \frac{c_j}{2} - d_j = 0$, and the only two ways this may happen are if $a_j = b_j = c_j = d_j = 0$, or $a_j = d_j = 1$ and $b_j = c_j = 0$. Consequently, either $\left(\frac{p-1}{2}\right)p^j, (p-1)p^j \notin \mathcal{D} \cup \mathcal{E}$; or $\left(\frac{p-1}{2}\right)p^j \in \mathcal{D}$ and $(p-1)p^j \in \mathcal{E}$. Moreover, the right side of Equation 6.6 equals 0, so by the inductive hypothesis $b_i = c_i = 0$ and if $a_i = 1$ then $d_i = 1$ for all $0 \leq i \leq j-1$. Rephrasing the results, we have $\mathcal{D} \subseteq \mathcal{A}$, $\mathcal{E} \subseteq \mathcal{B}$, and for each $0 \leq i \leq j$ such that $\left(\frac{p-1}{2}\right)p^i \in \mathcal{D}$, it follows $(p-1)p^i \in \mathcal{E}$.

□

Theorem 6.2.3. *Let $0 \leq j \in \mathbb{Z}$. Define sets $\mathcal{A} := \{2 \cdot 5^i \mid 0 \leq i \leq j\}$, $\mathcal{B} := \{4 \cdot 5^i \mid 0 \leq i \leq j\}$, and $\mathcal{S} := \mathcal{A} \cup \mathcal{B}$. If $\varnothing \neq \mathcal{D}, \mathcal{E} \subseteq \mathcal{S}$ such that $\mathcal{D} \cap \mathcal{E} = \varnothing$ and $\sum_{d\in\mathcal{D}} 2d = \sum_{e\in\mathcal{E}} e$, then*

1. *$\mathcal{D} \subseteq \mathcal{A}$*
2. *$\mathcal{E} \subseteq \mathcal{B}$*
3. *For each $0 \leq i \leq j$ such that $2 \cdot 5^i \in \mathcal{D}$, it follows $4 \cdot 5^i \in \mathcal{E}$*

Proof. Proceed by induction on j. Let $j = 0 \therefore \mathcal{A} = \{2\}$, $\mathcal{B} = \{4\}$, and $\mathcal{S} = \{2, 4\}$. By inspection, it is clear that the only choice of $\varnothing \neq \mathcal{D}, \mathcal{E} \subseteq \mathcal{S}$ so that $\mathcal{D} \cap \mathcal{E} = \varnothing$ and $\sum_{d\in\mathcal{D}} 2d = \sum_{e\in\mathcal{E}} e$ is $\mathcal{D} = \{2\}$ and $\mathcal{E} = \{4\}$. The three conclusions follow trivially.

Let $j \geq 1$, and assume the inductive hypothesis for all nonnegative integers less than j. As $\mathcal{S} = \mathcal{A} \cup \mathcal{B}$, any sum of elements from $\mathcal{S}$ is of the form

$$\sum_{i=0}^{j} \alpha_i \cdot 2 \cdot 5^i + \sum_{i=0}^{j} \beta_i \cdot 4 \cdot 5^i \tag{6.7}$$

where $\alpha_i, \beta_i \in \{0, 1\}$ for all $0 \leq i \leq j$.

Let $\varnothing \neq \mathcal{D}, \mathcal{E} \subseteq \mathcal{S}$ such that $\mathcal{D} \cap \mathcal{E} = \varnothing$ and $\sum_{d\in\mathcal{D}} 2d = \sum_{e\in\mathcal{E}} e$. Applying Equation 6.7, let

$$\sum_{d\in\mathcal{D}} d = \sum_{i=0}^{j} a_i \cdot 2 \cdot 5^i + \sum_{i=0}^{j} b_i \cdot 4 \cdot 5^i \tag{6.8}$$

$$\sum_{e\in\mathcal{E}} e = \sum_{i=0}^{j} c_i \cdot 2 \cdot 5^i + \sum_{i=0}^{j} d_i \cdot 4 \cdot 5^i \tag{6.9}$$

where $a_i, b_i, c_i, d_i \in \{0, 1\}$ for all $0 \leq i \leq j$. Then

$$0 = \sum_{e\in\mathcal{E}} e - 2\sum_{d\in\mathcal{D}} d \tag{6.10}$$

$$0 = \sum_{i=0}^{j} c_i \cdot 2 \cdot 5^i + \sum_{i=0}^{j} d_i \cdot 4 \cdot 5^i - 2\left(\sum_{i=0}^{j} a_i \cdot 2 \cdot 5^i + \sum_{i=0}^{j} b_i \cdot 4 \cdot 5^i\right) \tag{6.11}$$

Dividing by 2, and moving the j^{th}-term from each sum on the right of Equation 6.11 to the left of Equation 6.11 yields the formula

$$(2a_j + 4b_j - c_j - 2d_j) \cdot 5^j = \sum_{i=0}^{j-1} c_i \cdot 5^i + \sum_{i=0}^{j-1} d_i \cdot 2 \cdot 5^i - \left(\sum_{i=0}^{j-1} a_i \cdot 2 \cdot 5^i + \sum_{i=0}^{j-1} b_i \cdot 4 \cdot 5^i\right) \tag{6.12}$$

Two cases are considered based on whether the left of Equation 6.12 equals 0.

- *Case 1*: $(2a_j + 4b_j - c_j - 2d_j) \cdot 5^j \neq 0$

  It is clear that $|2a_j + 4b_j - c_j - 2d_j| \geq 1$. In fact, it is shown $|2a_j + 4b_j - c_j - 2d_j| \geq 2$. There are precisely three ways for $|2a_j + 4b_j - c_j - 2d_j| = 1$: the first is when $a_j = c_j = 1$ and $b_j = d_j = 0$; the second is when $b_j = c_j = d_j = 1$ and $a_j = 0$; the third is when $c_j = 1$ and $a_j = b_j = d_j = 0$. In the first case, $a_j = c_j = 1$ means $2 \cdot 5^j \in \mathcal{D} \cap \mathcal{E} = \varnothing$, a contradiction. In the second case, $b_j = d_j = 1$ means $4 \cdot 5^j \in \mathcal{D} \cap \mathcal{E} = \varnothing$, a contradiction.

  It remains to show the impossibility of the third case. Suppose $c_j = 1$ and $a_j = b_j = d_j = 0$. Then Equation 6.12 may be simplified to

$$-5^j = \sum_{i=0}^{j-1} (c_i + 2d_i - 2a_i - 4b_i) \cdot 5^i \tag{6.13}$$

Define $k \in \mathbb{Z}$ as $k \coloneqq \min\{h \mid c_h + 2d_h - 2a_h - 4b_h \neq 0\}$ with $0 \leq k \leq j-1$. Then Equation 6.13 may be simplified further to

$$-5^j = \sum_{i=k}^{j-1} (c_i + 2d_i - 2a_i - 4b_i) \cdot 5^i \tag{6.14}$$

If $k = j-1$, then Equation 6.14 reduces to $-5^j = (c_{j-1} + 2d_{j-1} - 2a_{j-1} - 4b_{j-1}) \cdot 5^{j-1} \therefore$ $-5 = c_{j-1} + 2d_{j-1} - 2a_{j-1} - 4b_{j-1}$. The only way for this to happen is for $a_{j-1} = b_{j-1} = c_{j-1} = 1$ and $d_{j-1} = 0$. However, $a_{j-1} = c_{j-1} = 1$ implies $2 \cdot 5^{j-1} \in \mathcal{D} \cap \mathcal{E} = \varnothing$, a contradiction.

If $0 \leq k < j-1$, then Equation 6.14 may be rewritten as

$$-5^j = 5^k \sum_{i=0}^{j-k-1} (c_{i+k} + 2d_{i+k} - 2a_{i+k} - 4b_{i+k}) \cdot 5^i \tag{6.15}$$

$$\therefore -5^{j-k} = \sum_{i=0}^{j-k-1} (c_{i+k} + 2d_{i+k} - 2a_{i+k} - 4b_{i+k}) \cdot 5^i \tag{6.16}$$

Rearranging Equation 6.16 yields

$$c_k + 2d_k - 2a_k - 4b_k = -5^{j-k} - \sum_{i=1}^{j-k-1} (c_{i+k} + 2d_{i+k} - 2a_{i+k} - 4b_{i+k}) \cdot 5^i \tag{6.17}$$

The right side of Equation 6.17 is divisible by $5 \therefore 5 \mid c_k + 2d_k - 2a_k - 4b_k$. As $c_k + 2d_k - 2a_k - 4b_k \neq 0$, the only possibility is $a_k = b_k = c_k = 1$ and $d_k = 0$. In particular, $a_k = c_k = 1$ implies $2 \cdot 5^k \in \mathcal{D} \cap \mathcal{E} = \varnothing$, a contradiction. This exhausts the ways that $|2a_j + 4b_j - c_j - 2d_j| = 1 \therefore |2a_j + 4b_j - c_j - 2d_j| \geq 2$.

Finally, compare the absolute values of the two sides of Equation 6.12

$$\begin{aligned}
& \left| \sum_{i=0}^{j-1} c_i \cdot 5^i + \sum_{i=0}^{j-1} d_i \cdot 2 \cdot 5^i - \left(\sum_{i=0}^{j-1} a_i \cdot 2 \cdot 5^i + \sum_{i=0}^{j-1} b_i \cdot 4 \cdot 5^i \right) \right| \\
= & \left| \sum_{i=0}^{j-1} (c_i + 2d_i - 2a_i - 4b_i) \cdot 5^i \right| \\
\leq & \sum_{i=0}^{j-1} |c_i + 2d_i - 2a_i - 4b_i| \cdot 5^i \\
\leq & \sum_{i=0}^{j-1} 6 \cdot 5^i \\
= & \frac{3}{2}(5^j - 1) \\
< & 2 \cdot 5^j \\
\leq & |2a_j + 4b_j - c_j - 2d_j| \cdot 5^j
\end{aligned}$$

Of course, the conclusion is that the absolute value of the left side of Equation 6.12 is strictly greater than the absolute value of the right side of Equation 6.12, a contradiction. This case is impossible.

- *Case 2*: $(2a_j + 4b_j - c_j - 2d_j) \cdot 5^j = 0$

  Then $2a_j + 4b_j - c_j - 2d_j = 0$, and the only two ways in which this may happen are if $a_j = b_j = c_j = d_j = 0$, or $a_j = d_j = 1$ and $b_j = c_j = 0$. Consequently, either $2 \cdot 5^j, 4 \cdot 5^j \notin \mathcal{D} \cup \mathcal{E}$; or $2 \cdot 5^j \in \mathcal{D}$ and $4 \cdot 5^j \in \mathcal{E}$. Moreover, the right side of Equation 6.12 equals 0, so by the inductive hypothesis $b_i = c_i = 0$ and if $a_i = 1$ then $d_i = 1$ for all $0 \leq i \leq j-1$. Rephrasing the results, we have $\mathcal{D} \subseteq \mathcal{A}$, $\mathcal{E} \subseteq \mathcal{B}$, and for each $0 \leq i \leq j$ such that $2 \cdot 5^i \in \mathcal{D}$, it follows $4 \cdot 5^i \in \mathcal{E}$.

□

Corollary 6.2.4. *Let $0 \leq j \in \mathbb{Z}$, and $5 \leq p$ be a prime. Define sets $\mathcal{A} \coloneqq \left\{\left(\frac{p-1}{2}\right) p^i \mid 0 \leq i \leq j\right\}$, $\mathcal{B} \coloneqq \left\{(p-1)\, p^i \mid 0 \leq i \leq j\right\}$, and $\mathcal{S} \coloneqq \mathcal{A} \cup \mathcal{B}$. If $\varnothing \neq \mathcal{D}, \mathcal{E} \subseteq \mathcal{S}$ such that $\mathcal{D} \cap \mathcal{E} = \varnothing$ and $\sum_{d \in \mathcal{D}} 2d = \sum_{e \in \mathcal{E}} e$, then*

1. *$\mathcal{D} \subseteq \mathcal{A}$*
2. *$\mathcal{E} \subseteq \mathcal{B}$*
3. *For each $0 \leq i \leq j$ such that $\left(\frac{p-1}{2}\right) p^i \in \mathcal{D}$, it follows $(p-1)p^i \in \mathcal{E}$*

Proof. Immediate by Theorems 6.2.2 and 6.2.3. □

6.2.2 $|\mathcal{T}_z| = 6$ for all Roots z of $E_{3p^i}(x)$

Theorem 6.2.5. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. Then $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p^i}(x)$.*

Proof. On the contrary, let z be a root of $E_{3p^i}(x)$ such that $|\mathcal{T}_z| = 2$. By Theorem 2.2.13, there exists a root $z' \in Orb(z)$ of $E_{3p^i}(x)$ of absolute value 1 such that $|\mathcal{T}_{z'}| = 2$. Define $f(x) \in \mathbb{Z}[x]$ to be the irreducible factor of $E_{3p^i}(x)$ with $f(z') = 0$. Again, by Theorem 2.2.13, every root of $f(x)$ has absolute value 1, and by Theorem 2.3.1, $f(x)$ is a self-reciprocal polynomial of even degree.

Define $g(x) \coloneqq f(-x-1) \in \mathbb{Z}[x]$. Then $g(x)$ is a non-self-reciprocal irreducible factor of $E_{3p^i}(x)$ (by Theorems 2.2.5, 2.2.18). As $E_{3p^i}(x)$ is self-reciprocal, it follows $g^{\dashv}(x)$ is also a non-self-reciprocal irreducible factor of $E_{3p^i}(x)$. Hence $h(x) \coloneqq g(x)g^{\dashv}(x) \in \mathbb{Z}[x]$ is a self-reciprocal factor of $E_{3p^i}(x)$.

As both $f(x)$ and $h(x)$ are self-reciprocal polynomials of even degree, the reciprocal transforms $f^*(x), h^*(x) \in \mathbb{Z}[x]$ exist. By Dickson's Theorem, $f^*(x)$ is irreducible. By Theorem 4 of Kleiman (1974), $h^*(x)$ is irreducible. Consequently, $f^*(x)$ and $h^*(x)$ are distinct irreducible factors of $E^*_{3p^i}(x)$. Also note, if $\deg(f) = d$, then $\deg(f^*) = \frac{d}{2}$ and $\deg(h^*) = d$.

It is apparent that $f^*(x-2), h^*(x-2) \in \mathbb{Z}[x]$ are distinct irreducible factors of $E^*_{3p^i}(x-2)$ with $\deg(f^*(x-2)) = \frac{d}{2}$ and $\deg(h^*(x-2)) = d$. By Dumas' Theorem, the Newton Polygons of $f^*(x-2)$ and $h^*(x-2)$ are composed of mutually disjoint segments of the Newton Polygon of $E^*_{3p^i}(x-2)$. Since $\deg(h^*(x-2)) = 2\deg(f^*(x-2))$, the sum of the widths of the segments of the Newton Polygon of $h^*(x-2)$ is twice the sum of the widths of the segments of the Newton Polygon of $f^*(x-2)$. Applying Corollary 6.2.4 to the widths of the segments of the Newton Polygon of $E^*_{3p^i}(x-2)$ from Corollary 6.1.2, it follows that any segment of the Newton Polygon of $f^*(x-2)$ has width $\left(\frac{p-1}{2}\right) p^j$ for some $0 \leq j \leq i-1$.

The segments of the Newton Polygon of $E^*_{3p^i}(x-2)$ with width $\left(\frac{p-1}{2}\right) p^j$ for some $0 \leq j \leq i-1$ all have negative slope. Consequently, if $f^*(x-2) = a_0 + a_1 x + \cdots + a_{\frac{d}{2}} x^{\frac{d}{2}}$, then $ord_p(a_0) > ord_p(a_{\frac{d}{2}}) \therefore$

$ord_p\left(\frac{a_0}{a_{\frac{d}{2}}}\right) > 0$. As the leading and constant coefficients of $E^*_{3p^i}(x-2)$ are both $\pm 3p^i$, it follows $1 < \frac{p}{3} \leq \left|\frac{a_0}{a_{\frac{d}{2}}}\right|$. In other words, the absolute value of the product of the roots of $f^*(x-2)$ is greater than 1.

Every root of $f(x)$ has absolute value 1, so by Proposition 4.2.3 every root of $f^*(x-2)$ is real and between 0 and 1. Therefore, the absolute value of the product of the roots of $f^*(x-2)$ is less than 1, a contradiction. □

Corollary 6.2.6. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. The product of the roots of any factor of $E^*_{3p^i}(x-2)$ is* 1.

Proof. Let $f^*(x-2)$ be a factor of $E^*_{3p^i}(x-2)$. By Lemma 4.2.6, the roots of $f^*(x-2)$ may be partitioned into some number of orbits $Orb^*_2(z_k)$. From Lemma 4.2.8, the product of the elements of each $Orb^*_2(z_k)$ is 1 $\therefore$ the product of all the roots of $f^*(x-2)$ is 1. □

Corollary 6.2.7. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. Up to sign, the leading and constant coefficient of any factor of $E^*_{3p^i}(x-2)$ are equal.*

Proof. Immediate from Corollary 6.2.6. □

Corollary 6.2.8. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. Then $E_{3p^i}(x)$ is a product of at most i irreducible polynomials.*

Proof. From Theorem 6.1.1, each segment of the Newton Polygon of $E^*_{3p^i}(x-2)$ has nonzero slope. On the other hand Corollary 6.2.7 shows that the leading and constant coefficient of any irreducible factor has the same p-valuation. Consequently, by Dumas' Theorem, the Newton Polygon of any irreducible factor of $E^*_{3p^i}(x-2)$ consists of at least two segments from the Newton Polygon of $E^*_{3p^i}(x-2)$. By Corollary 6.1.2, there are $2i$ segments in the Newton Polygon of $E^*_{3p^i}(x-2)$ $\therefore$ there are at most i irreducible factors of $E^*_{3p^i}(x-2)$ $\therefore$ there are at most i irreducible factors of $E^*_{3p^i}(x)$. The result follows from Corollary 4.3.4. □

The special case of $i = 1$ provides the second proof of the irreducibility of $E_{3p}(x)$.

Corollary 6.2.9. *Let $p \geq 5$ be prime. Then $E_{3p}(x)$ is irreducible.*

Proof. Immediate from Corollary 6.2.8. □

6.3 Additional Results

In Helou (1997), Tzermias (2007), and Tzermias (2009), it is shown that for each odd $n \geq 9$ there exists a polynomial $T_n(X) \in \mathbb{Q}[X]$ of degree $r := \frac{n-3-2e_n}{6}$ such that $E_n(X) = n(X^2+X)^{2r}T_n(J(X))$ (Note: $T_n(X)$ is not a Chebyshev Polynomial.) In fact, if $|\mathcal{T}_z| = 6$ for all roots z of $E_n(X)$, then $E_n(X)$ and $T_n(X)$ have the same number of irreducible factors, and for each distinct irreducible factor of $T_n(X)$ of degree d there is a distinct irreducible factor of $E_n(X)$ of degree $6d$. This is leveraged in the mentioned papers to obtain results regarding the Cauchy-Mirimanoff polynomials $E_p(X)$ for primes p because $|\mathcal{T}_z| = 6$ for all roots z of $E_p(X)$ (by Theorem 2.3.4). Theorem 6.2.5 proves $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p^i}(X)$, so $T_{3p^i}(X)$ is studied.

Theorem 6.3.1 (Tzermias (2009))**.** *For odd $n \geq 9$, we have*

$$T_n(X) = \sum_{m=0}^{r} \frac{1}{1+2r-2m}\binom{m+e_n+2r}{3m+e_n}X^m$$

with e_n as in Definition 2.1.2.

Corollary 6.3.2. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. Then*

$$T_{3p^i}(X) = \sum_{m=0}^{\frac{p^i-1}{2}} \frac{1}{p^i - 2m}\binom{m + p^i - 1}{3m} X^m$$

Proof. In Theorem 6.3.1, substitute $n = 3p^i$ and simplify. □

Theorem 6.3.3. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. The Newton Polygon of $T_{3p^i}(X)$ with respect to p has vertices*

$$(0, -i),\ (\frac{p^i - p^{i-1}}{2}, -(i-1)), \cdots,\ (\frac{p^i - p^2}{2}, -2),\ (\frac{p^i - p^1}{2}, -1),\ (\frac{p^i - 1}{2}, 0)$$

Proof. Using Corollary 6.3.2, let

$$a_k \coloneqq \frac{1}{p^i - 2m}\binom{m + p^i - 1}{3m}$$

The following two claims, and their proofs, are enough to determine the Newton Polygon of $T_{3p^i}(X)$

- *Claim 1*: Let $1 \leq j \leq i$. If $\frac{p^i - p^j}{2} < k \leq \frac{p^i - p^{j-1}}{2}$, then $ord_p(a_k) > -j$.
  Fix j with $1 \leq j \leq i$. It is enough to show that $ord_p(p^i - 2k) < j$. By the bound on k, there exists an $\alpha \in \mathbb{Z}$ with $0 \leq \alpha < \left(\frac{p-1}{2}\right) p^{j-1}$ such that $k = \frac{p^i - p^{j-1}}{2} - \alpha$. Let $\beta \coloneqq ord_p(\alpha)$, and note $\beta < j$. Then

  $$ord_p(p^i - 2k) = ord_p(p^{j-1} + 2\alpha) = ord_p(\alpha) = \beta < j$$

- *Claim 2*: Let $0 \leq j \leq i$. If $k = \frac{p^i - p^j}{2}$, then $ord_p(a_k) = -j$.
  Fix j with $0 \leq j \leq i$. Then substituting $k = \frac{p^i - p^j}{2}$ and simplifying,

  $$ord_p(a_k) = -j + ord_p\left(\binom{\frac{p^i - p^j}{2} + p^i - 1}{3\left(\frac{p^i - p^j}{2}\right)}\right) = -j + ord_p\left(\binom{\frac{3p^i - p^j - 2}{2}}{p^j - 1}\right)$$

  Expand the binomial coefficient as

  $$\binom{\frac{3p^i - p^j - 2}{2}}{p^j - 1} = \frac{\left(\frac{3p^i - p^j}{2} - 1\right)}{1}\frac{\left(\frac{3p^i - p^j}{2} - 2\right)}{2} \cdots \frac{\left(\frac{3p^i - p^j}{2} - (p^j - 1)\right)}{p^j - 1}$$

  So it is enough to show that $ord_p\left(\frac{\left(\frac{3p^i - p^j}{2} - \alpha\right)}{\alpha}\right) = 0$ for all $1 \leq \alpha \leq p^j - 1$. Let $\beta \coloneqq ord_p(\alpha)$, and note $\beta < j$. Then

  $$ord_p\left(\frac{\left(\frac{3p^i - p^j}{2} - \alpha\right)}{\alpha}\right) = ord_p\left(\frac{3p^i - p^j}{2} - \alpha\right) - ord_p(\alpha) = \beta - \beta = 0$$

□

Corollary 6.3.4. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. There are exactly i segments in the Newton Polygon of $T_{3p^i}(X)$ with respect to p, and the segments have widths (in order from left to right):*

$$\left(\frac{p-1}{2}\right)p^{i-1},\ \left(\frac{p-1}{2}\right)p^{i-2},\cdots,\ \left(\frac{p-1}{2}\right)p^{1},\ \left(\frac{p-1}{2}\right)$$

Proof. Immediate from Theorem 6.3.3. □

In the case $i = 1$, Corollary 6.3.4 gives a third proof of the irreducibility of $E_{3p}(x)$.

Corollary 6.3.5. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. Then $E_{3p}(x)$ is irreducible.*

Proof. Applying Dumas' Theorem to Corollary 6.3.4 shows that $T_{3p}(X)$ is irreducible. Since $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p}(x)$ by either Theorem 5.2.4 or 6.2.5, the irreducibility of $T_{3p}(X)$ implies the irreducibility of $E_{3p}(x)$. □

From Corollary 6.3.4, a number of results regarding the possible number of factors of $E_{3p^i}(X)$ and their degrees may be obtained. This chapter ends with three such results.

Corollary 6.3.6. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. Then $E_{3p^i}(X)$ has an irreducible factor of degree $d \geq 3(p-1)p^{i-1}$.*

Proof. The widest segment of the Newton Polygon of $T_{3p^i}(X)$ has width $\left(\frac{p-1}{2}\right)p^{i-1}$, so $T_{3p^i}(X)$ has an irreducible factor of degree at least $\left(\frac{p-1}{2}\right)p^{i-1}$. As $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p^i}(x)$ by Theorem 6.2.5, $E_{3p^i}(X)$ has an irreducible factor of degree at least $6\left(\frac{p-1}{2}\right)p^{i-1} = 3(p-1)p^{i-1}$. □

Corollary 6.3.7. *Let $p \geq 5$ be prime and $i \in \mathbb{N}$. Then every irreducible factor of $E_{3p^i}(X)$ has degree $d \geq 3(p-1)$.*

Proof. The least wide segment of the Newton Polygon of $T_{3p^i}(X)$ has width $\frac{p-1}{2}$, so every irreducible factor of $T_{3p^i}(X)$ has degree at least $\frac{p-1}{2}$. As $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p^i}(x)$ by Theorem 6.2.5, every irreducible factor of $E_{3p^i}(X)$ has degree at least $6\frac{p-1}{2} = 3(p-1)$. □

Corollary 6.3.8. *Let $p \geq 5$ be prime. Then $E_{3p^2}(X)$ is either irreducible or a product of two irreducible polynomials of degrees $3(p-1)$ and $3(p-1)p$.*

Proof. By Dumas' Theorem, either $T_{3p^2}(X)$ is irreducible or a product of two irreducible polynomials of degrees $\left(\frac{p-1}{2}\right)p$ and $\left(\frac{p-1}{2}\right)$. As $|\mathcal{T}_z| = 6$ for all roots z of $E_{3p^2}(x)$ by Theorem 6.2.5, $E_{3p^2}(X)$ is either irreducible or a product of two irreducible polynomials of degrees $3(p-1)$ and $3(p-1)p$. □

Bibliography

Beukers, F. (1997). On a sequence of polynomials. *J. Pure Appl. Algebra*, 117/118:97–103. Algorithms for algebra (Eindhoven, 1996).

Dickson, L. E. (1908). Criteria for the irreducibility of a reciprocal equation. *Bull. Amer. Math. Soc.*, 14(9):426–430.

Helou, C. (1997). Cauchy-Mirimanoff polynomials. *C. R. Math. Rep. Acad. Sci. Canada*, 19(2):51–57.

Kleiman, H. (1974). On irreducibility criteria of Dickson. *J. London Math. Soc. (2)*, 7:467–475.

Kronecker, L. (1857). Zwei sätze über Gleichungen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 53:173–175.

Mason, J. C. and Handscomb, D. C. (2003). *Chebyshev polynomials*. Chapman & Hall/CRC, Boca Raton, FL.

Meyn, H. (1990). On the construction of irreducible self-reciprocal polynomials over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 1(1):43–53.

Mirimanoff, D. (1903). Sur l'équation $(x + 1)^l - x^l - 1 = 0$. *Nouv. Ann. Math.*

Mott, J. L. (1995). Eisenstein-type irreducibility criteria. In *Zero-dimensional commutative rings (Knoxville, TN, 1994)*, volume 171 of *Lecture Notes in Pure and Appl. Math.*, pages 307–329. Dekker, New York.

Nanninga, P. (2009). *Euclidean and Hyperbolic Diophantine Equations (Under Revision)*. PhD thesis, Australian National University, Canberra.

Ribenboim, P. (1979). *13 lectures on Fermat's last theorem*. Springer-Verlag, New York.

Rivlin, T. J. (1990). *Chebyshev polynomials*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, second edition. From approximation theory to algebra and number theory.

Tzermias, P. (2007). On Cauchy-Liouville-Mirimanoff polynomials. *Canad. Math. Bull.*, 50(2):313–320.

Tzermias, P. (2009). On Cauchy-Liouville-Mirimanoff polynomials II. Preprint.

Appendices

Appendix A

Numerical Evidence Supporting Conjectures 2.3.10 and 2.3.11

In Section 2.3.2, Conjecture 2.3.10 and Conjecture 2.3.11 deal with the minimal number of irreducible factors of $\underline{E_n}$ over $\mathbb{F}_p$ for any prime p. In fact, the two conjectures, if proven, would prove the irreducibility of the Cauchy-Mirimanoff polynomials. In Table A.1, the first ten primes p such that, for odd n, $\underline{E_n}$ factors into exactly two distinct irreducible polynomials over $\mathbb{F}_p$ are given. This table provides numerical support to Conjecture 2.3.10. In Table A.2, the first ten primes p such that, for even n, $\underline{E_n}$ is irreducible over $\mathbb{F}_p$ are given. This table provides numerical support to Conjecture 2.3.11. While listing one prime would be sufficient to support the conjectures, the first ten primes are given to satisfy the curious reader that may be interested in looking for patterns or distributions amongst these primes.

Table A.1: For odd n, the first ten primes p, not dividing $Disc(E_n(X))$, such that E_n factors into exactly two distinct irreducible polynomials over $\mathbb{F}_p$

Odd n	First Ten Primes p
9	2, 7, 11, 19, 29, 37, 41, 47, 53, 73
11	2, 5, 7, 19, 41, 59, 71, 97, 101, 103
13	3, 11, 13, 17, 29, 47, 79, 97, 103, 109
15	11, 31, 41, 53, 67, 79, 83, 89, 173, 227
17	11, 29, 31, 53, 97, 103, 139, 199, 233, 239
19	13, 31, 79, 103, 109, 179, 199, 227, 239, 251
21	97, 109, 113, 167, 331, 349, 379, 463, 491, 499
23	23, 109, 227, 233, 347, 359, 367, 409, 421, 547
25	59, 149, 283, 307, 347, 353, 367, 383, 401, 467
27	113, 229, 269, 313, 353, 401, 479, 547, 571, 593
29	71, 83, 107, 181, 229, 359, 397, 587, 617, 691
31	23, 47, 79, 97, 157, 317, 367, 443, 463, 491
33	41, 73, 107, 173, 281, 313, 547, 593, 661, 683
35	113, 467, 563, 1069, 1103, 1163, 1237, 1279, 1307, 1321
37	31, 37, 79, 97, 269, 311, 457, 467, 503, 769

Continued on Next Page...

Table A.1 – Continued

Odd n	First Ten Primes p
39	11, 79, 353, 379, 449, 467, 571, 617, 787, 877
41	179, 233, 347, 389, 401, 463, 827, 1061, 1409, 1871
43	5, 83, 397, 419, 491, 503, 601, 887, 919, 1229
45	29, 151, 167, 331, 463, 887, 1109, 1117, 1223, 1279
47	19, 107, 191, 349, 547, 601, 631, 757, 863, 947
49	127, 337, 569, 601, 761, 857, 1291, 1523, 1559, 1801
51	139, 163, 179, 397, 577, 1097, 1103, 1451, 1489
53	191, 449, 647, 761, 883, 929, 1187, 1201, 1213, 1307
55	41, 389, 491, 659, 1213, 1889, 1907, 2753, 3191, 3469
57	83, 277, 307, 643, 1597, 1759, 1913, 1993, 2207, 2287
59	2, 5, 251, 311, 461, 601, 659, 691, 1301, 1451
61	233, 269, 419, 563, 593, 769, 941, 1069, 1297, 1381
63	41, 79, 127, 131, 179, 227, 239, 353, 419, 431
65	211, 347, 457, 601, 631, 887, 911, 953, 1031, 1039
67	67, 127, 421, 491, 1657, 1999, 2039, 2053, 2239, 2423
69	101, 191, 211, 401, 683, 1429, 1621, 1663, 1993, 2557
71	317, 1321, 1663, 2647, 2833, 3119, 3187, 3373, 3457, 4021
73	23, 179, 467, 953, 991, 1117, 1543, 2141, 2551, 2897
75	263, 421, 457, 563, 643, 733, 839, 2111, 2311, 2621
77	89, 313, 509, 661, 829, 1301, 1327, 1481, 1511, 1693
79	61, 89, 401, 701, 761, 919, 1021, 1229, 1459, 1627
81	199, 617, 911, 1277, 2143, 2447, 2647, 3697, 4229, 4441
83	29, 131, 433, 577, 1129, 2131, 2591, 2909, 3299, 3709
85	223, 499, 787, 797, 1063, 1277, 2617, 2803, 3259, 3673
87	167, 257, 397, 461, 577, 1423, 1627, 2339, 2617, 2633
89	7, 223, 461, 619, 941, 971, 1319, 1543, 1889, 2011
91	79, 109, 131, 307, 313, 337, 853, 1303, 1373, 1483
93	709, 1493, 1723, 1877, 1973, 2027, 2063, 2909, 3307, 3319
95	13, 397, 1303, 1321, 1439, 1483, 2087, 2357, 2687, 2969
97	151, 457, 719, 1087, 2957, 2999, 3257, 3623, 3761, 4447
99	23, 647, 761, 1409, 1433, 1567, 1901, 1987, 2111, 2333

Table A.2: For even n, the first ten primes p, not dividing $Disc(E_n(X))$, such that E_n is irreducible over $\mathbb{F}_p$

Even n	First Ten Primes p
8	3, 5, 43, 53, 109, 181, 233, 241, 257, 281
10	23, 59, 67, 71, 89, 103, 131, 167, 269, 271
12	5, 13, 31, 41, 53, 79, 127, 239, 349, 353
14	103, 107, 223, 281, 401, 409, 457, 491, 601, 613
16	5, 71, 173, 239, 373, 409, 443, 751, 929, 953
18	7, 13, 61, 151, 163, 173, 337, 397, 569, 631
20	83, 113, 577, 631, 859, 863, 881, 937, 1051, 1609
22	67, 229, 347, 491, 821, 859, 1129, 1499, 1549, 1583
24	5, 269, 431, 457, 487, 557, 709, 757, 1399, 1427
26	43, 139, 431, 1051, 1181, 1433, 1453, 1559, 1733, 1973
28	23, 307, 373, 419, 467, 587, 619, 701, 727, 977
30	7, 31, 61, 739, 823, 911, 1031, 1291, 1543, 1663
32	467, 673, 739, 863, 1093, 1109, 1231, 1453, 1543, 1669
34	277, 467, 499, 557, 719, 727, 1049, 1171, 1223, 1229
36	149, 373, 619, 823, 829, 1063, 1153, 1319, 1439, 1907
38	89, 197, 283, 313, 719, 991, 1091, 1307, 2003, 2423
40	193, 503, 839, 881, 907, 1277, 1289, 1459, 1667, 1823
42	59, 521, 661, 1187, 1429, 2339, 2687, 3253, 3413, 3457
44	281, 487, 577, 1013, 1181, 1607, 1697, 1901, 2293, 2549
46	1097, 1117, 1201, 1399, 1567, 1951, 2237, 2477, 3221, 3457
48	163, 181, 367, 491, 641, 997, 1601, 1627, 2381, 2447
50	701, 1399, 1993, 2251, 2393, 2957, 3109, 3491, 3517, 4373
52	17, 293, 733, 1163, 1637, 1787, 2153, 2179, 2267, 2699
54	607, 673, 881, 1277, 2239, 3251, 3613, 4111, 4289, 4591
56	359, 1021, 1153, 1459, 2213, 3253, 3301, 3343, 3853, 4093
58	593, 1249, 1901, 1979, 2381, 2551, 2729, 2927, 2999, 3847
60	61, 769, 887, 1523, 1621, 1847, 3079, 3847, 4783, 5507
62	37, 2699, 3169, 4603, 4673, 5023, 5209, 5581, 6653, 7349
64	13, 61, 97, 467, 523, 709, 1087, 1249, 1619, 1949
66	307, 563, 727, 2447, 3469, 3547, 3697, 3833, 4451, 4513
68	167, 277, 293, 659, 1861, 2179, 3067, 3853, 5987, 8581
70	37, 107, 701, 1229, 2399, 3701, 4271, 4337, 4733, 5167
72	449, 457, 479, 839, 911, 1039, 1609, 2141, 2473, 2549
74	769, 991, 1091, 1997, 2089, 3001, 4099, 4951, 4957, 5003
76	73, 149, 331, 617, 2137, 2161, 2861, 3863, 4007, 4127
78	131, 197, 1579, 2087, 3889, 3917, 4651, 6361, 6581, 6917
80	3, 653, 1237, 2131, 2237, 2683, 3169, 3301, 3313, 3673
82	647, 2729, 3067, 3229, 3251, 3413, 3637, 4273, 4289, 4919
84	17, 311, 821, 1861, 3067, 3547, 3583, 3623, 4447, 6823
86	5867, 6287, 7151, 8779, 9733, 10259, 11243, 11321, 11939, 12163

Continued on Next Page...

Table A.2 – Continued

Even n	First Ten Primes p
88	139, 821, 1033, 1759, 1877, 2251, 2381, 3559, 3929, 10883
90	283, 599, 2579, 2687, 3671, 4259, 4357, 4721, 5021, 5303
92	41, 337, 857, 1277, 1847, 3457, 3511, 3559, 4021, 4177
94	439, 2269, 5021, 5507, 5569, 6827, 8081, 8117, 8233, 8839
96	251, 911, 1051, 1423, 2647, 3119, 3169, 3853, 4339, 5527
98	367, 373, 1399, 1607, 1931, 2273, 2909, 4871, 6287, 6689
100	719, 2357, 2731, 3449, 4201, 4561, 6427, 6571, 7159, 7591

Vita

Brian Irick was raised in West Tennessee near Memphis. He graduated from Haywood High School in 1999, and thereafter attended the University of Tennessee, Knoxville, for his undergraduate education. He received a Bachelor of Science with a dual major in Mathematics and Physics in 2003. He stayed at UTK to pursue a doctoral degree in Mathematics, which was earned in May 2010.