Summer 2021

Polynomials, Primes and the PTE Problem

Joseph C. Foster

Polynomials, Primes and the PTE Problem

by

Joseph C Foster

Master of Mathematics
University of Leicester, 2015

Master of Research
University of Leicester, 2017

Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy in

Mathematics

College of Arts and Sciences

University of South Carolina

2021

Accepted by:

Michael Filaseta, Major Professor

Matthew Boylan, Committee Member

Ralph Howard, Committee Member

Alexander Duncan, Committee Member

Karl Gregory, Committee Member

Tracey L. Weldon, Interim Vice Provost and Dean of the Graduate School

Dedication

To Bailey.

Acknowledgments

First and foremost, Michael Filaseta. Thank you for liking fun problems and disliking the Oxford comma. I hope that I become a teacher as successful as you have been.

Acknowledging every professor that has had a role in my development as a mathematician would be an essay in and of itself, but there is one professor at the top of that list that needs to be mentioned here. Dr. Murray; It was your number theory class back in 2012 that condemned me to this path. You're to blame for why almost a decade later I still don't have a real job. Thank you good sir.

To my alliterative academic brethren Jacob and Jeremiah. Our genuinely joyful and justifiably juvenile jaunt from jittery jackasses doing Girardi's jumbo homeworks to jubilant journeymen with jobs just ended. Thanks for being the brothers I didn't want.

How does one spend ten years thinking about numbers without going insane you ask? Well, they don't. So it helps to be surrounded by a group of people that make it seem that that's socially acceptable. In order of appearance; Louis, Amarpreet, Henry, Nina, Corrie, Rianne, another Nina, Diana, Patrick, Aiyana, Sarah, Kate, Jared, Rosie, Laura, Venexia, Villy, Maggie, Dom, Rob, Claire, Steph, Lara, Dan and Greg. Super awks if I forgot someone....

To Danielle. Of all the things I will take away from South Carolina, the time spent with you is what I am most grateful for. Thank you.

Of course I saved the best till last. Mum. I may have been able to write this almost 100 page dissertation but writing my appreciation to you is something I can never do justice. I owe you everything and I love you.

Abstract

This dissertation considers three different topics. In the first part of the dissertation, we use Newton Polygons to show that for the arithmetic functions $g(n) = n^t$, where $t \geq 1$ is an integer, the polynomials defined with initial condition $P_0^g(X) = 1$ and recursion

$$P_n^g(X) = \frac{X}{n} \sum_{k=1}^{n} g(k) P_{n-k}^g(X)$$

are $X/(n!)$ times an irreducible polynomial.

In the second part of the dissertation, we show that, for $3 \leq n \leq 8$, there are infinitely many 2-adic integer solutions to the Prouhet-Tarry-Escott (PTE) problem, that are not rational integer solutions. In particular, we look at the 2-adic valuation of a certain constant associated with the PTE problem and for the case $n = 8$ there exist solutions whose valuation is strictly less than any known rational integer solution.

In the third part of the dissertation, we obtain a number of results pertaining to polynomials $f(x)$ with non-negative integer coefficients that take on a prime value at $x = b$, where $b \geq 2$ is an integer. In particular, we give an explicit bound $M_1(b)$ such that if the coefficients of $f(x)$ are each $\leq M_1(b)$, then $f(x)$ is irreducible. We also show that there are similarly explicit bounds $M_2(b)$, $M_3(b)$ and $M_4(b)$, for b sufficiently large (made explicit), that can be placed on the coefficients of $f(x)$ such that if $f(x)$ is reducible then it must be divisible by at least one of the shifted cyclotomic polynomials $\Phi_3(x-b)$, $\Phi_4(x-b)$ or $\Phi_6(x-b)$.

Table of Contents

Dedication iii

Acknowledgments iv

Abstract v

Chapter 1 Introduction 1

1.1 Irreducibility of a Family of Polynomials using Newton Polygons . . . 1

1.2 2-adic integer solutions to the Prouhet-Tarry-Escott problem 3

1.3 Irreducibility Criteria for Non-negative Integer Coefficient Polynomials 7

Chapter 2 Irreducibility of a Family of Polynomials using Newton Polygons 12

2.1 Preliminary Material 12

2.2 An Explicit Formulation of the Coefficients 13

2.3 Constructing the Newton polygons 15

2.4 Proof of Theorem 1.2 24

Chapter 3 2-adic integer solutions to the Prouhet-Tarry-Escott problem 25

3.1 Preliminary Material 25

3.2 Sequences of Ideal PTE Solutions modulo 2^k 32

3.3 2-adic Integer Solutions 55

Chapter 4 Irreducibility Criteria for Non-negative Integer Coefficient Polynomials 57

4.1 A Root Bounding Function 58

4.2 Bounds Based on Recurrence Relations 62

4.3 Establishing Bounds 72

4.4 Comparing the Bounds and Establishing Theorem 1.6 89

Bibliography 91

Chapter 1

Introduction

1.1 Irreducibility of a Family of Polynomials using Newton Polygons

In [24], Heim and Neuhauser were interested in the family of polynomials defined with initial condition $P_0(X) = 1$ and recursion

$$P_n(X) = \frac{X}{n} \sum_{k=1}^{n} \sigma(k) P_{n-k}(X) \tag{1.1}$$

for $n \geq 1$, where $\sigma(n)$ is the sum of divisors function. These polynomials arise as Fourier coefficients of powers of the Dedekind eta functions, shown by Newman in [32]. In [23], Heim, Luca and Neuhauser generalised the recurrence relation in (1.1) by replacing $\sigma(n)$ with other arithmetic functions. Namely, they studied the following.

Definition 1.1. Let $g(n)$ be an arithmetic function. Define a family of polynomials $P_n^g(X)$ associated with g by $P_0^g(X) := 1$ and

$$P_n^g(X) = \frac{X}{n} \sum_{k=1}^{n} g(k) P_{n-k}^g(X).$$

In particular they looked at the coefficients of X in $P_n^g(X)$ when $g(n) = n$ and $g(n) = n^2$ as these functions provide bounds on $\sigma(n)$. They found explicit formulas for the coefficients and concluded

$$P_n^n(X) = X \sum_{k=0}^{n-1} \frac{1}{(k+1)!} \binom{n-1}{k} X^k \quad \text{and} \quad P_n^{n^2}(X) = X \sum_{k=0}^{n-1} \frac{1}{(k+1)!} \binom{n+k}{2k+1} X^k.$$

In [23], Heim, Lucas and Neuhauser looked further at these polynomials. One of the results they obtained was the irreducibility of the polynomials

$$\widetilde{P}_n^n(X) = \frac{n!}{X} P_n^n(X) = \sum_{k=0}^{n-1} \frac{n!}{(k+1)!} \binom{n-1}{k} X^k.$$

They also conjectured the irreducibility of the polynomials

$$\widetilde{P}_n^{n^2}(X) = \frac{n!}{X} P_n^{n^2}(X) = \sum_{k=0}^{n-1} \frac{n!}{(k+1)!} \binom{n+k}{2k+1} X^k,$$

a result that was proven by J. Juillerat, J. Southwick and the author in [19].

Chapter 2 discusses the work between J. Southwick and the author to generalise the result of J. Juillerat, J. Southwick and the author. We look at the irreducibility of the polynomials that arise when $g(n) = n^t$ for any positive integer t. To obtain these polynomials, we modify the derivation of the polynomials in [24]. We begin by an observation from [23] that

$$\sum_{n=0}^{\infty} P_n^{n^t}(X)\, q^n = \exp\left(X \sum_{n=1}^{\infty} \frac{n^t}{n} q^n \right). \tag{1.2}$$

We expand the right-hand side of (1.2) and manipulate it to compare formally the coefficients of the different powers of q. We have

$$\begin{aligned}
\exp\left(X \sum_{n=1}^{\infty} \frac{n^t}{n} q^n \right) &= 1 + \sum_{k=1}^{\infty} \frac{1}{k!} X^k \left(\sum_{n=1}^{\infty} n^{t-1} q^n \right)^k \\
&= 1 + \sum_{k=1}^{\infty} \frac{1}{k!} X^k \left(\sum_{m_1=1}^{\infty} \cdots \sum_{m_k=1}^{\infty} m_1^{t-1} \cdots m_k^{t-1} q^{m_1+\cdots+m_k} \right) \\
&= 1 + \sum_{n=1}^{\infty} \sum_{k=1}^{n} \frac{1}{k!} X^k \left(\sum_{m_1+\cdots+m_k=n} m_1^{t-1} \cdots m_k^{t-1} \right) q^n,
\end{aligned}$$

where, in the innermost sum, the m_i are positive integers. Thus for $n \geq 1$ we obtain

$$P_n^{n^t}(X) = \sum_{k=1}^{n} \frac{1}{k!} \left(\sum_{m_1+\cdots+m_k=n} m_1^{t-1} \cdots m_k^{t-1} \right) X^k.$$

For $1 \leq k \leq n$ and t a positive integer, define

$$S(k \mid n, t) = \sum_{m_1+\cdots+m_k=n} m_1^t \cdots m_k^t.$$

Consequently the main goal of this work is to prove the following

Theorem 1.2. *The polynomials*

$$f\left(x \mid n, t\right) = \sum_{k=1}^{n} \frac{n!}{k!} S\left(k \mid n, t\right) x^{k-1} \tag{1.3}$$

are irreducible for all integers $n \geq 2$ *and* $t \geq 1$.

Here we note that $P_n^{n^t}\left(X\right) = \left(X/n!\right) f\left(X \mid n, t-1\right)$. The proof of Theorem 1.2 will follow similarly to that of the main result in [19]. In Section 2.1, we define Newton polygons along with stating a theorem of Dumas [12], and we list several results regarding factorials and binomial coefficients. Section 2.2 is dedicated to studying the expressions $S\left(k \mid n, t\right)$ so that we can construct the Newton polygons of $f\left(x \mid n, t\right)$ in Section 2.3. We bring everything together to prove Theorem 1.2 in Section 2.4.

1.2 2-adic integer solutions to the Prouhet-Tarry-Escott problem

For $n \geq 3$, we consider two lists of integers

$$X = \left[x_1, x_2, \ldots, x_n\right] \quad \text{and} \quad Y = \left[y_1, y_2, \ldots, y_n\right],$$

where $x_j \neq y_j$ for some $j \in \{1, 2, \ldots, n\}$, for any reordering of the x_j's. The Prouhet-Tarry-Escott problem (the PTE problem) asks for such X and Y satisfying

$$\sum_{j=1}^{n} x_j^e = \sum_{j=1}^{n} y_j^e \qquad \text{for } e \in \{1, 2, \ldots, k\} \tag{1.4}$$

where k is an integer in the interval $[2, n-1]$. If X and Y satisfy (1.4) then the pair is called a solution of the PTE problem, denoted $X =_k Y$. A solution is *ideal* if $k = n-1$. The significance of the case $k = n-1$ is that with X and Y distinct as required above, it is impossible for (1.4) to hold if $k > n-1$. Thus, the largest possible value for k in (1.4) is $n-1$.

Literature on the PTE problem is extensive. The problem is a focus of an entire chapter (Chapter 24) of L. E. Dickson's classical volumes "History of the Theory of Numbers" [11] and numerous early references can be found there. The problem is

also discussed in G. H. Hardy and E. M. Wright's well-known "An Introduction to the Theory of Numbers" [22], undoubtedly in part due to Wright's own interest in the problem (cf. [42, 43, 44]). We note that for the first half of the twentieth century, the problem was referred to as the Tarry-Escott problem, until Wright [43] pointed out that E. Prouhet [36] first discussed the problem in 1851. A few of the more recent investigations on the PTE problem include [4, 5, 9, 27, 38]. Interesting work on generalisations of the PTE problem can be found in [1, 8]. For applications arising from the PTE problem see [2, 21, 25, 31, 39].

An important open problem in the area is a conjecture of Wright [42] that for every natural number $n \geq 3$, an ideal solution exists. Despite its long history, ideal solutions are only known to exist for $3 \leq n \leq 10$ and $n = 12$. In particular, no ideal solution is known for n = 11.

To help formulate further discussion, we note that the following result and its corollary are fairly simple consequences of properties of elementary symmetric functions (see [3, 4]).

Lemma 1.3. *Let n and k be integers with $1 \leq k < n$. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ denote arbitrary integers. The following are equivalent:*

- $\sum_{j=1}^{n} x_j^e = \sum_{j=1}^{n} y_j^e$, *for* $e \in \{1, 2, \ldots, k\}$,
- $\deg\left(\prod_{j=1}^{n}(z - x_j) - \prod_{j=1}^{n}(z - y_j)\right) \leq n - k - 1$,
- $(z-1)^{k+1} \,\Big|\, \left(\sum_{j=1}^{n} z^{x_j} - \sum_{j=1}^{n} z^{y_j}\right)$.

Corollary 1.4. *The lists $X = [x_1, x_2 \ldots, x_n]$ and $Y = [y_1, y_2 \ldots, y_n]$ give an ideal PTE solution if and only if*

$$\prod_{j=1}^{n}(z - x_j) - \prod_{j=1}^{n}(z - y_j) = C \tag{1.5}$$

for some real constant $C \neq 0$.

We will view ideal PTE solutions over the integers as being a pair of lists $\{X, Y\}$ satisfying (1.5). For computational reasons (see [4, 7, 38]), information on possible values of C and, in particular, on the factorisation of C given (1.5), has played an important role in arriving at examples of ideal PTE solutions. As C depends on n, X and Y, we define, for $X =_{n-1} Y$, the constant

$$C_n = C_n(X, Y) = \prod_{j=1}^{n} (z - x_j) - \prod_{j=1}^{n} (z - y_j).$$

Define

$$\overline{C}_n = \prod_{j=1}^{\infty} p_j^{e_j}, \tag{1.6}$$

where p_j is the jth prime number and

$$e_j = \min\left\{e \mid p_j^e || C_n(X, Y) \text{ for some } X \text{ and } Y \text{ as above with } X =_{n-1} Y\right\}.$$

The values of $\overline{C}_n$ for $3 \le n \le 7$ are known (see [7]):

$$\begin{aligned}
\overline{C}_3 &= 2^2 \\
\overline{C}_4 &= 2^2 \cdot 3^2 \\
\overline{C}_5 &= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \\
\overline{C}_6 &= 2^5 \cdot 3^2 \cdot 5^2 \\
\overline{C}_7 &= 2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11.
\end{aligned}$$

For $n = 8$ and $n = 9$, [7] also gives

$$\begin{aligned}
\overline{C}_8 &= 2^{e_1} \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \\
\overline{C}_9 &= 2^{e_2} \cdot 3^{e_3} \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17^{e_4} \cdot 23^{e_5} \cdot 29^{e_6}
\end{aligned}$$

where

$$4 \le e_1 \le 8, \quad 7 \le e_2 \le 9, \quad 3 \le e_3 \le 4 \quad \text{and} \quad 0 \le e_j \le 1 \text{ for } j \in \{4, 5, 6\}. \tag{1.7}$$

In their paper, Filaseta and Markovich [18] improved on (1.7) and showed, using Newton polygons, that

$$6 \leq e_1 \leq 8 \quad \text{and} \quad e_2 = 9.$$

In the same paper, for $n = 8$, they gave the example

$$\begin{aligned} X = [&31914804930538, 392011859134314, 414199788923609, \\ &550721232905543, 563570240533272, 870589495146520, \\ &1039460985683225, 1113937730497799\ ] \end{aligned}$$

and

$$\begin{aligned} Y = [&226375709153429, 382003430459158, 502458387218286, \\ &690280771238587, 750383096702563, 764464731978500, \\ &790357673966989, 870082337037308\ ] \end{aligned}$$

which has the property that

$$\prod_{j=1}^{8} (z - x_j) - \prod_{j=1}^{8} (z - y_j) \equiv 95466849288194 \pmod{2^{50}},$$

where it should be observed that the number 95466849288194 is exactly divisible by 2^6. Filaseta and Markovich posed three questions based on the existence of this example:

Question 1. Is it possible to show that a 2-adic ideal solution exists for the PTE problem for every $n \geq 3$?

Question 2. For a prime, p, is it possible to have a p-adic solution to

$$\prod_{j=1}^{n} (z - x_j) - \prod_{j}^{n} (z - y_j) = C,$$

for which $\nu_p(C) < \nu_p\left(\overline{C}_n\right)$, where ν_p is the usual p-adic valuation and n is some integer ≥ 3?

Question 3. For a prime, p, does a p-adic ideal solution necessarily exist for $n = 11$?

In this chapter, we will address Question 1 restricted to $3 \leq n \leq 8$. Namely, we will prove the following.

Theorem 1.5. *For $3 \leq n \leq 8$ there exist lists of 2-adic integers $X = [x_1, x_2, \ldots x_n]$ and $Y = [y_1, y_2, \ldots y_n]$, such that at least one x_j or y_j is not in $\mathbb{Q}$, that satisfy*

$$\prod_{j=1}^{n} (z - x_j) - \prod_{j=1}^{n} (z - y_j) = C_n,$$

for some 2-adic integer C_n with $\nu_2(C_n) = k_n$, where

$$k_n = \begin{cases} 2 & \text{if } n = 3, 4, \\ 4 & \text{if } n = 5, \\ 5 & \text{if } n = 6, \\ 6 & \text{if } n = 7, 8. \end{cases}$$

The case $n = 8$ is particularly significant as there are currently no known examples over the integers where the same equation holds with $\nu_2(C_8) = 6$.

1.3 Irreducibility Criteria for Non-negative Integer Coefficient Polynomials

If $d_n d_{n-1} \ldots d_1 d_0$ is the decimal representation of a prime, then a result of A. Cohn [34] asserts that

$$f(x) = d_n x^n + d_{n-1} x^{n-1} + \cdots + d_1 x + d_0$$

is irreducible over the integers. If we generalise this setting and view $f(x)$ as a polynomial with non-negative integer coefficients and with $f(10)$ prime, does the irreducibility of $f(x)$ depend on the coefficients being less than 10? Is the base 10 special, or do similar results hold when 10 is replaced by a different base $b \geq 2$?

Some answers to these questions can be found in the literature. The result of Cohn has been extended to all bases $b \geq 2$ by J. Brillhart, M. Filaseta and A. Odlyzko [6]. In [15], M. Filaseta extended this to base b representations of kp where k is a positive integer $< b$ and p is a prime, and M. R. Murty [37] has obtained an analog in function fields over finite fields. Furthermore, [6] allows the coefficients d_j in Cohn's theorem to satisfy $0 \leq d_j \leq 167$ rather than $0 \leq d_j \leq 9$; and later M. Filaseta [16] showed that the d_j need only satisfy $0 \leq d_j \leq 10^{30} d_n$, and further that simply $d_j \geq 0$ suffices if $n \leq 31$.

Recent work by M. Filaseta and S. Gross [17] extended this last line of investigation even further. They showed that if $f(x)$ is a polynomial with non-negative coefficients bounded above by

$$495986669891512260981042445129 18$$

and $f(10)$ is prime, then $f(x)$ is irreducible over $\mathbb{Z}$. They also showed that if the coefficients are instead bounded above by

$$859244474352913581576954595593 6773,$$

then $f(x)$ is either irreducible over $\mathbb{Z}[x]$ or divisible by $x^2 - 20x + 101$. Furthermore, they showed that these values are sharp, in that they exhibited polynomials having non-negative integer coefficients with $f(10)$ prime and maximum coefficient one more than each of these numbers where in each case the polynomial factors in $\mathbb{Z}[x]$ and in the latter case is not divisible by $x^2 - 20x + 101$.

In [10], M. Cole, S. Dunn and M. Filaseta extended these results and found bounds $M_1(b)$ such that if the coefficients of $f(x)$ are bounded above by $M_1(b)$ and $f(b)$ is prime for an integer $b \in [2, 20]$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$. They also found bounds $M_2(b)$ such that if the coefficients of $f(x)$ are bounded above by $M_2(b)$ and $f(b)$ is prime for $3 \leq b \leq 5$, then $f(x)$ is either irreducible or divisible by $\Phi_3(x - b)$, where $\Phi_n(x)$ is the nth cyclotomic polynomial. Similarly, if $6 \leq b \leq 20$ and the

coefficients of $f(x)$ are bounded above by $M_2(b)$, then $f(x)$ is either irreducible or divisible by $\Phi_4(x-b)$. Furthermore, they established that the upper bounds $M_1(b)$ are sharp for $3 \leq b \leq 20$, and that the upper bounds $M_2(b)$ are sharp for $4 \leq b \leq 20$.

Work by M. Filaseta, J. Juillerat, J. Southwick and the author extends the results in [10] to all integers $b > 2$. That is, we prove the following.

Theorem 1.6. *Let $b \in \mathbb{Z}$ with $b > 2$. Let $f(x)$ be a polynomial with non-negative integer coefficients and $f(b)$ prime. For $n \in \mathbb{Z}^+$, let $\Phi_n(x)$ be the n^{th} cyclotomic polynomial and $\zeta_n = e^{2\pi i/n}$. Define*

$$\mathcal{B}_b^{(n)} = \max_{i\in\{0,1\}} \left(\sum_{k=0}^{\lfloor \frac{D_n-i}{2} \rfloor} \binom{D_n-i}{2k+1} (b+\operatorname{Re}(\zeta_n))^{D_n-2k-1-i} (-\operatorname{Im}(\zeta_n))^k \right) \Phi_n(1-b),$$

with $D_n = \lfloor \pi/\arg(b+\zeta_n) \rfloor$, and let

$$M_1(b) = \min_{n\in\{3,4\}} \mathcal{B}_b^{(n)}, \quad M_2(b) = \max_{n\in\{3,4\}} \mathcal{B}_b^{(n)}, \quad M_3(b) = \mathcal{B}_b^{(6)}$$

and

$$M_4(b) = \frac{(b-1.5221)^\kappa (b-2.5221)}{1+\cot(\pi/b^2)}, \quad \text{with} \quad \kappa = \left\lfloor \frac{(b^2-1)\pi}{b^2 \arctan\left(\frac{0.8444}{(b-0.2)}\right)} \right\rfloor.$$

Then

- *If $b > 2$ and each coefficient of $f(x)$ is less than $M_1(b)$, then $f(x)$ is irreducible.*
- *If $b > 2$ and each coefficient of $f(x)$ is less than $M_2(b)$ and $f(x)$ is reducible, then it is divisible by $\Phi_3(x-b)$ if $b \leq 5$ and divisible by $\Phi_4(x-b)$ if $b > 5$.*
- *If $b > 69$ and each coefficient of $f(x)$ is less than $M_3(b)$ and $f(x)$ is reducible, then it is divisible by at least one of $\Phi_3(x-b)$ or $\Phi_4(x-b)$.*
- *If $b > 69$ and each coefficient of $f(x)$ is less than $M_4(b)$ and $f(x)$ is reducible, then it is divisible by $\Phi_3(x-b)$, $\Phi_4(x-b)$ or $\Phi_6(x-b)$.*

In particular, for $b > 5$, $M_1(b)$ is equal to

$$\max_{i\in\{0,1\}} \left(\sum_{0\le k\le \frac{D_4-i}{2}} \binom{D_4-i}{2k+1} \left(-b^2\right)^k \right) \left(b^2-2b+2\right) b^{D_4-1-i}.$$

For $b = 10$, this gives

$$M_1\left(10\right) = 4959866698915122609810424451291 8,$$

which agrees with the bound by M. Filaseta and S. Gross given above.

Whereas M. Cole, S. Dunn and M. Filaseta were able to show for a fixed $b \in [4, 20] \cap \mathbb{Z}$ that the given upper bounds are sharp, we were not able to do so for general $b \geq 2$. However, the bounds in Theorem 1.6 agree with the prior sharp bounds obtained for $4 \leq b \leq 20$, and we conjecture the bounds for $M_1(b)$, $M_2(b)$ and $M_3(b)$ in Theorem 1.2 are sharp for all $b \geq 4$. Furthermore, the values $M_1(b)$, $M_2(b)$ and $M_3(b)$ are sharp in another way: For $b > 5$, if $\Phi_4(x-b)$ is a factor of $f(x)$ and $f(x)$ has non-negative coefficients (and where we no longer require that $f(b)$ is prime), then the largest coefficient must be at least as large as $M_1\left(b\right)$. Similarly, if $\Phi_3(x-b)$ is a factor of $f(x)$ and $f(x)$ has non-negative coefficients (and where we no longer require that $f(b)$ is prime), then the largest coefficient must be at least as large as $M_2\left(b\right)$. Finally, if $\Phi_6(x-b)$ is a factor of $f(x)$ and $f(x)$ has non-negative coefficients (and where we no longer require that $f(b)$ is prime), then the largest coefficient must be at least as large as $M_3\left(b\right)$.

The main focus of Chapter 4 is to provide the details on how to find the bounds $M_1(b)$, $M_2(b)$ and $M_3(b)$.

While Theorem 1.6 focuses on bounding the coefficients of $f(x)$, a secondary goal of our work was to examine the situation where the coefficients are unbounded (non-negative) integers with $f(b)$ prime for an integer $b \geq 2$. In this setting, what can be said about the irreducibility of such a polynomial? The existing literature provides some preliminary answers. M. Filaseta [16] has shown that for all $b \geq 2$, if the degree of such an $f(x)$ is bounded above by $\pi/\arcsin(1/b)$, then $f(x)$ is irreducible.

M. Cole, S. Dunn and M. Filaseta [10] further showed that for $2 \leq b \leq 20$ there are sharp bounds $D(b), D_1(b)$, and $D_2(b)$ on the degree of $f(x)$ so that if $f(x)$ has degree less than or equal to $D(b)$, then $f(x)$ is irreducible; if $f(x)$ has degree less than or equal to $D_1(b)$, then $f(x)$ is only reducible if it is divisible by $\Phi_4(x-b)$; while if $f(x)$ has degree less than or equal to $D_2(b)$, then $f(x)$ must be divisible by $\Phi_3(x-b)$ or $\Phi_4(x-b)$. The theorem below extends these ideas to all $b \geq 2$ and for $b \geq 26$ integrates a similar divisibility condition with $\Phi_6(x-b)$.

Theorem 1.7. *Fix an integer $b \geq 5$, and for $n \in \{3,4,6\}$ set*

$$D_n = D_n(b) = \left\lfloor \frac{\pi}{\arg(b+\zeta_n)} \right\rfloor \qquad \text{and} \qquad E = E(b) = \left\lfloor \frac{\pi}{\arctan\left(\frac{1732}{1000(2b+1)}\right)} \right\rfloor.$$

Let $f(x) \in Z[x]$ with non-negative coefficients and with $f(b)$ prime. If the degree of $f(x)$ is $\leq D_4$, then $f(x)$ is irreducible. Additionally, if the degree of $f(x)$ is $\leq D_3$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$. Furthermore, in the case that $b \geq 27$, if the degree of $f(x)$ is $\leq D_6$ and $f(x)$ is reducible, then $f(x)$ is divisible by either $\Phi_4(x-b)$ or $\Phi_3(x-b)$. Lastly, in the case that $b \geq 27$, if the degree of $f(x)$ is $\leq E$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_3(x-b)$, $\Phi_4(x-b)$, or $\Phi_6(x-b)$.

The proof of Theorem 1.7 is given in J. Southwick's dissertation [40].

Chapter 2

Irreducibility of a Family of Polynomials using Newton Polygons

2.1 Preliminary Material

We first introduce the notion of Newton polygons. Let $f(x) = \sum_{j=0}^{r} a_j x^j \in \mathbb{Z}[x]$ with $a_0 a_r \neq 0$ and fix a prime p. For an integer $m \neq 0$, denote $\nu_p(m)$ to be the p-adic valuation of m, that is, the exponent in the largest power of p dividing m. Let S be the set of lattice points $(j, \nu_p(a_{r-j}))$ for $0 \leq j \leq r$ with $a_{r-j} \neq 0$. The Newton polygon of $f(x)$ with respect to the prime p is the polygonal path along the lower convex hull of these points from $(0, \nu_p(a_r))$ to $(r, \nu_p(a_0))$. The endpoints of every edge belong to the set S, and the slopes of the edges strictly increase as we move from left to right along the Newton polygon.

Newton polygons hold a wealth of information regarding the irreduciblity of a polynomial. The main result we use regarding Newton polygons is due to Dumas ([12], [35]) and relates the Newton polygon of two polynomials to the Newton polygon of their product.

Theorem 2.1. *Let $g(x)$ and $h(x)$ be in $\mathbb{Z}[x]$ with $g(0)h(0) \neq 0$, and let p be a prime. Let k be a non-negative integer such that p^k divides the leading coefficient of $g(x)h(x)$ but p^{k+1} does not. Then the edges of the Newton polygon for $g(x)h(x)$ with respect to p can be formed by constructing a polygonal path beginning at $(0, k)$ and using translates of the edges in the Newton polygons for $g(x)$ and $h(x)$ with respect to the prime p, using exactly one translate for each edge of the Newton polygons for $g(x)$*

and $h(x)$. Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing from left to right.

We prove Theorem 1.2 by explicitly constructing the Newton polygons for the polynomials $f(x \mid n, t)$, for each prime p dividing $n-1$. To do this we make use of three lemmas regarding binomial coefficients, factorials and their p-adic valuation. The first is a classical result of Legendre [29].

Lemma 2.2. *Let n be a positive integer, and let p be a prime. Let $s_p(n)$ denote the sum of the base p digits of n. Then*

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Lemma 2.2 implies the following result due to Kummer [28].

Lemma 2.3. *Let n and j be integers with $0 \leq j \leq n$. Then*

$$\nu_p\left(\binom{n}{j}\right) = \frac{s_p(j) + s_p(n-j) - s_p(n)}{p-1}.$$

Equivalently, $\nu_p\left(\binom{n}{j}\right)$ is the number of borrows encountered when subtracting j from n in base p.

We also note Lucas's binomial theorem [30].

Lemma 2.4. *Let $n \geq j$ be non-negative integers. Write, in base p, $n = a_r p^r + \cdots + a_1 p + a_0$ and $j = j_r p^r + \cdots + j_1 p + j_0$ where $0 \leq a_i, j_i \leq p-1$ for each $i \in \{0, 1, \ldots, r\}$, and $a_r \neq 0$. Then*

$$\binom{n}{j} \equiv \binom{a_r}{j_r} \cdots \binom{a_1}{j_1}\binom{a_0}{j_0} \pmod{p}.$$

2.2 An Explicit Formulation of the Coefficients

To construct the Newton polygons of $f(x \mid n, t)$ we will require a clearer understanding of the numbers $S(k \mid n, t)$. Specifically, we will want to know enough about $S(k \mid n, t)$ so that we can talk about its p-adic valuation with respect to different primes.

Firstly, observe that

$$S\left(k \mid n, t\right) = \sum_{m_1+\cdots+m_k=n} m_1^t \cdots m_k^t = \left[x^n\right]\left(\left(x + 2^t x^2 + 3^t x^3 + 4^t x^4 + \cdots\right)^k\right),$$

where $\left[x^n\right]\left(h(x)\right)$ denotes the coefficient of x^n in the power series $h(x)$.

Secondly, taking $|x| < 1$, recall

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots,$$

and observe that

$$x\frac{d}{dx}\left(\frac{1}{1-x}\right) = x\left(1 + 2x + 3x^2 + 4x^3 + \cdots\right) = x + 2x^2 + 3x^3 + 4x^4 + \cdots.$$

Iterating this pair of operations t times, we obtain

$$\underbrace{x\frac{d}{dx}\left(\cdots\left(x\frac{d}{dx}\right.\right.}_{t \text{ times}}\left.\left.\left(\frac{1}{1-x}\right)\right)\cdots\right) = x + 2^t x^2 + 3^t x^3 + 4^t x^4 + \cdots.$$

For ease of notation, let $D\left(\cdot\right) := x\left(d/dx\right)\left(\cdot\right)$. Then

$$S\left(k \mid n, t\right) = \left[x^n\right]\left(\left(D^t\left(\left(1-x\right)^{-1}\right)\right)^k\right). \tag{2.1}$$

To study the numbers $S\left(k \mid n, t\right)$ we start by studying the sequence

$$\left\{D^t\left(1/\left(1-x\right)\right)\right\}_{t\in\mathbb{N}}.$$

An induction argument gives that $D^t\left(1/\left(1-x\right)\right)$ is x times a polynomial of degree $t-1$ divided by $\left(1-x\right)^{t+1}$. Define $A\left(t, j\right)$ by

$$D^t\left(\frac{1}{1-x}\right) = \frac{x\sum_{j=0}^{t-1} A\left(t, j\right) x^j}{\left(1-x\right)^{t+1}}. \tag{2.2}$$

Then, for any $t \geq 1$, we have

$$\begin{aligned}\frac{d}{dx}\left(D^t\left(\frac{1}{1-x}\right)\right) &= \frac{d}{dx}\left(\frac{x\sum_{j=0}^{t-1} A\left(t, j\right) x^j}{\left(1-x\right)^{t+1}}\right) \\ &= \frac{\left(1-x\right)^{t+1}\sum_{j=0}^{t-1}\left(j+1\right)A\left(t, j\right)x^j + \left(t+1\right)\left(1-x\right)^t\sum_{j=1}^{t} A\left(t, j-1\right)x^j}{\left(1-x\right)^{2t+2}}\end{aligned}$$

$$= \frac{\sum_{j=0}^{t-1}(j+1)A(t,j)x^j - \sum_{j=1}^{t} jA(t,j-1)x^j + (t+1)\sum_{j=1}^{t}A(t,j-1)x^j}{(1-x)^{t+2}}$$
$$= \frac{A(t,0) + \sum_{j=1}^{t-1}[(j+1)A(t,j) + (t-j+1)A(t,j-1))]x^j + A(t,t-1)x^t}{(1-x)^{t+2}}.$$

Observe that $A(1,0) = 1$ and from the above, for $0 \leq j \leq t$, we have

$$A(t+1,j) = \begin{cases} A(t,0) & \text{if } j = 0 \\ (j+1)A(t,j) + (t-j+1)A(t,j-1) & \text{if } 1 \leq j \leq t-1 \\ A(t,t-1) & \text{if } j = t. \end{cases}$$

The numbers $A(t,j)$ are the so-called Eulerian numbers. See [13], [14], [20] and [41]. We will make use of the following identities associated with the Eulerian numbers:

$$A(t,j) = \sum_{i=0}^{m}(-1)^i \binom{t+1}{i}(j+1-i)^t \tag{2.3}$$

$$x^t = \sum_{m=0}^{t-1} A(t,m)\binom{x+m}{t} \tag{2.4}$$

$$A(t,m) = A(t,t-1-m). \tag{2.5}$$

Combining (2.1) and (2.2) yields

$$S(k \mid n,t) = [x^n]\left(\left(\frac{x\sum_{j=0}^{t-1}A(t,j)x^j}{(1-x)^{t+1}}\right)^k\right) = \left[x^{n-k}\right]\left(\frac{\left(\sum_{j=0}^{t-1}A(t,j)x^j\right)^k}{(1-x)^{k(t+1)}}\right). \tag{2.6}$$

Substituting (2.3) into the right-hand side of (2.6) and expanding with multinomial coefficients yields the following

Lemma 2.5. *The value $S(k \mid n,t)$ is the coefficient of x^{n-k} in the expansion of*

$$\left(\sum_{k_0+\cdots+k_{t-1}=k}\binom{k}{k_0,\ldots,k_{t-1}}\left(\prod_{i=0}^{t-1}A(t,i)^{k_i}\right)x^{\sum_{i=0}^{t-1}ik_i}\right)\sum_{j=0}^{\infty}\binom{j+(t+1)k-1}{(t+1)k-1}x^j,$$

where $k_0, k_1, \ldots, k_{t-1}$ represent non-negative integers.

2.3 Constructing the Newton polygons

The remainder of this chapter follows the basic idea discussed in [19]. That is, we will first explicitly construct the Newton polygons for $f(x \mid n,t)$ with respect to each

prime $p \mid (n-1)$ and then apply Theorem 2.1 to show that any factor of $f(x \mid n, t)$ has degree at least $n-1$. We start by introducing some notation.

Let $v = \nu_p(n-1)$ and $u = \lfloor \log_p(n-1) \rfloor - v$. Note that since $p \mid (n-1)$ we have $v \geq 1$. Then

$$n - 1 = p^v \sum_{j=0}^{u} a_j p^j \qquad \text{where } a_u, a_0 \geq 1 \tag{2.7}$$

is the base p expansion of $n-1$. For each $J \in \{0, 1, \ldots, u\}$, we denote by n_J the p^{v+J}th truncation of $n-1$ in base p. That is,

$$n_J = p^v \sum_{j=0}^{J} a_j p^j. \tag{2.8}$$

Let $n_{-1} = 0$. It is useful to note at this point that when $J = u$, we get $n - n_J = 1$, and more generally when $J \in \{-1, 0, \ldots, u\}$, we have

$$n - n_J = 1 + p^v \sum_{j=J+1}^{u} a_j p^j. \tag{2.9}$$

We prove the following

Theorem 2.6. *Fix integers $n \geq 3$ and $t \geq 1$. Let $f(x \mid n, t)$ be as in (1.3). Let p be a prime dividing $n-1$, and let*

$$n - 1 = p^v \sum_{j=0}^{u} a_j p^j$$

be the p-ary expansion of $n-1$ as in (2.7). Then the vertices of the Newton polygon for $f(x \mid n, t)$ with respect to p are precisely the points in the set

$$\{(0,0)\} \cup \left\{ \left(\sum_{j=0}^{J} a_j p^{v+j}, \sum_{j=0}^{J} a_j \frac{p^{v+j} - 1}{p - 1} \right) \;\middle|\; J \in \{0, 1, \ldots, u\} \right\}. \tag{2.10}$$

To prove Theorem 2.6 it suffices to show each of the following:

1. The Newton polygon for $f(x \mid n, t)$ with respect to p is the lower convex hull of the points in (2.10).

2. The slopes of the edges joining the successive pairs of points in (2.10) are strictly increasing from left to right.

To do this we will first establish two lemmas.

Lemma 2.7. *Let $p \mid (n-1)$. For each $J \in \{0, \ldots, u\}$, we have $\nu_p\left(S\left(n - n_J \mid n, t\right)\right) = 0$.*

Proof. Since $n - (n - n_J) = n_J$, Lemma 2.5 implies that $S\left(n - n_J \mid n, t\right)$ is the coefficient of x^{n_J} in the expansion of

$$\left(\sum_{k_0+\cdots+k_{t-1}=n-n_J} \binom{n-n_J}{k_0, \ldots, k_{t-1}} \left(\prod_{i=0}^{t-1} A\left(t, i\right)^{k_i}\right) x^{\sum_{i=0}^{t-1} i k_i}\right) \tag{2.11}$$

times

$$\sum_{j=0}^{\infty} \binom{j + (t+1)(n-n_J) - 1}{(t+1)(n-n_J) - 1} x^j.$$

We first focus our attention on (2.11). We fix $0 < i_0 \leq t-1$ and derive conditions on k_{i_0} necessary for a given term in (2.11) to not contribute to $S\left(n - n_J \mid n, t\right)$. In particular, if $k_{i_0} \geq p^{v+J+1}$, then by (2.8) we have

$$\sum_{i=0}^{t-1} i k_i \geq i_0 k_{i_0} \geq p^{v+J+1} > n_J.$$

Thus no terms in (2.11) with such values for k_{i_0} would contribute to $S\left(n - n_J \mid n, t\right)$. So for all $i \in \{1, \ldots, t-1\}$, we need only consider terms from (2.11) with $k_i < p^{v+J+1}$.

Now we fix more generally $0 \leq i_0 \leq t-1$. By considering (2.9) we see for $J \in \{0, \ldots, u-1\}$ that if $k_{i_0} \not\equiv 0, 1 \pmod{p^{v+J+1}}$, then there will be at least one borrow when subtracting k_{i_0} from $n - n_J$ in base p. Hence by Lemma 2.3, we obtain $p \mid \binom{n-n_J}{k_{i_0}}$, implying

$$p \,\Big|\, \binom{n-n_J}{k_0, \ldots, k_{t-1}} = \binom{n-n_J}{k_{i_0}} \binom{n-n_J-k_{i_0}}{k_0, \ldots, k_{i_0-1}, k_{i_0+1}, \ldots k_{t-1}}.$$

Thus, to determine $S\left(n - n_J \mid n, t\right)$ modulo p, we need only consider terms in (2.11) with $k_0 \equiv 0, 1 \pmod{p^{v+J+1}}$ and $k_i = 0, 1$ for each $i \in \{1, 2, \ldots, t-1\}$.

With $i \in \{1, 2, \cdots, t-1\}$ and k_i as in the sum in (2.11), let z be the number of such i with $k_i = 1$. Then $k_0 = n - n_J - z \equiv 1 - z \pmod{p^{v+J+1}}$, where the congruence comes from (2.9). Since $k_0 \equiv 0, 1 \pmod{p^{v+J+1}}$, we must then have

$$z \equiv 1, 0 \pmod{p^{v+J+1}}.$$

If $z \geq p^{v+J+1}$, then we would have

$$\sum_{i=0}^{t-1} ik_i = \sum_{\substack{1 \leq i \leq t-1 \\ k_i = 1}} i \geq \sum_{\substack{1 \leq i \leq t-1 \\ k_i = 1}} 1 = z \geq p^{v+J+1} > n_J.$$

This means we only need consider $z = 1, 0$. Hence, since $A(t, 0) = 1$, we use (2.9) to deduce for each $J \in \{0, \ldots, u\}$ that

$$\begin{aligned} S(n - n_J \,|\, n, t) &\equiv \binom{n_J + (t+1)(n - n_J) - 1}{n_J} \\ &\quad + (n - n_J) \sum_{j=1}^{t-1} A(t, j) \binom{n_J - j + (t+1)(n - n_J) - 1}{n_J - j} \quad (2.12) \\ &\equiv \sum_{j=0}^{t-1} A(t, j) \binom{n_J - j + (t+1)(n - n_J) - 1}{n_J - j} \pmod{p}. \end{aligned}$$

Rewriting (2.12) yields

$$S(n - n_J \,|\, n, t) \equiv \sum_{j=0}^{t-1} A(t, j) \binom{n_J - j + (t+1)(n - 1 - n_J) + t}{n_J - j} \pmod{p}.$$

Since $(t+1)(n - 1 - n_J) \equiv 0 \pmod{p^{v+J+1}}$ and for $0 \leq j \leq t-1$, $n_J - j < p^{v+J+1}$, any borrows in the subtraction $(n_J - j + (t+1)(n - 1 - n_J) + t) - (n_J - j)$ in base p will come from the subtraction $(n_J - j + t) - (n_J - j)$ in base p.

We can use these facts to simplify $S(n - n_J \,|\, n, t)$ further. Via the division algorithm, we write $n_J - j + t = q \cdot p^{v+J+1} + r$ where $0 \leq r < p^{v+J+1}$. Then the base p expansion of $(n_J - j + (t+1)(n - 1 - n_J) + t)$ has its digits in the p^{v+J+1}-place and higher arising from $(t+1)(n - 1 - n_J) + q \cdot p^{v+J+1}$, while the lower digits arise from r. Thus we can use Lemma 2.4 to obtain

$$\binom{n_J - j + (t+1)(n - 1 - n_J) + t}{n_J - j} \equiv \binom{(t+1)(n - 1 - n_J)/p^{v+J+1} + q}{0} \binom{r}{n_J - j}$$

$$\equiv \binom{q}{0}\binom{r}{n_J - j} \equiv \binom{n_J - j + t}{n_J - j} \pmod{p}.$$

Substituting this simplification into $S(n - n_J \mid n, t)$, we obtain

$$S(n - n_J \mid n, t) \equiv \sum_{j=0}^{t-1} A(t, j) \binom{n_J - j + t}{n_J - j} \pmod{p}.$$

Using the symmetry of binomial coefficients, we have

$$S(n - n_J \mid n, t) \equiv \sum_{j=0}^{t-1} A(t, j) \binom{n_J - j + t}{t} \equiv (n_J + 1)^t \pmod{p},$$

where the second equivalence comes from (2.4) and (2.5). Recalling that n_J is divisible by p^v, we see $S(n - n_J \mid n, t) \equiv 1 \pmod{p}$ so that the lemma follows. □

While Lemma 2.7 will allow us to find candidates for the vertices on the Newton polygon of $f(x \mid n, t)$, we will use the following lemma to show that no other vertices can appear in the Newton polygon.

Lemma 2.8. *Let $p \mid (n-1)$. If $m \equiv n \pmod{p}$, then $\nu_p(S(n - m \mid n, t)) > 0$.*

Proof. By Lemma 2.5, we have that $S(n - m \mid n, t)$ is the coefficient of $x^{n-(n-m)} = x^m$ in the expansion of

$$\left(\sum_{k_0 + \cdots + k_{t-1} = n - n_J} \binom{n - n_J}{k_0, \ldots, k_{t-1}} \left(\prod_{i=0}^{t-1} A(t, i)^{k_i} \right) x^{\sum_{i=0}^{t-1} i k_i} \right)$$

times

$$\sum_{j=0}^{\infty} \binom{j + (t+1)(n - n_J) - 1}{(t+1)(n - n_J) - 1} x^j.$$

We fix $0 \leq i_0 \leq t - 1$ and consider the k_{i_0} appearing in the first factor above. Since $m \equiv n \pmod{p}$, we have $p \mid (n - m)$. If $p \nmid k_{i_0}$, then we can rewrite the multinomial coefficient and use Lemma 2.3 to obtain

$$\binom{n - m}{k_0, \ldots, k_{t-1}} = \binom{n - m}{k_{i_0}} \binom{n - m - k_{i_0}}{k_0, \ldots, k_{i_0 - 1}, k_{i_0 + 1}, \ldots, k_{t-1}} \equiv 0 \pmod{p},$$

since there will be a carry when subtracting k_{i_0} from $n-m$ in base p. Thus the only nonzero terms in

$$\sum_{k_0+\cdots+k_{t-1}=n-m} \binom{n-m}{k_0,\ldots,k_{t-1}} \left(\prod_{i=0}^{t-1} A\left(t,i\right)^{k_i}\right) x^{\sum_{i=0}^{t-1} ik_i},$$

when considered modulo p, are those where for each $i \in \{0,\ldots,t-1\}$ there are non-negative integers k_i' such that $k_i = pk_i'$. That is, reducing $S\left(n-m \,|\, n,t\right)$ modulo p, we only need consider the coefficient of x^m arising from the multiplication of

$$\sum_{pk_0'+\cdots+pk_{t-1}'=n-m} \binom{n-m}{pk_0',\ldots,pk_{t-1}'} \left(\prod_{i=0}^{t-1} A\left(t,i\right)^{pk_i'}\right) x^{\sum_{i=0}^{t-1} ipk_i'}$$

by

$$\sum_{j=0}^{\infty} \binom{j+\left(t+1\right)\left(n-m\right)-1}{\left(t+1\right)\left(n-m\right)-1} x^j.$$

For each term in the first sum in order to get a contribution to the coefficient of x^m in the product, we want to consider

$$j = m - \sum_{i=0}^{t-1} ipk_i'$$

in the second sum.

We now turn our attention to the binomial coefficients

$$\binom{j+\left(t+1\right)\left(n-m\right)-1}{\left(t+1\right)\left(n-m\right)-1} = \binom{m-\sum_{i=0}^{t-1} ipk_i'+\left(t+1\right)\left(n-m\right)-1}{\left(t+1\right)\left(n-m\right)-1}.$$

Recall $m \equiv n \equiv 1 \pmod{p}$, so

$$m - \sum_{i=0}^{t-1} ipk_i' + \left(t+1\right)\left(n-m\right) - 1 \equiv 0 \pmod{p}$$

and

$$\left(t+1\right)\left(n-m\right) - 1 \equiv p-1 \pmod{p}.$$

Thus, Lemma 2.3 implies that

$$\binom{m-\sum_{i=0}^{t-1} ipk_i'+\left(t+1\right)\left(n-m\right)-1}{\left(t+1\right)\left(n-m\right)-1} \equiv 0 \pmod{p}.$$

Hence, $S\left(n-m \,|\, n,t\right) \equiv 0 \pmod{p}$ since each term contributing to the coefficient of x^m in the product above is divisible by p. The lemma follows. □

We can now prove Theorem 2.6.

Proof of Theorem 2.6. Recall it suffices to show each of the following:

1. The Newton polygon for $f(x \mid n,t)$ with respect to p is the lower convex hull of the points in (2.10).

2. The slopes of the edges joining the successive pairs of points in (2.10) are strictly increasing from left to right.

Fix integers $n \geq 3$, $t \geq 1$ and a prime p dividing $n-1$. Starting with (1), for $0 \leq j \leq n-1$, set

$$c_j = \frac{n!}{j!} S(j \mid n,t) = (n-j)! \binom{n}{n-j} S(j \mid n,t).$$

Thus $f(x \mid n,t) = \sum_{j=1}^{n} c_j x^{j-1}$. For $J \in \{0,\ldots,u\}$ define n_J as in (2.8), with $n_{-1} = 0$. Note that since $f(x \mid n,t)$ is monic, $\nu_p(c_n) = \nu_p(1) = 0$, meaning $(0, \nu_p(c_n)) = (0,0)$ is on the Newton polygon with respect to p.

Next, we show for $J \in \{0,1,\ldots,u\}$ that

$$\nu_p(c_{n-n_J}) = \frac{1}{p-1} \sum_{j=0}^{J} a_j \left(p^{v+j} - 1\right). \tag{2.13}$$

Using the definition of $\nu_p(\cdot)$, we see that

$$\nu_p(c_{n-n_J}) = \nu_p(n_J!) + \nu_p\left(\binom{n}{n_J}\right) + \nu_p(S(n-n_J \mid n,t)). \tag{2.14}$$

Since $v \geq 1$, the difference $n - n_J$ requires no borrows in base p. So, applying Lemmas 2.2, 2.3 and 2.7 to the respective terms in (2.14), we see

$$\nu_p(c_{n-n_J}) = \frac{n_J - s_p(n_J)}{p-1} + 0 + 0 = \frac{1}{p-1} \sum_{j=0}^{J} a_j \left(p^{v+j} - 1\right).$$

Thus, we see (2.13) holds, and the set (2.10) is precisely the set

$$\{(n_J, \nu_p(c_{n-n_J})) \mid J \in \{-1,0,\ldots,u\}\}. \tag{2.15}$$

To prove (1) we must show that all points in the set

$$\{(j, \nu_p(c_{n-j})) \mid j \in \{0, 1, \ldots n-1\}\}$$

lie on or above the lines joining successive points in (2.15). It is clear that the points in (2.15) lie on said lines, so consider a point $(m, \nu_p(c_{n-m}))$ not belonging to (2.15).

If $n_J < m < n_{J+1}$ for some $J \in \{-1, 0, \ldots, u-1\}$, then it suffices to show

$$\frac{\nu_p(c_{n-m}) - \nu_p(c_{n-n_J})}{m - n_J} \geq \frac{\nu_p\left(c_{n-n_{J+1}}\right) - \nu_p(c_{n-n_J})}{n_{J+1} - n_J}. \tag{2.16}$$

Using the definition of $\nu_p(\cdot)$ once more with (2.13), the inequality in (2.16) is equivalent to

$$\frac{\nu_p(m!) + \nu_p\left(\binom{n}{m}\right) + \nu_p(S(n-m \mid n, t)) - (n_J - s_p(n_J))/(p-1)}{m - n_J} \geq \frac{p^{v+J+1} - 1}{(p-1)\, p^{v+J+1}}. \tag{2.17}$$

We note from (2.9) and $v \geq 1$ that $s_p(n) - s_p(n_J) = s_p(n - n_J)$. Using this observation along with Lemmas 2.2 and 2.3, we multiply both sides by $p-1$ to transform (2.17) into

$$\frac{(m - n_J) + (s_p(n-m) - s_p(n-n_J)) + (p-1)\,\nu_p(S(n-m \mid n, t))}{m - n_J} \geq \frac{p^{v+J+1} - 1}{p^{v+J+1}}.$$

Subtracting 1 and then multiplying both sides by $(m - n_J)$ yields

$$s_p(n-m) - s_p(n-n_J) + (p-1)\,\nu_p(S(n-m \mid n, t)) \geq -\frac{m - n_J}{p^{v+J+1}}. \tag{2.18}$$

From (2.9), we have that

$$n - n_J = n - 1 - n_J + 1 = p^v \sum_{j=J+1}^{u} a_j p^j + 1,$$

so

$$s_p(n - n_J) = 1 + \sum_{j=J+1}^{u} a_j. \tag{2.19}$$

Recall $n_J < m < n_{J+1}$. In the equations that follow we interpret a sum from $j = u+1$ to $j = u$ as 0, which arises when $J = u - 1$. Then we can write

$$n - m = (n - 1 - n_{J+1}) + (n_{J+1} + 1 - m) = p^v \sum_{j=J+2}^{u} a_j p^j + \sum_{j \in T} \epsilon_j p^j, \tag{2.20}$$

where $T \subseteq \{0, 1, \ldots J + v + 1\}$ is a non-empty set and each $\epsilon_j \in \{1, 2, \ldots, p-1\}$. Thus, we obtain

$$s_p(n - m) = \sum_{j=J+2}^{u} a_j + \sum_{j \in T} \epsilon_j. \tag{2.21}$$

Further, we can write

$$n - m = (n - 1 - n_J) + (n_J + 1 - m) = p^v \sum_{j=J+1}^{u} a_j p^j + n_J + 1 - m. \tag{2.22}$$

Setting the right-hand sides of (2.20) and (2.22) equal and solving for $n_J - m$ gives

$$n_J - m = \sum_{j \in T} \epsilon_j p^j - a_{J+1} p^{v+J+1} - 1. \tag{2.23}$$

Substituting (2.19), (2.21) and (2.23) into (2.18) yields

$$\sum_{j \in T} \epsilon_j - a_{J+1} - 1 + (p-1)\, \nu_p(S(n - m \,|\, n, t)) \geq \frac{\sum_{j \in T} \epsilon_j p^j - a_{J+1} p^{v+J+1} - 1}{p^{v+J+1}}.$$

Rearranging the above gives

$$\sum_{j \in T} \epsilon_j \left(1 - p^{j-v-J-1}\right) - 1 + (p-1)\, \nu_p(S(n - m \,|\, n, t)) \geq -p^{-v-J-1}. \tag{2.24}$$

Recall $T \neq \emptyset$. Observe that if $\nu_p(S(n - m \,|\, n, t)) > 0$, then the left-hand side of (2.24) is positive, and so the inequality holds. Alternatively, the contrapositive of Lemma 2.8 tells us that if $\nu_p(S(n - m \,|\, n, t)) = 0$, then $m \not\equiv n \pmod{p}$, implying $0 \in T$ so that $\epsilon_0 \geq 1$. This allows us to simplify the left-hand side of (2.24), obtaining

$$\sum_{j \in T} \epsilon_j \left(1 - p^{j-v-J-1}\right) - 1 \geq \epsilon_0 \left(1 - p^{-v-J-1}\right) - 1 \geq \left(1 - p^{-v-J-1}\right) - 1 = -p^{-v-J-1}.$$

Thus, (2.24) and the equivalent (2.16) holds. This completes the proof of (1).

For (2), let J be such that $n_J \neq n_{J+1}$. Then,

$$\frac{\nu_p\left(c_{n-n_{J+1}}\right) - \nu_p\left(c_{n-n_J}\right)}{n_{J+1} - n_J} = \frac{a_{J+1}\left(p^{v+J+1} - 1\right)}{(p-1)\, a_{J+1} p^{v+J+1}} = \frac{1}{p-1}\left(1 - \frac{1}{p^{v+J+1}}\right). \tag{2.25}$$

Since the right-hand side of (2.25) increases as J increases, we deduce that (2) holds. This completes the proof of the Theorem 2.6. □

2.4 Proof of Theorem 1.2

We now have what we need to prove Theorem 1.2, namely

Theorem 1.2. *The polynomials*

$$f\left(x \mid n,t\right)=\sum_{k=1}^{n}\frac{n!}{k!}S\left(k \mid n,t\right)x^{k-1}.$$

are irreducible for all integers $n \geq 2$ *and* $t \geq 1$.

Proof. When $n=2$, we have $f\left(x \mid 2,t\right)=x+2^{t}$ which is irreducible. For $n \geq 3$, let p be a prime dividing $n-1$ and adopt the notation of Section 4. From the proof of Theorem 2.6, the slope of the line segments joining two successive points in (2.10) is of the form

$$\frac{1}{p-1}\left(1-\frac{1}{p^{v+J+1}}\right)=\frac{p^{v+J+1}-1}{\left(p-1\right)p^{v+J+1}}$$

for $J \in \{-1,0,1,\ldots,u\}$. Observe that when this last fraction is reduced, the denominator is p^{v+J+1}. This implies that for a segment with this slope, the horizontal distance between the consecutive lattice points is p^{v+J+1}. In particular, from Theorem 2.6, the smallest horizontal distance between any two consecutive lattice points on the Newton polygon of $f\left(x \mid n,t\right)$ with respect to p is p^{v}, and so the horizontal distance between every pair of consecutive lattice points is divisible by p^{v}. This is true for every prime power p^{v} dividing $n-1$. Thus, any irreducible factor of $f\left(x \mid n,t\right)$ has degree divisible by $n-1$. Since the degree of $f\left(x \mid n,t\right)$ is $n-1$, the proof is complete. □

Chapter 3

2-adic integer solutions to the Prouhet-Tarry-Escott problem

3.1 Preliminary Material

Let n be a fixed positive integer and let $X = [x_1, x_2, \ldots, x_n]$ and $Y = [y_1, y_2, \ldots, y_n]$ be lists of integers. Define

$$w(z) = w(X, Y, z) = \prod_{j=1}^{n} (z - x_j) - \prod_{j=1}^{n} (z - y_j).$$

Recall from Corollary 1.4 that the pair $\{X, Y\}$ is an ideal PTE solution over the integers if and only if $w(z)$ is a non-zero constant. We adapt this definition in the following.

Definition 3.1. For a positive integer k, let X and Y be lists whose entries are integers that lie in the interval $\left[0, 2^k\right)$. We say that the pair $\{X, Y\}$ is an ideal PTE solution modulo 2^k if

$$w(X, Y, z) \equiv C \pmod{2^k}, \tag{3.1}$$

for some integer $C \not\equiv 0 \pmod{2^k}$.

Ideal PTE solutions modulo 2^k satisfy the following.

Proposition 3.2. *If $\{X, Y\}$ is an ideal PTE solution modulo 2^k, then*

$$\sum_{x \in X} x^i \equiv \sum_{y \in Y} y^i \pmod{2^k}, \quad \textit{for } i \in \{1, 2, \ldots, n-1\}.$$

Proof. Let $X = [x_1, x_2, \ldots, x_n]$ and $Y = [y_1, y_2, \ldots, y_n]$ be an ideal PTE solution modulo 2^k. Define, for $0 \leq j \leq n$, integers a_j and b_j such that

$$\prod_{j=1}^{n} (z - x_j) = \sum_{j=0}^{n} a_j z^j \quad \text{and} \quad \prod_{j=1}^{n} (z - y_j) \sum_{j=0}^{n} b_j z^j.$$

Note that

$$w(z) = \sum_{j=0}^{n-1} (a_j - b_j) z^j.$$

Since $\{X, Y\}$ is an ideal PTE solution modulo 2^k, we have that

$$a_j \equiv b_j \pmod{2^k} \quad \text{for } j \in \{1, 2, \ldots, n-1\}. \tag{3.2}$$

The integers a_j and b_j are precisely the $(n-j)^{\text{th}}$ elementary symmetric polynomials in X and Y, respectively. For each $0 \leq i \leq n-1$, we know that $\sum_{j=1}^{n} x_j^i$ and $\sum_{j=1}^{n} y_j^i$ can be expressed as linear combinations of a_j and b_j. By (3.2), the result follows. □

The converse to Proposition 3.2 is not true. For example, the lists $X = [1, 0, 0]$ and $Y = [1, 1, 1]$ satisfy the conclusion of Proposition 3.2 with $k = 1$, but $w(X, Y, z) \equiv z+1 \pmod 2$. This differs from the the result over the integers in Corollary 1.4. With this in mind, we define ideal PTE solutions modulo 2^k as we do in Definition 3.1 rather than an analog of (1.4) as we are interested in studying the 2-adic valuation of $\overline{C_n}$ defined in (1.6).

We will now look at some more properties of ideal PTE solutions modulo 2^k.

Lemma 3.3. *If $\{X, Y\}$ is an ideal PTE solution modulo 2^k, for some $k > 0$, then X and Y contain the same number of odd entries.*

Proof. Let o_x and o_y be the number of odd entries in X and Y respectively. Without loss of generality, suppose $o_x - o_y \geq 0$. Then

$$\begin{aligned} w(z) &\equiv z^{n-o_x} (z+1)^{o_x} + z^{n-o_y} (z+1)^{o_y} \pmod 2 \\ &\equiv z^{n-o_x} (z+1)^{o_y} \left((z+1)^{o_x - o_y} + z^{o_x - o_y} \right) \pmod 2. \end{aligned} \tag{3.3}$$

If $\{X, Y\}$ is an ideal PTE solution modulo 2^k, for some $k > 0$, then $\{X, Y\}$ satisfies (3.1) with $C = w(0)$. So we have,

$$w(z) \equiv w(0) \pmod 2,$$

which is constant. We see that (3.3) is constant only if

$$(z+1)^{o_x - o_y} + z^{o_x - o_y} \equiv 0 \pmod 2.$$

which happens only when $o_x - o_y = 0$. That is, $\{X, Y\}$ is an ideal PTE solution modulo 2^k only if X and Y have the same number of odd entries. □

Given an ideal PTE solution modulo 2^k, we are interested in whether or not there exists a lift of that solution that is an ideal PTE solution modulo 2^{k+1}. We now introduce some notation that will be useful when talking about lifting solutions. For ordered lists $A = [a_1, \ldots, a_n]$ and $B = [b_1, \ldots, b_n]$ and integers c we define list addition and scalar multiplication as

$$A + B = [a_1 + b_1, \ldots, a_n + b_n] \quad \text{and} \quad c \cdot A = [c \cdot a_1, \ldots, c \cdot a_n],$$

respectively. We will let $\{X_k, Y_k\}$ represent a solution modulo 2^k with each entry of X_k and Y_k in the interval $\left[0, 2^k\right)$. Further, $w_k(z)$ will represent the corresponding polynomial $w(X_k, Y_k, z)$. Let $T_k = 2^k \cdot [t_1, \ldots, t_n]$ and $U_k = 2^k \cdot [u_1, \ldots, u_n]$ where $t_j, u_j \in \{0, 1\}$ for $1 \le j \le n$. Let $\left\{X_k^+, Y_k^+\right\} = \{X_k + T_k, Y_k + U_k\}$, whose corresponding polynomial is

$$w_k^+(z) := \prod_{j=1}^{n} \left(z - x_j - 2^k t_j\right) - \prod_{j=1}^{n} \left(z - y_j - 2^k u_j\right). \tag{3.4}$$

Observe that each entry of X_k^+ and Y_k^+ is in the interval $(0, 2^{k+1}]$ and congruent to their corresponding entries in X_k and Y_k modulo 2^k. Also, $w_k^+(z) \equiv w_k(z) \pmod{2^k}$. We refer to $\{X_k^+, Y_k^+\}$ as a *lift* of $\{X_k, Y_k\}$. If $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, *lifting* will refer to the process of finding a pair $\{X_k^+, Y_k^+\}$ that is a

lift of $\{X_k, Y_k\}$. A pair $\{X_k, Y_k\}$ is said to be *lifted* if a lift $\{X_k^+, Y_k^+\}$ has been found. If $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, we say that $\{X_k, Y_k\}$ has been *successfully lifted* if we have found a lift $\{X_k^+, Y_k^+\}$ that is an ideal PTE solution modulo 2^{k+1}. In this case, $\{X_k^+, Y_k^+\}$ will be referred to as a *successful lift* of $\{X_k, Y_k\}$.

Studying the polynomials $w_k(z)$ and $w_k^+(z)$ is going to be key to us finding 2-adic solutions. Specifically, we want to get a handle on the coefficients of $w_k(z)$ and $w_k^+(z)$.

For a list $S = [s_1, \ldots, s_n]$ and $1 \leq j \leq |S|$, denote by $e_j(S)$ the j^{th} elementary symmetric polynomial whose variables are the elements in S. For later purposes, we note that $e_0(S) = 1$. We also make note of the following.

Lemma 3.4. *Let $S = [s_1, \ldots, s_n]$ be a list of integers and let n_{odd} denote the number of odd entries in S. Then*

$$e_j(S) \equiv 0 \pmod{2^{j-n_{odd}}}, \quad \textit{for } j > n_{odd}.$$

Proof. Each term in $e_j(S)$ is a product of j entries in S. If $j > n_{\text{odd}}$ then necessarily each term in $e_j(S)$ must contain at least $j - n_{\text{odd}}$ even entries. The result follows. □

For a pair $\{X_k, Y_k\}$, we can write

$$w_k(z) = w(X_k, Y_k, z) = \sum_{j=0}^{n-1} (-1)^{n-j} \left(e_{n-j}(X_k) - e_{n-j}(Y_k)\right) z^j.$$

If $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, then $w_k(z) \equiv w_k(0) \pmod{2^k}$. For $1 \leq j \leq n-1$, define the integers d_j by

$$d_j = \frac{e_{n-j}(X_k) - e_{n-j}(Y_k)}{2^k}.$$

Then

$$w_k(z) = w_k(0) + 2^k \sum_{j=1}^{n-1} (-1)^{n-j} d_j z^j. \tag{3.5}$$

Define $\hat{S}^i = [s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n]$. That is, $\hat{S}^i$ is the list S with the i^{th} entry removed. Expanding $w_k^+(z)$ given in (3.4) yields

$$\begin{aligned} w_k^+(z) &= 2^k \sum_{i=1}^{n} \left(-t_i \prod_{\substack{1 \le j \le n \\ j \neq i}} (z - x_j) + u_i \prod_{\substack{1 \le j \le n \\ j \neq i}} (z - y_j) \right) + w_k(z) + 2^{2k} p(z) \\ &= 2^k \sum_{j=0}^{n-1} (-1)^{n-j} \left(\sum_{i=1}^{n} \left(e_{n-1-j}\left(\hat{X}_k^i\right) t_i - e_{n-1-j}\left(\hat{Y}_k^i\right) u_i \right) \right) z^j \\ &\quad + w_k(z) + 2^{2k} p(z), \end{aligned} \tag{3.6}$$

for some polynomial $p(z)$ with integer coefficients. Let n_{odd} be the number of odd entries in each of X_k and Y_k. For each i, both $\hat{X}_k^i$ and $\hat{Y}_k^i$ contain at least $n_{\text{odd}} - 1$ odd entries. So, by Lemma 3.4, $e_{n-1}\left(\hat{X}_k^i\right) t_i - e_{n-1}\left(\hat{Y}_k^i\right) u_i$ is divisible by $2^{n-n_{\text{odd}}}$, for each $1 \le i \le n$. With this in mind and substituting (3.5) into the (3.6), we obtain

$$\begin{aligned} w_k^+(z) = 2^k \sum_{j=1}^{n-1} (-1)^{n-j} &\left(d_j + \sum_{i=1}^{n} \left(e_{n-1-j}\left(\hat{X}_k^i\right) t_i - e_{n-1-j}\left(\hat{Y}_k^i\right) u_i \right) \right) z^j \\ &+ w_k(0) + 2^{k+n-n_{\text{odd}}} C + 2^{2k} p(z), \end{aligned}$$

for some integer C. For $1 \le j \le n-1$, define

$$d_j^+ = d_j + \sum_{i=1}^{n} \left(e_{n-1-j}\left(\hat{X}_k^i\right) t_i - e_{n-1-j}\left(\hat{Y}_k^i\right) u_i \right).$$

Then

$$w_k^+(z) = 2^k \sum_{j=1}^{n-1} (-1)^{n-j} d_j^+ z^j + w_k(0) + 2^{k+n-n_{\text{odd}}} C + 2^{2k} p(z), \tag{3.7}$$

and in particular

$$w_k^+(0) = w_k(0) + 2^{k+n-n_{\text{odd}}} C + 2^{2k} p(0). \tag{3.8}$$

Proposition 3.5. *If $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k and $\{X_k^+, Y_k^+\}$ is any lift of $\{X_k, Y_k\}$, then $\nu_2(w_k^+(0)) = \nu_2(w_k(0))$.*

Proof. From (3.8), we have

$$\nu_2\left(w_k^+(0)\right) = \nu_2\left(w_k(0) + 2^{k+n-n_{\text{odd}}} C + 2^{2k} p(0)\right).$$

Since $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k we have $\nu_2(w_k(0)) < k$. Then, since $n \geq n_{\text{odd}}$, we have

$$\nu_2\left(w_k\left(0\right) + 2^{k+n-n_{\text{odd}}}C + 2^{2k}p\left(0\right)\right) = \nu_2\left(w_k\left(0\right)\right).$$

Hence $\nu_2(w_k^+(0)) = \nu_2\left(w_k\left(0\right)\right)$. □

The following corollary immediately follows.

Corollary 3.6. *If $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k and $(\{X_i, Y_i\})_{i=k+1}^{\infty}$ is a sequence of successive lifts of $\{X_k, Y_k\}$, then $\nu_2\left(w_i\left(0\right)\right) = \nu_2\left(w_k\left(0\right)\right)$.*

Proposition 3.7. *A lift $\{X_k^+, Y_k^+\}$ of an ideal PTE solution modulo 2^k is an ideal PTE solution modulo 2^{k+1} if and only if*

$$d_j^+ \equiv 0 \pmod 2 \tag{3.9}$$

for each $1 \leq j \leq n-1$.

Proof. From Definition 3.1 and Proposition 3.5, the lift $\{X_k^+, Y_k^+\}$ is an ideal PTE solution modulo 2^{k+1} if and only if

$$w_k^+\left(z\right) - w_k^+\left(0\right) \equiv 0 \pmod{2^{k+1}}.$$

This consequence is equivalent to having both 2^k dividing $w_k^+\left(z\right) - w_k^+\left(0\right)$ and the congruence $\left(w_k^+\left(z\right) - w_k^+\left(0\right)\right)/2^k \equiv 0 \pmod 2$. From (3.7) we see that

$$w_k^+\left(z\right) - w_k^+\left(0\right) \equiv 2^k \sum_{j=1}^{n-1} \left(-1\right)^{n-j} d_j^+ z^j \pmod{2^{k+1}}.$$

This is equivalent to 2^k dividing $w_k^+\left(z\right) - w_k^+\left(0\right)$ and

$$\frac{w_k^+\left(z\right) - w_k^+\left(0\right)}{2^k} \equiv \sum_{j=1}^{n-1} \left(-1\right)^{n-j} d_j^+ z^j \pmod 2. \tag{3.10}$$

The right-hand side of (3.10) is $0 \pmod 2$ if and only if (3.9) holds for each $1 \leq j \leq n-1$. Proposition 3.7 follows. □

The next examples illustrate that not every solution can lift and even if we can successfully lift a solution, we are not guaranteed to be able to lift the solution more than once.

If $n = 4$ and the pair $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, then Proposition 3.7 implies a lift $\left\{X_k^+, Y_k^+\right\}$ is an ideal PTE solution modulo 2^{k+1} if the $t_j, u_j \in \{0, 1\}$ satisfy

$$\begin{aligned}
0 &\equiv d_1 + \sum_{i=1}^{4} \left(e_2\left(\hat{X}_k^i\right) t_i - e_2\left(\hat{Y}_k^i\right) u_i\right) \pmod 2, \\
0 &\equiv d_2 + \sum_{i=1}^{4} \left(e_1\left(\hat{X}_k^i\right) t_i - e_1\left(\hat{Y}_k^i\right) u_i\right), \pmod 2, \\
0 &\equiv d_3 + \sum_{i=1}^{4} \left(e_0\left(\hat{X}_k^i\right) t_i - e_0\left(\hat{Y}_k^i\right) u_i\right) \pmod 2.
\end{aligned}$$

Suppose X_k and Y_k each contain exactly one odd entry. Without loss of generality we suppose that x_1 and y_1 are odd. Then the above congruences become

$$\begin{aligned}
0 &\equiv d_1 \pmod 2, \\
0 &\equiv d_2 + \sum_{i=2}^{4} (t_i + u_i) \pmod 2, \\
0 &\equiv d_3 + \sum_{i=1}^{4} (t_i + u_i) \pmod 2.
\end{aligned}$$

We can always find a solution to the last two congruences, but we have no control over the first. So, we can only lift the solution $\{X_k, Y_k\}$ if the coefficient of z in $w_k(z)$ is divisible by 2^{k+1}, which is not always the case. For example,

$$X_6 = [1, 42, 0, 0], \quad Y_6 = [33, 2, 4, 4] \quad \text{and} \quad w_6(z) = -320z^2 + 1088z - 1056,$$

is an ideal PTE solution modulo 2^6, but the coefficient of z in $w_k(z)$ is not divisible by 2^7, so we cannot lift $\{X_6, Y_6\}$ to an ideal PTE solution modulo 2^7.

Now consider

$$X_6 = [1, 34, 24, 0], \quad Y_6 = [33, 10, 12, 4] \quad \text{and} \quad w_6(z) = -192z^2 + 6528z - 15840,$$

which is also an ideal PTE solution modulo 2^6. The coefficient of z in $w_6(z)$ now is divisible by 2^7, so we can lift $\{X_6, X_6\}$ if we can choose the t_j's and u_j's so that they satisfy

$$1 \equiv \sum_{i=2}^{4} (t_i + u_i) \pmod 2,$$
$$0 \equiv \sum_{i=1}^{4} (t_i + u_i) \pmod 2.$$

One possible assignment is $t_2 = t_4 = u_1 = u_4 = 1$ and $t_1 = t_3 = u_2 = u_3 = 0$, which gives

$$X_6^+ = [1, 98, 24, 64], \quad Y_6^+ = [97, 10, 12, 68] \quad \text{and} \quad w_6^+(z) = 4224z - 640992.$$

This is an ideal PTE solution modulo 2^7. Similar to the first example, the coefficient of z in $w_6^+(z)$ is not divisible by 2^8, so we will not be able to find a successful lift of $\{X_6^+, Y_6^+\}$ to a solution modulo 2^8. If we make a different assignment above, however, say $t_3 = u_1 = 1$ and $t_1 = t_2 = t_4 = u_2 = u_3 = u_4 = 0$, we obtain

$$X_6^+ = [1, 34, 88, 0] \quad Y_6^+ = [97, 10, 12, 4] \quad \text{and} \quad w_6^+(z) = 384z^2 + 17664z - 46560.$$

With these lists, the coefficient of z in $w_6^+(z)$ is indeed divisible by 2^8, so we will be able to keep lifting. That is, we can let $\{X_7, Y_7\} = \{X_6^+, Y_6^+\}$ and repeat the lifting process.

What we have seen is that, even though Proposition 3.7 gives the criteria to find a successful lift of a pair $\{X_k, Y_k\}$, not all lifted solutions we obtain can continue to be lifted. In the next section, for $3 \leq n \leq 8$ we will present sufficient criteria for $\{X_k, Y_k\}$ to have a successful lift and give examples of ideal PTE solution modulo 2^k that can be lifted indefinitely.

3.2 Sequences of Ideal PTE Solutions modulo 2^k

For a positive integer K, suppose $(\{X_k, Y_k\})_{k=K}^{\infty}$ is a sequence of pairs such that $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k and $\{X_{k+1}, Y_{k+1}\}$ is a lift of $\{X_k, Y_k\}$

for each $k \geq K$. Define for each $k \geq K$ and $j \in \{1, 2, \ldots, n-1\}$ the integers $d_{k,j}$ by

$$d_{k,j} = \frac{e_{n-j}(X_k) - e_{n-j}(Y_k)}{2^k}. \tag{3.11}$$

Then, by (3.5), we obtain

$$w_k(z) = w_k(0) + 2^k \sum_{j=1}^{n-1} (-1)^{n-j} d_{k,j} z^j. \tag{3.12}$$

Since $\{X_{k+1}, Y_{k+1}\}$ is a lift of $\{X_k, Y_k\}$, by (3.7), we see that

$$w_{k+1}(z) = 2^k \sum_{j=1}^{n-1} (-1)^{n-j} d^+_{k,j} z^j + w_k(0) + 2^{k+n-n_{\text{odd}}} C'_k + 2^{2k} p_k(z), \tag{3.13}$$

for an integer C'_k, a polynomial $p_k(z) \in \mathbb{Z}[z]$, and

$$d^+_{k,j} = d_{k,j} + \sum_{i=1}^{n} \left(e_{n-1-j}\left(\hat{X}^i_k\right) t_{k,i} - e_{n-1-j}\left(\hat{Y}^i_k\right) u_{k,i} \right). \tag{3.14}$$

Lemma 3.8. *Suppose, for an integer k, that $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k and $\{X_{k+1}, Y_{k+1}\}$ is a lift of $\{X_k, Y_k\}$. Let $d_{k+1,j}$ and $d^+_{k,j}$ be as in* (3.11) *and* (3.14)*, respectively. Let m be a positive integer and a_j be an integer for $1 \leq j \leq n-1$. Then for $k > m$, we have*

$$\sum_{j=1}^{n-1} a_j d_{k+1,j} \equiv 0 \pmod{2^m} \tag{3.15}$$

if and only if

$$\sum_{j=1}^{n-1} a_j d^+_{k,j} \equiv 0 \pmod{2^{m+1}}.$$

Proof. Note that (3.15) holds if and only if

$$2 \sum_{j=1}^{n-1} a_j d_{k+1,j} \equiv 0 \pmod{2^{m+1}}. \tag{3.16}$$

Comparing (3.12) and (3.13) we have

$$2d_{k+1,j} = d^+_{k,j} + 2^k p_{k,j}, \quad \text{for } j \in \{1, 2, \ldots, n-1\},$$

for some integer $p_{k,j}$. Substituting the above into (3.16) yields

$$\sum_{j=1}^{n-1} a_j d^+_{k,j} + 2^k \sum_{j=1}^{n-1} a_j p_{k,j} \equiv 0 \pmod{2^{m+1}}.$$

Since $k > m$, the result follows. □

We will now show for $3 \leq n \leq 8$ that there exist infinitely many sequences of pairs $(\{X_k, Y_k\})_{k=k_n+1}^{\infty}$ such that, for each $k \geq k_n + 1$, we have $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k with $\nu_2(w_k(0)) = k_n$ and $\{X_{k+1}, Y_{k+1}\}$ is a lift of $\{X_k, Y_k\}$. In the next section we establish Theorem 1.5 by describing how one can construct a 2-adic integer solution from a sequence $(\{X_k, Y_k\})_{k=k_n+1}^{\infty}$.

3.2.1 $n = 3$

Lemma 3.9. *For $n = 3$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, for some $k > 0$, with $n_{odd} = 1$, then there exists a lift $\{X_k^+, Y_k^+\}$ of $\{X_k, Y_k\}$ that is an ideal PTE solution modulo 2^{k+1}.*

Proof. Without loss of generality we suppose that x_1 and y_1 are odd. By (3.14) we have

$$\begin{aligned} d_{k,1}^+ &\equiv d_{k,1} + t_{k,2} + t_{k,3} + u_{k,2} + u_{k,3} \pmod 2 \\ d_{k,2}^+ &\equiv d_{k,2} + t_{k1,} + t_{k,2} + t_{k,3} + u_{k,1} + u_{k,2} + u_{k,3} \pmod 2. \end{aligned} \tag{3.17}$$

Let

$$\begin{aligned} t_{k,1} &= d_{k,1} + d_{k,2} \pmod 2, & u_{k,1} &= 0, \\ t_{k,2} &= d_{k,1} \pmod 2, & t_{k,3} &= 0 \\ u_{k,2} &= u_{k,3}, & u_{k,3} &\in \{0, 1\}. \end{aligned} \tag{3.18}$$

Substituting (3.18) into (3.17) yields

$$\begin{aligned} d_{k,1}^+ &\equiv 0 \pmod 2 \\ d_{k,2}^+ &\equiv 0 \pmod 2. \end{aligned}$$

Thus (3.9) holds and so by Proposition 3.7, $\{X_k^+, Y_k^+\}$ is an ideal PTE solution modulo 2^{k+1}. □

Proposition 3.10. *There exist infinitely many sequences $(\{X_k, Y_k\})_{k=3}^{\infty}$ with*

$$\{X_3, Y_3\} = \{[1, 4, 0], [5, 6, 2]\},$$

such that for each $k > 3$, the pair $\{X_k, Y_k\}$ is a lift of $\{X_{k-1}, Y_{k-1}\}$ that is an ideal PTE solution modulo 2^k with $\nu_2(w_k(0)) = k_3 = 2$.

Proof. Observe that

$$w_3(z) = 8z^2 - 48z + 60 \equiv 4 \pmod{2^3}.$$

So, $\{X_3, Y_3\}$ is an ideal PTE solution modulo 2^3, that is not an integer solution to the PTE problem and that satisfies $\nu_2(w_3(0)) = 2$. Since $\{X_3, Y_3\}$ satisfies the hypothesis of Lemma 3.9, so will any lift $\{X_3, Y_3\}$, and we see that we can construct a sequence $(\{X_3, Y_3\})_{k=3}^{\infty}$ such that for each $k > 3$, the pair $\{X_k, Y_k\}$ is a lift of $\{X_{k-1}, Y_{k-1}\}$ that is an ideal PTE solution modulo 2^k, by lifting $\{X_3, Y_3\}$ successively with the assignments (3.18). By Corollary 3.6, it follows that $\nu_2(w_k(0)) = 2$ for all $k \geq 3$. To see that there are infinitely many such sequences, observe that in (3.18) we allow for $u_{k,3}$ to be either 0 or 1. Thus, we can construct a sequence $(\{X_k, Y_k\})_{k=3}^{\infty}$ corresponding to any sequence of 0's and 1's for the values of $u_{k,3}$. □

3.2.2 $n = 4$

Lemma 3.11. *For $n = 4$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, for some $k > 0$, with $n_{odd} = 2$ and*

$$0 \equiv d_{k,1} + d_{k,2} + d_{k,3} \pmod{2}, \tag{3.19}$$

then there exists a lift $\{X_k^+, Y_k^+\}$ of $\{X_k, Y_k\}$ that is an ideal PTE solution modulo 2^{k+1}.

Proof. Without loss of generality we suppose that x_j and y_j are odd for $j \in \{1, 2\}$. By (3.14) we have

$$\begin{aligned} d_{k,1}^+ &\equiv d_{k,1} + t_{k,3} + t_{k,4} + u_{k,3} + u_{k,4} \pmod{2}, \\ d_{k,2}^+ &\equiv d_{k,2} + t_{k,1} + t_{k,2} + u_{k,1} + u_{k,2} \pmod{2}, \\ d_{k,3}^+ &\equiv d_{k,3} + t_{k,1} + t_{k,2} + t_{k,3} + t_{k,4} + u_{k,1} + u_{k,2} + u_{k,3} + u_{k,4} \pmod{2}. \end{aligned} \tag{3.20}$$

Let $t_{k,j}$ and $u_{k,j}$ in $\{0,1\}$ be defined by

$$\begin{aligned} t_{k,1} &\equiv \frac{d_{k,1}+d_{k,2}+d_{k,3}}{2} \pmod 2, & t_{k,2} &= 0, \\ u_{k,1} &\equiv t_{k,1}+d_{k,2} \pmod 2, & u_{k,2} &= 0, \\ t_{k,3} &\equiv d_{k,2}+d_{k,3} \pmod 2, & t_{k,4} &= 0, \\ u_{k,3} &= u_{k,4}, & u_{k,4} &\in \{0,1\}. \end{aligned} \tag{3.21}$$

Note that such $t_{k,j}$ and $u_{k,j}$ in $\{0,1\}$ exist since (3.19) holds. Substituting (3.21) into (3.20) yields that each of $d_{k,1}^+$, $d_{k,2}^+$ and $d_{k,3}^+$ is 0 (mod 2). Thus, (3.9) holds and Proposition 3.7 implies that $\{X_k^+, Y_k^+\}$ is an ideal PTE solution modulo 2^{k+1}. □

Proposition 3.12. *There exist infinitely many sequences* $(\{X_k, Y_k\})_{k=3}^{\infty}$ *with*

$$\{X_3, Y_3\} = \{[1,1,0,0],[7,3,6,2]\}, \tag{3.22}$$

such that for each $k > 3$*, the pair* $\{X_k, Y_k\}$ *is a lift of* $\{X_{k-1}, Y_{k-1}\}$ *that is an ideal PTE solution modulo* 2^k *with* $\nu_2(w_k(0)) = k_4 = 2$*.*

Proof. Observe that

$$w_3(z) = 16z^3 - 112z^2 + 288z - 252 \equiv 4 \pmod{2^3}.$$

So, $\{X_3, Y_3\}$ is an ideal PTE solution modulo 2^3, that is not an integer solution to the PTE problem and that satisfies $\nu_2(w_3(0)) = 2$. Also note that

$$d_{3,1} + d_{3,2} + d_{3,3} = -36 - 14 - 2 \equiv 0 \pmod 2,$$

so $\{X_3, Y_3\}$ satisfies (3.19) with $k = 3$.

First we prove that we can construct a sequence $(\{X_k, Y_k\})_{k=3}^{\infty}$ of ideal PTE solutions modulo 2^k that are obtained by successively lifting $\{X_3, Y_3\}$. Since $\{X_3, Y_3\}$ satisfies the hypothesis of Lemma 3.11 with $k = 3$, it suffices to show that for an integer $k > 3$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k congruent to $\{X_3, Y_3\}$

(mod 8) that satisfies (3.19), then the lift of $\{X_k, Y_k\}$ obtained in the proof of Proposition 3.11 also satisfies (3.19) but with k replaced by $k+1$.

From (3.14) we note that for all $k > 3$ we have

$$d_{k,j}^{+} \equiv d_{k,j} + \sum_{i=1}^{n} \left(e_{n-1-j}\left(\hat{X_3^i}\right) t_{k,i} - e_{n-1-j}\left(\hat{Y_3^i}\right) u_{k,i} \right) \pmod{2^m}$$

for $j \in \{1,2,3\}$ and $m \leq 3$. Substituting (3.22) into the above with $m = 2$ yields

$$\begin{aligned}
d_{k,1}^{+} &\equiv d_{k,1} + t_{k,3} + t_{k,4} - u_{k,3} - u_{k,4} \pmod 4 \\
d_{k,2}^{+} &\equiv d_{k,2} + t_{k,1} + t_{k,2} + 2t_{k,3} + 2t_{k,4} + u_{k,1} + u_{k,2} \pmod 4 \\
d_{k,3}^{+} &\equiv d_{k,3} + t_{k,1} + t_{k,2} + t_{k,3} + t_{k,4} - u_{k,1} - u_{k,2} - u_{k,3} - u_{k,4} \pmod 4.
\end{aligned}$$

From the above we deduce that

$$d_{k,1}^{+} + d_{k,2}^{+} + d_{k,3}^{+} \equiv d_{k,1} + d_{k,2} + d_{k,3} + 2\left(t_{k,1} + u_{k,3} + u_{k,4}\right) \pmod 4.$$

Substituting the assignment (3.21) into the above yields

$$d_{k,1}^{+} + d_{k,2}^{+} + d_{k,3}^{+} \equiv 2\left(d_{k,1} + d_{k,2} + d_{k,3}\right) \pmod 4.$$

Since $\{X_k, Y_k\}$ satisfies (3.19), we have

$$d_{k,1}^{+} + d_{k,2}^{+} + d_{k,3}^{+} \equiv 0 \pmod 4,$$

and so by Lemma 3.8, we see that $\{X_{k+1}, Y_{k+1}\}$ satisfies (3.19) but with k replaced by $k+1$.

So, we can construct a sequence $(\{X_k, Y_k\})_{k=3}^{\infty}$ such that for each $k > 3$, the pair $\{X_k, Y_k\}$ is a lift of $\{X_{k-1}, Y_{k-1}\}$ that is an ideal PTE solution modulo 2^k, by lifting $\{X_3, Y_3\}$ successively with the assignments (3.21). By Corollary 3.6 it follows that $\nu_2\left(w_k(0)\right) = 2$ for all $k \geq 3$. To see that there are infinitely many such sequences, observe that in (3.21) we allow for $u_{k,4}$ to be either 0 or 1. Thus, we can construct a sequence $(\{X_k, Y_k\})_{k=3}^{\infty}$ corresponding to any sequence of 0's and 1's for the values of $u_{k,4}$. □

3.2.3 $n = 5$

Lemma 3.13. *For $n = 5$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, for some $k > 0$, with $n_{odd} = 1$ and*

$$0 \equiv d_{k,1} + 2d_{k,2} \pmod 8 \quad \textit{and} \quad 0 \equiv d_{k,2} \pmod 2, \tag{3.23}$$

then there exists a lift $\{X_k^+, Y_k^+\}$ of $\{X_k, Y_k\}$ that is an ideal PTE solution modulo 2^{k+1}.

Proof. From (3.23), we see that $2d_{k,2} \equiv 0 \pmod 4$, and so

$$d_{k,1} \equiv 0 \pmod 4.$$

Without loss of generality we suppose that x_1 and y_1 are odd. By (3.14) we have

$$\begin{aligned}
d_{k,1}^+ &\equiv d_{k,1} \pmod 2 \\
d_{k,2}^+ &\equiv d_{k,2} \pmod 2 \\
d_{k,3}^+ &\equiv d_{k,3} + \sum_{j=2}^{5} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,4}^+ &\equiv d_{k,4} + \sum_{j=1}^{5} (t_{k,j} + u_{k,j}) \pmod 2
\end{aligned} \tag{3.24}$$

Let $t_{k,j}$ and $u_{k,j}$ in $\{0, 1\}$ be defined by

$$\begin{aligned}
t_{k,1} &\equiv d_{k,3} + d_{k,4} \pmod 2, & u_{k,1} &= 0, \\
t_{k,2} &\equiv \frac{d_{k,2}}{2} + d_{k,3} \pmod 2, & t_{k,3} &= 0, \\
u_{k,2} &\equiv \frac{d_{k,1} + 2d_{k,2}}{8} \pmod 2, & t_{k,4} &= 0, \\
u_{k,3} &\equiv u_{k,2} + \frac{d_{k,2}}{2} \pmod 2, & t_{k,5} &= 0, \\
u_{k,4} &= u_{k,5}, & u_{k,5} &\in \{0, 1\}.
\end{aligned} \tag{3.25}$$

Note that such $t_{k,j}$ and $u_{k,j}$ in $\{0, 1\}$ exist since (3.23) holds. Substituting (3.25) into (3.24) yields that each $d_{k,j}^+$ in (3.24) is 0 (mod 2). Thus, (3.9) holds and so by Proposition 3.7, the pair $\{X_k^+, Y_k^+\}$ is an ideal PTE solution modulo 2^{k+1}. □

Proposition 3.14. *There exist infinitely many sequences* $(\{X_k, Y_k\})_{k=5}^{\infty}$ *with*

$$\{X_5, Y_5\} = \{[1, 4, 8, 16, 0], [17, 14, 10, 18, 2]\}, \tag{3.26}$$

such that for each $k > 5$*, the pair* $\{X_k, Y_k\}$ *is a lift of* $\{X_{k-1}, Y_{k-1}\}$ *that is an ideal PTE solution modulo* 2^k *with* $\nu_2(w_k(0)) = k_5 = 4$*.*

Proof. Observe that

$$w_5(z) = 32z^4 - 1152z^3 + 14080z^2 - 66816z + 85680 \equiv 16 \pmod{2^5}.$$

So, $\{X_5, Y_5\}$ is an ideal PTE solution modulo 2^5, that is not an integer solution to the PTE problem and that satisfies $\nu_2(w_5(0)) = 4$. Also note that

$$d_{5,1} + 2d_{5,2} = -2088 - 880 \equiv 0 \pmod{8},$$
$$d_{5,2} = -440 \equiv 0 \pmod{2},$$

so $\{X_5, Y_5\}$ satisfies (3.23), with $k = 5$.

First we prove that we can construct a sequence $(\{X_k, Y_k\})_{k=5}^{\infty}$ of ideal PTE solutions modulo 2^k that are obtained by successively lifting $\{X_5, Y_5\}$. Since $\{X_5, Y_5\}$ satisfies the hypothesis of Lemma 3.13 with $k = 5$, it suffices to show that for an integer $k > 5$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k congruent to $\{X_5, Y_5\}$ (mod 32) that satisfies (3.23), then the lift of $\{X_k, Y_k\}$ obtained in the proof of Proposition 3.13 also satisfies (3.23) but with k replaced by $k + 1$.

From (3.14) we note that for all $k > 5$ we have

$$d_{k,j}^{+} \equiv d_{k,j} + \sum_{i=1}^{n} \left(e_{n-1-j}\left(\hat{X}_5^i\right) t_{k,i} - e_{n-1-j}\left(\hat{Y}_5^i\right) u_{k,i} \right) \pmod{2^m},$$

for $j \in \{1, 2, \ldots, 4\}$ and $m \leq 5$. For $j \in \{1, 2\}$, substituting (3.26) into the above with $m = 4$ yields

$$d_{k,1}^{+} \equiv d_{k,1} - 4u_{k,2} - 4u_{k,3} - 4u_{k,4} - 4u_{k,5} \pmod{16},$$
$$d_{k,2}^{+} \equiv d_{k,2} + 8t_{k,2} + 4t_{k,3} - 4t_{k,4} - 4t_{k,5} + 6u_{k,2} + 2u_{k,3} - 6u_{k,4} - 6u_{k,5} \pmod{16}.$$

From the above we deduce that

$$d^+_{k,1} + 2d_{k,2} \equiv d_{k,1} + 2d_{k,2} + 8\left(t_{k,3} + t_{k,4} + t_{k,5} + u_{k,2}\right) \pmod{16},$$
$$d^+_{k,2} \equiv d_{k,2} + 2\left(u_{k,3} + u_{k,2}\right) \pmod{4}.$$

Substituting the assignment (3.25), into the above yields

$$d^+_{k,1} + 2d^+_{k,2} \equiv 2\left(d_{k,1} + 2d_{k,2}\right) \pmod{16},$$
$$d^+_{k,2} \equiv 2d_{k,2} \pmod{4}.$$

Since $\{X_k, Y_k\}$ satisfies (3.23), we have

$$d^+_{k,1} + 2d^+_{k,2} \equiv 0 \pmod{16},$$
$$d^+_{k,2} \equiv 0 \pmod{4},$$

and so by Lemma 3.8, we see that $\{X_{k+1}, Y_{k+1}\}$ satisfies (3.23) with k replaced by $k+1$.

So, we can construct a sequence $(\{X_k, Y_k\})_{k=5}^{\infty}$ such that for each $k > 5$, the pair $\{X_k, Y_k\}$ is a lift of $\{X_{k-1}, Y_{k-1}\}$ that is an ideal PTE solution modulo 2^k, by lifting $\{X_5, Y_5\}$ successively with the assignments (3.25). By Corollary 3.6 it follows that $\nu_2\left(w_k(0)\right) = 4$ for all $k \geq 5$. To see that there are infinitely many such sequences, observe that in (3.25) we allow for $u_{k,5}$ to be either 0 or 1. Thus, we can construct a sequence $(\{X_k, Y_k\})_{k=5}^{\infty}$ corresponding to any sequence of 0's and 1's for the values of $u_{k,5}$. □

3.2.4 $n = 6$

Lemma 3.15. *For $n = 6$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, for some $k > 0$, with $n_{odd} = 3$ and*

$$\begin{aligned} 0 &\equiv d_{k,1} - d_{k,2} + d_{k,3} - d_{k,4} + d_{k,5} \pmod{8}, \\ 0 &\equiv d_{k,2} + d_{k,4} \pmod{2}, \\ 0 &\equiv d_{k,3} + d_{k,5} \pmod{2}, \end{aligned} \tag{3.27}$$

then there exists a lift $\{X_k^+, Y_k^+\}$ *of* $\{X_k, Y_k\}$ *that is an ideal PTE solution modulo* 2^{k+1}.

Proof. From the first congruence in (3.27), we have

$$0 \equiv d_{k,1} + d_{k,2} + d_{k,3} + d_{k,4} + d_{k,5} \pmod 2.$$

Adding the second and third congruences in (3.27) to the above yields

$$d_{k,1} \equiv 0 \pmod 2.$$

Without loss of generality we suppose that x_j and y_j are odd for $j \in \{1, 2, 3\}$. By (3.14) we have

$$\begin{aligned}
d_{k,1}^+ &\equiv d_{k,1} \pmod 2 \\
d_{k,2}^+ &\equiv d_{k,2} + \sum_{j=4}^{6} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,3}^+ &\equiv d_{k,3} + \sum_{j=1}^{6} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,4}^+ &\equiv d_{k,4} + \sum_{j=4}^{6} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,5}^+ &\equiv d_{k,5} + \sum_{j=1}^{6} (t_{k,j} + u_{k,j}) \pmod 2.
\end{aligned} \tag{3.28}$$

Let $t_{k,j}$ and $u_{k,j}$ in $\{0, 1\}$ be defined by

$$\begin{aligned}
t_{k,1} &\equiv \frac{d_{k,2} + d_{k,4}}{2} \pmod 2, & t_{k,3} &= 0, \\
u_{k,2} &\equiv \frac{d_{k,1} - d_{k,2} + d_{k,3} - d_{k,4} + d_{k,5}}{8} \pmod 2, & t_{k,6} &= 0, \\
t_{k,5} &\equiv t_{k,1} + \frac{d_{k,3} + d_{k,5}}{2} \pmod 2, & u_{k,1} &= 0, \\
t_{k,4} &\equiv t_{k,5} + d_{k,4} \pmod 2, & u_{k,3} &= 0, \\
t_{k,2} &\equiv t_{k,1} + u_{k,2} + d_{k,4} + d_{k,5} \pmod 2, & u_{k,4} &= 0, \\
u_{k,5} &= u_{k,6}, & u_{k,6} &\in \{0, 1\}.
\end{aligned} \tag{3.29}$$

Note that such $t_{k,j}$ and $u_{k,j}$ in $\{0, 1\}$ exist since (3.27) holds. Substituting (3.29) into (3.28) yields that each $d_{k,j}^+$ in (3.28) is 0 (mod 2). Thus, (3.9) holds and so by Proposition 3.7, the pair $\{X_k^+, Y_k^+\}$ is an ideal PTE solution modulo 2^{k+1}. □

Proposition 3.16. *There exist infinitely many sequences* $(\{X_k, Y_k\})_{k=6}^{\infty}$ *with*

$$\{X_6, Y_6\} = \{[3, 1, 1, 2, 8, 0], [59, 29, 45, 42, 12, 20]\}, \tag{3.30}$$

such that for each $k > 6$*, the pair* $\{X_k, Y_k\}$ *is a lift of* $\{X_{k-1}, Y_{k-1}\}$ *that is an ideal PTE solution modulo* 2^k *with* $\nu_2(w_k(0)) = k_6 = 5$.

Proof. Observe that

$$\begin{aligned} w_6(z) &= 192z^5 - 17024z^4 + 717248z^3 - 16020991z^2 \\ &\quad + 179123712z - 776109600 \\ &\equiv 32 \pmod{2^6}. \end{aligned}$$

So, $\{X_6, Y_6\}$ is an ideal PTE solution modulo 2^6, that is not an integer solution to the PTE problem and that satisfies $\nu_2(w_6(0)) = 5$. Also note that

$$\begin{aligned} d_{6,1} - d_{6,2} + d_{6,3} - d_{6,4} + d_{6,5} &= -2798808 + 250328 \\ &\quad - 11207 + 266 - 3 \equiv 0 \pmod 8 \\ d_{6,2} + d_{6,4} &= -250328 - 26 \equiv 0 \pmod 2 \\ d_{6,3} + d_{6,5} &= -11207 - 3 \equiv 0 \pmod 2, \end{aligned}$$

so $\{X_6, Y_6\}$ satisfies (3.27), with $k = 6$.

First we prove that we can construct a sequence $(\{X_k, Y_k\})_{k=6}^{\infty}$ of ideal PTE solutions modulo 2^k that are obtained by successively lifting $\{X_6, Y_6\}$. Since $\{X_6, Y_6\}$ satisfies the hypothesis of Lemma 3.15 with $k = 6$, it suffices to show that for an integer $k > 6$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k congruent to $\{X_6, Y_6\}$ (mod 64) that satisfies (3.27), then the lift of $\{X_k, Y_k\}$ obtained in the proof of Proposition 3.15 also satisfies (3.27) but with k replaced by $k + 1$.

From (3.14) we note that for all $k > 6$ we have

$$d_{k,j}^{+} \equiv d_{k,j} + \sum_{i=1}^{n} \left(e_{n-1-j}\left(\hat{X}_6^i\right) t_{k,i} - e_{n-1-j}\left(\hat{Y}_6^i\right) u_{k,i} \right) \pmod{2^m},$$

for $j \in \{1, 2, \ldots, 5\}$ and $m \leq 6$. Substituting (3.30) into the above with $m = 4$ yields

$$\begin{aligned}
d^+_{k,1} &\equiv d_{k,1} + 8t_{k,4} + 6t_{k,5} - 2t_{k,6} - 2u_{k,5} + 6u_{k,6} \pmod{16} \\
d^+_{k,2} &\equiv d_{k,2} - 6t_{k,1} - 2t_{k,2} - 2t_{k,3} - 5t_{k,4} + t_{k,5} - 7t_{k,6} \\
&\qquad + 6u_{k,1} - 6u_{k,2} - 6u_{k,3} - 3u_{k,4} + 3u_{k,5} - 5u_{k,6} \pmod{16} \\
d^+_{k,3} &\equiv d_{k,3} + 5t_{k,1} - 5t_{k,2} - 5t_{k,3} - t_{k,4} + t_{k,5} - 7t_{k,6} \\
&\qquad + 3u_{k,1} + u_{k,2} + u_{k,3} - 7u_{k,4} - 5u_{k,5} + 3u_{k,6} \pmod{16} \qquad (3.31) \\
d^+_{k,4} &\equiv d_{k,4} - 4t_{k,1} - 2t_{k,2} - 2t_{k,3} - 3t_{k,4} + 7t_{k,5} - t_{k,6} \\
&\qquad - 4u_{k,1} - 2u_{k,2} - 2u_{k,3} - 5u_{k,4} - 3u_{k,5} + 5u_{k,6} \pmod{16} \\
d^+_{k,5} &\equiv d_{k,5} + t_{k,1} + t_{k,2} + t_{k,3} + t_{k,4} + t_{k,5} + t_{k,6} \\
&\qquad - u_{k,1} - u_{k,2} - u_{k,3} - u_{k,4} - u_{k,5} - u_{k,6} \pmod{16}.
\end{aligned}$$

Recall the $t_{k,j}$ and $u_{k,j}$ in (3.29) that were assigned to be zero.

$$t_{k,3} = 0, \quad t_{k,6} = 0, \quad u_{k,1} = 0, \quad u_{k,3} = 0 \quad \text{and} \quad u_{k,4} = 0.$$

Substituting the above into (3.31) yields

$$\begin{aligned}
d^+_{k,1} &\equiv d_{k,1} + 8t_{k,4} + 6t_{k,5} - 2u_{k,5} + 6u_{k,6} \pmod{16} \\
d^+_{k,2} &\equiv d_{k,2} - 6t_{k,1} - 2t_{k,2} - 5t_{k,4} + t_{k,5} - 6u_{k,2} + 3u_{k,5} - 5u_{k,6} \pmod{16} \\
d^+_{k,3} &\equiv d_{k,3} + 5t_{k,1} - 5t_{k,2} - t_{k,4} + t_{k,5} + u_{k,2} - 5u_{k,5} + 3u_{k,6} \pmod{16} \\
d^+_{k,4} &\equiv d_{k,4} - 4t_{k,1} - 2t_{k,2} - 3t_{k,4} + 7t_{k,5} - 2u_{k,2} - 3u_{k,5} + 5u_{k,6} \pmod{16} \\
d^+_{k,5} &\equiv d_{k,5} + t_{k,1} + t_{k,2} + t_{k,4} + t_{k,5} - u_{k,2} - u_{k,5} - u_{k,6} \pmod{16}.
\end{aligned}$$

From the above we deduce that

$$\begin{aligned}
d^+_{k,1} - d^+_{k,2} + d^+_{k,3} - d^+_{k,4} + d^+_{k,5} &\equiv d_{k,1} - d_{k,2} + d_{k,3} - d_{k,4} + d_{k,5} \\
&\qquad + 8\left(u_{k,2} + u_{k,5} + u_{k,6}\right) \pmod{16} \\
d^+_{k,2} + d^+_{k,4} &\equiv d_{k,2} + d_{k,4} + 2t_{k,1} \pmod{4} \\
d^+_{k,3} + d^+_{k,5} &\equiv d_{k,3} + d_{k,5} + 2\left(t_{k,1} + t_{k,5} + u_{k,5} + u_{k,6}\right) \pmod{4}.
\end{aligned}$$

Substituting the assignment (3.29) into the above yields

$$\begin{aligned} d_{k,1}^+ - d_{k,2}^+ + d_{k,3}^+ - d_{k,4}^+ + d_{k,5}^+ &\equiv 2\left(d_{k,1} - d_{k,2} + d_{k,3} - d_{k,4} + d_{k,5}\right) \pmod{16} \\ d_{k,2}^+ + d_{k,4}^+ &\equiv 2\left(d_{k,2} + d_{k,4}\right) \pmod{4} \\ d_{k,3}^+ + d_{k,5}^+ &\equiv 2\left(d_{k,3} + d_{k,5}\right) \pmod{4}. \end{aligned}$$

Since $\{X_k, Y_k\}$ satisfies (3.27), we have

$$\begin{aligned} d_{k,1}^+ - d_{k,2}^+ + d_{k,3}^+ - d_{k,4}^+ + d_{k,5}^+ &\equiv 0 \pmod{16} \\ d_{k,2}^+ + d_{k,4}^+ &\equiv 0 \pmod{4} \\ d_{k,3}^+ + d_{k,5}^+ &\equiv 0 \pmod{4}, \end{aligned}$$

and so by Lemma 3.8, we see that $\{X_{k+1}, Y_{k+1}\}$ satisfies (3.27) with k replaced by $k+1$.

So, we can construct a sequence $(\{X_k, Y_k\})_{k=6}^{\infty}$ such that for each $k > 6$, the pair $\{X_k, Y_k\}$ is a lift of $\{X_{k-1}, Y_{k-1}\}$ that is an ideal PTE solution modulo 2^k, by lifting $\{X_6, Y_6\}$ successively with the assignments (3.29). By Corollary 3.6 it follows that $\nu_2\left(w_k(0)\right) = 5$ for all $k \geq 6$. To see that there are infinitely many such sequences, observe that in (3.29) we allow for $u_{k,6}$ to be either 0 or 1. Thus, we can construct a sequence $(\{X_k, Y_k\})_{k=6}^{\infty}$ corresponding to any sequence of 0's and 1's for the values of $u_{k,6}$. □

3.2.5 $n = 7$

Lemma 3.17. *For $n = 7$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, for some $k > 0$, with $n_{odd} = 3$ and*

$$\begin{aligned} 0 &\equiv d_{k,1} + d_{k,2} - d_{k,3} + d_{k,4} - d_{k,5} + d_{k,6} \pmod{8}, \\ 0 &\equiv d_{k,2} + d_{k,3} - d_{k,4} - 3d_{k,5} - d_{k,6} \pmod{8}, \\ 0 &\equiv d_{k,3} + d_{k,5} \pmod{2}, \\ 0 &\equiv d_{k,4} + d_{k,6} \pmod{2}, \end{aligned} \tag{3.32}$$

then there exists a lift $\{X_k^+, Y_k^+\}$ *of* $\{X_k, Y_k\}$ *that is an ideal PTE solution modulo* 2^{k+1}.

Proof. From the first and second congruences in (3.32), we have

$$0 \equiv d_{k,1} + d_{k,2} + d_{k,3} + d_{k,4} + d_{k,5} + d_{k,6} \pmod 2,$$
$$0 \equiv d_{k,2} + d_{k,3} + d_{k,4} + d_{k,5} + d_{k,6} \pmod 2.$$

Combining these with the third and fourth congruences in (3.32) we deduce

$$0 \equiv d_{k,1} \pmod 2 \quad \text{and} \quad 0 \equiv d_{k,2} \pmod 2.$$

Taking x_j and y_j odd for $j \in \{1,2,3\}$ and using (3.14), we have

$$\begin{aligned}
d_{k,1}^+ &\equiv d_{k,1} \pmod 2 \\
d_{k,2}^+ &\equiv d_{k,2} \pmod 2 \\
d_{k,3}^+ &\equiv d_{k,3} + \sum_{j=4}^{7} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,4}^+ &\equiv d_{k,4} + \sum_{j=1}^{7} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,5}^+ &\equiv d_{k,5} + \sum_{j=4}^{7} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,6}^+ &\equiv d_{k,6} + \sum_{j=1}^{7} (t_{k,j} + u_{k,j}) \pmod 2
\end{aligned} \tag{3.33}$$

Let $t_{k,j}$ and $u_{k,j}$ in $\{0,1\}$ be defined by

$$\begin{aligned}
t_{k,1} &\equiv \frac{d_{k,3} + d_{k,5}}{2} \pmod 2, && t_{k,5} = 0 \\
t_{k,6} &\equiv t_{k,1} + \frac{d_{k,4} + d_{k,6}}{2} + d_{k,5} \pmod 2, && t_{k,7} = 0 \\
t_{k,3} &\equiv t_{k,6} + \frac{d_{k,1} + d_{k,2} - d_{k,3} + d_{k,4} - d_{k,5} + d_{k,6}}{8} \pmod 2, && u_{k,1} = 0 \\
t_{k,2} &\equiv t_{k,1} + t_{k,3} + d_{k,5} + d_{k,6} \pmod 2, && u_{k,2} = 0 \\
u_{k,4} &\equiv t_{k,2} + \frac{d_{k,2} + d_{k,3} - d_{k,4} - 3d_{k,5} - d_{k,6}}{8} \pmod 2, && u_{k,3} = 0 \\
t_{k,4} &\equiv t_{k,6} + u_{k,4} + d_{k,5} \pmod 2, && u_{k,5} = 0 \\
u_{k,6} &= u_{k,7}, && u_{k,7} \in \{0,1\}.
\end{aligned} \tag{3.34}$$

Note that such $t_{k,j}$ and $u_{k,j}$ in $\{0,1\}$ exist since (3.32) holds. Substituting (3.34) into (3.33) yields that each $d_{k,j}^{+}$ in (3.33) is 0 (mod 2). Thus, (3.9) holds and so by Proposition 3.7, the pair $\{X_k^{+}, Y_k^{+}\}$ is an ideal PTE solution modulo 2^{k+1}. □

Proposition 3.18. *There exist infinitely many sequences* $(\{X_k, Y_k\})_{k=7}^{\infty}$ *with*

$$\{X_7, Y_7\} = \{[3,5,1,10,2,0,0],[115,29,121,38,38,28,36]\}, \tag{3.35}$$

such that for each $k > 7$*, the pair* $\{X_k, Y_k\}$ *is a lift of* $\{X_{k-1}, Y_{k-1}\}$ *that is an ideal PTE solution modulo* 2^k *with* $\nu_2(w_k(0)) = k_7 = 6$.

Proof. Observe that

$$\begin{aligned} w_7(z) &= 384z^6 - 65024z^5 + 541708z^4 - 254614016z^3 \\ &\quad + 6846752256z^2 - 98422903808z + 587366176320 \\ &\equiv 64 \pmod{2^7}. \end{aligned}$$

So, $\{X_7, Y_7\}$ is an ideal PTE solution modulo 2^7, that is not an integer solution to the PTE problem and that satisfies $\nu_2(w_7(0)) = 6$. Also note that

$$\begin{aligned} d_{7,1} + d_{7,2} - d_{7,3} + d_{7,4} - d_{7,5} + d_{7,6} &= -768928936 - 53490252 + 1989172 \\ &\quad - 42321 + 508 - 3 \equiv 0 \pmod 8 \\ d_{7,2} + d_{7,3} - d_{7,4} - 3d_{7,5} - d_{7,6} &= -53490252 - 1989172 \\ &\quad + 42321 + 1524 + 3 \equiv 0 \pmod 8 \\ d_{7,3} + d_{7,5} &= -1989172 - 508 \equiv 0 \pmod 2 \\ d_{7,4} + d_{7,6} &= -42321 - 3 \equiv 0 \pmod 2, \end{aligned}$$

so $\{X_7, Y_7\}$ satisfies (3.32), with $k = 7$.

First we prove that we can construct a sequence $(\{X_k, Y_k\})_{k=7}^{\infty}$ of ideal PTE solutions modulo 2^k that are obtained by successively lifting $\{X_7, Y_7\}$. Since $\{X_7, Y_7\}$ satisfies the hypothesis of Lemma 3.17 with $k = 7$, it suffices to show that for an

integer $k > 7$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k congruent to $\{X_7, Y_7\}$ (mod 128) that satisfies (3.32), then the lift of $\{X_k, Y_k\}$ obtained in the proof of Proposition 3.17 also satisfies (3.32) but with k replaced by $k+1$.

From (3.14) we note that for all $k > 7$ we have

$$d_{k,j}^{+} \equiv d_{k,j} + \sum_{i=1}^{n} \left(e_{n-1-j}\left(\hat{X}_7^i\right) t_{k,i} - e_{n-1-j}\left(\hat{Y}_7^i\right) u_{k,i} \right) \pmod{2^m},$$

for $j \in \{1, 2, \ldots, 6\}$ and $m \leq 7$. Substituting (3.35) into the above with $m = 4$ yields

$$\begin{aligned}
d_{k,1}^{+} &\equiv d_{k,1} - 4t_{k,6} - 4t_{k,7} + 4u_{k,6} + 4u_{k,7} \pmod{16} \\
d_{k,2}^{+} &\equiv d_{k,2} + 4t_{k,1} - 4t_{k,2} - 4t_{k,3} - 2t_{k,4} + 6t_{k,5} \\
&\quad - 4u_{k,1} + 4u_{k,2} + 4u_{k,3} + 6u_{k,4} + 6u_{k,5} + 4u_{k,6} - 4u_{k,7} \pmod{16} \\
d_{k,3}^{+} &\equiv d_{k,3} + 4t_{k,1} + 4t_{k,2} + 4t_{k,3} - 3t_{k,4} + 5t_{k,5} + 7t_{k,6} + 7t_{k,7} \\
&\quad - 4u_{k,1} - 4u_{k,2} - 4u_{k,3} + 7u_{k,4} + 7u_{k,5} - 3u_{k,6} + 5u_{k,7} \pmod{16} \\
d_{k,4}^{+} &\equiv d_{k,4} + t_{k,1} + 7t_{k,2} + 3t_{k,3} - 7t_{k,4} + t_{k,5} + 7t_{k,6} + 7t_{k,7} \\
&\quad - u_{k,1} + u_{k,2} + 5u_{k,3} + 3u_{k,4} + 3u_{k,5} + 5u_{k,6} - 3u_{k,7} \pmod{16} \\
d_{k,5}^{+} &\equiv d_{k,5} + 2t_{k,1} + 4t_{k,3} - 5t_{k,4} + 3t_{k,5} + 5t_{k,6} + 5t_{k,7} \\
&\quad - 2u_{k,1} + 8u_{k,2} + 4u_{k,3} + u_{k,4} + u_{k,5} + 7u_{k,6} - u_{k,7} \pmod{16} \\
d_{k,6}^{+} &\equiv d_{k,6} + t_{k,1} + t_{k,2} + t_{k,3} + t_{k,4} + t_{k,5} + t_{k,6} + t_{k,7} \\
&\quad - u_{k,1} - u_{k,2} - u_{k,3} - u_{k,4} - u_{k,5} - u_{k,6} - u_{k,7} \pmod{16}.
\end{aligned} \tag{3.36}$$

Recall the $t_{k,j}$ and $u_{k,j}$ in (3.34) that were assigned to be zero.

$$t_{k,5} = 0, \quad t_{k,7} = 0, \quad u_{k,1} = 0, \quad u_{k,2} = 0 \quad u_{k,3} = 0 \quad \text{and} \quad u_{k,5} = 0.$$

Substituting the above into (3.36) yields

$$\begin{aligned}
d_{k,1}^{+} &\equiv d_{k,1} - 4t_{k,6} + 4u_{k,6} + 4u_{k,7} \pmod{16} \\
d_{k,2}^{+} &\equiv d_{k,2} + 4t_{k,1} - 4t_{k,2} - 4t_{k,3} - 2t_{k,4} + 6u_{k,4} + 4u_{k,6} - 4u_{k,7} \pmod{16} \\
d_{k,3}^{+} &\equiv d_{k,3} + 4t_{k,1} + 4t_{k,2} + 4t_{k,3} - 3t_{k,4} + 7t_{k,6} + 7u_{k,4} - 3u_{k,6} + 5u_{k,7} \pmod{16}
\end{aligned}$$

$$d^+_{k,4} \equiv d_{k,4} + t_{k,1} + 7t_{k,2} + 3t_{k,3} - 7t_{k,4} + 7t_{k,6} + 3u_{k,4} + 5u_{k,6} - 3u_{k,7} \pmod{16}$$

$$d^+_{k,5} \equiv d_{k,5} + 2t_{k,1} + 4t_{k,3} - 5t_{k,4} + 5t_{k,6} + u_{k,4} + 7u_{k,6} - u_{k,7} \pmod{16}$$

$$d^+_{k,6} \equiv d_{k,6} + t_{k,1} + t_{k,2} + t_{k,3} + t_{k,4} + t_{k,6} - u_{k,4} - u_{k,6} - u_{k,7} \pmod{16}.$$

From the above we deduce that

$$\begin{aligned} d^+_{k,1} + d^+_{k,2} - d^+_{k,3} + d^+_{k,4} - d^+_{k,5} + d^+_{k,6} &\equiv d_{k,1} + d_{k,2} - d_{k,3} + d_{k,4} - d_{k,5} + d_{k,6} \\ &\quad + 8t_{k,3} + 8t_{k,6} + 8u_{k,6} + 8u_{k,7} \pmod{16} \\ d^+_{k,2} + d^+_{k,3} - d^+_{k,4} - 3d^+_{k,5} - d^+_{k,6} &\equiv d_{k,2} + d_{k,3} - d_{k,4} - 3d_{k,5} - d_{k,6} \\ &\quad + 8t_{k,2} + 8u_{k,4} + 8u_{k,6} + 8u_{k,7} \pmod{16} \\ d^+_{k,3} + d^+_{k,5} &\equiv d_{k,3} + d_{k,5} + 2t_{k,1} \pmod{4} \\ d^+_{k,4} + d^+_{k,6} &\equiv d_{k,4} + d_{k,6} + 2t_{k,1} + 2t_{k,4} + 2u_{k,4} \pmod{4}. \end{aligned}$$

Substituting the assignment (3.34) into the above yields

$$\begin{aligned} d^+_{k,1} + d^+_{k,2} - d^+_{k,3} + d^+_{k,4} - d^+_{k,5} + d^+_{k,6} &\equiv 2d_{k,1} + 2d_{k,2} - 2d_{k,3} \\ &\quad + 2d_{k,4} - 2d_{k,5} + 2d_{k,6} \pmod{16} \\ d^+_{k,2} + d^+_{k,3} - d^+_{k,4} - 3d^+_{k,5} - d^+_{k,6} &\equiv 2\left(d_{k,2} + d_{k,3} - d_{k,4} - 3d_{k,5} - d_{k,6}\right) \pmod{16} \\ d^+_{k,3} + d^+_{k,5} &\equiv 2\left(d_{k,3} + d_{k,5}\right) \pmod{4} \\ d^+_{k,4} + d^+_{k,6} &\equiv 2\left(d_{k,4} + d_{k,6}\right) \pmod{4}. \end{aligned}$$

Since $\{X_k, Y_k\}$ satisfies (3.32), we have

$$\begin{aligned} d^+_{k,1} + d^+_{k,2} - d^+_{k,3} + d^+_{k,4} - d^+_{k,5} + d^+_{k,6} &\equiv 0 \pmod{16} \\ d^+_{k,2} + d^+_{k,3} - d^+_{k,4} - 3d^+_{k,5} - d^+_{k,6} &\equiv 0 \pmod{16} \\ d^+_{k,3} + d^+_{k,5} &\equiv 0 \pmod{4} \\ d^+_{k,4} + d^+_{k,6} &\equiv 0 \pmod{4}. \end{aligned}$$

and so by Lemma 3.8, we see that $\{X_{k+1}, Y_{k+1}\}$ satisfies (3.32) with k replaced by $k+1$.

So, we can construct a sequence $(\{X_k, Y_k\})_{k=7}^{\infty}$ such that for each $k > 7$, the pair $\{X_k, Y_k\}$ is a lift of $\{X_{k-1}, Y_{k-1}\}$ that is an ideal PTE solution modulo 2^k, by lifting $\{X_7, Y_7\}$ successively with the assignments (3.34). By Corollary 3.6 it follows that $\nu_2(w_k(0)) = 6$ for all $k \geq 7$. To see that there are infinitely many such sequences, observe that in (3.34) we allow for $u_{k,7}$ to be either 0 or 1. Thus, we can construct a sequence $(\{X_k, Y_k\})_{k=7}^{\infty}$ corresponding to any sequence of 0's and 1's for the values of $u_{k,7}$. □

3.2.6 $n = 8$

Lemma 3.19. *For $n = 8$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k, for some $k > 0$, with $n_{odd} = 4$ and*

$$\begin{aligned}
0 &\equiv d_{k,1} + d_{k,2} + d_{k,3} + d_{k,4} + d_{k,5} + d_{k,6} + d_{k,7} \pmod{16},\\
0 &\equiv d_{k,2} + d_{k,4} + d_{k,6} \pmod{8},\\
0 &\equiv d_{k,3} + 2d_{k,4} + d_{k,5} - 2d_{k,6} - 3d_{k,7} \pmod{8},\\
0 &\equiv d_{k,4} + d_{k,6} \pmod{2},\\
0 &\equiv d_{k,5} + d_{k,6} \pmod{2},
\end{aligned} \tag{3.37}$$

then there exists a lift $\{X_k^+, Y_k^+\}$ of $\{X_k, Y_k\}$ that is an ideal PTE solution modulo 2^{k+1}.

Proof. Without loss of generality we suppose that x_j and y_j are odd for $j \in \{1, 2, 3, 4\}$. In addition to (3.37), we will justify and make use of three additional congruences modulo 2 that follow from (3.37), namely

$$d_{k,1} \equiv 0 \pmod{2}, \quad d_{k,2} \equiv 0 \pmod{2}, \quad \text{and} \quad d_{k,3}+d_{k,6}+d_{k,7} \equiv 0 \pmod{2}. \tag{3.38}$$

The first of these follows from adding the first three congruences in (3.37), the second from adding the second and fourth congruences in (3.37), and the third from adding the third and fifth congruences in (3.37).

By (3.14) we have

$$\begin{aligned}
d_{k,1}^{+} &\equiv d_{k,1} \pmod 2 \\
d_{k,2}^{+} &\equiv d_{k,2} \pmod 2 \\
d_{k,3}^{+} &\equiv d_{k,3} + \sum_{j=5}^{8} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,4}^{+} &\equiv d_{k,4} + \sum_{j=1}^{4} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,5}^{+} &\equiv d_{k,5} + \sum_{j=1}^{4} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,6}^{+} &\equiv d_{k,6} + \sum_{j=1}^{4} (t_{k,j} + u_{k,j}) \pmod 2 \\
d_{k,7}^{+} &\equiv d_{k,7} + \sum_{j=1}^{8} (t_{k,j} + u_{k,j}) \pmod 2.
\end{aligned} \tag{3.39}$$

Let $t_{k,j}$ and $u_{k,j}$ in $\{0,1\}$ be defined by

$$\begin{aligned}
t_{k,1} &\equiv \frac{d_{k,1}+d_{k,2}+d_{k,3}+d_{k,4}+d_{k,5}+d_{k,6}+d_{k,7}}{16} \pmod 2, & t_{k,2} &= 0, \\
t_{k,7} &\equiv \frac{d_{k,4}+d_{k,6}}{2} + d_{k,6} + d_{k,7} \pmod 2, & t_{k,4} &= 0, \\
u_{k,3} &\equiv t_{k,1} + \frac{d_{k,2}+d_{k,4}+d_{k,6}}{8} \pmod 2, & t_{k,6} &= 0, \\
u_{k,1} &\equiv t_{k,1} + t_{k,7} + \frac{d_{k,5}+d_{k,6}}{2} + d_{k,6} \pmod 2, & t_{k,8} &= 0, \\
t_{k,3} &\equiv t_{k,1} + u_{k,3} + u_{k,1} + d_{k,6} \pmod 2, & u_{k,2} &= 0, \\
u_{k,5} &\equiv t_{k,1} + t_{k,3} + \frac{d_{k,3}+2d_{k,4}+d_{k,5}-2d_{k,6}-3d_{k,7}}{8} \pmod 2, & u_{k,4} &= 0, \\
t_{k,5} &\equiv u_{k,5} + \frac{d_{k,4}+d_{k,6}}{2} \pmod 2, & u_{k,6} &= 0, \\
u_{k,7} &= u_{k,8}, & u_{k,8} &\in \{0,1\}.
\end{aligned} \tag{3.40}$$

Note that such $t_{k,j}$ and $u_{k,j}$ in $\{0,1\}$ exist since (3.37) holds. Substituting (3.40) into (3.39) yields that each $d_{k,j}^{+}$ in (3.39) is 0 (mod 2), where here we make use of the congruences in both (3.37) and (3.38). Thus, (3.9) holds and so by Proposition 3.7, the pair $\{X_k^{+}, Y_k^{+}\}$ is an ideal PTE solution modulo 2^{k+1}. □

Proposition 3.20. *There exist infinitely many sequences* $(\{X_k, Y_k\})_{k=7}^{\infty}$ *with*

$$\{X_7, Y_7\} = \{[83, 19, 33, 1, 42, 10, 64, 0], [15, 7, 13, 101, 14, 22, 28, 52]\}, \tag{3.41}$$

such that for each $k > 7$*, the pair* $\{X_k, Y_k\}$ *is a lift of* $\{X_{k-1}, Y_{k-1}\}$ *that is an ideal PTE solution modulo* 2^k *with* $\nu_2(w_k(0)) = k_8 = 6$.

Proof. Observe that

$$\begin{aligned} w_7(z) &= 256z^6 + 22272z^5 - 4687360z^4 + 213128960z^3 \\ &\quad - 3822272256z^2 + 27546254848z - 61825283520 \\ &\equiv 64 \pmod{2^7}. \end{aligned}$$

So, $\{X_7, Y_7\}$ is an ideal PTE solution modulo 2^7, that is not an integer solution to the PTE problem and that satisfies $\nu_2(w_7(0)) = 6$. Also note that

$$\begin{aligned} d_{k,1} + d_{k,2} + d_{k,3} + d_{k,4} + d_{k,5} + d_{k,6} + d_{k,7} &= -215205116 \\ &\quad - 29861502 - 1665070 - 36620 \\ &\quad - 174 + 2 + 0 \equiv 0 \pmod{16}, \\ d_{k,2} + d_{k,4} + d_{k,6} &= -29861502 - 36620 + 2 \equiv 0 \pmod{8}, \\ d_{k,3} + 2d_{k,4} + d_{k,5} - 2d_{k,6} - 3d_{k,7} &= -1665070 - 73240 \\ &\quad - 174 - 4 - 0 \equiv 0 \pmod{8}, \\ d_{k,4} + d_{k,6} &= -36620 + 2 \equiv 0 \pmod{2}, \\ d_{k,5} + d_{k,6} &= -174 + 2 \equiv 0 \pmod{2}, \end{aligned}$$

so $\{X_7, Y_7\}$ satisfies (3.37) with $k = 7$.

First we prove that we can construct a sequence $(\{X_k, Y_k\})_{k=7}^{\infty}$ of ideal PTE solutions modulo 2^k that are obtained by successively lifting $\{X_7, Y_7\}$. Since $\{X_7, Y_7\}$ satisfies the hypothesis of Lemma 3.19 with $k = 7$, it suffices to show that for an integer $k > 7$, if $\{X_k, Y_k\}$ is an ideal PTE solution modulo 2^k congruent to $\{X_7, Y_7\}$

(mod 128) that satisfies (3.37), then the lift of $\{X_k, Y_k\}$ obtained in the proof of Proposition 3.19 also satisfies (3.37) but with k replaced by $k+1$.

From (3.14) we note that for all $k > 7$ we have

$$d^+_{k,j} \equiv d_{k,j} + \sum_{i=1}^{n} \left(e_{n-1-j}\left(\hat{X}_7^i\right) t_{k,i} - e_{n-1-j}\left(\hat{Y}_7^i\right) u_{k,i} \right) \pmod{2^m},$$

for $j \in \{1, 2, \ldots, 7\}$ and $m \leq 7$. Substituting (3.41) into the above with $m = 5$ yields

$$\begin{aligned}
d^+_{k,1} &\equiv d_{k,1} + 4t_{k,7} + 4t_{k,8} + 16u_{k,5} + 16u_{k,6} - 4u_{k,7} - 4u_{k,8} \pmod{32},\\
d^+_{k,2} &\equiv d_{k,2} + 12t_{k,1} + 12t_{k,2} + 4t_{k,3} + 4t_{k,4} - 6t_{k,5}\\
&\quad - 6t_{k,6} - 12t_{k,7} - 12t_{k,8} + 4u_{k,1} + 4u_{k,2} + 12u_{k,3}\\
&\quad + 12u_{k,4} + 10u_{k,5} - 14u_{k,6} + 8u_{k,7} \pmod{32},\\
d^+_{k,3} &\equiv d_{k,3} - 8t_{k,1} - 8t_{k,2} + 16t_{k,3} + 16t_{k,4} - 7t_{k,5} - 7t_{k,6} + t_{k,7} + t_{k,8}\\
&\quad - 8u_{k,1} - 8u_{k,2} + 7u_{k,5} + 7u_{k,6} - u_{k,7} - u_{k,8} \pmod{32},\\
d^+_{k,4} &\equiv d_{k,4} - 13t_{k,1} - 13t_{k,2} - 15t_{k,3} - 15t_{k,4} - 12t_{k,5}\\
&\quad - 12t_{k,6} + 16t_{k,7} + 16t_{k,8} + 9u_{k,1} + u_{k,2} - 5u_{k,3}\\
&\quad - 13u_{k,4} + 4u_{k,5} - 12u_{k,6} + 8u_{k,7} - 8u_{k,8} \pmod{32},\\
d^+_{k,5} &\equiv d_{k,5} + 15t_{k,1} + 15t_{k,2} - t_{k,3} - t_{k,4} + 6t_{k,5}\\
&\quad + 6t_{k,6} - 6t_{k,7} - 6t_{k,8} + 9u_{k,1} - 7u_{k,2} + 9u_{k,3}\\
&\quad - 7u_{k,4} + 10u_{k,5} + 10u_{k,6} + 6u_{k,7} + 6u_{k,8} \pmod{32},\\
d^+_{k,6} &\equiv d_{k,6} + 9t_{k,1} + 9t_{k,2} - 5t_{k,3} - 5t_{k,4} - 14t_{k,5}\\
&\quad - 14t_{k,6} - 4t_{k,7} - 4t_{k,8} - 13u_{k,1} + 11u_{k,2} - 15u_{k,3}\\
&\quad + 9u_{k,4} - 14u_{k,5} - 6u_{k,6} - 8u_{k,8} \pmod{32},\\
d^+_{k,7} &\equiv d_{k,7} + t_{k,1} + t_{k,2} + t_{k,3} + t_{k,4} + t_{k,5} + t_{k,6} + t_{k,7} + t_{k,8}\\
&\quad - u_{k,1} - u_{k,2} - u_{k,3} - u_{k,4} - u_{k,5} - u_{k,6} - u_{k,7} - u_{k,8} \pmod{32}.
\end{aligned} \tag{3.42}$$

Recall from (3.40) that we have

$$t_{k,2} = 0, \quad t_{k,4} = 0, \quad t_{k,6} = 0, \quad t_{k,8} = 0 \quad u_{k,2} = 0 \quad u_{k,4} = 0 \quad \text{and} \quad u_{k,6} = 0.$$

Substituting the above into (3.42) yields

$$\begin{aligned}
d^+_{k,1} &\equiv d_{k,1} + 4t_{k,7} + 16u_{k,5} - 4u_{k,7} - 4u_{k,8} \pmod{32},\\
d^+_{k,2} &\equiv d_{k,2} + 12t_{k,1} + 4t_{k,3} - 6t_{k,5}\\
&\qquad - 12t_{k,7} + 4u_{k,1} + 12u_{k,3} + 10u_{k,5} + 8u_{k,7} \pmod{32},\\
d^+_{k,3} &\equiv d_{k,3} - 8t_{k,1} + 16t_{k,3} - 7t_{k,5}\\
&\qquad + t_{k,7} - 8u_{k,1} + 7u_{k,5} - u_{k,7} - u_{k,8} \pmod{32},\\
d^+_{k,4} &\equiv d_{k,4} - 13t_{k,1} - 15t_{k,3} - 12t_{k,5}\\
&\qquad + 16t_{k,7} + 9u_{k,1} - 5u_{k,3} + 4u_{k,5} + 8u_{k,7} - 8u_{k,8} \pmod{32},\\
d^+_{k,5} &\equiv d_{k,5} + 15t_{k,1} - t_{k,3} + 6t_{k,5}\\
&\qquad - 6t_{k,7} + 9u_{k,1} + 9u_{k,3} + 10u_{k,5} + 6u_{k,7} + 6u_{k,8} \pmod{32},\\
d^+_{k,6} &\equiv d_{k,6} + 9t_{k,1} - 5t_{k,3} - 14t_{k,5}\\
&\qquad - 4t_{k,7} - 13u_{k,1} - 15u_{k,3} - 14u_{k,5} - 8u_{k,8} \pmod{32},\\
d^+_{k,7} &\equiv d_{k,7} + t_{k,1} + t_{k,3} + t_{k,5}\\
&\qquad + t_{k,7} - u_{k,1} - u_{k,3} - u_{k,5} - u_{k,7} - u_{k,8} \pmod{32}.
\end{aligned}$$

From the above we deduce that

$$\begin{aligned}
d^+_{k,1} + d^+_{k,2} + d^+_{k,3} + d^+_{k,4} + d^+_{k,5} + d^+_{k,6} + d^+_{k,7} &\equiv d_{k,1} + d_{k,2} + d_{k,3} + d_{k,4}\\
&\qquad + d_{k,5} + d_{k,6} + d_{k,7} + 16t_{k,1}\\
&\qquad + 16u_{k,7} + 16u_{k,8} \pmod{32},\\
d^+_{k,2} + d^+_{k,4} + d^+_{k,6} &\equiv d_{k,2} + d_{k,4} + d_{k,6}\\
&\qquad + 8t_{k,1} + 8u_{k,3} \pmod{16},\\
d^+_{k,3} + 2d^+_{k,4} + d^+_{k,5} - 2d^+_{k,6} - 3d^+_{k,7} &\equiv d_{k,3} + 2d_{k,4} + d_{k,5} - 2d_{k,6} - 3d_{k,7}\\
&\qquad + 8t_{k,1} + 8t_{k,3} + 8u_{k,5}\\
&\qquad + 8u_{k,7} + 8u_{k,8} \pmod{16},\\
d^+_{k,4} + d^+_{k,6} &\equiv d_{k,4} + d_{k,6} + 2t_{k,5} + 2u_{k,5} \pmod{4},
\end{aligned}$$

$$d^+_{k,5} + d^+_{k,6} \equiv d_{k,5} + d_{k,6} + 2t_{k,3} + 2t_{k,7} + 2u_{k,3} + 2u_{k,7} + 2u_{k,8} \pmod 4.$$

Substituting the assignment (3.40) into the above yields

$$\begin{aligned}
d^+_{k,1} + d^+_{k,2} + d^+_{k,3} + d^+_{k,4} + d^+_{k,5} + d^+_{k,6} + d^+_{k,7} &\equiv 2d_{k,1} + 2d_{k,2} + 2d_{k,3} + 2d_{k,4} \\
&\quad + 2d_{k,5} + 2d_{k,6} + 2d_{k,7} \pmod{32}, \\
d^+_{k,2} + d^+_{k,4} + d^+_{k,6} &\equiv 2\left(d_{k,2} + d_{k,4} + d_{k,6}\right) \pmod{16}, \\
d^+_{k,3} + 2d^+_{k,4} + d^+_{k,5} - 2d^+_{k,6} - 3d^+_{k,7} &\equiv 2d_{k,3} + 4d_{k,4} + 2d_{k,5} \\
&\quad - 4d_{k,6} - 6d_{k,7} \pmod{16}, \\
d^+_{k,4} + d^+_{k,6} &\equiv 2\left(d_{k,4} + d_{k,6}\right) \pmod 4, \\
d^+_{k,5} + d^+_{k,6} &\equiv 2\left(d_{k,5} + d_{k,6}\right) \pmod 4.
\end{aligned}$$

Since $\{X_k, Y_k\}$ satisfies (3.37), we have

$$\begin{aligned}
d^+_{k,1} + d^+_{k,2} + d^+_{k,3} + d^+_{k,4} + d^+_{k,5} + d^+_{k,6} + d^+_{k,7} &\equiv 0 \pmod{32}, \\
d^+_{k,2} + d^+_{k,4} + d^+_{k,6} &\equiv 0 \pmod{16}, \\
d^+_{k,3} + 2d^+_{k,4} + d^+_{k,5} - 2d^+_{k,6} - 3d^+_{k,7} &\equiv 0 \pmod{16}, \\
d^+_{k,4} + d^+_{k,6} &\equiv 0 \pmod 4, \\
d^+_{k,5} + d^+_{k,6} &\equiv 0 \pmod 4.
\end{aligned}$$

and so by Lemma 3.8, we see that $\{X_{k+1}, Y_{k+1}\}$ satisfies (3.37) with k replaced by $k+1$.

So, we can construct a sequence $(\{X_k, Y_k\})_{k=7}^{\infty}$ such that for each $k > 7$, the pair $\{X_k, Y_k\}$ is a lift of $\{X_{k-1}, Y_{k-1}\}$ that is an ideal PTE solution modulo 2^k, by lifting $\{X_7, Y_7\}$ successively with the assignments (3.40). By Corollary 3.6 it follows that $\nu_2\left(w_k(0)\right) = 6$ for all $k \geq 7$. To see that there are infinitely many such sequences, observe that in (3.40) we allow for $u_{k,8}$ to be either 0 or 1. Thus, we can construct a

sequence $(\{X_k, Y_k\})_{k=7}^{\infty}$ corresponding to any sequence of 0's and 1's for the values of $u_{k,8}$. □

3.3 2-adic Integer Solutions

We now prove Theorem 1.5.

Theorem 1.5. *For $3 \leq n \leq 8$ there exist lists of 2-adic integers $X = [x_1, x_2, \ldots x_n]$ and $Y = [y_1, y_2, \ldots y_n]$, such that at least one x_j or y_j is not in $\mathbb{Q}$, that satisfy*

$$\prod_{j=1}^{n} (z - x_j) - \prod_{j=1}^{n} (z - y_j) = C_n,$$

for some 2-adic integer C_n with $\nu_2(C_n) = k_n$, where

$$k_n = \begin{cases} 2 & \text{if } n = 3, 4, \\ 4 & \text{if } n = 5, \\ 5 & \text{if } n = 6, \\ 6 & \text{if } n = 7, 8. \end{cases}$$

Proof. Fix n and let $\{X_{k_n+1}, Y_{k_n+1}\}$ be the corresponding pair from the list below.

$$\{[1, 4, 0], [5, 6, 2]\},$$

$$\{[1, 1, 0, 0], [7, 3, 6, 2]\},$$

$$\{[1, 4, 8, 16, 0], [17, 14, 10, 18, 2]\},$$

$$\{[3, 1, 1, 2, 8, 0], [59, 29, 45, 42, 12, 20]\},$$

$$\{[3, 5, 1, 10, 2, 0, 0], [115, 29, 121, 38, 38, 28, 36]\},$$

$$\{[83, 19, 33, 1, 42, 10, 64, 0], [15, 7, 13, 101, 14, 22, 28, 52]\}.$$

In the previous section we established that, from each of the above ideal PTE solutions modulo 2^{k_n+1}, we can construct a sequence $(\{X_k, Y_k\})_{k=k_n+1}^{\infty}$ such that for each $k > k_n+1$, the pair $\{X_k, Y_k\}$ is a lift of $\{X_{k-1}, Y_{k-1}\}$ that is an ideal PTE solution modulo 2^k.

For $1 \leq j \leq n$ and $k \geq k_n + 1$, we let $x_{k,j}$ and $y_{k,j}$ denote the j^{th} entry of X_k and Y_k, respectively, and let $t_{k,j}$ and $u_{k,j}$ denote the corresponding t_j and u_j when lifting from $\{X_k, Y_k\}$ to $\{X_{k+1}, Y_{k+1}\}$. For $0 \leq k < k_n + 1$, let $t_{k,j}, u_{k,j} \in \{0, 1\}$ be such that

$$x_{k_n+1,j} = \sum_{k=0}^{k_n} t_{k,j} 2^k \quad \text{and} \quad y_{k_n+1,j} = \sum_{k=0}^{k_n} u_{k,j} 2^k.$$

For $1 \leq j \leq n$, define the formal power series

$$x_j = \sum_{k=0}^{\infty} t_{k,j} 2^k \quad \text{and} \quad y_j = \sum_{k=0}^{\infty} u_{k,j} 2^k.$$

For $3 \leq n \leq 8$, the sequence $(\{X_k, Y_k\})_{k=k_n+1}^{\infty}$ can be constructed by successively using the assignments given in (3.18), (3.21), (3.25), (3.29), (3.34) and (3.40), respectively. In each of these assignments we have $u_{k,n-1} = u_{k,n}$, and we have a free choice of whether we want them both to equal 0 or both to equal 1. If we choose $u_{k,n}$ to be equal to 1 infinitely often with no repeating pattern then we ensure that y_n, and y_{n-1}, are 2-adic integers that are not rational integers (or rational numbers).

Recall that the field of 2-adic numbers, $\mathbb{Q}_2$, is a metric space with respect to the metric $d(p, q) = 2^{-\nu_2(p-q)}$, for $p, q \in \mathbb{Q}_2$. From (3.8) we see that $w_{k+m}(0) - w_k(0) \equiv 0 \pmod{2^k}$ for each $k \geq k_n + 1$ and $m \geq 1$. Thus, the sequence $(w_k(0))_{i=k_n+1}^{\infty}$ is Cauchy in $\mathbb{Q}_2$, and so, since $\mathbb{Q}_2$ is complete, $(w_k(0))_{i=k_n+1}^{\infty}$ is convergent in $\mathbb{Q}_2$. Define

$$C_n = \lim_{k \to \infty} w_k(0) \in \mathbb{Q}_2.$$

Then the x_j and y_j are 2-adic integers satisfying

$$\prod_{j=1}^{n} (z - x_j) - \prod_{j=1}^{n} (z - y_j) = C_n.$$

By construction, our choice of $\{X_{k_n+1}, Y_{k_n+1}\}$ gives

$$w_{k_n+m}(0) \equiv w_{k_n+1}(0) \equiv 2^{k_n} \pmod{2^{k_n+1}},$$

which implies $\nu_2(C_n) = k_n$. This completes the proof. □

Chapter 4

Irreducibility Criteria for Non-negative Integer Coefficient Polynomials

Recall Theorem 1.6.

Theorem 1.6. *Let $b \in \mathbb{Z}$ with $b > 2$. Let $f(x)$ be a polynomial with non-negative integer coefficients and $f(b)$ prime. For $n \in \mathbb{Z}^+$, let $\Phi_n(x)$ be the n^{th} cyclotomic polynomial and $\zeta_n = e^{2\pi i/n}$. Define*

$$\mathcal{B}_b^{(n)} = \max_{i\in\{0,1\}} \left(\sum_{k=0}^{\left\lfloor \frac{D_n - i}{2} \right\rfloor} \binom{D_n - i}{2k+1} (b + \operatorname{Re}(\zeta_n))^{D_n - 2k - 1 - i} (-\operatorname{Im}(\zeta_n))^k \right) \Phi_n(1-b), \quad (4.1)$$

with $D_n = \lfloor \pi / \arg(b + \zeta_n) \rfloor$, and let

$$M_1(b) = \min_{n\in\{3,4\}} \mathcal{B}_b^{(n)}, \quad M_2(b) = \max_{n\in\{3,4\}} \mathcal{B}_b^{(n)}, \quad M_3(b) = \mathcal{B}_b^{(6)}$$

and

$$M_4(b) = \frac{(b - 1.5221)^\kappa (b - 2.5221)}{1 + \cot(\pi/b^2)}, \quad \text{with} \quad \kappa = \left\lfloor \frac{(b^2-1)\pi}{b^2 \arctan\left(\frac{0.8444}{(b-0.2)}\right)} \right\rfloor.$$

Then

- *If $b > 2$ and each coefficient of $f(x)$ is less than $M_1(b)$, then $f(x)$ is irreducible.*
- *If $b > 2$ and each coefficient of $f(x)$ is less than $M_2(b)$ and $f(x)$ is reducible, then it is divisible by $\Phi_3(x-b)$ if $b \leq 5$ and divisible by $\Phi_4(x-b)$ if $b > 5$.*
- *If $b > 69$ and each coefficient of $f(x)$ is less than $M_3(b)$ and $f(x)$ is reducible, then it is divisible by at least one of $\Phi_3(x-b)$ or $\Phi_4(x-b)$.*

- *If $b > 69$ and each coefficient of $f(x)$ is less than $M_4(b)$ and $f(x)$ is reducible, then it is divisible by $\Phi_3(x-b)$, $\Phi_4(x-b)$ or $\Phi_6(x-b)$.*

The focus of this chapter is to give the details on how to find the bounds $M_1(b)$, $M_2(b)$ and $M_3(b)$. The bound $M_4(b)$ is found in J. Juillerat's dissertation [26]. To start, in Section 4.1 we explain why the polynomials $\Phi_n(b)$ for $n \in \{3, 4, 6\}$ play such an important role, which in turn gives the motivation for finding the bounds $M_1(b)$, $M_2(b)$ and $M_3(b)$.

4.1 A Root Bounding Function

The following lemma can be found in [16, Lemma 1].

Lemma 4.1. *Fix an integer $b \geq 2$. Let $f(x)$ be a polynomial with non-negative integer coefficients such that $f(b)$ is prime. If $f(x)$ is reducible, then $f(x)$ has a non-real root in the disc $\mathfrak{D}_b = \{z \in \mathbb{C} : |b - z| \leq 1\}$.*

A motivating idea for this section is to replace the disc $\mathfrak{D}_b$ in Lemma 4.1 with a different region such that if $\alpha = re^{i\theta}$ is in this region, then $|\theta|$ is bounded above by a small number.

For a given integer $b \geq 6$, to establish the bounds $M_1(b)$, $M_2(b)$ and $M_3(b)$ in Theorem 1.6 we utilise three main methods. First, we introduce certain rational functions that will give us information about the location of possible roots of $f(x)$ assuming $f(x)$ is reducible. While better rational functions can be chosen, as in [10], we will make choices to simplify the results in later sections. Second, we will obtain four upper bounds for the coefficients of $f(x)$ such that if a bound is satisfied, then $f(x)$ cannot have a root at a certain location. Third, we will determine the minimum $M(b)$ of these four bounds; hence, if the coefficients of $f(x)$ are bounded above by $M(b)$, then $f(x)$ cannot have roots at the locations required for $f(x)$ to be reducible. In the remainder of this section, we focus on the first of these ideas.

Recall that $\Phi_n(x)$ denotes the nth cyclotomic polynomial, and let $\zeta_n = e^{2\pi i/n}$. As usual, for $z \in \mathbb{C}$, the notation $\overline{z}$ will refer to the complex conjugate of z. Thus, $\overline{\zeta_n} = e^{-2\pi i/n}$. Fix an integer $b \geq 2$, and let $f(x)$ be a non-constant polynomial with non-negative integer coefficients such that $f(b)$ is prime. Suppose $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, $g(x)$ and $h(x)$ have positive leading coefficients, and $g(x)$ and $h(x)$ are not identically ± 1. Since $f(b)$ is prime, we may take, without loss of generality, $g(b) = \pm 1$ and $h(b) = \pm f(b)$. Using the ideas of [17], we want to show that either $g(x)$ has a root in common with one of

$$\Phi_3(x-b) = x^2 - (2b-1)x + b^2 - b + 1,$$
$$\Phi_4(x-b) = x^2 - 2bx + b^2 + 1,$$
$$\Phi_6(x-b) = x^2 - (2b+1)x + b^2 + b + 1,$$

or $g(x)$ has a root in a certain region $\mathcal{R}_b$ to be defined shortly.

We define

$$\mathcal{F}_b(z) = \frac{\mathcal{N}_b(z)}{\mathcal{D}_b(z)},$$

where

$$\mathcal{N}_b(z) = |b-1-z|^{2e_2}(|b+\zeta_3-z||b+\overline{\zeta_3}-z|)^{2e_3}$$
$$\cdot (|b+i-z||b-i-z|)^{2e_4}(|b+\zeta_6-z||b+\overline{\zeta_6}-z|)^{2e_6},$$
$$\mathcal{D}_b(z) = |b-z|^{4(e_3+e_4+e_6)+2(e_2+d+1)},$$

and e_2, e_3, e_4, e_6, and d are all non-negative integers that could depend on b. Although we want some flexibility on the choices for e_2, e_3, e_4, e_6, and d for a given b, for clarity, we indicate in Table 4.1 the choices for these variables we use to establish Theorem 1.6. Note that the values for $b \leq 20$ are the same as the values chosen in [10]. The values we chose for $b \geq 21$ are not sufficient to obtain results that include $b \leq 20$. Thus, we will refer to [10] to make a statement about all $b \geq 2$. Our choices for $b \geq 21$ were based on trial and error to give us our desired results.

Table 4.1 Numbers used in $\mathcal{F}_b(z)$ for b

b	2	3	4	5	$6 \leq b \leq 20$	$b \geq 21$
$e_2(b)$	20	0	0	0	0	0
$e_3(b)$	4	15	9	6	4	1
$e_4(b)$	0	2	2	2	2	1
$e_6(b)$	0	0	3	3	3	1
$d(b)$	0	3	3	3	3	1

Setting $z = x + iy$, direct computations show that the following expressions in $\mathcal{N}_b$ and $\mathcal{D}_b$ simplify as shown:

$$|b - 1 - z|^2 = y^2 + (x - b)^2 + 2(x - b) + 1,$$

$$\begin{aligned}(|b + \zeta_3 - z||b + \overline{\zeta_3} - z|)^2 &= y^4 + (2(x - b)^2 + 2(x - b) - 1)y^2 \\ &\quad + \Big((x - b)^2 + (x - b) + 1\Big)^2,\end{aligned}$$

$$(|b + i - z||b - i - z|)^2 = y^4 + (2(x - b)^2 - 2)y^2 + ((x - b)^2 + 1)^2,$$

$$\begin{aligned}(|b + \zeta_6 - z||b + \overline{\zeta_6} - z|)^2 &= y^4 + (2(x - b)^2 - 2(x - b) - 1)y^2 \\ &\quad + ((x - b)^2 - (x - b) + 1)^2,\end{aligned}$$

and

$$|b - z|^2 = y^2 + (x - b)^2.$$

Notice that each one of these expressions is in $\mathbb{Z}[b, x, y^2]$. Thus, $\mathcal{N}_b(z)$ and $\mathcal{D}_b(z)$ are in $\mathbb{Z}[b, x, y^2]$, making $\mathcal{F}_b(z)$ a rational function in b, x and y^2. Moreover, we observe that for each integer $b \geq 3$, the polynomial

$$\mathcal{P}_b(x, y) = \mathcal{D}_b(x + iy) - \mathcal{N}_b(x + iy)$$

can be written as

$$\mathcal{P}_b(x, y) = \sum_{j=0}^{r} a_j(b, x)y^{2j}$$

where $r = 2(e_3 + e_4 + e_6) + e_2 + d + 1$ and each $a_j(b, x)$ is in $\mathbb{Z}[b, x]$. We write the factor $g(x)$ of $f(x)$ in the form

$$g(x) = c \prod_{j=1}^{m} (x - \beta_j),$$

where c is the leading coefficient of $g(x)$ and $\beta_1, \ldots, \beta_m$ are the roots of $g(x)$ and, therefore, roots of $f(x)$. One can check that

$$\frac{|g(b-1)|^{2e_2}|g(b+\zeta_3)g(b+\overline{\zeta_3})|^{2e_3}|g(b+i)g(b-i)|^{2e_4}|g(b+\zeta_6)g(b+\overline{\zeta_6})|^{2e_6}}{|g(b)|^{4(e_3+e_4+e_6)+2(e_2+d+1)}}$$

and

$$\frac{1}{c^{2(d+1)}} \prod_{j=1}^{m} \mathcal{F}_b(\beta_j)$$

are equal. We denote this common value by $V = V_b(g)$.

Since each of $g(b+\zeta_3)g(b+\overline{\zeta_3})$, $g(b+i)g(b-i)$ and $g(b+\zeta_6)g(b+\overline{\zeta_6})$ is a symmetric polynomial in the roots of an irreducible monic quadratic in $\mathbb{Z}[x]$, we conclude that each of these expressions are themselves integers. Also, $g(b-1)$ is an integer and, by assumption, $g(b) = \pm 1$. Thus, by looking at the first expression for V, either $V = 0$ or $V \in \mathbb{Z}^+$.

We can say more about when $V = 0$. Since $f(x)$ has non-negative integer coefficients, it cannot have a positive real root, and neither can its factor $g(x)$. Therefore, $g(b-1) \neq 0$. Either expression for V now implies that $V = 0$ if and only if $g(b+\zeta_3)g(b+\overline{\zeta_3})$, $g(b+i)g(b-i)$, or $g(b+\zeta_6)g(b+\overline{\zeta_6})$ is zero, which happens precisely when $g(x)$ is divisible by at least one of $\Phi_3(x-b)$, $\Phi_4(x-b)$ and $\Phi_6(x-b)$. If one of these is not a factor of $g(x)$, we have $V \in \mathbb{Z}^+$. Observe that $\mathcal{F}_b(z)$ is a non-negative real number for all $z \in \mathbb{C}$ with $z \neq b$. By looking at the product in the second expression for V, we see that if $V \neq 0$, then $\mathcal{F}_b(\beta_j) \geq 1$ for at least one value of $j \in \{1, \ldots, m\}$. Said differently, if $V \neq 0$, then there is a root β_j of $g(x)$, and thus of $f(x)$, that lies in

$$\mathcal{R}_b = \{z \in \mathbb{C} : \mathcal{F}_b(z) \geq 1\}.$$

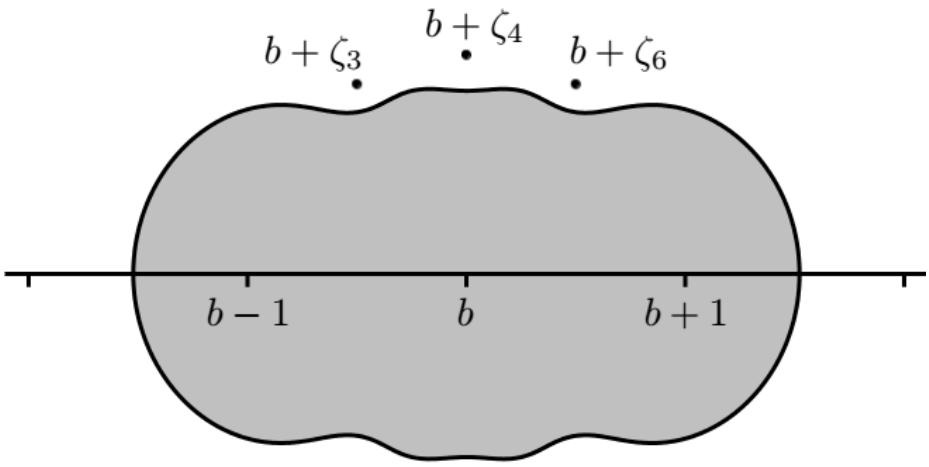

Figure 4.1 The region $\mathcal{R}_b$ for $b \geq 21$, along with the location of $b+\zeta_n$ for $n \in \{3,4,6\}$.

We have, then, four locations where roots of $g(x)$ may lie. Our next step is to find four bounds, $\mathcal{B}_b^{(3)}$, $\mathcal{B}_b^{(4)}$, $\mathcal{B}_b^{(6)}$ and $\mathcal{B}_b$ such that if $g(x)$ shares a root in common with $\Phi_n(x-b)$, for $n \in \{3,4,6\}$, or the region $\mathcal{R}_b$, then it has a coefficient at least as large as $\mathcal{B}_b^{(n)}$, for $n \in \{3,4,6\}$, or $\mathcal{B}_b$, respectively. Comparing these four bounds will allow us to find the four bounds as stated in Theorem 1.6. In the next two sections we present the details of finding the bounds $\mathcal{B}_b^{(n)}$ for $n \in \{3,4,6\}$. J. Juillerat gives the details for finding the bound $\mathcal{B}_b$ in their dissertation [26], which is

$$\mathcal{B}_b = \frac{(b-1.5221)^{\kappa}(b-2.5221)}{1+\cot(\pi/b^2)} \quad \text{with} \quad \kappa = \kappa(b) = \left\lfloor \frac{(b^2-1)\pi}{b^2 \arctan\left(\frac{0.8444}{(b-0.2)}\right)} \right\rfloor. \quad (4.2)$$

4.2 Bounds Based on Recurrence Relations

In this section we will establish results that will help us find bounds $\mathcal{B}_b^{(n)}$ for $n \in \{3,4,6\}$ such that if $f(x)$ is divisible by $\Phi_n(x-b)$, then $f(x)$ must have a coefficient $\geq \mathcal{B}_b^{(n)}$. We take $b \geq 5$.

Much of this section is based on the work done in [10] and [17]. We give enough background from these to describe our work for general b.

Fix positive integers A and B and integers b_j such that

$$f(x) = h(x)g(x) = (b_0x^s + b_1x^{s-1} + \cdots + b_{s-1}x + b_s)(x^2 - Ax + B) \tag{4.3}$$

is a polynomial of degree $n = s+2$ with non-negative integer coefficients. We restrict ourselves to the case where

$$x^2 - Ax + B = \Phi_n(x - b), \quad \text{with } n \in \{3, 4, 6\}$$

so that

$$(A, B) \in \{(2b-1, b^2-b+1), (2b, b^2+1), (2b+1, b^2+b+1)\}.$$

Recalling $b \geq 5$, for these values of (A, B), the following inequalities can be directly verified and will be used later:

$$\begin{aligned} \sqrt{B} - 2 &> 0 & A^2 - 3B &> 0 \\ 1 - A + B &> 1 & 1 - A &< 0 \\ 2B - A &> 0 & -B^2 + A^2 - B &< 0 \\ 4B - A^2 &> 0 & A^3 - AB - B^2 &< -1 \quad (\text{if } b \geq 7). \\ 3 - 3A + 2B &> 0 \end{aligned} \tag{4.4}$$

Define $b_j = 0$ for all $j < 0$ and all $j > s$. Since the coefficients of $f(x)$ are all non-negative, we deduce that $b_0 \geq 1$ and $b_j \geq Ab_{j-1} - Bb_{j-2}$ for all $j \in \mathbb{Z}$. Define

$$\beta_j = \begin{cases} 0 & \text{if } j < 0, \\ 1 & \text{if } j = 0, \\ A\beta_{j-1} - B\beta_{j-2} & \text{if } j \geq 1, \end{cases} \tag{4.5}$$

so that the β_j satisfy a recurrence relation for $j \geq -1$. In particular, $\beta_1 = A$ and $\beta_2 = A^2 - B$. Also, with our restriction on our choice of $x^2 - Ax + B$ above, we have

$$\beta_1 \in \{2b-1, 2b, 2b+1\},$$

so the sequence $\beta_0, \beta_1, \ldots$ is initially increasing. We obtain a closed form for the solution to this recurrence relation. The recurrence relation has characteristic polynomial $x^2 - Ax + B$, which has roots $b + \zeta_n$ and $b + \overline{\zeta_n}$ for some $n \in \{3, 4, 6\}$. So β_j has the closed form

$$\beta_j = c_1(b + \zeta_n)^j + c_2(b + \overline{\zeta_n})^j,$$

for some constants c_1 and c_2 depending on A and B. Taking $j = 0$, we obtain $c_2 = 1 - c_1$; and taking $j = -1$, we see that $c_1 = (b + \zeta_n) \,/\, \left(\zeta_n - \overline{\zeta_n}\right)$. Substituting these values for c_1 and c_2 and reducing, we deduce

$$\begin{aligned} \beta_j &= \frac{1}{\zeta_n - \overline{\zeta_n}} \left[(b + \zeta_n)^{j+1} - (b + \overline{\zeta_n})^{j+1}\right] \\ &= \frac{|b + \zeta_n|^{j+1} e^{i(j+1)\arg(b+\zeta_n)} - |b + \overline{\zeta_n}|^{j+1} e^{-i(j+1)\arg(b+\zeta_n)}}{\zeta_n - \overline{\zeta_n}} \\ &= \frac{|b + \zeta_n|^{j+1}}{\sin(2\pi/n)} \sin\left((j+1)\arg(b + \zeta_n)\right). \end{aligned} \tag{4.6}$$

We note that B is the constant term of the minimal polynomial for $b + \zeta_n$, so

$$B = |b + \zeta_n|^2. \tag{4.7}$$

For ease of notation, we set

$$\theta = \theta_n = \arg(b + \zeta_n) \in (0, \pi/2) \quad \text{and} \quad D = D_n = \lfloor \pi/\theta_n \rfloor \tag{4.8}$$

where θ and D depend on both b and n. We now take a moment to obtain some useful inequalities involving θ and D that will be used later.

Lemma 4.2. *Let $b \in \mathbb{Z}$ with $b \geq 3$, and let $n \in \{3, 4, 6\}$. Then $\pi/\theta_n \notin \mathbb{Z}$.*

Proof. Letting $r = \arg(b + \zeta_n)/\pi$, it suffices to show $r \notin \mathbb{Q}$. Observe that for $n \in \{3, 4, 6\}$ we have

$$\arg(b + \zeta_n) = \arctan(x) \quad \text{where} \quad x \in \left\{\frac{\sqrt{3}}{2b - 1}, \frac{1}{b}, \frac{\sqrt{3}}{2b + 1}\right\}.$$

In each case, we have $\sin^2(\arctan(x)) = x^2/(x^2+1) \in \mathbb{Q}$, and hence

$$\cos(2\pi r) = 1 - 2\sin^2(\pi r) = 1 - 2\sin^2(\arg(b+\zeta_n)) \in \mathbb{Q}.$$

By Corollary 3.12 in [33], we deduce that if $r \in \mathbb{Q}$ and $\cos(2\pi r) \in \mathbb{Q}$, then $\cos(2\pi r)$ is an element of $\{0, \pm 1/2, \pm 1\}$. One checks that $0 < \arg(3+\zeta_n) < \pi/6$ for each $n \in \{3,4,6\}$. Since, for fixed $n \in \{3,4,6\}$, the value of $\pi r = \arg(b+\zeta_n)$ decreases to 0 as b increases, we see that $1/2 < 1 - 2\sin^2(\pi r) < 1$. Thus, $\cos(2\pi r) \notin \{0, \pm 1/2, \pm 1\}$, and the lemma follows. □

From Lemma 4.2, we obtain

$$D_n = \left\lfloor \frac{\pi}{\theta_n} \right\rfloor < \frac{\pi}{\theta_n} = \frac{\pi}{\arg(b+\zeta_n)} \quad \text{for } b \geq 3 \text{ and } n \in \{3,4,6\}. \tag{4.9}$$

For $n \in \{1,2\}$ and for $n \geq 4$, the inequality

$$\arg(b+\zeta_n) \leq \arg(b+\zeta_4) \tag{4.10}$$

is easily verified for all $b \geq 4$. For $n = 3$, we show that (4.10) also holds for $b \geq 4$. Observe that

$$\arg(b+\zeta_3) = \arctan\left(\frac{\sqrt{3}}{2b-1}\right) \qquad \text{and} \qquad \arg(b+\zeta_4) = \arctan\left(\frac{1}{b}\right).$$

We deduce that, for $n = 3$ and $b \geq 4$, it suffices to show

$$\frac{\sqrt{3}}{2b-1} \leq \frac{1}{b}.$$

The latter inequality holds for $b \geq 3.74$. Thus, (4.10) holds for all $b \geq 4$ and $n \geq 1$.

From (4.10), for $b \geq 4$ and all $n \in \mathbb{N}$, we deduce that

$$\arg(b+\zeta_n) \leq \arg(b+\zeta_4) = \frac{\pi}{\pi/\arg(b+\zeta_4)} < \frac{\pi}{\lfloor \pi/\arg(b+\zeta_4) \rfloor} = \frac{\pi}{D_4}, \tag{4.11}$$

where the strict inequality follows from (4.9).

From (4.6) and (4.7), we obtain

$$\beta_j = \frac{\sqrt{B}^{j+1}}{\sin(2\pi/n)} \sin((j+1)\theta). \tag{4.12}$$

By taking $j = 0$ in (4.6), with (4.5), we see that

$$\sin(\theta) = \frac{\sin(2\pi/n)}{\sqrt{B}}. \tag{4.13}$$

From (4.12), we deduce $\beta_j > 0$ provided $\sin((j+1)\theta) > 0$. Thus, $\beta_j > 0$ if $0 < (j+1)\theta < \pi$ or, equivalently, if $0 \leq j \leq D-1$. On the other hand, we have

$$\pi < (\lfloor \pi/\theta \rfloor + 1)\theta < 2\pi$$

so that (4.12) implies $\beta_D < 0$.

We claim that $\beta_{j-1} < \beta_j$ for $1 \leq j \leq D-2$. Given (4.12), we can view β_j as a differentiable function of j. Differentiating β_j with respect to j, we obtain

$$\frac{d\beta_j}{dj} = \frac{\sqrt{B}^{j+1}}{\sin(2\pi/n)} \left[\sin((j+1)\theta) \log\sqrt{B} + \theta \cos((j+1)\theta) \right].$$

Setting this last expression equal to 0 to find critical values, we have

$$\log\sqrt{B} \sin((j+1)\theta) + \theta \cos((j+1)\theta) = 0,$$

which implies

$$\tan((j+1)\theta) = -\frac{\theta}{\log\sqrt{B}} = -\frac{2\theta}{\log B}.$$

Solving for $j+1$, we find the solutions

$$j + 1 = \frac{m\pi - \arctan(2\theta/\log B)}{\theta}$$

where $m \in \mathbb{Z}$. The smallest positive solution for $j+1$ occurs when $m = 1$. Since $b \geq 5$, we have $\log B \geq \log 21 > 3$. Also, $\arctan(x) < x$ for all $x > 0$. Thus, the smallest positive solution for $j+1$ is

$$\frac{\pi}{\theta} - \frac{\arctan(2\theta/\log B)}{\theta} > \frac{\pi}{\theta} - \frac{\arctan(\theta)}{\theta} > \frac{\pi}{\theta} - 1 \geq \left\lfloor \frac{\pi}{\theta} \right\rfloor - 1 = D - 1.$$

Thus, the least positive critical point occurs for some $j > D-2$. Since the sequence $\beta_0, \beta_1, \ldots$ is initially increasing, we see that the derivative is positive for $j \leq D-2$.

We show next that

$$\beta_{D-1} \neq \beta_{D-2}.$$

Assume otherwise. Then (4.12) gives

$$\sqrt{B}\sin(D\theta) = \sin((D-1)\theta) = \sin(D\theta)\cos(\theta) - \cos(D\theta)\sin(\theta).$$

From (4.9), we have $D\theta < \pi$. Also,

$$(D+1)\theta = (\lfloor \pi/\theta + 1 \rfloor)\theta > \pi \quad \text{and} \quad 0 < \theta < \pi/2,$$

so

$$D\theta > \pi - \theta > \pi/2.$$

Thus, we obtain $\sin(D\theta) > \sin(\pi - \theta) = \sin(\theta)$. Hence,

$$\begin{aligned} 0 &= \sin(D\theta)(\sqrt{B} - \cos(\theta)) + \cos(D\theta)\sin(\theta) \\ &> \sin(\theta)(\sqrt{B} - 1) - \sin(\theta) \\ &= \sin(\theta)(\sqrt{B} - 2) > 0, \end{aligned}$$

where the last inequality holds by (4.4). Thus, we have a contradiction, so

$$\beta_{D-1} \neq \beta_{D-2}.$$

Summarizing, we now know

$$\beta_D < 0 < \beta_0 < \beta_1 < \cdots < \beta_{D-2} \neq \beta_{D-1}. \tag{4.14}$$

Define J to be the smallest positive integer such that

$$\beta_{J+1} < \beta_J \qquad \text{and} \qquad \beta_{J-1} < \beta_J.$$

Observe that (4.14) implies that J is well-defined and

$$J = D - 2 \qquad \text{or} \qquad J = D - 1. \tag{4.15}$$

As a consequence, recalling (4.9) again, we have

$$0 < (J+1)\theta < \pi. \tag{4.16}$$

Since $\theta = \arg(b + \zeta_n)$ Recalling $b \geq 5$, (4.11) and (4.8), and using $\arctan x < x$ for $x > 0$, we also obtain

$$J \geq D - 2 \geq \frac{\pi}{\theta} - 3 \geq \frac{\pi}{\arg(b+\zeta_4)} - 3 = \frac{\pi}{\arctan(1/b)} - 3 > b\pi - 3 > 6. \tag{4.17}$$

In (14) of [17], the definition of J was used to establish

$$b_j \geq \beta_j b_0 \quad \text{for all integers } j \leq J+1. \tag{4.18}$$

The identical argument works to establish (4.18) here, and we will take advantage of this inequality as well.

We now note some further useful observations from [17]. Let

$$U = U(A,B) = \max_{j \geq 0}\{b_j\} \qquad \text{and} \qquad L = L(A,B) = \min_{j \geq 0}\{b_j\}. \tag{4.19}$$

Since $b_j = 0$ for $j > s$, we have the trivial bound $L \leq 0$. From equation (4.18), we obtain $U \geq \beta_J b_0$.

We are interested in A and B with $f(x)$ divisible by $\Phi_n(x-b) = x^2 - Ax + B$, where $n \in \{3,4,6\}$. We view A and B as fixed. We want $f(x)$ to have non-negative integer coefficients but with the largest coefficient as small as possible. Theorem 3.8 in [40] implies such $f(x)$ exist (also, see Lemma 3 in [16]). Let

$$M = M(A,B) \text{ denote the maximum coefficient for such an } f(x). \tag{4.20}$$

Let $\ell \in \mathbb{Z}^+$. We consider the matrix equation

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ -A & B & 0 & \dots & 0 & 0 & 0 \\ 1 & -A & B & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & B & 0 & 0 \\ 0 & 0 & 0 & \dots & -A & B & 0 \\ 0 & 0 & 0 & \dots & 1 & -A & B \end{pmatrix} \begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \\ \vdots \\ \mu_{\ell-3} \\ \mu_{\ell-2} \\ \mu_{\ell-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{4.21}$$

in the unknowns $\mu_0, \mu_1, \dots, \mu_{\ell-1}$. Let $\ell = J + 1$. We make some observations about the solutions to (4.21), as well as produce a closed form for such a solution.

Lemma 4.3. *Let b be an integer ≥ 5. Let A and B be such that $x^2 - Ax + B$ is $\Phi_n(x-b)$ where $n \in \{3, 4, 6\}$. The above matrix equation has a solution where $\mu_j > 0$ for all $0 \leq j \leq J$.*

Proof. Let $\mathcal{M}$ be the matrix in (4.21) with $\ell = J + 1$. The equation in (4.21) arising from the second row of $\mathcal{M}$ is equivalent to the condition $\mu_1 = A\mu_0/B$. The next $\ell - 2 = J - 1$ rows of $\mathcal{M}$ correspond to a recurrence relation for $\mu_0, \mu_1, \dots, \mu_J$ beginning with μ_0 and μ_1 and satisfying

$$\mu_j = \frac{A\mu_{j-1}}{B} - \frac{\mu_{j-2}}{B} \quad \text{for } 2 \leq j \leq J.$$

We will have a solution in μ_j to (4.21) provided then that we can find $\mu_0 > 0$ for which $\mu_1 = A\mu_0/B$ and the above recurrence gives $\sum_{0 \leq j \leq J} \mu_j = 1$. Observe that with μ_0 defined arbitrarily, this solution gives each μ_j as a multiple of μ_0. With this in mind, we define $\mu_j^* = \mu_j/\mu_0$.

As before, we find the characteristic polynomial for this recurrence relation to find the general term. This recurrence has characteristic polynomial $x^2 - Ax/B + 1/B$, which is the reciprocal polynomial of $x^2 - Ax + B$ divided by B; hence, the roots of

the characteristic polynomial are $1/(b+\zeta_n)$ and $1/(b+\overline{\zeta_n})$. So

$$\mu_j^* = c_1 \left(\frac{1}{b+\zeta_n}\right)^j + c_2 \left(\frac{1}{b+\overline{\zeta_n}}\right)^j \tag{4.22}$$

for $j \geq 0$, where c_1 and c_2 are constants to be determined. Taking $j = 0$ in (4.22), we see that since $\mu_0^* = 1$ we obtain $c_2 = 1 - c_1$. Next, we take $j = 1$ and use both $\overline{\zeta_n} - \zeta_n = -2i \sin(2\pi/n)$ and (4.7). Since $\mu_1^* = A/B$, we obtain

$$c_1 = \frac{\frac{A}{B} - \frac{1}{b+\overline{\zeta_n}}}{\frac{1}{b+\zeta_n} - \frac{1}{b+\overline{\zeta_n}}} = \frac{A - (b+\zeta_n)}{-2i \sin(2\pi/n)}$$

and

$$c_2 = 1 - c_1 = \frac{\overline{\zeta_n} - \zeta_n}{-2i \sin(2\pi/n)} - \frac{A - (b+\zeta_n)}{-2i \sin(2\pi/n)} = \frac{A - (b+\overline{\zeta_n})}{2i \sin(2\pi/n)}.$$

Thus, for $0 \leq j \leq J$, we have

$$\begin{aligned}\mu_j^* &= \frac{A - (b+\zeta_n)}{-2i \sin(2\pi/n)} \left(\frac{1}{b+\zeta_n}\right)^j + \frac{A - (b+\overline{\zeta_n})}{2i \sin(2\pi/n)} \left(\frac{1}{b+\overline{\zeta_n}}\right)^j \\ &= \frac{1}{2B \sin(2\pi/n)} \left[\frac{B - A(b+\overline{\zeta_n})}{i(b+\zeta_n)^{j-1}} + \frac{A(b+\zeta_n) - B}{i(b+\overline{\zeta_n})^{j-1}}\right].\end{aligned}$$

Recall (4.8). As in (4.6), for any $t \in \mathbb{Z}$, we deduce

$$(b+\overline{\zeta_n})^t - (b+\zeta_n)^t = -2i|b+\zeta_n|^t \sin(t\theta).$$

Taking $t = j$ and $t = j-1$ with $0 \leq j \leq J$, we obtain

$$\begin{aligned}\mu_j^* &= \frac{1}{2B \sin(2\pi/n)} \left[\frac{2Ai|b+\zeta_n|^j \sin(j\theta) - 2Bi|b+\zeta_n|^{j-1} \sin((j-1)\theta)}{i|b+\zeta_n|^{2(j-1)}}\right] \\ &= \frac{1}{B \sin(2\pi/n)} \left[\frac{A|b+\zeta_n|^j \sin(j\theta) - B|b+\zeta_n|^{j-1} \sin((j-1)\theta)}{B^{j-1}}\right].\end{aligned}$$

Using (4.5) and (4.6), we get

$$\mu_j^* = \frac{A\beta_{j-1} - B\beta_{j-2}}{B^j} = \frac{\beta_j}{B^j} \tag{4.23}$$

for $1 \leq j \leq J$. As $\mu_0^* = 1 = \beta_0/B^0$, we see that $\mu_j^* = \beta_j/B^j$ for all $j \in [0, J] \cap \mathbb{Z}$. The definition of J implies μ_j^* is positive for $0 \leq j \leq J$.

Recall that we want $\sum_{0\le j\le J}\mu_j = 1$, which is equivalent to $\sum_{0\le j\le J}\mu_j^* = 1/\mu_0$. Set

$$K = \sum_{j=0}^{J}\mu_j^* = \sum_{j=0}^{J}\frac{\beta_j}{B^j}. \tag{4.24}$$

As $K > 0$, we can take $\mu_0 = 1/K$ to deduce that the lemma holds. □

From the proof of Lemma 4.3, we have a closed form for $\mu_j > 0$ satisfying (4.21). Because we will be using this closed form, we would like a nicer way to write K. To do so, observe that, for m a positive integer, we have

$$\begin{aligned}
\sum_{j=1}^{m} r^j \sin(j\theta) &= \sum_{j=1}^{m} r^j \cdot \frac{e^{ij\theta} - e^{-ij\theta}}{2i} \\
&= \frac{1}{2i}\sum_{j=1}^{m}(re^{i\theta})^j - (re^{-i\theta})^j \\
&= \frac{1}{2i}\left[re^{i\theta}\sum_{j=0}^{m-1}(re^{i\theta})^j - re^{-i\theta}\sum_{j=0}^{m-1}(re^{-i\theta})^j\right] \\
&= \frac{1}{2i}\left[re^{i\theta}\frac{1-r^m e^{mi\theta}}{1-re^{i\theta}} - re^{-i\theta}\frac{1-r^m e^{-mi\theta}}{1-re^{-i\theta}}\right] \\
&= \frac{re^{i\theta}(1-r^m e^{mi\theta})(1-re^{-i\theta}) - re^{-i\theta}(1-r^m e^{-mi\theta})(1-re^{i\theta})}{2i|1-re^{i\theta}|^2} \\
&= \frac{re^{i\theta} - re^{-i\theta} - r^{m+1}e^{(m+1)i\theta} + r^{m+1}e^{-(m+1)i\theta} + r^{m+2}e^{mi\theta} - r^{m+2}e^{-mi\theta}}{2i|1-re^{i\theta}|^2} \\
&= \frac{r\sin(\theta) - r^{m+1}\sin((m+1)\theta) + r^{m+2}\sin(m\theta)}{|1-re^{i\theta}|^2}.
\end{aligned} \tag{4.25}$$

From (4.12) and (4.24), we see that

$$\begin{aligned}
K = \sum_{j=0}^{J}\frac{\beta_j}{B^j} &= \frac{1}{\sin(2\pi/n)}\sum_{j=0}^{J}\frac{\sqrt{B}^{j+1}\sin((j+1)\theta)}{\sqrt{B}^{2j}} \\
&= \frac{\sqrt{B}^2}{\sin(2\pi/n)}\sum_{j=0}^{J}\left(\frac{1}{\sqrt{B}}\right)^{j+1}\sin((j+1)\theta) \\
&= \frac{B}{\sin(2\pi/n)}\sum_{j=1}^{J+1}\left(\frac{1}{\sqrt{B}}\right)^{j}\sin(j\theta).
\end{aligned}$$

Using (4.25) with $r = 1/\sqrt{B}$ and $m = J+1$, we get

$$K = \frac{B}{\sin(2\pi/n)} \frac{\sqrt{B}^{-1}\sin(\theta) - \sqrt{B}^{-J-2}\sin((J+2)\theta) + \sqrt{B}^{-J-3}\sin((J+1)\theta)}{|1-\sqrt{B}^{-1}e^{i\theta}|^2}$$

$$= \frac{B}{\sin(2\pi/n)} \frac{\sqrt{B}^{2J+3}\sin(\theta) - \sqrt{B}^{J+2}\sin((J+2)\theta) + \sqrt{B}^{J+1}\sin((J+1)\theta)}{\sqrt{B}^{2J+4}B^{-2}|B-\sqrt{B}e^{i\theta}|^2}.$$

Using (4.13) and rearranging, we obtain

$$K = \frac{1}{B^{J-1}|B-\sqrt{B}e^{i\theta}|^2}\left(B^{J+1} - \frac{\sqrt{B}^{J+2}\sin((J+2)\theta)}{\sin(2\pi/n)} + \frac{\sqrt{B}^{J+1}\sin((J+1)\theta)}{\sin(2\pi/n)}\right).$$

By (4.7) and (4.8), we see $\sqrt{B}e^{i\theta} = |b+\zeta_n|e^{i\arg(b+\zeta_n)} = b+\zeta_n$ for each $n \in \{3,4,6\}$. Thus, from (4.12) with $j = J+1$ and $j = J$, we acquire

$$K = \frac{B^{J+1} - \beta_{J+1} + \beta_J}{B^{J-1}|b+\zeta_n - B|^2}. \tag{4.26}$$

Recalling from the proof of Lemma 4.3 that $\mu_j^* = \mu_j/\mu_0$, $\mu_0 = 1/K$ and (4.23), we see that

$$\mu_j = \frac{\beta_j}{B^j K}. \tag{4.27}$$

In the next section, we will use the value of K in (4.26) and β_j in the formulation of μ_j in (4.27) to obtain bounds for $L = L(A,B)$ and $M = M(A,B)$, which were defined in (4.19) and (4.20).

4.3 Establishing Bounds

Recall the setup thus far. Let $f(x) = g(x)h(x)$ be a polynomial in $\mathbb{Z}[x]$ with non-negative coefficients where $g(x) = x^2 - Ax + B$ is $\Phi_3(x-b)$, $\Phi_4(x-b)$, or $\Phi_6(x-b)$, and $h(x)$ has positive leading coefficient denoted b_0 as in (4.3). Recall that $M(A,B)$ is the smallest value that the largest coefficient of $f(x)$ can be under these conditions. It is worth noting that we do not require $f(b)$ to be prime in the definition of $M(A,B)$.

We proceed towards proving Theorem 1.6. Using the previous sections, we will find three bounds, $\mathcal{B}_b^{(3)}$, $\mathcal{B}_b^{(4)}$, and $\mathcal{B}_b^{(6)}$ such that if $f(x)$ has coefficients less than

or equal to $\mathcal{B}_b^{(n)}$ with $f(b)$ prime, then $f(x)$ cannot be divisible by $\Phi_n(x-b)$ for $n \in \{3,4,6\}$. Note the difference between $\mathcal{B}_b^{(n)}$ and $M(A,B)$; $M(A,B)$ does not require $f(b)$ to be prime while $\mathcal{B}_b^{(n)}$ does. We begin by showing both of the following:

(i) The value of $M(A,B)$ is $(1-A+B)\cdot\beta_J$ for each $n \in \{3,4,6\}$.

(ii) If the maximal coefficient of $f(x)$ equals $M(A,B)$, then $f(b)$ is composite.

Assuming (i) and (ii), we explain now that we can take $\mathcal{B}_b^{(n)} = M(A,B)$. If $f(x)$ has each coefficient less than $M(A,B)$, then $f(x)$ cannot be divisible by $\Phi_n(x-b)$ by the minimality of $M(A,B)$. Note that this conclusion does not require $f(b)$ to be prime. If we further require $f(b)$ to be prime, then by (ii), we would also have that the largest coefficient of $f(x)$ cannot equal $M(A,B)$. Hence, we can take $\mathcal{B}_b^{(n)} = M(A,B)$.

Notice the dependence on n; A and B are the integers such that $x^2 - Ax + B$ is $\Phi_n(x-b)$, so A and B depend on n. Also, β_J depends on D and θ, both defined in (4.8), so β_J depends on n.

We start by establishing (i). We follow the method used in [10]. Suppose first that

$$M(A,B) \leq (1-A+B)\cdot\beta_J. \tag{4.28}$$

We eventually want a contradiction if strict inequality holds; however, there will be a significance in seeing what this inequality gives us. Since $M(A,B)$ is a coefficient of $f(x)$, it must be positive. Also, by definition, $\beta_J > 0$; thus, in order for (4.28) to make sense, we must have $1 - A + B > 0$, which follows from (4.4).

We start by setting

$$u = \mu_0 B, \quad v = \mu_{\ell-2} - \mu_{\ell-1}A \text{ and } w = \mu_{\ell-1}, \tag{4.29}$$

where μ_j is as in (4.27) and where $\ell = J+1$. Then [17] establishes that

$$M \geq \left\lceil \frac{u^2 - (v+w)^2}{u} \cdot U \right\rceil \geq \frac{u^2-(v+w)^2}{u}\cdot U \tag{4.30}$$

$$\geq \frac{u^2-(v+w)^2}{u}\beta_J b_0 \geq \frac{(u^2-(v+w)^2)\beta_J}{u}$$

and

$$0 \leq -L \leq \frac{v+w}{u^2-(v+w)^2} \cdot M. \tag{4.31}$$

From (4.28) and (4.30), we have

$$b_0\beta_J \leq U(A,B) \leq \frac{uM(A,B)}{u^2-(v+w)^2} \leq \frac{u(1-A+B)\cdot\beta_J}{u^2-(v+w)^2}. \tag{4.32}$$

We make an observation about this inequality with $\ell = J+1$.

Lemma 4.4. *With the prior notation,*

$$\frac{u(1-A+B)\cdot\beta_J}{u^2-(v+w)^2} < \beta_J + 1.$$

Proof. Simplifying the left-hand side of the inequality above, we obtain

$$\begin{aligned}
\frac{u(1-A+B)\cdot\beta_J}{u^2-(v+w)^2} &= \frac{\mu_0 B(1-A+B)\beta_J}{\mu_0^2B^2-(\mu_{J-1}-\mu_J(A-1))^2} \\
&= \frac{\frac{1}{K}B(1-A+B)\beta_J}{\frac{B^2}{K^2}-(\frac{\beta_{J-1}}{KB^{J-1}}-\frac{\beta_J}{KB^J}(A-1))^2} \\
&= \frac{KB^{2J+1}(1-A+B)\beta_J}{B^{2J+2}-(B\beta_{J-1}-A\beta_J+\beta_J)^2} \\
&= \frac{KB^{2J+1}(1-A+B)\beta_J}{B^{2J+2}-(\beta_J-\beta_{J+1})^2}.
\end{aligned}$$

From the definition of K in (4.26), we obtain

$$\frac{u(1-A+B)\cdot\beta_J}{u^2-(v+w)^2} = \frac{B^{2J+1}(1-A+B)\beta_J(B^{J+1}-\beta_{J+1}+\beta_J)}{B^{J-1}|b+\zeta_n-B|^2(B^{2J+2}-(\beta_J-\beta_{J+1})^2)}.$$

Since $n \in \{3,4,6\}$, the field $\mathbb{Q}(\zeta_n)$ is of degree 2 over $\mathbb{Q}$ and $|b+\zeta_n-B|^2$ is the norm of $b+\zeta_n-B$ in the field $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$. The norm of $b+\zeta_n-B$ is the constant term of its minimal polynomial over $\mathbb{Q}$, which is $(x+B)^2-A(x+B)+B$. Thus, we see that

$$|b+\zeta_n-B|^2 = B(1-A+B).$$

Therefore,

$$\begin{aligned}\frac{u(1-A+B)\cdot\beta_J}{u^2-(v+w)^2} &= \frac{B^{J+2}(1-A+B)\beta_J(B^{J+1}-\beta_{J+1}+\beta_J)}{B(1-A+B)(B^{J+1}-\beta_J+\beta_{J+1})(B^{J+1}+\beta_J-\beta_{J+1})}\\ &= \frac{B^{J+1}\beta_J}{B^{J+1}-\beta_J+\beta_{J+1}}\\ &= \frac{B^{J+1}\beta_J}{B^{J+1}-\beta_J+A\beta_J-B\beta_{J-1}}\\ &= \frac{B^{J+1}}{\frac{B^{J+1}}{\beta_J}+A-1-B\frac{\beta_{J-1}}{\beta_J}}.\end{aligned}$$

To prove the lemma, we need to show

$$\frac{B^{J+1}}{\frac{B^{J+1}}{\beta_J}+A-1-B\frac{\beta_{J-1}}{\beta_J}} < \beta_J+1,$$

which is the same as showing

$$B^{J+1} < B^{J+1}+\frac{B^{J+1}}{\beta_J}+\left(A-1-B\frac{\beta_{J-1}}{\beta_J}\right)(\beta_J+1).$$

Moving all terms to one side, this is equivalent to

$$\left(1-A+B\frac{\beta_{J-1}}{\beta_J}\right)(\beta_J+1)-\frac{B^{J+1}}{\beta_J} < 0.$$

For ease of notation, let

$$\Delta = 1-A+B\frac{\beta_{J-1}}{\beta_J} < 1-A+B, \tag{4.33}$$

where the inequality follows from the definition of J which implies $\beta_J > \beta_{J-1}$. From (4.12), it suffices to show

$$\Delta\left(\frac{\sqrt{B}^{J+1}\sin((J+1)\theta)}{\sin(2\pi/n)}+1\right)-\frac{B^{J+1}\sin(2\pi/n)}{\sqrt{B}^{J+1}\sin((J+1)\theta)} < 0.$$

From (4.16), we have $\sin((J+1)\theta) > 0$. Multiplying by $\sin(2\pi/n)\sin((J+1)\theta)$ in the previous inequality, we see that we want

$$\Delta\left(\sqrt{B}^{J+1}\sin^2((J+1)\theta)+\sin((J+1)\theta)\sin(2\pi/n)\right)-\sqrt{B}^{J+1}\sin^2(2\pi/n) < 0.$$

Rearranging, we want to show

$$\sqrt{B}^{J+1}\left[\Delta\sin^2((J+1)\theta)-\sin^2(2\pi/n)\right]+\Delta\sin(2\pi/n)\sin((J+1)\theta)<0.$$

From (4.33), we see that it suffices to show that

$$\begin{aligned}\sqrt{B}^{J+1}[(1-A+B)\sin^2((J+1)\theta)-\sin^2(2\pi/n)]&\\ +\Delta\sin(2\pi/n)\sin((J+1)\theta)<0.&\end{aligned}\tag{4.34}$$

We now break the proof into two cases, $J=D-1$ and $J=D-2$. Because $\sin((D-1)\theta)$ is close to $\sin(\pi)=0$, we will do some simple approximations to prove (4.34) when $J=D-1$. When $J=D-2$, the value of $\sin((D-2)\theta)$ is not close enough to 0 to do the same approximations, so a different technique is employed.

Recall (4.8) which implies for $b\geq 5$ that

$$0<\theta=\arctan(b+\zeta_n)\leq\arctan(5+\zeta_4)=\arctan(1/5)<\pi/4.$$

Hence, when $J=D-1$, we have

$$\pi>D\theta\geq(\pi/\theta-1)\theta=\pi-\theta>\pi/2,\tag{4.35}$$

so $\sin(D\theta)<\sin(\pi-\theta)=\sin(\theta)=\sin(2\pi/n)/\sqrt{B}$ by (4.13). With $J=D-1$ and (4.33), and since $1-A+B>0$ by (4.4), the left-hand side of (4.34) is

$$\begin{aligned}&\sqrt{B}^{D}[(1-A+B)\sin^2(D\theta)-\sin^2(2\pi/n)]+\Delta\sin(D\theta)\sin(2\pi/n)\\ &\quad<\sqrt{B}^{D}\left[(1-A+B)\frac{\sin^2(2\pi/n)}{B}-\sin^2(2\pi/n)\right]+(1-A+B)\frac{\sin^2(2\pi/n)}{\sqrt{B}}.\end{aligned}$$

Thus, it suffices to show the right side above is <0 to establish (4.34). After dividing out by $\sin^2(2\pi/n)$, we want to establish the equivalent inequality

$$\sqrt{B}^{D}\left[\frac{1-A+B}{B}-1\right]+\frac{1-A+B}{\sqrt{B}}=\sqrt{B}^{D}\left[\frac{1-A}{B}\right]+\frac{1-A+B}{\sqrt{B}}<0.$$

Multiplying both sides of the inequality by $B\sqrt{B}$, we now want to show

$$\sqrt{B}^{D+1}[1-A]+B(1-A+B)<0,$$

or equivalently

$$(1-A)\left(\sqrt{B}^{D+1}+B\right)+B^2<0.$$

By (4.4), we see that $1-A<0$ for $b\geq 3$. One can check directly that $D\geq 3$ for each $n\in\{3,4,6\}$ where D is defined in (4.8). Thus the above inequality holds for $b\geq 3$, so (4.34) has been established for $J=D-1$.

We now move towards proving (4.34) for $J=D-2$. Recall (4.13) and note that $\sin(2\pi/n)=\operatorname{Im}(b+\zeta_n)=\sqrt{4B-A^2}/2$, so

$$\begin{aligned}\sin(\theta)=\frac{\sqrt{4B-A^2}}{2\sqrt{B}}=\frac{\sin(2\pi/n)}{\sqrt{B}},\quad \cos(\theta)=\frac{A}{2\sqrt{B}},\quad \text{and}\\ \tan(\theta)=\frac{\sqrt{4B-A^2}}{A}=\frac{2\sin(2\pi/n)}{A}.\end{aligned}\tag{4.36}$$

By the definition of J, we have $\beta_J>\beta_{J+1}$, which for $J=D-2$ is $\beta_{D-2}>\beta_{D-1}$. Using (4.12), we obtain

$$\sin((D-1)\theta)>\sqrt{B}\sin(D\theta).\tag{4.37}$$

Define η by

$$D\theta=\pi-\eta.$$

Then, by the definition of D and Lemma 4.2, we have $0<\eta<\theta$.

From (4.37) and (4.36), we obtain now that

$$\begin{aligned}\sqrt{B}&<\frac{\sin((D-1)\theta)}{\sin(D\theta)}=\frac{\sin(\pi-\eta-\theta)}{\sin(\pi-\eta)}\\ &=\frac{\sin(\eta+\theta)}{\sin(\eta)}=\frac{\sin(\eta)\cos(\theta)+\cos(\eta)\sin(\theta)}{\sin(\eta)}\\ &=\cos(\theta)+\sin(\theta)\cot(\eta).\end{aligned}$$

After manipulating this, we see that

$$\eta<\arctan\left(\frac{\sin(\theta)}{\sqrt{B}-\cos(\theta)}\right)=\arctan\left(\frac{\sqrt{4B-A^2}}{2B-A}\right)=:\tau.$$

From the definition of τ we obtain the values

$$\begin{gathered}\sin(\tau)=\frac{\sqrt{4B-A^2}}{2\sqrt{B(1-A+B)}},\quad \cos(\tau)=\frac{2B-A}{2\sqrt{B(1-A+B)}},\\ \text{and}\quad \tan(\tau)=\frac{\sqrt{4B-A^2}}{2B-A},\end{gathered}\tag{4.38}$$

which are well-defined by (4.4).

Lastly, by comparing $\sin(\theta)$ and $\sin(\tau)$ in (4.36) and (4.38) and noting $1-A+B>1$ by (4.4), we see that $\tau<\theta$. Using the inequality $\arctan x\le x$ for $x\in(0,\pi/2)$, we observe that for $b\ge 2$ and $n\in\{3,4,6\}$ we have

$$\eta+\theta<\tau+\theta<2\theta<\frac{\pi}{2}.\tag{4.39}$$

To prove (4.34), we first show that $\Delta>0$. Using (4.12), we have

$$\begin{aligned}\Delta&=1-A+B\,\frac{\beta_{D-3}}{\beta_{D-2}}\\ &=1-A+\sqrt{B}\,\frac{\sin(D\theta-2\theta)}{\sin(D\theta-\theta)}\\ &=1-A+\sqrt{B}\,\frac{\sin(\eta+2\theta)}{\sin(\eta+\theta)}.\end{aligned}\tag{4.40}$$

Recall that $\eta<\tau$ and by (4.39) we have both $\eta+\theta$ and $\tau+\theta$ are in $(0,\pi/2)$, so

$$\frac{\sin(\eta+2\theta)}{\sin(\eta+\theta)}=\cos(\theta)+\sin(\theta)\cot(\eta+\theta)>\cos(\theta)+\sin(\theta)\cot(\tau+\theta).\tag{4.41}$$

Using (4.36) and (4.38) we see that

$$\begin{aligned}\cos(\theta)+\sin(\theta)\cot(\tau+\theta)&=\cos(\theta)+\sin(\theta)\,\frac{1-\tan(\tau)\tan(\theta)}{\tan(\tau)+\tan(\theta)}\\ &=\frac{A}{2\sqrt{B}}+\frac{\sqrt{4B-A^2}}{2\sqrt{B}}\cdot\frac{1-\frac{\sqrt{4B-A^2}}{2B-A}\frac{\sqrt{4B-A^2}}{A}}{\frac{\sqrt{4B-A^2}}{2B-A}+\frac{\sqrt{4B-A^2}}{A}}\\ &=\frac{A}{2\sqrt{B}}+\frac{\sqrt{4B-A^2}}{2\sqrt{B}}\cdot\frac{A(2B-A)-(4B-A^2)}{2B\sqrt{4B-A^2}}.\\ &=\frac{A}{2\sqrt{B}}+\frac{A-2}{2\sqrt{B}}\\ &=\frac{A-1}{\sqrt{B}}\end{aligned}\tag{4.42}$$

Combining (4.40), (4.41), and (4.42), we deduce that

$$\Delta > 0 \qquad \text{for} \quad J = D - 2. \tag{4.43}$$

Note $\sin(2\pi/n)\sin((J+1)\theta) < 1$, so to show (4.34) it suffices to show

$$\sqrt{B}^{D-1}[(1 - A + B)\sin^2((D-1)\theta) - \sin^2(2\pi/n)] + \Delta < 0. \tag{4.44}$$

From (4.40), we see that (4.44) is equivalent to

$$\sqrt{B}^{D-1}[(1 - A + B)\sin^2(\eta + \theta) - \sin^2(2\pi/n)] + 1 - A + \sqrt{B}\,\frac{\sin(\eta + 2\theta)}{\sin(\eta + \theta)} < 0. \tag{4.45}$$

To show this inequality, we are going to view η in (4.45) as a variable and let it range from 0 to τ, and see that the left-hand side of (4.45) is increasing to zero in this range.

Observe what happens if we let $\eta = \tau$ in (4.45). The inequality in (4.41) becomes an equality. When combined with (4.42), we obtain $\Delta = 0$. Thus, the left-hand side of (4.45) is equal to

$$\sqrt{B}^{D-1}[(1 - A + B)\sin^2(\theta + \tau) - \sin^2(2\pi/n)]. \tag{4.46}$$

Using (4.36) and (4.38), we see that

$$\begin{aligned}
\sin^2(\theta + \tau) &= (\sin\theta\cos\tau + \cos\theta\sin\tau)^2 \\
&= \left(\frac{\sin(2\pi/n)}{\sqrt{B}}\frac{2B - A}{2\sqrt{B}\sqrt{1 - A + B}} + \frac{A}{2\sqrt{B}}\frac{\sin(2\pi/n)}{\sqrt{B}\sqrt{1 - A + B}}\right)^2 \\
&= \frac{\sin^2(2\pi/n)}{4B^2(1 - A + B)}(2B)^2 \\
&= \frac{\sin^2(2\pi/n)}{1 - A + B}.
\end{aligned}$$

Hence, the expression in (4.46), which is the left-hand side of (4.45), is zero.

We now move to showing that (4.45) is negative when η ranges from 0 to τ. We begin by showing the similar expression

$$\sqrt{B}\,[(1 - A + B)\sin^2(\eta + \theta) - \sin^2(2\pi/n)] + 1 - A + \sqrt{B}\,\frac{\sin(\eta + 2\theta)}{\sin(\eta + \theta)} \tag{4.47}$$

is negative for η between 0 and τ. By applying angle-sum identities for sine and cosine and rearranging, we rewrite (4.47) as

$$\begin{aligned}
&-4\left(1-A+B\right)\left(A^2-B\right)\sqrt{4B-A^2}\cos^3\left(\eta\right)\\
&\qquad+\left(3A^2\left(1-A+B\right)-B\left(4B-A^2\right)+4\sqrt{B}\right)\sqrt{4B-A^2}\cos\left(\eta\right)\\
&\qquad+\left(4A\left(1-A+B\right)\left(A^2-3B\right)\right)\sin^3\left(\eta\right)\\
&\qquad+\left(A\left(4B-A^2\right)\left(3-3A+2B\right)-4\left(2B-A\right)\sqrt{B}\right)\sin\left(\eta\right)
\end{aligned}$$

divided by

$$4\left(\sqrt{4B-A^2}\cos\left(\eta\right)+A\sin\left(\eta\right)\right)\sqrt{B}. \tag{4.48}$$

It is clear that the denominator (4.48) is positive, so we focus on the numerator, which we call W. If we can show that W is increasing for $0<\eta<\tau$, then it must be negative. Differentiating W with respect to η yields

$$\begin{aligned}
\frac{dW}{d\eta}=\;&12\left(1-A+B\right)\left(A^2-B\right)\sqrt{4B-A^2}\cos^2\left(\eta\right)\sin\left(\eta\right)\\
&+B\left(4B-A^2\right)\sin\left(\eta\right)\\
&+12\left(1-A+B\right)\left(A^2-3B\right)\cos\left(\eta\right)\sin^2\left(\eta\right)\\
&+A\left(4B-A^2\right)\left(3-3A+2B\right)\cos\left(\eta\right)\\
&-\left(3A^2\left(1-A+B\right)+4\sqrt{B}\right)\sqrt{4B-A^2}\sin\left(\eta\right)\\
&-4\left(2B-A\right)\sqrt{B}\cos\left(\eta\right),
\end{aligned} \tag{4.49}$$

where (4.49) is written so that each expression in A and B that appears is positive by (4.4), a trait that will be carried forward for the remainder of this argument. We now bound (4.49) below by an expression that does not depend on η. Recall that $0<\eta<\tau<\theta$. Then, using (4.36) and (4.38), the bounds

$$\frac{A}{2\sqrt{B}}=\cos\left(\theta\right)\leq\cos\left(\eta\right)\leq 1 \qquad \text{and} \qquad 0\leq\sin\left(\eta\right)\leq\sin\left(\tau\right)=\frac{\sqrt{4B-A^2}}{2\sqrt{B\left(1-A+B\right)}}$$

give us

$$\begin{aligned}\frac{dW}{d\eta} >& \frac{A^2\left(4B-A^2\right)\left(3-3A+2B\right)}{2\sqrt{B}} \\ &- \frac{\left(3A^2\left(1-A+B\right)+4\sqrt{B}\right)\left(4B-A^2\right)}{2\sqrt{B\left(1-A+B\right)}} - 4\left(2B-A\right)\sqrt{B},\end{aligned} \tag{4.50}$$

where in (4.49), the first 3 terms have been bounded by $0 \leq \sin\left(\eta\right)$, the fourth has been bounded by $\cos\left(\theta\right) \leq \cos\left(\eta\right)$, the fifth has been bounded by $\sin\left(\tau\right) \geq \sin\left(\eta\right)$, and the sixth has been bounded by $1 \geq \cos\left(\eta\right)$.

Since $B - 2A > 0$ for $b \geq 3$ and $b \geq 2$, we have

$$0 < 3\left(B-2A\right) < 3B-4A < 4-4A+3B < B\left(4-4A+3B\right),$$

which when rearranged gives

$$4B\left(1-A+B\right) > B^2. \tag{4.51}$$

Also, by the arithmetic-geometric mean inequality, we obtain

$$\frac{A^2+4B}{2A} \geq 2\sqrt{B}. \tag{4.52}$$

Using (4.51) and (4.52), we bound the right-hand side of (4.50) below by

$$\begin{aligned}&\frac{A^2\left(4B-A^2\right)\left(3-3A+2B\right)}{\left(A^2+4B\right)/\left(2A\right)} \\ &\qquad - \frac{\left(3A^2\left(1-A+B\right)+2\left(A^2+4B\right)/\left(2A\right)\right)\left(4B-A^2\right)}{B} \\ &\qquad - 2\left(2B-A\right)\frac{A^2+4B}{2A}.\end{aligned} \tag{4.53}$$

Substituting $A = 2\left(b+\mathrm{Re}\left(\zeta_n\right)\right)$ and $B = \left(b+\zeta_n\right)\left(b+\overline{\zeta_n}\right)$, the expression in (4.53) becomes

$$\begin{aligned}&-32\left(4b^2-9b+3\right)\cos^8\left(2\pi/n\right) \\ &\quad - 16\left(40b^3-111b^2+62b-12\right)\cos^7\left(2\pi/n\right)\end{aligned}$$

$$
\begin{aligned}
&- 8\left(164b^4 - 546b^3 + 400b^2 - 121b + 9\right)\cos^6(2\pi/n) \\
&- 4\left(352b^5 - 1380b^4 + 1188b^3 - 307b^2 - 84b + 23\right)\cos^5(2\pi/n) \\
&- 4\left(208b^6 - 948b^5 + 873b^4 + 223b^3 - 562b^2 + 227b - 45\right)\cos^4(2\pi/n) \\
&- 8\left(32b^7 - 168b^6 + 128b^5 + 430b^4 - 516b^3 + 305b^2 - 80b + 11\right)\cos^3(2\pi/n) \\
&- 8\left(4b^8 - 24b^7 - 16b^6 + 394b^5 - 449b^4 + 355b^3 - 86b^2 + 30b + 2\right)\cos^2(2\pi/n) \\
&+ 4\left(32b^7 - 308b^6 + 384b^5 - 380b^4 + 92b^3 - 57b^2 - 28b + 1\right)\cos(2\pi/n) \\
&+ 4\left(4b^8 - 44b^7 + 64b^6 - 76b^5 + 23b^4 - 19b^3 - 14b^2 + b - 3\right)
\end{aligned}
$$

divided by

$$
\begin{aligned}
2b\cos^4(2\pi/n) &+ \left(11b^2 + 1\right)\cos^3(2\pi/n) \\
&+ b\left(17b^2 + 7\right)\cos^2(2\pi/n) \\
&+ \left(10b^4 + 9b^2 + 1\right)\cos(2\pi/n) \\
&+ b\left(2b^2 + 1\right)\left(b^2 + 1\right).
\end{aligned}
$$

The final lower bound comes from bounding the first of these below and the second of these above using $|\cos(2\pi/n)| \leq 1/2$. Doing this and collecting powers of b yields

$$\frac{dW}{d\eta} > \frac{64b^8 - 1280b^7 + 3232b^6 - 8216b^5 + 3950b^4 - 3288b^3 - 374b^2 - 110b - 149}{16b^5 + 40b^4 + 58b^3 + 47b^2 + 23b + 5}.$$

The denominator is positive, and one checks that the numerator is as well for $b \geq 18$.

To prove the expression in (4.45) is negative, we observe that since $\Delta \geq 0$, we have

$$(1 - A + B)\sin^2((D-1)\theta) - \sin^2(2\pi/n) < 0.$$

Since $D \geq 1$, the expression in (4.47) being negative implies (4.45) holds. □

Recall the setup so far. We are working under the assumptions that $f(x)$ is a polynomial with non-negative integer coefficients such that

$$f(x) = h(x)g(x) = (b_0x^s + b_1x^{s-1} + \cdots b_{s-1}x + b_s)(x^2 - Ax + B)$$

where $\Phi_n(x-b) = x^2 - Ax + B$. From Lemma 4.4 and (4.32), we see that $b_0 < 2$, and since b_0 is an non-negative integer, $b_0 = 1$. Thus, (4.28) implies that $h(x)$ is monic. Also, using Lemma 4.4 and (4.32) with $b_0 = 1$, we have

$$\beta_J \leq U(A,B) < \beta_J + 1.$$

Thus, we have established that $U(A,B) = \beta_J$. Recalling (4.19), we see that the largest coefficient of $h(x)$ is β_J. Next, we observe the following.

Lemma 4.5. *Under the assumption* (4.28) *with u, v, and w defined as in* (4.29)*, we have*

$$\delta := \frac{v+w}{u^2 - (v+w)^2} \cdot M(A,B) \in (0,1)$$

for all $b \geq 3$.

Proof. From (4.31), we see that $\delta \geq 0$. We now claim that $\delta \neq 0$. The only way δ could $= 0$ is if $M(A,B) = 0$ or $v + w = 0$. From the definition of $M(A,B)$, we see that $M(A,B) \geq 1$. By way of contradiction, assume that $v + w = 0$, then $v = -w$. By the definitions of v and w in (4.29) with $\ell = J + 1$ we have

$$\mu_{J-1} - \mu_J A = -\mu_J.$$

From (4.27), we see that $\mu_J \neq 0$ and

$$0 = 1 - A + \frac{\mu_{J-1}}{\mu_J} = 1 - A + B\frac{\beta_{J-1}}{\beta_J}.$$

Notice that the right-hand side is the definition of Δ in (4.33). We showed that $\Delta > 0$ for $J = D - 2$ by (4.43), so recalling (4.15), we restrict our attention to the case that $J = D - 1$. Using (4.12), the sum of angles formula for sine, and (4.36), we obtain

$$\begin{aligned}\Delta &= 1 - A + B\frac{\beta_{D-2}}{\beta_{D-1}} = 1 - A + \sqrt{B}\frac{\sin(D\theta - \theta)}{\sin(D\theta)} \\ &= 1 - A + \sqrt{B}\,\frac{\sin(D\theta)\cos(\theta) - \cos(D\theta)\sin(\theta)}{\sin(D\theta)}\end{aligned}$$

$$= 1 - A + \sqrt{B}\left(\cos(\theta) - \sin(\theta)\cot(D\theta)\right)$$

$$= 1 - A + \sqrt{B}\left(\frac{A}{2\sqrt{B}} - \frac{\sin(2\pi/n)}{\sqrt{B}}\cot(D\theta)\right)$$

$$= 1 - \frac{A}{2} - \sin(2\pi/n)\cot(D\theta).$$

From (4.35) and (4.36), we see that

$$\begin{aligned}
\Delta &= 1 - \frac{A}{2} - \sin(2\pi/n)\cot(D\theta) \\
&> 1 - \frac{A}{2} - \sin(2\pi/n)\cot(\pi - \theta) \\
&= 1 - \frac{A}{2} + \sin(2\pi/n)\cot(\theta) \\
&= 1 - \frac{A}{2} + \frac{A\sin(2\pi/n)}{2\sin(2\pi/n)} \\
&= 1.
\end{aligned}$$

Thus we have a contradiction in both cases, so $v + w \neq 0$. Hence, $\delta > 0$.

Next, we show that $\delta < 1$. We start by observing that Lemma 4.4 and (4.28) give us

$$\delta = \frac{uM(A,B)}{u^2 - (v+w)^2}\frac{v+w}{u} < (\beta_J + 1)\frac{v+w}{u}.$$

Using the definitions of u, v, and w in (4.29) with $\ell = J + 1$, we obtain

$$\delta < (\beta_J + 1)\frac{v+w}{u} = (\beta_J + 1)\,\frac{\mu_{J-1} - \mu_J(A-1)}{\mu_0 B}.$$

From (4.27) and (4.12), we have

$$\begin{aligned}
\delta &< (\beta_J + 1)\,\frac{\mu_{J-1} - \mu_J(A-1)}{\mu_0 B} = \frac{\beta_J + 1}{B}\left(\frac{\beta_{J-1}}{B^{J-1}} - \frac{\beta_J}{B^J}(A-1)\right) \\
&= \frac{\beta_J + 1}{B^{J+1}}\left(B\beta_{J-1} + (1-A)\beta_J\right) \\
&= \frac{\frac{\sqrt{B}^{J+1}\sin((J+1)\theta)}{\sin(2\pi/n)} + 1}{B^{J+1}}\left(\frac{\sqrt{B}^{J+2}\sin(J\theta)}{\sin(2\pi/n)} + (1-A)\frac{\sqrt{B}^{J+1}\sin((J+1)\theta)}{\sin(2\pi/n)}\right) \\
&= \frac{\sqrt{B}^{J+1}\sin((J+1)\theta) + \sin(2\pi/n)}{\sqrt{B}^{J+1}\sin^2(2\pi/n)}\left(\sqrt{B}\sin(J\theta) + (1-A)\sin((J+1)\theta)\right).
\end{aligned}$$

We make a few observations to help simplify. First, $(1-A)\sin((J+1)\theta) \leq 0$ since $\sin((J+1)\theta) > 0$ by (4.16). Second, using (4.16), (4.15), and noting that $D > \pi/\theta - 1$, we have

$$\pi > J\theta \geq (D-2)\theta > (\pi/\theta - 3)\theta = \pi - 3\theta.$$

$$\arg(b+\zeta_n) \leq \arg(b+\zeta_4) = \frac{\pi}{\pi/\arg(b+\zeta_4)} < \frac{\pi}{\lfloor \pi/\arg(b+\zeta_4) \rfloor} = \frac{\pi}{D_4},$$

From (4.9) and (4.11), for $b \geq 5$ we obtain

$$\theta \leq \arg(b+\zeta_4) < \frac{\pi}{\theta_4} = \frac{\pi}{\arctan(1/b)} < \frac{\pi}{6}.$$

Putting these together, we get for $b \geq 5$ that

$$\pi > J\theta > \pi - 3\theta > \frac{\pi}{2},$$

so $\sin(J\theta) < \sin(3\theta)$. Likewise, from (4.16), we have $\pi > (J+1)\theta > \pi - 2\theta > \pi/2$. Thus, $\sin((J+1)\theta) < \sin(2\theta)$. Using these bounds, we acquire

$$\delta < \frac{\sqrt{B}^{J+1}\sin(2\theta) + \sin(2\pi/n)}{\sqrt{B}^{J}\sin^2(2\pi/n)}\sin(3\theta).$$

Using double and triple angle formulas for $\sin\theta$ and (4.36) with $\sqrt{4B-A^2} = 2\sin(2\pi/n)$, we get

$$\begin{aligned}
\delta &< \frac{\sqrt{B}^{J+1}2\sin\theta\cos\theta + \sin(2\pi/n)}{\sqrt{B}^{J}\sin^2(2\pi/n)}(3\sin\theta - 4\sin^3\theta) \\
&= \frac{\sqrt{B}^{J+1}\dfrac{A\sin(2\pi/n)}{B} + \sin(2\pi/n)}{\sqrt{B}^{J}\sin^2(2\pi/n)}\left(3\frac{\sin(2\pi/n)}{\sqrt{B}} - 4\frac{\sin^3(2\pi/n)}{B\sqrt{B}}\right) \\
&= \frac{A\sqrt{B}^{J-1}+1}{\sqrt{B}^{J}}\left(\frac{3}{\sqrt{B}} - 4\frac{\sin^2(2\pi/n)}{B\sqrt{B}}\right) \\
&= \frac{A\sqrt{B}^{J-1}+1}{\sqrt{B}^{J+3}}(3B - 4\sin^2(2\pi/n)) \\
&= \frac{A\sqrt{B}^{J-1}+1}{\sqrt{B}^{J+3}}(A^2 - B).
\end{aligned}$$

This last expression is less than 1 precisely when

$$(A\sqrt{B}^{J-1}+1)(A^2-B)-\sqrt{B}^{J+3}<0.$$

Thus, since $J>6$ by (4.17), and using (4.4), we get

$$\begin{aligned}(A\sqrt{B}^{J-1}+1)(A^2-B)-\sqrt{B}^{J+3} &= \sqrt{B}^{J-1}(A^3-AB-B^2)+A^2-B\\ &< -\sqrt{B}^{J-1}+A^2-B<-B^2+A^2-B<0\end{aligned}$$

for $b\geq 7$. Thus, the lemma holds for $b\geq 7$. Direct calculations on small b show that Lemma 4.5 holds for $b\geq 3$. □

Thus, from Lemma 4.5 and (4.31) we see that $L=0$ where L is defined in (4.19). Putting this together with the consequences of Lemma 4.4, we see that (4.28) implies $h(x)$ is monic, the largest coefficient of $h(x)$ corresponds to the value of β_J, and all the coefficients of $h(x)$ are non-negative. The proofs of (i) and (ii) now follow directly from [10, page 172], which we reproduce here.

We continue to assume (4.28) and deduce as in [17] that $h(x)$ can be written as a sum over non-negative integers k of polynomials which are x^k times

$$\begin{aligned}\Big(\beta_0x^J+\beta_1x^{J-1}+\cdots+\beta_J\Big)x^{J+t'}+\Big(x^{J+t'-1}+x^{J+t'-2}+\cdots+x^J\Big)\beta_J\\ +\Big(\beta_J-\beta_0\Big)x^{J-1}+\Big(\beta_J-\beta_1\Big)x^{J-2}+\cdots+\Big(\beta_J-\beta_{J-1}\Big),\end{aligned}\tag{4.54}$$

where $t'=t'(k)$ is a non-negative integer. The values of k are taken so that there are no overlapping terms for different k and so that the coefficient of x^{k-1} in $h(x)$ is 0.

To show (i), we assume that strict inequality holds in (4.28). Observe that since $f(x)=(x^2-Ax+B)h(x)$ with $h(x)$ as described above, we see that $f(x)$ has a coefficient equal to

$$\begin{aligned}(\beta_J-\beta_1)-A(\beta_J-\beta_0)+B\beta_J &= (1-A+B)\beta_J-\beta_1+A\beta_0\\ &= (1-A+B)\beta_J,\end{aligned}$$

which corresponds to the coefficient of x^J when the expression in (4.54) is multiplied by $x^2 - Ax + B$. This contradicts our assumption, showing that $M(A, B) \geq (1 - A + B)\beta_J$.

To show that equality holds, we will exhibit a polynomial motivated by (4.54) with $t' = 0$. Consider

$$\begin{aligned} h_0(x) = \beta_0 x^{2J} + \beta_1 x^{2J-1} + \cdots + \beta_J x^J \\ + (\beta_J - \beta_0)x^{J-1} + (\beta_J - \beta_1)x^{J-2} + \cdots + (\beta_J - \beta_{J-1}). \end{aligned}$$

Applying (4.5), we deduce that

$$\begin{aligned} (x^2 - Ax + B)h_0(x) = x^{2J+2} + \Big((1 - A)\beta_J + B\beta_{J-1} - 1\Big)x^{J+1} \\ + (1 - A + B)\beta_J x^J + \cdots + (1 - A + B)\beta_J x^2 \\ + \Big((B - A)\beta_J + A\beta_{J-1} - B\beta_{J-2}\Big)x + B(\beta_J - \beta_{J-1}). \end{aligned}$$

Note that the coefficient of x here can be rewritten as $(1 - A + B)\beta_J$. Furthermore, the constant term of $(x^2 - Ax + B)h_0(x)$ can be rewritten as

$$(1 - A + B)\beta_J - \beta_J + \beta_{J+1}.$$

Since J was defined so that $\beta_{J-1} < \beta_J$ and $\beta_{J+1} < \beta_J$, we see that the maximal coefficient of $(x^2 - Ax + B)h_0(x)$ is $(1 - A + B)\beta_J$. The definition of $M(A, B)$ now implies that the equality given in (i) holds.

Now we prove (ii). Since (i) holds, we have $f(x) = (x^2 - Ax + B)h(x)$ where $h(x)$ is a sum over some non-negative integers k of polynomials which are x^k times polynomials of the form (4.54). We refer to the polynomial in (4.54) as part of $h(x)$. We begin by showing that with A, B and J fixed, but t' arbitrary, each part of $h(x)$ is divisible by

$$h_1(x) = \sum_{j=0}^{J} (\beta_{J-j} - \beta_{J-j-1})x^j,$$

where we recall from (4.5) that $\beta_{-1} = 0$. From this definition of $h_1(x)$, we have

$$\sum_{j=0}^{J} \beta_{J-j} x^j \equiv \sum_{j=0}^{J} \beta_{J-j-1} x^j \equiv \sum_{j=1}^{J} \beta_{J-j} x^{j-1} \pmod{h_1(x)}.$$

We deduce that the polynomial in (4.54) is

$$\begin{aligned}
&\left(\sum_{j=0}^{J} \beta_{J-j} x^j\right) x^{J+t'} + \left(\sum_{j=0}^{J+t'-1} x^j\right)\beta_J - \sum_{j=1}^{J} \beta_{J-j} x^{j-1} \\
&\qquad \equiv \left(\sum_{j=1}^{J} \beta_{J-j} x^{j-1}\right) x^{J+t'} + \left(\sum_{j=0}^{J+t'-1} x^j\right)\beta_J - \sum_{j=1}^{J} \beta_{J-j} x^{j-1} \\
&\qquad \equiv \left(\sum_{j=0}^{J} \beta_{J-j} x^j\right) x^{J+t'-1} + \left(\sum_{j=0}^{J+t'-2} x^j\right)\beta_J - \sum_{j=1}^{J} \beta_{J-j} x^{j-1} \\
&\qquad \equiv \left(\sum_{j=0}^{J} \beta_{J-j} x^j\right) x^{J+t'-2} + \left(\sum_{j=0}^{J+t'-3} x^j\right)\beta_J - \sum_{j=1}^{J} \beta_{J-j} x^{j-1} \\
&\qquad \vdots \\
&\qquad \equiv \sum_{j=0}^{J} \beta_{J-j} x^j - \sum_{j=1}^{J} \beta_{J-j} x^{j-1} \equiv 0 \pmod{h_1(x)}.
\end{aligned}$$

Thus, we obtain that each part of $h(x)$, and therefore $h(x)$ itself is divisible by $h_1(x)$. Using that $h(x)$ consists of at least one part as in (4.54) with $t' \geq 0$ and $J \geq 1$, we deduce that

$$h(b) \geq (\beta_0 b^J + \beta_1 b^{J-1} + \cdots + \beta_J) b^J > \beta_0 b^J + \beta_1 b^{J-1} + \cdots + \beta_J > h_1(b) > 1.$$

This means $h(b)$ is the integer $h_1(b)$ times an integer that is greater than 1. We deduce that $f(b) = g(b)h(b) = h(b)$ is composite. This finishes the proof of (ii).

Thus, for $n \in \{3, 4, 6\}$, we have bounds $\mathcal{B}_b^{(n)}$ such that if $f(x)$ is a polynomial with non-negative integer coefficients with $f(b)$ a prime, and has coefficients less than or equal to

$$\mathcal{B}_b^{(n)} = (1 - A + B)\beta_J, \tag{4.55}$$

then $f(x)$ cannot be divisible by $\Phi_n(x - b)$. To see how the explicit expression for $\mathcal{B}_n^{(n)}$ in (4.1) comes to be, we have, from the definition of β_j in (4.6),

$$\beta_j = \frac{1}{2i \operatorname{Im}(\zeta_n)} \left[(b + \zeta_n)^{j+1} - (b + \overline{\zeta}_n)^{j+1}\right]$$

$$= \frac{1}{2i\,\mathrm{Im}(\zeta_n)} \left[(b + \mathrm{Re}(\zeta_n) + i\,\mathrm{Im}(\zeta_n))^{j+1} - (b + \mathrm{Re}(\zeta_n) - i\,\mathrm{Im}(\zeta_n))^{j+1} \right].$$

Writing out the binomial expansion of each term and combining like terms yields

$$\begin{aligned}
\beta_j = \frac{1}{2i\,\mathrm{Im}(\zeta_n)} \Bigg[& \sum_{k=0}^{j+1} \binom{j+1}{k} (i\,\mathrm{Im}(\zeta_n))^k (b + \mathrm{Re}(\zeta_n))^{j+1-k} \\
& - \sum_{k=0}^{j+1} \binom{j+1}{k} (-i\,\mathrm{Im}(\zeta_n))^k (b + \mathrm{Re}(\zeta_n))^{j+1-k} \Bigg] \\
= \frac{1}{2i\,\mathrm{Im}(\zeta_n)} & \left[\sum_{k=0}^{j+1} \binom{j+1}{k} (b + \mathrm{Re}(\zeta_n))^{j+1-k} \left((i\,\mathrm{Im}(\zeta_n))^k - (-i\,\mathrm{Im}(\zeta_n))^k \right) \right] \\
= & \sum_{0 \le k \le \frac{j+1}{2}} \binom{j+1}{2k+1} (b + \mathrm{Re}(\zeta_n))^{j-2k} (-\mathrm{Im}(\zeta_n)^2)^k.
\end{aligned}$$

Recall that in (4.15), J was defined to be either $D_n - 1$ or $D_n - 2$. Evaluating β_j at $j = D_n - 1$ and $j = D_n - 2$, we get

$$\beta_{D_n-1} = \sum_{0 \le k \le \frac{D_n}{2}} \binom{D_n}{2k+1} (b + \mathrm{Re}(\zeta_n))^{D_n-2k-1} (-\mathrm{Im}(\zeta_n)^2)^k$$

and

$$\beta_{D_n-2} = \sum_{0 \le k \le \frac{D_n-1}{2}} \binom{D_n-1}{2k+1} (b + \mathrm{Re}(\zeta_n))^{D_n-2k-2} (-\mathrm{Im}(\zeta_n)^2)^k,$$

respectively. Thus,

$$\beta_J = \max_{i \in \{0,1\}} \left(\sum_{0 \le k \le \frac{D_n-i}{2}} \binom{D_n - i}{2k+1} (b + \mathrm{Re}\,(\zeta_n))^{D_n-2k-1-i} (-\mathrm{Im}\,(\zeta_n))^k \right). \tag{4.56}$$

Further, observe that

$$(1 - A + B) = \Phi_n\,(1 - b)\,, \tag{4.57}$$

for $n \in \{3, 4, 6\}$. Substituting (4.56) and (4.57) into (4.55) yields (4.1).

4.4 Comparing the Bounds and Establishing Theorem 1.6

We summarize what we have done so far. Let b be an integer greater than or equal to 2, and let $f(x)$ be in $\mathbb{Z}[x]$ with non-negative coefficients and $f(b)$ prime. We write

$f(x) = g(x)h(x)$ with $g(x) \not\equiv \pm 1$, $h(x) \not\equiv \pm 1$, and both $g(x)$ and $h(x)$ having positive leading coefficients. Using the fact that $f(b)$ is prime, we reduced our considerations to $g(b) = \pm 1$. We then showed that either $g(x)$, and hence $f(x)$, is divisible by at least one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, and $\Phi_6(x-b)$, or $g(x)$ has a root $\beta \in \mathcal{R}_b$. In the previous sections we established that if the coefficients of $f(x)$ are less than or equal to $\mathcal{B}_b^{(n)}$ defined in (4.55), then $f(x)$ does not have a root in common with $\Phi_n(x-b)$ for $n \in \{3, 4, 6\}$. In [26] it is shown that if the coefficients of $f(x)$ are less than or equal to $\mathcal{B}_b$, with $\mathcal{B}_b$ as in (4.2), then $f(x)$ does not have a root in the region $\mathcal{R}_b$.

Letting $M(b)$ be the minimum of these four bounds, then if the coefficients of $f(x)$ are less than or equal to $M(b)$, $f(x)$ is irreducible. In [26], J. Juillerat shows the following.

$$\begin{cases} \mathcal{B}_b^{(3)} < \mathcal{B}_b^{(4)} & \text{for } 2 \leq b \leq 5, \\ \mathcal{B}_b^{(4)} < \mathcal{B}_b^{(3)} & \text{for } b \geq 6, \\ \mathcal{B}_b^{(3)} < \mathcal{B}_b^{(6)} & \text{for } b \geq 2, \\ \mathcal{B}_b^{(3)} < \mathcal{B}_b & \text{for } b \geq 3, \\ \mathcal{B}_b^{(6)} < \mathcal{B}_b & \text{for } b \geq 70. \end{cases}$$

Having established these inequalities, we have that for b large enough, each of the following hold; if the coefficients of $f(x)$ are less than or equal to $\mathcal{B}_b^{(4)}$, then $f(x)$ is irreducible; if the coefficients of $f(x)$ are less than or equal to $\mathcal{B}_b^{(3)}$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$; if the coefficients of $f(x)$ are less than or equal to $\mathcal{B}_b^{(6)}$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$ or $\Phi_3(x-b)$; and if the coefficients of $f(x)$ are less than or equal to $\mathcal{B}_b$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$, $\Phi_3(x-b)$, or $\Phi_6(x-b)$.

With respect to Theorem 1.6, we note that $M_1(b) = \mathcal{B}_b^{(3)}$ and $M_2(b) = \mathcal{B}_b^{(4)}$, for $3 \leq b \leq 5$, and $M_1(b) = \mathcal{B}_b^{(4)}$ and $M_2(b) = \mathcal{B}_b^{(3)}$, for $b > 5$. Further, $M_3(b) = \mathcal{B}_b^{(6)}$, and $M_4(b) = \mathcal{B}_b$. This establishes Theorem 1.6.

Bibliography

[1] Andreas Alpers and Rob Tijdeman. "The two-dimensional Prouhet–Tarry–Escott problem". In: *Journal of Number Theory* 123.2 (2007), pp. 403–412. DOI: https://doi.org/10.1016/j.jnt.2006.07.001.

[2] Bernd Borchert, Pierre McKenzie, and Klaus Reinhardt. "Few Product Gates but Many Zeroes". In: *Chic. J. Theor. Comput. Sci.* 2013 (2013).

[3] Peter Borwein. *Computational Excursions in Analysis and Number Theory.* Springer-Verlag, 2002.

[4] Peter Borwein, Petr Lisonek, and Colin Percival. "Computational investigations of the Prouhet-Tarry-Escott Problem". In: *Math. Comput.* 72 (Oct. 2003), pp. 2063–2070. DOI: 10.1090/S0025-5718-02-01504-1.

[5] Peter Borwein, Petr Lisoněk, and Colin Percival. "Computational Investigations of the Prouhet-Tarry-Escott Problem". In: *Mathematics of Computation* 72.244 (2003), pp. 2063–2070.

[6] John Brillhart, Michael Filaseta, and Andrew Odlyzko. "On an irreducibility theorem of A. Cohn". In: *Canadian J. Math.* 33.5 (1981), pp. 1055–1059.

[7] Timothy Caley. "The Prouhet-Tarry-Escott problem". Doctor of Philosophy thesis. 2012.

[8] Timothy Caley. "The Prouhet-Tarry-Escott problem for Gaussian integers". In: *Mathematics of Computation* 82.282 (2013), pp. 1121–1137. ISSN: 00255718, 10886842. URL: http://www.jstor.org/stable/42002689.

[9] Ajai Choudhry. "Ideal solutions of the Tarry-Escott problem of degrees four and five and related Diophantine systems". In: *Enseign. Math.* 49 (2003), pp. 101–108.

[10] Morgan Cole, Scott Dunn, and Michael Filaseta. "Further irreducibility criteria for polynomials with non-negative coefficients". In: *Acta Arith.* 175.2 (2016), pp. 137–181.

[11] Leonard Eugnene Dickson. *History of the Theory of Numbers*. Vol. II. Dover Publications, 1971. Chap. 24.

[12] Gustave Dumas. "Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels". In: *J. Math. Pures Appl.* 2 (1906), pp. 191–258.

[13] Paul S. Dwyer. "The Computation of moments with the use of cumulative totals". In: *Ann. Math. Stat.* 9 (1938), pp. 288–304.

[14] Leonhard Euler. *Institutiones calculi differentialis cum eius usu in analysi finitorum ac Doctrina serierum*. Academiae imperialis scientiarum Petropolitanae, 1755.

[15] Michael Filaseta. "A further generalization of an irreducibility theorem of A. Cohn". In: *Canad. J. Math.* 34.6 (1982), pp. 1390–1395.

[16] Michael Filaseta. "Irreducibility criteria for polynomials with nonnegative coefficients". In: *Canad. J. Math.* 40.2 (1988), pp. 339–351.

[17] Michael Filaseta and Samuel Gross. "4959866698915122609810424451291 8". In: *J. Number Theory* 137 (2014), pp. 16–49.

[18] Michael Filaseta and Maria Markovich. "Newton polygons and the Prouhet–Tarry–Escott problem". In: *Journal of Number Theory* 174 (2017), pp. 384–400. DOI: https://doi.org/10.1016/j.jnt.2016.10.009.

[19] Joseph C Foster, Jacob Juillerat, and Jeremiah Southwick. "The irreducibility of polynomials arising from the study of Fourier coefficients of powers of the Dedekind-eta function". In: *Journal of Combinatorics and Number Theory* 10.3 (2018).

[20] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley, 1994. ISBN: 0-201-55802-5.

[21] Kálmán Győry, Lajos Hajdu, and Robert Tijdeman. "Irreducibility criteria of Schur-type and Pólya-type". In: *Monatshefte für Mathematik* 163 (2011), pp. 415–443.

[22] Harold Hardy and Edward M. Wright. *An Introduction to the Theory of Numbers*. 3rd ed. Oxford, at the Clarendon Press, 1954.

[23] Bernhard Heim, Florian Luca, and Markus Neuhauser. "Recurrence relations for polynomials obtained by arithmetic functions". In: *Int. J. Number Theory* 15.6 (2019), pp. 1291–1303.

[24] Bernhard Heim and Markus Neuhauser. "Log-concavity of recursively defined polynomials". In: *J. Integer Seq.* 22.1 (2019).

[25] Santos Hernández and Florian Luca. "Integer Roots Chromatic Polynomials of Non-Chordal Graphs and the Prouhet-Tarry-Escott Problem". In: *Graphs and Combinatorics* 21 (Sept. 2005), pp. 319–323. DOI: 10.1007/s00373-005-0617-0.

[26] Jacob Juillerat. "Widely digitally stable numbers and irreducibility criteria for polynomials with prime values". In: *Doctoral Dissertation* (2021).

[27] Howard Kleiman. "An note on the Tarry-Escott problem." In: *J. Reine Angew. Math.* 1975 (1975), pp. 48–51.

[28] Ernst E. Kummer. "Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen". In: *J. Reine Angew. Math.* 44 (1852), pp. 93–146.

[29] Adrien-Marie Legendre. *Théorie des Nombres*. Firmin Didot Frères, 1830.

[30] Edouard Lucas. "Théorie des Fonctions Numériques Simplement Périodiques". In: *Am. J. Math.* 1.2 (1878), pp. 184–196. ISSN: 00029327, 10806377. URL: http://www.jstor.org/stable/2369308.

[31] Roy Maltby. "Pure product polynomials and the Prouhet-Tarry-Escott problem". In: *Math. Comput.* 66 (1997), pp. 1323–1340.

[32] Ernst E. Newman. "An identity for the coefficients of certain modular forms". In: *J. Lond. Math. Soc.* 30 (1955), pp. 488–493.

[33] Ivan Niven. *Irrational Numbers*. Mathematical Association of America, 1956. DOI: 10.5948/9781614440116.

[34] Georg Pólya and Gabor Szegő. *Aufgaben und Lehrsätze aus der Analysis. Band II: Funktionentheorie, Nullstellen, Polynome Determinanten, Zahlentheorie*. Vierte Auflage, Heidelberger Taschenbücher, Band 74. Springer-Verlag, Berlin-New York, 1971, xii+407 pp. (loose errata).

[35] Victor V. Prasolov. *Polynomials*. Vol. 11. Algorithms and Computation in Mathematics. Springer-Verlag Berlin Heidelberg, 2004. ISBN: 978-3-540-40714-0.

[36] Eugene Prouhet. "Mémoire sur quelques relations entre les puissances des nombres". In: *C. R. Acad. Sci. Paris* srie I.33 (1851).

[37] Maruti Ram Murty. "Prime numbers and irreducible polynomials". In: *Amer. Math. Monthly* 109.5 (2002), pp. 452–458.

[38] Elmer Rees and Christopher Smyth. "On the constant in the tarry-escott problem". In: *Lecture Notes in Mathematics 1415* (1990), pp. 196–208. DOI: 10.1007/BFb0084888.

[39] Arto Salomaa. "Subword balance, position indices and power sums". In: *J. Comput. Syst. Sci.* 76 (2010), pp. 861–871.

[40] Jeremiah Southwick. "Two inquiries related to the digits of prime numbers". In: *Doctoral Dissertation* (2020).

[41] J. Worpitzky. "Studien über die Bernoullischen und Eulerschen Zahlen." In: *J. Reine Angew. Math.* 94 (1883), pp. 203–232.

[42] Edward M. Wright. "On Tarry's problem (I)". In: *Quart. J. Math.* 6 (1935), pp. 261–267.

[43] Edward M. Wright. "Prouhet's 1851 Solution of the Tarry-Escott Problem of 1910". In: *American Mathematical Monthly* 66 (1959), pp. 199–201.

[44] Edward M. Wright. "The Tarry-Escott and the "easier" Waring problems". In: *J. Reine Angew. Math.* 311/312 (1979), pp. 170–173.