1-1-2013

Selected Research In Covering Systems of the Integers and the Factorization of Polynomials

Joshua Harrington
University of South Carolina - Columbia

Selected Research in Covering Systems of the Integers and the Factorization of Polynomials

by

Joshua Harrington

Bachelor of Arts
Shippensburg University 2009

Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosphy in

Mathematics

College of Arts and Sciences

University of South Carolina

2013

Accepted by:

Michael Filaseta, Major Professor

Ognian Trifonov, Committee Member

Matthew Boylan, Committee Member

Stephen Dilworth, Committe Member

Marco Valtorta, External Examiner

Lacy Ford, Vice Provost and Dean of Graduate Studies

Acknowledgments

There are many people that have played important roles in the events leading to the completion of this dissertation. Most of them fit into two categories. There are those that have helped me along mathematically and there are those that have helped motivate and inspire me.

First, I would like to give thanks to those that have helped me mathematically. For their collaboration in three of the four papers in this dissertation, I owe my greatest thanks to Lenny Jones, Carrie Finch, Michael Filaseta, Daniel White, and Andrew Vincent. I owe a special thanks to Michael, my advisor. He sat with me for many hours and provided much needed direction and guidance to see that this dissertation get finished. I feel like I was often a demanding and probably difficult student, and I thank him for his time and patience. I also owe thanks to Scott Dunn and Kenny Brown, with whom I've published a paper not presented in this dissertation. In addition to my coauthors, I would also like to show my gratitude to Sam Gross, Bill Kay, Aaron Dutle, John Webb, and John Schulte. In the last four years I have turned to each of these guys with many questions, mathematical or otherwise, and they always tried to provide answers when they could.

Secondly, I owe an immense amount of gratitude to those that have helped motivate and inspire me, both in school, and in life. First, I would like to thank my wife, Heather, for believing in me, even when I did not. I can only imagine the amount of patience and understanding that a woman must have to help and encourage their husband through graduate school. She is, by far, the strongest and most wonderful woman that I know, or have ever known. Next, I would like to thank my daughters,

Taylor and Ava. At eight and six years old, they can't possibly imagine the ways that they've helped make this dissertation, and my dreams come true. Third, I'd like to thank parents, Twyla and David, and my brother, Jeremy. These are the three people that have been in my life since my earliest memories. I thank them for the laughs, for their understanding, and for their faith in me. I would also like to thank Andy and Lisa, two people who will probably never know just how much they've helped me get where I am today.

Finally, I give a second, and special thanks to Lenny Jones. Aside from being a coauthor, he has been a great friend and an invaluable mentor to me for the past six years. It was Lenny who first saw the mathematical potential within me, and without him, going to graduate school may have remained nothing but a dream.

Abstract

In 1960, Sierpiński proved that there exist infinitely many odd positive integers k such that $k \cdot 2^n + 1$ is composite for all positive integers n. Such integers are known as Sierpiński numbers. Letting $f(x) = ax^r + bx + c \in \mathbb{Z}[x]$, Chapter 2 of this document explores the existence of integers k such that $f(k)2^n + d$ is composite for all positive integers n. Chapter 3 then looks into a polynomial variation of a similar question. In particular, Chapter 3 addresses the question, for what integers d does there exist a polynomial $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -d$ such that $f(x)x^n + d$ is reducible for all positive integers n. The last two chapters of the document then explore the reducibility and factorization of polynomials taking on a prescribed form. Specifically, Chapter 4 addresses the reducibility and factorization of polynomials of the form $x^n + cx^{n-1} + d \in \mathbb{Z}[x]$, while Chapter 5 addresses the reducibility and factorization of polynomials of the more general form $f(x)x^n + g(x) \in \mathbb{Z}[x]$.

Table of Contents

Chapter 1

An Introduction to Terminology

The work in each chapter of this document is intended to be independent of previous chapters. As such, each chapter contains its own individual introduction and concluding remarks. That being said, we present here some definitions and background to help guide the reader.

A *covering system* (or *covering*) of the integers is a finite system of congruences $n \equiv r_i \pmod{m_i}$, such that every integer satisfies at least one of the congruences. For example, it is easily checked that the system of congruences

$$\begin{aligned} n &\equiv 0 \pmod 3 \\ n &\equiv 1 \pmod 3 \\ n &\equiv 2 \pmod 3 \end{aligned}$$

forms a covering of the integers. Perhaps a less trivial example of a covering system is

$$\begin{aligned} n &\equiv 0 \pmod 2 \\ n &\equiv 0 \pmod 3 \\ n &\equiv 1 \pmod 4 \\ n &\equiv 1 \pmod 6 \\ n &\equiv 11 \pmod{12}. \end{aligned}$$

We define a *Sierpiński number* to be an odd integer k such that $k \cdot 2^n + 1$ is composite for all positive integers n. The existence of such numbers was proven by Sierpiński [23] in 1960. It was earlier shown by Riesel [19] in 1956 that there exists infinitely many odd integers k such that $k \cdot 2^n - 1$ is composite for all positive integers

n. Letting $f(x) = ax^r + bx + c$ for certain integers a, b, c, and r, in Chapter 2 we make use of covering systems to show that for various values of d there exists infinitely many integers k such that $f(k) \cdot 2^n + d$ is composite for all positive integers n.

The last three chapters of the document will focus on the reducibility and factorization of polynomials. We say that a polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ (or irreducible over $\mathbb{Z}$) provided that $f(x) \not\equiv \pm 1$ and if $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$, then either $g(x) \equiv \pm 1$ or $h(x) \equiv \pm 1$. If $f(x) \in \mathbb{Z}[x]$ is not irreducible in $\mathbb{Z}[x]$ and $f(x) \not\equiv \pm 1$, then we say that $f(x)$ is reducible in $\mathbb{Z}[x]$. Similarly, we say that a polynomial $f(x) \in \mathbb{Q}[x]$ is irreducible in $\mathbb{Q}[x]$ (or irreducible over $\mathbb{Q}$) provided that $f(x)$ is not constant and if $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{Q}[x]$, then either $g(x)$ or $h(x)$ is constant. If $f(x) \in \mathbb{Q}[x]$ is not irreducible in $\mathbb{Q}[x]$ and $f(x)$ is not constant, then we say that $f(x)$ is reducible in $\mathbb{Q}[x]$. In Chapter 3 we investigate the following question.

Question. *For what integers d does there exist a polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -d$ and $f(x)x^n + d$ is reducible in $\mathbb{Q}[x]$ for all integers $n \geq 0$?*

We include the restriction $f(1) \neq -d$ to avoid trivial solutions. Let $\mathcal{S}$ be the set of integers for which there exists a polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -d$ and $f(x)x^n + d$ is reducible over the rationals for all integers $n \geq 0$. It was shown by Filaseta [8] that if $d \equiv 0 \pmod 4$, then $d \in \mathcal{S}$. Jones [17] later showed that there are infinitely many $d \in \mathcal{S}$ with $d \equiv 2 \pmod 4$. We will show in Chapter 3 that if $d \equiv 0 \pmod 2$, then $d \in \mathcal{S}$.

The last two chapters will address the reducibility and factorization of polynomials in $\mathbb{Z}[x]$ taking on a prescribed form. Specifically, chapter 4 addresses the reducibility and factorization of polynomials of the form $x^n + cx^{n-1} + d \in \mathbb{Z}[x]$, while chapter 5 addresses the reducibility and factorization of polynomials of the more general form $f(x)x^n + g(x) \in \mathbb{Z}[x]$.

Much of the work in this document was completed with various collaborators. All but the last chapter appear as articles in professional journals. Chapter 2 is joint work with Lenny Jones and Carrie Finch and is published in Journal of Number Theory [13]. Chapter 3 is joint work with Michael Filaseta and is published in Acta Arithmetica [11]. The fourth chapter is work solely of the author's and is published in International Journal of Number Theory [14]. Finally, Chapter 5 is joint work with Andrew Vincent and Daniel White.

Chapter 2

Nonlinear Sierpiński and Riesel Numbers

2.1 Introduction

The following concept, originally due to Erdős [7], is instrumental in establishing all results in this article.

Definition 2.1. A *covering* of the integers is a finite system of congruences $n \equiv z_i \pmod{m_i}$ such that every integer satisfies at least one of the congruences.

Quite often when a covering is used to solve a problem, there is a set of prime numbers associated with the covering. In the situations occurring in this article, for each congruence $n \equiv z_i \pmod{m_i}$ in the covering, there exists a corresponding prime p_i, such that $2^{m_i} \equiv 1 \pmod{p_i}$, and $p_j \neq p_i$ for all $j \neq i$. Because of this correspondence, we indicate the covering using a set $\mathcal{C}$ of ordered triples (z_i, m_i, p_i). We abuse the definition of a covering slightly by referring to the set $\mathcal{C}$ as a "covering".

In 1960, using a particular covering, Sierpiński [23] published a proof of the fact that there exist infinitely many odd positive integers k such that $k \cdot 2^n + 1$ is composite for all natural numbers n. Any such value of k is called a *Sierpiński number*. Since then, several authors [2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 17] have investigated generalizations and variations of this result. We should also mention a paper of Riesel [19], which actually predates the paper of Sierpiński, in which Riesel proves a similar result for the sequence of integers $k \cdot 2^n - 1$. We include a proof of Sierpiński's original theorem since it provides an easy introduction to the techniques used in this paper.

Theorem 2.1 (Sierpiński [23])**.** *There exist infinitely many odd positive integers k such that $k \cdot 2^n + 1$ is composite for all integers $n \geq 1$.*

Proof. Consider the covering

$$\begin{aligned}\mathcal{C} = \{&(1,2,3),(2,4,5),(4,8,17),(8,16,257),\\ &(16,32,65537),(32,64,641),(0,64,6700417)\}.\end{aligned}$$

To illustrate exactly how $\mathcal{C}$ is used to prove this result, start with the triple $(1,2,3) \in \mathcal{C}$. We want $k \cdot 2^n + 1 \equiv 0 \pmod 3$ when $n \equiv 1 \pmod 2$. But $k \cdot 2^n + 1 \equiv k \cdot 2 + 1 \pmod 3$ when $n \equiv 1 \pmod 2$, which tells us that $k \cdot 2^n + 1$ is divisible by 3 if $k \equiv 1 \pmod 3$. Continuing in this manner gives us the system

$$\begin{aligned} k &\equiv 1 \pmod 3\\ k &\equiv 1 \pmod 5\\ k &\equiv 1 \pmod{17}\\ k &\equiv 1 \pmod{257}\\ k &\equiv 1 \pmod{65537}\\ k &\equiv 1 \pmod{641}\\ k &\equiv -1 \pmod{6700417}. \end{aligned}$$

Since we require that k be odd, we add the congruence $k \equiv 1 \pmod 2$ to our system, and then using the Chinese remainder theorem, we get the solution

$$k \equiv 155113807464625933 81 \pmod{2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417}.$$

Therefore, for any integer $n \geq 1$ and any such k, we have that at least one prime from the set $\{3, 5, 17, 257, 641, 65537, 6700417\}$ is a divisor of $k \cdot 2^n + 1$. □

In this article we are concerned with variations of Theorem 2.1 which are non-linear in nature, replacing the variable k with a nonlinear polynomial in k. The investigation into such nonlinear situations began with Chen [5], who showed that for

any positive integer $r \not\equiv 0, 4, 6, 8 \pmod{12}$, there exist infinitely many odd positive integers k such that $k^r \cdot 2^n + d$ is composite for all integers $n \geq 1$, where $d \in \{-1, 1\}$. He conjectured that the result is true for all positive integers r. Recently, Filaseta, Finch and Kozek [9] have been able to lift all restrictions on r when $d = 1$ to verify Chen's conjecture in this case, and they showed that the conjecture is also true for $r = 4$ and $r = 6$ when $d = -1$. (More recently, Finch, Groth, Jones and Mugabe have verified Chen's conjecture for $r = 8$ and $r = 12$ when $d = -1$.) In their paper [9], Filaseta, Finch and Kozek also asked if infinitely many positive integers k can be found such that $f(k) \cdot 2^n + 1$ is composite for all integers $n \geq 1$, where $f(x)$ is any nonconstant polynomial in $\mathbb{Z}[x]$. In this article we focus on the situation when $f(x) = ax^r + bx + c \in \mathbb{Z}[x]$, where $a \geq 1$. If, for such a particular polynomial $f(x)$ and an integer d, we can prove there exist infinitely many positive integers k such that $f(k) \cdot 2^n + d$ is composite for all integers $n \geq 1$, then we say that particular value of r can be *captured*. The *r-density* for a particular polynomial $f(x)$ is simply the density of the set of captured values of r. Our main focus in this article is when $d \in \{-1, 1\}$. For any nonlinear polynomial $f(x)$, we call the integer k a *nonlinear Sierpiński number* if $f(k) \cdot 2^n + 1$ is composite for all integers $n \geq 1$, and a *nonlinear Riesel number* if $f(k) \cdot 2^n - 1$ is composite for all integers $n \geq 1$. A list of the results established in this article follows.

Theorem 2.2. *Let $f(x) = x^r + x + c \in \mathbb{Z}[x]$, where $0 \leq c \leq 100$.*

- *(Nonlinear Sierpiński Numbers) For any positive integer r and any*

$$\begin{aligned} c \in \{&1, 3, 4, 5, 6, 8, 10, 11, 12, 15, 17, 18, 19, 20, 22, 26, \\ &27, 29, 31, 32, 34, 38, 40, 41, 45, 46, 47, 48, 50, 53, \\ &55, 57, 59, 60, 62, 64, 67, 68, 71, 74, 76, 78, 81 \\ &82, 83, 85, 87, 88, 89, 92, 94, 95, 96, 97\}, \end{aligned}$$

  there exist infinitely many positive integers k such that $f(k) \cdot 2^n + 1$ is composite for all integers $n \geq 1$.

- *(Nonlinear Riesel Numbers) For any positive integer r, and any*

$$\begin{aligned} c \in \{&2, 5, 8, 9, 11, 12, 13, 14, 16, 17, 20, 21, 22, 23, 24 \\ &27, 29, 30, 32, 35, 36, 37, 38, 39, 40, 41, 44, 50, 51, \\ &53, 56, 58, 59, 60, 61, 62, 65, 66, 67, 68, 69, 71, \\ &72, 74, 77, 80, 81, 82, 83, 84, 85, 86, 87, 89, \\ &92, 93, 95, 97, 98\}, \end{aligned}$$

  there exist infinitely many positive integers k such that $f(k) \cdot 2^n - 1$ is composite for all integers $n \geq 1$.

Theorem 2.3. *Let $f(x) = ax^r + c \in \mathbb{Z}[x]$, where $a \geq 1$, and let d be an odd integer. If a is not divisible by any element in the set of primes*

$$\begin{aligned} \{&3, 5, 7, 11, 13, 17, 19, 37, 41, 73, 257, 641, 65537, \\ &286721, 3602561, 96645260801, 67280421310721\}, \end{aligned}$$

then there exist infinitely many positive integers k such that $f(k) \cdot 2^n + d$ is composite for all integers $n \geq 1$, either when $r \equiv \pm 1 \pmod 6$, or when both $r \equiv 3 \pmod 6$ and r is not divisible by any element in the set of primes

$$\{5, 7, 11, 13, 29, 47, 373, 433, 23669, 2998279\}.$$

Theorem 2.4. *Let* $f(x) = x^r + 1$.

- *(Nonlinear Sierpiński Numbers) There exist infinitely many positive integers* k *such that* $f(k) \cdot 2^n + 1$ *is composite for all integers* $n \geq 1$ *when either* $r \not\equiv 0 \pmod 8$ *and* $r \not\equiv 0 \pmod{17449}$*, or when* $r \not\equiv z \pmod{30}$ *where* $z \in \{0, 6, 12, 15, 18, 24\}$.

- *(Nonlinear Riesel Numbers) There exist infinitely many positive integers* k *such that* $f(k) \cdot 2^n - 1$ *is composite for all integers* $n \geq 1$ *when* $r \not\equiv 0 \pmod 6$.

Theorem 2.5.

- *Let* $f(x) = x^r + 1$. *There exists a set* S *of* r*-density 8/33, such that for each* $r \in S$*, there exist infinitely many positive integers* k *for which* $f(k)$ *is odd, and both* $f(k) \cdot 2^n + 1$ *and* $f(k) \cdot 2^n - 1$ *are composite for all integers* $n \geq 1$.

- *Let* $f(x) = x^r + x + 1$. *There exists a set* S *with* r*-density approximately .47, such that for each* $r \in S$*, there exist infinitely many positive integers* k *for which* $f(k)$ *is odd, and both* $f(k) \cdot 2^n + 1$ *and* $f(k) \cdot 2^n - 1$ *are composite for all integers* $n \geq 1$.

For each positive integer $c \leq 100$ not listed in the Sierpiński part of Theorem 2.2, the r-density is no smaller than $2/3$, and for each positive integer $c \leq 100$ not listed in the Riesel part, the r-density is no smaller than .749. Since the r-densities for the Riesel part and Sierpiński part of Theorem 2.2 are similar, we provide in Table 2.1 the approximate r-densities only for the Sierpiński part. The value of $c = 100$ here is simply an arbitrary stopping point. The methods used in the proof of Theorem 2.2 can be applied to larger values of c as well as other polynomials.

Theorem 2.3 is a more general theorem in that the values of the parameters a, c and d are not fixed. In some sense, Theorem 2.3 generalizes the work of Filaseta, Finch and Kozek [9] since their work is the special case of $a = d = 1$ and $c = 0$ in

Theorem 2.3. However, we are not able to achieve an r-density of 1 in this case using our methods. In the specific case of $a = c = d = 1$ in Theorem 2.3, the r-density is slightly less than .42. Applying the techniques used to prove Theorem 2.2 to this special case, this density improves to 2/3. The proof of the first part of Theorem 2.4 uses a different approach and improves this density to slightly more than .94. Although we do not provide the details here, it can be shown that by combining all of these results, the r-density in this case can be improved to slightly less than .96.

Theorem 2.5 addresses the following natural question. Given a specific polynomial $f(x)$, do there exist infinitely many positive integers k such that both $f(k) \cdot 2^n + 1$ and $f(k) \cdot 2^n - 1$ are simultaneously composite for all integers $n \geq 1$? That is, are there positive integers that are both nonlinear Sierpiński numbers and nonlinear Riesel numbers? For certain polynomials and sets with positive r-density, this question is answered affirmatively in Section 2.3 where the proof of Theorem 2.5 is given.

Remark 2.1. Computer computations in this article were done using either MAGMA, Maple or a C++ program written by Professor Simon Levy in the computer science department at Washington and Lee University.

2.2 Proofs of the Theorems

We begin with some preliminaries from finite group theory that are useful in establishing some of the main results in this paper.

Lemma 2.1. *Let G be a finite abelian group, and suppose that r is a positive integer such that* $\gcd(|G|, r) = 1$. *Then the map $\theta_r : G \longrightarrow G$ defined by $\theta_r(x) = x^r$ is an automorphism of G.*

Proof. Since G is abelian, θ_r is clearly a homomorphism. The kernel of θ is $K = \{x \in G \mid x^r = 1\}$. Since the order of any $x \in K$ divides both r and $|G|$, it follows that K is trivial, which proves the lemma. □

The following corollary is immediate from Lemma 2.1.

Corollary 2.1. *Let p be a prime, and let $(\mathbb{Z}_p)^*$ denote the group of units modulo p. For any positive integer r with $\gcd(r, p-1) = 1$, let θ_r be the automorphism of $(\mathbb{Z}_p)^*$ defined by $\theta_r(x) = x^r$, and let $\widehat{\theta}_r$ be the extension of the map θ_r to the commutative multiplicative monoid $\mathbb{Z}_p$ by defining $\widehat{\theta}_r(0) = 0$. If $\gcd(r, p-1) = 1$, then $\widehat{\theta}_r$ is a bijection on $\mathbb{Z}_p$.*

The next corollary extends the previous ideas to generate subsets S of $\mathbb{Z}_p$ which are fixed under $\widehat{\theta}_r$ for certain values of r.

Corollary 2.2. *Let p be a prime, and suppose that $p - 1 = q^z m$, where q is a prime such that $m \not\equiv 0 \pmod{q}$. Let*

$$S = \widehat{\theta}_{q^z}(\mathbb{Z}_p) = \left(\widehat{\theta}_q\right)^z (\mathbb{Z}_p).$$

Then $\widehat{\theta}_q(S) = S$. Moreover, each such set S is nonempty since $0 \in S$.

Proof. The kernel of the homomorphism θ_q on $\theta_{q^z}\left((\mathbb{Z}_p)^*\right)$ is trivial. □

The following lemma is used in the proofs of both Theorem 2.3 and Theorem 2.4.

Lemma 2.2. *Let $\mathcal{C} = \{(z_i, m_i, p_i)\}$ be a covering. Let r be a positive integer such that $\gcd(r, p_i - 1) = 1$ for all i, and let $a > 0$ be an integer that is not divisible by p_i for all i. Then, for any integers c and d, with d odd, there exist infinitely many positive integers k such that $(a \cdot k^r + c) \cdot 2^n + d$ is composite for all integers $n \geq 1$.*

Proof. Let $(z_i, m_i, p_i) \in \mathcal{C}$. For each i, $\widehat{\theta}_r$ is a bijection on $\mathbb{Z}_{p_i}$ by Corollary 2.1, and since a is invertible mod p_i, we have that there exists $v_i \in \mathbb{Z}_{p_i}$ such that

$$v_i^r \equiv a^{-1}\left(-d \cdot 2^{-n} - c\right) \equiv a^{-1}\left(-d \cdot 2^{-z_i} - c\right) \pmod{p_i}.$$

Then we use the Chinese remainder theorem to solve the system of congruences $k \equiv v_i \pmod{p_i}$. Since $\mathcal{C}$ is a covering, we have shown that, for any positive integer n, the

term $(a \cdot k^r + c) \cdot 2^n + d$ is divisible by at least one prime p_i, which completes the proof of the lemma. $\square$

Theorem 2.2

We first outline in more generality the procedure used in the proof of Theorem 2.2. Let $\mathcal{C} = \{(z_i, m_i, p_i)\}$ be a covering, where p_i is odd for all i. Recall that $2^{m_i} \equiv 1 \pmod{p_i}$, and that no prime p_i is repeated. Then $2^n \equiv 2^{z_i} \pmod{p_i}$ when $n \equiv z_i \pmod{m_i}$. Define $L_{\mathcal{C}} := \operatorname{lcm}_i \{p_i - 1\}$. Note that $L_{\mathcal{C}}$ is independent of the list of residues in $\mathcal{C}$. Let

$$f(x) = x^r + x^e + a_{e-1}x^{e-1} + \cdots + a_1 x + a_0 \tag{2.2.1}$$

be a nonconstant polynomial with integer coefficients, where e is a fixed nonnegative integer. The coefficient on x^e is 1 to exclude the possibility that $f(x) \equiv 0 \pmod{p_i}$ for some i, when $r \leq e$. We wish to determine the values of r for which there exist infinitely many positive integers k such that $s_n := f(k) \cdot 2^n + d$ is composite for all integers $n \geq 1$, for a fixed $d \in \{-1, 1\}$. We use $\mathcal{C}$ to examine the behavior of s_n modulo each p_i, and then piece together the results using the Chinese remainder theorem. We only need to check values of r with $0 \leq r \leq L_{\mathcal{C}} - 1$. We proceed as follows. Let r be a fixed integer with $0 \leq r \leq L_{\mathcal{C}} - 1$. Then, for each i, we calculate the values $f(k)$, with $0 \leq k \leq p_i - 1$, to determine whether there is a k such that $f(k) \equiv -d2^{-z_i} \pmod{p_i}$. If so, then we know there exists β_i such that $k \equiv \beta_i \pmod{p_i}$ is a solution to $s_n \equiv 0 \pmod{p_i}$ when $n \equiv z_i \pmod{m_i}$. Continuing in this manner, if β_i exists for each i, then we can use the Chinese remainder theorem to solve the resulting system of congruences in k. Thus, in this case, we have captured that particular value of r, which contributes a value of $1/L_{\mathcal{C}}$ to the total density. This process can be repeated for every list of residues for which a covering exists. In addition, this process can be repeated for coverings with different lists of moduli. To

combine all of these results in a sensible manner, one must take care since the values of r captured using one list of moduli must be "meshed" with the values of r captured using a different list of moduli. This can be done by examining values of $r \pmod{\mathcal{L}}$, where $\mathcal{L} = \operatorname{lcm}_{\mathcal{C}} L_{\mathcal{C}}$, for all coverings $\mathcal{C}$ under consideration. Then the density of the set of captured values of r will be the cardinality of the union of these various sets divided by $\mathcal{L}$. We call this density a *Sierpiński r-density* or *Riesel r-density* for this particular polynomial $f(x)$, depending on whether $d = 1$ or $d = -1$, respectively.

Remark 2.2. Note that if $a_0 \equiv 1 \pmod 2$ or $a_{e-1} + \cdots + a_1 + a_0 \equiv 1 \pmod 2$ in (2.2.1), then adding, respectively, the additional congruence $k \equiv 0 \pmod 2$ or $k \equiv 1 \pmod 2$ to the system of congruences for k will ensure that $f(k)$ is odd.

Proof of Theorem 2.2. Consider the following lists:

$$\begin{aligned} M_1 &= [2, 3, 4, 9, 12, 18, 36] & P_1 &= [3, 7, 5, 73, 13, 19, 37] \\ M_2 &= [2, 3, 4, 8, 12, 24] & P_2 &= [3, 7, 5, 17, 13, 241] \\ M_3 &= [2, 3, 4, 5, 10, 12, 15, 20, 60] & P_3 &= [3, 7, 5, 31, 11, 13, 151, 41, 61], \end{aligned}$$

where each M_j is a list of moduli to be used to construct a covering, and P_j is the list of corresponding primes. Here $\mathcal{L} = 3600$. Let N_j be the total number of coverings having M_j as the list of moduli. Then $N_1 = 144$, $N_2 = 48$ and $N_3 = 2880$. For each $d \in \{-1, 1\}$, apply the procedure outlined above to the polynomials $f(x) = x^r + x + c$, with $0 \leq c \leq 100$, using these 3072 coverings to get the results contained in the statement of the theorem. □

It may be that not all lists of moduli M_j above, or all coverings for a particular list of moduli, are needed to achieve the results for a certain value of c in Theorem 2.2. For example, it can be shown for $c = 1$ that only 24 of the coverings with the moduli M_1 are needed to prove that the Sierpiński r-density is 1.

Table 2.1 Approximate Sierpiński r-densities smaller than 1 using Theorem 2.2

c	r-density	c	r-density	c	r-density	c	r-density
0	0.8247	27	0.9997	51	0.8333	72	0.8314
2	0.8333	28	0.8333	52	0.9164	73	0.9994
3	0.9997	30	0.8331	54	0.7500	75	0.9167
7	0.8333	33	0.9942	56	0.8333	77	0.8333
9	0.6667	34	0.9997	57	0.9997	79	0.8333
10	0.9997	35	0.8333	58	0.8331	80	0.9969
13	0.8314	36	0.9167	60	0.9997	81	0.9997
14	0.8331	37	0.8331	61	0.9942	84	0.6667
15	0.9997	38	0.9997	62	0.9997	86	0.8333
16	0.8333	39	0.7500	63	0.8333	87	0.9997
20	0.9997	40	0.9997	65	0.8331	90	0.9167
21	0.8333	42	0.7500	66	0.9167	91	0.8331
22	0.9997	43	0.9975	67	0.9997	93	0.8331
23	0.8333	44	0.8319	69	0.7494	98	0.8331
24	0.7478	49	0.8333	70	0.8317	99	0.7497
25	0.9769					100	0.8286

Theorem 2.3

The strategy here is to use Lemma 2.2 exclusively to determine which values of r can be captured in the general situation $(a \cdot k^r + c) \cdot 2^n + d$, where $a, c, d \in \mathbb{Z}$, with $a > 0$ and d odd. However, since a corresponding odd prime p_i in any covering is such that $p_i - 1 \equiv 0 \pmod 2$, Lemma 2.2 alone is ineffective in addressing any even value of r.

Remark 2.3. Note that if $c \equiv 1 \pmod 2$ or $a + c \equiv 1 \pmod 2$, then adding, respectively, the additional congruence $k \equiv 0 \pmod 2$ or $k \equiv 1 \pmod 2$ to the system of congruences for k will ensure that $f(k) = a \cdot k^r + c$ is odd.

Proof of Theorem 2.3. Suppose first that $r \equiv \pm 1 \pmod 6$, and consider the covering

$$\begin{aligned}\mathcal{C}_1 = \{&(1, 2, 3), (0, 3, 7), (0, 4, 5), (5, 9, 73),\\ &(10, 12, 13), (2, 18, 19), (26, 36, 37)\}.\end{aligned}$$

For each $(z_i, m_i, p_i) \in \mathcal{C}_1$, note that $a \not\equiv 0 \pmod{p_i}$ and that $p_i - 1 \not\equiv 0 \pmod q$ for any prime $q \geq 5$. Since $\gcd(r, 6) = 1$, the first part of the theorem is established.

Now suppose that $r \equiv 3 \pmod 6$, and consider the covering

$$\begin{aligned}\mathcal{C}_2 = \{&(1, 2, 3), (0, 4, 5), (2, 8, 17), (6, 10, 11), (14, 16, 257), (18, 20, 41),\\ &(6, 32, 65537), (22, 64, 641), (118, 128, 67280421310721),\\ &(310, 320, 3602561), (182, 640, 286721), (54, 640, 96645260801)\}.\end{aligned}$$

It is easy to check using a computer that $\mathcal{C}_2$ is indeed a covering. For each $(z_i, m_i, p_i) \in \mathcal{C}_2$, note that $a \not\equiv 0 \pmod{p_i}$. In addition, the union of the sets of odd prime divisors of $p_i - 1$ for all i is precisely

$$\{5, 7, 11, 13, 29, 47, 373, 433, 23669, 2998279\}.$$

Invoking Lemma 2.2 completes the proof. □

Theorem 2.4

While the hypotheses of Lemma 2.2 are sufficient in addressing a particular value of r, they are not necessary, as we see in Theorem 2.4 where we consider the special case of $f(x) = x^r + 1$.

Proof of Theorem 2.4. We first prove the Sierpiński half of the theorem. Suppose that r is not divisible by either 8 or 17449, and consider the covering

$$\begin{aligned}\mathcal{C} =&\{(0,2,3),(1,4,5),(3,8,17),(7,16,257),(15,32,65537),\\ &(31,64,641),(63,64,6700417)\}.\end{aligned}$$

The covering $\mathcal{C}$ gives rise to the system of congruences

$$\begin{aligned} k^r &\equiv 1 \pmod 3\\ k^r &\equiv 1 \pmod 5\\ k^r &\equiv 1 \pmod{17}\\ k^r &\equiv 1 \pmod{257}\\ k^r &\equiv 1 \pmod{65537}\\ k^r &\equiv 1 \pmod{641}\\ k^r &\equiv -3 \pmod{6700417}. \end{aligned}$$

It is clear that $k \equiv 1 \pmod{p_i}$ is a solution to each of the first six congruences above. To see that the last congruence has a solution, first note that

$$(-3)^{\frac{6700416}{12}} \equiv 1 \pmod{6700417}.$$

Let $d = \gcd(r, 6700416)$. Since $r \not\equiv 0 \pmod 8$ and $r \not\equiv 0 \pmod{17449}$, we have that d divides 12. Thus,

$$1 \equiv 1^{\frac{12}{d}} \equiv (-3)^{\frac{6700416}{d}} \pmod{6700417}.$$

Hence, it follows from the generalization of Euler's criterion for rth power residues [18] that there exists a value k such that

$$k^r \equiv -3 \pmod{6700417}.$$

Using the Chinese remainder theorem completes the proof for these values of r.

To establish the second part of the Sierpiński half of Theorem 2.4, first consider the covering

$$\mathcal{C}_1 = \{(1,2,3),(1,3,7),(2,4,5),(3,9,73),(8,12,13),(0,18,19),(24,36,37)\}.$$

Since $p_i - 1 \equiv 0 \pmod 2$ for each p_i in $\mathcal{C}_1$, we see that θ_2 is not an automorphism of $(\mathbb{Z}_{p_i})^*$. However, for each i, by Corollary 2.2, there exists a nonempty subset S_i of $\mathbb{Z}_{p_i}$ such that

$$\left(\widehat{\theta}_2\right)^j (S_i) = \widehat{\theta}_{2^j}(S_i) = S_i$$

for all positive integers j. That is, for any nonnegative integers j and n, there exists $u_i \in \mathbb{Z}_{p_i}$ such that $(u_i^{2^j} + 1) \cdot 2^n + 1 \equiv 0 \pmod{p_i}$ provided that $-2^{-n} - 1 \pmod{p_i} \in S_i$. The residues z_i in the covering $\mathcal{C}_1$ have been chosen carefully so that $-2^{-n} - 1 \equiv -2^{-z_i} - 1 \pmod{p_i}$ is an element of S_i for each value of i.

Now let $r = 2^j m$, where $\gcd(m, 6) = 1$ and $j \geq 0$. Note that the set of all prime divisors of $p_i - 1$ for all p_i in $\mathcal{C}_1$ is $\{2, 3\}$. Therefore, for each i, there exists, by Corollary 2.1, $v_i \in \mathbb{Z}_{p_i}$ such that $v_i^m \equiv u_i \pmod{p_i}$. Consequently,

$$v_i^r = v_i^{2^j m} = (v_i^m)^{2^j} \equiv (u_i)^{2^j} \equiv -2^{-z_i} - 1 \pmod{p_i}.$$

Thus, we can use the Chinese remainder theorem to solve the system of seven congruences $k \equiv v_i \pmod{p_i}$ to get infinitely many positive integers k such that $(k^r + 1) \cdot 2^n + 1$ is composite for all integers $n \geq 1$. The values of $r \pmod{30}$ captured in this stage are

$$\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29\}.$$

Next, consider the covering

$$\begin{aligned}\mathcal{C}_2 =\{&(1,2,3),(0,4,5),(0,5,31),(2,8,17),(4,10,11),(10,12,13),\\ &(6,15,151),(18,20,41),(14,24,241),(42,60,61)\}.\end{aligned}$$

Here we have that $p_i - 1 \equiv 0 \pmod 3$ for some values of i so that θ_3 is not an automorphism of $(\mathbb{Z}_{p_i})^*$ for these values of i. However, as was the case for θ_2 above, by Corollary 2.2 there exists a nonempty subset S_i of $\mathbb{Z}_{p_i}$ such that

$$\left(\widehat{\theta}_3\right)^j (S_i) = \widehat{\theta}_{3^j}(S_i) = S_i$$

for all positive integers j. That is, for any nonnegative integers j and n, there exists $u_i \in \mathbb{Z}_{p_i}$ such that $(u_i^{3^j} + 1) \cdot 2^n + 1 \equiv 0 \pmod{p_i}$ provided that $-2^{-n} - 1 \pmod{p_i} \in S_i$. Again, the residues z_i here in the covering $\mathcal{C}_2$ are chosen carefully so that $-2^{-n} - 1 \equiv -2^{-z_i} - 1 \pmod{p_i}$ is an element of S_i for each value of i.

Now let $r = 3^j m$, where $\gcd(m, 30) = 1$ and $j \geq 0$. Note that the set of all prime divisors of $p_i - 1$ for all i is $\{2, 3, 5\}$. Hence, for each i, Corollary 2.1 implies the existence of $v_i \in \mathbb{Z}_{p_i}$ such that $v_i^m \equiv u_i \pmod{p_i}$. Therefore,

$$v_i^r = v_i^{3^j m} = (v_i^m)^{3^j} \equiv (u_i)^{3^j} \equiv -2^{-z_i} - 1 \pmod{p_i}.$$

Thus, we can apply the Chinese remainder theorem to solve the system of eleven congruences $k \equiv v_i \pmod{p_i}$ to get infinitely many positive integers k such that $(k^r + 1) \cdot 2^n + 1$ is composite for all integers $n \geq 1$. The values of $r \pmod{30}$ captured in this stage are

$$\{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29\}.$$

Combining the results from the two coverings used here completes the proof of the Sierpiński part of the theorem.

Since the Riesel half of this theorem can be established using either the methods used in the proof of Theorem 2.2 or the methods used in the proof of the second part of the Sierpiński half of this theorem, we omit the details.

□

Remark 2.4. The techniques used in the proof of the first part of the Sierpiński half of Theorem 2.4 do not improve the result in the Riesel half of Theorem 2.4.

2.3 Simultaneous Nonlinear Sierpiński and Riesel Numbers

In this section we are concerned with determining a set of r values of positive density for which infinitely many positive integers k exist such that both $f(k) \cdot 2^n + 1$ and $f(k) \cdot 2^n - 1$ are composite for all integers $n \geq 1$, where $f(x) = x^r + 1$ or $f(x) = x^r + x + 1$.

Proof of Theorem 2.5. First let $f(x) = x^r + 1$. We use the following coverings:

$$\begin{aligned}\mathcal{C}_S = \{&(0,2,3),(1,3,7),(8,9,73),(11,18,19),(5,36,37),\\ &(23,36,109),(4,5,31),(5,10,11),(12,15,151),\\ &(21,30,331),(33,60,61),(3,60,1321)\}\end{aligned}$$

$$\begin{aligned}\text{and } \mathcal{C}_R = \{&(1,2,3),(0,4,5),(6,8,17),(10,16,257),\\ &(6,12,13),(2,24,241),(34,48,97)\}.\end{aligned}$$

The covering $\mathcal{C}_S$ is used to construct nonlinear Sierpiński numbers, while the covering $\mathcal{C}_R$ is used to construct nonlinear Riesel Numbers. Since $k^r \equiv 1 \pmod 3$ in both cases, and no other prime in $\mathcal{C}_S$ appears in $\mathcal{C}_R$, these two coverings are consistent, and we can construct a single system of congruences in k^r so that any solution k will be simultaneously a nonlinear Sierpiński number and a nonlinear Riesel number. Let $\mathcal{P} = \{p_i - 1 | p_i \in \mathcal{C}_S \text{ or } p_i \in \mathcal{C}_R\}$. Then, for a fixed value of $r < \text{lcm}(\mathcal{P})$, we examine the values of k with $0 \leq k \leq p_i - 1$ for each prime p_i. This process produces the conclusion of the theorem in this case.

Now, let $f(x) = x^r + x + 1$. Using the sets of moduli in $\mathcal{C}_S$ and $\mathcal{C}_R$ above, we construct a set of coverings for the Sierpiński case and a set of coverings for the Riesel case, such that each of the 1592 pairs (S, R), where S is a Sierpiński covering and R is a Riesel covering, is consistent as explained above. Let (S, R) be such a consistent Sierpiński-Riesel covering pair. For each element $(z, m, p) \in S$, we first

solve the congruence $x = -2^{-z} - 1 \pmod{p}$. Then we determine the values of r, with $1 \leq r \leq p-1$ for which there exists a value of k, with $0 \leq k \leq p-1$, such that $k^r + k = x \pmod{p}$. This process generates a set of "good" r-values for each prime p. We repeat this procedure for each element $(z', m', p') \in R$, with the modification that in this case we solve the congruence $x = 2^{-z'} - 1 \pmod{p'}$, and we get a set of "good" r-values for each prime p'. Thus, we have sets

$$GS_1, GS_2, \ldots, GS_s, GR_1, GR_2, \ldots, GR_t,$$

where GS_i is a set of "good" Sierpiński r-values, and GR_j is a set of "good" Riesel r-values. The next step is to find the intersection of all these sets. We start by finding the intersection of GS_1 and GS_2. Suppose that p is the prime corresponding to the set GS_1 and q is the prime corresponding to the set GS_2. For each pair $(a, b) \in GS_1 \times GS_2$, if $a \equiv b \pmod{g}$, where $g = \gcd(p-1, q-1)$, then we can use the generalized Chinese remainder theorem to find a solution x to the system $x \equiv a \pmod{p-1}$ and $x \equiv b \pmod{q-1}$, which gives an element in the intersection $W = GS_1 \cap GS_2$. Next, we find the intersection $W \cap GS_3$. We continue in this manner to determine the set of all values of r captured using this particular pair (S, R). The union of these sets of r-values for all pairs (S, R) in our collection yields the result of the theorem. □

Remark 2.5. The technique of using multiple pairs of consistent coverings in the proof of Theorem 2.5 for the case when $f(x) = x^r + x + 1$ does not seem to improve the r-density in the case when $f(x) = x^r + 1$.

Remark 2.6. The two coverings $\mathcal{C}_S$ and $\mathcal{C}_R$ used in the proof of Theorem 2.5 were used by Filaseta, Finch and Kozek [9] to determine the smallest known positive integer that is simultaneously a Sierpiński number and a Riesel number.

2.4 Concluding Remarks

The methods used in this paper differ from both the approach used previously by Chen, and the approach used by Filaseta, Finch and Kozek. In fact, the techniques used by Filaseta, Finch and Kozek to achieve r-density 1 are not applicable in Theorem 2.2, Theorem 2.4 and the majority of cases in Theorem 2.3. We should point out that both the paper of Chen [5] and the paper of Filaseta, Finch and Kozek [9] contain the stronger result that each term in the sequence $k^r \cdot 2^n + 1$ actually has at least two distinct prime divisors. Unfortunately, their methods used to establish this fact seem inapplicable here as well.

Chapter 3

A Polynomial Investigation Inspired by Work of Schinzel and Sierpiński

3.1 Introduction

Define a covering system (or covering) of the integers as a finite collection of congruences $x \equiv a_j \pmod{m_j}$, with $1 \leq j \leq r$, such that every integer satisfies at least one of these congruences. As an interesting application of coverings, W. Sierpiński [23] showed that there are odd positive integers k for which $k \cdot 2^n + 1$ is composite for all integers $n \geq 0$. For $d \in \mathbb{Z}$, Filaseta [8] considered the analogous problem of finding $f(x) \in \mathbb{Z}[x]$ such that $f(x) \cdot x^n + d$ is reducible over the rationals for all integers $n \geq 0$. To make the problem non-trivial, we also require here that $f(1) \neq -d$. This problem was motivated by the work of A. Schinzel in [22]. Among the open problems on covering systems is the problem of determining whether there is an odd covering, that is a covering that consists of distinct odd moduli > 1. Schinzel showed that if there is an $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -1$ and $f(x) \cdot x^n + 1$ is reducible for all integers $n \geq 0$, then there must be an odd covering. In fact, he showed considerably more than this, and the reader is directed to [22] for more details. For the general problem concerning $f(x)x^n + d$, the following is an easy consequence of the work of Schinzel [22] (see also [8]).

Theorem 3.1. *Let d be an odd integer. If there is an $f(x) \in \mathbb{Z}[x]$ satisfying $f(1) \neq -d$ and $f(x) \cdot x^n + d$ is reducible over the rationals for all integers $n \geq 0$, then there is an odd covering of the integers.*

The polynomial

$$f(x) = 5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3,$$

motivated by an example given by Schinzel in [22], satisfies $f(1) \neq -12$ and $f(x)x^n + 12$ is reducible for all $n \geq 0$. To justify the latter, one can make use of the following implications:

$$\begin{aligned}
n \equiv 0 \pmod 2 &\implies f(x)x^n + 12 \equiv 0 \pmod{x+1} \\
n \equiv 2 \pmod 3 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1} \\
n \equiv 1 \pmod 4 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+1} \\
n \equiv 1 \pmod 6 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2-x+1} \\
n \equiv 3 \pmod{12} &\implies f(x)x^n + 12 \equiv 0 \pmod{x^4-x^2+1}.
\end{aligned}$$

The congruences involving n on the left can be shown to form a covering of the integers; in other words, every integer n will satisfy at least one of these congruences. Each implication can be justified by noting that the modulus on the right is a cyclotomic polynomial $\Phi_m(x)$ with m corresponding to the modulus used on n on the left. We deduce from these implications that for each integer $n \geq 0$, the polynomial $f(x)x^n + 12$ is divisible by $\Phi_m(x)$ for some m dividing 12 and, hence, reducible.

In [8], Filaseta showed that a similar example exists whenever d is an integer divisible by 4. Thus, if $4|d$, then there is an $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -d$ and $f(x) \cdot x^n + d$ is reducible over the rationals for all integers $n \geq 0$. L. Jones [17] has shown that there are also similar examples for infinitely many positive integers $d \equiv 2 \pmod 4$. The smallest such d he gives with his method is $d = 90$.

The purpose of this paper is to improve on the work in [8] and [17] by showing that examples similar to Schinzel's example above exist for every even integer d. Thus, examples exist for every d for which Theorem 3.1 does not apply. Specifically, we show the following.

Theorem 3.2. *Let d be an even integer. There is an $f(x) \in \mathbb{Z}[x]$ satisfying both $f(1) \neq -d$ and $f(x) \cdot x^n + d$ is reducible over the rationals for all integers $n \geq 0$.*

3.2 Further Preliminaries

Our arguments begin with the following lemma which appears in [8].

Lemma 3.1. *Let d be a positive integer. Suppose that S is a system of congruences*

$$x \equiv 2^{j-1} \pmod{2^j} \qquad \text{for } j \in \{1, 2, \ldots, k\} \tag{3.2.1}$$

for some positive integer k together with

$$x \equiv a_j \pmod{m_j} \qquad \text{for } j \in \{1, 2, \ldots, r\} \tag{3.2.2}$$

for some positive integer r satisfying:

(i) The system S is a covering of the integers.

(ii) The moduli in (3.2.1) and (3.2.2) are all distinct and > 1.

(iii) For each $j \in \{1, 2, \ldots, r\}$,

$$\left(\prod_{\substack{1 \leq i \leq r \\ i \neq j}} a(i,j) \right) \left(\prod_{i=1}^{k} b(i,j) \right) \quad \text{divides} \quad d$$

where

$$a(i,j) = \begin{cases} p & \text{if } m_i/m_j = p^t \text{ for some prime } p \text{ and some integer } t \\ 1 & \text{otherwise} \end{cases}$$

and

$$b(i,j) = \begin{cases} p & \text{if } m_j/2^i = p^t \text{ for some prime } p \text{ and some integer } t \\ 1 & \text{otherwise.} \end{cases}$$

(iv) The double product $\prod_{i=1}^{k} \prod_{j=1}^{r} b(i,j)$ divides d.

Then there exists $f(x) \in \mathbb{Z}[x]$ with positive coefficients such that $f(x)x^n+d$ is reducible over the rationals for all non-negative integers n.

We proceed now as follows. Next, we state a lemma establishing the existence of a certain covering system. Then we will explain how this lemma will allow us to obtain Theorem 3.2. Finally, we give a proof of the lemma by explicitly establishing the needed covering.

Lemma 3.2. *There is a covering of the integers consisting of moduli $m_1, m_2, \ldots, m_r$ satisfying:*

(i) Each m_ℓ is odd and > 1.

(ii) If m_ℓ is a prime number, then $m_j \neq m_\ell$ for each $j \neq \ell$, with $1 \leq j \leq r$.

(iii) If m_ℓ has at least two distinct prime factors, then there is at most one $j \neq \ell$, with $1 \leq j \leq r$, such that $m_j = m_\ell$.

We show that Lemma 3.2 implies that there is an $f(x) \in \mathbb{Z}[x]$ with positive coefficients such that $f(x)x^n + 2$ is reducible over the rationals for all non-negative integers n. Observe that by simply multiplying through by an appropriate positive integer, we can deduce that for every even integer d, there is an $f(x) \in \mathbb{Z}[x]$, depending on d, with positive coefficients such that $f(x)x^n + d$ is reducible over the rationals for all non-negative integers n. More interesting examples, where for example the greatest common divisor of the coefficients of $f(x)$ is 1, can be obtained for general even d by adding a polynomial of the form $x^m + x^{m-1} + \cdots + x + 1$ for an appropriate large positive integer m. In any case, $f(1) \neq -d$.

To obtain $f(x) \in \mathbb{Z}[x]$ with positive coefficients such that $f(x)x^n + 2$ is reducible over the rationals for all non-negative integers n, Lemma 3.1 implies that we need only show the existence of a certain covering system. Our goal is to revise the covering system in Lemma 3.2 to show that the covering system for Lemma 3.1 exists.

Let $x \equiv a_j \pmod{m_j}$ for $j \in \{1, 2, \ldots, r\}$ denote the r congruences given by Lemma 3.2. Suppose that the first s of these congruences have prime moduli and the remaining do not. We suppose as we may (from Lemma 3.2 (iii)) that if $m_i = m_j$ for some integers i and j with $s+1 \leq j < i \leq r$, then $i = j+1$. Define

$$m'_j = \begin{cases} m_j & \text{for } j \in \{1, 2, \ldots, s\} \\ 2^{j-s} m_j & \text{for } j \in \{s+1, s+2, \ldots, r\}. \end{cases}$$

Let $b_j = a_j$ for $1 \leq j \leq s$. For each $j \in \{s+1, s+2, \ldots, r\}$, we define b_j as the nonnegative integer $< 2^{j-s} m_j$ satisfying

$$b_j \equiv a_j \pmod{m_j} \qquad \text{and} \qquad b_j \equiv 0 \pmod{2^{j-s}},$$

which exists by the Chinese Remainder Theorem. We consider the congruences

$$x \equiv 2^{j-1} \pmod{2^j} \qquad \text{for } j \in \{1, 2, \ldots, r-s\} \tag{3.2.3}$$

together with

$$x \equiv b_j \pmod{m'_j} \qquad \text{for } j \in \{1, 2, \ldots, r\}. \tag{3.2.4}$$

We show that these congruences form a system S of congruences satisfying the conditions of Lemma 3.1 with $d = 2$, $k = r - s$ and the m_j there replaced by m'_j.

Suppose n is an integer that does not satisfy one of the congruences in (3.2.3). Observe that if j is the largest positive integer for which 2^{j-1} divides n, then $n \equiv 2^{j-1} \pmod{2^j}$. Since n does not satisfy the congruences in (3.2.3), we deduce $n \equiv 0 \pmod{2^{r-s}}$. Also, since the congruences $x \equiv a_j \pmod{m_j}$ for $j \in \{1, 2, \ldots, r\}$ form a covering of the integers, $n \equiv a_j \pmod{m_j}$ for some $j \in \{1, 2, \ldots, r\}$. By the definition of b_j, we have for that choice of j that $x \equiv b_j \pmod{m'_j}$. Hence, n satisfies one of the congruences in (3.2.4). Thus, S satisfies the condition (i) of Lemma 3.1.

Condition (ii) of Lemma 3.1 is easily checked for the congruences in (3.2.3) and (3.2.4). To verify conditions (iii) and (iv) of Lemma 3.1 for the congruences in (3.2.3)

and (3.2.4), we alter the definitions of $a(i,j)$ and $b(i,j)$ accordingly so that m_i and m_j are replaced by m_i' and m_j'. Note that the conditions in Lemma 3.2 and the definition of s imply that $m_1', m_2', \ldots, m_s'$ are distinct primes and $m_{s+1}', m_{s+2}', \ldots, m_r'$ are distinct numbers each having ≥ 3 distinct prime factors. Further, the largest powers of 2 dividing the numbers $m_{s+1}', m_{s+2}', \ldots, m_r'$, namely $2, 2^2, \ldots, 2^{r-s}$, are distinct. It follows that if the ratio $m_j'/m_i' = p^t$ for some prime p and some integer t, then $p = 2$ and, consequently, $m_j = m_i$. Recall that for j fixed, the conditions $i \neq j$ and $m_j = m_i$ imply there is at most one possibility for i. We deduce that for each $j \in \{1, 2, \ldots, r\}$,

$$\prod_{\substack{1 \leq i \leq r \\ i \neq j}} a(i,j) \text{ divides } 2.$$

The conditions in Lemma 3.2 imply that each m_j with $j > s$ and, hence, each even m_j' has at least two odd prime divisors. It follows that $b(i,j) = 1$ for every choice of i and j in $\{1, 2, \ldots, r\}$. Conditions (iii) and (iv) of Lemma 3.1 now easily follow.

3.3 Construction for Lemma 3.2

Given lists $[b_1, \ldots, b_t]$ and $[n_1, \ldots, n_t]$ with $n_1, \ldots, n_t$ pairwise relatively prime positive integers, we denote by

$$([b_1, \ldots, b_t], [n_1, \ldots, n_t])$$

the congruence $x \equiv b \mod n$ where $n = n_1 \cdots n_t$ and $b \in \{0, 1, \ldots, n-1\}$ satisfies $b \equiv b_j \pmod{n_j}$ for $1 \leq j \leq t$. That such a b exists follows from the Chinese Remainder Theorem. Note that, with b and n so defined, the congruences represented by $([b_1, \ldots, b_t], [n_1, \ldots, n_t])$ and $([b], [n])$ are identical. With this same notation, we denote by

$$\mathcal{I}([b_1, \ldots, b_t], [n_1, \ldots, n_t]) = \mathcal{I}([b], [n])$$

the set of integers satisfying $x \equiv b \mod n$. We say that a collection of congruences covers a set of integers if every integer in the set satisfies at least one congruence in the collection.

In this section, we elaborate on the covering system, say $\mathcal{S}$, satisfying the conditions of Lemma 3.2. Noting that every integer belongs to one of the sets $\mathcal{I}([1],[3])$, $\mathcal{I}([2],[3])$ and $\mathcal{I}([3],[3]) = \mathcal{I}([0],[3])$, we determine congruences for $\mathcal{S}$ by finding collections $\mathcal{S}_1$, $\mathcal{S}_2$ and $\mathcal{S}_3$ of congruences that cover each of these three sets. The system $\mathcal{S}$, then, will be the union of the congruences given in $\mathcal{S}_1$, $\mathcal{S}_2$ and $\mathcal{S}_3$.

For $\mathcal{I}([1],[3])$, we simply use the congruence $([1],[3])$. For $\mathcal{I}([2],[3])$, we consider the integers in each of the five residue classes modulo 5. We cover the integers in $\mathcal{I}([2],[3])$ that are 1 modulo 5 by using the congruence $([1],[5])$. For later purposes, we note that this same congruence will cover the integers in $\mathcal{I}([3],[3])$ that are 1 modulo 5. We cover the integers in $\mathcal{I}([2],[3])$ that are 2 modulo 5 and 5 modulo 5 by using congruences modulo 15. Recall that the conditions in Lemma 3.2 allow us to use the modulus 15 for two different congruences. Thus, we can use the two congruences $([2,2],[3,5])$ and $([2,5],[3,5])$. So far our congruences $\mathcal{S}$ include the four congruences given by

$$([1],[3]), \quad ([1],[5]), \quad ([2,2],[3,5]), \quad ([2,5],[3,5]). \tag{3.3.1}$$

With these, we have covered $\mathcal{I}([1],[3])$ and three-fifths of $\mathcal{I}([2],[3])$. We still need to elaborate on the congruences of $\mathcal{S}$ that cover the integers in $\mathcal{I}([2],[3])$ that are 3 and 4 modulo 5 and that cover the integers in $\mathcal{I}([3],[3])$ (that are not 1 modulo 5).

We explain next the congruences used to cover $\mathcal{I}([2,3],[3,5])$. We will make use here of moduli of the form $3^{j+1}\cdot 5$ and moduli of the form $3^j \cdot 5 \cdot 23$ where j is a positive integer. We keep in mind that each such modulus can be used for two congruences in $\mathcal{S}$, though we only take advantage of this fact for those of the form $3^{j+1} \cdot 5$. Each integer in $\mathcal{I}([2],[3])$ is either 2, 5 or 8 modulo 9. In the first two of these three cases, the integers that are also 3 modulo 5 satisfy one of the congruences $([2,3],[3^2,5])$ and $([5,3],[3^2,5])$. The integers that are 8 modulo 9 are either 8, 17 or 26 modulo 27. Those that are 8 or 17 modulo 27 satisfy one of the congruences $([8,3],[3^3,5])$ and $([17,3],[3^3,5])$. In general, for each positive integer j, the integers that are $3^j - 1$

modulo 3^j are either 3^j-1, $2\cdot 3^j-1$ or $3\cdot 3^j-1=3^{j+1}-1$ modulo 3^{j+1}. Those that are 3^j-1 or $2\cdot 3^j-1$ modulo 3^{j+1} and 3 modulo 5 are covered by $([3^j-1,3],[3^{j+1},5])$ and $([2\cdot 3^j-1,3],[3^{j+1},5])$. We deduce that the congruences

$$([3^j-1,3],[3^{j+1},5]),\quad ([2\cdot 3^j-1,3],[3^{j+1},5]),\quad \text{for } 1\le j\le 22, \tag{3.3.2}$$

cover all the integers in $\mathcal{I}([2],[3])$ that are 3 modulo 5 except those that are $3^{23}-1$ modulo 3^{23}. Since each such integer is also congruent to some positive integer ≤ 23 modulo 23, we deduce that these integers are covered by the congruences

$$([3^{23}-1,3,j],[3^j,5,23]),\quad \text{for } 1\le j\le 23. \tag{3.3.3}$$

Thus, the congruences in (3.3.2) and (3.3.3) cover the integers in $\mathcal{I}([2],[3])$ that are 3 modulo 5.

To finish covering the integers that are in $\mathcal{I}([2],[3])$, we are left with finding congruences that cover those that are also 4 modulo 5. In other words, we are wanting now to cover $\mathcal{I}([2,4],[3,5])$. We divide these integers into classes modulo 7, covering each in turn. We start with the congruences

$$([1],[7]),\quad ([2,4,2],[3,5,7]),\quad ([2,4,3],[3,5,7]),\quad ([4,4],[5,7]), \tag{3.3.4}$$

to cover those integers in $\mathcal{I}([2,4],[3,5])$ that are 1, 2, 3 or 4 modulo 7. Next, we mimic what was done in (3.3.2) and (3.3.3) to cover $\mathcal{I}([2,3],[3,5])$ by restricting these same congruences to integers that are 5 modulo 7. Specifically, we include

$$([3^j-1,4,5],[3^{j+1},5,7]),\ ([2\cdot 3^j-1,4,5],[3^{j+1},5,7]),\ \text{for } 1\le j\le 22, \tag{3.3.5}$$

and

$$([3^{23}-1,4,5,j],[3^j,5,7,23]),\quad \text{for } 1\le j\le 23, \tag{3.3.6}$$

in our system $\mathcal{S}$ to cover $\mathcal{I}([2,4,5],[3,5,7])$. To finish covering $\mathcal{I}([2,4],[3,5])$, we consider separately those in $\mathcal{I}([2,4,6],[3,5,7])$ and $\mathcal{I}([2,4,7],[3,5,7])$.

To cover $\mathcal{I}([2,4,6],[3,5,7])$, we use that each is in one of 7 different residue classes modulo 7^2. We keep in mind that, although our required system $\mathcal{S}$ for Lemma 3.2 can involve moduli divisible by p^e where p is an odd prime and e an integer ≥ 2, it cannot have moduli that are equal to these prime powers. For $\mathcal{I}([2,4,6],[3,5,7])$, we cover 6 of the needed residue classes modulo 7^2 using

$$\begin{gathered}([2,6],[3,7^2]),\quad ([2,13],[3,7^2]),\quad ([4,20],[5,7^2]),\quad ([4,27],[5,7^2]),\\ ([2,4,34],[3,5,7^2]),\quad ([2,4,41],[3,5,7^2]).\end{gathered} \tag{3.3.7}$$

For the final residue class modulo 7^2, we use congruences similar to (3.3.2) and (3.3.3). This last class modulo 7^2 is covered by

$$\begin{gathered}([3^j-1,4,48],[3^{j+1},5,7^2]),\\ ([2\cdot 3^j-1,4,48],[3^{j+1},5,7^2]),\quad \text{for } 1\leq j\leq 22,\\ ([3^{23}-1,4,48,j],[3^j,5,7^2,23]),\quad \text{for } 1\leq j\leq 23.\end{gathered} \tag{3.3.8}$$

To finish covering $\mathcal{I}([2],[3])$, we need only cover $\mathcal{I}([2,4,7],[3,5,7])$. This is a thin enough set that we are able to get away with using the prime 19 to complete this case. The idea then is to consider each of the 19 possible residue classes that each of these integers can belong to. We cover 15 of these residue classes using

$$\begin{gathered}([1],[19]),\quad ([2,2],[3,19]),\quad ([2,3],[3,19]),\quad ([4,4],[5,19]),\\ ([4,5],[5,19]),\quad ([2,4,6],[3,5,19]),\quad ([2,4,7],[3,5,19]),\\ ([7,8],[7,19]),\quad ([7,9],[7,19]),\quad ([2,7,10],[3,7,19]),\\ ([2,7,11],[3,7,19]),\quad ([4,7,12],[5,7,19]),\quad ([4,7,13],[5,7,19]),\\ ([2,4,7,14],[3,5,7,19]),\quad ([2,4,7,15],[3,5,7,19]).\end{gathered} \tag{3.3.9}$$

We make use of the idea in (3.3.2) and (3.3.3) to cover the remaining classes modulo 19, each class making use of such a list of congruences. Those integers congruent to

16 modulo 19 in $\mathcal{I}([2,4,7],[3,5,7])$ are covered by

$$\begin{gathered}([3^j-1,16],[3^{j+1},19]),\ ([2\cdot 3^j-1,16],[3^{j+1},19]),\ \text{for } 1\le j\le 22,\\ ([3^{23}-1,16,j],[3^j,19,23]),\quad \text{for } 1\le j\le 23;\end{gathered} \tag{3.3.10}$$

those congruent to 17 modulo 19 by

$$\begin{gathered}([3^j-1,4,17],[3^{j+1},5,19]),\\ ([2\cdot 3^j-1,4,17],[3^{j+1},5,19]),\quad \text{for } 1\le j\le 22,\\ ([3^{23}-1,4,17,j],[3^j,5,19,23]),\quad \text{for } 1\le j\le 23;\end{gathered} \tag{3.3.11}$$

those congruent to 18 modulo 19 by

$$\begin{gathered}([3^j-1,7,18],[3^{j+1},7,19]),\\ ([2\cdot 3^j-1,7,18],[3^{j+1},7,19]),\quad \text{for } 1\le j\le 22,\\ ([3^{23}-1,7,18,j],[3^j,7,19,23]),\quad \text{for } 1\le j\le 23;\end{gathered} \tag{3.3.12}$$

those congruent to 19 (or 0) modulo 19 by

$$\begin{gathered}([3^j-1,4,7,19],[3^{j+1},5,7,19]),\\ ([2\cdot 3^j-1,4,7,19],[3^{j+1},5,7,19]),\quad \text{for } 1\le j\le 22,\\ ([3^{23}-1,4,7,19,j],[3^j,5,7,19,23]),\quad \text{for } 1\le j\le 23.\end{gathered} \tag{3.3.13}$$

The congruences above combine then to cover $\mathcal{I}([2],[3])$.

Next, we use an approach similar to the case of $\mathcal{I}([2],[3])$ and break up $\mathcal{I}([3],[3])$ into the five residue classes modulo 5. The second congruence in (3.3.1) will cover $\mathcal{I}([3,1],[3,5])$. In each of the four remaining cases $\mathcal{I}([3,j],[3,5])$, with $2\le j\le 5$, we will divide the integers up into their residue classes modulo 7. What is of particular importance to us here is that the first congruence in (3.3.4) and the congruences

$$([3,2],[3,7]),\quad ([3,3],[3,7]) \tag{3.3.14}$$

cover three of the seven residue classes modulo 7 for each $\mathcal{I}([3,j],[3,5])$. Further, we can cover a fourth residue class modulo 7 in each $\mathcal{I}([3,j],[3,5])$ by using the congruences

$$\begin{gathered}([3^j,5],[3^{j+1},7]),\quad ([2\cdot 3^j,5],[3^{j+1},7]),\quad \text{for } 1\le j\le 22,\\ ([3^{23},5,j],[3^j,7,23]),\quad \text{for } 1\le j\le 23.\end{gathered}\tag{3.3.15}$$

To finish covering $\mathcal{I}([3],[3])$, we are left with covering the integers congruent to 4, 6 and 7 modulo 7 in each $\mathcal{I}([3,j],[3,5])$, with $2\le j\le 5$. We note that we have deliberately covered the residue class 5 modulo 7 instead of 4 modulo 7 so that we can make use of the last congruence in (3.3.4) when we consider $\mathcal{I}([3,4],[3,5])$.

We finish covering $\mathcal{I}([3,2],[3,5])$ as follows. As noted above, the congruences in (3.3.14) and (3.3.15) cover four residue classes modulo 7. We make use of this momentarily, but for the time being we instead break up the integers in $\mathcal{I}([3,2],[3,5])$ into their five residue classes modulo 5^2 with the goal of covering each of these five classes in turn. The congruences corresponding to $j=1$ in the list

$$([3,5^j+2],[3,5^{j+1}]),\quad ([3,2\cdot 5^j+2],[3,5^{j+1}]),\quad \text{for } 1\le j\le 22,\tag{3.3.16}$$

cover the residue classes 7 and 12 modulo 5^2. The collection of $2\cdot 22+23$ congruences corresponding to $j=1$ in

$$\begin{gathered}([3^i,3\cdot 5^j+2],[3^{i+1},5^{j+1}]),\\ ([2\cdot 3^i,3\cdot 5^j+2],[3^{i+1},5^{j+1}]),\quad \text{for } 1\le i,j\le 22,\\ ([3^{23},3\cdot 5^j+2,i],[3^i,5^{j+1},23]),\quad \text{for } 1\le i\le 23, 1\le j\le 22\end{gathered}\tag{3.3.17}$$

cover the integers that are 17 modulo 5^2. To cover the integers that are 22 modulo 5^2, we consider their residue classes modulo 7 and recall that we have already covered the integers in $\mathcal{I}([3,2],[3,5])$ that are 1, 2, 3 and 5 modulo 7. We use the case $j=1$

in

$$\begin{gathered}([4\cdot 5^j+2,4],[5^{j+1},7]),\quad ([4\cdot 5^j+2,6],[5^{j+1},7]),\\ ([3,4\cdot 5^j+2,7],[3,5^{j+1},7]),\quad \text{for } 1\le j\le 23,\end{gathered}\tag{3.3.18}$$

to finish covering the integers that are 22 modulo 5^2. We still need to cover $\mathcal{I}([3,2],[3,5^2])$. We divide these into five residue classes modulo 5^3 and use $j=2$ in (3.3.16), (3.3.17) and (3.3.18) to cover the four of these five classes that are not 2 modulo 5^3. Continuing with $3\le j\le 22$ to cover residue classes modulo 5^{j+1}, we see that the congruences in (3.3.16), (3.3.17) and (3.3.18) cover all the integers in $\mathcal{I}([3,2],[3,5^2])$ except those that are in $\mathcal{I}([3,2],[3,5^{23}])$. We cover these by using the congruences

$$([2,j],[5^j,23]),\quad \text{for } 1\le j\le 23,\tag{3.3.19}$$

noting the jth congruence in this list covers those integers in $\mathcal{I}([3,2],[3,5^{23}])$ that are j modulo 23.

Next, we cover $\mathcal{I}([3,3],[3,5])$. We break up these integers into their residue classes modulo 7. Recall we only need to cover the residue classes modulo 4, 6 and 7 modulo 7. In (3.3.4), the modulus $5\cdot 7$ was used once, and we use it again here to cover $\mathcal{I}([3,3,4],[3,5,7])$ with

$$([3,4],[5,7]).\tag{3.3.20}$$

We cover all integers in $\mathcal{I}([3,3,6],[3,5,7])$ except those congruent to 6 modulo 11 using

$$\begin{gathered}([1],[11]),\quad ([3,2],[3,11]),\quad ([3,3],[3,11]),\quad ([3,4],[5,11]),\\ ([3,3,5],[3,5,11]),\quad ([3,6,7],[3,7,11]),\quad ([3,6,8],[3,7,11]),\\ ([6,9],[7,11]),\quad ([6,10],[7,11]),\quad ([3,6,11],[5,7,11]).\end{gathered}\tag{3.3.21}$$

For later purposes, note that we have only used some moduli dividing $3 \cdot 5 \cdot 7 \cdot 11$ above once. To cover $\mathcal{I}([3,3,6,6],[3,5,7,11])$, we use

$$\begin{gathered}([3^j,6],[3^{j+1},11]),([2\cdot 3^j,6],[3^{j+1},11]), \quad \text{for } 1\le j\le 22,\\ ([3^{23},6,j],[3^j,11,23]), \quad \text{for } 1\le j\le 23.\end{gathered} \tag{3.3.22}$$

Next, we turn to $\mathcal{I}([3,3,7],[3,5,7])$ and consider their residue classes modulo 13. We cover all integers in $\mathcal{I}([3,3,7],[3,5,7])$ except those congruent to 12 and 13 modulo 13 in a manner very similar to our approach for covering $\mathcal{I}([3,3,6],[3,5,7])$ above but with 11 replaced by 13. Specifically, we use

$$\begin{gathered}([1],[13]),\quad ([3,2],[3,13]),\quad ([3,3],[3,13]),\quad ([3,4],[5,13]),\\ ([3,3,5],[3,5,13]),\quad ([3,7,7],[3,7,13]),\quad ([3,7,8],[3,7,13]),\\ ([7,9],[7,13]),\quad ([7,10],[7,13]),\quad ([3,7,11],[5,7,13]).\end{gathered} \tag{3.3.23}$$

and

$$\begin{gathered}([3^j,6],[3^{j+1},13]),([2\cdot 3^j,6],[3^{j+1},13]), \quad \text{for } 1\le j\le 22,\\ ([3^{23},6,j],[3^j,13,23]), \quad \text{for } 1\le j\le 23.\end{gathered} \tag{3.3.24}$$

We use

$$([3,3,7,12],[3,5,7,13]) \tag{3.3.25}$$

to cover $\mathcal{I}([3,3,7,12],[3,5,7,13])$ and

$$\begin{gathered}([3^j,7,13],[3^{j+1},7,13]),([2\cdot 3^j,7,13],[3^{j+1},7,13]), \text{ for } 1\le j\le 22,\\ ([3^{23},7,13,j],[3^j,7,13,23]), \quad \text{for } 1\le j\le 23.\end{gathered} \tag{3.3.26}$$

to cover $\mathcal{I}([3,3,7,13],[3,5,7,13])$. We deduce that the congruences (3.3.20) - (3.3.26) cover $\mathcal{I}([3,3],[3,5])$.

To cover $\mathcal{I}([3,4],[3,5])$, we need only cover those integers that are in the residue classes modulo 4, 6 and 7 modulo 7 (the other residue classes being covered already above). The congruence $([4,4],[5,7])$ in (3.3.4) covers the integers in $\mathcal{I}([3,4,4],[3,5,7])$.

To cover $\mathcal{I}([3,4,6],[3,5,7])$, we can reuse several of the congruences in (3.3.21) and (3.3.22) (those with moduli not divisible by 5) to cover the integers in certain residue classes modulo 11. Specifically, the integers in $\mathcal{I}([3,4,6],[3,5,7])$ that are 1, 2, 3, 6, 7, 8, 9 or 10 modulo 11 are covered by congruences in (3.3.21) and (3.3.22). We only used the moduli $5 \cdot 11$, $3 \cdot 5 \cdot 11$ and $5 \cdot 7 \cdot 11$ once in (3.3.21), so we use now

$$([4,4],[5,11]), \quad ([3,4,5],[3,5,11]), \quad ([4,6,11],[5,7,11]) \tag{3.3.27}$$

to cover the integers in $\mathcal{I}([3,4,6],[3,5,7])$ that are 4, 5 or 11 modulo 11. This completes covering $\mathcal{I}([3,4,6],[3,5,7])$. Turning to $\mathcal{I}([3,4,7],[3,5,7])$, we can reuse congruences in (3.3.23), (3.3.24) and (3.3.26) to cover those integers here that lie in the residue classes 1, 2, 3, 6, 7, 8, 9, 10 or 13 modulo 13. We use

$$\begin{gathered} ([4,4],[5,13]), \quad ([3,4,5],[3,5,13]), \\ ([4,7,11],[5,7,13]), \quad ([3,4,7,12],[3,5,7,13]) \end{gathered} \tag{3.3.28}$$

to cover the remaining integers in $\mathcal{I}([3,4,7],[3,5,7])$.

We are left with covering $\mathcal{I}([3,5],[3,5])$. More precisely, we need only cover $\mathcal{I}([3,5,4],[3,5,7])$, $\mathcal{I}([3,5,6],[3,5,7])$ and $\mathcal{I}([3,5,7],[3,5,7])$. We split up the integers in $\mathcal{I}([3,5,4],[3,5,7])$ into residue classes modulo 17. Let $a \in \mathcal{I}([3,5,4],[3,5,7])$, and let $m_1, m_2, \dots, m_7$ be the divisors of $3 \cdot 5 \cdot 7$ that are > 1. We use

$$([a,j],[m_j,17]), \quad ([a,j+7],[m_j,17]), \quad \text{for } 1 \le j \le 7, \tag{3.3.29}$$

to cover the integers in $\mathcal{I}([3,5,4],[3,5,7])$ that are in the residue classes $1, 2, 3, \dots, 13$ or 14 modulo 17. We cover the remaining integers using

$$([15],[17]), \tag{3.3.30}$$

$$\begin{gathered} ([3^j,16],[3^{j+1},17]), \ ([2 \cdot 3^j,16],[3^{j+1},17]), \quad \text{for } 1 \le j \le 22, \\ ([3^{23},16,j],[3^j,17,23]), \quad \text{for } 1 \le j \le 23, \end{gathered} \tag{3.3.31}$$

and

$$\begin{aligned}&([3^j,5,17],[3^{j+1},5,17]),\ ([2\cdot 3^j,5,17],[3^{j+1},5,17]),\ \text{for } 1\le j\le 22,\\ &\qquad ([3^{23},5,17,j],[3^j,5,17,23]),\quad \text{for } 1\le j\le 23.\end{aligned}\tag{3.3.32}$$

We turn to covering $\mathcal{I}([3,5,6],[3,5,7])$ and once again use the congruences in (3.3.21) and (3.3.22). With these, we cover the integers in $\mathcal{I}([3,5,6],[3,5,7])$ that are 1, 2, 3, 6, 7, 8, 9 or 10 modulo 11. We use

$$([3,5,6,4],[3,5,7,11]),\quad ([3,5,6,5],[3,5,7,11]),\tag{3.3.33}$$

to cover those integers in $\mathcal{I}([3,5,6],[3,5,7])$ that are 4 or 5 modulo 11. We cover those that are 11 modulo 11 using

$$\begin{aligned}&([3^j,5,11],[3^{j+1},5,11]),([2\cdot 3^j,5,11],[3^{j+1},5,11]),\ \text{for } 1\le j\le 22,\\ &\qquad ([3^{23},5,11,j],[3^j,5,11,23]),\quad \text{for } 1\le j\le 23.\end{aligned}\tag{3.3.34}$$

For $\mathcal{I}([3,5,7],[3,5,7])$, we use congruences in (3.3.23), (3.3.24) and (3.3.26) again to cover integers in the residue classes 1, 2, 3, 6, 7, 8, 9, 10 or 13 modulo 13. The congruences

$$\begin{aligned}&([3^j,5,4],[3^{j+1},5,13]),([2\cdot 3^j,5,4],[3^{j+1},5,13]),\quad \text{for } 1\le j\le 22,\\ &\qquad ([3^{23},5,4,j],[3^j,5,13,23]),\quad \text{for } 1\le j\le 23.\end{aligned}\tag{3.3.35}$$

and

$$\begin{aligned}&([3^j,5,7,5],[3^{j+1},5,7,13]),\\ &\qquad ([2\cdot 3^j,5,7,5],[3^{j+1},5,7,13]),\quad \text{for } 1\le j\le 22,\\ &([3^{23},5,7,5,j],[3^j,5,7,13,23]),\quad \text{for } 1\le j\le 23.\end{aligned}\tag{3.3.36}$$

cover the integers in $\mathcal{I}([3,5,7],[3,5,7])$ that are in the residue classes 4 or 5 modulo 13. We can use the congruences in (3.3.21) and (3.3.22) to cover those integers in each of $\mathcal{I}([3,5,7,11],[3,5,7,13])$ and $\mathcal{I}([3,5,7,12],[3,5,7,13])$ that are 1, 2, 3 or 6

modulo 11. Recall $m_1, m_2, \ldots, m_7$ are the divisors of $3 \cdot 5 \cdot 7$ that are > 1. Let $b \in \mathcal{I}([3,5,7],[3,5,7])$. We cover the remaining integers using

$$\begin{gathered}([b, j+3, 11], [m_j, 11, 13]), \\ ([b, j+3, 12], [m_j, 11, 13]), \text{ for } 1 \leq j \leq 2,\end{gathered} \tag{3.3.37}$$

and

$$\begin{gathered}([b, j+4, 11], [m_j, 11, 13]), \\ ([b, j+4, 12], [m_j, 11, 13]), \text{ for } 3 \leq j \leq 7.\end{gathered} \tag{3.3.38}$$

We note that the modulus $11 \cdot 13$, which could have been used twice, was not used here.

As just shown, the congruences in (3.3.1) - (3.3.38) form a covering of the integers. We use these congruences to form the set $\mathcal{S}$ needed for Lemma 3.2. What is left is to verify the conditions (i), (ii) and (iii) in Lemma 3.2, which can be done directly going through the various moduli indicated above. This completes the proof.

3.4 Concluding Remarks

We made use of 2773 congruences for the construction given in the previous section, that is to obtain a covering satisfying the conditions in Lemma 3.2. This corresponds to 5539 congruences to construct a polynomial $f(x) \in \mathbb{Z}[x]$, based on Lemma 3.1, such that $f(1) \neq -2$ and $f(x)x^n + 2$ is reducible for all integers $n \geq 0$. Although the method used in [8] is similar to the approach here, the covering system obtained for constructing an analogous $f(x)$ with $d = 4$ there was more complicated due to the fact that prime moduli were not used (i.e., Lemma 3.2 (ii) was not considered in [8]).

The approach given by L. Jones in [17] was to show first that there is an $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -d$ and $f(x)x^n + d$ is reducible for all integers $n \geq 0$ if there is a covering system with distinct moduli > 1 and with the least common multiple of the moduli equal to d. Jones then uses this information to show that such an $f(x)$

can be constructed for infinitely many $d \equiv 2 \pmod 4$. In particular, he is able to produce an explicit $f(x)$ in the case $d = 90$. We note that, although the values of d found by Jones in [17] were not found by Filaseta in [8], Lemma 3.1 (which appears as Theorem 3 in [8]) can be used to produce them.

Chapter 4

On the Factorization of the Trinomials $x^n + cx^{n-1} + d$

4.1 Introduction

The results in this chapter were inspired by curiosities about the factorization of polynomials of the form

$$f(x) = x^n + cx^{n-1} + cx^{n-2} + \cdots + cx + c \in \mathbb{Z}[x].$$

In particular, we ask,

Question 4.1. *For what positive integers n and non-zero integers c is $f(x)$ irreducible?*

Question 4.2. *If $f(x)$ is reducible, then how does it factor?*

The answers to these questions are well known for certain values of c. For example, if p is a prime such that $p \parallel c$ then $f(x)$ is irreducible for all positive integers n since such an $f(x)$ satisfies the well known Eisenstein Criterion. The questions are also answered easily whenever $c = 1$ with the use of cyclotomic polynomials. To answer the questions for values of c with $|c| > 1$ we first establish the following theorem.

Theorem 4.1. *Let n, c, and d be positive integers with $n \geq 3$, $d \neq c$, $d \leq 2(c-1)$, and $(n, c) \neq (3, 3)$. If the trinomial $f(x) = x^n \pm cx^{n-1} \pm d$ is reducible in $\mathbb{Z}[x]$, then $f(x) = (x \pm 1)g(x)$ for some irreducible $g(x) \in \mathbb{Z}[x]$.*

Using Theorem 4.1 we then answer the opening questions for $|c| > 1$ with the following theorem.

Theorem 4.2. *Let n and c be positive integers with $c \geq 2$. Then the polynomials*

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

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

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

We note here that the special case of $h(x)$ in Theorem 4.2 follows from a result due to Alfred Brauer in [1]. Brauer's theorem also handles the case $c = 1$ in the special case of $h(x)$. In particular, Brauer proved

Theorem 4.3. *Let $f(x) = x^n - (a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n) \in \mathbb{Z}[x]$. If $a_1 \geq a_2 \geq \cdots \geq a_n > 0$ then $f(x)$ is irreducible in $\mathbb{Z}[x]$.*

4.2 Preliminaries

In this section we present some general results about the irreducibility of polynomials as well as some notation. Throughout the paper we use $\mathcal{C}$ to represent the set $\{z \in \mathbb{C} : |z| < 1\}$ and $\overline{\mathcal{C}} = \{z \in \mathbb{C} : |z| \leq 1\}$. Using this notation we now present the first two lemmas. We note that while these lemmas follow from the work of Perron in [20], we provide proofs for completeness and accessibility.

Lemma 4.1. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial with $f(0) \neq 0$. If $f(x)$ has only one root (counting multiplicity) in $\mathbb{C} \setminus \mathcal{C}$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.*

Proof. Let $f(x)$ be as in the statement of the lemma and let $f(\alpha) = 0$ for some $\alpha \in \mathbb{C}$ with $|\alpha| \geq 1$. Assume by way of contradiction that $f(x)$ is not irreducible. Since $f(x)$

is monic we can then write $f(x) = g(x)h(x)$ for some monic $g(x) \in \mathbb{Z}[x]$ and monic $h(x) \in \mathbb{Z}[x]$, each having positive degree. Without loss of generality we may assume that $g(\alpha) = 0$. Now let r be the degree of $h(x)$ and let $\alpha_1, \cdots, \alpha_r$ be the roots of $h(x)$. Since $f(0) \neq 0$, this then implies that

$$0 < |h(0)| = \prod_{j=1}^{r} |\alpha_j| < 1.$$

This is a contradiction since $h(x) \in \mathbb{Z}[x]$. Hence, $f(x)$ must be irreducible. □

Lemma 4.2. *Let $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 \in \mathbb{Q}[x]$ with $n \geq 1$ and $a_0 \neq 0$. If $|a_{n-1}| > 1 + \sum_{j=0}^{n-2} |a_j|$, then $f(x)$ has exactly one root (counting multiplicity) in $\mathbb{C} \setminus \mathcal{C}$.*

Proof. Let $f(x)$ be as in the statement of the lemma and let $g(x) = -a_{n-1}x^{n-1}$. Then for $z \in \mathbb{C}$ with $|z| = 1$ we have that

$$\begin{aligned} |f(z) + g(z)| &= \left| z^n + \sum_{j=0}^{n-2} a_j z^j \right| \leq |z^n| + \sum_{j=0}^{n-2} \left| a_j z^j \right| \\ &= 1 + \sum_{j=0}^{n-2} |a_j| < |a_{n-1}| = \left| a_{n-1} z^{n-1} \right| = |g(z)| . \end{aligned}$$

Hence, the lemma follows from Rouché's Theorem. □

Remark 4.1. In [20], Perron shows that if $f(x) \in \mathbb{Z}[x]$ is as in the statement of Lemma 4.2, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Now using Lemma 4.2 we can establish the following corollary.

Corollary 4.1. *Let n be a positive integer and let*

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 \in \mathbb{Q}[x]$$

with $a_0 \neq 0$. If $|a_{n-1}| = 1 + \sum_{j=0}^{n-2} |a_j|$, then $f(x)$ has at most one root in $\mathbb{C} \setminus \overline{\mathcal{C}}$.

Proof. Let $f(x)$ be as in the statement of the corollary and let $\{G_k(x)\}$ be a sequence of polynomials in $\mathbb{Q}[x]$ defined by $G_k(x) = f(x) - a_0 \cdot \frac{1}{k}$. Notice that Lemma 4.2 implies for $k > 1$ that $G_k(x)$ has exactly $n-1$ roots in $\mathcal{C}$. With the use of Rouché's Theorem this then implies that $f(x)$ has at most one root in $\mathbb{C} \setminus \overline{\mathcal{C}}$. □

4.3 Main Results

To prove Theorem 4.1 and Theorem 4.2 we first establish three lemmas.

Lemma 4.3. *Let n, m, c, and d be positive integers with $n > m$ and $d \geq c+1$. Then the trinomial $f(x) = x^n \pm cx^m \pm d$ has no roots in $\mathcal{C}$. Furthermore, if $d > c+1$, then $f(x)$ has no roots in $\overline{\mathcal{C}}$. Lastly, if $d = c+1$ and $f(\alpha) = 0$ for some $\alpha \in \{z \in \mathbb{C} : |z| = 1\}$, then $\alpha^{2gcd(m,n)} = 1$ and $f(x)$ is reducible in $\mathbb{Z}[x]$.*

Proof. Let n, m, c, and d be positive integers with $n > m$ and let $\alpha \in \mathbb{C}$ with $|\alpha| \leq 1$. Suppose that $d \geq c+1$ and $\alpha^n \pm c\alpha^m \pm d = 0$. Then

$$d = |\alpha^n \pm c\alpha^m| \leq |\alpha^n| + |c\alpha^m| \leq 1 + c \leq d.$$

Clearly each of the inequalities above can be replaced by an equality. Hence, we deduce that $|\alpha| = 1$ and $d = c+1$. Thus the first two parts of the lemma are true. So, suppose that $d = c+1$ and $|\alpha| = 1$. The equality

$$|\alpha^n \pm c\alpha^m| = |\alpha^n| + |c\alpha^m|$$

implies that α^n and α^m lie on the same line passing through the origin. Since $\alpha^n \pm c\alpha^m = \mp d \in \mathbb{Z}^*$, it must be the case that $\alpha^n = \pm 1$ and $\alpha^m = \pm 1$. Thus, $\alpha^{2gcd(n,m)} = 1$. This implies that α is a root of a cyclotomic polynomial. Since $d > 1$ we know that $f(x)$ is not cyclotomic. Hence, $f(x)$ must be reducible. With this, the lemma is proven. □

Lemma 4.4. *Let n, c, and d be positive integers with $n \geq 2$ and $d < (c-1)^{n-1}$. Then the trinomial $f(x) = x^n \pm cx^{n-1} \pm d$ has a root $\alpha \in \mathbb{R}$ with $|\alpha| > c-1$.*

Proof. Let n, c, and d be positive integers with $n \geq 2$ and $d < (c-1)^{n-1}$. We will prove the result in its entirety for $f(x) = x^n + cx^{n-1} + d$ and mention how to prove it for the other three cases. So first let $f(x) = x^n + cx^{n-1} + d$. Write

$$f(x) = (-1)^{n-1}(-x)^{n-1}(x+c) + d$$

and consider

$$f(-c+1) = (-1)^{n-1}(c-1)^{n-1} + d$$

and

$$f(-c-1) = -(-1)^{n-1}(c+1)^{n-1} + d.$$

Notice that if n is odd then $f(-c-1) < 0$ since $d < (c+1)^{n-1}$. On the other hand, if n is even then $f(-c+1) < 0$ since $d < (c-1)^{n-1}$. In either case the result follows by the Intermediate Value Theorem since $f(-c) = d > 0$. If $f(x) = x^n + cx^{n-1} - d$ then the result follows similarly since $f(-c) < 0$ while $f(-c+1) > 0$ when n is odd and $f(-c-1) > 0$ when n is even. The result then follows for the last two cases by considering $f(c), f(c-1)$, and $f(c+1)$. □

Lemma 4.5. *Let K be a positive integer and let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial with no roots in the set $\{z \in \mathbb{C} : |z| \leq K\}$. If $f(x)$ has a root α with $|\alpha| > \frac{|f(0)|}{K+1}$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.*

Proof. Let K be a positive integer, let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial with no roots in the set $\{z \in \mathbb{C} : |z| \leq K\}$, and let $f(\alpha) = 0$ for some $\alpha \in \mathbb{C}$ with $|\alpha| > \frac{|f(0)|}{K+1}$. Suppose that $f(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$ with $g(x) \not\equiv \pm 1$ and $h(x) \not\equiv \pm 1$. Since $f(x)$ is monic it must be the case that the degree of each $g(x)$ and $h(x)$ is non-zero. We may assume without loss of generality that $g(\alpha) = 0$. Now let r be the degree of $h(x)$ and write $h(x) = \prod_{i=1}^{r}(x - \alpha_i)$. Since $f(x)$ has no roots in the set $\{z \in \mathbb{C} : |z| \leq K\}$ we know that $|\alpha_i| > K$ for $1 \leq i \leq r$. Since $h(x) \in \mathbb{Z}[x]$, we deduce that $|h(0)| = \prod_{i=1}^{r} |\alpha_i| \geq K + 1$. Similarly, we have that $|g(0)| > \frac{|f(0)|}{K+1}$.

Hence,

$$|f(0)| = |g(0)|\,|h(0)| > \frac{|f(0)|}{K+1} \cdot (K+1) = |f(0)|\,.$$

This contradiction proves the lemma. □

With these lemmas established we can now prove the main results.

Proof of Theorem 4.1. Let n, c, and d be positive integers with $n \geq 3$. If $d < c-1$, then the theorem follows from Lemma 4.1 and Lemma 4.2. If $c+1 < d \leq 2(c-1)$, then $c > 3$ and the irreducibility of $f(x) = x^n \pm cx^{n-1} \pm d$ follows from Lemma 4.3, Lemma 4.4, and Lemma 4.5 since $\frac{d}{2} \leq c-1$.

This leaves the cases $d = c-1$ and $d = c+1$ to consider. So suppose that $d = c-1$. Notice that Corollary 4.1 implies that $f(x) = x^n \pm cx^{n-1} \pm (c-1)$ has at most one root in $\mathbb{C} \setminus \overline{\mathcal{C}}$. Thus, if $f(x)$ has no roots $\alpha \in \mathbb{C}$ with $|\alpha| = 1$ then $f(x)$ is irreducible by Lemma 4.1. So suppose that $f(\alpha) = 0$ for some $\alpha \in \{z \in \mathbb{C} : |z| = 1\}$. Write $\alpha = a + bi$ for some $a, b \in \mathbb{R}$. Then

$$\begin{aligned}
|\alpha^{n-1}(\alpha \pm c)| = c-1 \quad &\Rightarrow \quad |a \pm c + bi| = c-1 \\
&\Rightarrow \quad (a \pm c)^2 + b^2 = (c-1)^2 \\
&\Rightarrow \quad a^2 + b^2 + c^2 \pm 2ac = c^2 - 2c + 1 \\
&\Rightarrow \quad a = \pm 1 \qquad \text{and} \qquad b = 0.
\end{aligned}$$

Hence, $\alpha = \pm 1$. Notice that 1 and -1 cannot both be roots of $f(x)$. So we can write $f(x) = (x-\alpha)g(x)$ for some $g(x) \in \mathbb{Z}[x]$ for which $g(-\alpha) \neq 0$. Furthermore, since $f'(x) = nx^{n-1} \pm c(n-1)x^{n-2}$ does not have ± 1 as root we know that $g(\alpha) \neq 0$. Hence, since $f(x)$ has at most one root in $\mathbb{C} \setminus \overline{\mathcal{C}}$, this shows that $g(x)$ has at most one root in $\mathbb{C} \setminus \mathcal{C}$. So $g(x)$ is irreducible by Lemma 4.1.

Now suppose that $c+1 = d \leq 2(c-1)$ and $c \neq 3$ when $n = 3$. Notice that with these assumptions $c \geq 3$ and $2(c-1) < (c-1)^{n-1}$. We know from Lemma 4.3 that $f(x)$ has no roots in $\mathcal{C}$ and if $f(x)$ has a root $\alpha \in \{z \in \mathbb{C} : |z| = 1\}$ then $\alpha = \pm 1$. Notice that 1 and -1 cannot both be roots of $f(x)$. So suppose that $\alpha = \pm 1$ is a root of $f(x)$. Then we can write $f(x) = (x-\alpha)g(x)$ for some $g(x) \in \mathbb{Z}[x]$ for which $g(-\alpha) \neq 0$. Notice however that $f'(x) = nx^{n-1} \pm c(n-1)x^{n-2}$ does not have ± 1 as a root. Hence, $g(\alpha) \neq 0$. Since $f(x)$ has no roots in $\mathcal{C}$, this shows that $g(x)$ has no roots in $\overline{\mathcal{C}}$. Hence, $g(x)$ is irreducible by Lemma 4.4 and Lemma 4.5. □

Proof of Theorem 4.2. Let $f(x), g(x), h(x)$, and $k(x)$ be as in the statement of the theorem. If $n = 1$ then the theorem holds trivially. If $c = 2$ or $c = 3$ then the $f(x)$, $g(x)$, $h(x)$, and $k(x)$ all meet Eisenstein's Criterion, and are therefore irreducible. So assume that $c \geq 4$. Notice that

$$\begin{aligned}
x^{n+1} + (c-1)x^n - c &= (x-1)f(x), && \text{for all positive integers } n,\\
x^{n+1} - (c-1)x^n + c &= (x+1)g(x), && \text{whenever } n \text{ is even},\\
x^{n+1} - (c-1)x^n - c &= (x+1)g(x), && \text{whenever } n \text{ is odd},\\
x^{n+1} - (c+1)x^n + c &= (x-1)h(x) && \text{, for all positive integers } n,\\
x^{n+1} + (c+1)x^n + c &= (x+1)k(x), && \text{whenever } n \text{ is odd, and}\\
x^{n+1} + (c+1)x^n - c &= (x+1)k(x), && \text{whenever } n \text{ is even.}
\end{aligned}$$

With this we see that Theorem 4.1 implies the Theorem 4.2 for $n \geq 2$ and $c \geq 4$ as long as $c \neq 4$ whenever $n = 2$. In the case $c = 4$ when $n = 2$ we have $x^2+4x+4 = (x+2)^2$ and $x^2 - 4x + 4 = (x-2)^2$. While it's clear that $x^2 - 4x - 4$ and $x^2 + 4x - 4$ are irreducible, we note here that the irreducibility of these polynomials also follows from Theorem 4.1. □

4.4 Concluding Remarks

In answering the opening questions of this paper we ended up proving a result about trinomials of the form $f(x) = x^n \pm cx^{n-1} \pm d \in \mathbb{Z}[x]$. This result now leads us to more questions.

Question 4.3. *Let n and c be positive integers. For what values of $d > 2(c-1)$ is $f(x) = x^n \pm cx^{n-1} \pm d \in \mathbb{Z}[x]$ irreducible in $\mathbb{Z}[x]$?*

As a remark toward Question 4.3, it is not difficult to show that if n and c are positive integers with n odd, then there are infinitely many positive integers d for which $f(x) = x^n \pm cx^{n-1} \pm d$ has a linear factor. This is of course not the case when n is even since d can be chosen large enough so that $f(x)$ has no real roots. This brings us to our next question.

Question 4.4. *Given positive integers c and n with n even, is there a positive integer K so that $g(x) = x^n \pm cx^{n-1} \pm d \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ for all integers $d \geq K$?*

Finally, we leave the reader with the following conjecture.

Conjecture 4.1. *Let n and c be positive integers with $c \geq 2$ and let $f(x) = x^n \pm cx^{n-1} \pm c$. If $f(x) \neq x^2 + 4x + 4$ and $f(x) \neq x^2 - 4x + 4$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.*

This conjecture has been verified computationally for $1 \leq n \leq 500$ with $2 \leq c \leq 1000$.

Chapter 5

On the Factorization of $f(x)x^n + g(x)$ when $\deg f \leq 2$

5.1 Introduction

Factorization of polynomials of the form $f(x)x^n+g(x)$, where $f(x)$ and $g(x)$ are fixed and n is large, has been considered by Schinzel in [21] and [22], and later by Filaseta, Ford, and Konyagin in [10]. In this paper we consider the special case $f(x) = x^2+bx+c \in \mathbb{Z}[x]$ with $c \geq 2$ and $|b| < 2\sqrt{c-1}$. We additionally impose certain restrictions on $g(x)$. All of the polynomials throughout the chapter are monic polynomials. As such, when we say that a polynomial is reducible, we mean irreducible over $\mathbb{Z}$. In this chapter we prove the following two main theorems.

Theorem 5.1. *Let $f(x) = x^2 + bx + c \in \mathbb{Z}[x]$ with $c \geq 2$ and $|b| < 2\sqrt{c-1}$. Let ϵ be such that $0 < \epsilon < \sqrt{c} - 1$ and $\epsilon \leq 1$. If $g(x) = \sum_{j=0}^{t} a_j x^j \in \mathbb{Z}[x]$ with*

$$1 + |b| + c + \sum_{j=1}^{t} |a_j| < |a_0| < 2(\sqrt{c} - \epsilon)^2,$$

then the polynomial $f(x)x^n + g(x)$ is irreducible for all

$$n > \max\left\{t, \frac{t\log(\sqrt{c}+\epsilon) + \log|a_0| + \log(\min\{t+1,2\}) - \log(\epsilon) - \log\left|\sqrt{4c-b^2} - \epsilon\right|}{\log(\sqrt{c}-\epsilon)}\right\}.$$

For the second theorem we need the following definition.

Definition 5.1. We define the non-cyclotomic part of a non-zero polynomial $w(x) \in \mathbb{Z}[x]$ to be $w(x)$ with all of its cyclotomic factors removed. That is, $k(x)$ is the non-

cyclotomic part of $w(x)$ if we can write $w(x) = h(x)k(x)$ where $h(x)$ is identically 1 or a product of cyclotomic polynomials and $k(x)$ has no cyclotomic factors.

Theorem 5.2. *Let $f(x) = x^2 + bx + c \in \mathbb{Z}[x]$ with $c \geq 2$ and $|b| < 2\sqrt{c-1}$. Let ϵ be such that $0 < \epsilon < \sqrt{c} - 1$ and $\epsilon \leq 1$. Let $g(x) = \sum_{j=0}^{t} a_j x^j \in \mathbb{Z}[x]$ with*

$$1 + |b| + c + \sum_{j=1}^{t} |a_j| = |a_0| < 2(\sqrt{c} - \epsilon)^2.$$

Then for any integer $n \geq t+1$, any cyclotomic factor of $P(x) = f(x)x^n + g(x)$ must be in $\{x+1, x-1\}$. Furthermore, if

$$n > \max\left\{t, \frac{t\log(\sqrt{c}+\epsilon) + \log|a_0| + \log(\min\{t+1,2\}) - \log(\epsilon) - \log(\sqrt{4c-b^2}-\epsilon)}{\log(\sqrt{c}-\epsilon)}\right\},$$

then the non-cyclotomic part of the polynomial $P(x) = f(x)x^n + g(x)$ is irreducible.

We follow up each of these results with several corollaries. Similar results in the case that $f(x)$ is monic and linear are mentioned in the concluding remarks of the paper.

5.2 Three Preliminary Lemmas

Before proving Theorems 5.1 and 5.2 we first establish 3 lemmas.

Lemma 5.1. *Let $f(x)$ and $g(x)$ be non-zero polynomials in $\mathbb{Z}[x]$ of degrees r and t respectively. Let a be the leading coefficient of $f(x)$, and let $\alpha_1, \ldots, \alpha_r$ be the roots of $f(x)$. Let $H(g)$ be the height of $g(x)$; in other words, $H(g)$ is the maximum of the absolute values of the coefficients of $g(x)$. Fix $\epsilon > 0$ and $j \in \{1, \ldots, r\}$. If $|\alpha_j| > 1+\epsilon$ and $f(x)$ has no roots in the set $\{z \in \mathbb{C} : |z - \alpha_j| = \epsilon\}$, then the polynomial $P(x) = f(x)x^n + g(x)$ has at least one root in the set $\{z \in \mathbb{C} : |z - \alpha_j| < \epsilon\}$ for all*

$$n > \frac{t\log(|\alpha_j|+\epsilon) + \log(H(g)) + \log(t+1) - \log|a\epsilon| - \log\left(\prod_{\substack{1\leq i\leq r\\ i\neq j}} ||\alpha_j - \alpha_i| - \epsilon|\right)}{\log(|\alpha_j| - \epsilon)}.$$

Proof. Let $f(x)$ and $g(x)$ be as in the statement of the lemma and let $\epsilon > 0$. For $1 \leq j \leq r$, suppose that $f(x)$ has no roots in the set $\{z \in \mathbb{C} : |z - \alpha_j| = \epsilon\}$. Then for $0 \leq \theta < 2\pi$,

$$\begin{aligned}
\left|f(\alpha_j + \epsilon e^{i\theta})\right| &= \left|a \prod_{i=1}^{r} (\alpha_j + \epsilon e^{i\theta} - \alpha_i)\right| \\
&= |a\epsilon| \prod_{\substack{1 \leq i \leq r \\ i \neq j}} \left|\alpha_j - \alpha_i + \epsilon e^{i\theta}\right| \\
&\geq |a\epsilon| \prod_{\substack{1 \leq i \leq r \\ i \neq j}} \left||\alpha_j - \alpha_i| - \epsilon\right|.
\end{aligned}$$

We also know that for $0 \leq \theta < 2\pi$,

$$\left|g(\alpha_j + \epsilon e^{i\theta})\right| \leq (t+1)H(g)(|\alpha_j| + \epsilon)^t.$$

So let

$$n > \frac{t \log(|\alpha_j| + \epsilon) + \log(H(g)) + \log(t+1) - \log|a\epsilon| - \log\left(\prod_{\substack{1 \leq i \leq r \\ i \neq j}} \left||\alpha_j - \alpha_i| - \epsilon\right|\right)}{\log(|\alpha_j| - \epsilon)}.$$

Then the result follows from Rouché's Theorem since

$$|P(z_0) - f(z_0)z_0^n| = |g(z_0)| < |f(z_0)|\,|z_0|^n$$

for all $z_0 \in \{z \in \mathbb{C} : |z - \alpha_j| = \epsilon\}$. □

Remark 5.1. If $g(x) = \sum_{k=0}^{t} a_k x^k$, then theorems in this paper require $\sum_{k=1}^{t} |a_k| <$

$|a_0|$. Notice then that under the assumptions of Lemma 5.1

$$\begin{aligned}
\left|g(\alpha_j + \epsilon e^{i\theta})\right| &\leq \sum_{k=0}^{t} |a_k| \left(|\alpha_j| + \epsilon\right)^k \\
&\leq \sum_{k=0}^{t} |a_k| \left(|\alpha_j| + \epsilon\right)^t \\
&= \left(|\alpha_j| + \epsilon\right)^t \left(H(g) + \sum_{k=1}^{t} |a_k|\right) \\
&< \left(|\alpha_j| + \epsilon\right)^t (H(g) + H(g)) \\
&= 2H(g)(|\alpha_j| + \epsilon)^t.
\end{aligned}$$

Thus, for the purposes of the theorems in this paper we may take

$$n > \frac{t\log(|\alpha_j| + \epsilon) + \log(H(g)) + \log\left(\min\{t+1, 2\}\right) - \log|a\epsilon| - \log\left(\prod_{\substack{1 \leq i \leq r \\ i \neq j}} ||\alpha_j - \alpha_i| - \epsilon|\right)}{\log(|\alpha_j| - \epsilon)}$$

in the statement of Lemma 5.1.

Lemma 5.2. *Let $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Q}[x]$ and suppose that $a_i \neq 0$ and $a_j \neq 0$ for some $0 \leq i < j \leq n$. Suppose further that*

$$\sum_{\substack{0 \leq k \leq n \\ k \neq t}} |a_k| \leq q^t \cdot |a_t|$$

for some $0 \leq t \leq n$ with $t \neq i$ and $t \neq j$ and $q \in \mathbb{R}$ with $0 < q \leq 1$. If $f(x)$ has a root α in the set $\{z \in \mathbb{C} : q \leq |z| \leq 1\}$, then it must be the case that

$$\sum_{\substack{0 \leq k \leq n \\ k \neq t}} |a_k| = q^t \cdot |a_t|$$

and $|\alpha| = 1$ with $\alpha^{2(j-i)} - 1 = 0$.

Proof. Let $f(x)$ be as in the statement of the theorem. Suppose $\alpha \in \mathbb{C}$ is a root of $f(x)$ with $q \leq |\alpha| \leq 1$. Then

$$\begin{aligned}
q^t \cdot |a_t| &\leq \left|a_t \alpha^t\right| \\
&= \left|a_j \alpha^j + a_i \alpha^i + \sum_{\substack{0 \leq k \leq n \\ k \neq i, k \neq j, k \neq t}} a_k \alpha^k\right| \\
&\leq \left|a_j \alpha^j + a_i \alpha^i\right| + \sum_{\substack{0 \leq k \leq n \\ k \neq i, k \neq j, k \neq t}} \left|a_k \alpha^k\right| \\
&\leq \sum_{\substack{0 \leq k \leq n \\ k \neq t}} \left|a_k \alpha^k\right| \\
&\leq \sum_{\substack{0 \leq k \leq n \\ k \neq t}} |a_k| \\
&\leq q^t \cdot |a_t| .
\end{aligned}$$

Thus, we see immediately that

$$\sum_{\substack{0 \leq k \leq n \\ k \neq t}} |a_k| = q^t \cdot |a_t|$$

and $|\alpha| = 1$. It also follows that $\alpha^{2(j-i)} - 1 = 0$ since

$$\left|a_j \alpha^{j-i} + a_i\right| = \left|a_j \alpha^j + a_i \alpha^i\right| = \left|a_j \alpha^j\right| + \left|a_i \alpha^i\right| .$$

This completes the proof. □

Remark 5.2. The lemma implies that if $i \neq 0$, $j \neq 0$, and $t = 0$, then f has no roots in $\{z \in \mathbb{C} : 0 \leq |z| < 1\}$. To see this, let $0 < q < 1$ get arbitrarily close to 0. This shows that $f(x)$ has no roots in $\{z \in \mathbb{C} : 0 < |z| < 1\}$. Now by assumption, $a_i \neq 0$, $a_j \neq 0$, and $a_0 = a_t \geq |a_i| + |a_j|$. Thus, $f(0) \neq 0$.

Lemma 5.3. *Let $f(x) \in \mathbb{Z}[x]$ be monic with no roots in $\{z \in \mathbb{C} : |z| \leq 1\}$. If $f(x)$ has a root $\alpha \in \mathbb{C} \setminus \mathbb{R}$ with $|\alpha| > \sqrt{\frac{|f(0)|}{2}}$, then $f(x)$ is irreducible.*

Proof. Let $f(x) \in \mathbb{Z}[x]$ be monic with no roots in $\{z \in \mathbb{C} : |z| \leq 1\}$ and let $f(\alpha) = 0$ for some $\alpha \in \mathbb{C} \setminus \mathbb{R}$ with $|\alpha| > \sqrt{\frac{|f(0)|}{2}}$. Suppose that $f(x)$ is not irreducible. Then we can write $f(x) = h(x)k(x)$ for some monic $h(x) \in \mathbb{Z}[x]$ and monic $k(x) \in \mathbb{Z}[x]$, each of positive degree. Since $f(\alpha) = 0$ we may assume without loss of generality that $k(\alpha) = 0$. Since $\alpha \in \mathbb{C}\setminus\mathbb{R}$, this then implies $k(\overline{\alpha}) = 0$. Now let r be the degree of $h(x)$ and let $\alpha_1, \ldots, \alpha_r$ be the roots of $h(x)$. Since $f(x)$ has no roots in $\{z \in \mathbb{C} : |z| \leq 1\}$, we know that $|\alpha_i| > 1$ for $1 \leq i \leq r$. Thus, $|h(0)| \geq 2$, since $h(x) \in \mathbb{Z}[x]$. Similarly, we see that $|k(0)| \geq |\alpha\overline{\alpha}| > \frac{|f(0)|}{2}$. Hence, $|f(0)| = |h(0)|\,|k(0)| > 2 \cdot \frac{|f(0)|}{2} = |f(0)|$. This contradiction proves the lemma. □

5.3 Theorem 5.1 and its Corollaries

With the lemmas in the previous section established, we now prove Theorem 5.1 and provide several corollaries illustrating how the theorem can be used.

Proof of Theorem 5.1. Let $f(x) = x^2 + bx + c \in \mathbb{Z}[x]$ with $c \geq 2$ and $|b| < 2\sqrt{c-1}$. Then the two roots of $f(x)$ are

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4c}}{2} \qquad \text{and} \qquad \alpha_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Since $|b| < 2\sqrt{c-1}$ we see that $b^2 - 4c < -4$. Thus, α_1 and α_2 are non-real and have absolute value $\sqrt{c}$. Now let ϵ be such that $0 < \epsilon < \sqrt{c} - 1$ and $\epsilon \leq 1$. Then

$$|\alpha_j| = \sqrt{c} > 1 + \epsilon \quad \text{for } j \in \{1, 2\}$$

and

$$|\alpha_1 - \alpha_2| = \left|\sqrt{b^2 - 4c}\right| > 2 > \epsilon.$$

Thus, by Lemma 5.1 and the remark after, for $g(x) = \sum_{j=0}^{t} a_j x^j \in \mathbb{Z}[x]$, if

$$n > \max\left\{t, \frac{t\log(\sqrt{c} + \epsilon) + \log|a_0| + \log(\min\{t+1, 2\}) - \log(\epsilon) - \log\left|\sqrt{4c - b^2} - \epsilon\right|}{\log(\sqrt{c} - \epsilon)}\right\},$$

then the polynomial $P(x) = f(x)x^n + g(x)$ has a root α with $|\alpha - \alpha_j| < \epsilon$ for each $j \in \{1, 2\}$. Notice that such an α must be non-real since $b^2 - 4c < -4$ implies that

$$|\mathrm{Im}(\alpha)| = |\mathrm{Im}(\alpha_1 + \alpha - \alpha_1)| \geq |\mathrm{Im}(\alpha_1)| - |\mathrm{Im}(\alpha - \alpha_1)|$$

$$\geq \frac{\left|\sqrt{b^2 - 4c}\right|}{2} - |\alpha - \alpha_2| > 1 - \epsilon \geq 0$$

Now let

$$1 + |b| + c + \sum_{j=1}^{t} |a_j| < |a_0| < 2(\sqrt{c} - \epsilon)^2.$$

Since $|\alpha_j| = \sqrt{c}$, we see that

$$|\alpha| > |\alpha_1 + \alpha - \alpha_1| \geq |\alpha_1| - |\alpha - \alpha_1| > \sqrt{c} - \epsilon > \sqrt{\frac{|a_0|}{2}} = \sqrt{\frac{|P(0)|}{2}}.$$

Also, we deduce from Lemma 5.2 that $P(x)$ has no roots in $\{z \in \mathbb{C} : |z| \leq 1\}$. Hence, $P(x)$ is irreducible by Lemma 5.3. □

Remark 5.3. Let $\epsilon = 1$, $c \geq 16$, $|b| < 2\sqrt{c-1}$, and $|a_0| < 2(\sqrt{c} - \epsilon)^2$. Then

$$\frac{t\log(\sqrt{c} + \epsilon) + \log|a_0| + \log(\min\{t+1, 2\}) - \log(\epsilon) - \log\left|\sqrt{4c - b^2} - \epsilon\right|}{\log(\sqrt{c} - \epsilon)}$$

$$\leq \frac{t\log(\sqrt{c} + 1) + \log(2(\sqrt{c} - 1)^2) + \log(2)}{\log(\sqrt{c} - 1)}$$

$$= 2 + \log(2) + \log(2) + \frac{t\log(\sqrt{c} + 1)}{\log(\sqrt{c} - 1)}$$

$$< 4 + \frac{t\log(\sqrt{c} + 1)}{\log(\sqrt{c} - 1)}.$$

Letting

$$A(c) = \frac{\log(\sqrt{c} + 1)}{\log(\sqrt{c} - 1)}$$

it can be checked that $A(c)$ is a decreasing function of c and $A(c) = 1.46\ldots < \frac{3}{2}$. Thus, if $c \geq 16$ in Theorem 5.1, then one can take $\epsilon = 1$ and the result holds for $n \geq 4 + \frac{3t}{2}$.

Now, letting $\epsilon = 1$ we use Theorem 5.1 to prove the following four corollaries. We note here that the results in these corollaries can be improved slightly by letting $0 < \epsilon < 1$.

Corollary 5.1. *Let n and c be positive integers, and let $d \in \mathbb{Z}$ such that $c+1 < |d| < 2(\sqrt{c}-1)^2$. Then the trinomial $x^{n+2} + cx^n + d$ is irreducible.*

Proof. Let n and c be positive integers, and let $d \in \mathbb{Z}$ such that $c + 1 < |d| < 2(\sqrt{c}-1)^2$. Notice then that $c \geq 16$. Now we write $P(x) = f(x)x^n + g(x)$ where $f(x) = x^2 + c$ and $g(x) = d$. Since $t = \deg\, g = 0$, we deduce from Theorem 5.1 that if

$$\frac{\log|d| - \log(2\sqrt{c}-1)}{\log(\sqrt{c}-1)} < \frac{\log(2(\sqrt{c}-1)^2) - \log(2\sqrt{c}-1)}{\log(\sqrt{c}-1)} < 1 \leq n,$$

then $P(x)$ is irreducible. □

Corollary 5.2. *Let n and c be positive integers with $n \geq 3$, and let d and $\ell \neq 0$ be integers such that $1 + c + |\ell| < |d| < 2(\sqrt{c}-1)^2$. Then the quadrinomial $x^{n+2} + cx^n + \ell x + d$ is irreducible.*

Proof. Let n and c be positive integers with $n \geq 3$, and let d and $\ell \neq 0$ be integers such that $1 + c + |\ell| < |d| < 2(\sqrt{c}-1)^2$. Since $1 + c + |\ell| < |d| < 2(\sqrt{c}-1)^2$ it must be the case that $c \geq 17$. Now we write $P(x) = f(x)x^n + g(x)$ where $f(x) = x^2 + c$ and $g(x) = \ell x + d$. Since $t = \deg\, g = 1$, we deduce from Theorem 5.1 that if

$$\frac{\log(\sqrt{c}+1) + \log(2) + \log(2(\sqrt{c}-1)^2) - \log(2\sqrt{c}-1)}{\log(\sqrt{c}-1)} < 3 \leq n,$$

then $P(x)$ is irreducible. □

Corollary 5.3. *Let n and c be positive integers with $n \geq 3$, and let d and b be integers such that $0 < |b| \leq 2\sqrt{c-1}$ and $1+c+|b| < |d| < 2(\sqrt{c}-1)^2$. Then the quadrinomial $x^{n+2} + bx^{n+1} + cx^n + d$ is irreducible.*

Proof. Let n and c be positive integers with $n \geq 3$ and let d and b be integers such that $0 < |b| \leq 2\sqrt{c-1}$ and $1 + c + |b| < |d| < 2(\sqrt{c}-1)^2$. Since $1 + c + |b| < |d| < 2(\sqrt{c}-1)^2$ it must be the case that $c \geq 17$. Now we write $P(x) = f(x)x^n + g(x)$ where $f(x) = x^2 + bx + c$ and $g(x) = d$. Since $t = \deg\, g = 0$, we deduce from Theorem 5.1 that if

$$\frac{\log|d| - \log(\sqrt{4c-b^2}-1)}{\log(\sqrt{c}-1)} < \frac{\log(2(\sqrt{c}-1)^2)}{\log(\sqrt{c}-1)} < 3 \leq n,$$

then $P(x)$ is irreducible. □

Corollary 5.4. *Let b and t be integers with $t \geq 1$ and let $g(x) = \sum_{j=1}^{t} a_j x^j \in \mathbb{Z}[x]$. There exists a positive integer λ so that for all integers $c \geq \lambda$ and all integers $n \geq t+3$, if d is an integer with $1 + |b| + |c| + \sum_{j=1}^{t} |a_j| < |d| < 2(\sqrt{c}-1)^2$, then the polynomial $(x^2 + bx + c)x^n + g(x) + d$ is irreducible.*

Proof. Let b and t be integers with $t \geq 1$ and let $g(x) = \sum_{j=1}^{t} a_j x^j \in \mathbb{Z}[x]$. Choose λ_1 so that $\max\left\{5, \frac{b^2}{4} + 1\right\} < \lambda_1$. Then for any integers c and d with $c \geq \lambda_1$ and $|d| < 2(\sqrt{c}-1)^2$,

$$\frac{t\log(\sqrt{c}+1) + \log(\min\{t+1, 2\}) + \log|d| - \log\left|\sqrt{4c-b^2}-1\right|}{\log(\sqrt{c}-1)}$$

$$< \quad \frac{t\log(\sqrt{c}+1) + \log(2) + \log(2(\sqrt{c}-1)^2)}{\log(\sqrt{c}-1)}.$$

Now notice that

$$\lim_{c\to\infty} \frac{t\log(\sqrt{c}+1) + \log(2) + \log(2(\sqrt{c}-1)^2)}{\log(\sqrt{c}-1)} = t + 2.$$

Thus, λ_2 can be chosen so that for all $c \geq \lambda_2$,

$$\frac{t\log(\sqrt{c}+1) + \log(2) + \log(2(\sqrt{c}-1)^2)}{\log(\sqrt{c}-1)} < t + 3.$$

Now by Theorem 5.1, letting $\epsilon = 1$ and $\lambda = \max\{\lambda_1, \lambda_2\}$ proves the result. □

5.4 Theorem 5.2 and its Corollaries

Next we prove Theorem 5.2 and provide several corollaries illustrating how the theorem can be used.

Proof of Theorem 5.2. Let $f(x) = x^2 + bx + c \in \mathbb{Z}[x]$ with $c \geq 2$ and $|b| < 2\sqrt{c-1}$. Let $g(x) = \sum_{j=0}^{t} a_j x^j \in \mathbb{Z}[x]$ with $|a_0| < 2(\sqrt{c} - \epsilon)^2$. Now choose ϵ so that $0 < \epsilon < \sqrt{c} - 1$ and $\epsilon \leq 1$. Following the proof of Theorem 5.1 we see that if

$$n > \max\left\{t, \frac{t\log(\sqrt{c}+\epsilon) + \log|a_0| + \log(\min\{t+1,2\}) - \log(\epsilon) - \log\left|\sqrt{4c-b^2} - \epsilon\right|}{\log(\sqrt{c}-\epsilon)}\right\},$$

then the polynomial $P(x) = f(x)x^n + g(x)$ has a root $\alpha \in \mathbb{C} \setminus \mathbb{R}$ with $|\alpha| > \sqrt{c} - \epsilon > \sqrt{\frac{|a_0|}{2}}$.

Now suppose that

$$1 + |b| + c + \sum_{j=1}^{t} |a_j| = |a_0|.$$

Then for $n \geq t+1$ we deduce from Lemma 5.2 that $P(x)$ has no roots in $\{z \in \mathbb{C} : |z| < 1\}$. Furthermore, Lemma 5.2 implies that if $P(x)$ has a root $\beta \in \{z \in \mathbb{C} : |z| = 1\}$, then $\beta^4 = 1$ since $c \neq 0$. Lemma 5.2 further implies that if $b \neq 0$, then $\beta^2 = 1$. Notice however that in the case $b = 0$,

$$\left|(-1+c)i^n + \sum_{j=1}^{t} a_j i^j\right| \leq |c-1| + \sum_{j=1}^{t} |a_j| < c + 1 + \sum_{j=1}^{t} |a_j| = |a_0|.$$

From this we deduce that $P(i) \neq 0$. Thus, β is a root of some cyclotomic polynomial in $\{x+1, x-1\}$. This proves the first implication of the theorem.

Now write $P(x) = h(x)k(x)$ so that $h(x)$ is a product of cyclotomic polynomials and $k(x)$ has no cyclotomic factors. It then follows that $|k(0)| = |a_0|$ and $k(x)$ has no roots in $\{z \in \mathbb{C} : |z| \leq 1\}$. Also, since $h(x)$ is the product of cyclotomic polynomials and $|\alpha| > \sqrt{c} - \epsilon > 1$, we know that $k(\alpha) = 0$. Since

$$|\alpha| > \sqrt{\frac{|a_0|}{2}} = \sqrt{\frac{|k(0)|}{2}},$$

we deduce from Lemma 5.3 that $k(x)$ must be irreducible. □

Remark 5.4. Notice that Theorem 5.2 implies that $P(x)$ is reducible if and only if $P(x)$ has a root in $\{-1, 1\}$.

Corollary 5.5. *Let n and c be positive integers with $c \geq 2$. Then for $\nu \in \{-1, 1\}$, the following are true for the trinomial $P(x) = x^{n+2} + cx^n + \nu \cdot (c+1)$:*

1. *If n is odd and $\nu = 1$, then $P(x) = (x+1)k(x)$ for some irreducible $k(x) \in \mathbb{Z}[x]$.*
2. *If n is even and $\nu = 1$, then $P(x)$ is irreducible unless $P(x) = x^4 + 3x^2 + 4$ or $P(x) = x^4 + 5x^2 + 6$.*
3. *If n is odd and $\nu = -1$, then $P(x) = (x-1)k(x)$ for some irreducible $k(x) \in \mathbb{Z}[x]$.*
4. *If n is even and $\nu = -1$, then $P(x) = (x+1)(x-1)k(x)$ for some irreducible $k(x) \in \mathbb{Z}[x]$ unless $P(x) = x^6 + 3x^4 - 4$.*

Proof. Let n and c be positive integers with $c \geq 2$ and let $\nu \in \{-1, 1\}$. It follows from Theorem 5.2 that if $P(x) = x^{n+2} + cx^n + \nu \cdot (c+1)$ has a cyclotomic factor, then it must be in the set $\{x+1, x-1\}$. Furthermore, since $P'(x) = (n+2)x^{n+1} + cnx^{n-1}$, we see that any roots of $P(x)$ in $\{-1, 1\}$ must be of multiplicity one. Hence, if $c \geq 16$, then the result follows from Theorem 5.2 by letting $\epsilon = 1$. Now suppose that $2 \leq c \leq 15$. Let

$$\epsilon = \frac{\sqrt{c} - \sqrt{\frac{c+1}{2}}}{2} < \sqrt{c} - 1$$

so that $c + 1 < 2(\sqrt{c} - \epsilon)^2$ and $\epsilon \leq 1$. A computation gives that

$$\frac{\log(c+1) - \log(\epsilon) - \log(2\sqrt{c} - \epsilon)}{\log(\sqrt{c} - \epsilon)} < 9.$$

Thus, the result follows from Theorem 5.2 with $\epsilon = \frac{\sqrt{c} - \sqrt{\frac{c+1}{2}}}{2}$ for $2 \leq c \leq 15$ and $n \geq 9$. The remaining cases can easily be checked computationally. □

Corollary 5.6. *Let n and c be positive integers with $c \geq 2$. Then the polynomials*

$$f(x) = x^{2n} - x^{2n-1} + c(x^{2n-2} - x^{2n-3} + x^{2n-4} - \cdots - x + 1)$$

$$g(x) = x^{2n} + x^{2n-1} + c(x^{2n-2} + x^{2n-3} + \cdots + x + 1)$$

$$\textit{and} \qquad h(x) = x^{2n} + c(x^{2(n-1)} + x^{2(n-2)} + \cdots + x^2 + 1)$$

are all irreducible, with the exception $h(x) = x^4 + 4x^2 + 4$.

Proof. Let k and c be positive integers with $c \geq 2$. The result follows by observing that

$$\begin{aligned}
x^{k+2} + cx^k + (c+1) &= (x+1)f(x), && \text{whenever } k = 2n-1,\\
x^{k+2} + cx^k - (c+1) &= (x-1)g(x), && \text{whenever } k = 2n-1,\\
x^{k+2} + cx^k - (c+1) &= (x+1)(x-1)h(x), && \text{whenever } k = 2n
\end{aligned}$$

and applying Corollary 5.5. □

Corollary 5.7. *Let n, c, and ℓ be integers with $n \geq 4$, $c \geq 3$, and $0 < |\ell| \leq c-2$. Then for $\nu \in \{-1, 1\}$, the following are true for the quadrinomial $P(x) = x^{n+2} + cx^n + \ell x + \nu \cdot (c + 1 + |\ell|)$:*

1. *If n is odd, $\ell > 0$, and $\nu = 1$, then $P(x) = (x+1)k(x)$ for some irreducible $k(x) \in \mathbb{Z}[x]$.*
2. *If n is even, $\ell > 0$, and $\nu = 1$, then $P(x)$ is irreducible.*
3. *If n is even, $\ell < 0$, and $\nu = -1$, then $P(x) = (x+1)k(x)$ for some irreducible $k(x) \in \mathbb{Z}[x]$.*
4. *If n is odd, $\ell < 0$, and $\nu = -1$, then $P(x)$ is irreducible.*
5. *If $\ell > 0$ and $\nu = -1$, then $P(x) = (x-1)k(x)$ for some irreducible $k(x) \in \mathbb{Z}[x]$.*
6. *If $\ell < 0$ and $\nu = 1$, then $P(x)$ is irreducible.*

Proof. Let $n \geq 4$, $c \geq 3$ and $0 < |\ell| \leq c-2$. It follows from Theorem 5.2 that if $P(x) = x^{n+2} + cx^n + \ell x + \nu \cdot (c+1)$ has a cyclotomic factor, then it must be in the set $\{x+1, x-1\}$. Furthermore, since $P'(x) = (n+2)x^{n+1} + cnx^{n-1} + \ell$ and $|\ell| \leq c-2$, we see that any roots of $P(x)$ in $\{-1, 1\}$ must be of multiplicity one. Now let $\epsilon = \frac{1}{4\sqrt{c}}$ so that $0 < \epsilon < \sqrt{c} - 1$ and $\epsilon \leq 1$. Notice then that $c + |\ell| + 1 \leq 2c - 1 < 2(\sqrt{c} - \epsilon)^2$. Also notice that

$$\begin{aligned}
&\frac{\log(\sqrt{c}+\epsilon) + \log(c+|\ell|+1) + \log(2) - \log(\epsilon) - \log(2\sqrt{c}-\epsilon)}{\log(\sqrt{c}-\epsilon)} \\
&\qquad \leq \frac{\log(\sqrt{c}+\epsilon) + \log(2(\sqrt{c}-\epsilon)^2) + \log(2) - \log(\epsilon) - \log(2(\sqrt{c}-\epsilon))}{\log(\sqrt{c}-\epsilon)} \\
&\qquad \leq 1 + \frac{\log(\sqrt{c}+\epsilon)}{\log(\sqrt{c}-\epsilon)} + \frac{\log(2)}{\log(\sqrt{c}-\epsilon)} - \frac{\log(\epsilon)}{\log(\sqrt{c}-\epsilon)} \\
&\qquad \leq 1 + \frac{\log(8c+2)}{\log\left(\sqrt{c} - \frac{1}{2\sqrt{3}}\right)}.
\end{aligned}$$

Letting

$$A(c) = 1 + \frac{\log(8c+2)}{\log\left(\sqrt{c} - \frac{1}{2\sqrt{3}}\right)},$$

one can check that $A(c)$ is a decreasing function of c. Thus, when $c \geq 79$ the result follows from Theorem 5.2 since $A(c) < 4$. We then check computationally that $A(c) < 10$ for $c \in \{3, \ldots, 78\}$. With this the result follows from Theorem 5.2 for $n \geq 10$ and $c \in \{3, \ldots, 78\}$. The remaining cases can then be checked computationally. □

5.5 Concluding Remarks

The methods used to prove Theorems 5.1 and 5.2 are similar to methods found in Chapter 3 of this document. There we investigated the factorization of trinomials of the form $x^{n+1} + cx^n + d = (x+c)x^n + d \in \mathbb{Z}[x]$ with certain restrictions on n, c, and d. The following is a result given in that chapter.

Lemma 5.4. *Let K be a positive integer and let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial with no roots in the set $\{z \in \mathbb{C} : |z| \leq K\}$. If $f(x)$ has a root α with $|\alpha| > \frac{|f(0)|}{K+1}$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.*

Using this lemma with $K = 1$ along with Lemma 5.1 and the remark after, as well as Lemma 5.2, one can prove the following two theorems. We omit proofs here, as the results follow similarly to the proofs of Theorems 5.1 and 5.2.

Theorem 5.3. *Let $|c| \geq 2$ and let $0 < \epsilon < |c| - 1$. If $g(x) = \sum_{j=0}^{t} a_j k^j \in \mathbb{Z}[x]$ with*

$$1 + |c| + \sum_{j=1}^{t} |a_j| < |a_0| < 2(|c| - \epsilon),$$

then the polynomial $(x + c)x^n + g(x)$ is irreducible for all

$$n > \max\left\{t, \frac{t\log(|c| + \epsilon) + \log|a_0| + \log(\min\{t + 1, 2\}) - \log(\epsilon)}{\log(|c| - \epsilon)}\right\}.$$

Theorem 5.4. *Let $|c| \geq 2$ and let $0 < \epsilon < |c| - 1$. Let $g(x) = \sum_{j=0}^{t} a_j k^j \in \mathbb{Z}[x]$ with*

$$1 + |c| + \sum_{j=1}^{t} |a_j| = |a_0| < 2(|c| - \epsilon).$$

For

$$n > \max\left\{t, \frac{t\log(|c| + \epsilon) + \log|a_0| + \log(\min\{t + 1, 2\}) - \log(\epsilon)}{\log(|c| - \epsilon)}\right\},$$

the non-cyclotomic part of the polynomial $P(x) = (x + c)x^n + g(x)$ is irreducible. Furthermore, any cyclotomic factor of $P(x)$ must be in $\{x + 1, x - 1\}$.

Bibliography

[1] A. Brauer, On algebraic equations with all but one root in the interior of the unit circle, Math. Nachr. 4 (1951) 250-257.

[2] Y.G. Chen, On integers of the form $2^n \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, Proc. Amer. Math. Soc. 128 (2000) 1613-1616.

[3] Y.G. Chen, On integers of the form $k2^n + 1$, Proc. Amer. Math. Soc. 129 (2001) 355-361.

[4] Y.G. Chen, On integers of the forms $k - 2^n$ and $k2^n + 1$, J. Number Theory 89 (2001) 121-125.

[5] Y.G. Chen, On integers of the forms $k^r - 2^n$ and $k^r 2^n + 1$, J. Number Theory 98 (2003) 310-319.

[6] Y.G. Chen, On integers of the forms $k \pm 2^n$ and $k2^n \pm 1$, J. Number Theory 125 (2007) 14-25.

[7] P. Erdős, On integers of the form $2^k + p$ and some related problems, Summa Brasil. Math. (1950) 113-123.

[8] M. Filaseta, Coverings of the integers associated with an irreducibility theorem of A. Schinzel, in Number theory for the millennium, II (Urbana, IL, 2000), pages 1–24, A K Peters, Natick, MA, 2002.

[9] M. Filaseta, C. Finch, M. Kozek, On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture, J. Number Theory 128 (2008) 1916-1940.

[10] M. Filaseta, K. Ford, S. Konyagin, On an irreducibility theorem of A. Schinzel associated with covering of the integers, Illinois J. Math. 44(3) (2000), 633-643.

[11] M. Filaseta, J. Harrington, A polynomial investigation inspired by work of Schinzel and Sierpiński, Acta Arith., 155 (2012) 149-161.

[12] M. Filaseta, M. Matthews Jr., On the irreducibility of 0,1-polynomials of the form $f(x)x^n + g(x)$, Colloq. math. 99 (2004) 1-5.

[13] C. Finch, J. Harrington, L. Jones, Nonlinear Sierpiński and Riesel numbers, J. Number Theory, 133 (2013) 534-544.

[14] J. Harrington, On the Factorization of the Trinomials $x^n + cx^{n-1} + d$, Int. J. Number Theory , 08 (2012), 1513-1518.

[15] A.S. Izotov, A note on Sierpiński numbers, Fibonacci Quart. 33 (1995) 206-207.

[16] L. Jones, Variations on a theme of Sierpiński, J. Integer Seq. 10 (2007), Article 07.4.4, 15pp. (electronic.)

[17] L. Jones, Polynomial variations on a theme of Sierpiński, Int. J. Number Theory 5 (2009), 999-1015.

[18] M.B. Nathanson, Elementary Methods in Number Theory, Springer-Verlag, 2000.

[19] H. Riesel, Nagra stora primtal, Elementa 39 (1956) 258-260.

[20] O. Perron, Neue kriterion für die Irreduzibilität algebraischer gleichungen, Journal für die reine und angewandte Mathematik, 132 (1907) 288-307.

[21] A. Schinzel, On the reducibility of polynomials and in particular of trinomials, Acta. Arith. 11 (1965), 1-34.

[22] A. Schinzel, Reducibility of polynomials and covering systems of congruences, Acta. Arith. 13 (1967), 91-101.

[23] W. Sierpiński, Sur un problème concernant les nombres $k \cdot 2^n + 1$, Elem. Math. 15 (1960), 73–74.