Summer 2023

Widely Digitally Delicate Brier Primes and Irreducibility Results for Some Classes of Polynomials

Thomas David Luckner

Widely Digitally Delicate Brier Primes and Irreducibility Results for Some Classes of Polynomials

by

Thomas David Luckner

Bachelor of Science
Eastern Connecticut State University 2018

Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy in

Mathematics

College of Arts and Sciences

University of South Carolina

2023

Accepted by:

Michael Filaseta, Major Professor

Ognian Trifinov, Committee Member

Frank Thorne, Committee Member

Stephen Fenner, Committee Member

Ann Vail, Dean of the Graduate School

Dedication

To my mom and dad for their continued positivity and support of my education.

Acknowledgments

The journey to this point has been both difficult and rewarding. Without the support and positivity of my family and friends, I would not have been able to get to this crucial point in my life. The first of which I would like to thank is my advisor, Dr. Michael Filaseta. Thank you for agreeing to work with me and dealing with my inability to form grammatically correct sentences. Your expertise and direction are a large reason why this dissertation is complete. I would also like to thank my committee members for their understanding in this tedious process while also showing interest in my graduate school journey.

Next I would like to extend my gratitude to the many others who have supported me at some point throughout this process. First is my family: Aunt Judy, Uncle Patrick, Aunt Jen, Uncle Dan, Aunt Cheryl, Katie, Ally, and Elizabeth. Second is all of my chosen family Maria, Jack, Tamang, Mizan, Doug Connor, Emma, Tito, and Miss Cindy.

Saving the best for last, I would like to thank my immediate family; Mom, Dad, and Kevin. You three have been by my side through everything in my life and my graduate school career was no exception. The confidence you instilled in me, even when you no longer understood what I was doing in school, is something that very few people are able to have. Your perfect balance of high expectations with support in any decision I make is a recipe for success in any child. I owe you the world for everything I have achieved.

Abstract

This dissertation considers three different sections of results. In the first part of the dissertation, a result on consecutive primes which are widely digitally delicate and Brier numbers is discussed. Making use of covering systems and a theorem of D. Shiu, M. Filaseta and J. Juillerat showed that for every positive integer k, there exist k consecutive widely digitally delicate primes. They also noted that for every positive integer k, there exist k consecutive primes which are Brier numbers. We show that for every positive integer k, there exist k consecutive primes that are both widely digitally delicate and Brier numbers. This is joint work with M. Filaseta and J. Juillerat.

In the second part of the dissertation, we prove an irreducibilty result for a class of polynomials. Consider the polynomial $F(x) = f(x) + Mg(x)$ where M is a positive integer and $f(x), g(x) \in \mathbb{Z}[x]$ such that $\gcd(f(x), g(x)) = 1$. A version of Hilbert's Irreducibility Theorem in this setting implies that $F(x)$ is irreducible for almost all M. In the case that $\deg f < \deg g$, recent results by M. Cavachi, M. Vajaitu, and A. Zaharescu [14] and by N.C. Bonciocat, Y. Bugeaud, M. Cipu, and M. Mignotte [9] have given definitive examples where irreducibility occurs by taking M to be a prime power bounded below by an explicit function depending on f and g. We provide a wider class of definitive examples by taking M with a large prime factor, and in particular our explicit examples include a set of M with positive asymptotic density in the integers. We then extend the result to bivariate polynomials in a manner similar to work by N.C. Bonciocat, Y. Bugeaud, M. Cipu, and M. Mignotte [9]. This is joint work with M. Filaseta.

In the third part of the dissertation, we prove the irreducibility of nth order Euler polynomials of even degree n. For m an even positive integer and p a prime, we show that the generalized Euler polynomial $E_{mp}^{(mp)}(x)$ is in Eisenstein form with respect to p if and only if p does not divide $m(2^m - 1)B_m$. As a consequence, we deduce that at least $1/3$ of the generalized Euler polynomials $E_n^{(n)}(x)$ are in Eisenstein form with respect to a prime p dividing n and, hence, irreducible over $\mathbb{Q}$. This is joint work with M. Filaseta.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

In this dissertation, we will go into detail on two main topics in number theory: classes of prime numbers and irreducibility of polynomials. This introduction is broken into three sections; the first section is on results from M. Filaseta, J. Juillerat and the author of this dissertation in [22]. The second section is on irreducibility results for a specific class of polynomials. The third section is on results in [24] for the irreducibility of some generalized Euler polynomials. The chapters following the introduction will be in three separate chapters based on the sections in this introduction.

1.1 Consecutive primes which are widely digitally delicate and Brier numbers

In [44], R.M. Robinson constructed a table which represents all primes of the form $k\cdot 2^n+1$ for all odd integers $1 \leq k < 100$ and all integers $0 \leq n \leq 512$. The table brings up many questions about primes of this form. At first glance one may notice some k producing many primes of this form while others have few. More interestingly, when $k = 47$, there was not a single prime found. This sparked some interest in determining if 47 or any other k will result in $k \cdot 2^n + 1$ always being composite for any positive integer n. W. Sierpiński was one such mathematician motivated by this phenomenon, later proving that there are infinitely many positive k such that $k\cdot 2^n+1$ is composite for all positive integers n [46]. This motivated the following definition.

Definition 1 (Sierpiński Number)**.** *Any positive odd integer k such that $k \cdot 2^n + 1$ is*

composite for positive integers n is called a Sierpiński number.

In fact, Sierpiński showed that for every nonnegative integer m the number

$$k = 15511380746462593381 + 36893488147419103230\, m$$

is a Sierpiński number. Note that the original paper of Sierpiński did not require k to be odd. This condition was added later in response to the search for the smallest Sierpiński number.

The search for the smallest Sierpiński number has been an ongoing project. In 1962, J. Selfridge (see [47]) found $k = 78557$ to be a Sierpiński number and asked whether it is the smallest. Selfridge used the common technique of covering systems to prove this, which will be a technique discussed in more detail later in this dissertation. It is widely believed this is, in fact, the smallest Sierpiński number. However, it has not been proven to be the smallest. In order to prove this, it must be shown that for each positive odd integer k less than 78557, the number $k \cdot 2^n + 1$ is a prime for some positive integer n. Although seemingly simple, this task has proven difficult. In March of 2002, there was a set $\mathcal{R}$ of 17 remaining odd positive integers k less than 78557 for which no positive integer n was known with $k \cdot 2^n + 1$ prime. The problem quickly became a computational project, and L. Heim and D. Norris started the Seventeen or Bust project in hopes of proving 78557 is the smallest Sierpiński number (see [41]). The project was successful in reducing the size of the set $\mathcal{R}$ to 6. In October 2016, one of the remaining 6 odd positive integers k less than 78557 was shown to have the property that $k \cdot 2^n + 1$ is prime for some positive integer n by the successor of the Seventeen or Bust project, PrimeGrid. As of February 2023, there are still 5 more odd positive integers less than 78557, namely 21181, 22699, 24737, 55459, and 67607, to confirm are not Sierpiński numbers before proving 78557 is the smallest Sierpiński number. PrimeGrid has verified for all $n \leq 31875742$ that $k \cdot 2^n + 1$ is composite for these remaining 5 integers k.

If k is allowed to be even, then 65536 is most likely the smallest Sierpiński number. This conjecture is more strongly believed since, for a positive integer n, the number $65536 \cdot 2^n + 1 = 2^{n+16} + 1$ is prime only when $n + 16$ is a power of 2. It is widely believed due to heuristic arguments that the largest Fermat prime, $2^n + 1$, is $2^{16} + 1$. If so, then $2^{16} = 65536$ is a Sierpiński number (if Sierpiński numbers are allowed to be even).

Following Sierpiński's success with $k \cdot 2^n + 1$, many tried to replicate results by altering the form. Just four years after the publication of Sierpiński's result, Bowen [11] showed, in a short note, given a fixed base b, there are infinitely many positive integers k for which $k \cdot b^n + 1$ is odd and composite for all positive integers n. This result proved Sierpiński's original result for any base b. A. Brunner, C. Caldwell, et. al. [12] strengthened Bowen's result by showing that there exists such k but with also $\gcd(k + 1, b - 1) = 1$ and k not a rational power of b. These extra conditions avoid some simple constructions given by Bowen.

A natural question that also follows from the table in Robinson's paper is to instead look at k for which $k \cdot 2^n - 1$ is composite for all positive integers n. Consequently, around the same time as Sierpiński's work, Hans Riesel [43] showed for every nonnegative integer m, when

$$k = 509203 + 11184810\, m,$$

the number $k \cdot 2^n - 1$ is composite for all positive integers n. This led to the following definition.

Definition 2 (Riesel Number)**.** *Any positive odd integer k such that $k \cdot 2^n - 1$ is composite for all positive integers n is called a Riesel number.*

Just like Sierpiński numbers, there is a conjectured smallest Riesel number which happens to be 509203 in the arithmetic progression discovered by Riesel above (See OEIS [51]) . In August 2003, The Riesel Sieve Project took to being the analogous

project to the Seventeen or Bust project and sought to show all odd positive integers less than 509203 are not Riesel numbers. The project paired up with PrimeGrid to reduce the number of possible Riesel numbers less than 509203 down to 48. No progress has been made although it has been shown for the remaining 48 that $k \cdot 2^n - 1$ is composite for $n \leq 11300000$ (See OEIS [51]).

As mentioned previously, a common technique among these related results is the use of covering systems. Not only is this a common technique amongst the related material in this dissertation, but often times a very powerful tool in number theory.

Definition 3 (Covering System)**.** *For nonnegative integers a_i and positive integers b_i, the set of congruence classes*

$$\{a_1 \pmod{b_i}, \quad a_2 \pmod{b_2}, \quad \ldots, \quad a_m \pmod{b_m}\}$$

is called a covering system (or a covering for short) if, for every integer n, we have $n \equiv a_i \pmod{b_i}$ for at least one $i \in \{1, 2, \ldots, m\}$.

Consider the collection of congruence classes in Table 1.1. We claim every integer

Table 1.1 Covering System

Congruence Classes
$n \equiv 0 \pmod{2}$
$n \equiv 0 \pmod{3}$
$n \equiv 1 \pmod{4}$
$n \equiv 5 \pmod{6}$
$n \equiv 7 \pmod{12}$

satisfies one of the congruence classes in Table 1.1. Any integer will be of the form $12t + j$ where t is an integer and $j \in \{0, 1, \ldots, 11\}$. One can check that for every j (regardless of t), the number $12t + j$ satisfies one of the congruence classes in Table 1.1. More precisely, even numbers (where j is even) satisfy 0 modulo 2. Similarly for 0 modulo 3 covers the integers where j is divisible by 3. We are left with $j \in \{1, 5, 7, 11\}$.

Both $12t+1$ and $12t+5$ are 1 modulo 4. The remaining numbers $12t+11$ and $12t+7$ satisfy the last two congruence classes of Table 1.1, respectively.

To help give insight as to how a covering argument may take shape, consider Table 1.2. To confirm the collection of congruence classes in Table 1.2 is a covering,

Table 1.2 Covering System 2

Congruence Classes
$n \equiv 0 \pmod 2$
$n \equiv 0 \pmod 3$
$n \equiv 1 \pmod 4$
$n \equiv 3 \pmod 8$
$n \equiv 7 \pmod{12}$
$n \equiv 23 \pmod{24}$

following the ideas of the previous example, we only need to check every nonnegative integer up to the least common multiple of the moduli satisfies one of the congruence classes. Any even integer is congruent to 0 modulo 2. After also eliminating those which are 0 modulo 3, we are left with showing 1, 5, 7, 11, 13, 17, 19, and 23 are in at least one of the congruence classes. The numbers 1, 5, 13, and 17 all are 1 modulo 4. Both 11 and 19 are 3 modulo 8. That leaves 7 and 23 which are in the last two congruence classes respectively. Thus, the congruences in Table 1.2 form a covering system.

The notion of a covering system was introduced by Erdős in the 1930s as a means to find counterexamples to de Polignac's question "is it the case that every sufficiently large odd integer $x > 1$ can be written as $x = p + 2^n$ for some nonnegative integer n and some prime p?" It had been shown there are infinitely many odd integers where this is not possible, so Erdős sought to find an infinite arithmetic progression of counterexamples. Erdős chose congruence classes for x to satisfy such that $|x - 2^n|$ is composite for all nonnegative integers n.

Since the congruence classes for n in Table 1.2 form a covering, all n must satisfy one of the congruence classes. We take x so that it satisfies all of the congruences

Table 1.3 Erdős Problem Solution

Congruence Classes for n	Congruence Classes for x	Prime Dividing $x - 2^n$
$n \equiv 0 \pmod 2$	$x \equiv 1 \pmod 3$	3
$n \equiv 0 \pmod 3$	$x \equiv 1 \pmod 7$	7
$n \equiv 1 \pmod 4$	$x \equiv 2 \pmod 5$	5
$n \equiv 3 \pmod 8$	$x \equiv 8 \pmod{17}$	17
$n \equiv 7 \pmod{12}$	$x \equiv 11 \pmod{13}$	13
$n \equiv 23 \pmod{24}$	$x \equiv 121 \pmod{241}$	241

in column 2 of Table 1.3, which is possible by the Chinese Remainder Theorem. Consider the first row of Table 1.3. When $n \equiv 0 \pmod 2$ and $x \equiv 1 \pmod 3$, we have that $n = 2k$ for some integer k and

$$x - 2^n \equiv 1 - 2^{2k} \equiv 0 \pmod 3$$

just as the last column of Table 1.3 indicates. The Chinese Remainder Theorem gives that $x - 2^n$ is divisible by at least one of 3, 7, 5, 17, 13, and 241 for all nonnegative integers n when $x \equiv 7629217 \pmod{11184810}$, that is, when

$$x = 7629217 + 11184810\, m,$$

for any nonnegative integer m. Thus, all x in the arithmetic progression are counterexamples to de Polignac's question as long as $x - 2^n$ is not one of the primes in column 3 of Table 1.3 for some nonnegative integer n.

One can confirm that $x - 2^n$ is never one of the primes in column 3 of Table 1.3 by considering $x - 2^n$ modulo 7 and modulo 3. For every nonnegative integer n, the number 2^n is congruent to 1, 2, or 4 modulo 7. Since $x \equiv 1 \pmod 7$, the number $x - 2^n$ is congruent to 0, 4, or 6 modulo 7. The only primes in column 3 of Table 1.3 that are 0, 4, or 6 modulo 7 are 7 and 13. Similarly, 2^n is congruent to either 1 or 2 modulo 3 for all nonnegative integers n and, since $x \equiv 1 \pmod 3$, the number $x - 2^n$ is congruent to either 0 or 2 modulo 2. Both 7 and 13 are congruent to 1 modulo 3. Therefore, there is no x in the arithmetic progression such that $x - 2^n$ is a prime in

column 3 of Table 1.3 and all x in the arithmetic progression are counterexamples to de Polignac's question.

For another example more applicable to the results in this dissertation of how one can use a covering system argument, consider Sierpiński numbers. Pick $a_1, \ldots, a_m$ and $b_1, \ldots, b_m$ as in the definition of a covering system, with the b_i not necessarily distinct, and suppose we can find distinct primes $p_1, p_2, \ldots, p_m$ such that p_i divides $2^{b_i} - 1$. Then

$$k \cdot 2^{a_i + \ell_i b_i} + 1 \equiv k \cdot 2^{a_i} + 1 \pmod{p_i}$$

for all $1 \leq i \leq m$. Thus, for at least $k > \max_{1 \leq i \leq m}\{p_i\}$, solutions k to the m congruences

$$\{k \cdot 2^{a_1} + 1 \equiv 0 \pmod{p_1}, \quad \ldots, \quad k \cdot 2^{a_m} + 1 \equiv 0 \pmod{p_m}\}$$

are Sierpiński numbers. This kind of construction of a covering system works for obtaining Riesel numbers in a similar way. The solutions to this type of construction is typically given as an arithmetic progression based on the congruence classes k satisfies.

Just like we can use this technique to find k which are Sierpiński numbers or Riesel numbers, we can use covering systems to find k which are both Sierpiński and Riesel. Such k are called Brier numbers. Below we formally define these numbers.

Definition 4 (Brier Numbers)**.** *Any positive odd integer k such that $k \cdot 2^n + 1$ is composite for all positive integers n and $k \cdot 2^n - 1$ is composite for all positive integers n is called a Brier number. In other words, if k is both a Sierpiński number and a Riesel number, then k is a Brier number.*

Just like Sierpiński numbers and Riesel numbers, Brier showed that such odd integers exist and there infinitely many of them although his result was unpublished in 1998 (see [19] for this result formally) . In fact, Brier showed that

$$29364695660123543278115025405114452910889$$

is a Brier number and found an arithmetic progression of odd integers k that are Brier numbers via the same covering system technique mentioned previously. The existence of Brier numbers gave rise to the same questions as Sierpiński numbers and Riesel numbers. For example, what is the smallest Brier number. In August 2009, A. Wesolowski showed that the smallest Brier number must be larger than 10^9 (see [29]). In December 2013, Clavier showed that any number in the arithmetic progression

$$3316923598096294713661 + 377021473959660125796259470411 0\, m,$$

is a Brier number for a nonnegative integer m (see [29]). In fact, the smallest known Brier number is 331692359809629471366 1 as found via Clavier's arithmetic progression. A consequence of Clavier's arithmetic progression, as noted by M. Filaseta and J. Juillerat in [19], is the following corollary.

Corollary 5. *For every positive integer k, there exists k consecutive primes all of which are Brier numbers.*

Corollary 5 relies on heavily on a result of D. Shiu [45].

Theorem 6 (D. Shiu, [45])**.** *Let $Am + B$ be an arithmetic progression with A and B nonnegative integers, and let k be any positive integer. If $Am + B$ contains infinitely many primes, then there exist k consecutive primes $p_1, p_2, \ldots, p_k$ in the arithmetic progression.*

Based on the statement of Theorem 6, Corollary 5 relies on Clavier's arithmetic progression containing infinitely many primes. An arithmetic progression $Am + B$ with A, B, and m nonnegative integers and $A > 0$ contains infinitely many primes exactly when A and B are relatively prime. Notice that

$$3316923598096294713661 \quad \text{and} \quad 377021473959660125796259470411 0$$

are relatively prime as we wanted, thus proving Corollary 5. This approach will be a key ingredient for the main result of the associated chapter of this dissertation. Theo-

rem 6 was strengthened by W.D. Banks, T. Freiberg, and C.L. Turnage-Butterbaugh [5] and J. Maynard [37] (also, see T. Freiberg [27]). The main result of the associated chapter for this dissertation will make use of Theorem 7 instead of Theorem 6.

Theorem 7 (J. Maynard, [37]). *For every positive integer k, in any arithmetic progression $Am + B$, where $A > 0$, $B \geq 0$, $m \geq 0$ are integers with A and B fixed and $\gcd(A, B) = 1$, a positive proportion of positive integers ℓ are such that $p_\ell, p_{\ell_1}, \ldots, p_{\ell+k-1}$ are all in the arithmetic progression $Am + B$ where p_i is the i^{th} prime.*

So far, we have only discussed the first class of integers which the main result of the associated chapter will address; Brier numbers. The remaining class of integers the main result will refer to is widely digitally delicate primes. First we define the less restrictive class of integers, digitally delicate primes.

Definition 8 (Digitally Delicate). *Let b be an integer ≥ 2. A prime number is called digitally delicate in base b (or simply digitally delicate for $b = 10$) if changing any base b digit of the prime to another base b digit results in a composite number.*

In 1979, the credited inventor of the use of covering systems, P. Erdős, showed that there are infinitely many digitally delicate primes [16], just like Sierpiński numbers, Riesel numbers, and Brier numbers. Similarly, the smallest digitally delicate prime was found: 294001. In other words,

$$d94001, \quad 2d4001, \quad 29d001, \quad 294d01, \quad 2940d1, \quad \text{and} \quad 29400d$$

are composite or equal to 294001 for every $d \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Once again, the technique of covering systems was used by Erdős although only a "partial" covering system combined with a sieve argument came into play. Tao, in 2011, refined the sieve argument to show a positive lower asymptotic density of primes are digitally

delicate [49]. Applying this concept to composite numbers, Konyagin proved a positive lower asymptotic density of composite numbers which are coprime to 10 remain composite if any base 10 digit of the number is changed to another base 10 digit [33]. Both Tao and Konyagin have similar results for every base.

The idea of digitally delicate primes was extended in base 10 by Filaseta and J. Southwick in [25] by adding the condition that changing any of the infinitely many leading zeroes still results in a composite number. Not only did they show an analogous result to Erdős', but also to Tao's result.

Definition 9 (Widely Digitally Delicate)**.** *Let b be an integer ≥ 2. A prime number is widely digitally delicate in base b if changing any base b digit of the prime, including the infinitely many leading 0's, to another base b digit results in a composite number. Note that we refer to widely digitally delicate primes in base 10 as, simply, widely digitally delicate primes.*

Filaseta and Southwick [25] discussed a similar result for some other bases as well. To illustrate the extent at which widely digitally delicate primes is more restrictive than digitally delicate primes, consider a positive integer n in base 10 with r digits. Then there are 9^r numbers formed by changing a digit of n, each of which one wants to check for primality. If you add in checking the leading zeros, now you have infinitely many possible digit changes that could imply the integer is not widely digitally delicate. For example, consider the smallest digitally delicate prime, 294001. To be widely digitally delicate, the leading zeros must not result in a prime number when changed to a different digit. However, 10294001 is a prime number where the second leading zero digit of 294001 was changed to a 1. Thus, 294001 is not widely digitally delicate. In fact, Filaseta and Southwick showed none of the primes $< 10^9$ are widely digitally delicate [25]. This discovery and result was mentioned in Quanta Magazine [38] along with a related result from Filaseta and J. Juillerat [19] (also see [40]).

Theorem 10. *For every positive integer k, there exist k consecutive widely digitally delicate primes.*

J. Grantham [30] found the first (currently only) known explicit example of a widely digitally delicate prime. The prime contains 4032 digits. Note early versions of his paper as well as a comment in [38] contain an example he provided which was later corrected.

In the associated chapter of this dissertation, we use methods from [19] used to prove Theorem 10 to obtain a similar result where the widely digitally delicate primes are also Brier numbers.

Theorem 11 (Main Theorem of Chapter 2)**.** *For every positive integer k, there exist k consecutive primes $p_\ell, p_{\ell+1}, \ldots, p_{\ell+k-1}$, each of which is both a widely digitally delicate prime and a Brier number. Furthermore, the first primes p_ℓ in consecutive lists of k such primes have positive density (depending on k) in the set of prime numbers. In particular, a positive proportion of the primes are both a widely digitally delicate prime and a Brier number.*

As corollaries to Theorem 11, we will establish the following.

Corollary 12. *For every positive integer k, there exist k consecutive primes that are widely digitally delicate in both base 2 and base 10.*

Our next result should be compared to the definition of a Sierpiński number.

Corollary 13. *For every positive integer k, there are k consecutive primes, $p_\ell, p_{\ell+1}, \ldots, p_{\ell+k-1}$ such that for any integer $a \in [2, 937]$, $p_i \cdot a^n + 1$ is composite for every positive integer n and all $\ell \leq i \leq \ell + k - 1$.*

The proof of Corollary 13, a consequence not so much of Theorem 11 but rather of its proof, was the motivation for additional joint research (outside this dissertation) by the author of this dissertation. This additional research [18] was done with M. Filaseta

and R. Groth. We proved a stronger result than Corollary 13 which will be featured in the dissertation of Groth in the upcoming years. Therefore, the proof of this stronger result will be omitted from this dissertation. The proof of Corollary 13 will be given at the end of Chapter 2. For clarification, we state our stronger result below.

Theorem 14. *Pick A to be a positive integer ≥ 2. For every positive integer k, there are k consecutive primes, $p_\ell, p_{\ell+1}, \ldots, p_{\ell+k-1}$ such that for every $a \in [2, A]$, the number $p_i \cdot a^n + 1$ is composite for every positive integer n and all $\ell \leq i \leq \ell + k - 1$.*

1.2 A lower bound for the irreducibility of the sum of two relatively prime polynomials

In 1892, D. Hilbert [31] proved what is now called the Hilbert Irreducibility Theorem. The theorem has many variations and proofs, but in general terms the theorem says that an irreducible polynomial in several variables can find infinitely many specializations of some preselected variables so the resulting polynomial remains irreducible in the remaining variables. In the associated section of this dissertation, we consider polynomials of the form $F(x, M) = f(x) + Mg(x)$ where $f(x)$ and $g(x)$ are nonconstant relatively prime polynomials in $\mathbb{Z}[x]$. Hilbert's Irreducibility Theorem implies then that $F(x, M)$ is irreducible over $\mathbb{Q}$ for infinitely many (even most) positive integers M. However, Hilbert's Irreducibility Theorem does not give us explicit M for which $F(x, M)$ is irreducible over $\mathbb{Q}$. The goal of the associated section of this dissertation is to provide the reader with explicit integers M, depending on $f(x)$ and $g(x)$, of positive asymptotic density such that $F(x, M)$ is irreducible. First, we mention prior works that motivate this result.

In [13], M. Cavachi, with some inspiration from Fried and Langmann in [28] and [35] respectively, showed that for relatively prime polynomials $f(x), g(x) \in \mathbb{Q}[x]$ with $\deg f < \deg g$, the polynomial $f(x) + pg(x)$ is irreducible over $\mathbb{Q}$ for all but finitely

many primes p. Once again, the result does not indicate for which p the polynomial $f(x) + pg(x)$ is irreducible in $\mathbb{Q}[x]$.

In [14], M. Cavachi, M. Vajaitu, and A. Zaharescu established an explicit lower bound b, depending only on $f(x)$ and $g(x)$, such that for all primes $p > b$, the polynomial $f(x) + pg(x)$ is irreducible over $\mathbb{Q}$ given the same conditions in Cavachi's earlier result. In [9], N.C. Bonciocat, Y. Bugeaud, M. Cipu, and M. Mignotte were able to give a similar result in the case that M is a power of a prime, which we state next.

Theorem 15 ([9]). *Let $f, g \in \mathbb{Z}[x]$ be two relatively prime polynomials with $\deg g = n$ and $\deg f = n - d$, where $d \geq 1$. Then for any prime number p that divides none of the leading coefficients of f and g, and any positive integer k relatively prime to d such that*

$$p^k \geq \left(2 + \frac{1}{2^{n+1-d}H(g)^{n+1}}\right)^{n+1-d} H(f)H(g)^n - \frac{H(f)}{H(g)},$$

the polynomial $f(x) + p^k g(x)$ is irreducible over $\mathbb{Q}$.

Note that here H refers to the height of a polynomial so that, for example, $H(f)$ is the maximum of the coefficients of $f(x)$ in absolute value. Three years later in [7], Bonciocat proved a lower bound on p where $f(x) + p^k g(x)$ is irreducible over $\mathbb{Q}$.

Theorem 16 ([7]). *Let $f, g \in \mathbb{Z}[x]$ be relatively prime polynomials with $\deg f < \deg g$. Then for any prime p and any positive integer k relatively prime to $\deg g$ such that*

$$p > \left(2 + \frac{1}{2^{k(\deg f+1)(\deg g-1)}}\right)^{(\deg f+1)(\deg g-1)} H(f)^{\deg g-1} H(g)^{\deg f(\deg g-1)+1},$$

the polynomial $f(x) + p^k g(x)$ is irreducible over $\mathbb{Q}$.

In Theorem 15 and Theorem 16, the focus is on primes and prime powers. The set of all prime powers has asymptotic density 0 in the set of integers. The associated section of this dissertation will focus on describing explicit positive integers M,

depending only on f and g, with $f(x) + Mg(x)$ irreducible over $\mathbb{Q}$ and where the set of such M has positive asymptotic density in the set of integers.

Similar to the proofs of Theorem 15 and 16, the proof of the main result in the associated section of this dissertation makes use of a theorem of Dumas [15]. To understand this theorem, first we must define Newton polygons.

Definition 17. *Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$, and let p be a prime. For $j \in \{0, \ldots, n\}$, define (x_j, y_j) in the extended plane by taking $x_j = j$ and $y_j = +\infty$ if $a_{n-j} = 0$ and otherwise $y_j \in \mathbb{Z}^+ \cup \{0\}$ such that $p^{y_j} \mid a_{n-j}$ but $p^{y_j+1} \nmid a_{n-j}$. Let*

$$S_f = \{(x_0, y_0), \ldots, (x_n, y_n)\}.$$

Consider the lower edges along the convex hull of these points. The polygonal path formed by these edges is the Newton polygon for $f(x)$ with respect to p.

We refer to *an edge of a Newton polygon* as a line segment along the Newton polygon, including its endpoints, with no two edges having the same slope. The path formed by the convex hull always has the left-most edge starting at (x_0, y_0) and the right-most edge ending at (x_n, y_n). Notice that the slopes of the edges are increasing from the left-most edge to the right-most edge.

Consider the following example where $f(x) = 3x^3 + 9x^2 + 2x + 27$. If we want to construct the Newton polygon of $f(x)$ with respect to 3, we compute the set of points

$$S_f = \{(0, 1), (1, 2), (2, 0), (3, 3)\}.$$

The convex hull of these points is made up of two edges, one from $(0, 1)$ to $(2, 0)$ and one from $(2, 0)$ to $(3, 3)$. This gives us the Newton polygon for $f(x)$ with respect to 3 in Figure 1.1.

This geometric representation of a polynomial with respect to a prime is useful in determining reducibility of the polynomial. The following theorem of Dumas [15] provides the tools needed to use Newton polygons for arguments of reducibility.

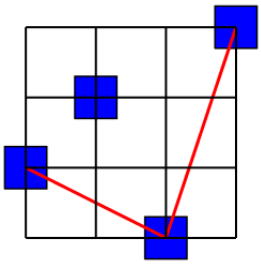

Figure 1.1 Newton Polygon for $f(x)$ with respect to 3

Theorem 18. *Let $g(x)$ and $h(x)$ be in $\mathbb{Z}[x]$ with $g(0)h(0) \neq 0$, and let p be a prime. Let k be a nonnegative integer such that p^k divides the leading coefficient of $g(x)h(x)$ but p^{k+1} does not. Then the edges of the Newton polygon of $g(x)h(x)$ with respect to p can be formed by constructing a polygonal path beginning at $(0, k)$ and using translates of the edges in the Newton polygons for $g(x)$ and $h(x)$ with respect to the prime p, using exactly one translate for each edge of the Newton polygons for $g(x)$ and $h(x)$. Necessarily, the translated edges are translated in such a way as to form a polygonal path with slopes of the edges increasing.*

To illustrate the theorem, consider the polynomials $f(x) = 3x^3 + 9x^2 + 2x + 27$ and $g(x) = 2x^2 + 9x + 3$. The Newton polygon for $f(x)$ with respect to 3 is Figure 1.1 where the first edge has slope of $-1/2$ and the second edge has a slope of 3. Now consider the Newton polygon for $g(x)$ with respect to 3. Figure 1.2 shows this Newton polygon.

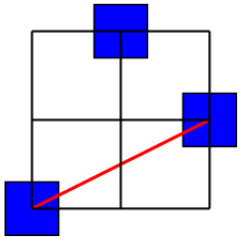

Figure 1.2 Newton Polygon for $g(x)$ with respect to 3

Notice in Figure 1.2 that there is only one edge, and it has slope $1/2$. The product

of the two polynomials is $h(x) = 6x^5 + 45x^4 + 92x^3 + 90x^2 + 246x + 81$ which has the Newton polygon with respect to 3 shown in Figure 1.3.

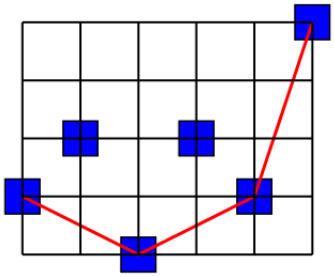

Figure 1.3 Newton Polygon for $h(x)$ with respect to 3

In Figure 1.3, there are 3 edges for the Newton polygon of $h(x)$. The first edge from left to right has a slope of $-1/2$. The second edge has a slope of $1/2$. The last edge has a slope of 3. A quick comparison shows that each of the edges of $h(x)$ is a translate of one of edges in the Newton polygons of $f(x)$ or $g(x)$.

We can also use Dumas' theorem to prove irreducibilty. Consider the polynomial $F(x) = 6x^4 + 12x^3 + 9x^2 + 4x + 6$ and its Newton polygon with respect to 2 in Figure 1.4.

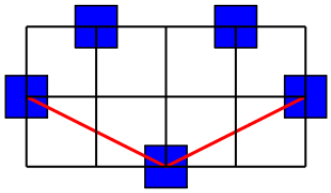

Figure 1.4 Newton Polygon for $F(x)$ with respect to 2

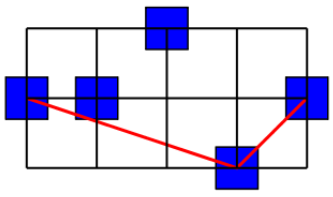

Figure 1.5 Newton Polygon for $F(x)$ with respect to 3

In Figure 1.4, the two edges indicate that if $F(x)$ is reducible, it has two irreducible

quadratic factors. However, in Figure 1.5, which shows the Newton polygon of $F(x)$ with respect to 3, the two edges indicate that if $F(x)$ is reducible, it is the product of a linear polynomial and an irreducible cubic. Thus, we can conclude that $F(x)$ is irreducible in $\mathbb{Z}[x]$. This technique will be crucial in the proof of the main result.

We also extend the main result of the associated section of this dissertation to bivariate polynomials in a manner similar to [9]. For this purpose, we use the following version of Dumas' theorem to multivariate polynomials as stated there. To clarify, the definition of a Newton polygon with respect to a prime p in R below is defined in the analogous way to Definition 17.

Theorem 19. *Let R be a unique factorization domain, p be a prime element of R, and let $f = gh$, where f, g, and h are nonconstant polynomials in $R[y]$. Then the system of vectors forming the Newton polygon of f with respect to p is the union of the system of vectors forming the Newton polygons of g and h with respect to p.*

To help illustrate the extension, we provide an example with a bivariate polynomial. Suppose $f(x, y) = x^5y^5 + x^2y^4 - y^2 + x^4y + x^6 \in R[y]$, where $R = \mathbb{Z}[x]$. We will look at the Newton polygon of $f(x, y)$ with respect to the prime element x in R. We form the convex hull from the set of points

$$S_f = \{(0, 5), (1, 2), (2, +\infty), (3, 0), (4, 4), (5, 6)\}.$$

From this set of points, $(0, 5)$, $(1, 2)$, $(3, 0)$, and $(5, 6)$ are the points that form the convex hull. Thus, Figure 1.6 below is the Newton polygon for $f(x, y)$ with respect to x.

Notice the Newton polygon is made of 3 vectors: $(0, 5)$ to $(1, 2)$, $(1, 2)$ to $(3, 0)$, and $(3, 0)$ to $(5, 6)$. Therefore, the Newton polygon with respect to x for any factors of $f(x, y)$ must contain some translations of these vectors just as in the univariate case of Dumas' theorem.

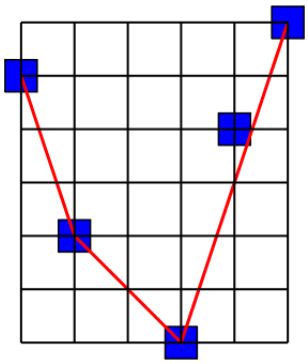

Figure 1.6 Newton Polygon for $f(x, y)$ with respect to x

1.3 On *n*th order Eisenstein Polynomials of degree n that are Eisenstein

For m a positive integer, the mth order Bernoulli polynomial of degree n, denoted $B_n^{(m)}(x)$, and the mth order Euler polynomial of degree n, denoted $E_n^{(m)}(x)$, are defined by

$$\left(\frac{t}{e^t-1}\right)^m e^{tx} = \sum_{n=0}^{\infty} B_n^{(m)}(x)\frac{t^n}{n!}$$

and

$$\left(\frac{2}{e^t+1}\right)^m e^{tx} = \sum_{n=0}^{\infty} E_n^{(m)}(x)\frac{t^n}{n!}, \tag{1.1}$$

respectively. Let ν_p denote the usual p-adic valuation so that, in particular, for non-zero integers a and b, we have $\nu_p(a) = k \in \mathbb{Z}^+ \cup \{0\}$ means that $p^k \mid a$ and $p^{k+1} \nmid a$ and $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$. A polynomial $f(x) \in \mathbb{Q}[x]$ is said to be *Eisenstein* if there is an integer a and a prime p for which the well-known Eisenstein criterion applies to $f(x+a) = \sum_{j=0}^{n} a_j x^j$ so that $\nu_p(a_n) = 0$, $\nu_p(a_j) \geq 1$ for $j \in \{0, 1, \ldots, n-1\}$, and $\nu_p(a_0) = 1$. Eisenstein's criterion implies that Eisenstein polynomials are irreducible over $\mathbb{Q}$ if $n \geq 1$. In the special case that $a = 0$, we say that $f(x)$ *is in Eisenstein form* or, if p is fixed, that $f(x)$ *is in Eisenstein form with respect to* p. A. Adelberg and M. Filaseta [4] showed, somewhat surprisingly, that Eisenstein's criterion applies to many of the nth order Bernoulli polynomials of degree n. More precisely, they

showed that

$$\liminf_{t\to\infty} \frac{|\{n \le t : B_n^{(n)}(x) \text{ is in Eisenstein form}\}|}{t} > \frac{1}{5}. \tag{1.2}$$

Experimentally, the author of this dissertation and M. Filaseta noticed that the Euler polynomials $E_n^{(n)}(x)$ often also appear to be in Eisenstein form. The polynomials $E_n^{(n)}(x)$ have been investigated less in the literature, so we are not as readily able to apply known results to derive such a result. However, as we will see, we are still able to establish the following results.

Theorem 20. *Let m be an even positive integer and p be an odd prime. Then $E_{mp}^{(mp)}(x)$ is in Eisenstein form with respect to p if and only if p does not divide $m(2^m-1)B_m$.*

To clarify, since m is even, the number $m(2^m-1)B_m$ appearing in Theorem 20 is an integer (cf. [4, Lemma 1]).

Theorem 21. *Asymptotically, more than one-third of the polynomials $E_n^{(n)}(x)$ are irreducible (and in fact Eisenstein). More precisely,*

$$\liminf_{t\to\infty} \frac{|\{n \le t : E_n^{(n)}(x) \text{ is in Eisenstein form}\}|}{t} \ge \frac{\log 2}{2} = 0.34657\ldots.$$

The main part of the associated chapter is devoted to the proof of Theorem 20. The proof of Theorem 21 is based on applying Theorem 20 in the case that $p > m$. As a positive proportion of n have a prime factor greater than $\sqrt{n}$, it is reasonable to expect that one can deduce a positive proportion of n can be shown to be Eisenstein in this manner. The ideas for the proof of Theorem 20 are closely related to arguments in [4]. However, we are able to get a better density bound by modifying the arguments slightly. The better bound applies to the case of the Bernoulli polynomials $B_n^{(n)}(x)$ dealt with in [4] and as a consequence the right-hand side of (1.2) can be replaced with $(\log 2)/2$. As the argument for this sharpening of (1.2) is essentially identical to our proof of Theorem 21, we do not elaborate on improving (1.2) further.

Before leaving this section of the introduction, we note that $E_n^{(n)}(x)$ is not Eisenstein for every odd $n > 1$. To see this, it suffices to show, for such n, that $E_n^{(n)}(n/2) = 0$, as then $E_n^{(n)}(x)$ is reducible. By (1.1), we obtain

$$\sum_{n=0}^{\infty} E_n^{(m)}(m/2)\frac{t^n}{n!} = \left(\frac{2}{e^t+1}\right)^m e^{tm/2} = \left(\frac{2}{e^{t/2}+e^{-t/2}}\right)^m,$$

which is an even function of t. Thus, in fact, we have $E_n^{(m)}(m/2) = 0$ for all positive integers n and m, with n odd.

Chapter 2

Consecutive primes which are widely digitally delicate and Brier numbers

This chapter will focus on the results from section 1.1 of the introduction. The aim is to prove Theorem 11, Corollary 12, and Corollary 13. We will begin by providing some preliminary results necessary in proving Corollary 12 and then provide the proof of Corollary 12. Then, we will discuss the proof of Theorem 11. Lastly, we will provide the proof of Corollary 13 along with some discussion of its connections to other works.

2.1 Some preliminaries and a proof of Corollary 12

In the section 1.1 of the introduction, we discussed the proof of Theorem 10 based on the use of Shiu's theorem. This included finding an arithmetic progression $Am + B$ where $\gcd(A, B) = 1$ and every number in the arithmetic progression is a Brier number. The goal for establishing Theorem 11 is to construct an arithmetic progression $Am + B$, with fixed positive relatively prime integers A and B, with A divisible by 10 and having a prime divisor > 10, and with a variable nonnegative integer m, such that every integer k of the form $Am + B$ satisfies

- for every nonnegative integer n and $d \in \{-9, \ldots, -1, 1, \ldots, 9\}$, the number $k + d \cdot 10^n$ is divisible by at least one prime p dividing A,
- for every nonnegative integer n, the number $k \cdot 2^n + 1$ is divisible by at least one prime p dividing A, and

- for every nonnegative integer n, the number $k \cdot 2^n - 1$ is divisible by at least one prime p dividing A.

Provided we can also find such a progression that avoids the expressions $k + d \cdot 10^n$, $k \cdot 2^n + 1$ and $k \cdot 2^n - 1$ above from being equal to a prime divisor of A, then Theorem 11 will follow directly from Shiu's theorem. Observe that for $m \geq 2$, we have $k \cdot 2^n + 1$ and $k \cdot 2^n - 1$ are both at least $(2A + B)2^n - 1 \geq 2A$, which is larger than any prime divisor of A. By replacing B then by $2A + B$, we obtain a new arithmetic progression with every element contained in the previous progression, so that the three bulleted items above are still satisfied. Thus, with B so changed, the expressions $k \cdot 2^n + 1$ and $k \cdot 2^n - 1$ cannot equal a prime divisor of A. The next lemma allows us to adjust A and B further so that the expressions $k + d \cdot 10^n$ in the first bullet above cannot equal a prime divisor of A.

Lemma 22. *Let b be an integer ≥ 2. Let A and B be positive relatively prime integers such that A has a prime divisor $> b$ and every prime dividing b divides A. Suppose further that for every nonnegative integers m and k and for*

$$d \in \{-(b-1), -(b-2), \ldots, -1\} \cup \{1, 2, \ldots, b-1\},$$

there is a prime p dividing A which also divides $Am + B + d \cdot b^k$. Then, a subprogression $A_0 m + B_0$ can be found, with A_0 and B_0 relatively prime and A dividing A_0, such that for every nonnegative integers m and k and for d as above, there is a prime p dividing A_0 with

$$p \mid \left(A_0 m + B_0 + d \cdot b^k\right) \quad \text{and} \quad A_0 m + B_0 + d \cdot b^k \neq \pm p.$$

Proof. Let A' be the largest positive integer dividing A that is relatively prime to b. Then there is a positive integer u such that A divides $b^u A'$. Furthermore, taking $v = \phi(A')$ and a positive integer $\ell \geq u$, we see that A divides $b^{\ell(v+1)} - b^\ell$. We take

$\ell \geq \max\{u, 2\}$ sufficiently large so that also $b^\ell > A + B$, and set

$$A_0 = b^{\ell(v+2)}A \qquad \text{and} \qquad B_0 = b^{\ell(v+1)} - b^\ell + B.$$

Note that $\ell \geq 2$ ensures that $\ell(v+1)-1 \geq 2\ell-1 \geq \ell+1$, which we use momentarily. Since A divides $b^{\ell(v+1)} - b^\ell$, we see that for every nonnegative integer m, there is a nonnegative integer m' such that $A_0m+B_0 = Am'+B$, so the arithmetic progression A_0m+B_0 is a subprogression of the arithmetic progression $Am+B$. By the properties of the progression $Am + B$, we deduce that for every nonnegative integers m and k and for $d \in \{-(b-1), -(b-2), \ldots, -1\} \cup \{1, 2, \ldots, b-1\}$, there is a prime p dividing A, and hence A_0, with $p \mid \left(A_0m + B_0 + d \cdot b^k\right)$. Furthermore, if $k \leq \ell(v+1) - 1$, we see that

$$\begin{aligned} A_0m + B_0 + d \cdot b^k &= b^{\ell(v+2)}Am + b^{\ell(v+1)} - b^\ell + B + d \cdot b^k \\ &\geq b^{\ell(v+1)} - b^\ell + B - (b-1)b^{\ell(v+1)-1} \\ &= b^{\ell(v+1)-1} - b^\ell + B \geq b^{\ell+1} - b^\ell + B \\ &> b^\ell > A \end{aligned}$$

for every nonnegative integer m. Also, if $k \geq \ell(v+1)$, then $k \geq 2\ell$ so that

$$A_0m + B_0 + d \cdot b^k \equiv -b^\ell + B \pmod{b^{2\ell}}.$$

Since $b^\ell > A + B$, we see that

$$-b^{2\ell} + A < b^\ell - b^{2\ell} < -b^\ell < -b^\ell + B < -A.$$

In this case, $A_0m + B_0 + d \cdot b^k$ is in a residue class modulo $b^{2\ell}$ represented by an integer in $(A, b^{2\ell} - A)$. In both cases, that is $k \leq \ell(v+1) - 1$ and $k \geq \ell(v+1)$, we deduce that since $p \leq A$, we have $A_0m + B_0 + d \cdot b^k \neq \pm p$ □

As noted before Lemma 22, we will find an arithmetic progression $Am + B$, with $10 \mid A$ and A divisible by a prime > 10, satisfying the bullets above. The comments

before Lemma 22 together with Lemma 22 with $b = 10$ allow us to find a subprogression of $Am + B$ such that every prime k in the subprogression is both widely digitally delicate and a Brier number. Shiu's theorem will then imply Theorem 11.

We are now ready to prove Corollary 12.

Proof of Corollary 12 (assuming the existence of $Am + B$ as above). To establish an integer k is widely digitally delicate in base 2, it suffices to show $k \pm 2^n$ is composite for all nonnegative integers n. Let $k = Am + B$, with A and B as above and m a nonnegative integer. Fix a nonnegative integer n. Let

$$T = n \prod_{p|A} (p - 1).$$

Then by the second bullet above, there is a prime p dividing A such that

$$(Am + B) \cdot 2^{T-n} + 1 \equiv 0 \pmod{p},$$

Since $2^T \equiv 1 \pmod{p}$, we deduce

$$(Am + B) \cdot 2^{-n} + 1 \equiv 0 \pmod{p}.$$

Multiplying both sides of the congruence by 2^n gives

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

Thus, for each nonnegative integer n, the number $k + 2^n$ is divisible by a prime dividing A. Similarly, for each nonnegative integer n, we can see that the third bullet above implies that the number $k - 2^n$ is divisible by a prime dividing A. By applying Lemma 22 first with $b = 10$ and then with $b = 2$, we see that there is a subprogression of $Am + B$ containing infinitely many primes such that every prime in the subprogression is widely digitally delicate in both base 10 and base 2. Shiu's theorem applies as before to complete the proof. □

2.2 The coverings

As explained in the previous section, we are interested in finding an arithmetic progression $Am + B$, with $\gcd(A, B) = 1$ and with A divisible by 10 and some prime > 10, satisfying the bulleted items at the beginning of the previous section. By replacing A with a power of A, we may suppose that $B < A$ and do so. We will refer to properties (i), (ii) and (iii) analogous to the bullets of the previous section as follows.

(i) If $d \in \{-9, -8, \ldots, -1\} \cup \{1, 2, \ldots, 9\}$, then each number in the set

$$\mathcal{A}_d = \mathcal{A}_d(A, B) = \left\{Am + B + d \cdot 10^n : m \in \mathbb{Z}^+ \cup \{0\},\ n \in \mathbb{Z}^+ \cup \{0\}\right\}$$

is composite.

(ii) Each number in the set

$$\mathcal{B}_S = \mathcal{B}_S(A, B) = \{(Am + B) \cdot 2^n + 1 : m \in \mathbb{Z}^+ \cup \{0\},\ n \in \mathbb{Z}^+ \cup \{0\}\}$$

is composite.

(iii) Each number in the set

$$\mathcal{B}_R = \mathcal{B}_R(A, B) = \{(Am + B) \cdot 2^n - 1 : m \in \mathbb{Z}^+ \cup \{0\},\ n \in \mathbb{Z}^+ \cup \{0\}\}$$

is composite.

In the above, a negative integer is composite if its absolute value is composite.

The statement (i) is exactly the condition we want for each prime in the progression $Am + B$ to be widely digitally delicate. Similarly, (ii) and (iii), imply that each prime in the progression $Am + B$ is a Sierpiński number and Riesel number, respectively.

Note that we want relatively prime A and B satisfying (i), (ii), and (iii). However, we go about this indirectly by finding relatively prime A_1 and B_1 so that each number

in $\mathcal{A}_d(A_1, B_1)$ is composite, by finding relatively prime A_2 and B_2 so that each number in $\mathcal{B}_S(A_2, B_2)$ is composite, and by finding relatively prime A_3 and B_3 so that each number in $\mathcal{B}_R(A_3, B_3)$ is composite. Thus, for example, every positive integer that is B_1 modulo A_1 is such that if we add $d \cdot 10^n$ to the integer, where $n \in \mathbb{Z}^+ \cup \{0\}$ and $d \in \{-9, -8, \ldots, -1\} \cup \{1, 2, \ldots, 9\}$, the resulting number is composite.

Let

$$\mathcal{P}(A) = \{p : p \text{ is prime and } p|A\}.$$

We will take each of A_1, A_2, and A_3 to be a product of distinct primes. In other words, each A_j is squarefree. The A_j's and B_j's will have the properties

$$\begin{gathered}\mathcal{P}(A_1) \cap \mathcal{P}(A_2) = \emptyset, \quad \mathcal{P}(A_1) \cap \mathcal{P}(A_3) = \emptyset, \quad \mathcal{P}(A_2) \cap \mathcal{P}(A_3) = \{2, 5\}, \\ B_2 \equiv B_3 \pmod{10}.\end{gathered} \tag{2.1}$$

By applying the Chinese Remainder Theorem, we can then establish (i), (ii), and (iii) for some relatively prime A and B by taking $A = A_1A_2A_3/10$ and $B \in [0, A-1]$ so that

$$\begin{gathered}B \equiv B_1 \pmod{A_1}, \quad B \equiv B_2 \pmod{A_2/10}, \quad B \equiv B_3 \pmod{A_3/10}, \\ B \equiv B_2 \equiv B_3 \pmod{10}.\end{gathered} \tag{2.2}$$

The first and third authors [19] constructed A_1 squarefree and B_1 so that (i) holds with $\mathcal{A}_d(A, B)$ replaced by $\mathcal{A}_d(A_1, B_1)$. Thus, this paper will focus on constructing the pair (A_2, B_2) as well as the pair (A_3, B_3) such that (2.1) holds and (ii) and (iii) hold with $\mathcal{B}_S(A, B)$ and $\mathcal{B}_R(A, B)$ replaced by $\mathcal{B}_S(A_2, B_2)$ and $\mathcal{B}_R(A_3, B_3)$, respectively.

Since the construction of the pairs (A_2, B_2) and (A_3, B_3) is similar, we will discuss the construction of the pair (A_2, B_2) and then explain how this translates to constructing the pair (A_3, B_3). To show that $(A_2m + B_2) \cdot 2^n + 1$ is composite for all nonnegative integers n, we will show that for each nonnegative integer n, there is a prime, $p \in \mathcal{P}(A_2)$ such that p divides $(A_2m + B_2) \cdot 2^n + 1$. We will choose A_2 and B_2 large enough so that each number of the form $(A_2m + B_2) \cdot 2^n + 1$, with m and n

in $\mathbb{Z}^+ \cup \{0\}$, is greater than each prime in $\mathcal{P}(A_2)$. Thus, every number of the form $(A_2m + B_2) \cdot 2^n + 1$ will be composite.

For a prime $p \in \mathcal{P}(A_2)$, observe that $(A_2m + B_2) \cdot 2^n + 1$ is divisible by p if and only if $B_2 \cdot 2^n + 1$ is divisible by p. Initially, we do not know the values of A_2 and B_2; we want to construct them. The idea then is to find a finite set $\mathcal{P}_2$ of primes so that for some positive integer B_2 and all nonnegative integers n, the number $B_2 \cdot 2^n + 1$ is divisible by one of the primes in $\mathcal{P}_2$. Then A_2 will be determined by taking A_2 to be the product of the primes in $\mathcal{P}_2$ so that $\mathcal{P}(A_2) = \mathcal{P}_2$. We want to construct B_2 as above in such a way that $\gcd(A_2, B_2) = 1$. The focus now is on finding the set $\mathcal{P}_2$ and how to construct B_2 from this set.

For an odd prime p and an arbitrary integer a, we can determine $B_2 \equiv -2^{-a} \pmod{p}$ so that

$$B_2 \cdot 2^n + 1 \equiv 0 \pmod{p},$$

when $n \equiv a \pmod{b}$ with $b = \mathrm{ord}_p(2)$. The idea now is to determine primes p (our set $\mathcal{P}_2$) so that the orders of 2 modulo these primes and appropriate choices for a as above provide us with a list of congruence classes $n \equiv a \pmod{b}$ that form a covering system for the integers. In this way, for every nonnegative integer n, there will be a prime p such that p divides $B_2 \cdot 2^n + 1$, where p depends on a congruence class satisfied by n.

We now use an example to illustrate how a congruence class in the covering system gives a congruence class for B_2 to satisfy. We take $p = 5$. The order of 2 modulo 5 is 4, so the modulus for the congruence on n will be 4. Suppose we want the congruence $n \equiv 0 \pmod{4}$ in the covering system for n. If we let $B_2 \equiv -2^{-0} \equiv 4 \pmod{5}$, then for some integer t, we have

$$B_2 \cdot 2^n + 1 = B_2 \cdot 2^{4t} + 1 \equiv 4 \cdot 1 + 1 \equiv 0 \pmod{5}.$$

Thus, whenever $n \equiv 0 \pmod{4}$, the number $B_2 \cdot 2^n + 1$ is divisible by 5. Then $n \equiv 0$

(mod 4) is part of the covering system we want to help establish (ii), where we want

$$A_2 \equiv 0 \pmod 5 \quad \text{and} \quad B_2 \equiv 4 \pmod 5.$$

In order for (2.1) to hold, observe that we need $5 \notin \mathcal{P}(A_1)$. The value of A_1 is given in [19], and throughout this paper, we avoid using primes in $\mathcal{P}(A_1)$. It is the case that $5 \notin \mathcal{P}(A_1)$, so using 5 as above is permissible. We note that the primes 2 and 5 were not in $\mathcal{P}(A_1)$ because, in [19], the authors were interested in choosing moduli for the coverings based on the order of 10 modulo the primes dividing A_1. This led them to avoiding the primes 2 and 5 for which no such order exists. Similarly in this paper, we will want 2 to have an order modulo each of the primes dividing A_2 or A_3, and thus we will seemingly want to avoid the prime 2. However, we have already indicated that we want $A_j m + B_j$ to be odd for $j \in \{2, 3\}$, so we are taking 2 to be in both $\mathcal{P}(A_2)$ and $\mathcal{P}(A_3)$ with the added conditions that B_2 and B_3 are 1 modulo 2.

Now, suppose we want to show that $(A_2 m + B_2) \cdot 2^n + 1$ is composite as in (ii) whenever $n \equiv 2 \pmod 4$. Since 5 is the only prime p with 2 of order 4 modulo p, the idea is to work modulo 8 instead and show that $(A_2 m + B_2) \cdot 2^n + 1$ is composite when $n \equiv 2 \pmod 8$ and when $n \equiv 6 \pmod 8$. Each of these will require a number of congruence classes, particularly since we want to avoid primes in $\mathcal{P}(A_1)$ and the only prime p with 2 of order 8 modulo p is $p = 17 \in \mathcal{P}(A_1)$. For the discussion now, we consider the case of showing $(A_2 m + B_2) \cdot 2^n + 1$ is composite when $n \equiv 2 \pmod 8$.

By the above arguments, we want to find primes so that if B_2 satisfies certain congruence classes, then whenever $n \equiv 2 \pmod 8$, one of these primes divides $B_2 \cdot 2^n + 1$. The primes we found are given in the second column in Table 2.1. Momentarily, we will describe how we determined the primes more clearly, but if $n \equiv a \pmod b$ and p are the columns in a row of Table 2.1, then the order of 2 modulo p is b. To see that every integer $n \equiv 2 \pmod 8$ satisfies a congruence class in the first column, observe that if $n \equiv 128 \pmod{144}$, then n satisfies one of the last 3 congruence classes in the

first column of Table 2.1. With the prior two congruence classes modulo 144, every $n \equiv 42 \pmod{48}$ will satisfy one of the last 5 congruence classes in the first column. If $n \equiv 74 \pmod{96}$, then it satisfies one of the congruence classes in rows 4-6 in the first column. Thus, if $n \equiv 26 \pmod{48}$, then it satisfies one of the congruence classes in rows 3-6 in the first column. Now, if $n \equiv 10 \pmod{16}$, then it satisfies one of the congruence classes in rows 2-10 in the first column. Since integers which are 2 modulo 16 satisfy the first congruence class in the first column, we see that every integer $n \equiv 2 \pmod{8}$ satisfies at least one congruence class in the first column of Table 2.1.

Table 2.1 Congruence classes used to satisfy $n \equiv 2 \pmod{8}$

Congruence class	prime
$n \equiv 2 \pmod{16}$	257
$n \equiv 10 \pmod{48}$	673
$n \equiv 26 \pmod{96}$	22253377
$n \equiv 74 \pmod{288}$	1153
$n \equiv 170 \pmod{288}$	6337
$n \equiv 266 \pmod{288}$	38941695937
$n \equiv 42 \pmod{144}$	577
$n \equiv 90 \pmod{144}$	487824887233
$n \equiv 138 \pmod{432}$	4261383649
$n \equiv 282 \pmod{432}$	209924353
$n \equiv 426 \pmod{432}$	249290608182653604517081 93

So we will choose A_2 so that it is divisible by each prime in the second column of Table 2.1. Corresponding to each congruence $n \equiv a \pmod{b}$ and prime p in a row, we take $B_2 \equiv -2^{-a} \pmod{p}$ as noted earlier. Then whenever $n \equiv 2 \pmod{8}$ and $m \in \mathbb{Z}$, we have $(A_2 m + B_2) \cdot 2^n + 1$ is divisible by a prime in the second column of Table 2.1.

Next, we describe more clearly where our choice of primes came from. The idea in the example above is to find a system $\mathcal{C}$ of congruence classes such that every $n \equiv 2 \pmod{8}$ satisfies a congruence $n \equiv a \pmod{b}$ in $\mathcal{C}$. Each such congruence class will correspond to a prime $p \notin \mathcal{P}(A_1)$ for which 2 has order b modulo p. To find the

primes p for which 2 has order b modulo p, where b is a modulus we want to use for $\mathcal{C}$, we look at the prime divisors of $\Phi_b(2)$, where $\Phi_b(x)$ is the b^{th} cyclotomic polynomial. As noted in [19] and [23] (with 2 replaced by 10), each prime divisor p of $\Phi_b(2)$ either will be the largest prime divisor of b or will satisfy that 2 has order b modulo p. Thus, looking at prime divisors of $\Phi_b(2)$, which are not in $\mathcal{P}(A_1)$, determines whether we can use the modulus b for $\mathcal{C}$ and how many times we can use b as a modulus. Thus, in general, we found what moduli were possible for our systems of congruence classes by looking at the number of distinct prime divisors of $\Phi_b(2)$, not in $\mathcal{P}(A_1)$, for different choices of b, and then we determined our covering systems based on this information.

Observe in Table 2.1 that we could have interchanged the primes with 2 of a given order b. For example, for the congruences $n \equiv 74 \pmod{288}$, $n \equiv 170 \pmod{288}$, and $n \equiv 266 \pmod{288}$, we could have selected the primes in the right-most column as 38941695937, 1153, and 6337, respectively.

Tables A.1 and A.2 describe the results of looking at prime factors of $\Phi_b(2)$ to determine the moduli b we can use for our covering systems and the number of times we can use each modulus (that is, the number of distinct prime factors of $\Phi_b(2)$ that do not divide b and are not in $\mathcal{P}(A_1)$). Table A.1 indicates the number of distinct prime factors of $\Phi_b(2)$ that do not divide b and are not in $\mathcal{P}(A_1)$ but are in $\mathcal{P}(A_2) \cup \mathcal{P}(A_3)$. Table A.2 shows the remaining number of distinct prime factors of $\Phi_b(2)$ which we know exist and do not divide b and are not in $\mathcal{P}(A_1)$ for each modulus. If a modulus b appears in Table A.1 but not in Table A.2, then all the distinct prime factors of $\Phi_b(2)$ that do not divide b and are not in $\mathcal{P}(A_1)$ have been used in $\mathcal{P}(A_2) \cup \mathcal{P}(A_3)$.

The above describes how we obtained a covering system for determining A_2 and B_2 so that (ii) holds. We obtain a covering system for determining A_3 and B_3 similarly so that (iii) holds. In this case, each congruence $n \equiv a \pmod{b}$ corresponds to an odd prime p dividing A_3, with b equal to the order of 2 modulo p, and we want

$$B_3 \equiv 2^{-a} \pmod{p} \tag{2.3}$$

so that

$$B_3 \cdot 2^n - 1 \equiv 0 \pmod{p}$$

for $n \equiv a \pmod{b}$.

For $p = 5$ above, we took $B_2 \equiv 4 \pmod{5}$. Also, B_2 is odd, so we have $B_2 \equiv 9 \pmod{10}$. For (2.1) to hold, we therefore want $B_3 \equiv 9 \pmod{10}$. In particular, $B_3 \equiv 4 \pmod{5}$. From (2.3), with $p = 5$, we want $a = 2$. As the order of 2 modulo 5 is 4, the congruence we want associated with $p = 5$ and (iii) is $n \equiv 2 \pmod{4}$.

Each prime counted in Table A.1 in the last column, besides $p = 5$ with $b = 4$, can be used to provide a congruence class for the covering system corresponding to either (ii) or (iii) and not both, due to the restriction made in (2.1) that $\mathcal{P}(A_2) \cap \mathcal{P}(A_3) = \{2, 5\}$. The complete covering systems used for determining A_j and B_j, for $j \in \{2, 3\}$, can be found in the appendix. In the next section, we explain how we verified that the congruence classes we tabulated for the covering systems in fact form covering systems.

2.3 Verifying the Covering Systems

Consider the collection of congruence classes

$$\mathcal{C}_0 = \{0 \pmod 3,\ 1 \pmod 3,\ 2 \pmod 9,\ 5 \pmod 9,\ 8 \pmod 9\}.$$

We can verify $\mathcal{C}_0$ is a covering system as follows. Every nonnegative integer is either 0, 1 or 2 (mod 3). The congruence classes 0 (mod 3) and 1 (mod 3) are in $\mathcal{C}_0$, so we are left with covering integers which are 2 (mod 3) using other congruences in $\mathcal{C}_0$. Every integer that is 2 (mod 3) is either 2 (mod 9), 5 (mod 9), or 8 (mod 9). These congruence classes modulo 9 are in $\mathcal{C}_0$. Thus, $\mathcal{C}_0$ is a covering system.

Due to the complexity of the coverings in the previous section, this method for verifying in general a

$$\mathcal{C} = \{a_1 \pmod{b_1}, \quad a_2 \pmod{b_2}, \quad \ldots, \quad a_m \pmod{b_m}\}$$

is a covering is quite time consuming. An alternate way of verifying $\mathcal{C}$ is a covering is to check every integer in $[0, \ell - 1]$, where $\ell = \text{lcm}(b_i)$. To see this, suppose that every integer in $[0, \ell - 1]$ is in at least one congruence class in $\mathcal{C}$. We want to show that all integers k are in at least one congruence class in $\mathcal{C}$. We can rewrite k as

$$k = q \cdot \ell + r$$

where q and r are integers with $0 \leq r \leq \ell - 1$. Since $r \in [0, \ell - 1]$, we have that r is in at least one congruence class, $a \pmod{b}$, in $\mathcal{C}$. As a consequence of b dividing ℓ, we deduce

$$k \equiv r \equiv a \pmod{b}.$$

Thus, k is in the congruence class $a \pmod{b}$ in $\mathcal{C}$, as we wanted.

In the example above with $\mathcal{C}_0$, this process is emulated by checking that every $k \in [0, 8]$ satisfies a congruence class in $\mathcal{C}_0$. Table 2.2 confirms that $\mathcal{C}_0$ is a covering by listing a congruence class each such k satisfies in $\mathcal{C}_0$ in the second column.

Table 2.2 Verifying the Covering $\mathcal{C}_0$

k	Congruence Classes in $\mathcal{C}_0$
0	$0 \pmod 3$
1	$1 \pmod 3$
2	$2 \pmod 9$
3	$0 \pmod 3$
4	$1 \pmod 3$
5	$5 \pmod 9$
6	$0 \pmod 3$
7	$1 \pmod 3$
8	$8 \pmod 9$

While this method works and is easily implemented by a computer, if $\ell = \text{lcm}(b_i)$ is too large, this process takes a substantial amount of time. In the coverings used in this paper for Sierpiński and Riesel numbers, the least common multiples

are 236107872000 and 922078080000, respectively. Also, the number of congruence classes in the coverings are 447 and 459, respectively. Thus, an alternative verification method, as seen in the paper [19], was used.

Let $\mathcal{C}$ be a set of congruence classes $a_i \pmod{b_i}$. Fix a positive integer w to be chosen later, and let u be an integer in $[0, w-1]$. Let $\mathcal{C}_u$ be the congruence classes $a_i \pmod{b_i}$ in $\mathcal{C}$ such that

$$a_i \equiv u \pmod{\gcd(b_i, w)}.$$

If $|\mathcal{C}_u| = 0$, then $\mathcal{C}$ is not a covering. Now consider the case that $|\mathcal{C}_u| > 0$. Let ℓ' be the lcm of the moduli in $\mathcal{C}_u$, and set $d = \gcd(w, \ell')$. In [19], the authors show the following.

Lemma 23. *With the above notation, if for each $u \in [0, w-1]$, every*

$$k = wt + u, \quad \text{with } t \in [0, (\ell'/d) - 1] \cap \mathbb{Z},$$

satisfies a congruence class in $\mathcal{C}_u$, then $\mathcal{C}$ is a covering system.

Let $\mathcal{C}$ be one of the systems of congruence classes created in the previous section, that is for constructing arithmetic progressions for either Sierpiński or Riesel numbers. We take $w = 4 \cdot 3 \cdot 5 \cdot q$ where q is the largest prime dividing the least common multiple of the moduli in $\mathcal{C}$ as done in [19]. Applying Lemma 23 with this choice of w allowed us to easily verify our congruence classes form a covering system.

2.4 Proof of Corollary 13

The proof of Corollary 13 is a consequence of thoughts during and after the construction of the main result of Chapter 2 that motivated the author to explore the topic. More precisely, Corollary 13 is a consequence of the covering system in Table A.3. However, there is some additional work to be done to apply the covering system in Table A.3.

Proof. We start by only considering a positive integer $a \geq 3$. Let $\mathcal{P}$ be the collection of primes < 937 and define

$$\mathcal{S} = \{-1 \pmod{p} : p \in \mathcal{P}\}.$$

Let

$$A_{\mathcal{S}} = \prod_{p \in \mathcal{P}} p \quad \text{and} \quad B_{\mathcal{S}} = \left(\prod_{p \in \mathcal{P}} p \right) - 1.$$

Then, for all $p \in \mathcal{P}$ and k in the arithmetic progression $A_{\mathcal{S}}m + B_{\mathcal{S}}$, we have

$$k \equiv -1 \pmod{p}.$$

In particular, if p is taken to be a prime divisor of $a - 1$ with $a \in [2, 937]$, we see that

$$k \cdot a^n + 1 \equiv 0 \pmod{p}.$$

Thus, by applying Theorem 7 to the arithmetic progression, we have Corollary 13 for all $a \in [3, 937]$. In fact, this argument is easily adjusted so that we can instead consider $a \in [3, A]$ for A arbitrarily large. What we need to address for the full strength of Corollary 13 is how to handle $a = 2$ as well.

For the rest of the proof we look to find A' and B' such that $(A'm + B') \cdot 2^n + 1$ is a Sierpiński number for any nonnegative integer m and $\gcd(A', B') = \gcd(A', A_{\mathcal{S}}) = 1$. Once such A' and B' have been constructed, we can use the Chinese Remainder Theorem to construct an arithmetic progression $(A_{\mathcal{S}}A')m + B''$ such that

- $A_{\mathcal{S}}A'$ and B'' are relatively prime and
- for all $a \in [2, 937]$, we have $(A_{\mathcal{S}}A'm + B'') \cdot a^n + 1$ is composite for all positive integers n and nonnegative integers m.

With such a progression, Theorem 7 finishes the proof.

Consider A_2 and B_2 as constructed in Section 2.2 of this chapter for Theorem 11 using Table A.3. The numbers A_2 and B_2 were constructed so that A_2 and B_2 are

relatively prime and $A_2m + B_2$ is a Sierpiński number for all nonnegative integers m. However, A_2 and $A_{\mathcal{S}}$ are not relatively prime. Thus, the rest of the proof is focused on adjusting the arithmetic progression to match the properties of A' and B' above.

Suppose $n \equiv 0 \pmod 2$. Then

$$k \cdot 2^n + 1 \equiv k + 1 \pmod 3.$$

Since $A_{\mathcal{S}}m + B_{\mathcal{S}} \equiv -1 \pmod 3$ for all nonnegative integers m, if we take k in the arithmetic progression $A_{\mathcal{S}}m + B_{\mathcal{S}}$, we see that $k \cdot 2^n + 1$ is divisible by 3. Thus, whatever primes were used in the construction of A_2 and B_2 for $n \equiv 0 \pmod 2$ are unnecessary for the construction of A' and B'. Denote this set of primes as $\mathcal{P}^{(2)}$. We clarify that the primes in $\mathcal{P}^{(2)}$ were not used to cover $n \equiv 1 \pmod 2$ for Theorem 11. Let

$$A' = \frac{A_2}{\prod_{p \in \mathcal{P}^{(2)}} p},$$

and choose $B' \in [0, A' - 1]$ so that $B' \equiv B_2 \pmod{A'}$. Notice A' and B' are relatively prime since A_2 and B_2 are. One can check Table A.3 and [21] to see that A' and $A_{\mathcal{S}}$ are relatively prime since the largest prime dividing A' is 937. Therefore, the arithmetic progression $A_{\mathcal{S}}A'm + B''$ is as desired, and Theorem 7 finishes the proof. □

Chapter 3

A lower bound for the irreducibility of the sum of two relatively prime polynomials

This chapter will focus on two results that related to the results mentioned in section 1.2 of the introduction. The aim is to prove Theorem 24 and Theorem 28. The proofs of Theorem 24 and Theorem 28 will mirror each other, but require different machinery. We will start by providing necessary notation and some preliminaries. Then we give a proof of the univariate case which is Theorem 24. Then we will extend the result to the bivariate case which is Theorem 28.

3.1 Proof of Univariate Case

Let $w(x) = c_n x^n + \cdots + c_1 x + c_0$ be a nonzero polynomial in $\mathbb{Z}[x]$. Define

$$h_w = \max\{|c_i| : 0 \leq i \leq n\},$$
$$\ell_w = c_n, \text{ and}$$
$$d_w = \deg w(x) = n.$$

Also, for two polynomials $w_1(x)$ and $w_2(x)$ in $\mathbb{Z}[x]$, denote the resultant of $w_1(x)$ and $w_2(x)$ as $\mathrm{Res}(w_1, w_2)$. Now we formally state the main result of this section.

Theorem 24. *Let $f(x)$ and $g(x)$ be nonzero relatively prime polynomials in $\mathbb{Z}[x]$ with $d_f < d_g$ and $0 < \delta < 1/d_g$. Let M be a positive integer satisfying*

$$M > \max\left\{\frac{|\ell_f|}{|\ell_g|}\Big(h_f/|\ell_f| + h_g/|\ell_g| + 3\Big)^{d_f}, \Big(2h_f|\ell_g|^{d_g}(h_g/|\ell_g| + 2)^{d_f}\Big)^{1/(1-\delta d_g)}\right\}. \quad (3.1)$$

Set $F(x) = f(x) + Mg(x)$. Suppose further that there is a prime p, not dividing $\ell_f \ell_g$, and a positive integer k, with $\gcd(k, d_g - d_f) = 1$, such that

$$p^k \mid M, \quad p^{k+1} \nmid M \quad \textit{and} \quad p^k > M^{1-\delta}.$$

Then $F(x)$ is irreducible over $\mathbb{Q}$.

Before proceeding, we observe that a positive proportion of positive integers M will have a prime factor $p > M^{1-1/(2d_g)}$. Thus, by taking $\delta = 1/(2d_g)$ and $k = 1$ in Theorem 24, we obtain a positive proportion, depending on $f(x)$ and $g(x)$, of explicit positive integers M such that $F(x) = f(x) + Mg(x)$ is irreducible. Prior work in [7], [9], [13] and [14] only produced thin sets of such M (not a positive proportion).

The proof of Theorem 24 relies heavily on Lemma 27. The proof of Lemma 27 makes use of another lemma that is fairly easy to prove and follows from work of Cauchy (cf. Theorem 8.1.3 and (8.1.9) in [42]).

Lemma 25. *If $w(x) \in \mathbb{C}[x]$ and monic, then the complex roots of $w(x)$ have absolute value $\leq h_w + 1$.*

Proof. Let $w(x)$ be as in lemma such that

$$w(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

where $a_i \in \mathbb{C}$ for all i. Let α be a root of $w(x)$ and assume for a contradiction $|\alpha| > h_w + 1$. We deduce that

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$

By our assumption and the above equality we also can deduce

$$\begin{aligned}
|\alpha|^n = |\alpha| \cdot |\alpha|^{n-1} &> (1 + h_w)|\alpha|^{n-1} = |\alpha|^{n-1} + h_w|\alpha|^{n-1} \geq |\alpha|^{n-1} + |a_{n-1}| \cdot |\alpha|^{n-1} \\
&> (1 + h_w)|\alpha|^{n-2} + |a_{n-1}| \cdot |\alpha|^{n-1} \geq |\alpha|^{n-2} + |a_{n-2}| \cdot |\alpha|^{n-2} + |a_{n-1}| \cdot |\alpha|^{n-1} \\
&\vdots \\
&> |a_{n-1}||\alpha|^{n-1} + \cdots + |a_1||\alpha| + |a_0| \geq |\alpha|^n.
\end{aligned}$$

This is a clear contradiction and completes the proof. □

Lemma 26 is a consequence of Lemma 25 for nonmonic $w(x)$ and the proof follows very similarly. We will leave the proof of Lemma 26 to the reader.

Lemma 26. *If $w(x) \in \mathbb{C}[x]$, then the complex roots of $w(x)$ have absolute value $\leq (h_w/|\ell_w|) + 1$.*

With Lemma 26, we can state Lemma 27 and give its proof.

Lemma 27. *Let $f(x)$ and $g(x)$ be nonzero relatively prime polynomials in $\mathbb{Z}[x]$ with $d_f < d_g$. Let M be a positive integer satisfying*

$$M > \frac{|\ell_f|}{|\ell_g|}\Big(h_f/|\ell_f| + h_g/|\ell_g| + 3\Big)^{d_f}. \tag{3.2}$$

Set $F(x) = f(x) + Mg(x)$, and suppose $F(x)$ has a factor $u(x) \in \mathbb{Z}[x]$ of degree ≥ 1. Then

$$|\ell_u| \geq \left(\frac{M}{2h_f\Big(h_g/|\ell_g| + 2\Big)^{d_f}}\right)^{1/d_g}.$$

Proof. Let $F(x)$ and $u(x)$ be as above and assume that $u(x)$ has a root θ that satisfies

$$|\theta| \geq h_g/|\ell_g| + 2. \tag{3.3}$$

Since $F(\theta) = 0$, we deduce $f(\theta) = -Mg(\theta)$. We write $f(x)$ and $g(x)$ as

$$f(x) = \ell_f(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{d_f}) \quad \text{and} \quad g(x) = \ell_g(x-\beta_1)(x-\beta_2)\cdots(x-\beta_{d_g})$$

where α_j, $\beta_j \in \mathbb{C}$. Lemma 26 applied to each α_j and β_j implies

$$|\theta - \alpha_j| \leq |\theta| + |\alpha_j| \leq |\theta| + h_f/|\ell_f| + 1, \qquad \text{for } 1 \leq j \leq d_f,$$

and

$$|\theta - \beta_j| \geq |\theta| - |\beta_j| \geq |\theta| - h_g/|\ell_g| - 1, \qquad \text{for } 1 \leq j \leq d_g.$$

We deduce that

$$|f(\theta)| \leq |\ell_f|\Big(|\theta| + h_f/|\ell_f| + 1\Big)^{d_f}$$

and

$$|g(\theta)| \geq |\ell_g|\Big(|\theta| - h_g/|\ell_g| - 1\Big)^{d_g}.$$

Since $f(\theta) = -Mg(\theta)$, we will obtain a contradiction if we show

$$|\ell_f|\Big(|\theta| + h_f/|\ell_f| + 1\Big)^{d_f} < M|\ell_g|\Big(|\theta| - h_g/|\ell_g| - 1\Big)^{d_g}$$

or, equivalently,

$$M > \frac{|\ell_f|\Big(|\theta| + h_f/|\ell_f| + 1\Big)^{d_f}}{|\ell_g|\Big(|\theta| - h_g/|\ell_g| - 1\Big)^{d_g}}. \tag{3.4}$$

We now focus on reformulating the right-hand side of the last inequality before obtaining a contradiction. Specifically, we observe that

$$\begin{aligned}
\frac{|\ell_f|\Big(|\theta| + h_f/|\ell_f| + 1\Big)^{d_f}}{|\ell_g|\Big(|\theta| - h_g/|\ell_g| - 1\Big)^{d_g}} &= \frac{|\ell_f|\left[\dfrac{|\theta| + h_f|\ell_f| + 1}{|\theta| - h_g/|\ell_g| - 1}\right]^{d_f}}{|\ell_g|\,(|\theta| - h_g/|\ell_g| - 1)^{d_g - d_f}} \\
&= \frac{|\ell_f|\left[\dfrac{|\theta| + h_f|\ell_f| + 1 + |\theta| - h_g/|\ell_g| - 1 - |\theta| + h_g/|\ell_g| + 1}{|\theta| - h_g/|\ell_g| - 1}\right]^{d_f}}{|\ell_g|\,(|\theta| - h_g/|\ell_g| - 1)^{d_g - d_f}} \\
&= \frac{|\ell_f|\left(1 + \dfrac{h_f/|\ell_f| + h_g/|\ell_g| + 2}{|\theta| - h_g/|\ell_g| - 1}\right)^{d_f}}{|\ell_g|\Big(|\theta| - h_g/|\ell_g| - 1\Big)^{d_g - d_f}} \leq \frac{|\ell_f|}{|\ell_g|}\Big(h_f/|\ell_f| + h_g/|\ell_g| + 3\Big)^{d_f},
\end{aligned}$$

where we have used the assumption (3.3) to obtain the inequality. From (3.2), we obtain (3.4) and the desired contradiction. Therefore, (3.3) does not hold and, when $u(\theta) = 0$, we deduce that

$$|\theta| < h_g/|\ell_g| + 2. \tag{3.5}$$

Note that if $u(\theta) = 0$ and $g(\theta) = 0$, then

$$f(\theta) = -Mg(\theta) = 0,$$

contradicting $g(x)$ and $f(x)$ are relatively prime. Thus, $u(x)$ and $g(x)$ have no common roots. Let $\theta_1, \ldots, \theta_{d_u}$ be all the roots of $u(x)$ including repeated roots. Since

$u(x)$ and $g(x)$ have no common roots, we deduce

$$\left|\ell_u^{d_g}\prod_{j=1}^{d_u} g(\theta_j)\right| = \left|\mathrm{Res}(u,g)\right| \geq 1. \tag{3.6}$$

Since each θ_j is a root of $F(x)$, we deduce that

$$\left|\ell_u^{d_g}\prod_{j=1}^{d_u} f(\theta_j)\right| = M^{d_u}\left|\ell_u^{d_g}\prod_{j=1}^{d_u} g(\theta_j)\right|. \tag{3.7}$$

We focus on bounding the left-hand side of (3.7). Using (3.5), we obtain

$$\begin{aligned}
\left|\ell_u^{d_g}\prod_{j=1}^{d_u} f(\theta_j)\right| &\leq |\ell_u|^{d_g}\prod_{j=1}^{d_u}\left|h_f\cdot\sum_{j=0}^{d_f}\Big(h_g/|\ell_g|+2\Big)^j\right| \\
&\leq |\ell_u|^{d_g}\prod_{j=1}^{d_u}\left|h_f\cdot\Big(h_g/|\ell_g|+2\Big)^{d_f}\sum_{i=0}^{d_f}\frac{1}{\Big(h_g/|\ell_g|+2\Big)^{d_f-i}}\right| \\
&\leq |\ell_u|^{d_g}\prod_{j=1}^{d_u}\left|h_f\cdot\Big(h_g/|\ell_g|+2\Big)^{d_f}\sum_{i=0}^{d_f}\frac{1}{2^{d_f-i}}\right| \\
&\leq |\ell_u|^{d_g}\prod_{j=1}^{d_u}\left|2h_f\cdot\Big(h_g/|\ell_g|+2\Big)^{d_f}\right| \\
&= |\ell_u|^{d_g}2^{d_u}h_f^{d_u}\Big(h_g/|\ell_g|+2\Big)^{d_f d_u}.
\end{aligned} \tag{3.8}$$

Applying (3.6) and (3.8) to (3.7), we deduce

$$M^{d_u} \leq |\ell_u|^{d_g}2^{d_u}h_f^{d_u}\Big(h_g/|\ell_g|+2\Big)^{d_f d_u}.$$

Thus,

$$M \leq 2h_f|\ell_u|^{d_g/d_u}\Big(h_g/|\ell_g|+2\Big)^{d_f} \leq 2h_f|\ell_u|^{d_g}\Big(h_g/|\ell_g|+2\Big)^{d_f}$$

and

$$|\ell_u| \geq \left(\frac{M}{2h_f\Big(h_g/|\ell_g|+2\Big)^{d_f}}\right)^{1/d_g}.$$

This completes the proof of Lemma 27. □

Using Lemma 27, we can begin the proof of Theorem 24.

Proof of Theorem 24. Assume the conditions in Theorem 24 and that

$$F(x) = u(x)v(x)$$

where $u(x)$, $v(x) \in \mathbb{Z}[x]$ of degree at least 1. In the conditions, we have a prime p such that $p \nmid \ell_f \ell_g$ and

$$p^k \mid M, \quad p^{k+1} \nmid M \quad \text{and} \quad p^k > M^{1-\delta}.$$

Since $d_g > d_f$, we deduce $d_F = d_g$ and all terms of $F(x)$ having degree larger than d_f will be terms in $Mg(x)$. Thus, p^k divides all these terms of $F(x)$. Since $p \nmid \ell_g$, we see that p^{k+1} does not divide the leading coefficient of $F(x)$. Since, $p \nmid \ell_f$, the term of $F(x)$ of degree d_f will have a coefficient that is not divisible by p. From the conditions in the theorem, we have $\gcd(k, d_g - d_f) = 1$. Thus, there are no lattice points on the leftmost edge of the Newton polygon with respect to p from $(0, k)$ to $(d_g - d_f, 0)$. Therefore, one factor, which we will take to be $v(x)$, has a translation of this edge in its Newton polygon with respect to p. Then, $p \nmid \ell_u$ and

$$|\ell_u| \leq \frac{M|\ell_g|}{p^k} < M^{\delta}|\ell_g|.$$

Lemma 27 implies

$$M^{\delta}|\ell_g| > \left(\frac{M}{2h_f \left(h_g/|\ell_g| + 2\right)^{d_f}}\right)^{1/d_g}.$$

Therefore,

$$M^{\frac{1-\delta d_g}{d_g}} = M^{(1/d_g)-\delta} < |\ell_g| \left(2h_f \left(h_g/|\ell_g| + 2\right)^{d_f}\right)^{1/d_g}$$

so that

$$M < \left(2h_f |\ell_g|^{d_g} (h_g/|\ell_g| + 2)^{d_f}\right)^{1/(1-\delta d_g)}.$$

By the lower bound on M in the statement of Theorem 24, this is a contradiction. Thus, $F(x)$ is irreducible over $\mathbb{Q}$. □

3.2 Bivariate Case

Now we extend Theorem 24 to polynomials of two variables following the set-up given by Bonciocat et. al. in [8]. For the rest of the paper, we let K be a field. We define the nonarchimedean absolute value $|\cdot|$ on $K[x]$ (justified momentarily), as in [8], which

is as follows. Fix $\rho > 1$. Define $|0| = 0$ and, for any nonzero polynomial $h(x) \in K[x]$, define

$$|h(x)| = \rho^{\deg h(x)}.$$

Let $f(x, y)$ and $g(x, y)$ be polynomials in $(K[x])[y]$. In other words, we will consider $f(x, y)$ and $g(x, y)$ as polynomials in the variable y with coefficients in $K[x]$ so that we can write

$$f(x, y) = a_n(x)y^n + a_{n-1}(x)y^{n-1} + \ldots + a_1(x)y + a_0(x)$$

and

$$g(x, y) = b_m(x)y^m + b_{m-1}(x)y^{m-1} + \ldots + b_1(x)y + b_0(x)$$

where $a_i(x)$ and $b_j(x)$ are in $K[x]$ for all i and j and the polynomials $a_n(x)$ and $b_m(x)$ are nonzero. We define

$$\begin{aligned} h_f &= \max\{|a_i(x)| : 0 \leq i \leq n\}, \\ \ell_f &= a_n(x), \\ d_f &= \deg_y f(x, y) = n, \text{ and} \\ L_f &= \left(\frac{h_f}{|\ell_f|}\right)^{1/d_f}. \end{aligned}$$

We also use the analogous notation for any nonzero polynomial in $(K[x])[y]$, so in particular h_g, ℓ_g, d_g, and L_g are defined similarly. Notice that we can extend $|\cdot|$ by defining

$$\left|\frac{h(x)}{w(x)}\right| = \frac{|h(x)|}{|w(x)|},$$

for $h(x), w(x) \in K[x]$ and $w(x) \neq 0$. To see that this definition is well-defined, observe that if $h(x), w(x), u(x) \in K[x]$ with $h(x), w(x), u(x)$ nonzero, then

$$\left|\frac{h(x)u(x)}{w(x)u(x)}\right| = \frac{|h(x)u(x)|}{|w(x)u(x)|} = \frac{\rho^{\deg h + \deg u}}{\rho^{\deg w + \deg u}} = \frac{\rho^{\deg h}}{\rho^{\deg w}} = \frac{|h(x)|}{|w(x)|} = \left|\frac{h(x)}{w(x)}\right|.$$

The case that $h(x) = 0$ is easily handled separately. Thus, the absolute value is well-defined for elements in $K(x)$.

We also establish $(K(x), |\cdot|)$ is a metric space. We first show $|\cdot|$ is an absolute value on $K[x]$ and $K(x)$. Then we show the absolute value defines a metric on $K(x)$. For $|\cdot|$ to be an absolute value for $K[x]$, we want the following to hold:

1. For all $f \in K[x]$, $|f| \geq 0$ with equality if and only if $f = 0$.

2. For all $f, g \in K[x]$, $|f \cdot g| = |f| \cdot |g|$.

3. For all $f, g \in K[x]$, $|f + g| \leq |f| + |g|$.

Property 1 is true by the choice of $\rho > 1$ and the definition for $f = 0$. For Property 2, take $f, g \in K[x]$. If f or g is 0, then $f \cdot g = 0$ and Property 2 holds. Otherwise,

$$|f \cdot g| = \rho^{\deg f + \deg g} = \rho^{\deg f} \cdot \rho^{\deg g} = |f| \cdot |g|.$$

Property 3 is clear if f or g is 0. Otherwise, for Property 3, we use that

$$|f + g| \leq \rho^{\max\{\deg f, \deg g\}} = \max\{|f|, |g|\} \leq |f| + |g|.$$

Therefore, $|\cdot|$ is an absolute value over $K[x]$. We can extend $|\cdot|$ to $K(x)$ by taking $f = h_1/w_1$ and $g = h_2/w_2$ elements of $K(x)$. In particular, we can see Property 3 holds in $K(x)$ using $|\cdot|$ is well-defined, as shown above, and the above properties in $K[x]$ to deduce

$$\begin{aligned} |f + g| &= \left|\frac{h_1}{w_1} + \frac{h_2}{w_2}\right| = \left|\frac{h_1 w_2 + h_2 w_1}{w_1 w_2}\right| = \frac{|h_1 w_2 + h_2 w_1|}{|w_1 w_2|} \leq \frac{|h_1 w_2| + |h_2 w_1|}{|w_1 w_2|} \\ &= \frac{|h_1 w_2|}{|w_1 w_2|} + \frac{|h_2 w_1|}{|w_1 w_2|} = \left|\frac{h_1 w_2}{w_1 w_2}\right| + \left|\frac{h_2 w_1}{w_1 w_2}\right| = \left|\frac{h_1}{w_1}\right| + \left|\frac{h_2}{w_2}\right| = |f| + |g|. \end{aligned}$$

Next we show $|\cdot|$ is a metric for $K(x)$. In other words, we show the following:

A. If $f, g \in K(x)$, then $|f - g| \geq 0$.

B. If $f, g \in K(x)$, then $|f - g| = 0$ if and only if $f = g$.

C. If $f, g \in K(x)$, then $|f - g| = |g - f|$.

D. If $f, g, h \in K(x)$, then $|f - g| \leq |f - h| + |h - g|$.

Property A is true by Property 1. Property B is true since $f - g = 0$ by Property 1 as well. Since Property 2 holds, we have

$$|f - g| = |-(g - f)| = |-1| \cdot |g - f| = |g - f|,$$

establishing Property C. Property D follows from Property 3 by

$$|f - g| = |(f - h) + (h - g)| \leq |f - h| + |h - g| = |f - h| + |g - h|.$$

Therefore, $|\cdot|$ is a metric in $K(x)$ and $(K(x), |\cdot|)$ is a metric space.

There is a unique field extension that is complete with respect to the absolute value such that the nonarchimedean absolute value can also be extended as a nonarchimedean absolute value in the completion (cf. [48, Theorem 24, Lemma 25]). One can also give an explicit formula for the extension of the nonarchimedean absolute value in $\overline{K(x)}$, the algebraic closure of $K(x)$ (cf. [50, Theorem 4.2]). More precisely, let $\theta(x)$ be an element of $\overline{K(x)}$ so that there is an irreducible monic

$$w(x, y) = y^n + a_{n-1}(x)y^{n-1} + \ldots + a_0(x) \in (K(x))[y]$$

such that $w(x, \theta(x)) = 0$. Define the extension of $|\cdot|$ to $\overline{K(x)}$ by

$$|\theta(x)| = \left|(-1)^n a_0(x)\right|^{1/n}.$$

Alternatively, if $\theta(x)$ is a root of an irreducible polynomial

$$w(x, y) = a_n(x)y^n + a_{n-1}(x)y^{n-1} + \ldots + a_0(x) \in (K[x])[y],$$

then we can define

$$|\theta(x)| = \left|(-1)^n \frac{a_0(x)}{a_n(x)}\right|^{1/n}.$$

Note that for either form of $w(x, y)$ and $\theta(x)$ as above, we have

$$|\theta(x)| \leq L_w = \left(\frac{h_w}{|\ell_w|}\right)^{1/d_w}.$$

For $w(x,y) \in K[x]$ (that is $w(x,y)$ constant in $(K[x])[y]$), we define $\mathcal{L}_w = 0$. Otherwise, set

$$w(x,y) = \ell_w w_1(x,y) \cdots w_s(x,y)$$

where each w_i is monic and irreducible in $(K(x))[y]$, and define

$$\mathcal{L}_w = \max\{L_{w_1}, \ldots, L_{w_s}\}.$$

For $\theta(x)$ a root of $w(x,y) \in (K[x])[y]$, we therefore have

$$|\theta(x)| \leq \mathcal{L}_w. \tag{3.9}$$

Observe that $\mathcal{L}_w \geq 1$, which will be valuable later. Using (3.9), we will prove a useful lemma just as we did in the one variable case. First, we give the desired result of this section.

Theorem 28. *Let $f(x,y)$ and $g(x,y)$ be nonzero polynomials in $K[x,y]$ relatively prime over $K(x)$ with $d_f < d_g$ and $0 < \delta < 1/d_g$. Let $M(x)$ be a polynomial in $K[x]$ satisfying*

$$|M(x)| > \max\left\{ \frac{|\ell_f|}{|\ell_g|}(\mathcal{L}_f + \mathcal{L}_g + 1)^{d_f}, \left(h_f |\ell_g|^{d_g} (\mathcal{L}_g + 1)^{d_f}\right)^{\frac{1}{1-\delta d_g}} \right\}. \tag{3.10}$$

Set $F(x,y) = f(x,y) + M(x)g(x,y)$. Then $F(x,y)$ is irreducible over $K(x)$ if there is an irreducible polynomial $p(x)$ in $K[x]$, not dividing $\ell_f \ell_g$, and a positive integer k, with $\gcd(k, d_g - d_f) = 1$, such that

$$p(x)^k \mid M(x), \quad p(x)^{k+1} \nmid M(x) \quad \text{and} \quad |p(x)|^k > |M(x)|^{1-\delta}.$$

For $f(x,y) \in K[x]$ so that $d_f = 0$, the bound (3.10) is not needed, as a Newton polygon argument given in the proof of Theorem 28 will show that the conditions on $p(x)$ and $\gcd(k, d_g - d_f) = 1$ are enough to see that $F(x,y)$ is irreducible over $K(x)$. We leave the reader to check this detail, and suppose for the remainder of this section that $d_f \geq 1$.

Lemma 29 below will be the main ingredient in proving Theorem 28.

Lemma 29. *Let $f(x,y)$ and $g(x,y)$ be nonconstant polynomials in $K[x,y]$ relatively prime over $K(x)$ with $d_f < d_g$. Let $M(x) \in K[x]$ satisfy*

$$|M(x)| > \frac{|\ell_f|}{|\ell_g|}(\mathcal{L}_f + \mathcal{L}_g + 1)^{d_f}. \tag{3.11}$$

Set $F(x,y) = f(x,y)+M(x)g(x,y)$, and suppose $F(x,y)$ has a factor $u(x,y) \in K[x,y]$ with $d_u \geq 1$. Then

$$|\ell_u| \geq \left(\frac{|M(x)|}{h_f(\mathcal{L}_g+1)^{d_f}}\right)^{1/d_g}.$$

Proof. Let $u(x,y)$ be as above and $\theta(x) \in \overline{K[x]}$ be such that $u(x,\theta(x)) = 0$. Assume first that

$$|\theta(x)| \geq \mathcal{L}_g + 1. \tag{3.12}$$

Since $F(x,\theta(x)) = 0$, we deduce $f(x,\theta(x)) = -M(x)g(x,\theta(x))$. We rewrite $f(x,y)$ and $g(x,y)$ as

$$f(x,y) = \ell_f(y-\alpha_1(x))(y-\alpha_2(x))\cdots(y-\alpha_{d_f}(x))$$

and

$$g(x,y) = \ell_g(y-\beta_1(x))(y-\beta_2(x))\cdots(y-\beta_{d_g}(x)),$$

where $\alpha_j(x), \beta_j(x) \in \overline{K[x]}$. Equation (3.9) applied to the $\alpha_j(x)$ and $\beta_j(x)$ implies

$$|\theta(x)-\alpha_j(x)| \leq |\theta(x)| + |\alpha_j(x)| \leq |\theta(x)| + \mathcal{L}_f$$

and

$$|\theta(x)-\beta_i(x)| \geq |\theta(x)| - |\beta_i(x)| \geq |\theta(x)| - \mathcal{L}_g,$$

for $1 \leq j \leq d_f$ and $1 \leq i \leq d_g$. From the above, we deduce

$$|f(x,\theta(x))| \leq |\ell_f|(|\theta(x)| + \mathcal{L}_f)^{d_f}$$

and

$$|g(x,\theta(x))| \geq |\ell_g|(|\theta(x)| - \mathcal{L}_g)^{d_g}.$$

Since $f(x,\theta(x)) = -M(x)g(x,\theta(x))$, we will obtain a contradiction when

$$|\ell_f|(|\theta(x)| + \mathcal{L}_f)^{d_f} < |M(x)||\ell_g|(|\theta(x)| - \mathcal{L}_g)^{d_g}$$

or, equivalently,

$$|M(x)| > \frac{|\ell_f|(|\theta(x)| + \mathcal{L}_f)^{d_f}}{|\ell_g|(|\theta(x)| - \mathcal{L}_g)^{d_g}}.$$

We now focus on altering the right-hand side of this last inequality to obtain the contradiction. Specifically, we observe that

$$\begin{aligned}
\frac{|\ell_f|(|\theta(x)| + \mathcal{L}_f)^{d_f}}{|\ell_g|(|\theta(x)| - \mathcal{L}_g)^{d_g}} &= \frac{|\ell_f|\left[\dfrac{|\theta(x)| + \mathcal{L}_f}{|\theta(x)| - \mathcal{L}_g}\right]^{d_f}}{|\ell_g|\left(|\theta(x)| - \mathcal{L}_g\right)^{d_g - d_f}} \\
&= \frac{|\ell_f|\left[\dfrac{|\theta(x)| + \mathcal{L}_f + |\theta(x)| - \mathcal{L}_g - |\theta(x)| + \mathcal{L}_g}{|\theta(x)| - \mathcal{L}_g}\right]^{d_f}}{|\ell_g|\left(|\theta(x)| - \mathcal{L}_g\right)^{d_g - d_f}} \\
&= \frac{|\ell_f|\left(1 + \dfrac{\mathcal{L}_f + \mathcal{L}_g}{|\theta(x)| - \mathcal{L}_g}\right)^{d_f}}{|\ell_g|\Big(|\theta(x)| - \mathcal{L}_g\Big)^{d_g - d_f}} \;\leq\; \frac{|\ell_f|}{|\ell_g|}\Big(\mathcal{L}_f + \mathcal{L}_g + 1\Big)^{d_f},
\end{aligned}$$

where we have used the assumption (3.12) to obtain the inequality. From (3.11), we obtain the desired contradiction. Therefore, (3.12) does not hold and, when $u(x,\theta(x)) = 0$, we deduce that

$$|\theta(x)| < \mathcal{L}_g + 1. \tag{3.13}$$

Note that if $u(x,\theta(x)) = 0$ and $g(x,\theta(x)) = 0$, then

$$f(x,\theta(x)) = -M(x)g(x,\theta(x)) = 0,$$

contradicting that $f(x,y)$ and $g(x,y)$ are relatively prime over $K(x)$. Thus, $u(x,y)$ and $g(x,y)$ have no common roots. Let $\theta_1(x),\ldots,\theta_{d_u}(x)$ be all the roots of $u(x,y)$ including repeated roots. Since $u(x,y)$ and $g(x,y)$ have no common roots, we deduce

$$\left|\ell_u^{d_g}\prod_{j=1}^{d_u} g(x,\theta_j(x))\right| = \Big|\mathrm{Res}(u,g)\Big| \geq 1, \tag{3.14}$$

since $\mathrm{Res}(u, g) \in K[x]$. Since each $\theta_j(x)$ is a root of $F(x, y)$, we deduce that

$$\left|\ell_u^{d_g} \prod_{j=1}^{d_u} f(x, \theta_j(x))\right| = |M(x)|^{d_u} \left|\ell_u^{d_g} \prod_{j=1}^{d_u} g(x, \theta_j(x))\right|. \tag{3.15}$$

We focus on bounding the left-hand side of (3.15). Observe that by the nonarchimedean property of absolute value and (3.13), we have

$$|f(x, \theta_j(x))| \leq h_f(\mathcal{L}_g + 1)^{d_f}.$$

We deduce that

$$\left|\ell_u^{d_g} \prod_{j=1}^{d_u} f(x, \theta_j(x))\right| = |\ell_u|^{d_g} \prod_{j=1}^{d_u} |f(x, \theta_j(x))| \leq |\ell_u|^{d_g} \left(h_f(\mathcal{L}_g + 1)^{d_f}\right)^{d_u}. \tag{3.16}$$

Applying (3.14) and (3.16) to (3.15), we deduce

$$|M(x)|^{d_u} \leq |\ell_u|^{d_g} \left(h_f(\mathcal{L}_g + 1)^{d_f}\right)^{d_u}.$$

Thus,

$$|M(x)| \leq |\ell_u|^{d_g/d_u} h_f(\mathcal{L}_g + 1)^{d_f}.$$

Since $|\ell_u| \geq 1$ and $d_g > d_f \geq 0$, we obtain

$$|M(x)| \leq |\ell_u|^{d_g} h_f(\mathcal{L}_g + 1)^{d_f}$$

and

$$|\ell_u| \geq \left(\frac{|M(x)|}{h_f(\mathcal{L}_g + 1)^{d_f}}\right)^{1/d_g}.$$

This completes the proof of Lemma 29. □

Now, we can begin the proof of Theorem 28 by using Theorem 19. This proof is done similar to the proof of Theorem 24.

Proof of Theorem 28. Assume the conditions in Theorem 28 with $d_f \geq 1$ and that

$$F(x, y) = u(x, y)v(x, y),$$

where $u(x,y)$ and $v(x,y)$ are in $(K[x])[y]$ such that $d_u, d_v \geq 1$. The conditions imply that we have an irreducible polynomial $p(x)$ in $K[x]$ such that $p(x) \nmid \ell_f \ell_g$ and

$$p(x)^k \mid M(x), \quad p(x)^{k+1} \nmid M(x) \quad \text{and} \quad |p(x)|^k > |M(x)|^{1-\delta}.$$

Since $d_g > d_f$, we deduce $d_F = d_g$ and all terms of $F(x,y)$ having degree larger than d_f in y will be terms in $M(x)g(x,y)$. Thus, $p^k(x)$ divides all these terms of $F(x,y)$. Since $p(x) \nmid \ell_g$, we see that $p(x)^{k+1}$ does not divide ℓ_F. Since $p(x) \nmid \ell_f$, the term of $F(x,y)$ of degree d_f in y will have a coefficient that is not divisible by $p(x)$. From the conditions in the theorem, we have $\gcd(k, d_g - d_f) = 1$. Thus, there are no lattice points besides the endpoints on the leftmost vector of the Newton polygon of $F(x,y)$ with respect to $p(x)$ from $(0,k)$ to $(d_g - d_f, 0)$. Therefore, one factor, which we take to be $v(x,y)$, has a translation of this vector in its Newton polygon with respect to $p(x)$. Then $p(x) \nmid \ell_u$ and

$$|\ell_u| \leq \frac{|M(x)||\ell_g|}{|p(x)^k|} < |M(x)|^{\delta}|\ell_g|.$$

Lemma 29 implies

$$\left(\frac{|M(x)|}{h_f(\mathcal{L}_g+1)^{d_f}}\right)^{1/d_g} < |M(x)|^{\delta}|\ell_g|.$$

Therefore,

$$|M(x)|^{\frac{1-\delta d_g}{d_g}} = |M(x)|^{(1/d_g)-\delta} < |\ell_g| \left(h_f(\mathcal{L}_g+1)^{d_f}\right)^{1/d_g}$$

so that

$$|M(x)| < \left(h_f|\ell_g|^{d_g}(\mathcal{L}_g+1)^{d_f}\right)^{\frac{1}{1-\delta d_g}}.$$

By the lower bound on $|M(x)|$ in the statement of Theorem 28, this is a contradiction. Thus, $F(x,y)$ is irreducible over $K(x)$. □

Chapter 4

On the nth order Euler Polynomials of degree n that are Eisenstein

This chapter will focus on the results from section 1.3 of the introduction. The aim is to prove Theorem 20 and Theorem 21. We will begin by providing some background and preliminary results necessary for proving Theorem 20and the proof of Theorem 20. Lastly, we will discuss the consequence of Theorem 20 and the proof of Adelberg and Filaseta's main result in [4], Theorem 21.

4.1 Background

Recall that the mth order Euler polynomial of degree n, denoted $E_n^{(m)}(x)$, is defined by (1.1). The left-hand side of the equation is to be interpreted as the formal product of Maclaurin series in t. We will focus on the generalized Euler polynomials $E_n^{(n)}(x)$, or in other words, the case $m = n$.

We obtain information on the Maclaurin series of $2/(e^t + 1)$ as follows. Observe that

$$\frac{2}{e^t+1} - 1 = \frac{1-e^t}{1+e^t} = \frac{e^{-t/2} - e^{t/2}}{e^{-t/2} + e^{t/2}} = -\tanh(t/2).$$

The Maclaurin series for the hyperbolic tangent is well understood, and in particular we deduce (cf. [1])

$$\frac{2}{e^t+1} - 1 = \sum_{n=0}^{\infty} \frac{-2(2^{2n}-1)B_{2n}t^{2n-1}}{(2n)!},$$

where B_{2n} denotes the $2n^{th}$ Bernoulli number. Therefore, we see that

$$\frac{2}{e^t+1} = \sum_{n=0}^{\infty} \frac{\ell_n}{n!\,2^n}\, t^n,$$

where

$$\ell_0 = 1, \quad \ell_{2n} = 0 \ \text{ for } \ n \geq 1, \quad \text{and} \quad \ell_{2n-1} = \frac{-2^{2n-1}(2^{2n}-1)B_{2n}}{n} \ \text{ for } \ n \geq 1.$$

It is known that $\ell_n \in \mathbb{Z}$ for all $n \geq 0$ (cf. the discussion of C_v in [39, pp. 27–28]).

Since $e^{tx} = \sum_{m=0}^{\infty} x^m t^m/m!$, we see from (1.1) that $E_n^{(n)}(x)$ is $n!$ times the coefficient of t^n in the expression

$$\left(\sum_{j=0}^{\infty} \frac{\ell_j}{j!\,2^j} t^j\right)^n \left(\sum_{m=0}^{\infty} \frac{x^m t^m}{m!}\right).$$

For an integer $k \in [0,n]$, the Multinomial Theorem implies the coefficient of t^{n-k} in the power in the expression above is

$$\sum_{\substack{e_1+2e_2+\cdots+ne_n=n-k \\ e_0=n-e_1-e_2-\cdots-e_n \\ e_1\geq 0,\ldots,e_n\geq 0}} \frac{n!}{e_0!e_1!e_2!\cdots e_n!} \prod_{j=1}^{n} \left(\frac{\ell_j}{j!\,2^j}\right)^{e_j},$$

where in the product if $\ell_j = e_j = 0$, then $(\ell_j/(j!\,2^j))^{e_j}$ is to be interpreted as 1. We deduce that

$$E_n^{(n)}(x) = \sum_{k=0}^{n} E_{n,k} x^k,$$

where

$$E_{n,k} = \frac{n!}{k!} \sum_{\substack{e_1+2e_2+\cdots+ne_n=n-k \\ e_0=n-e_1-e_2-\cdots-e_n \\ e_1\geq 0,\ldots,e_n\geq 0}} \frac{n!}{e_0!e_1!e_2!\cdots e_n!} \prod_{j=1}^{n} \left(\frac{\ell_j}{j!\,2^j}\right)^{e_j}. \tag{4.1}$$

Note that $E_n^{(n)}(x)$ is a monic polynomial with rational coefficients. Given that $e_1 + 2e_2 + \cdots + ne_n = n-k$ and $e_0 = n - e_1 - e_2 - \cdots - e_n$ in the sums above, the expressions

$$\frac{n!}{k!} \prod_{j=1}^{n} \left(\frac{1}{j!}\right)^{e_j} \qquad \text{and} \qquad \frac{n!}{e_0!e_1!e_2!\cdots e_n!}$$

can be viewed as multinomial coefficients and hence integers. Thus, the coefficients of $E_n^{(n)}(x)$ times a power of 2 will lie in $\mathbb{Z}$. We deduce that, for some $N = N(n) \in \mathbb{Z}^+$, we have

$$E_{n,n} = 1 \quad \text{and} \quad 2^N E_n^{(n)}(x) \in \mathbb{Z}[x]. \tag{4.2}$$

4.2 Preliminaries for $n = mp$

For the rest of this paper, assume $n = mp$ where p is an odd prime and m is a positive even integer. Our next goal is to establish Theorem 20.

For $0 \le k \le mp$, we obtain from (4.1) that

$$E_{mp,k} = \frac{(mp)!}{k!} \sum_{\substack{e_1+2e_2+\cdots+mpe_{mp}=mp-k \\ e_0=mp-e_1-e_2-\cdots-e_{mp} \\ e_1\ge 0,\ldots,e_{mp}\ge 0}} \frac{(mp)!}{e_0!e_1!e_2!\cdots e_{mp}!} \prod_{j=1}^{mp} \left(\frac{\ell_j}{j!\,2^j}\right)^{e_j}. \tag{4.3}$$

Hence, (4.2) holds with $n = mp$, and for some $N = N(m,p) \in \mathbb{Z}^+$, we have

$$E_{mp,mp} = 1 \quad \text{and} \quad 2^N E_{mp}^{(mp)}(x) \in \mathbb{Z}[x]. \tag{4.4}$$

Observe that $E_{mp}^{(mp)}(x)$ is in Eisenstein form with respect to the odd prime p if and only if each of the following holds:

(a) $p \nmid 2^N E_{mp,mp}$,

(b) $p \mid 2^N E_{mp,k}$ for all $0 \le k \le mp-1$, and

(c) $p^2 \nmid 2^N E_{mp,0}$.

Proof that part (a) always holds. We obtain from (4.4) that $2^N E_{mp,mp} = 2^N$. Since p is an odd prime, $p \nmid 2^N E_{mp,mp}$. □

Proof that part (b) always holds. Recall $\ell_j \in \mathbb{Z}$ for all j and $\ell_{2n} = 0$ for positive integer n. From (4.3), it suffices to show p divides at least one of the multinomial coefficients

$$a_k(e_1,\ldots,e_{mp}) = \frac{(mp)!}{k!} \prod_{j=1}^{mp} \left(\frac{1}{j!}\right)^{e_j} \quad \text{and} \quad b_k(e_1,\ldots,e_{mp}) = \frac{(mp)!}{e_0!e_1!e_2!\cdots e_{mp}!}$$

for each integer $k \in [0, mp)$ and each possible set $\{e_1,\ldots,e_{mp}\}$ of non-negative integers with $e_1+2e_2+\cdots+mpe_{mp} = mp-k$. To do so, we will make use of the following lemma due to E. E. Kummer [34].

Lemma 30 (Kummer [34]). *Let n and u be integers with $n \geq u \geq 0$, and let p be a prime. If v is the number of carries when adding u and $n-u$ in base p, then*

$$\nu_p\left(\binom{n}{u}\right) = v.$$

Corollary 31. *Let n be a positive integer, and let $u_1, u_2, \ldots, u_r$ be non-negative integers such that $n = u_1 + u_2 + \cdots + u_r$. Then*

$$\nu_p\left(\frac{n!}{u_1! \cdots u_r!}\right) = v$$

where v is the number of carries when performing the additions $u_1 + u_2 + \ldots + u_r$ in base p from left to right.

Corollary 31 is an immediate consequence of Lemma 30 and the identity

$$\frac{n!}{u_1! \cdots u_r!} = \binom{u_1+u_2}{u_2}\binom{u_1+u_2+u_3}{u_3}\cdots\binom{u_1+u_2+\ldots+u_r}{u_r}.$$

Observe that the corollary implies that the number of carries in Corollary 31 is independent of the order in which we add the numbers $u_1, u_2, \ldots, u_r$ in base p. Our main interest in Corollary 31 is the case where $v = 0$, which occurs precisely when there are no carries when adding the numbers $u_1, u_2, \ldots, u_r$ in base p. To put this another way, let $d_j^{(i)} \in \{0, 1, \ldots, p-1\}$ (digits in base p) for all i and j with $0 \leq i \leq r$ and $0 \leq j \leq n_p = \lfloor \log n / \log p \rfloor$. Suppose

$$n = \sum_{j=0}^{n_p} d_j^{(0)} p^j \quad \text{and} \quad u_i = \sum_{j=0}^{n_p} d_j^{(i)} p^j \text{ for } i \in \{1, \ldots, r\}.$$

Then $v = 0$ precisely when

$$d_j^{(0)} = d_j^{(1)} + d_j^{(2)} + \cdots + d_j^{(r)}, \quad \text{for all } j \in \{0, 1, \ldots, n_p\}. \tag{4.5}$$

Now, suppose p does not divide $b_k = b_k(e_1, \ldots, e_{mp})$. We complete the proof of (b) by showing $a_k = a_k(e_1, \ldots, e_{mp})$ is divisible by p. Since the multinomial coefficient b_k given above has numerator $(mp)!$, we deduce from Corollary 31 with $v = 0$ that each e_j is divisible by p. Since $k < mp$, we have $e_1 + 2e_2 + \cdots + mpe_{mp} = mp - k > 0$ so

that at least one of $e_1, \ldots, e_{mp}$ is positive. Suppose such an e_j is $e_{j'}$. Since $p \mid e_{j'}$, we deduce $e_{j'} \geq p$. On the other hand, there are $e_{j'}$ occurrences of $j'!$ in the denominator of the multinomial coefficient a_k, and it is impossible to add a positive integer to itself p times in base p without having a carry (just consider what happens to the the right-most digit in base p during the additions or refer to (4.5)). We deduce $p \mid a_k$. $\square$

We are thus left with determining when (c) occurs in order to determine when $E_{mp}^{(mp)}(x)$ is in Eisenstein form with respect to p. As (c) is a result about the constant term of $E_{mp}^{(mp)}(x)$, we study this constant term next. To finish the proof of Theorem 20, we want to show that $p^2 \mid E_{mp,0}$ if and only if p divides $m(2^m - 1)B_m$.

4.3 The constant term of $E_{mp}^{(mp)}(x)$

To show part (c), we make use of work of G. D. Liu and W. P. Zhang [36] on generalized Euler numbers, which we will write as $\overline{E}_{2n}^{(x)}$ using a slightly different notation than in [36] to avoid confusion with the generalized Euler polynomials. The authors in [36] define $\overline{E}_{2n}^{(x)}$ through the equation

$$\left(\frac{2}{e^t + e^{-t}}\right)^x = \sum_{n=0}^{\infty} \overline{E}_{2n}^{(x)} \frac{t^{2n}}{(2n)!}.$$

Observe that the left-hand side above is an even function, so its Maclaurin series only involves terms of even degree in t as shown. Also, by taking $t = 0$, one can see that $\overline{E}_0^{(k)} = 1$ for all positive integers k. Note that $\overline{E}_{2n}^{(1)}$ denotes the classical $(2n)^{th}$ Euler number.

Define the Stirling numbers of the first kind $s(n, k)$ for integers n and k with $n \geq k \geq 0$ by the double recurrence relations

$$s(n, 0) = 0, \quad \forall n \geq 1, \qquad s(n, n) = 1, \quad \forall n \geq 0, \qquad \text{and}$$
$$s(n, k) = s(n-1, k-1) - (n-1)s(n-1, k), \quad \forall n > k \geq 1.$$

Also, define the central factorial numbers $T(n,k)$ for integers n and k with $n \geq k \geq 0$ by the double recurrence relations

$$T(n,0) = 0, \quad \forall n \geq 1, \qquad T(n,n) = 1, \quad \forall n \geq 0, \qquad \text{and}$$
$$T(n,k) = T(n-1,k-1) + k^2 T(n-1,k), \quad \forall n > k \geq 1.$$

Though other definitions of these numbers would suffice for our purposes, these recurrence relations help emphasize that the numbers $s(n,k)$ and $T(n,k)$ are integers. Following [36], for integers n and k with $n \geq k \geq 1$, we also define

$$\rho(n,k) = (-1)^k \sum_{j=k}^{n} \frac{(2j)!}{2^j j!} s(j,k) T(n,j).$$

As $2^j j!$ can be viewed as the product of the even positive integers $\leq 2j$, we deduce that $\rho(n,k) \in \mathbb{Z}$. The following is due to G. D. Liu and W. P. Zhang (see Theorem 2.1, the sentence after (2.18), and (3.16) in [36]).

Theorem 32 (Liu and Zhang [36], 2008)**.** *Let n and k be positive integers. Then*

$$\overline{E}_{2n}^{(k)} = \sum_{i=1}^{n} \rho(n,i)\, k^i.$$

Furthermore,

$$\rho(n,1) = -\overline{E}_{2n-2}^{(2)} = -\frac{2^{2n-1}(2^{2n}-1)B_{2n}}{n}.$$

Since $\rho(n,i) \in \mathbb{Z}$ for every $i \in \{1,2,\ldots,n\}$, we deduce from the first equation in Theorem 32 that $\overline{E}_{2n}^{(k)} \in \mathbb{Z}$ for all positive integers n and k. Recall also that $\overline{E}_0^{(k)} = 1$ for every integer $k \geq 1$. We turn now to connecting the numbers $\overline{E}_{2n}^{(x)}$ to the constant term $E_{mp,0} = E_{mp}^{(mp)}(0)$ in our generalized Euler polynomial $E_{mp}^{(mp)}(x)$.

As before, we take m to be an even positive integer and p to be an odd prime. By setting $x = 0$ in (1.1) and replacing t with $2t$, we see that

$$\begin{aligned}\left(\sum_{n=0}^{\infty} \overline{E}_{2n}^{(mp)} \frac{t^{2n}}{(2n)!}\right)\left(\sum_{j=0}^{\infty} \frac{(-mp)^j t^j}{j!}\right) &= \left(\frac{2}{e^t + e^{-t}}\right)^{mp} e^{-mpt} \\ &= \left(\frac{2}{e^{2t}+1}\right)^{mp} \\ &= \sum_{n=0}^{\infty} E_n^{(mp)}(0) \frac{(2t)^n}{n!}.\end{aligned} \tag{4.6}$$

To obtain the term of degree t^{mp} in the product on the left, we want to add terms of the form

$$\overline{E}_{mp-j}^{(mp)} \frac{t^{mp-j}}{(mp-j)!} \cdot \frac{(-mp)^j t^j}{j!} = (-1)^j \binom{mp}{j} (mp)^j \, \overline{E}_{mp-j}^{(mp)} \frac{t^{mp}}{(mp)!},$$

where $0 \leq j \leq mp$. Therefore, from (4.6), we obtain

$$2^{mp} E_{mp}^{(mp)}(0) = \sum_{j=0}^{mp} (-1)^j \binom{mp}{j} (mp)^j \, \overline{E}_{mp-j}^{(mp)}.$$

Since $\overline{E}_{mp-j}^{(mp)} \in \mathbb{Z}$ for each j in the sum, we obtain the congruence

$$2^{mp} E_{mp}^{(mp)}(0) \equiv \overline{E}_{mp}^{(mp)} \pmod{p^2}. \tag{4.7}$$

Since m is even and $\rho(n,i) \in \mathbb{Z}$, from Theorem 32, we see that

$$\overline{E}_{mp}^{(mp)} = \sum_{i=1}^{mp/2} \rho\left(\frac{mp}{2}, i\right) (mp)^i \equiv mp \, \rho\left(\frac{mp}{2}, 1\right) \pmod{p^2}, \tag{4.8}$$

which in particular implies from (4.7) that $E_{mp}^{(mp)}(0)$ is divisible by p. Furthermore, Theorem 32 implies

$$\rho\left(\frac{mp}{2}, 1\right) = -\frac{2^{mp-1}(2^{mp}-1)B_{mp}}{mp/2} = -\frac{2^{mp}(2^{mp}-1)B_{mp}}{mp}. \tag{4.9}$$

We consider now two cases, depending on whether $p-1$ divides divides m or not, beginning with the latter.

Case 1. *$p-1$ does not divide m.*

Since $p-1$ does not divide m, Kummer's congruence (cf. Corollary 2 in [3]) implies

$$\frac{B_{mp}}{mp} \equiv \frac{B_m}{m} \pmod{p}.$$

Also, Fermat's Little Theorem gives us

$$2^{mp} \equiv 2^m \pmod{p} \qquad \text{and} \qquad 2^{mp} - 1 \equiv 2^m - 1 \pmod{p}.$$

Combining the above with (4.7), (4.8) and (4.9), we deduce

$$E_{mp}^{(mp)}(0) \equiv -p\,(2^m - 1) B_m \pmod{p^2}.$$

In this case, $E_{mp}^{(mp)}(x)$ is in Eisenstein form with respect to p if and only if $p \nmid 2(2^m-1)B_m$, where the extra factor of 2 is simply to ensure $2(2^m-1)B_m$ is an integer. On the other hand, if $p \mid m$, then by an observation going back to J. C. Adams [2] and which follows from Kummer's congruence noted above, we have that p divides the numerator of B_m so that $p \mid 2(2^m-1)B_m$. Recalling m is even, it follows that, for this case, $E_{mp}^{(mp)}(x)$ is in Eisenstein form with respect to p if and only if $p \nmid m(2^m-1)B_m$.

Case 2. *$p-1$ divides m.*

The main difference in this case is that the von Staudt-Clausen Theorem (cf. [4]) implies that p exactly divides the denominator of B_m and B_{mp} (that is, p divides these denominators and p^2 does not). We will return to using this information shortly.

If $p \mid m$, then (4.8) implies $\overline{E}_{mp}^{(mp)}$ is divisible by p^2 since $\rho(mp/2,1) \in \mathbb{Z}$. From (4.7), we deduce $p^2 \mid E_{mp}^{(mp)}(0)$ so that $E_{mp}^{(mp)}(x)$ is not in Eisenstein form with respect to p.

Suppose now $p \nmid m$. Let e be the order of 2 modulo p, and let $r = \nu_p(2^e-1)$. Note then that

$$p^r \mid (2^e-1) \qquad \text{and} \qquad p^{r+1} \nmid (2^e-1),$$

and e is the order of 2 modulo p^r. We claim that the order of 2 modulo p^{r+j} is ep^j for every integer $j \geq 0$. It suffices to show that

$$p^{r+j} \mid \left(2^{ep^j}-1\right) \qquad \text{and} \qquad p^{r+j+1} \nmid \left(2^{ep^j}-1\right), \tag{4.10}$$

for every $j \geq 0$. The case $j=0$ holds from the above. We give an induction argument, supposing now that for some integer $j_0 \geq 0$, we know (4.10) holds with $j = j_0$. Then there is an integer s such that

$$2^{ep^{j_0}} = 1 + sp^{r+j_0} \qquad \text{and} \qquad p \nmid s.$$

We deduce, from the Binomial Theorem, that

$$2^{ep^{j_0+1}} = (1+sp^{r+j_0})^p \equiv 1 + sp^{r+j_0+1} \pmod{p^{r+j_0+2}}.$$

We obtain from this that (4.10) holds with $j = j_0 + 1$, establishing (4.10) for all $j \geq 0$ by induction. Thus, the order of 2 modulo p^{r+j} is ep^j for every integer $j \geq 0$.

Since e divides $p-1$ and $p-1$ divides m but $p \nmid m$, we deduce that

$$p^r \mid (2^m - 1), \quad p^{r+1} \nmid (2^m - 1), \quad p^{r+1} \mid (2^{mp} - 1), \quad \text{and} \quad p^{r+2} \nmid (2^{mp} - 1).$$

We consider two possibilities depending on whether $r = 1$ or $r > 1$.

For the first possibility, where $r = 1$, in (4.9), we have B_{mp} has a denominator exactly divisible by p, p also exactly divides the denominator mp since $p \nmid m$, and the expression $2^{mp}(2^{mp} - 1)$ is exactly divisible by $p^{r+1} = p^2$. Thus, (4.9) implies that $\rho(mp/2, 1)$ is not divisible by p, and (4.7) and (4.8) in turn imply that $E_{mp}^{(mp)}(x)$ is in Eisenstein form with respect to p. Furthermore, $p \nmid m$, $p^r = p$ exactly divides $2^m - 1$, and p exactly divides the denominator of B_m so that p does not divide $m(2^m - 1)B_m$.

Now, consider the possibility that $r > 1$. Then B_{mp} has a denominator exactly divisible by p and the expression $2^{mp}(2^{mp} - 1)$ is divisible by p^{r+1} and hence p^3. We deduce from (4.9) that $\rho(mp/2, 1)$ is divisible by p, so that (4.7) and (4.8) imply that $E_{mp}^{(mp)}(x)$ is not in Eisenstein form with respect to p. Here, $2^m - 1$ is divisible by p^2 and p exactly divides the denominator of B_m so that p divides $m(2^m - 1)B_m$.

Combining the above, we see that in the case $p - 1$ divides m, we have $E_{mp}^{(mp)}(x)$ is in Eisenstein form with respect to p if and only if $p \nmid m(2^m - 1)B_m$.

4.4 Proof of Theorem 21

In this section, we justify Theorem 21. We begin with the following, which is contained in the argument for Lemma 2 in [4].

Lemma 33. *The inequality $|2(2^m - 1)B_m| \leq m^m$ holds for every $m \in \mathbb{Z}^+$.*

Proof. We use that $B_1 = -1/2$, and for $k \geq 1$, we have $B_{2k+1} = 0$ and

$$B_{2k} = (-1)^{k-1} \frac{2(2k)!}{(2\pi)^{2k}} \zeta(2k)$$

(cf. [10]). For $m = 1$, we have $|2(2^m - 1)B_m| = 1 = m^m$, so the stated inequality holds. For $m = 2k \geq 2$, we have $|\zeta(2k)| \leq |\zeta(2)| < 2$ so that

$$|2(2^m - 1)B_m| \leq 2(2^m - 1)\frac{4(m!)}{(2\pi)^m} < \frac{8(m!)}{\pi^m} < m^m,$$

completing the proof. □

The basic idea is to consider the positive integers $n = mp \leq t$ where $m \in \mathbb{Z}^+$ and $p > m$ is a prime. For such n, Theorem 20 implies that if p does not divide the integer $2(2^m - 1)B_m$, then $E_{mp}^{(mp)}(x)$ is in Eisenstein form with respect to p. We show that most such n (asymptotically almost all) are such that $E_n^{(n)}(x)$ is in Eisenstein form with respect to the largest prime divisor p of n.

Fix $\varepsilon > 0$. Let $\mathcal{S} = \mathcal{S}(\varepsilon, t)$ be the set of pairs (m, p) with

$$m \in \mathbb{Z}^+, \quad m \leq t^{(1/2)-\varepsilon}, \quad m \text{ even},$$
$$p > m \text{ a prime}, \quad mp \leq t, \quad \text{and} \quad p \nmid 2(2^m - 1)B_m.$$

By Theorem 20, the pairs $(m, p) \in \mathcal{S}$ correspond to unique positive integers $n = mp \leq t$ for which $E_n^{(n)}(x)$ is in Eisenstein form. Our interest is in counting the number of pairs in $\mathcal{S}$.

We make use of the notation $\pi(x)$ for the number of primes $\leq x$ and $f(t) = (1 + o(1))g(t)$ to indicate that for every fixed $\varepsilon' > 0$ and $t \geq t_0(\varepsilon')$ sufficiently large, we have $(1 - \varepsilon')g(t) < |f(t)| < (1 + \varepsilon')g(t)$. For a fixed $m \in \mathbb{Z}^+$ with $m \leq t^{(1/2)-\varepsilon}$ and m even, there are $\pi(t/m) - \pi(m)$ different primes $p > m$ for which $mp \leq t$. By Lemma 33, there are $< m$ primes $p > m$ which divide $2(2^m - 1)B_m$. From the Prime Number Theorem, the number of pairs $(m, p) \in \mathcal{S}$, with m still fixed, is at least

$$\pi\left(\frac{t}{m}\right) - \pi(m) - m \geq (1 + o(1))\frac{t}{m\log(t/m)} - 2t^{(1/2)-\varepsilon}$$
$$= (1 + o(1))\frac{t}{m\log(t/m)},$$

where the equality follows from

$$\frac{t}{m\log(t/m)} \geq \frac{t}{t^{(1/2)-\varepsilon}\log t} = \frac{t^{(1/2)+\varepsilon}}{\log t}.$$

The above only depends on $t/m \geq t^{(1/2)+\varepsilon}$ being sufficiently large compared to $t^{(1/2)-\varepsilon}$, and in particular the $o(1)$ notation is uniform in $m \leq t^{(1/2)-\varepsilon}$. We obtain that

$$|S| \geq (1+o(1)) \sum_{\substack{m \leq t^{(1/2)-\varepsilon} \\ m \text{ even}}} \frac{t}{m\log(t/m)} = (1+o(1))\frac{\log(2)\, t}{2},$$

where the latter can be deduced from a comparison of the sum to the integral

$$\int_1^z \frac{t}{(2x)\log(t/(2x))}\, dx = -\frac{t\log\log(t/(2x))}{2}\bigg|_1^z$$

where $z = (1/2)\, t^{(1/2)-\varepsilon}$. Theorem 21 follows.

Bibliography

[1] M. Abramowitz and I. Stegun, Handbook of mathematical functions with formulas, graphs, and mathematical tables, National Bureau of Standards Applied Mathematics Series, No. 55 U. S. Government Printing Office, Washington, D.C., 1964.

[2] J. C. Adams, *Table of the values of the first sixty-two numbers of Bernoulli*, J. Reine Angew. Math. 85 (1878), 269–272.

[3] A. Adelberg, *Congruences of p-adic integer order Bernoulli numbers*, J. Number Theory 59 (1996), 374–388.

[4] A. Adelberg and M. Filaseta, *On mth order Bernoulli polynomials of degree m that are Eisenstein*, Colloq. Math. 93 (2002), 21–26.

[5] W. D. Banks, T. Freiberg and C. L. Turnage-Butterbaugh, *Consecutive primes in tuples*, Acta Arith., 167 (2015), 261–266.

[6] G. Barnes, author, "Riesel conjectures and proofs", On page of No Prime Left Behind Project at http://www.noprimeleftbehind.net/crus/Riesel-conjectures.htm, Updated Sept. 6, 2021.

[7] N.C. Bonciocat, *An irreducibility criterion for the sum of two relatively prime polynomials*, Funct. Approx. Comment. Math. **54** (2016), no. 2 163–171.

[8] N.C. Bonciocat, Y. Bugeaud, M. Cipu, and M. Mignotte, *Irreducibility criteria for sums of two relatively prime multivariate polynomials*, Math. Derecen **87** (2015), no. 3-4 255–267.

[9] N.C. Bonciocat, Y. Bugeaud, M. Cipu, and M. Mignotte, *Irreducibility criteria for sums of two relatively prime polynomials*, Int. J. Number Theory **9** (2013), no. 6 1529–1539.

[10] Z. I. Borevich and I. R. Shafarevich, Number Theory, Academic Press, New York, 1966.

[11] R. Bowen, *The sequence $ka^n + 1$ composite for all n*, Math. Monthly 71 (1964), 175–176.

[12] A. Brunner, C. Caldwell, D. Krywaruczenko and C. Lownsdale, *Generalized Sierpiński numbers base b*, preprint on University of Tennessee at Martin page (2008), https://www.utm.edu/staff/caldwell/preprints/2to100.pdf.

[13] M. Cavachi, *On a special case of Hilbert's irreducibility theorem*, J. Number Theory **82** (2000), no. 1 96–99.

[14] M. Cavachi, M. Vajaitu and A. Zaharescu, *A class of irreducible polynomials*, J. Ramanujan Math. Soc. **17** (2002), no. 3 161–172.

[15] G. Dumas, *Sur quelques cas d'irreductibilite des polynomes a coefficients rationnels*, J. de Math. Pure et Appl. **2** (1906), 191–258.

[16] P. Erdős, *Solution to problem 1029: Erdős and the computer*, Mathematics Magazine 52 (1979), 180-181.

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

[18] M. Filaseta, R. Groth and T. Luckner, *Generalized Sierpiński Numbers*, arXiv:2305.09219.

[19] M. Filaseta and J. Juillerat, *Consecutive primes which are widely digitally delicate*, INTEGERS: Ron Graham Memorial Volume, Vol. 21A, 2021, Paper No. A12, 37 pp.; also see, Number Theory and Combinatorics: A Collection in Honor of the Mathematics of Ronald Graham, edited by Bruce M. Landman, Florian Luca, Melvyn B. Nathanson, Jaroslav Nešetřil and Aaron Robertson, Berlin, Boston: De Gruyter, 2022, pp. 209–248.

[20] M. Filaseta and J. Juillerat, Data for "Consecutive primes which are widely digitally delicate," https://people.math.sc.edu/filaseta/ConsecutiveWDDPrimes.html.

[21] M. Filaseta, J. Juillerat and T. Luckner Data for "Consecutive primes which are widely digitally delicate and Brier numbers," https://people.math.sc.edu/filaseta/ConsecutiveWDDBrierNumbers.html.

[22] M. Filaseta, J. Juillerat and T. Luckner, *Consecutive primes which are widely digitally delicate and Brier numbers*, arXiv:2209.10646.

[23] M. Filaseta, J. Juillerat and J. Southwick, Widely Digitally Stable Numbers, in *Combinatorial and Additive Number Theory IV* (ed. M. Nathanson), Springer Proc. Math. Stat. 347, Springer, Cham, 2021, 161–193.

[24] M. Filaseta and T. Luckner, *On n^{th} order Euler polynomials of degree n that are Eisenstein*, arXiv:2305.09227.

[25] M. Filaseta and J. Southwick, *Primes that become composite after changing an arbitrary digit*, Math. Comp. 90 (2021), 979–993.

[26] M. Filaseta and R. Wilcox, *An explicit dense universal Hilbert set*, Math. Proc. Cambridge Philos. Soc. **167** (2019), no. 3 531–547.

[27] T. Freiberg, *A note on the Theorem of Maynard and Tao*, arXiv:1311.5319.

[28] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–231.

[29] O. Gerard, author, The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org/A076335, Nov. 7, 2002.

[30] J. Grantham, *Finding a Widely Digitally Delicate Prime*, Integers **23** (2023), A22, 5 pages.

[31] D. Hilbert, *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. für die reine und angewandte Mathematik **110** (1892), no. 3 104–129.

[32] N.R. Kanasari, V. Laohakosol, and P. Singthongla, *Reducibility of polynomials over algebraic number fields*, Integers **17** (2020), 11 pages.

[33] S. V. Konyagin, *Numbers that become composite after changing one or two digits*, Pioneer Jour. of Algebra, Number Theory and Appl. 6 (2013), 1–7.

[34] E. E. Kummer, *Über die Ergnzungssätze zu den allgemeinen Reciprocitätsgesetzen*, Journal für die reine und angewandte Mathematik, 44 (1852), 93–146.

[35] K. Langmann, *Der Hilbertsche irreduzibilitatssatz und primzahlfragen*, J. Reine Angew. Math. **413** (1991), 213–219.

[36] G. D. Liu and W. P. Zhang, *Applications of an explicit formula for the generalized Euler numbers*, Acta Math. Sin. (Engl. Ser.) 24 (2008), 343–352.

[37] J. Maynard, *Dense clusters of primes in subsets*, Compositio Math. 152 (2016), 1517–1554.

[38] S. Nadis, "Mathematicians Find a New Class of Digitally Delicate Primes", Quanta Magazine, March 30, 2021, https://www.quantamagazine.org/mathematicians-find-a-new-class-of-digitally-delicate-primes-20210330/.

[39] N. E. Nörlund, Vorlesungen Über Differenzenrechnung, Chelsea, New York, 1954.

[40] M. Parker, Stand-Up Maths: How do you prove a prime is infinitely fragile?, July 28, 2021, `https://www.youtube.com/watch?v=p3Khnx0lUDE`.

[41] "PrimeGrid", https://www.primegrid.com/ (Updates per prime search).

[42] Q. I. Rahman and G. Schmeisser, *Analytic Theory of Polynomials*, London Mathematical Society Monographs, New Series 26, The Clarendon Press, Oxford University Press, Oxford, 2002.

[43] H. Riesel, *Några stora primtal*, Elementa 39 (1956), 258–260.

[44] R. M. Robinson, *A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers*, Proc. Amer. Math. Soc. 9 (1958), 673–681.

[45] D. K. L. Shiu, *Strings of congruent primes*, J. Lond. Math. Soc. 61 (2000), 359–373.

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

[47] N. J. A. Sloane, author, The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org/A076336, Nov. 7, 2002.

[48] A. Swaminathan, *An introduction to the theory of valued fields*, Harvard Jun. Paper (2015).

[49] T. Tao, *A remark on primality testing and decimal expansions*, J. Aust. Math. Soc. 91 (2011), 405–413.

[50] J. Vaaler, "Notes on absolute values on fields and heights", Chapter 3, `https://web.ma.utexas.edu/users/voloch/Preprints/vaalerch3.pdf`. (For all chapters see `https://web.ma.utexas.edu/users/voloch/390-08.html`.)

[51] D. W. Wilson, editor, The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org/A101036, Jan. 17, 2005.

Appendix A

Coverings for Chapter 2

To aid in verifying the computations in this dissertation, all the data in this appendix can be found in [21] as lists suitable for computations. This appendix begins with Table A.1, which lists the number of distinct primes used, $L = L(b)$, that divide $\Phi_b(2)$, do not divide b, and are not in $\mathcal{P}(A_1)$. Note the * indicates the prime 5 is used once in each covering. The b listed correspond to moduli used in our coverings. Table A.2 gives a lower bound on number of distinct primes, $M = M(b)$, that divide $\Phi_b(2)$, do not divide b, are not in $\mathcal{P}(A_1)$, and are not used in either covering. The * in this table represents an $M(b)$ that is a lower bound; that is, we did not completely factor $\Phi_b(2)$.

Tables A.3 and A.4 list the congruence classes $n \equiv a \pmod{b}$ that form the covering systems we obtained for $k \cdot 2^n + 1$ and $k \cdot 2^n - 1$ respectively. Recall that, with the order b of 2 fixed, the choice of a prime p associated with a given congruence class does not matter. Thus, for example, $\Phi_{64}(2)$ has exactly two prime factors, 641 and 6700417, neither of which are in $\mathcal{P}(A_1)$. These two primes are in the count for $L(64)$ in Table A.1. We associate some ordering of these two primes. The second column of Table A.3 indicates that one of these primes is associated with the congruence $n \equiv 22 \pmod{64}$ (indicated by "1" in the second column) and the other is associated with the congruence $n \equiv 54 \pmod{64}$ (indicated by "2" in the second column). Note that we do not attempt to clarify which of the two primes is associated with which congruence as it does not matter.

Table A.1 Number of primes used in both coverings, $L = L(b)$

b	L	b	L	b	L	b	L	b	L
4	1*	176	3	462	1	960	4	1690	2
13	1	182	3	468	5	968	4	1716	8
16	1	195	1	480	2	975	4	1728	4
25	2	198	2	484	4	980	5	1755	6
26	1	200	4	486	3	1014	3	1792	4
27	1	208	1	495	2	1040	4	1848	5
32	1	216	2	507	1	1053	3	1872	4
33	1	220	2	520	5	1056	4	1875	5
35	1	224	2	528	2	1078	3	1890	3
39	1	225	3	540	4	1080	3	1960	4
40	1	231	1	546	2	1089	4	1980	5
48	1	234	1	550	1	1092	5	2016	3
50	1	240	2	560	4	1100	7	2028	4
55	1	242	2	572	6	1120	4	2080	3
64	2	250	2	585	4	1125	3	2100	3
65	1	260	3	594	4	1134	3	2106	3
66	1	264	2	616	3	1155	2	2112	4
70	1	270	3	624	3	1170	5	2156	5
75	2	273	3	625	4	1183	3	2160	5
77	1	275	2	637	7	1188	6	2178	2
78	1	280	1	648	7	1232	2	2184	6
80	1	286	3	650	5	1248	3	2200	2
81	3	288	3	660	5	1250	2	2250	6
88	1	297	2	672	2	1260	3	2268	9
91	2	300	3	676	5	1274	3	2275	4
96	1	308	3	693	3	1300	7	2310	2
99	2	312	1	700	3	1320	4	2340	3
100	2	324	4	702	2	1344	4	2366	2
104	2	325	2	704	4	1350	3	2464	4
105	3	330	2	715	3	1352	4	2496	4
108	1	336	3	720	2	1365	4	2520	4
110	2	338	2	726	3	1375	3	2548	5
112	2	350	2	728	2	1386	1	2574	4
117	4	351	5	750	3	1400	2	2600	4
120	1	352	2	756	2	1404	7	2640	2
121	1	360	2	770	3	1408	3	2704	4
125	2	363	4	780	5	1430	2	2730	3
130	2	364	2	784	5	1440	4	2750	2
132	2	375	1	792	2	1452	2	2772	8
135	2	378	4	810	6	1456	4	2808	4
140	2	385	3	825	4	1485	3	2816	4
143	3	390	2	832	3	1512	1	2912	4
144	2	396	4	840	3	1540	4	2925	5
150	1	416	5	845	3	1560	3	3024	2
154	2	420	2	858	2	1568	2	3080	3
156	1	429	3	864	2	1584	2	3120	3
160	2	432	3	880	4	1620	2	3136	4
162	1	440	4	896	2	1625	5	3234	2
165	1	448	2	910	4	1638	3	3276	3
169	3	450	2	924	2	1664	2	3300	3
175	3	455	2	936	4	1680	4	3360	5

b	L
3432	4
3510	9
3640	4
3696	3
3744	3
3780	2
3822	3
3960	2
4095	4
4160	4
4224	2
4290	4
4312	2
4320	2
4368	3
4550	2
4732	4
5040	3
5096	2
5148	3
5200	2
5280	4
5544	2
5632	3
5824	4
5850	4
6006	4
6160	2
6240	4
6600	4
6825	3
7040	4
7392	2
7800	3
8190	2
8316	3
8580	2
8775	3
9100	4
9240	4
10080	2
10296	2
11264	2
11700	2
12012	4
13650	3
18018	3

Table A.2 Number of primes, $M = M(b)$, not used in both coverings

b	M
225	1
288	1
300	1
350	2
637	1
960	1
968	1*
1080	1
1120	1
1125	1*
1155	1
1232	1
1250	2
1260	1
1350	2*
1352	1
1430	3*
1452	3*
1485	1*
1568	1
1584	2
1620	6
1625	2*
1664	1*
1690	2*
1792	1*
1875	1*
1960	3*
2016	1*
2028	2*
2112	1*

b	M
2200	3*
2310	2*
2340	4*
2704	1*
2730	1*
2750	4*
3024	1*
3120	1*
3136	1*
3234	1*
3276	1*
3744	1*
3780	2*
3960	2*
4312	1
4320	4*
4368	1*
4732	2*
5096	1*
5200	3*
6240	2*
6825	1*
7392	2*
7800	3*
8316	1*
8580	3*
10296	1*
11264	1*
11700	4*
12012	1*

Table A.3 Covering information for Sierpiński numbers

congruence	p
$n \equiv 0 \pmod 4$	1
$n \equiv 2 \pmod{16}$	1
$n \equiv 6 \pmod{32}$	1
$n \equiv 22 \pmod{64}$	1
$n \equiv 54 \pmod{64}$	2
$n \equiv 10 \pmod{48}$	1
$n \equiv 26 \pmod{96}$	1
$n \equiv 74 \pmod{288}$	1
$n \equiv 170 \pmod{288}$	2
$n \equiv 266 \pmod{288}$	3
$n \equiv 42 \pmod{144}$	1
$n \equiv 90 \pmod{144}$	2
$n \equiv 138 \pmod{432}$	1
$n \equiv 282 \pmod{432}$	2
$n \equiv 426 \pmod{432}$	3
$n \equiv 14 \pmod{112}$	1
$n \equiv 30 \pmod{112}$	2
$n \equiv 46 \pmod{224}$	1
$n \equiv 158 \pmod{224}$	2
$n \equiv 62 \pmod{336}$	1
$n \equiv 174 \pmod{336}$	2
$n \equiv 286 \pmod{336}$	3
$n \equiv 78 \pmod{448}$	1
$n \equiv 190 \pmod{448}$	2
$n \equiv 302 \pmod{896}$	1
$n \equiv 750 \pmod{896}$	2
$n \equiv 414 \pmod{1792}$	1
$n \equiv 862 \pmod{1792}$	2
$n \equiv 1310 \pmod{1792}$	3
$n \equiv 1758 \pmod{1792}$	4
$n \equiv 94 \pmod{672}$	1
$n \equiv 206 \pmod{672}$	2
$n \equiv 318 \pmod{1344}$	1
$n \equiv 990 \pmod{1344}$	2
$n \equiv 430 \pmod{1344}$	3
$n \equiv 1102 \pmod{1344}$	4
$n \equiv 542 \pmod{2016}$	1
$n \equiv 1214 \pmod{2016}$	2
$n \equiv 1886 \pmod{2016}$	3
$n \equiv 654 \pmod{3360}$	1
$n \equiv 1326 \pmod{3360}$	2
$n \equiv 1998 \pmod{3360}$	3
$n \equiv 2670 \pmod{3360}$	4
$n \equiv 3342 \pmod{3360}$	5
$n \equiv 110 \pmod{784}$	1
$n \equiv 222 \pmod{784}$	2
$n \equiv 334 \pmod{784}$	3
$n \equiv 446 \pmod{784}$	4
$n \equiv 558 \pmod{784}$	5
$n \equiv 670 \pmod{1568}$	1
$n \equiv 1454 \pmod{1568}$	2

congruence	p
$n \equiv 782 \pmod{3136}$	1
$n \equiv 1566 \pmod{3136}$	2
$n \equiv 2350 \pmod{3136}$	3
$n \equiv 3134 \pmod{3136}$	4
$n \equiv 0 \pmod{13}$	1
$n \equiv 1 \pmod{26}$	1
$n \equiv 2 \pmod{39}$	1
$n \equiv 15 \pmod{117}$	1
$n \equiv 54 \pmod{117}$	2
$n \equiv 93 \pmod{117}$	3
$n \equiv 28 \pmod{117}$	4
$n \equiv 67 \pmod{351}$	1
$n \equiv 184 \pmod{351}$	2
$n \equiv 301 \pmod{351}$	3
$n \equiv 106 \pmod{351}$	4
$n \equiv 223 \pmod{351}$	5
$n \equiv 340 \pmod{1053}$	1
$n \equiv 691 \pmod{1053}$	2
$n \equiv 1042 \pmod{1053}$	3
$n \equiv 3 \pmod{156}$	1
$n \equiv 55 \pmod{468}$	1
$n \equiv 211 \pmod{468}$	2
$n \equiv 367 \pmod{468}$	3
$n \equiv 107 \pmod{468}$	4
$n \equiv 263 \pmod{468}$	5
$n \equiv 419 \pmod{1404}$	1
$n \equiv 887 \pmod{1404}$	2
$n \equiv 1355 \pmod{1404}$	3
$n \equiv 29 \pmod{260}$	1
$n \equiv 81 \pmod{260}$	2
$n \equiv 133 \pmod{260}$	3
$n \equiv 185 \pmod{780}$	1
$n \equiv 445 \pmod{780}$	2
$n \equiv 705 \pmod{780}$	3
$n \equiv 237 \pmod{780}$	4
$n \equiv 497 \pmod{780}$	5
$n \equiv 757 \pmod{2340}$	1
$n \equiv 1537 \pmod{2340}$	2
$n \equiv 2317 \pmod{2340}$	3
$n \equiv 17 \pmod{104}$	1
$n \equiv 43 \pmod{104}$	2
$n \equiv 69 \pmod{312}$	1
$n \equiv 173 \pmod{936}$	1
$n \equiv 485 \pmod{936}$	2
$n \equiv 797 \pmod{936}$	3
$n \equiv 277 \pmod{936}$	4
$n \equiv 589 \pmod{1872}$	1
$n \equiv 1525 \pmod{1872}$	2
$n \equiv 901 \pmod{1872}$	3
$n \equiv 1837 \pmod{1872}$	4
$n \equiv 95 \pmod{520}$	1

congruence	p
$n \equiv 199 \pmod{520}$	2
$n \equiv 303 \pmod{520}$	3
$n \equiv 407 \pmod{520}$	4
$n \equiv 511 \pmod{520}$	5
$n \equiv 5 \pmod{208}$	1
$n \equiv 31 \pmod{416}$	1
$n \equiv 239 \pmod{416}$	2
$n \equiv 57 \pmod{416}$	3
$n \equiv 265 \pmod{416}$	4
$n \equiv 83 \pmod{416}$	5
$n \equiv 291 \pmod{2080}$	1
$n \equiv 707 \pmod{2080}$	2
$n \equiv 1123 \pmod{2080}$	3
$n \equiv 1539 \pmod{4160}$	1
$n \equiv 3619 \pmod{4160}$	2
$n \equiv 1955 \pmod{4160}$	3
$n \equiv 4035 \pmod{4160}$	4
$n \equiv 109 \pmod{624}$	1
$n \equiv 317 \pmod{624}$	2
$n \equiv 525 \pmod{624}$	3
$n \equiv 135 \pmod{832}$	1
$n \equiv 343 \pmod{832}$	2
$n \equiv 551 \pmod{832}$	3
$n \equiv 759 \pmod{1664}$	1
$n \equiv 1591 \pmod{1664}$	2
$n \equiv 161 \pmod{1040}$	1
$n \equiv 369 \pmod{1040}$	2
$n \equiv 577 \pmod{1040}$	3
$n \equiv 785 \pmod{1040}$	4
$n \equiv 993 \pmod{3120}$	1
$n \equiv 2033 \pmod{3120}$	2
$n \equiv 3073 \pmod{3120}$	3
$n \equiv 187 \pmod{1248}$	1
$n \equiv 395 \pmod{1248}$	2
$n \equiv 603 \pmod{1248}$	3
$n \equiv 811 \pmod{2496}$	1
$n \equiv 2059 \pmod{2496}$	2
$n \equiv 1019 \pmod{2496}$	3
$n \equiv 2267 \pmod{2496}$	4
$n \equiv 1227 \pmod{3744}$	1
$n \equiv 2475 \pmod{3744}$	2
$n \equiv 3723 \pmod{3744}$	3
$n \equiv 19 \pmod{78}$	1
$n \equiv 45 \pmod{234}$	1
$n \equiv 123 \pmod{702}$	1
$n \equiv 357 \pmod{702}$	2
$n \equiv 591 \pmod{2106}$	1
$n \equiv 1293 \pmod{2106}$	2
$n \equiv 1995 \pmod{2106}$	3
$n \equiv 201 \pmod{1404}$	1
$n \equiv 435 \pmod{1404}$	2

Table A.3 Covering information for Sierpiński numbers cont.

congruence	p
$n \equiv 669 \pmod{1404}$	3
$n \equiv 903 \pmod{1404}$	4
$n \equiv 1137 \pmod{2808}$	1
$n \equiv 2541 \pmod{2808}$	2
$n \equiv 1371 \pmod{2808}$	3
$n \equiv 2775 \pmod{2808}$	4
$n \equiv 71 \pmod{858}$	1
$n \equiv 149 \pmod{858}$	2
$n \equiv 227 \pmod{1716}$	1
$n \equiv 1085 \pmod{1716}$	2
$n \equiv 305 \pmod{1716}$	3
$n \equiv 1163 \pmod{1716}$	4
$n \equiv 383 \pmod{1716}$	5
$n \equiv 1241 \pmod{1716}$	6
$n \equiv 461 \pmod{1716}$	7
$n \equiv 1319 \pmod{1716}$	8
$n \equiv 539 \pmod{2574}$	1
$n \equiv 1397 \pmod{2574}$	2
$n \equiv 2255 \pmod{2574}$	3
$n \equiv 617 \pmod{2574}$	4
$n \equiv 1475 \pmod{5148}$	1
$n \equiv 4049 \pmod{5148}$	2
$n \equiv 2333 \pmod{5148}$	3
$n \equiv 4907 \pmod{10296}$	1
$n \equiv 10055 \pmod{10296}$	2
$n \equiv 695 \pmod{3432}$	1
$n \equiv 1553 \pmod{3432}$	2
$n \equiv 2411 \pmod{3432}$	3
$n \equiv 3269 \pmod{3432}$	4
$n \equiv 773 \pmod{4290}$	1
$n \equiv 1631 \pmod{4290}$	2
$n \equiv 2489 \pmod{4290}$	3
$n \equiv 3347 \pmod{4290}$	4
$n \equiv 4205 \pmod{8580}$	1
$n \equiv 8495 \pmod{8580}$	2
$n \equiv 851 \pmod{6006}$	1
$n \equiv 1709 \pmod{6006}$	2
$n \equiv 2567 \pmod{6006}$	3
$n \equiv 3425 \pmod{6006}$	4
$n \equiv 4283 \pmod{12012}$	1
$n \equiv 10289 \pmod{12012}$	2
$n \equiv 5141 \pmod{12012}$	3
$n \equiv 11147 \pmod{12012}$	4
$n \equiv 5999 \pmod{18018}$	1
$n \equiv 12005 \pmod{18018}$	2
$n \equiv 18011 \pmod{18018}$	3
$n \equiv 7 \pmod{130}$	1
$n \equiv 33 \pmod{130}$	2
$n \equiv 59 \pmod{650}$	1
$n \equiv 189 \pmod{650}$	2
$n \equiv 319 \pmod{650}$	3

congruence	p
$n \equiv 449 \pmod{650}$	4
$n \equiv 579 \pmod{650}$	5
$n \equiv 85 \pmod{1170}$	1
$n \equiv 215 \pmod{1170}$	2
$n \equiv 345 \pmod{1170}$	3
$n \equiv 475 \pmod{1170}$	4
$n \equiv 605 \pmod{1170}$	5
$n \equiv 735 \pmod{3510}$	1
$n \equiv 1905 \pmod{3510}$	2
$n \equiv 3075 \pmod{3510}$	3
$n \equiv 865 \pmod{3510}$	4
$n \equiv 2035 \pmod{3510}$	5
$n \equiv 3205 \pmod{3510}$	6
$n \equiv 995 \pmod{3510}$	7
$n \equiv 2165 \pmod{3510}$	8
$n \equiv 3335 \pmod{3510}$	9
$n \equiv 1125 \pmod{5850}$	1
$n \equiv 2295 \pmod{5850}$	2
$n \equiv 3465 \pmod{5850}$	3
$n \equiv 4635 \pmod{5850}$	4
$n \equiv 5805 \pmod{11700}$	1
$n \equiv 11655 \pmod{11700}$	2
$n \equiv 111 \pmod{1300}$	1
$n \equiv 241 \pmod{1300}$	2
$n \equiv 371 \pmod{1300}$	3
$n \equiv 501 \pmod{1300}$	4
$n \equiv 631 \pmod{1300}$	5
$n \equiv 761 \pmod{1300}$	6
$n \equiv 891 \pmod{1300}$	7
$n \equiv 1021 \pmod{2600}$	1
$n \equiv 2321 \pmod{2600}$	2
$n \equiv 1151 \pmod{2600}$	3
$n \equiv 2451 \pmod{2600}$	4
$n \equiv 1281 \pmod{5200}$	1
$n \equiv 3881 \pmod{5200}$	2
$n \equiv 2581 \pmod{7800}$	1
$n \equiv 5181 \pmod{7800}$	2
$n \equiv 7781 \pmod{7800}$	3
$n \equiv 8 \pmod{65}$	1
$n \equiv 21 \pmod{195}$	1
$n \equiv 86 \pmod{585}$	1
$n \equiv 281 \pmod{585}$	2
$n \equiv 476 \pmod{585}$	3
$n \equiv 151 \pmod{585}$	4
$n \equiv 346 \pmod{1755}$	1
$n \equiv 931 \pmod{1755}$	2
$n \equiv 1516 \pmod{1755}$	3
$n \equiv 541 \pmod{1755}$	4
$n \equiv 1126 \pmod{1755}$	5
$n \equiv 1711 \pmod{1755}$	6
$n \equiv 34 \pmod{325}$	1

congruence	p
$n \equiv 99 \pmod{325}$	2
$n \equiv 164 \pmod{975}$	1
$n \equiv 489 \pmod{975}$	2
$n \equiv 814 \pmod{975}$	3
$n \equiv 229 \pmod{975}$	4
$n \equiv 554 \pmod{2925}$	1
$n \equiv 1529 \pmod{2925}$	2
$n \equiv 2504 \pmod{2925}$	3
$n \equiv 879 \pmod{2925}$	4
$n \equiv 1854 \pmod{2925}$	5
$n \equiv 2829 \pmod{8775}$	1
$n \equiv 5754 \pmod{8775}$	2
$n \equiv 8679 \pmod{8775}$	3
$n \equiv 294 \pmod{1625}$	1
$n \equiv 619 \pmod{1625}$	2
$n \equiv 944 \pmod{1625}$	3
$n \equiv 1269 \pmod{1625}$	4
$n \equiv 1594 \pmod{1625}$	5
$n \equiv 47 \pmod{390}$	1
$n \equiv 177 \pmod{390}$	2
$n \equiv 307 \pmod{1560}$	1
$n \equiv 697 \pmod{1560}$	2
$n \equiv 1087 \pmod{1560}$	3
$n \equiv 1477 \pmod{6240}$	1
$n \equiv 3037 \pmod{6240}$	2
$n \equiv 4597 \pmod{6240}$	3
$n \equiv 6157 \pmod{6240}$	4
$n \equiv 60 \pmod{455}$	1
$n \equiv 125 \pmod{455}$	2
$n \equiv 190 \pmod{1365}$	1
$n \equiv 645 \pmod{1365}$	2
$n \equiv 1100 \pmod{1365}$	3
$n \equiv 255 \pmod{1365}$	4
$n \equiv 710 \pmod{4095}$	1
$n \equiv 2075 \pmod{4095}$	2
$n \equiv 3440 \pmod{4095}$	3
$n \equiv 1165 \pmod{4095}$	4
$n \equiv 6625 \pmod{8190}$	1
$n \equiv 3895 \pmod{8190}$	2
$n \equiv 320 \pmod{2275}$	1
$n \equiv 775 \pmod{2275}$	2
$n \equiv 1230 \pmod{2275}$	3
$n \equiv 1685 \pmod{2275}$	4
$n \equiv 2140 \pmod{6825}$	1
$n \equiv 4415 \pmod{6825}$	2
$n \equiv 6690 \pmod{6825}$	3
$n \equiv 385 \pmod{3640}$	1
$n \equiv 1295 \pmod{3640}$	2
$n \equiv 2205 \pmod{3640}$	3
$n \equiv 3115 \pmod{3640}$	4
$n \equiv 905 \pmod{4550}$	1

Table A.3 Covering information for Sierpiński numbers cont.

congruence	p
$n \equiv 1815 \pmod{4550}$	2
$n \equiv 2725 \pmod{9100}$	1
$n \equiv 7275 \pmod{9100}$	2
$n \equiv 3635 \pmod{9100}$	3
$n \equiv 8185 \pmod{9100}$	4
$n \equiv 4545 \pmod{13650}$	1
$n \equiv 9095 \pmod{13650}$	2
$n \equiv 13645 \pmod{13650}$	3
$n \equiv 9 \pmod{91}$	1
$n \equiv 22 \pmod{91}$	2
$n \equiv 35 \pmod{273}$	1
$n \equiv 126 \pmod{273}$	2
$n \equiv 217 \pmod{273}$	3
$n \equiv 139 \pmod{364}$	1
$n \equiv 321 \pmod{364}$	2
$n \equiv 61 \pmod{1092}$	1
$n \equiv 243 \pmod{1092}$	2
$n \equiv 425 \pmod{1092}$	3
$n \equiv 607 \pmod{1092}$	4
$n \equiv 789 \pmod{1092}$	5
$n \equiv 971 \pmod{3276}$	1
$n \equiv 2063 \pmod{3276}$	2
$n \equiv 3155 \pmod{3276}$	3
$n \equiv 74 \pmod{637}$	1
$n \equiv 165 \pmod{637}$	2
$n \equiv 256 \pmod{637}$	3
$n \equiv 347 \pmod{637}$	4
$n \equiv 438 \pmod{637}$	5
$n \equiv 529 \pmod{637}$	6
$n \equiv 620 \pmod{637}$	7
$n \equiv 87 \pmod{728}$	1
$n \equiv 269 \pmod{728}$	2
$n \equiv 451 \pmod{2184}$	1
$n \equiv 1179 \pmod{2184}$	2
$n \equiv 1907 \pmod{2184}$	3
$n \equiv 633 \pmod{2184}$	4
$n \equiv 1361 \pmod{2184}$	5
$n \equiv 2089 \pmod{2184}$	6
$n \equiv 23 \pmod{182}$	1
$n \equiv 49 \pmod{182}$	2
$n \equiv 75 \pmod{182}$	3
$n \equiv 101 \pmod{546}$	1
$n \equiv 283 \pmod{546}$	2
$n \equiv 465 \pmod{1638}$	1
$n \equiv 1011 \pmod{1638}$	2
$n \equiv 1557 \pmod{1638}$	3
$n \equiv 127 \pmod{910}$	1
$n \equiv 309 \pmod{910}$	2
$n \equiv 491 \pmod{910}$	3
$n \equiv 673 \pmod{910}$	4
$n \equiv 855 \pmod{2730}$	1

congruence	p
$n \equiv 1765 \pmod{2730}$	2
$n \equiv 2675 \pmod{2730}$	3
$n \equiv 153 \pmod{1274}$	1
$n \equiv 335 \pmod{1274}$	2
$n \equiv 517 \pmod{1274}$	3
$n \equiv 699 \pmod{2548}$	1
$n \equiv 1973 \pmod{2548}$	2
$n \equiv 881 \pmod{2548}$	3
$n \equiv 2155 \pmod{2548}$	4
$n \equiv 1063 \pmod{2548}$	5
$n \equiv 2337 \pmod{5096}$	1
$n \equiv 4885 \pmod{5096}$	2
$n \equiv 1245 \pmod{3822}$	1
$n \equiv 2519 \pmod{3822}$	2
$n \equiv 3793 \pmod{3822}$	3
$n \equiv 179 \pmod{1456}$	1
$n \equiv 361 \pmod{1456}$	2
$n \equiv 543 \pmod{1456}$	3
$n \equiv 725 \pmod{1456}$	4
$n \equiv 907 \pmod{2912}$	1
$n \equiv 2363 \pmod{2912}$	2
$n \equiv 1089 \pmod{2912}$	3
$n \equiv 2545 \pmod{2912}$	4
$n \equiv 1271 \pmod{4368}$	1
$n \equiv 2727 \pmod{4368}$	2
$n \equiv 4183 \pmod{4368}$	3
$n \equiv 1453 \pmod{5824}$	1
$n \equiv 2909 \pmod{5824}$	2
$n \equiv 4365 \pmod{5824}$	3
$n \equiv 5821 \pmod{5824}$	4
$n \equiv 11 \pmod{143}$	1
$n \equiv 24 \pmod{143}$	2
$n \equiv 37 \pmod{143}$	3
$n \equiv 193 \pmod{286}$	1
$n \equiv 63 \pmod{286}$	2
$n \equiv 219 \pmod{286}$	3
$n \equiv 89 \pmod{429}$	1
$n \equiv 232 \pmod{429}$	2
$n \equiv 375 \pmod{429}$	3
$n \equiv 245 \pmod{572}$	1
$n \equiv 531 \pmod{572}$	2
$n \equiv 115 \pmod{572}$	3
$n \equiv 401 \pmod{572}$	4
$n \equiv 271 \pmod{572}$	5
$n \equiv 557 \pmod{572}$	6
$n \equiv 141 \pmod{715}$	1
$n \equiv 284 \pmod{715}$	2
$n \equiv 427 \pmod{715}$	3
$n \equiv 1285 \pmod{1430}$	1
$n \equiv 713 \pmod{1430}$	2
$n \equiv 12 \pmod{169}$	1

congruence	p
$n \equiv 25 \pmod{169}$	2
$n \equiv 38 \pmod{169}$	3
$n \equiv 51 \pmod{338}$	1
$n \equiv 233 \pmod{338}$	2
$n \equiv 77 \pmod{507}$	1
$n \equiv 753 \pmod{2028}$	1
$n \equiv 1767 \pmod{2028}$	2
$n \equiv 415 \pmod{2028}$	3
$n \equiv 1429 \pmod{2028}$	4
$n \equiv 259 \pmod{676}$	1
$n \equiv 597 \pmod{676}$	2
$n \equiv 103 \pmod{676}$	3
$n \equiv 441 \pmod{676}$	4
$n \equiv 285 \pmod{676}$	5
$n \equiv 623 \pmod{2704}$	1
$n \equiv 1299 \pmod{2704}$	2
$n \equiv 1975 \pmod{2704}$	3
$n \equiv 2651 \pmod{2704}$	4
$n \equiv 129 \pmod{845}$	1
$n \equiv 298 \pmod{845}$	2
$n \equiv 467 \pmod{845}$	3
$n \equiv 1481 \pmod{1690}$	1
$n \equiv 805 \pmod{1690}$	2
$n \equiv 311 \pmod{1014}$	1
$n \equiv 649 \pmod{1014}$	2
$n \equiv 987 \pmod{1014}$	3
$n \equiv 155 \pmod{1183}$	1
$n \equiv 324 \pmod{1183}$	2
$n \equiv 493 \pmod{1183}$	3
$n \equiv 1845 \pmod{2366}$	1
$n \equiv 831 \pmod{2366}$	2
$n \equiv 2183 \pmod{4732}$	1
$n \equiv 4549 \pmod{4732}$	2
$n \equiv 1169 \pmod{4732}$	3
$n \equiv 3535 \pmod{4732}$	4
$n \equiv 337 \pmod{1352}$	1
$n \equiv 675 \pmod{1352}$	2
$n \equiv 1013 \pmod{1352}$	3
$n \equiv 1351 \pmod{1352}$	4

Table A.4 Covering information for Riesel numbers

congruence	p
$n \equiv 2 \pmod 4$	1
$n \equiv 4 \pmod{40}$	1
$n \equiv 24 \pmod{80}$	1
$n \equiv 64 \pmod{160}$	1
$n \equiv 144 \pmod{160}$	2
$n \equiv 8 \pmod{120}$	1
$n \equiv 28 \pmod{240}$	1
$n \equiv 148 \pmod{240}$	2
$n \equiv 48 \pmod{360}$	1
$n \equiv 168 \pmod{360}$	2
$n \equiv 288 \pmod{1080}$	1
$n \equiv 648 \pmod{1080}$	2
$n \equiv 1008 \pmod{1080}$	3
$n \equiv 68 \pmod{480}$	1
$n \equiv 188 \pmod{480}$	2
$n \equiv 308 \pmod{960}$	1
$n \equiv 788 \pmod{960}$	2
$n \equiv 428 \pmod{960}$	3
$n \equiv 908 \pmod{960}$	4
$n \equiv 88 \pmod{720}$	1
$n \equiv 208 \pmod{720}$	2
$n \equiv 328 \pmod{1440}$	1
$n \equiv 1048 \pmod{1440}$	2
$n \equiv 448 \pmod{1440}$	3
$n \equiv 1168 \pmod{1440}$	4
$n \equiv 568 \pmod{2160}$	1
$n \equiv 1288 \pmod{2160}$	2
$n \equiv 2008 \pmod{2160}$	3
$n \equiv 688 \pmod{2160}$	4
$n \equiv 1408 \pmod{2160}$	5
$n \equiv 2128 \pmod{4320}$	1
$n \equiv 4288 \pmod{4320}$	2
$n \equiv 108 \pmod{840}$	1
$n \equiv 228 \pmod{840}$	2
$n \equiv 348 \pmod{840}$	3
$n \equiv 468 \pmod{1680}$	1
$n \equiv 1308 \pmod{1680}$	2
$n \equiv 588 \pmod{1680}$	3
$n \equiv 1428 \pmod{1680}$	4
$n \equiv 708 \pmod{2520}$	1
$n \equiv 1548 \pmod{2520}$	2
$n \equiv 2388 \pmod{2520}$	3
$n \equiv 828 \pmod{2520}$	4
$n \equiv 1668 \pmod{5040}$	1
$n \equiv 4188 \pmod{5040}$	2
$n \equiv 2508 \pmod{5040}$	3
$n \equiv 5028 \pmod{10080}$	1
$n \equiv 10068 \pmod{10080}$	2
$n \equiv 12 \pmod{100}$	1
$n \equiv 32 \pmod{100}$	2
$n \equiv 52 \pmod{200}$	1

congruence	p
$n \equiv 152 \pmod{200}$	2
$n \equiv 72 \pmod{200}$	3
$n \equiv 172 \pmod{200}$	4
$n \equiv 92 \pmod{300}$	1
$n \equiv 192 \pmod{300}$	2
$n \equiv 292 \pmod{300}$	3
$n \equiv 16 \pmod{140}$	1
$n \equiv 36 \pmod{140}$	2
$n \equiv 56 \pmod{280}$	1
$n \equiv 196 \pmod{1120}$	1
$n \equiv 476 \pmod{1120}$	2
$n \equiv 756 \pmod{1120}$	3
$n \equiv 1036 \pmod{1120}$	4
$n \equiv 76 \pmod{420}$	1
$n \equiv 216 \pmod{420}$	2
$n \equiv 356 \pmod{1260}$	1
$n \equiv 776 \pmod{1260}$	2
$n \equiv 1196 \pmod{1260}$	3
$n \equiv 96 \pmod{560}$	1
$n \equiv 236 \pmod{560}$	2
$n \equiv 376 \pmod{560}$	3
$n \equiv 516 \pmod{560}$	4
$n \equiv 116 \pmod{700}$	1
$n \equiv 256 \pmod{700}$	2
$n \equiv 396 \pmod{700}$	3
$n \equiv 536 \pmod{1400}$	1
$n \equiv 1236 \pmod{1400}$	2
$n \equiv 676 \pmod{2100}$	1
$n \equiv 1376 \pmod{2100}$	2
$n \equiv 2076 \pmod{2100}$	3
$n \equiv 136 \pmod{980}$	1
$n \equiv 276 \pmod{980}$	2
$n \equiv 416 \pmod{980}$	3
$n \equiv 556 \pmod{980}$	4
$n \equiv 696 \pmod{980}$	5
$n \equiv 836 \pmod{1960}$	1
$n \equiv 1816 \pmod{1960}$	2
$n \equiv 976 \pmod{1960}$	3
$n \equiv 1956 \pmod{1960}$	4
$n \equiv 0 \pmod{25}$	1
$n \equiv 5 \pmod{25}$	2
$n \equiv 10 \pmod{50}$	1
$n \equiv 35 \pmod{150}$	1
$n \equiv 85 \pmod{450}$	1
$n \equiv 235 \pmod{450}$	2
$n \equiv 385 \pmod{1350}$	1
$n \equiv 835 \pmod{1350}$	2
$n \equiv 1285 \pmod{1350}$	3
$n \equiv 135 \pmod{750}$	1
$n \equiv 285 \pmod{750}$	2
$n \equiv 435 \pmod{750}$	3

congruence	p
$n \equiv 585 \pmod{2250}$	1
$n \equiv 1335 \pmod{2250}$	2
$n \equiv 2085 \pmod{2250}$	3
$n \equiv 735 \pmod{2250}$	4
$n \equiv 1485 \pmod{2250}$	5
$n \equiv 2235 \pmod{2250}$	6
$n \equiv 15 \pmod{75}$	1
$n \equiv 40 \pmod{75}$	2
$n \equiv 65 \pmod{225}$	1
$n \equiv 140 \pmod{225}$	2
$n \equiv 215 \pmod{225}$	3
$n \equiv 20 \pmod{125}$	1
$n \equiv 45 \pmod{125}$	2
$n \equiv 70 \pmod{250}$	1
$n \equiv 195 \pmod{250}$	2
$n \equiv 95 \pmod{375}$	1
$n \equiv 220 \pmod{1125}$	1
$n \equiv 595 \pmod{1125}$	2
$n \equiv 970 \pmod{1125}$	3
$n \equiv 345 \pmod{1875}$	1
$n \equiv 720 \pmod{1875}$	2
$n \equiv 1095 \pmod{1875}$	3
$n \equiv 1470 \pmod{1875}$	4
$n \equiv 1845 \pmod{1875}$	5
$n \equiv 120 \pmod{625}$	1
$n \equiv 245 \pmod{625}$	2
$n \equiv 370 \pmod{625}$	3
$n \equiv 495 \pmod{625}$	4
$n \equiv 620 \pmod{1250}$	1
$n \equiv 1245 \pmod{1250}$	2
$n \equiv 7 \pmod{35}$	1
$n \equiv 49 \pmod{70}$	1
$n \equiv 21 \pmod{105}$	1
$n \equiv 56 \pmod{105}$	2
$n \equiv 91 \pmod{105}$	3
$n \equiv 28 \pmod{175}$	1
$n \equiv 63 \pmod{175}$	2
$n \equiv 98 \pmod{175}$	3
$n \equiv 133 \pmod{350}$	1
$n \equiv 343 \pmod{350}$	2
$n \equiv 0 \pmod{27}$	1
$n \equiv 3 \pmod{81}$	1
$n \equiv 30 \pmod{81}$	2
$n \equiv 57 \pmod{81}$	3
$n \equiv 33 \pmod{108}$	1
$n \equiv 87 \pmod{756}$	1
$n \equiv 195 \pmod{756}$	2
$n \equiv 303 \pmod{2268}$	1
$n \equiv 1059 \pmod{2268}$	2
$n \equiv 1815 \pmod{2268}$	3
$n \equiv 411 \pmod{2268}$	4

Table A.4 Covering information for Riesel numbers cont.

congruence	p
$n \equiv 1167 \pmod{2268}$	5
$n \equiv 1923 \pmod{2268}$	6
$n \equiv 519 \pmod{2268}$	7
$n \equiv 1275 \pmod{2268}$	8
$n \equiv 2031 \pmod{2268}$	9
$n \equiv 627 \pmod{1512}$	1
$n \equiv 1383 \pmod{3024}$	1
$n \equiv 2895 \pmod{3024}$	2
$n \equiv 9 \pmod{135}$	1
$n \equiv 36 \pmod{135}$	2
$n \equiv 63 \pmod{540}$	1
$n \equiv 333 \pmod{540}$	2
$n \equiv 117 \pmod{540}$	3
$n \equiv 387 \pmod{540}$	4
$n \equiv 39 \pmod{162}$	1
$n \equiv 93 \pmod{486}$	1
$n \equiv 255 \pmod{486}$	2
$n \equiv 417 \pmod{486}$	3
$n \equiv 147 \pmod{810}$	1
$n \equiv 309 \pmod{810}$	2
$n \equiv 471 \pmod{810}$	3
$n \equiv 633 \pmod{1620}$	1
$n \equiv 1443 \pmod{1620}$	2
$n \equiv 15 \pmod{216}$	1
$n \equiv 69 \pmod{216}$	2
$n \equiv 123 \pmod{648}$	1
$n \equiv 339 \pmod{648}$	2
$n \equiv 555 \pmod{648}$	3
$n \equiv 177 \pmod{864}$	1
$n \equiv 393 \pmod{864}$	2
$n \equiv 609 \pmod{1728}$	1
$n \equiv 1473 \pmod{1728}$	2
$n \equiv 825 \pmod{1728}$	3
$n \equiv 1689 \pmod{1728}$	4
$n \equiv 99 \pmod{270}$	1
$n \equiv 153 \pmod{270}$	2
$n \equiv 207 \pmod{270}$	3
$n \equiv 261 \pmod{810}$	1
$n \equiv 531 \pmod{810}$	2
$n \equiv 801 \pmod{810}$	3
$n \equiv 21 \pmod{324}$	1
$n \equiv 75 \pmod{324}$	2
$n \equiv 129 \pmod{324}$	3
$n \equiv 183 \pmod{324}$	4
$n \equiv 237 \pmod{648}$	1
$n \equiv 561 \pmod{648}$	2
$n \equiv 291 \pmod{648}$	3
$n \equiv 615 \pmod{648}$	4
$n \equiv 51 \pmod{378}$	1
$n \equiv 159 \pmod{378}$	2
$n \equiv 213 \pmod{378}$	3

congruence	p
$n \equiv 267 \pmod{378}$	4
$n \equiv 321 \pmod{1134}$	1
$n \equiv 699 \pmod{1134}$	2
$n \equiv 1077 \pmod{1134}$	3
$n \equiv 753 \pmod{1890}$	1
$n \equiv 1131 \pmod{1890}$	2
$n \equiv 1509 \pmod{1890}$	3
$n \equiv 1887 \pmod{3780}$	1
$n \equiv 3777 \pmod{3780}$	2
$n \equiv 11 \pmod{33}$	1
$n \equiv 22 \pmod{99}$	1
$n \equiv 55 \pmod{99}$	2
$n \equiv 88 \pmod{297}$	1
$n \equiv 187 \pmod{297}$	2
$n \equiv 583 \pmod{594}$	1
$n \equiv 1 \pmod{55}$	1
$n \equiv 67 \pmod{165}$	1
$n \equiv 122 \pmod{495}$	1
$n \equiv 287 \pmod{495}$	2
$n \equiv 452 \pmod{1485}$	1
$n \equiv 947 \pmod{1485}$	2
$n \equiv 1442 \pmod{1485}$	3
$n \equiv 23 \pmod{275}$	1
$n \equiv 78 \pmod{275}$	2
$n \equiv 133 \pmod{825}$	1
$n \equiv 683 \pmod{825}$	2
$n \equiv 188 \pmod{825}$	3
$n \equiv 463 \pmod{825}$	4
$n \equiv 243 \pmod{1375}$	1
$n \equiv 518 \pmod{1375}$	2
$n \equiv 793 \pmod{1375}$	3
$n \equiv 2443 \pmod{2750}$	1
$n \equiv 1343 \pmod{2750}$	2
$n \equiv 89 \pmod{330}$	1
$n \equiv 199 \pmod{330}$	2
$n \equiv 13 \pmod{66}$	1
$n \equiv 35 \pmod{264}$	1
$n \equiv 101 \pmod{264}$	2
$n \equiv 167 \pmod{792}$	1
$n \equiv 431 \pmod{792}$	2
$n \equiv 695 \pmod{1584}$	1
$n \equiv 1487 \pmod{1584}$	2
$n \equiv 233 \pmod{1320}$	1
$n \equiv 497 \pmod{1320}$	2
$n \equiv 761 \pmod{1320}$	3
$n \equiv 1289 \pmod{1320}$	4
$n \equiv 3 \pmod{77}$	1
$n \equiv 25 \pmod{231}$	1
$n \equiv 179 \pmod{693}$	1
$n \equiv 410 \pmod{693}$	2
$n \equiv 641 \pmod{693}$	3

congruence	p
$n \equiv 113 \pmod{308}$	1
$n \equiv 267 \pmod{308}$	2
$n \equiv 47 \pmod{308}$	3
$n \equiv 201 \pmod{1540}$	1
$n \equiv 509 \pmod{1540}$	2
$n \equiv 817 \pmod{1540}$	3
$n \equiv 1433 \pmod{1540}$	4
$n \equiv 58 \pmod{385}$	1
$n \equiv 212 \pmod{385}$	2
$n \equiv 289 \pmod{385}$	3
$n \equiv 751 \pmod{1155}$	1
$n \equiv 1136 \pmod{1155}$	2
$n \equiv 223 \pmod{462}$	1
$n \equiv 377 \pmod{1386}$	1
$n \equiv 839 \pmod{2772}$	1
$n \equiv 2225 \pmod{2772}$	2
$n \equiv 1301 \pmod{2772}$	3
$n \equiv 2687 \pmod{2772}$	4
$n \equiv 15 \pmod{88}$	1
$n \equiv 37 \pmod{440}$	1
$n \equiv 213 \pmod{440}$	2
$n \equiv 301 \pmod{440}$	3
$n \equiv 389 \pmod{440}$	4
$n \equiv 59 \pmod{528}$	1
$n \equiv 235 \pmod{528}$	2
$n \equiv 323 \pmod{2112}$	1
$n \equiv 851 \pmod{2112}$	2
$n \equiv 1379 \pmod{2112}$	3
$n \equiv 1907 \pmod{2112}$	4
$n \equiv 499 \pmod{2640}$	1
$n \equiv 1027 \pmod{2640}$	2
$n \equiv 2083 \pmod{5280}$	1
$n \equiv 4723 \pmod{5280}$	2
$n \equiv 2611 \pmod{5280}$	3
$n \equiv 5251 \pmod{5280}$	4
$n \equiv 81 \pmod{616}$	1
$n \equiv 169 \pmod{616}$	2
$n \equiv 257 \pmod{616}$	3
$n \equiv 345 \pmod{1232}$	1
$n \equiv 961 \pmod{1232}$	2
$n \equiv 433 \pmod{2464}$	1
$n \equiv 1049 \pmod{2464}$	2
$n \equiv 1665 \pmod{2464}$	3
$n \equiv 2281 \pmod{2464}$	4
$n \equiv 521 \pmod{3080}$	1
$n \equiv 1137 \pmod{3080}$	2
$n \equiv 1753 \pmod{3080}$	3
$n \equiv 2369 \pmod{6160}$	1
$n \equiv 5449 \pmod{6160}$	2
$n \equiv 27 \pmod{110}$	1
$n \equiv 49 \pmod{110}$	2

Table A.4 Covering information for Riesel numbers cont.

congruence	p
$n \equiv 71 \pmod{220}$	1
$n \equiv 181 \pmod{220}$	2
$n \equiv 93 \pmod{550}$	1
$n \equiv 203 \pmod{1100}$	1
$n \equiv 753 \pmod{1100}$	2
$n \equiv 313 \pmod{1100}$	3
$n \equiv 863 \pmod{1100}$	4
$n \equiv 423 \pmod{1100}$	5
$n \equiv 973 \pmod{1100}$	6
$n \equiv 533 \pmod{1100}$	7
$n \equiv 1083 \pmod{2200}$	1
$n \equiv 2183 \pmod{2200}$	2
$n \equiv 6 \pmod{121}$	1
$n \equiv 17 \pmod{242}$	1
$n \equiv 149 \pmod{242}$	2
$n \equiv 160 \pmod{363}$	1
$n \equiv 281 \pmod{363}$	2
$n \equiv 50 \pmod{363}$	3
$n \equiv 292 \pmod{363}$	4
$n \equiv 61 \pmod{484}$	1
$n \equiv 303 \pmod{484}$	2
$n \equiv 193 \pmod{484}$	3
$n \equiv 435 \pmod{484}$	4
$n \equiv 83 \pmod{726}$	1
$n \equiv 325 \pmod{726}$	2
$n \equiv 215 \pmod{726}$	3
$n \equiv 457 \pmod{1452}$	1
$n \equiv 1183 \pmod{1452}$	2
$n \equiv 105 \pmod{968}$	1
$n \equiv 347 \pmod{968}$	2
$n \equiv 589 \pmod{968}$	3
$n \equiv 831 \pmod{968}$	4
$n \equiv 116 \pmod{1089}$	1
$n \equiv 358 \pmod{1089}$	2
$n \equiv 479 \pmod{1089}$	3
$n \equiv 721 \pmod{1089}$	4
$n \equiv 1931 \pmod{2178}$	1
$n \equiv 2173 \pmod{2178}$	2
$n \equiv 7 \pmod{132}$	1
$n \equiv 29 \pmod{132}$	2
$n \equiv 73 \pmod{660}$	1
$n \equiv 337 \pmod{660}$	2
$n \equiv 469 \pmod{660}$	3
$n \equiv 601 \pmod{660}$	4
$n \equiv 227 \pmod{660}$	5
$n \equiv 359 \pmod{1980}$	1
$n \equiv 1019 \pmod{1980}$	2
$n \equiv 1679 \pmod{1980}$	3
$n \equiv 491 \pmod{1980}$	4
$n \equiv 1151 \pmod{1980}$	5
$n \equiv 1811 \pmod{3960}$	1

congruence	p
$n \equiv 3791 \pmod{3960}$	2
$n \equiv 623 \pmod{3300}$	1
$n \equiv 1283 \pmod{3300}$	2
$n \equiv 1943 \pmod{3300}$	3
$n \equiv 2603 \pmod{6600}$	1
$n \equiv 5903 \pmod{6600}$	2
$n \equiv 3263 \pmod{6600}$	3
$n \equiv 6563 \pmod{6600}$	4
$n \equiv 19 \pmod{154}$	1
$n \equiv 41 \pmod{154}$	2
$n \equiv 239 \pmod{770}$	1
$n \equiv 393 \pmod{770}$	2
$n \equiv 547 \pmod{770}$	3
$n \equiv 701 \pmod{2310}$	1
$n \equiv 1471 \pmod{2310}$	2
$n \equiv 107 \pmod{924}$	1
$n \equiv 415 \pmod{924}$	2
$n \equiv 569 \pmod{2772}$	1
$n \equiv 1493 \pmod{2772}$	2
$n \equiv 2417 \pmod{2772}$	3
$n \equiv 877 \pmod{2772}$	4
$n \equiv 1801 \pmod{5544}$	1
$n \equiv 4573 \pmod{5544}$	2
$n \equiv 2725 \pmod{8316}$	1
$n \equiv 5497 \pmod{8316}$	2
$n \equiv 8269 \pmod{8316}$	3
$n \equiv 129 \pmod{1078}$	1
$n \equiv 283 \pmod{1078}$	2
$n \equiv 437 \pmod{1078}$	3
$n \equiv 591 \pmod{2156}$	1
$n \equiv 1669 \pmod{2156}$	2
$n \equiv 745 \pmod{2156}$	3
$n \equiv 1823 \pmod{2156}$	4
$n \equiv 899 \pmod{2156}$	5
$n \equiv 1977 \pmod{4312}$	1
$n \equiv 4133 \pmod{4312}$	2
$n \equiv 2131 \pmod{3234}$	1
$n \equiv 3209 \pmod{3234}$	2
$n \equiv 151 \pmod{1848}$	1
$n \equiv 305 \pmod{1848}$	2
$n \equiv 613 \pmod{1848}$	3
$n \equiv 767 \pmod{1848}$	4
$n \equiv 1075 \pmod{1848}$	5
$n \equiv 1229 \pmod{3696}$	1
$n \equiv 3077 \pmod{3696}$	2
$n \equiv 1537 \pmod{3696}$	3
$n \equiv 3385 \pmod{7392}$	1
$n \equiv 7081 \pmod{7392}$	2
$n \equiv 1691 \pmod{9240}$	1
$n \equiv 3539 \pmod{9240}$	2
$n \equiv 5387 \pmod{9240}$	3

congruence	p
$n \equiv 9083 \pmod{9240}$	4
$n \equiv 9 \pmod{176}$	1
$n \equiv 31 \pmod{176}$	2
$n \equiv 53 \pmod{176}$	3
$n \equiv 75 \pmod{352}$	1
$n \equiv 251 \pmod{352}$	2
$n \equiv 97 \pmod{704}$	1
$n \equiv 273 \pmod{704}$	2
$n \equiv 449 \pmod{704}$	3
$n \equiv 625 \pmod{704}$	4
$n \equiv 119 \pmod{880}$	1
$n \equiv 471 \pmod{880}$	2
$n \equiv 647 \pmod{880}$	3
$n \equiv 823 \pmod{880}$	4
$n \equiv 317 \pmod{1056}$	1
$n \equiv 493 \pmod{1056}$	2
$n \equiv 845 \pmod{1056}$	3
$n \equiv 1021 \pmod{1056}$	4
$n \equiv 163 \pmod{1408}$	1
$n \equiv 339 \pmod{1408}$	2
$n \equiv 515 \pmod{1408}$	3
$n \equiv 691 \pmod{2816}$	1
$n \equiv 2099 \pmod{2816}$	2
$n \equiv 867 \pmod{2816}$	3
$n \equiv 2275 \pmod{2816}$	4
$n \equiv 1043 \pmod{4224}$	1
$n \equiv 3859 \pmod{4224}$	2
$n \equiv 1219 \pmod{5632}$	1
$n \equiv 2627 \pmod{5632}$	2
$n \equiv 4035 \pmod{5632}$	3
$n \equiv 5443 \pmod{11264}$	1
$n \equiv 11075 \pmod{11264}$	2
$n \equiv 2803 \pmod{7040}$	1
$n \equiv 4211 \pmod{7040}$	2
$n \equiv 5619 \pmod{7040}$	3
$n \equiv 7027 \pmod{7040}$	4
$n \equiv 43 \pmod{198}$	1
$n \equiv 65 \pmod{198}$	2
$n \equiv 109 \pmod{396}$	1
$n \equiv 307 \pmod{396}$	2
$n \equiv 131 \pmod{396}$	3
$n \equiv 329 \pmod{396}$	4
$n \equiv 175 \pmod{594}$	1
$n \equiv 373 \pmod{594}$	2
$n \equiv 571 \pmod{594}$	3
$n \equiv 197 \pmod{1188}$	1
$n \equiv 395 \pmod{1188}$	2
$n \equiv 593 \pmod{1188}$	3
$n \equiv 791 \pmod{1188}$	4
$n \equiv 989 \pmod{1188}$	5
$n \equiv 1187 \pmod{1188}$	6