PRODUCTS OF DISTINCT CYCLOTOMIC POLYNOMIALS

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

in

Mathematics

by

Lola Thompson

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 24, 2012

Examining Committee:

Carl Pomerance, Chair

Chantal David

Paul Pollack

Thomas Shemanske

Andrew Yang

Brian Pogue
Dean of Graduate Studies

Abstract

A polynomial is a product of distinct cyclotomic polynomials if and only if it is a divisor over $\mathbb{Z}[x]$ of $x^n - 1$ for some positive integer n. In this thesis, we will examine two natural questions concerning the divisors of $x^n - 1$: "For a given n, how large can the coefficients of divisors of $x^n - 1$ be?" and "How often does $x^n - 1$ have a divisor of every degree between 1 and n?" We consider the latter question when $x^n - 1$ is factored in both $\mathbb{Z}[x]$ and $\mathbb{F}_p[x]$. The primary tools used in our investigation arise from the study of the "anatomy of integers." We also make use of a number of results stemming from Hooley's conditional proof of Artin's Primitive Root Conjecture in our work over $\mathbb{F}_p[x]$.

Acknowledgements

I would like to thank my adviser, Carl Pomerance, for taking me on as a student and for all of the guidance that he has provided over the past three years. I cannot imagine a more ideal mentor for someone with my particular set of mathematical interests, strengths and weaknesses. Carl suggested many of the problems in this thesis, and skillfully guided me through every step of the process. Working with him has made me a more careful and detail-oriented researcher, as well as a stronger speaker and writer. Moreover, he has instilled in me a level of confidence that I previously lacked. I hope that I will be able to pass along the knowledge and skills that Carl has imparted in me to my own students one day.

I would like to thank Paul Pollack, who has been an outstanding roommate, collaborator, pet sitter, mentor, and friend. I have Paul to thank for convincing me to apply to the Ph.D. program at Dartmouth in the first place. Paul's encouragement and generosity in sharing his mathematical wisdom have kept me moving forward at times when I've felt like giving up. I appreciate all of the improvements that came about from his thorough reading of my thesis, and look forward to working with him next year at the University of Georgia.

The faculty at Dartmouth have played a tremendous role in my success as a graduate student. I would especially like to thank Tom Shemanske, Rustam Sadykov and Dana Williams for helping me through the grueling qualifying examination process. I would also like to thank Tom for his informal mentoring over the course of the past five years. He was never afraid to give me his honest opinion, and because of that, I have become a better teacher and colleague.

I am fortunate to have received a number of helpful suggestions from my thesis committee members. In addition to those mentioned above, I am grateful to Tom Shemanske, Andy Yang and Chantal David for their careful attention in reading my work. I would also like to thank Chantal for traveling to Hanover for the defense and for all of the support that she has shown for me.

There have been several mathematicians outside of my thesis committee whose contributions have improved this body of work. First, I would like to thank Pieter Moree for sharing his unpublished manuscripts on Artin's primitive root conjecture and cyclotomic polynomial heights. His encyclopedic treatment of these topics has saved me countless hours of searching through back issues of journals. Secondly, I would like to thank Greg Martin for suggesting the problem posed in Proposition 6.10. Greg independently came up with some of the questions posed in chapter 4 of this thesis several years ago, so I am also grateful to him for deciding not to go through with answering them. Finally, I would like to thank Michael Filaseta, who suggested a number of improvements to the wording in section 2 of the Introduction.

I will forever be grateful to the Ross Mathematics Program for fostering my love of mathematics and, in particular, number theory. The Ross Program gave me the tools and confidence to approach new problems and has been a major influence on my own pedagogical practices. Moreover, the Ross Program introduced me to the question about heights of cyclotomic polynomials that would ultimately form the basis for the topic of this thesis.

Lastly, I would like to thank my parents for being so supportive of my decision to pursue a career in mathematics. I know that they must have been surprised when their daughter (who was earning straight C's in her undergraduate math courses at the time) approached them about spending an extra year in college in order to prepare for applying to mathematics Ph.D. programs. If they had their doubts, they never expressed them in front of me. Throughout graduate school, they've shared in my triumphs and consoled me every time that I've called them in tears. Above all, they never stopped believing in me.

Contents

List of Tables

Chapter 1

Introduction

This thesis assembles the results contained in three of the author's papers on the divisors of the polynomial $x^n - 1$. In this introductory chapter, we examine the history of results on this family of polynomials in order to provide context for our own work in the area. We also give an overview of several of the major techniques that we employ in chapters 2, 4 and 6.

1.1 A brief history of cyclotomic polynomials

The n^{th} cyclotomic polynomial, $\Phi_n(x)$, is the minimal polynomial for $e^{2\pi i/n}$. It follows that $\Phi_n(x)$ is the unique, monic irreducible polynomial in $\mathbb{Z}[x]$ whose roots are the primitive n^{th} roots of unity. Moreover, it is easy to show that $\Phi_n(x)$ has degree $\varphi(n)$, which corresponds (via Galois theory) to the size of the unit group of $(\mathbb{Z}/n\mathbb{Z})^\times$. Cyclotomic polynomials are intrinsic to our study of the divisors of $x^n - 1$. The identity

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

shows that the irreducible divisors of $x^n - 1$ in $\mathbb{Z}[x]$ are precisely the d^{th} cyclotomic polynomials, for values of d dividing n. As a result, every divisor of $x^n - 1$ in $\mathbb{Z}[x]$ is a product of

distinct cyclotomic polynomials. Moreover, every product of distinct cyclotomic polynomials is a divisor of $x^n - 1$ for some positive integer n.

The coefficients of cyclotomic polynomials have been studied for some time. In 1883, Migotti [30] showed that $\Phi_{105}(x)$ is the first cyclotomic polynomial to have coefficients that lie outside the set $\{\pm 1, 0\}$:

$$\begin{aligned}\Phi_{105}(x) = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} \\ & + x^{34} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} \\ & + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1.\end{aligned}$$

The fact that the new coefficient appearing in $\Phi_{105}(x)$ has absolute value 2 led to the natural question, "How do the coefficients grow (in absolute value) as n increases?"

One approach has been to examine the coefficients of $\Phi_n(x)$ for values of n with a certain number of distinct odd prime factors. In the same paper in which Migotti described his observation about the coefficients of $\Phi_{105}(x)$, he also proved that, if $n = pq$ with p and q distinct odd primes, then all of the coefficients of $\Phi_n(x)$ lie in the set $\{\pm 1, 0\}$. In fact, the values of the coefficients of $\Phi_{pq}(x)$ can be described completely explicitly for any pair of primes p and q (see, for example, Theorem 2.3 in [39]). It is interesting to note that the example discovered by Migotti has n as a product of the first three distinct, odd primes. In general, when $n = pqr$ where p, q, r are odd primes such that $p < q < r$, explicit values are not known for the coefficients. There has been greater success with bounding the magnitude of the largest coefficient of $\Phi_{pqr}(x)$, which is called its *height*. The earliest work in this area is due to Bang [3], who proved in 1895 that the height of $\Phi_{pqr}(x)$ is at most $p - 1$. This bound was subsequently improved independently by Beiter [7] and Bloom [9] in 1968, who obtained an upper bound of $(p + 1)/2$ in the special case where q or r is congruent to $\pm 1 \pmod{p}$. Beiter also conjectured [8] that this is the best possible upper bound that holds in general. Subsequent work by Beiter [8], Möller [31] and Bachman [1] goes a long way towards

confirming Beiter's conjecture. There have been a number of recent developments on this subject. In 2003, Bachman [1] provided a second infinite family of examples that support Beiter's conjecture, namely the cyclotomic polynomials $\Phi_{pqr}(x)$ with q or r congruent to $\pm 2 \pmod{p}$. In 2009, Kaplan [22] obtained a periodicity result; he showed that, if $s > q$ is a prime with $s \equiv \pm r \pmod{pq}$, then $A(pqr) = A(pqs)$. In the same paper, he proved a technical lemma that explicitly relates the coefficients of $\Phi_{pqr}(x)$ to those of $\Phi_{pq}(x)$. Gallott and Morree [15] used Kaplan's lemma in order to construct an infinite family of counterexamples to Beiter's conjecture. They showed that $A(pqr) > (p+1)/2$ holds for each $p \geq 11$ and for infinitely many values of q and r. In the same paper, they conjectured that $A(pqr) \leq \frac{2}{3}p$. They showed that there exist triples $p < q < r$ with p arbitrarily large for which $A(pqr) > (\frac{2}{3} - \varepsilon)p$ for $\varepsilon > 0$, which means that the conjectured upper bound is optimal if it is true. In 2010, Bzdega [6] obtained density results on polynomials $\Phi_{pqr}(x)$ with $A(pqr) \leq cp$. In particular, with p fixed, he showed that at least $\frac{25}{27} + O(\frac{1}{p})$ of the polynomials $\Phi_{pqr}(x)$ satisfy the conjectured bound of Gallot and Moree.

Other work has focused on bounding the magnitude of the maximal coefficient of $\Phi_n(x)$ for integers n with an arbitrary but fixed number of prime factors. We will denote this magnitude by $A(n)$. Bateman [4] was the first to obtain a bound for $\Phi_n(x)$ with n having k distinct odd prime factors, where k ranges over all positive integers. He gave a simple argument in 1949 which showed that the height of $\Phi_n(x)$ is at most $n^{2^{k-1}}$. There were a number of improvements on Bateman's result in papers of Erdös [11], Vaughan [40] and Bateman, Pomerance, and Vaughan [5], the last of which gives an upper bound of $n^{\frac{2^{k-1}}{k}-1}$. We remark that this bound is nearly best possible; in the same paper, Bateman, Pomerance and Vaughan show that $A(n) \geq n^{\frac{2^{k-1}}{k}-1}/(5\log n)^{2^{k-1}}$ holds for infinitely many n with exactly k distinct odd prime factors. Moreover, under the assumption of the prime k-tuples conjecture, they show that for each k there exists a constant c_k such that $A(n) \geq c_k n^{\frac{2^{k-1}}{k}-1}$ holds for infinitely many n with exactly k distinct odd prime factors. We can re-state these results without the dependence on k by using the fact that the maximal order of $\omega(n)$ is

$\frac{\log n}{\log\log n}$. This yields an upper bound of $A(n) \leq e^{n^{(\log 2+o(1))/\log\log n}}$ that holds for all positive integers n, as well as a lower bound of $A(n) \geq e^{n^{(\log 2+o(1))/\log\log n}}$ that holds for infinitely many values of n.

Maier shows in [28] and [27] that stronger results can be obtained for "typical" n; that is, for all n except for a set with asymptotic density 0. In particular, he proved that if $\psi(n)$ is any function defined for all positive integers such that $\psi(n)$ tends to infinity as n tends to infinity, then the height of $\Phi_n(x)$ is at most $n^{\psi(n)}$ for almost all n. Moreover, he was able to obtain a complementary lower bound, showing that if $\varepsilon(n)$ is any function that tends to 0 as n tends to infinity, then the height of $\Phi_n(x)$ is at least $n^{\varepsilon(n)}$ for almost all n. Maier's work on the upper bound will be discussed at length in Chapter 2.

1.2 Summary of later chapters

A natural generalization of the work on heights of cyclotomic polynomials is to consider the maximal height over all divisors of $x^n - 1$. Pomerance and Ryan [33] first examined this problem, showing that the maximal height is at most $\exp\{n^{(\log 3+o(1))/\log\log n}\}$. This inequality is "best possible," in the sense that it can be reversed for infinitely many values of n. In 2009, Kaplan [22] provided an explicit formula for the maximal height over all divisors of $x^n - 1$ when $n = p^2q$, where $p < q$ are primes. In the same paper, he obtained upper and lower bounds for the maximal height when $n = pqr$, where $p < q < r$ are primes.

In Chapter 2, we will discuss an analogue of Maier's result for "typical" n that holds in this setting. We show how Maier's approach can be adapted in order to obtain an improvement on Pomerance and Ryan's upper bound that holds for "typical" n. Let $\tau(n)$ denote the number of positive divisors of an integer n. In particular, we prove the following:

Theorem 1.1. *Let $\psi(n)$ be any function defined for all positive integers such that $\psi(n)$ tends to infinity as $n \to \infty$. Then, the inequality*

$$B(n) \leq n^{\tau(n)\psi(n)}$$

holds for almost all n.

Up until now, most of the literature on the divisors of $x^n - 1$ has focused on describing the size of the coefficients. In Chapter 4, we turn our attention to the degrees of the divisors of $x^n - 1$. We ask, "How often does $x^n - 1$ have a divisor of every degree between 1 and n, when factored in $\mathbb{Z}[x]$?" We call an integer n with this property *φ-practical*. An elementary argument shows that the φ-practical numbers are rare; in fact, they have asymptotic density 0 within the set of positive integers, which we demonstrate in Section 4.2. However, it is more difficult to get an accurate estimate for the count of φ-practical numbers in a given interval.

The φ-practical numbers are named for their connection with the *practical numbers*, integers n for which every m with $1 \leq m \leq n$ can be written as a sum of distinct divisors of n. We can see that the φ-practical numbers are analogues of the practical numbers by using the elementary facts that $x^n - 1 = \prod_{d|n} \Phi_d(x)$ and $\deg \Phi_d(x) = \varphi(d)$. The question of whether $x^n - 1$ has a divisor of every degree up to n thus amounts to asking whether every integer between 1 and n can be written as a sum of $\varphi(d)$'s, where the d's come from some subset of divisors of n. Saias [34] obtains the strongest result for the count of practical numbers $n \leq X$. He shows that $\#\{n \leq X : n \text{ is practical}\}$ is of order of magnitude $\frac{X}{\log X}$. The practical numbers and Saias' work concerning their distribution will be described in much greater depth in Chapter 3.

In Sections 4.3 - 4.5, we will demonstrate how portions of Saias' approach can be used in order to handle the φ-practical numbers. In Section 4.3, we give a necessary condition for an integer n to be φ-practical and use it to obtain an upper bound of $C_2 \frac{X}{\log X}$ for the count of φ-practical numbers up to X, where C_2 is a positive constant. In Sections 4.4 and 4.5, we define the *strictly 2-dense integers* and describe their connection to the φ-practical numbers, culminating in a proof that $\frac{X}{\log X}$ is the true order of magnitude for the number of φ-practicals up to X. In other words, we show:

Theorem 1.2. *Let $X \geq 2$. Let $F(X)$ denote the number of φ-practical numbers in $[1, X]$.*

Then, there exist two positive constants, C_1 and C_2, such that

$$C_1 \frac{X}{\log X} \leq F(X) \leq C_2 \frac{X}{\log X}.$$

We conclude chapter 4 with proofs that there are at least a constant multiple of $\frac{X}{\log X}$ integers $n \leq X$ that are practical but not φ-practical, and vice versa.

The remainder of the thesis focuses on variations of the problem posed in Chapter 4. In chapter 5, we describe the relationship between multiplicative orders and the degrees of the irreducible factors of $x^n - 1$ in $\mathbb{F}_p[x]$. We also provide the necessary background on Artin's Primitive Root Conjecture, which describes the density of primes with a fixed integer a as a primitive root. We conclude by discussing how Hooley's conditional proof of Artin's Primitive Root Conjecture, which depends on the validity of the Generalized Riemann Hypothesis, will be used indirectly in chapter 6.

In chapter 6, we consider the factorization of $x^n - 1$ in $\mathbb{F}_p[x]$ and call n *p-practical* if the corresponding polynomial has a divisor of every degree in $\mathbb{F}_p[x]$. We give a conditional proof (on the Generalized Riemann Hypothesis) that, in spite of the extra divisions that occur, these polynomials still do not usually have a divisor of every degree between 1 and n.

We also define the notion of λ-practical numbers: integers that are p-practical for every rational prime p. In Section 6.3, we demonstrate an alternative criterion for an integer n to be λ-practical that involves Carmichael's λ-function, which represents the universal exponent for the multiplicative group of integers modulo n. In contrast with the definition of a λ-practical number, we show that every positive integer n is p-practical for some prime p. Next, we show that there are a constant multiple of $\frac{X}{\log X}$ integers up to X that are λ-practical but not φ-practical; we also show that, for each prime p, there are at least a constant multiple of $\frac{X}{\log X}$ integers in the same range that are p-practical but not λ-practical. These proofs can be found in Sections 6.5 and 6.6, respectively.

This chapter culminates with a discussion of the order of magnitude of the count of p-practicals up to X. Since every φ-practical number is λ-practical (and, hence, p-practical

for all p), our work from Chapter 4 implies that $\#\{n \leq X : n \text{ is } p\text{-practical}\}$ is at least a constant times $\frac{X}{\log X}$. The difficulty lies in finding an upper bound for this count. In Section 6.7, we show:

Theorem 1.3. *Let $X \geq 2$ and $F_p(X) = \#\{n \leq X : n \text{ is } p\text{-practical}\}$. Then, assuming that the Generalized Riemann Hypothesis holds, we have*

$$F_p(X) = O\left(X\sqrt{\frac{\log\log X}{\log X}}\right).$$

1.3 Open problems

The work discussed in the preceding section can be extended in a number of ways. First, it would be natural to try to extend Maier's method for obtaining a lower bound for $A(n)$ in order to prove a complementary result for our $B(n)$ upper bound. Certainly, Maier's lower bound will also be a lower bound for $B(n)$. However, we believe that the lower bound can be improved:

Conjecture 1.4. *Let $\varepsilon(n)$ be any function defined for all positive integers n that tends to 0 as n tends to infinity. Then, for almost all n, we have*

$$B(n) \geq n^{\tau(n)\varepsilon(n)}.$$

Second, there is an obvious parallel between the bounds that we obtain for the size of the set of φ-practical numbers and the bounds given by Chebyshev's inequality:

Theorem 1.5 (Chebyshev, 1852)**.** *Let $\pi(X)$ denote the number of primes in $[1, X]$. There exist positive constants c_1 and c_2 such that*

$$c_1\frac{X}{\log X} \leq \pi(X) \leq c_2\frac{X}{\log X}.$$

Of course, the story does not end with Chebyshev's inequality; nearly half a century

later, the celebrated Prime Number Theorem was proven.

Theorem 1.6 (Hadamard & de la Valée Poussin, 1896)**.** *Let $\pi(X)$ denote the number of primes in $[1, X]$. Then, we have*

$$\lim_{X\to\infty} \frac{\pi(X)}{X/\log X} = 1.$$

It would be interesting to know whether

$$\lim_{X\to\infty} \frac{F(X)}{X/\log X}$$

exists and, if so, what it approaches. Using Sage, we have been able to compute the following table of ratios:

X	$F(X)$	$F(X)/(X/\log X)$
10^2	28	1.289448
10^3	174	1.201949
10^4	1198	1.103399
10^5	9301	1.070817
10^6	74461	1.028717
10^7	635528	1.024350
10^8	5525973	1.017922
10^9	48386047	1.002717

Table 1.1: Ratios for φ-practicals

The table seems to suggest the following conjecture:

Conjecture 1.7. *Let $F(X) = \#\{n \leq X : n \text{ is } \varphi\text{-practical}\}$. Then, $\lim_{X\to\infty} \frac{F(X)}{X/\log X}$ exists and, in particular,*

$$\lim_{X\to\infty} \frac{F(X)}{X/\log X} = 1.$$

Proving this may be exceedingly difficult; for one thing, there does not appear to be an L-function whose zeros correspond to the distribution of φ-practical numbers, so it does not seem likely that any of the analytic approaches for proving the Prime Number Theorem will

be useful in this scenario.

Another natural goal would be to find a sharper estimate for the order of magnitude of $F_p(X)$. For example, when $p = 2$, we can use Sage to compute a table of ratios of $F_2(X)/\frac{X}{\log X}$.

X	$F_2(X)$	$F_2(X)/(X/\log X)$
10^2	34	1.565758
10^3	243	1.678585
10^4	1790	1.648651
10^5	14703	1.692745
10^6	120276	1.661674
10^7	1030279	1.660614

Table 1.2: Ratios for 2-practicals

The table looks similar for other small values of p. For example, when $p = 3, 5$ we have:

X	$F_3(X)$	$F_3(X)/(X/\log X)$
10^2	41	1.888120
10^3	258	1.782201
10^4	1881	1.732465
10^5	15069	1.734883
10^6	127350	1.759405
10^7	1080749	1.741962

Table 1.3: Ratios for 3-practicals

X	$F_5(X)$	$F_5(X)/(X/\log X)$
10^2	46	2.118378
10^3	286	1.975618
10^4	2179	2.006933
10^5	16847	1.939583
10^6	141446	1.954149
10^7	1223577	1.972173

Table 1.4: Ratios for 5-practicals

The fact that the sequence of ratios appears to be bounded suggests the following conjecture:

Conjecture 1.8. *For each rational prime p, $\lim_{X\to\infty} F_p(X)/\frac{X}{\log X}$ exists and is finite.*

At the very least, it would be nice to establish the true order of magnitude of $F_p(X)$. The table seems to suggest that $F_p(X)$ is on the order of $X/\log X$, which given Theorem 1.2 requires establishing:

Conjecture 1.9. *For each rational prime p, we have*

$$F_p(X) \ll \frac{X}{\log X}.$$

Another natural direction would be to examine the factorization of $x^n - 1$ in other polynomial rings; for example, with F an arbitrary number field, we could ask the same questions in $F[x]$. (This problem was suggested to me by Paul Pollack.)

1.4 Notation

For ease of reference, we compile a list of the common notation that will be used throughout the thesis.

Let n always represent a positive integer. We will use d to refer to an arbitrary divisor of n, and $1 = d_1 < d_2 < \cdots$ to refer to the increasing sequence of divisors of n.

We will use a number of arithmetic functions throughout this body of work. Let $\varphi(n)$ refer to the Euler totient function, i.e. $\varphi(n)$ represents the number of positive integers m satisfying $1 \leq m \leq n$ and $\gcd(m, n) = 1$. We will use $\tau(n)$ to designate the number of positive divisors of n. Furthermore, we let $\omega(n)$ denote the number of distinct prime factors of n and $\Omega(n)$ denote the number of prime factors of n counting multiplicity. Finally, let $\lambda(n)$ denote the Carmichael λ-function, which represents the exponent of the multiplicative group of integers modulo n.

Much of our work makes use of the prime factorization of various integers. Let p and q, as well as any subscripted variations, represent primes. Let $P(n)$ denote the largest prime factor of n, with $P(1) = 1$, and let $\Psi(X, Y) = \#\{n \leq X : P(n) \leq Y\}$. We say that an

integer n is Y-*smooth* if $P(n) \leq Y$; thus, $\Psi(X, Y)$ represents the counting function for the Y-smooth integers up to X. Moreover, we will use $P^-(n)$ to denote the smallest prime factor of n, with $P^-(1) = +\infty$.

We will use $\log(x)$ to denote the natural logarithm function, and $\log_k(x)$ to denote the k^{th} iterate of the natural logarithm function.

For the sake of clarity, we will use x to denote the indeterminate in a single variable polynomial and X to denote a positive real number. For example, $f(x) = x^2 + x + 1$ is a polynomial in x, and $F(X) = \#\{n \leq X\}$ counts the number of positive integers up to X.

Throughout this thesis, we will make use of standard notation from analytic number theory, such as the symbols $(o(\cdot), O(\cdot), \gg, \ll, \sim, \asymp)$ for indicating orders of magnitude. We write the Landau "Big Oh" notation, $f = O(g)$, to indicate that there exists a constant $C > 0$ such that $|f| \leq C|g|$. Along the same lines, we use the Vinogradov symbol, $f \ll g$, to indicate that there exists a positive constant C satisfying $|f| \leq C|g|$. The notation $f \asymp g$ indicates that $f \ll g$ and $g \ll f$; in other words, f and g have the same order of magnitude. We write $f \sim g$ if $\lim_{X\to\infty} \frac{f(X)}{g(X)} = 1$. Finally, we write $f = o(g)$ if $\lim_{X\to\infty} \frac{f(X)}{g(X)} = 0$.

Chapter 2

Heights of divisors of $x^n - 1$

In this chapter, we will examine the coefficients of divisors of $x^n - 1$. In particular, we will obtain an upper bound for the largest coefficient (in absolute value) over all divisors of $x^n - 1$.

2.1 Introduction

We define the *height* of a polynomial with integer coefficients to be the largest coefficient in absolute value. We will denote the height of a polynomial f by $H(f)$. Much has been studied about $H(\Phi_n)$, which shall henceforth be denoted $A(n)$. In Section 1.1, we gave a detailed history of the progress in this area. Related to these problems are questions concerning the maximal height over all divisors of $x^n - 1$. It is well-known that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Thus, $x^n - 1$ has $\tau(n)$ distinct monic irreducible divisors, where $\tau(n)$ is the number of divisors of n. Therefore, $x^n - 1$ has $2^{\tau(n)}$ divisors in $\mathbb{Z}[x]$.

Let $B(n) = \max\{H(f) : f(x) \mid x^n - 1, f(x) \in \mathbb{Z}[x]\}$. In particular, $A(n) \leq B(n)$ since $\Phi_n(x)$ divides $x^n - 1$ and $B(n)$ is the maximum height over all divisors of $x^n - 1$. In general, much less is known about $B(n)$ than $A(n)$. In 2005, Pomerance and Ryan [33] proved that

as $n \to \infty$, $\log B(n) \leq n^{(\log 3 + o(1))/\log\log n}$. They also showed that this inequality can be reversed for infinitely many n.

In [27], Maier found an upper bound for $A(n)$ that holds for most n.

Theorem 2.1 (Maier)**.** *Let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ as $n \to \infty$. Then $A(n) \leq n^{\psi(n)}$ for almost all n, i.e., for all n except for a set with asymptotic density 0.*

Maier's upper bound has been shown to be best possible [28]. In this chapter, we consider an upper bound for $B(n)$ that holds for most n.

Theorem 2.2. *Let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ as $n \to \infty$. Then $B(n) \leq n^{\tau(n)\psi(n)}$ for almost all n, i.e., for all n except for a set with asymptotic density 0.*

It is not yet known whether this upper bound for $B(n)$ is best possible.

2.2 Proof strategy for Theorem 2.2

Since $x^n - 1 = \prod_{d|n} \Phi_d(x)$, then $B(n) = H\left(\prod_{d\in\mathcal{D}} \Phi_d(x)\right)$, where $\mathcal{D}$ is a subset of divisors of n for which $\prod_{d\in\mathcal{D}} \Phi_d(x)$ has maximal height over all products of distinct cyclotomic polynomials dividing $x^n - 1$.

In [33], Pomerance and Ryan show that if $f_1, ..., f_k \in \mathbb{Z}[x]$ with $\deg f_1 \leq \cdots \leq \deg f_k$ then
$H(f_1 ... f_k) \leq \prod_{i=1}^{k-1}(1+\deg f_i) \prod_{i=1}^{k} H(f_i)$. Thus, when $n > 1$,

$$B(n) = H\left(\prod_{d\in\mathcal{D}} \Phi_d(x)\right) \leq \prod_{d\in\mathcal{D}} (1+\varphi(d)) \prod_{d\in\mathcal{D}} A(d) \leq n^{\#\mathcal{D}} \prod_{d\in\mathcal{D}} A(d) \leq n^{\tau(n)} \prod_{d|n} A(d). \quad (2.1)$$

Let $A_0(n) := \max_{d|n} A(d)$. Then from (2.1), $B(n) \leq n^{\tau(n)} A_0(n)^{\tau(n)}$, since $A(d) \leq A_0(n)$

for each $d \mid n$. So, if we show that $A_0(n) \leq n^{\psi(n)}$ for almost all n, we will have

$$B(n) \leq n^{\tau(n)} A_0(n)^{\tau(n)} \leq n^{\tau(n)} \cdot n^{\tau(n)\psi(n)} = n^{\tau(n)(1+\psi(n))} \tag{2.2}$$

for almost all n. Since $\psi(n)$ is any function that goes to infinity as n approaches infinity, we will have proved the theorem.

Thus, we have reduced the proof of Theorem 2.2 to the following proposition, which shall be proven in Section 4.

Proposition 2.3. *We have $A_0(n) \leq n^{\psi(n)}$ for almost all n.*

2.3 Key Lemmas

Let $\omega(n)$ be defined as in Section 1. Write the prime factorization of n as $p_1^{e_1} \cdots p_{\omega(n)}^{e_{\omega(n)}}$, where $p_1 > p_2 > \cdots > p_{\omega(n)}$, $e_k \geq 1$ for $1 \leq k \leq \omega(n)$. Thus, we have functions $p_k = p_k(n)$ defined when $k \leq \omega(n)$. If $k > \omega(n)$, we let $p_k(n) = 1$.

To prove our proposition, we will show that for most integers, the size of the prime factors p_k decreases rapidly on a logarithmic scale as k increases.

Lemma 2.4. *Let $2 < \gamma < e$. The set $\{n : \omega(n) \geq \frac{\log\log n}{\log \gamma}\}$ has density 0.*

Proof. Since $2 < \gamma < e$ then $\log \gamma \in (0, 1)$, so $1 < \frac{1}{\log \gamma}$. Now, the normal order of $\omega(n)$ is $\log\log n$ [32, p.111], so for each $\varepsilon > 0$, $\omega(n) < (1+\varepsilon)\log\log n$ must hold, except for a set of n with asymptotic density 0. In particular, since $\varepsilon = \frac{1}{\log \gamma} - 1 > 0$, then $\omega(n) < \frac{1}{\log \gamma} \log\log n$ for almost all n. □

Let $\mu(n)$ be the Möbius function. From [27, Lemma 5], we know that if $2 < \gamma < e$ then there is a constant $c(\gamma) > 0$ such that for each natural number $k <$log log x/log γ,

$$\#\{n \leq x : \mu(n) \neq 0,\ \log p_k > \gamma^{-k} \log x\} \ll x e^{-c(\gamma)k}.$$

The following lemma says that we can remove the restriction that $\mu(n) \neq 0$, i.e., we do not need to assume that n is square-free.

Lemma 2.5. *Let $2 < \gamma < e$. Let $x > 1$. There are positive constants $c_0(\gamma), C_2$ such that for each natural number $k < \log\log x/\log\gamma$,*

$$\#\{n \leq x : \log p_k > \gamma^{-k} \log x\} \leq C_2 x e^{-c_0(\gamma)k}.$$

Proof. We adopt the same strategy as in [27]. The following is a classical result, due to Halberstam and Richert [16, Thm 01]: Let f be a nonnegative real-valued multiplicative function such that for some numbers A and B and for all numbers $y \geq 0$, we have

$$\sum_{p \leq y} f(p) \log p \leq Ay, \qquad \sum_{p} \sum_{\nu \geq 2} \frac{f(p^\nu)}{p^\nu} \log p^\nu \leq B, \tag{2.3}$$

where p runs over primes and ν runs over integers. Then, for all numbers $x > 1$,

$$\sum_{n \leq x} f(n) \leq (A + B + 1) \frac{x}{\log x} \sum_{n \leq x} \frac{f(n)}{n}. \tag{2.4}$$

We apply this theorem with $f(n) = b^{\omega([t,x],n)}$, where $w([t,x],n)$ is the number of distinct prime factors of n in the interval $[t,x]$, with $t = x^{\gamma^{-k}}$, $b > 1$ (b will be specified later). In order to apply the theorem, we need to check that both conditions in (2.3) are satisfied.

As usual, let $\theta(y) = \sum_{p \leq y} \log p$. Since $\theta(y) \leq 2y \log 2 < 2y$ [32, p.108] then

$$\sum_{p \leq y} f(p) \log p \leq 2by$$

for all y. Thus, the first condition is satisfied, with $A = 2b$.

Next, we show that the second condition is satisfied for a suitable number B, namely that the double sum converges. Consider the sum $\sum_p \sum_\nu \frac{\log p^\nu}{p^\nu} b^{\omega([t,y],p^\nu)}$, where p runs over

primes, $\nu \geq 2$. Since ω counts only distinct prime factors, we have $\omega([t,y],p^\nu) \leq 1$. So,

$$\sum_p \sum_{\nu \geq 2} \frac{\log p^\nu}{p^\nu} b^{\omega([t,y],p^\nu)} \leq b \sum_p \left(\frac{2\log p}{p^2} + \frac{3\log p}{p^3} + \cdots \right) = b \sum_p \left(\frac{2}{p^2} + \frac{3}{p^3} + \cdots \right) \log p.$$

It is easy to see that

$$\sum_p \left(\frac{2}{p^2} + \frac{3}{p^3} + \cdots \right) \log p = 2 \sum_p \frac{\log p}{p(p-1)} \tag{2.5}$$

holds, and that the sum in (2.5) is less than 4. Thus, the second condition is satisfied, with $B = 4b$.

Therefore, by (2.4), we have

$$\sum_{n \leq x} b^{\omega([t,x],n)} \leq (2b + 4b + 1) \frac{x}{\log x} \sum_{n \leq x} \frac{f(n)}{n} \leq 7b \frac{x}{\log x} \sum_{n \leq x} \frac{f(n)}{n}. \tag{2.6}$$

Now, $\sum_{n \leq x} \frac{f(n)}{n} \leq \prod_{p \leq x} \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots \right)$, since f is a non-negative multiplicative function (certainly all prime factors of each $n \leq x$ are in this product). Taking the log of both sides, we have

$$\begin{aligned} \log \left(\sum_{n \leq x} \frac{f(n)}{n} \right) &\leq \log \prod_{p \leq x} \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots \right) \\ &= \log \prod_{p \leq x} \left(1 + f(p) \left(\frac{1}{p} + \frac{1}{p^2} + \cdots \right) \right) \\ &= \log \prod_{p \leq x} \left(1 + \frac{f(p)}{p-1} \right) = \sum_{p \leq x} \log \left(1 + \frac{f(p)}{p-1} \right). \end{aligned}$$

Thus,

$$\log \left(\sum_{n \leq x} \frac{f(n)}{n} \right) \leq \sum_{p \leq x} \frac{f(p)}{p-1} = \sum_{p < t} \frac{1}{p-1} + \sum_{t \leq p \leq x} \frac{b}{p-1},$$

since $f(p) = 1$ when $p < t$ and $f(p) = b$ when $t \leq p \leq x$. By Mertens' first theorem [32,

p.92],

$$\sum_{p<t} \frac{1}{p-1} + \sum_{t \le p \le x} \frac{b}{p-1} = \log\log x + (b-1)(\log\log x - \log\log t) + O(b).$$

Let α be the constant associated with $O(b)$. After undoing the logarithms, we are left with

$$\sum_{n \le x} \frac{f(n)}{n} \le C_1 \log x \left(\frac{\log x}{\log t}\right)^{b-1}, \tag{2.7}$$

where $C_1 = e^{\alpha b}$. Inserting (2.7) into (2.6), we have

$$\sum_{n \le x} b^{\omega([t,x],n)} \le 7bC_1 x \left(\frac{\log x}{\log t}\right)^{b-1}. \tag{2.8}$$

Let $C_2 = 7bC_1$. Let

$$N = \#\{n \le x : \omega([t,x],n) > \frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t)\}.$$

Using (2.8), we have

$$Nb^{\frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t)} \le \sum_{n \le x} b^{\omega([t,x],n)} \le C_2 x \left(\frac{\log x}{\log t}\right)^{b-1}.$$

But

$$b^{\frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t)} = e^{(1+\varepsilon)(b-1)(\log\log x - \log\log t)} = \left(\frac{\log x}{\log t}\right)^{(1+\varepsilon)(b-1)}.$$

So

$$N \le \frac{C_2 x (\frac{\log x}{\log t})^{b-1}}{(\frac{\log x}{\log t})^{(1+\varepsilon)(b-1)}} = C_2 x \left(\frac{\log x}{\log t}\right)^{-\varepsilon(b-1)}.$$

In other words,

$$\omega([t,x],n) \le \frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t) \tag{2.9}$$

for all $n \le x$ except for a set of cardinality at most $C_2 x(\frac{\log x}{\log t})^{-\varepsilon(b-1)}$.

Now, fix $\varepsilon > 0$, $b > 1$ such that $\frac{(1+\varepsilon)(b-1)}{\log b} \log \gamma \le 1$. Let $k < \log\log x / \log \gamma$. Recall that $t = x^{\gamma^{-k}}$. Then, if $\log p_k > \gamma^{-k} \log x$, we have

$$\omega([t,x],n) \ge k \ge \frac{(1+\varepsilon)(b-1)}{\log b} k \log \gamma. \tag{2.10}$$

Since $k \log \gamma = \log\log x - \log\log t$, we have $\omega([t,x],n) \ge \frac{(1+\varepsilon)(b-1)}{\log b}(\log\log x - \log\log t)$. But this contradicts (2.9) except for a set of cardinality at most $C_2 x(\frac{\log x}{\log t})^{-\varepsilon(b-1)}$. Thus, the set of $n \le x$ with $\log p_k > \gamma^{-k} \log x$ has a cardinality of at most $C_2 x(\frac{\log x}{\log t})^{-\varepsilon(b-1)}$. Since $t = x^{\gamma^{-k}}$, we have

$$\#\{n \le x : \log p_k > \gamma^{-k} \log x\} \le C_2 x e^{-k\varepsilon(b-1)\log(\gamma)}.$$

Taking $c_0(\gamma) = \varepsilon(b-1)\log(\gamma)$, we obtain the desired result. □

The following lemma says that, except for a sparse set of integers n, $\log p_k$ is small when k is sufficiently large.

Lemma 2.6. *Let $2 < \gamma < e$. Let $\varepsilon > 0$ be arbitrary and let $k_0 = \frac{\log(\varepsilon(1-e^{-c_0(\gamma)})/C_2)}{-c_0(\gamma)}$, where $c_0(\gamma)$ and C_2 are as in Lemma 2.5. Then, for x sufficiently large, the set $\{n \le x : \log p_k > \gamma^{-k} \log x$ for some $k \ge k_0\}$ has cardinality at most $2\varepsilon x$.*

Proof. Fix $\varepsilon > 0$. Let $\mathcal{S} = \{n \le x : \log p_k > \gamma^{-k} \log x$ for some $k \ge k_0\}$ and let $S_k = \{n \le x : \log p_k > \gamma^{-k} \log x\}$. By Lemma 2.5, we have

$$\#\,\mathcal{S} \le \sum_{k=\lceil k_0 \rceil}^{\lfloor \frac{\log\log x}{\log \gamma} \rfloor} \#\,\mathcal{S}_k + \#\{n : \omega(n) > \frac{\log\log x}{\log \gamma}\} \le \sum_{k=\lceil k_0 \rceil}^{\infty} C_2 x e^{-c_0(\gamma)k} + \varepsilon x$$

for sufficiently large x, since $\{n : \omega(n) > \frac{\log\log x}{\log \gamma}\}$ has density 0 by Lemma 2.4. But the sum

on the right is a convergent geometric series, so

$$\#\ \mathcal{S} \leq \frac{C_2 x e^{-c_0(\gamma)k_0}}{1 - e^{-c_0(\gamma)}} + \varepsilon x.$$

Thus, using the definition of k_0,

$$\#\{n \leq x : \log p_k > \gamma^{-k} \log x \text{ for some } k \geq k_0\} \leq 2\varepsilon x.$$

□

2.4 Proof of Proposition 2.2

Proof. Maier shows in [2] that if $\psi(n)$ is any function defined on all positive integers n such that $\psi(n) \to \infty$ as $n \to \infty$ then $A(n) \leq n^{\psi(n)}$ for almost all n. Key to this proof is the fact that

$$\log A(n) \leq C \sum_{k=1}^{\omega(n)} 2^k \log p_k \tag{2.11}$$

for all square-free integers n, where $C > 0$ is a constant and $p_k = p_k(n)$ is as above.

We define the radical of n, denoted $\mathrm{rad}(n)$, to be the largest square-free divisor of n. Since $\Phi_n(x) = \Phi_{\mathrm{rad}(n)}(x^{n/\mathrm{rad}(n)})$, the coefficients of $\Phi_n(x)$ are the same as the coefficients of $\Phi_{\mathrm{rad}(n)}(x)$. Thus, $A(n) = A(\mathrm{rad}(n))$. As a result, we can use (2.11) for any positive integer n, since

$$\log A(n) = \log A(\mathrm{rad}(n)) \leq C \sum_{k=1}^{\omega(n)} 2^k \log p_k.$$

For each d dividing n, let $d = p_{1,d}^{e_{1,d}} p_{2,d}^{e_{2,d}} \cdots p_{\omega(d),d}^{e_{\omega(d),d}}$, where $p_{1,d} > p_{2,d} > \cdots > p_{\omega(d),d}$ and $e_{k,d} \geq 1$ for $1 \leq k \leq \omega(d)$. Also, let $p_{k,d} = 1$ for $k > \omega(d)$. Since $d \mid n$ then the primes dividing d also divide n. Thus, $p_{k,d} \leq p_k$ for all k, so

$$\sum_{k=1}^{\omega(d)} 2^k \log p_{k,d} \leq \sum_{k=1}^{\omega(d)} 2^k \log p_k \leq \sum_{k=1}^{\omega(n)} 2^k \log p_k.$$

Thus, $\log A(d) \leq C \sum_{k=1}^{\omega(n)} 2^k \log p_k$ holds for all n and for all $d \mid n$. Since $\log A_0(n) = \log A(d)$ for some $d \mid n$ we then have $\log A_0(n) \leq C \sum_{k=1}^{\omega(n)} 2^k \log p_k$.

Let $\varepsilon > 0$ be arbitrary and let k_0 be as in Lemma 2.6. Combining the above inequality with Lemma 2.6, we have

$$\log A_0(n) \leq C \sum_{k=1}^{\omega(n)} 2^k \log p_k = C \sum_{k \leq \lfloor k_0 \rfloor} 2^k \log p_k \ + C \sum_{k=\lfloor k_0 \rfloor + 1}^{\omega(n)} 2^k \log p_k \tag{2.12}$$

$$\leq C \sum_{k \leq \lfloor k_0 \rfloor} 2^k \log p_k + C \sum_{k=\lfloor k_0 \rfloor + 1}^{\omega(n)} (2/\gamma)^k \log x \tag{2.13}$$

for all $n \leq x$ except for a set with cardinality $\leq 2\varepsilon x$. Since $2 < \gamma < e$ then $(2/\gamma) < 1$. Hence, $\sum_{k=\lfloor k_0 \rfloor}^{\omega(n)} (2/\gamma)^k$ is part of a convergent geometric series, so it is bounded above by some positive constant L that is independent of n.

Now, if $\sqrt{x} \leq n \leq x$ then $2 \log n > \log x$, so

$$\sum_{k=\lfloor k_0 \rfloor + 1}^{\omega(n)} (2/\gamma)^k \log x \leq 2 \log n \sum_{k=\lfloor k_0 \rfloor + 1}^{\omega(n)} (2/\gamma)^k = 2L \log n.$$

Then, if n is such that (2.13) holds,

$$\begin{aligned} \log A_0(n) &\leq C \sum_{k \leq \lfloor k_0 \rfloor} 2^k \log p_k \ + 2L \log n \\ &\leq 2^{\lfloor k_0 \rfloor} C \sum_{k \leq \lfloor k_0 \rfloor} \log p_k \ + 2L \log n \\ &= 2^{\lfloor k_0 \rfloor} C \log(\prod_{k \leq \lfloor k_0 \rfloor} p_k) + 2L \log n \\ &\leq \log(n^{2^{\lfloor k_0 \rfloor} C}) + \log(n^{2L}). \end{aligned}$$

Thus, $A_0(n) \le n^{2^{\lfloor k_0 \rfloor} C} \cdot n^{2L}$. Then, we have

$$A_0(n) \le n^{2^{\frac{\log(\varepsilon(1-e^{-c_0(\gamma)})/C_2)}{-c_0(\gamma)}}} \cdot n^{2L} \le n^{e^{\frac{\log(\varepsilon(1-e^{-c_0(\gamma)})/C_2)}{-c_0(\gamma)}}} \cdot n^{2L} = n^{(\varepsilon(1-e^{-c_0(\gamma)})/C_2)^{-c_0(\gamma)}} \cdot n^{2L}.$$

As mentioned, this holds for all n with $\sqrt{x} \le n \le x$ and for which (2.13) holds. Therefore, for any $\varepsilon > 0$ there is a constant $C_3 = (\frac{\varepsilon(1-e^{-c_0(\gamma)})}{C_2})^{-c_0(\gamma)} + 2L$ such that for all sufficiently large x, every $n \le x$ satisfies $A_0(n) \le n^{C_3}$, except for at most $2\varepsilon x + \sqrt{x}$ of them. Since $\varepsilon > 0$ is arbitrary, this proves Proposition 2.3, which concludes the proof of our main theorem. $\square$

Chapter 3

Practical numbers and their anatomy

In this chapter, we will describe how ideas from the study of the "anatomy" of integers can be used in order to answer questions about the distribution of practical numbers. We will discuss results of Saias and Tenenbaum in this vein, which will serve as a model for our approach to the problems considered in the chapters that follow.

3.1 Practical numbers: a brief history

A positive integer n is called *practical* if every integer m with $1 \leq m \leq n$ can be written as a sum of distinct divisors of n. Srinivasan coined the term 'practical number' in 1948. He attempted to classify them, remarking that:

> The revelation of the structure of these numbers is bound to open some good research in the theory of numbers... Our table shows that about 25 per cent of the first 200 natural numbers are 'practical.' It is a matter for investigation what percentage of the natural numbers will be 'practical' in the long run.

Srinivasan succeeded in giving a partial classification of the practical numbers, but he did not obtain any results concerning the distribution of practical numbers. In a 1950 paper, Erdős asserted, without proof, that the practical numbers have asymptotic density 0; in Section 4.2, we provide a proof that is likely to be the one that Erdős had in mind. A few years later, in 1954, Stewart gave the full classification of practical numbers that Srinivasan had sought:

Theorem 3.1 (Stewart)**.** *If $n = p_1^{e_1} p_2^{e_2} \cdots {p_j}^{e_j}$, where $p_1 < p_2 < \cdots < p_j$ are primes and $e_i \geq 1$ for $i = 1, \cdots, j$, then n is practical if and only if for every i, $p_i \leq \sigma(p_1^{e_1} p_2^{e_2} \cdots p_{i-1}^{e_{i-1}}) + 1$, where σ is the sum-of-divisors function.*

One can prove this theorem by the same method that we will use to prove Lemma 4.9.

The most recent efforts involving the practical numbers have focused on determining their distribution. Let $PR(X) = \#\{n \leq X : n \text{ is practical}\}$. Determining the true size of $PR(X)$ has been of interest for some time. In 1986, Hausman and Shapiro [19] asserted that there exists a positive constant C_β such that

$$PR(X) \leq C_\beta \frac{X}{(\log X)^\beta}$$

for every fixed $\beta < 2^{-1}(1/\log 2 - 1)^2 = 0.0979$. Their proof contains an error (the error appears in Lemma 3.2 in [19]); however, one can use their argument to show that

$$PR(X) \leq X/(\log X)^{\alpha + o(1)},$$

where $\alpha = 1 - \frac{1+\log\log 2}{\log 2} \approx 0.0860713$. Hausman and Shapiro's result was improved upon by Tenenbaum [38] in the same year, who showed that for $\lambda = 4.20002$ and for $X \geq 16$,

$$\frac{X}{\log X}(\log\log X)^{-\lambda} \ll PR(X) \ll \frac{X}{\log X} \log\log X \log\log\log X.$$

Based on computational data, Margenstern [29] conjectured in 1991 that $PR(X) \sim cX/\log X$, where c is a positive constant. This conjecture was partially proven in 1997 by Saias [34], who showed that there exist two strictly positive constants c_3 and c_4 such that for $X \geq 2$, we have

$$c_3 \frac{X}{\log X} \leq PR(X) \leq c_4 \frac{X}{\log X}. \tag{3.1}$$

Saias obtained these bounds by improving upon techniques that Tenenbaum [38] developed to obtain slightly weaker bounds for $PR(X)$ in an earlier paper. The ideas used by Saias and Tenenbaum come from the study of the "anatomy" of integers. For the remainder of this chapter, we present a summary of their methods, which are central to our own main argument in Chapter 4.

3.2 The anatomy of practical numbers

Let n be a positive integer with $1 = d_1 < d_2 < \cdots < d_{\tau(n)}$ its increasing sequence of divisors. We say that an integer n has Z-dense divisors if the inequality $\frac{d_{i+1}}{d_i} \leq Z$ holds for every index i with $1 \leq i \leq \tau(n)$. The main objective of Saias' paper is to bound the number of integers with Z-dense divisors in the interval $[1, X]$. As it turns out, the integers with 2-dense divisors are all practical numbers; thus, a lower bound for the number of integers with 2-dense divisors in $[1, X]$ will also be a lower bound for the count of practical numbers up to X. Moreover, Saias is able to employ the same overarching method to find upper bounds for the number of integers with Z-dense divisors as well as the count of practical numbers in the interval $[1, X]$.

In both his upper and lower bound arguments, Saias uses a method that was initially developed by Tenenbaum in [37]. Let $\mathcal{H}(X)$ denote a specified set of integers that are all less than or equal to X; for example, we could take $\mathcal{H}(X)$ to represent the set of practical numbers up to X or, if we were to fix a value of Z, we could let $\mathcal{H}(X)$ denote the number

of integers in $[1, X]$ with Z-dense divisors. In order to determine the order of magnitude of the function $H(X) := \#\mathcal{H}(X)$, the idea is to extend $H(X)$ in the following manner:

$$H(X, Y) = \#\{n \in \mathcal{H}(X) : P(n) \leq Y\}.$$

In other words, $H(X, Y)$ counts the number of Y-smooth integers in $\mathcal{H}(X)$. When $Y = X$, then we have $H(X, X) = H(X)$; this is what we mean when we say that $H(X, Y)$ "extends" $H(X)$.

By partitioning the integers counted in $H(X, Y)$ into subsets according to the size of the largest prime factor, it is easy to see that the function $H(X, Y)$ satisfies the following identity:

$$H(X, Y) = 1 + \sum_{p \leq \min(Y,\ h(X))} H(X/p, p) + \text{ Error Term},$$

where the function $h(X)$ depends on how much is swept into the error term. In his arguments for both the practical and Z-dense bounds, Saias takes $h(X)$ to be roughly $\sqrt{X}$, which yields an inconsequential error term relative to the order of magnitude $\frac{X}{\log X}$ (the fact that the error term is inconsequential for the practical numbers follows from Stewart's Theorem). Thus, by omitting the error term, Saias is left with the following identity:

$$H(X, Y) = 1 + \sum_{p \leq \min(Y, \sqrt{X})} H(X/p, p) \text{ for } X \geq 1 \text{ and } Y \geq 1. \tag{3.2}$$

There is an advantage to writing $H(X, Y)$ in this form; namely, the righthand side of the identity lends itself particularly well to induction on the size of the range of permissible values of X. Ignoring the base case momentarily, Saias assumes that a particular upper bound for $H(X, Y)$ holds when $2 \leq Y \leq X \leq 2^k$ (for integer values of $k \geq 2$), and shows that the same bound must hold when $2 \leq Y \leq X \leq 2^{k+1}$. In this manner, he is able to prove that his upper bounds for $H(X, Y)$ hold over the full range of $X, Y \geq 2$.

In order to determine what the bounds for $H(X, Y)$ should be for the base case, Saias

instead examines a "smoothed" version of (3.2), given by the integral

$$H^*(X,Y) = \int_1^{\min(Y,\sqrt{X})} H^*(X/t,t)\frac{dt}{\log t}. \tag{3.3}$$

Let ρ be a continuous function that satisfies the differential equation

$$u\rho'(u) + \rho(u-1) = 0 \tag{3.4}$$

with initial conditions $\rho(u) = 1$ for $u \leq 1$. Saias shows that the function $H^*(X,Y) = X\rho(u-1)/\log X$ satisfies the equation (3.3). The fact that the Dickman ρ-function makes an appearance is not surprising, given that it is often used to estimate the frequency of Y-smooth numbers of a given size. Moreover, it is natural to conjecture that $H(X,Y) \asymp H^*(X,Y)$ and Saias establishes that such an asymptotic relationship holds. However, he is unable to directly estimate the size of $H^*(X,Y)$.

Instead, Saias devises a new function $\overline{H}(X,Y)$ that has the following properties:

(1) $\overline{H}(X,X) \asymp H^*(X,X) = X/\log X$

(2) $\overline{H}(X,Y) \leq 1 + \sum_{p \leq \min(Y,\sqrt{X})} \overline{H}(X/p,p)$

(3) $H(X,Y) \geq \overline{H}(X,Y)$

He notes that the simplest choice for $\overline{H}$ would be to take $\overline{H}(X,Y) = \overline{c}H^*(X,Y)$, where $\overline{c}$ is a small constant. However, because the difference $\pi(X) - \mathrm{Li}(X)$ changes signs as X increases, Saias is able to show that the function

$$\overline{c}H^*(X,Y) - \left(1 + \sum_{p \leq \min(Y,\sqrt{X})} \overline{c}H^*(X/p,p)\right)$$

also changes signs when X and Y are large relative to $\overline{c}$. In particular, when this function

is negative, condition (2) from above is no longer satisfied. Saias makes a few modifications to ensure that condition (2) is satisfied on the full range of permissible values of X and Y, ultimately defining

$$\overline{H}(X,Y) = \overline{c}\frac{X(1+\delta(X))\rho(u(1+\varepsilon(Y))-1)}{\log X},$$

where $\varepsilon(Y)$ is a function that tends to 0 as Y tends to infinity and $\delta(X)$ is a positive function that decreases slowly as X tends to infinity. Note that ε and δ are specific to this context (i.e. they are not arbitrary functions).

In summary, Saias has carefully constructed a function $\overline{H}(X,Y)$ that satisfies

$$\begin{aligned} H(X,Y) &\geq 1 + \sum_{p \leq \min(Y,\sqrt{X})} H(X/p,p) \\ &\geq 1 + \sum_{p \leq \min(Y,\sqrt{X})} \overline{H}(X/p,p) \\ &\geq \overline{H}(X,Y) \end{aligned}$$

and for which $\overline{H}(X,X) \gg \frac{X}{\log X}$. Furthermore, using a process that is nearly identical to the one described above for $\overline{H}$, Saias was able to construct a second function $\widetilde{H}$ that satisfies

$$\begin{aligned} H(X,Y) &\leq 1 + \sum_{p \leq \min(Y,\sqrt{X})} H(X/p,p) \\ &\leq 1 + \sum_{p \leq \min(Y,\sqrt{X})} \widetilde{H}(X/p,p) \\ &\leq \widetilde{H}(X,Y) \end{aligned}$$

and for which $\widetilde{H}(X,X) \ll \frac{X}{\log X}$. Again, it would be most natural to take $\widetilde{H}(X,Y) = \widetilde{c}H^*(X,Y)$, where $\widetilde{c}$ is, in this case, a large constant; however, to account for the sign

changes in $\pi(X) - \mathrm{Li}(X)$ as X increases, Saias instead defines

$$\widetilde{H}(X,Y) = \widetilde{c}\ \frac{X(1+\delta'(X))\rho(u(1+\varepsilon'(Y))-1)}{\log X},$$

where $\varepsilon'(Y)$ and $\delta'(X)$ satisfy the same conditions as $\varepsilon(Y)$ and $\delta(X)$ (respectively). The bulk of his work lies in showing that the functions H, H^*, $\overline{H}$ and $\widetilde{H}$ have the stated properties. We use Saias' methods, as well as several of the results that he produces using these methods, in Section 4.5.

Chapter 4

Polynomials with divisors of every degree

In this chapter, we will begin our study of the degrees of divisors of $x^n - 1$. In particular, we will answer the question "How often does $x^n - 1$ have a divisor of every degree between 1 and n when factored in $\mathbb{Z}[x]$?"

4.1 Introduction and statement of results

Which polynomials with integer coefficients have integral divisors of every degree? The trivial answer is that $f(x) = 0$ is the unique polynomial with this property. However, if we clarify the problem by specifying that we are interested in polynomials $f(x)$ with divisors of every degree up to $\deg f(x)$, then the question becomes more interesting. Certainly, any polynomial that splits completely into linear factors, such as $f(x) = x^n$, satisfies this criterion. However, there are other choices of polynomials that are not as obvious. In this chapter, we examine polynomials of the form $x^n - 1$, where n is a positive integer.

In order to determine the values of n for which $x^n - 1$ has a divisor of every degree up

to n, it will be helpful to use the following identity:

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \tag{4.1}$$

where $\Phi_d(x)$ is the d^{th} cyclotomic polynomial. Since $\deg \Phi_d(x) = \varphi(d)$ and each $\Phi_d(x)$ is irreducible, then the following statements are equivalent:

(1) The polynomial $x^n - 1$ has a divisor of every degree between 1 and n.

(2) Every integer m with $1 \leq m \leq n$ can be written in the form

$$m = \sum_{d \in \mathcal{D}} \varphi(d),$$

where $\mathcal{D}$ is a subset of divisors of n.

We will call such a positive integer n *φ-practical*. The nomenclature stems from the striking similarity between the statement in **(2)** and the definition of a practical number given in chapter 3. In this chapter, we prove the following results on φ-practical numbers:

Theorem 4.1. *The set of φ-practical numbers has asymptotic density* 0.

Theorem 4.2. *Let $F(X) = \#\{n \leq X : n \text{ is } \varphi\text{-practical}\}$. There exist two positive constants c_1 and c_2 such that for $X \geq 2$, we have*

$$c_1 \frac{X}{\log X} \leq F(X) \leq c_2 \frac{X}{\log X}. \tag{4.2}$$

While Theorem 4.2 immediately implies Theorem 4.1, there is a much simpler proof of Theorem 4.1 that we will present in Section 4.2. In order to prove Theorem 4.2, we will rely on several results and tools from the literature on practical numbers discussed in chapter 3. In particular, we will make use of Stewart's Condition (Theorem 3.1) and Saias' methods for producing the bounds for $PR(X)$ given in (3.1).

It is interesting to note that our work on the φ-practical integers allows us to classify a second family of polynomials with divisors of every degree. Namely, $x^n + 1$ has an integral

divisor of every degree up to n if and only if n is odd and φ-practical. This follows from the fact that, when n is even, $x^n + 1$ has no divisor of degree 1. On the other hand, when n is odd, we have $x^n + 1 = -((-x)^n - 1)$, hence $x^n + 1$ has divisors of all of the same degrees as those of $x^n - 1$.

4.2 Proof of Theorem 4.1

Below we present our proof of Theorem 4.1, which we believe is likely to be similar to the argument that Erdős had in mind for the practical numbers.

Proof. From the definitions of the functions $\omega(n), \tau(n), \Omega(n)$, it is clear that $2^{\omega(n)} \leq \tau(n) \leq 2^{\Omega(n)}$. Fix $\varepsilon = 1/1000$. Since $\omega(n)$ and $\Omega(n)$ both have normal order $\log\log n$ (cf.[17, Theorem 431]), then for all n except for a set with asymptotic density 0, we have

$$2^{(1-\varepsilon)\log\log n} \leq \tau(n) \leq 2^{(1+\varepsilon)\log\log n} = (\log n)^{(1+\varepsilon)\log 2} < (\log n)^{0.7}. \tag{4.3}$$

We can factor the polynomial $x^n - 1 = \prod_{d|n} \Phi_d(x)$, where $\Phi_d(x)$ is the d^{th} cyclotomic polynomial. Since each $\Phi_d(x)$ is irreducible, the number of monic divisors of $x^n - 1$ in $\mathbb{Z}[x]$ is $2^{\tau(n)}$, since every divisor is uniquely determined by deciding whether or not to include each $\Phi_d(x)$ with $d \mid n$ in its factorization. Thus, in order for n to be φ-practical, we need $n \leq 2^{\tau(n)}$; otherwise, $x^n - 1$ would not have a divisor of every degree less than or equal to n. Taking the logarithm of both sides of this inequality and combining it with (4.3), we have

$$\log n \leq \tau(n)\log 2 < \tau(n) < (\log n)^{0.7}.$$

But this is impossible, so the numbers n that are φ-practical are in the set with asymptotic density 0 where (4.3) does not hold. □

4.3 Proof of the upper bound of Theorem 4.2

Stewart's Condition (Theorem 3.1) shows the form that every practical number must take. The key to proving this is a recursive argument showing that each practical number M can be used to generate new practical numbers via the following set of conditions:

Lemma 4.3 (Stewart)**.** *If M is a practical number and p is a prime with $(p, M) = 1$, then $M' = p^k M$ is practical (for $k \geq 1$) if and only if $p \leq \sigma(M) + 1$.*

Stewart's Condition would be a simple corollary of Lemma 4.3 if it were not for the following subtlety: while Lemma 4.3 provides a method for building an infinite family of practical numbers, it is not immediately obvious that all practical numbers arise in the prescribed manner. Stewart's Condition confirms our suspicions.

The simple necessary-and-sufficient condition in Lemma 4.3 turns out to be a powerful tool. In addition to being an important component in the proof of Stewart's condition, it is also used in Saias' proofs of the upper and lower bounds for the size of $PR(X)$. Unfortunately, we have not found such a simple statement for the φ-practical numbers. Stewart's Condition implies that each practical number $M' > 1$ can be constructed by multiplying a smaller practical number M by a prime power p^k, where $p > P(m)$. However, the same cannot be said for the φ-practical numbers. For example, $315 = 3^2 \cdot 5 \cdot 7$ is φ-practical, but $45 = 3^2 \cdot 5$ is not, since there are no totient-sum representations for 22 and 23.

A more natural means of classifying the φ-practical numbers would be to use the following criterion: Let $w_1 \leq w_2 \leq \cdots \leq w_k$ be the set of totients of divisors of a positive integer n, rearranged so that they appear in non-decreasing order. Then n is φ-practical if and only if, for each $i < k$, we have

$$w_{i+1} \leq 1 + w_1 + \cdots + w_i.$$

Unfortunately, this criterion for φ-practicality is not particularly useful to us from a theoretical standpoint, since the totients of divisors of n are not monotonic in general. However, it has proven to be quite useful in our computational work and will be discussed in greater

detail in the Appendix.

To get around these problems, we will only give a necessary condition for a number to be φ-practical, which is all that is needed in order to determine the stated upper bound for $F(X)$. In Section 4, we will give a necessary-and-sufficient condition for a squarefree integer to belong to the set of φ-practical numbers, which will be used to obtain the lower bound for $F(X)$ in Section 5.

Definition 4.4. Let $n = p_1^{e_1} \cdots p_k^{e_k}$, where $p_1 < p_2 < \cdots < p_k$ are primes and $e_i \geq 1$ for $1 \leq i \leq k$. Define $m_i = p_1^{e_1} \cdots p_i^{e_i}$ for $i = 0, ..., k-1$. We say that such an integer n is *weakly φ-practical* if the inequality $p_{i+1} \leq m_i + 2$ holds for $i = 0, ..., k-1$.

Lemma 4.5. *Every φ-practical number is weakly φ-practical.*

Proof. Let $n = p_1^{e_1} \cdots p_k^{e_k}$, with $p_1 < p_2 < \cdots < p_k$ and $e_i \geq 1$ for $i \leq 1 \leq k$. Suppose that there exists an integer i for which $p_{i+1} > m_i + 2$. Observe that, if $i = 0$, then $m_0 = 1$. Hence, if $p_{i+1} > m_i + 2$ holds at $i = 0$, we must have $p_1 > 3$. Then, $n > 3$ and $x^n - 1$ has no divisor of degree 2, so n is not φ-practical. Thus, we may assume that $i > 0$. Now, $p_{i+1} > m_i + 2$ implies that $\varphi(p_{i+1}) > m_i + 1$. Moreover, it is always the case that $m_i = \sum_{d|m_i} \varphi(d)$. Hence, if $d \mid n$ and $d \nmid m_i$, then $\varphi(d) > m_i + 1$. In particular, $x^n - 1$ has no divisor of degree $m_i + 1$. Therefore, n cannot be φ-practical. □

The converse to Lemma 4.5 is false. For example, 45 is not φ-practical, but it is weakly φ-practical. We can use Lemma 4.5 in order to obtain the stated upper bound for $F(x)$.

Lemma 4.6. *If n is practical and $p \leq P(n)$, then pn is practical. The same holds for weakly φ-practical numbers.*

Proof. This is immediate from Stewart's condition and from the definition of weakly φ-practical numbers. □

Lemma 4.7. *Every even weakly φ-practical number is practical.*

Proof. Let n be an even weakly φ-practical number with $\omega(n) = k$. Since n is weakly φ-practical, it must be the case that $p_{i+1} \leq m_i + 2$ for all $i < k$. Furthermore, since n is even then $m_i \geq 2$ for $i \geq 1$, hence $m_i + 2 \leq \sigma(m_i) + 1$ holds for all such i. Therefore, each p_{i+1} satisfies the inequality from Lemma 4.3, so n is practical. □

Theorem 4.8. *There exists a positive constant c_2 such that, for $X \geq 2$, we have*

$$F(X) \leq c_2 \frac{X}{\log X}.$$

Proof. If n is a φ-practical number then, by Lemma 4.5, n is weakly φ-practical. Thus, if n is even, Lemma 4.7 implies that n is practical. If n is odd, then $2^\ell n$ is practical for every $\ell \geq 1$, by Lemmas 4.6 and 4.7. Moreover, for each odd integer n in $(0, X]$, there is a unique positive integer ℓ_0 such that $2^{\ell_0} n$ is in the interval $(X, 2X]$. Therefore, we have

$$\begin{aligned} F(X) &= \#\{n \leq X : n \text{ even and } \varphi\text{-practical}\} + \#\{n \leq X : n \text{ odd and } \varphi\text{-practical}\} \\ &\leq \#\{n \leq X : n \text{ is practical}\} + \#\{X < m \leq 2X : m \text{ is practical}\} \\ &= PR(2X). \end{aligned}$$

By (3.1), we have

$$PR(X) \leq c_4 \frac{X}{\log X}.$$

Taking $c_2 = 2c_4$, we obtain $F(X) \leq PR(2X) \leq c_2 \frac{X}{\log X}$. □

4.4 Preliminary lemmas for the lower bound of Theorem 4.2

In order to acquire the stated lower bound for the size of the set of φ-practical numbers, it suffices to find a lower bound for the size of the set of squarefree φ-practicals. Although we were unable to give a necessary-and-sufficient condition that characterizes all φ-practical

numbers, we are able to find such a condition for the squarefree φ-practical numbers. This condition will play a crucial role in Section 5, when we give a proof for the lower bound of $F(x)$. In order to obtain this condition, we will need the following lemma, which is our analogue to Lemma 4.3.

Lemma 4.9. *If M is φ-practical and p is prime with $(p, M) = 1$, then $M' = pM$ is φ-practical if and only if $p \leq M + 2$. Moreover, $M' = p^k M, k \geq 2$ is φ-practical if and only if $p \leq M + 1$.*

Proof. For the first case, we take $M' = pM$. If $p > M + 2$, then Lemma 4.5 implies that M' cannot be φ-practical.

For the other direction, we assume that $p \leq M + 2$ and $M' = pM$. Suppose that we can write an integer n in the form $n = (p - 1)q + r$, with $0 \leq q, r \leq M$. Since $q, r \leq M$ and M is φ-practical, we can write $q = \sum_{d \in \mathcal{D}} \varphi(d), r = \sum_{d' \in \mathcal{D}'} \varphi(d')$, for some subsets $\mathcal{D}, \mathcal{D}'$ of divisors of M. Then

$$n = \sum_{pd \in p\mathcal{D}} \varphi(pd) + \sum_{D \in \mathcal{D}'} \varphi(D)$$

where $p\mathcal{D} = \{pd : d \in \mathcal{D}\}$. There is no overlap between $p\mathcal{D}$ and $\mathcal{D}'$, since the first set only contains divisors of pM that are not divisors of M. So, there exists a polynomial with degree n that divides $x^{pM} - 1$.

Thus, in order to conclude that M' is φ-practical, it remains for us to show that every integer $n \leq M'$ can be written in the form $(p - 1)q + r$, with $0 \leq q, r \leq M$. We will break $[0, M']$ into subintervals of the form $[(p - 1)q, (p - 1)q + M]$. Since $p \leq M + 2$ then $(p-1)q+M \geq (p-1)q+(p-2)$, which is adjacent to $(p-1)(q+1)$. Thus, all of the intervals are overlapping or, at least, contiguous. Moreover, the first subinterval starts at 0 and the last subinterval ends at M'. Thus, M' is φ-practical.

For the second case, we take $M' = p^k M, k \geq 2$. We have seen that $p \leq M + 2$. Now, suppose that $p = M + 2$. Then, from the first case, we know that pM is φ-practical.

However, the smallest irreducible divisor of $x^{M'} - 1$ that has degree larger than pM has degree $\varphi(p^2)$. Since $p = M + 2$, we have

$$\varphi(p^2) = M^2 + 3M + 2 > M^2 + 2M + 1 = pM + 1,$$

so there is no divisor of $x^{M'} - 1$ with degree $pM+1$. Thus, M' is not φ-practical if $p = M+2$.

For the other direction, we assume that $p \leq M + 1$. We will use induction on the power of p, taking the case where $M' = pM$ to be our base case. For our induction hypothesis, we assume that $p^{k-1}M$ is φ-practical. Now, suppose that $n \in [0, p^k M]$. Let q_1 be the largest integer in $[0, M]$ with $\varphi(p^k)q_1 \leq n$. If $q_1 = M$, then

$$n - \varphi(p^k)q_1 = n - \varphi(p^k)M \leq (p^k - \varphi(p^k))M = p^{k-1}M.$$

By our induction hypothesis, $p^{k-1}M$ is φ-practical, so we have

$$n - \varphi(p^k)M = \sum_{d \in \mathcal{D}} \varphi(d)$$

where $\mathcal{D}$ is a subset of divisors of $p^{k-1}M$. Thus, we can write

$$n = \sum_{d \in \mathcal{D}} \varphi(d) + \sum_{d | M} \varphi(p^k d).$$

Therefore, when $q_1 = M$, we see that n is φ-practical. If $q_1 < M$ then, using the assumption that $p \leq M + 1$, we have

$$n - \varphi(p^k)q_1 < \varphi(p^k)(q_1 + 1) - \varphi(p^k)q_1 = \varphi(p^k) = p^{k-1}(p - 1) \leq p^{k-1}M.$$

Once again, we see that our induction hypothesis implies that n is φ-practical. □

Recall the definition of weakly φ-practical from Definition 4.4.

Corollary 4.10. *A squarefree integer n is φ-practical if and only if it is weakly φ-practical.*

Proof. Let $n = p_1 \cdots p_k$, with $p_1 < p_2 < \cdots < p_k$, and suppose that n is weakly φ-practical. We proceed by induction on the number of prime factors of n. For our base case, we observe that $n = 1$ is both weakly φ-practical and φ-practical. Suppose that all squarefree integers n with at most $k-1$ prime factors that are weakly φ-practical are, in fact, φ-practical. Hence, since $\frac{n}{p_k}$ is weakly φ-practical, it is also φ-practical, according to our induction hypothesis. But then $n = p_k \cdot \frac{n}{p_k}$ with $\frac{n}{p_k}$ φ-practical, and $p_k \leq \frac{n}{p_k} + 2$, since n is weakly φ-practical. Therefore, by Lemma 4.9, n is φ-practical. The other direction of the proof is an immediate consequence of Lemma 4.5. □

4.5 Proof of the lower bound of Theorem 4.2

Throughout the remainder of this chapter, we will use the following notation. Let

$$F'(X) = \#\{n \leq X : n \text{ is } \varphi\text{-practical and squarefree}\}.$$

Let $1 = d_1(n) < d_2(n) < \cdots < d_{\tau(n)}(n) = n$ denote the increasing sequence of divisors of n. Let $p_1 < p_2 < \cdots < p_{\omega(n)}$ be the increasing sequence of prime factors of n. For integers n, we define

$$T(n) = \max_{1 \leq i < \tau(n)} \frac{d_{i+1}(n)}{d_i(n)}.$$

Let

$$D(X, Y, Z) = \#\{1 \leq n \leq X : T(n) \leq Z, P(n) \leq Y \text{ and } n \text{ is squarefree}\},$$

and let

$$D(X) = D(X, X, 2).$$

Definition 4.11. An integer n is called *Z-dense* if n is squarefree and $T(n) \leq Z$.

Note: This is not the way that Saias defines 2-dense integers. His definition does not

include the stipulation that n is squarefree. For the purposes of this chapter, we will only need to consider squarefree integers. The results of Saias that we cite below are valid for squarefree n.

Using the notation defined above, we see that $D(X, X, Z)$ counts the number of Z-dense integers up to X. Saias notes that the set of 2-dense integers is properly contained within the set of squarefree practical numbers. As a result, if $PR'(X)$ denotes the number of squarefree practical numbers up to X, then a lower bound for $D(X)$ will also be a lower bound for $PR'(X)$. The bulk of Saias' work is, therefore, in obtaining a lower bound for $D(X, Y, Z)$, where $2 \leq Z \leq Y \leq X$. In the particular case when $X = Y$ and $Z = 2$, he obtains the following inequalities, the first of which immediately yields his stated lower bound for $PR(X)$:

Lemma 4.12 (Saias)**.** *There exist positive constants κ_1 and κ_2 such that*

$$\kappa_1 \frac{X}{\log X} \leq D(X) \leq \kappa_2 \frac{X}{\log X}$$

for all $X \geq 2$.

Unfortunately, the same relationship does not exist between $F'(X)$ and $D(X)$. For example, 66 is 2-dense but not φ-practical. In order to get around this problem, we introduce the following modified definition of 2-dense integers:

Definition 4.13. A positive integer n is *strictly 2-dense* if n is squarefree, if $\frac{d_{i+1}}{d_i} < 2$ holds for all i satisfying $1 < i < \tau(n) - 1$, and if $\frac{d_2}{d_1} = 2 = \frac{d_{\tau(n)}}{d_{\tau(n)-1}}$. Note that this forces n to be even.

Although this modification is subtle, it is sufficient for removing the non-φ-practical 2-dense integers from our consideration.

Lemma 4.14. *Every strictly 2-dense number is φ-practical.*

Proof. Write $n = p_1 p_2 \cdots p_k$, where $2 = p_1 < p_2 < \cdots < p_k$. If $k = 1$, then the only strictly 2-dense integer with exactly 1 prime factor is $n = 2$, which is also φ-practical. Assume

that $k > 1$ and n is not φ-practical. Then, as n is squarefree, Corollary 4.10 implies that n is not weakly φ-practical either. As a result, the inequality from the definition of weakly φ-practical numbers must fail for some prime p_j dividing n, with $j > 1$. Let $n_j = \prod_{i<j} p_i$, so $p_j > n_j + 2$. Now, the largest proper divisor of n_j is $\frac{n_j}{2}$. Moreover, there are no divisors of n between $\frac{n_j}{2}$ and n_j, since all of the other prime factors of n are greater than or equal to p_j. Therefore, there exist divisors d_i, d_{i+1} of n with $\frac{d_{i+1}}{d_i} \geq 2$, namely $d_i = \frac{n_j}{2}$ and $d_{i+1} = n_j$. Since $j > 1$, then $d_{i+1} = n_j > 2 = d_2$, so $i > 1$. On the other hand, since $n_j < p_j$, we must have $i < \tau(n) - 1$. Thus, we have shown that there exists an index i with $1 < i < \tau(n) - 1$ such that $\frac{d_{i+1}}{d_i} \geq 2$, so n is not strictly 2-dense. □

Let

$$D'(X) = \#\{1 \leq n \leq X : n \text{ is strictly 2-dense}\}.$$

From Lemma 4.14, a lower bound for $D'(X)$ will also serve as a lower bound for $F'(X)$. One might wonder why we have only defined $D'(X)$ in terms of a single parameter, while Saias' function $D(X)$ is initially defined in terms of both X and Y. This departure stems from a difference in our approaches. Saias' proofs for $D(X)$ relied on a number of iterative arguments that restricted the size of the largest prime factor of n, but our proofs for $D'(X)$ will not require any similar restrictions.

In his proof of the lower bound for $D(X, Y)$, Saias relies heavily on the following condition for 2-dense numbers:

Lemma 4.15 (Tenenbaum)**.** *For every integer $n \geq 1$, $T(n) \leq 2$ if and only if*

$$T(n/P(n)) \leq 2$$

and

$$P(n) \leq \sqrt{2n}.$$

The proof of Saias relied heavily on Lemma 4.15, while our proof will rely heavily on an

analogue of Lemma 4.15 for strictly 2-dense integers, which we will give below. Although the statements of these lemmas are quite similar, their proofs differ substantially. The proof of Lemma 4.15 relies on a structure theorem of Tenenbaum [38, Lemma 2.2] that describes all Z-dense numbers in terms of their prime factorization, while our approach will not make use of any heavy machinery. We will prove our version of Lemma 4.15 in three parts.

Lemma 4.16. *For every squarefree integer $n > 1$, n is strictly 2-dense if $n/P(n)$ is strictly 2-dense and $P(n) < \sqrt{n}$.*

Proof. Assume that n is squarefree, $m = n/P(n)$ is strictly 2-dense, and $P(n) < \sqrt{n}$. In other words we are assuming that $P(n)^2 < n$, so $P(n) < \frac{n}{P(n)} = m$. Suppose that the divisors of m are $1 = d_1 < d_2 < \cdots < d_k = m$. Let $P(n) = p$. Then $p = pd_1 < pd_2 < \cdots < pd_k = pm$, along with the divisors of m, form the divisors of pm. Now, since m is strictly 2-dense, it follows that m is even, hence n is even as well. As a result, we have

$$\frac{d_2}{d_1} = 2 = \frac{pd_k}{pd_{k-1}}.$$

Thus, the only ratios that may pose an obstruction to mp being strictly 2-dense are $\frac{d_k}{d_{k-1}}$ and $\frac{pd_2}{pd_1}$. In order to show that these ratios do not cause a problem, we will show that there exist divisors d_i, d_j of m with $pd_i \in (\frac{m}{2}, m)$ and $d_j \in (p, 2p)$. The general principle behind the argument is that, if m is strictly 2-dense and X is a real number with $1 < X < m/2$, then m has a divisor in the interval $(X, 2X)$, since otherwise we would have two consecutive divisors d_i, d_{i+1} with $1 < i < \tau(n) - 1$ and $d_i \leq X$, $d_{i+1} \geq 2X$, i.e. $\frac{d_{i+1}}{d_i} \geq 2$. There are three cases to consider:

Case 1: If $p > \frac{m}{2}$ then, since $p < m$, we have $p < m < 2p$. Moreover, since $\frac{m}{2} < p < m$, we see that both conditions are satisfied; that is, we can let $d_i = 1$ and $d_j = m$.

Case 2: If $\frac{m}{4} < p < \frac{m}{2}$, then $p < \frac{m}{2} < 2p < m$. Hence, we have $p < \frac{m}{2} = d_{k-1} < 2p$ and $\frac{m}{2} < 2p = pd_2 < m$, so both conditions are met.

Case 3: If $p < \frac{m}{4}$, consider the interval $(p, 2p)$. Since $p < \frac{m}{4}$, then $2p < \frac{m}{2} = d_{k-1}$,

hence the existence of a divisor d_j of m with $d_j \in (p, 2p)$ follows from the fact that m is strictly 2-dense. Furthermore, since m is strictly 2-dense, there exists a divisor d_i of m in the interval $(\frac{m}{2p}, \frac{m}{p})$. Therefore, $pd_i \in (\frac{m}{2}, m)$. □

Lemma 4.17. *If a squarefree integer $m \geq 6$ satisfies Definition 4.13 for all ratios of divisors $\frac{d_{i+1}}{d_i}$ up to $d_{i+1} = P(m)$, then m is strictly 2-dense.*

Proof. We proceed by induction on the number of distinct prime factors of m. We remark that there is no case where there is one distinct prime factor, since $m \geq 6$ and, in order for m to be strictly 2-dense, its smallest prime factor must be 2. For our base case, we observe that if m has 2 distinct prime factors, then the only integer m for which Definition 4.13 holds for all divisors up to $P(m)$ is 6, which is strictly 2-dense. For our induction hypothesis, we suppose that if m has at most $\ell - 1$ distinct prime factors and $\frac{d_{i+1}}{d_i} < 2$ holds for all pairs of consecutive divisors (d_i, d_{i+1}) up to $d_{i+1} = p_{\ell-1}$, then m is strictly 2-dense. Now, consider an integer m with ℓ distinct prime factors, i.e., $m = p_1 \cdots p_\ell$ with $p_1 < \cdots < p_\ell$, and suppose that the strictly 2-dense definition holds for all consecutive pairs of divisors (d_i, d_{i+1}) up to $d_{i+1} = p_\ell$. If $p_\ell > \frac{m}{p_\ell}$, then there is no divisor of m between $\frac{m}{2p_\ell}$ and $\frac{m}{p_\ell}$. This contradicts our assumption that all pairs of consecutive divisors (d_i, d_{i+1}) up to $d_{i+1} = p_\ell$ satisfy $\frac{d_{i+1}}{d_i} < 2$. Thus, it must be the case that $p_\ell < \frac{m}{p_\ell}$, i.e., $p_\ell < \sqrt{m}$. Moreover, since $P(\frac{m}{p_\ell}) = p_{\ell-1} < p_\ell$, then our induction hypothesis implies that $\frac{m}{p_\ell}$ is strictly 2-dense. Therefore, m is strictly 2-dense by Lemma 4.16. □

Lemma 4.18. *For every squarefree integer $n > 6$, n is strictly 2-dense if and only if $n/P(n)$ is strictly 2-dense and $P(n) < \sqrt{n}$.*

Proof. Let n be a squarefree integer larger than 6, let $m = n/P(n)$, and let $p = P(n)$. Assume that n is strictly 2-dense. Then, n must be even, hence m is even. First, we assume that $p > m$. Then, we have $\frac{m}{2} < m < p$ as consecutive divisors of n. Since $n > 6$ then $m = \frac{n}{p} > \frac{6}{3} = 2$, hence $\frac{m}{2} > 1$. Therefore, there exists some integer $1 < i < \tau(n) - 1$ for which $d_i = \frac{m}{2}$, $d_{i+1} = m$ and $d_{i+2} = p$. Clearly, $\frac{d_{i+1}}{d_i} \geq 2$, so n cannot be strictly 2-dense.

Secondly, continuing with our assumption that n is strictly 2-dense, we suppose that m is not. Then, there is some pair of divisors d_i, d_{i+1} of m, with $1 < i < k-1$, for which $\frac{d_{i+1}}{d_i} \geq 2$. Without loss of generality, we may assume that d_i, d_{i+1} is the smallest pair with this property. Now, in order for n to be strictly 2-dense, it must be the case that a multiple of p falls between d_i and d_{i+1}, since p is the smallest divisor of n that is not also a divisor of m. However, since p is the largest prime divisor of n, then $P(m) < p$, so the strictly 2-dense definition holds for all divisors of m up to $P(m)$. But, if the strictly 2-dense definition holds for all divisors of m up to $P(m)$ then, by Lemma 4.17, m must be strictly 2-dense. However, this contradicts our prior assumption that m is not strictly 2-dense. Therefore, if m is not strictly 2-dense then n cannot be strictly 2-dense.

The second direction of the proof follows immediately from Lemma 4.16. □

In order to obtain a lower bound for $D'(X)$, we will use Lemmas 4.15 and 4.18 to show that a positive proportion of 2-dense integers are strictly 2-dense. Thus, Saias' lower bound for $D(X)$ will also serve as a lower bound for $D'(X)$. Before we commence with the proof, we will pause to discuss a technique from the study of the anatomy of integers that will be useful in this context. For the remainder of this section, we will use the following notation. Let $u = \frac{\log X}{\log Y}$. Let $\rho(t)$ be the Dickman function defined by (3.4). As in [34], we will define

$$H(X,Y) = \begin{cases} \frac{X \log 2}{\log X}(1 - \frac{1}{\log_2(\log X/\log 2)})\rho(u(1-\frac{1}{\sqrt{\log Y}})-1) & (0 < u < 3(\log X)^{1/3}), \\ \Psi(X,Y) & (u \geq 3(\log X)^{1/3}). \end{cases}$$

Using the methods outlined in Section 3.2, Saias constructs $H(X,Y)$ to serve as a more tractable model for $D(X,Y)$. After much difficult work, he shows that

$$D(X) \asymp H(X,X) \asymp \frac{X}{\log X}.$$

In addition, he proves that $H(X,Y)$ satisfies the following Buchstab-type inequality:

Lemma 4.19 (Saias)**.** *For $X \geq 2^{16}, Y \geq 2$ and $0 < u < 3(\log X)^{1/3}$, we have*

$$H(X,Y) \geq 1 + \sum_{p \leq \min(Y, \sqrt{2X}\ell(X))} H(X/p, p),$$

where $\ell(X) = \exp\{\frac{\log X}{(\log_2 X)(\log_3 X)^3}\}$.

In other words, $H(X,Y)$ was constructed so that it has roughly the same order of magnitude as $D(X,Y)$ and, like $D(X,Y)$, it can be expressed recursively using a Buchstab inequality. In fact, Saias was able to demonstrate a more explicit relationship between these two functions, which will be useful in our lower bound argument for $D'(X)$:

Lemma 4.20 (Saias)**.** *There exists a constant $c \geq 1$ such that, under the conditions $X \geq 2$ and $Y \geq 2$, we have*

$$D(X,Y) \leq cH(X,Y).$$

Now that we have some information about the behavior of the function $H(X,Y)$ and its relationship with $D(X,Y)$, we have all of the ingredients necessary to prove our lower bound for $D'(X)$.

Theorem 4.21. *For $X \geq 2$, we have*

$$D'(X) \gg \frac{X}{\log X}.$$

Proof. We will show that a positive proportion of 2-dense integers are strictly 2-dense, except for some possible obstructions at small primes. We will then use a counting argument to deal with these small obstructions. We begin by counting integers $n \leq X$ that are 2-dense but not strictly 2-dense. Let $n = mpj$, where m is a 2-dense integer, p is a prime satisfying $m < p < 2m$, and j is an integer that has the following properties: $j \leq X/mp$, $P^-(j) > p$ and the prime factors of j satisfy the conditions necessary for mpj to be 2-dense. Since we have specified that $m < p < 2m$ then, by Lemma 4.15, mpj is 2-dense. However, we know from Lemma 4.18 that mpj will not be strictly 2-dense for values of p in this range. Thus,

the integers n that we have constructed are all 2-dense but not strictly 2-dense. By varying the sizes of m and j, as well as our choice of the prime p, we can construct, in this manner, all integers that are 2-dense but not strictly 2-dense.

Now, let $C > 16$ be an integer that is chosen to be large relative to the size of the constant κ_1 from Lemma 4.12. For each integer $k > C$, consider those 2-dense numbers $m \in (2^{k-1}, 2^k]$. Since $m < p < 2m$, we must have $p \in (2^{k-1}, 2^{k+1})$. We will say that n has an *obstruction at* k if m and p land within these intervals, i.e., if p is a prime in our construction that prevents n from being strictly 2-dense. Thus, for values of k in this range, the number of 2-dense integers that are not strictly 2-dense is at most

$$\sum_{k>C} \sum_{\substack{m\in(2^{k-1},2^k)\\ m \text{ 2-dense}}} \sum_{\substack{p\in(2^{k-1},2^{k+1})\\ p \text{ prime}\\ m<p<2m}} \sum_{\substack{j\le X/mp\\ mpj \text{ 2-dense}\\ P^-(j)>p}} 1. \tag{4.4}$$

Observe that, when $j = 1$, we are counting

$$\#\{n \le X : n = mp, m < p < 2m, m \text{ is 2-dense}\}. \tag{4.5}$$

The conditions that $m \le X/p$ and $m < p$ together imply that $m < X/m$, i.e., $m < \sqrt{X}$. Similarly, the conditions on p force us to have $p < \sqrt{2X}$. Thus, the quantity counted in (4.5) is at most

$$1 + \sum_{p<\sqrt{2X}} \#\{m \le \sqrt{X} : m \text{ is 2-dense}\}. \tag{4.6}$$

From Lemma 4.12, we have

$$\#\{m \le \sqrt{X} : m \text{ is 2-dense}\} = D(\sqrt{X}) \ll \frac{\sqrt{X}}{\log \sqrt{X}} \ll \frac{\sqrt{X}}{\log X}. \tag{4.7}$$

Moreover, the number of terms in the summation is at most $\pi(\sqrt{2X})$. By Chebyshev's

Inequality (cf. [32, Theorem 3.5]),

$$\pi(\sqrt{2X}) \ll \frac{\sqrt{2X}}{\log\sqrt{2X}} \ll \frac{\sqrt{X}}{\log X}.$$

Therefore, the quantity counted in (4.6) is bounded above by a constant times

$$\frac{\sqrt{X}}{\log X} \cdot \frac{\sqrt{X}}{\log X} = \frac{X}{\log^2 X},$$

which is negligible compared with the magnitude of $D(X)$ given in Lemma 4.12.

Assume hereafter that $j > 1$ and, for now, let k be fixed. Our first order of business will be to show that we can take $m < \exp\{C\sqrt{\log X}\}$, which we will now demonstrate. Instead of estimating the full sum in j, we could ignore the stipulation that mpj is 2-dense and use a cruder estimate for

$$\sum_{\substack{j \le X/mp \\ mpj \text{ squarefree} \\ P^-(j) > p}} 1.$$

Since $X/mp > p$, we can use Brun's Sieve (cf. [18, Theorem 2.2]) to show that

$$\#\{j \le X/mp : q \mid j, q \text{ prime } \Rightarrow q > p\} \ll \frac{X}{mp} \prod_{q \le p} \left(1 - \frac{1}{q}\right).$$

Moreover, since $2^{k-1} < p \le X$, we can apply Mertens' Theorem (cf. [32, Theorem 3.15]), which allows us to obtain

$$\prod_{q \le 2^{k-1}} \left(1 - \frac{1}{q}\right) \ll \frac{1}{\log 2^{k-1}} \ll \frac{1}{k}.$$

Thus, we have the following crude estimate for the sum in j:

$$\frac{X}{mp} \prod_{q \le 2^{k-1}} \left(1 - \frac{1}{q}\right) \ll \frac{X}{mpk}.$$

Using our crude estimate in (4.4) yields

$$\sum_{\substack{m\in(2^{k-1},2^k)\\ m \text{ 2-dense}}} \sum_{\substack{p\in(2^{k-1},2^{k+1})\\ p \text{ prime}}} \sum_{\substack{j\le X/mp\\ mpj \text{ squarefree}\\ P^-(j)>p}} 1 \ll \sum_{\substack{m\in(2^{k-1},2^k)\\ m \text{ 2-dense}}} \frac{x}{mk} \sum_{\substack{p\in(2^{k-1},2^{k+1})\\ p \text{ prime}}} \frac{1}{p}.$$

Now, the largest term in the sum in p is at most $\frac{1}{2^{k-1}}$, and the number of terms in this sum is certainly less than $\pi(2^{k+1})$. Hence, by Chebyshev's Inequality (cf. [32, Theorem 3.5]), we have

$$\sum_{\substack{p\in(2^{k-1},2^{k+1})\\ p \text{ prime}}} \frac{1}{p} \ll \frac{1}{2^{k-1}} \cdot \frac{2^{k+1}}{\log 2^{k+1}} \ll \frac{1}{k}.$$

As a result,

$$\sum_{\substack{m\in(2^{k-1},2^k)\\ m \text{ 2-dense}}} \frac{X}{mk} \sum_{\substack{p\in(2^{k-1},2^{k+1})\\ p \text{ prime}}} \frac{1}{p} \ll \frac{X}{k^2} \sum_{\substack{m\in(2^{k-1},2^k)\\ m \text{ 2-dense}}} \frac{1}{m}.$$

Similarly, we can use the fact that the largest term in the sum in m is at most $\frac{1}{2^{k-1}}$ and the number of terms is less than $D(2^k)$. Thus, using the upper bound for $D(X)$ given in Lemma 4.12, we obtain

$$\frac{X}{k^2} \sum_{\substack{m\in(2^{k-1},2^k)\\ m \text{ 2-dense}}} \frac{1}{m} \ll \frac{X}{k^3}.$$

Summing over all values of $k > Y$ allows us to see that

$$\sum_{k>Y} \frac{X}{k^3} \le X \int_{Y-1}^{\infty} \frac{1}{t^3} dt = \frac{X}{2(Y-1)^2}.$$

In particular, when $Y \ge 1 + C\sqrt{\log X}$, we have

$$\sum_{k>Y} \frac{X}{k^3} \le \frac{X}{C^2 \log X}.$$

Thus, if C is large, then the number of 2-dense integers with obstructions at $k \ge C\sqrt{\log X}$ is small relative to the number of 2-dense integers. Hence, it suffices to take $k < C\sqrt{\log X}$ in

our computations, which means that we can take $m < \exp\{C\sqrt{\log X}\}$. Now, since $p < 2m$ in our construction, then $pm < 2m^2 < 2\exp\{2C\sqrt{\log X}\}$. Therefore,

$$\frac{X}{mp\log(X/mp)} \leq \frac{X}{mp\log(X(2\exp\{2C\sqrt{\log X}\})^{-1})} \ll \frac{X}{mp\log X}.$$

Next, we will bound the integers counted by the sum in j in (4.4). We have

$$\begin{aligned}\sum_{\substack{1<j\leq X/mp\\ mpj \text{ 2-dense}\\ P^-(j)>p}} 1 &= \#\{n \leq X : mp \mid n, n \text{ is 2-dense}, P^-(n/mp) > p\}\\ &= \sum_{q\leq X} \#\{qM \leq X : mp \mid M, M \text{ is 2-dense}, q \text{ is prime}, P(M) < q < 2M\} \quad (4.8)\\ &\leq \sum_{q\leq X/mp} D(X/mpq, q),\end{aligned}$$

where the second line follows from Lemma 4.15 and the third line follows from the definition of $D(X, Y)$. We can improve upon this final bound slightly. Namely, since we are counting integers M with $\frac{q}{2} < M \leq \frac{X}{q}$ in the second line, we see that $D(X/mpq, q) = 0$ when $q > \sqrt{2X}$. Now, to simplify our notation, let $Z = X/mp$. Then, using the bound that we just derived for q in conjunction with (4.8) yields

$$\begin{aligned}\sum_{\substack{j\leq Z\\ mpj \text{ 2-dense}\\ P^-(j)>p}} 1 &\leq \sum_{q\leq \min(Z,\sqrt{2X})} D(Z/q, q)\\ &\leq c \sum_{q\leq \min(Z,\sqrt{2X})} H(Z/q, q),\end{aligned}$$

where the second inequality follows from Lemma 4.20. Since $j > 1$ and $P^-(j) > p$, then $j > p > 2^C$ implies, in particular, that $Z > 2^{16}$. Let $\ell(X)$ be defined as in Lemma 4.19. We will show that

$$\sqrt{2Z}\ell(Z) > \sqrt{2X}, \quad (4.9)$$

which will allow us to apply Lemma 4.19 in order to obtain an upper bound of $cH(Z,Z)$ for the sum given in the previous display. To prove 4.9, we recall that we can take $m < \exp\{C\sqrt{\log X}\}$ and $p < 2m < 2\exp\{C\sqrt{\log X}\}$. Hence,

$$Z = \frac{X}{mp} > \frac{X}{2e^{2C\sqrt{\log X}}} > X^{1/2}.$$

Now,

$$\ell(Z) > e^{(\log Z)^{2/3}},$$

so we can use the fact that $Z > X^{1/2}$ to show that $\ell(Z) > e^{(\log X)^{3/5}}$. Thus, for sufficiently large X, we have

$$\sqrt{mp} < \sqrt{2}e^{C\sqrt{\log X}} < e^{(\log X)^{3/5}} < \ell(Z),$$

so

$$\sqrt{2Z}\ell(Z) = \sqrt{\frac{2X}{mp}}\ell(Z) > \sqrt{2X}.$$

As a result, we can apply Lemma 4.19 to obtain an upper bound of $cH(Z,Z)$, since $\ell(Z) \geq 1$ when $Z \geq 2^{16}$. By appealing to the definition of the function $H(X,Y)$, we have

$$1 \ll H(Z,Z) \ll \frac{Z}{\log Z} = \frac{X}{mp\log(X/mp)}. \tag{4.10}$$

$$\sum_{\substack{j \leq Z \\ mpj \text{ 2-dense} \\ P^-(j) > p}}$$

Now, it will suffice to replace $\log(X/mp)$ with $\log X$ in the denominator of (4.10) in order to arrive at a more precise estimate for the sum in j. In other words, we have

$$\sum_{\substack{m \in (2^{k-1},2^k) \\ m \text{ 2-dense}}} \sum_{\substack{p \in (2^{k-1},2^{k+1}) \\ p \text{ prime}}} \sum_{\substack{j \leq X/mp \\ mpj \text{ 2-dense} \\ P^-(j) > p}} 1 \ll \sum_{\substack{m \in (2^{k-1},2^k) \\ m \text{ 2-dense}}} \frac{X}{m\log X} \sum_{\substack{p \in (2^{k-1},2^{k+1}) \\ p \text{ prime}}} \frac{1}{p}.$$

Moreover, using the same estimates for the summations in m and p that we found above

allows us to obtain

$$\sum_{\substack{m\in(2^{k-1},2^k)\\ m \text{ 2-dense}}} \frac{X}{m\log X} \sum_{\substack{p\in(2^{k-1},2^{k+1})\\ p \text{ prime}}} \frac{1}{p} \ll \frac{X}{k^2\log X}.$$

Summing over all values of $k > C$ allows us to see that

$$\frac{X}{\log X}\sum_{k>C}\frac{1}{k^2} \leq \frac{X}{\log X}\int_C^\infty \frac{1}{t^2}dt \leq \frac{X}{C\log X}.$$

Since we have chosen C to be large relative to the size of Saias' lower bound constant for $D(X)$, then our count of 2-dense integers with obstructions at $k > C$ is negligible relative to the full count of 2-dense integers.

All that remains, then, is for us to consider the 2-dense integers n that have no obstructions at values of $k > C$. Let

$$\mathcal{N} = \{n \leq X : n \text{ is 2-dense with no obstructions at } k > C\}.$$

Since we chose C to be large relative to the implicit constant κ_1 from Lemma 4.12, we can use this lemma, along with our count of 2-dense integers with obstructions at $k > C$, to show that for all large X,

$$\#\mathcal{N} \geq \kappa\frac{X}{\log X},$$

where $\kappa > 0$ is some absolute constant. Define $f\colon \mathcal{N} \to \mathbb{Z}^+$ to be a function that maps each element $n \in \mathcal{N}$ to its largest 2-dense divisor m with all prime factors at most 2^C. Let $\mathcal{M} = \mathrm{Im}f$. By the Pigeonhole Principle, there is some $m_0 \in \mathcal{M}$ with at least $\frac{\#\mathcal{N}}{\#\mathcal{M}} \geq \frac{\kappa}{4^{2^C}}\frac{X}{\log X}$ elements in its preimage, since Chebyshev's bound (cf. [32, pg. 108]) implies $\prod_{p\leq 2^C} p \leq 4^{2^C}$. In other words, m_0 divides at least the average number of integers in a pre-image. For each

$n \in \mathcal{N}$ with $f^{-1}(m_0) = n$, let

$$n' = n \prod_{\substack{p \leq 2^C \\ p \text{ prime} \\ p \nmid m_0}} p.$$

Then, n' is squarefree, since the only primes dividing n that are smaller than 2^C are also divisors of m_0. Moreover, n' is strictly 2-dense, since the strict inequality form of Bertrand's Postulate implies that the product of all primes up to 2^C is strictly 2-dense. Finally, since we multiplied every n in the pre-image of m_0 by the same sequence of primes, there is a one-to-one correspondence between the strictly 2-dense integers up to $4^{2^C}X$ that we have constructed and the 2-dense numbers in the pre-image of m_0. Thus, at least $\frac{\kappa}{4^{2^C}} \frac{X}{\log X}$ of the integers up to $4^{2^C}X$ are strictly 2-dense. Therefore, since $D'(4^{2^C}X) \geq \frac{\kappa}{4^{2^C}} \frac{X}{\log X}$, we have the stated result. □

The proof of Theorem 4.21 can be used to obtain the following results on the relationship between the practical and φ-practical numbers.

Corollary 4.22. *For X sufficiently large, we have*

$$\#\{n \leq X : n \textit{ is practical but not } \varphi\textit{-practical}\} \gg \frac{X}{\log X}.$$

Proof. As in the proof of Theorem 4.21, let

$$\mathcal{N} = \#\{n \leq X : n \text{ is 2-dense with no obstructions at } k > C\}.$$

We know that, for sufficiently large X, we have $\#\mathcal{N} \geq \kappa \frac{X}{\log X}$, where $\kappa > 0$ is some absolute constant. As before, let $f \colon \mathcal{N} \to \mathbb{Z}^+$ map each $n \in \mathcal{N}$ to its largest 2-dense divisor m satisfying the condition that $P(m) \leq 2^C$. Then, from the proof of Theorem 4.21, there exists some $m_0 \in \mathrm{Im} f$ with at least $\frac{\kappa}{4^{2^C}} \frac{X}{\log X}$ elements in its pre-image. For each $n \in \mathcal{N}$

with $f^{-1}(m_0) = n$, let

$$n' = \frac{2 \cdot 7^2}{\gcd(15, m_0)} n \prod_{\substack{7 < p \leq 2^C \\ p \nmid m_0}} p.$$

Since n is squarefree and 2-dense, then $2^2 \| n'$. Thus, we can write $n' = 28M$, where M is an integer with $P^-(M) \geq 7$. Observe that 28 is not φ-practical, since $x^{28} - 1$ has no divisor with degree 5. Moreover, as all prime divisors of M are at least 7, it follows that $x^{n'} - 1$ has no divisor of degree 5. Hence, n' is not φ-practical. On the other hand, let

$$l = n \prod_{\substack{7 < p \leq 2^C \\ p \nmid m_0}} p.$$

Since n is 2-dense, Bertrand's Postulate implies that l is 2-dense, hence practical. In particular, this means that all of the prime factors of l must satisfy the inequality from Proposition 1.3. Now, let $r = \frac{2 \cdot 7^2}{\gcd(15, m_0)}$. Since $2 \cdot 7^2 > 15$ then, as each prime p dividing l satisfies $p \leq \sigma(m) + 1$, it must be the case that $p \leq \sigma(rm) + 1$. Therefore, n' is practical.

In order to construct the integers n', we multiplied every n in the pre-image of m_0 by the same number. As a result, there is a one-to-one correspondence between the practical numbers up to $r \cdot 4^{2^C} X$ that we have constructed and the 2-dense numbers in the pre-image of m_0. Therefore, at least $\frac{\kappa}{4^{2^C}} \frac{X}{\log X}$ of the integers up to $r \cdot 4^{2^C}$ are practical but not φ-practical. □

Corollary 4.23. *For X sufficiently large, we have*

$$\#\{n \leq X : n \text{ is } \varphi\text{-practical but not practical}\} \gg \frac{X}{\log X}.$$

Proof. In Theorem 4.21, we showed that $\#\{n \leq X : n \text{ even, squarefree and } \varphi\text{-practical}\} \gg \frac{X}{\log X}$. Now, either a positive proposition of the integers counted in this set are divisible by 7 or a positive proportion are not divisible by 7. In the first case, let n be a strictly 2-dense number that is divisible by 7, and let $n' = \frac{3}{2}n$. In the second case, we can take n to be a

strictly 2-dense number with $(7, n) = 1$, and $n' = \frac{21}{2}n$. In either case, n' can be re-written in the form

$$n' = 3^2 \cdot 5 \cdot 7 \cdot \prod_{\substack{7<p\leq X \\ p|n}} p.$$

Since $3^2 \cdot 5 \cdot 7$ is φ-practical and n is strictly 2-dense, then n' is φ-practical by Lemmas 4.9 and 4.14. However, n' is not practical since it is odd. □

We remark that Corollary 4.23 also shows that a positive proportion of φ-practical numbers are odd.

Chapter 5

Multiplicative orders and Artin's conjecture

In this chapter, we highlight a few important results regarding multiplicative orders and discuss how they fit in with the work that we will present in Chapter 6.

5.1 Introduction

There is an inextricable link between multiplicative orders and the degrees of the irreducible divisors of $x^n - 1$ in $\mathbb{F}_p[x]$. Let $\ell_a(n)$ denote the multiplicative order of $a \pmod{n}$ for integers a with $(a, n) = 1$. The following well-known proposition [10] demonstrates the important connection between $\ell_p(d)$ and the factorization of $\Phi_d(x)$:

Proposition 5.1. *The following two cases completely characterize the factorization of* $\Phi_d(x)$ *over* $\mathbb{F}_p$*:*

1) If $(d, p) = 1$*, then* $\Phi_d(x)$ *decomposes into a product of distinct irreducible polynomials, each with degree* $\ell_p(d)$ *in* $\mathbb{F}_p[x]$*.*

2) If $d = mp^k$*,* $(m, p) = 1$*, then* $\Phi_d(x) = \Phi_m(x)^{\varphi(p^k)}$ *over* $\mathbb{F}_p$*.*

In particular, this result implies that when p is a primitive root (mod d), the polynomial $\Phi_d(x)$ remains irreducible in $\mathbb{F}_p[x]$. Thus, as we count the integers n for which $x^n - 1$ has a divisor of every degree between 1 and n, it will be important to understand how often p is a primitive root (mod d). The study of primitive roots dates back at least to Gauss, who observed that the period of the repeating decimals in the expansion of $\frac{1}{p}$ is precisely $\ell_{10}(p)$. His tables in articles 315-317 of Disquisitiones Arithmeticae include a number of examples of primes p for which $\frac{1}{p}$ has a period of length $p-1$; that is, primes for which 10 is a primitive root modulo p. He conjectured that there are infinitely many primes p with this property, but was unable to prove his conjecture.

It is natural to ask the more general question: "For which integers a are there infinitely many primes p such that a is a primitive root modulo p?" If we exclude 2, as Gauss did, then all of the groups $(\mathbb{Z}/p\mathbb{Z})^\times$ have even order; thus, squares of integers cannot be cyclic generators. Another obvious value of a that we can exclude is -1, since -1 has order dividing 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$. Thus, a necessary condition on a for there to be infinitely many primes p with a as a primitive root would be that a cannot be a square and $a \neq -1$. In 1927, Artin conjectured that these trivially necessary conditions are also sufficient:

Conjecture 5.2 (Artin's primitive root conjecture)**.** *If the integer a is not a square and not -1, then there are infinitely many primes with a as a primitive root.*

In fact, he made the following stronger conjecture:

Conjecture 5.3. *If the integer a is not a square and not -1, then there is a positive number $A(a)$ such that the number of primes $p \leq X$ with primitive root a is asymptotically $A(a) \cdot \pi(X)$ as $X \to \infty$.*

For all values of a, $A(a)$ is a rational multiple of Artin's constant, which is defined as follows:

$$A = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) = 0.3739558136....$$

Artin gave a heuristic argument that led him to conjecture a set of values for $A(a)$. However, Lehmer provided numerical evidence that called some of Artin's conjectured values into question. According to Hooley [20] Artin's heuristic argument was later revised by Heilbronn, who came up with the following formula for $A(a)$ when a is squarefree:

$$A(a) = \begin{cases} A, & a \not\equiv 1 \pmod 4 \\ A\left(1 - \prod_{q|a} \frac{1}{1+q-q^2}\right), & a \equiv 1 \pmod 4 \end{cases}$$

Heilbronn's conjectured values for $A(a)$ appear to agree with Lehmer's numerical computations, and are currently accepted to be the "correct" values of $A(a)$. (As we will discuss below, a conditional proof of Artin's primitive root conjecture was given by Hooley in 1967; the values for $A(a)$ that he obtained agree with Heilbronn's conjectured values.)

5.2 A heuristic argument

To provide some intuition for why the quantitative form of Artin's Conjecture should be true, we will start by providing a heuristic argument.

Condition 5.4. *An integer a is a primitive root* $\pmod p$ *if and only if for every prime q dividing $p-1$, a is not a q^{th} power* $\pmod p$.

Choose a squarefree $a \neq 1$. For each fixed q, we are interested in computing the density of primes p for which the condition above does not hold. In other words, we wish to compute the density of primes p such that

$$p \equiv 1 \pmod q \tag{5.1}$$

and

$$a^{\frac{p-1}{q}} \equiv 1 \pmod p. \tag{5.2}$$

We will say that a pair (a, p) "fails the q-test" if it satisfies both of these conditions. It is not difficult to determine the proportion of numbers a that "fail the q-test" when p is fixed and $q \mid p-1$. Namely, $\frac{1}{q}$ of all values of a will have this property.

On the other hand, it is quite difficult to determine this proportion when a is fixed and p varies over all primes that are $\equiv 1 \pmod{q}$. For each fixed prime q, the Prime Number Theorem for Arithmetic Progressions implies that $p \equiv 1 \pmod{q}$ occurs with frequency $\frac{1}{\varphi(q)} = \frac{1}{q-1}$. Fermat's Little Theorem implies that $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$. In other words, when $p \nmid a$, then $a^{\frac{p-1}{q}}$ is a solution to the congruence

$$x^q \equiv 1 \pmod{p}.$$

This congruence has q solutions, one of which is equivalent to $1 \pmod{q}$. So, the proportion of primes that satisfy condition (5.2) should be $\frac{1}{q}$. As a result, if we assume that the events "$p \equiv 1 \pmod{q}$" and "$a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$" are independent, then the probability that conditions (5.1) and (5.2) are met simultaneously is $\frac{1}{q(q-1)}$. On the other hand, if p has a as a primitive root, then conditions (5.1) and (5.2) cannot occur simultaneously for any q.

Thus, we would expect a natural density of

$$\prod_q \left(1 - \frac{1}{q(q-1)}\right)$$

for primes p for which a is a primitive root $\pmod{p}$. Therefore, we would expect that

$$\#\{p \leq X : a \text{ is a generator } \pmod{p}\} = \prod_q \left(1 - \frac{1}{q(q-1)}\right) \frac{X}{\log X} + \text{Some Error Term.}$$

Assuming the Generalized Riemann Hypothesis, one can prove that this estimate is correct when $a \not\equiv 1 \pmod{4}$. In the next section, we will discuss a rigorous version of this argument, due to Hooley [20].

5.3 Hooley's approach

We will now sketch Hooley's argument in the simplest case, where a is squarefree and $a \not\equiv 1 \pmod 4$. Let $K_q := \mathbb{Q}(\zeta_q, a^{1/q})$. From basic properties of Kummerian fields, we know that:

$$p \text{ splits completely in } K_q \iff p \equiv 1 \pmod q \text{ and } a^{\frac{p-1}{q}} \equiv 1 \pmod p.$$

Thus, we can translate "failing the q-test" into a problem in algebraic number theory. A special case of the GRH-conditional Chebotarev Density Theorem implies that

$$\sum_{\substack{p \le X \\ p \text{ splits} \\ \text{completely in } K_q}} 1 \sim \frac{1}{[K_q : \mathbb{Q}]} \frac{X}{\log X},$$

as $X \to \infty$. Thus, if $n(q) = [K_q : \mathbb{Q}]$, we have

$$\sum_{\substack{p \le X \\ p \text{ does not split} \\ \text{completely in } K_q}} 1 \sim \left(1 - \frac{1}{n(q)}\right) \frac{X}{\log X}. \tag{5.3}$$

We want to find the density of primes p that do not split completely in any K_q. In order to compute this, we can do a simple inclusion-exclusion. Start with:

$$1 - \frac{1}{n(2)} - \frac{1}{n(3)} - \frac{1}{n(5)} - \cdots.$$

The subtraction above double-counts primes that split completely in both K_i and K_j, so we need to add back terms to account for these primes. So, we will add

$$\frac{1}{n(6)} + \frac{1}{n(10)} + \frac{1}{n(14)} + \frac{1}{n(15)} + \cdots.$$

Continuing in this fashion, we would expect to obtain something like:

$$\#\{p \leq X : a \text{ is a generator mod } p\} \sim \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} \frac{X}{\log X},$$

as $X \to \infty$. Since $a \not\equiv 1 \pmod 4$, the fields K_q are linearly disjoint; this implies that, for squarefree k,

$$n(k) = \prod_{q|k} n(q).$$

Thus, we have

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} = \prod_{q} \left(1 - \frac{1}{q(q-1)}\right) = A.$$

This suggests that

$$\#\{p \leq x : a \text{ is a generator mod } p\} \sim A \frac{X}{\log X}.$$

However, we are ignoring the accumulation of the error terms that arise from using inclusion-exclusion on (5.3). Nevertheless, using the Chebotarev Density Theorem, one can show that the same asymptotic estimate holds for the count of primes $p \leq X$ which pass all of the q-tests for $q \leq \log\log X$. It remains to show that $o(\pi(X))$ of these primes fail the q-test for some $q > \log\log X$.

We split these large q into three subintervals:

$$(1)\ \log\log X < q \leq \tfrac{\sqrt{X}}{\log^2 X},$$

$$(2)\ \tfrac{\sqrt{X}}{\log^2 X} < q \leq \sqrt{X}\log X,$$

$$(3)\ \sqrt{X}\log X \leq q \leq X.$$

For notational convenience, let $\eta_1 = \frac{\sqrt{X}}{\log^2 X}$ and $\eta_2 = \sqrt{X}\log X$. For primes $q \leq \eta_1$, the special case of the GRH-conditional Chebotarev Density Theorem described above gives an estimate of $O(\frac{\pi(X)}{q^2})$ primes $p \leq X$ that fail the q-test. The sum over the primes q satisfying $\log\log X < q \leq \eta_1$ is $o(\pi(X))$.

In the case where $\eta_1 < q \leq \eta_2$, we observe that the primes p that fail the q-test satisfy $p \equiv 1 \pmod{q}$. Thus, the number of these primes up to X is at most $\pi(X; q, 1)$. The Brun-Titchmarsh inequality yields

$$\pi(X; q, 1) \leq \frac{2X}{\varphi(q) \log(X/q)}$$

for $1 \leq q \leq X$. Thus,

$$\begin{aligned}\#\{p \leq X : p \text{ splits completely in some } K_q, \eta_1 \leq q \leq \eta_2\} &\leq \sum_{\eta_1 \leq q \leq \eta_2} \pi(X; q, 1) \\ &= O\left(\frac{X}{\log X} \sum_{\eta_1 \leq q \leq \eta_2} \frac{1}{q}\right).\end{aligned}$$

By Mertens' Theorem: $\sum_{q \leq X} \frac{1}{q} = \log\log X + \text{constant} + O(\frac{1}{\log X})$. As a result, we have

$$\sum_{\eta_1 \leq q \leq \eta_2} \frac{1}{q} = O\left(\frac{\log\log X}{\log X}\right).$$

Therefore,

$$\#\{p \leq X : p \text{ splits completely in some } K_q, \eta_1 \leq q \leq \eta_2\} = O\left(\frac{X \log\log X}{\log^2 X}\right).$$

Lastly, we consider the case where $\eta_2 < q \leq X$. If p splits completely in some K_q with $\eta_2 \leq q \leq X$, then $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ and $p \equiv 1 \pmod{q}$, so $\ell_a(p) \leq a^{\frac{p-1}{\eta_2}} \leq a^{\frac{X}{\eta_2}}$. Thus, p divides $a^m - 1$ for some $m < \frac{\sqrt{X}}{\log X}$. Let

$$M(X; \eta_2, X) := \#\{p \leq X : p \text{ splits completely in some } K_q,\ \eta_2 \leq q \leq X\}.$$

Observe that

$$2^{M(X;\eta_2,X)} < \prod_{\substack{p \text{ counted by} \\ M(X;\ \eta_2,\ X)}} p \leq \prod_{m < \frac{\sqrt{X}}{\log X}} a^m - 1.$$

Thus, we have

$$M(X;\eta_2,X) < \frac{\log a}{\log 2} \sum_{m<\frac{\sqrt{X}}{\log X}} m = O\left(\frac{X}{\log^2 X}\right).$$

This completes our sketch of Hooley's proof.

5.4 Related work

Hooley's ideas have been used in a number of subsequent papers concerning the function $\ell_a(n)$. In this thesis, we will make use of the following lemma of Li and Pomerance [25], which relies on components of Hooley's argument:

Lemma 5.5 (Li, Pomerance)**.** *(GRH) Suppose that q is an odd prime and that a is not a q^{th} power. Let A_q denote the set of primes $p \equiv 1 \pmod{q}$ with $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$. The number of integers $n \leq X$ divisible by a prime $p \in A_q$ with $p \geq q^2 \log^4 q$ is $O\left(\frac{X}{q \log q} + \frac{X \log\log X}{q^2}\right)$.*

Consequently, several of the results proven in Section 6.7 depend on the validity of the Generalized Riemann Hypothesis; see Lemmas 6.34 and 6.35, as well as Theorem 6.4.

Chapter 6

Degrees of divisors of $x^n - 1$ in $\mathbb{F}_p[x]$

In this chapter, we will examine an extension of the problem posed in the previous chapter; we will determine how often $x^n - 1$ has a divisor of every degree between 1 and n when factored over $\mathbb{F}_p[x]$. We will also introduce the concept of λ-practical numbers and describe their relationship with the φ-practical numbers.

6.1 Introduction and statement of results

For each rational prime p, we will define an integer n to be *p-practical* if $x^n - 1$ has a divisor in $\mathbb{F}_p[x]$ of every degree less than or equal to n. In order to better understand the relationship between φ-practical and p-practical numbers, we will define an intermediate set of numbers which we shall call the λ-practical numbers. An integer n is *λ-practical* if and only if it is p-practical for every rational prime p. Clearly each φ-practical number is λ-practical. In Sections 6.2 and 6.3, we will give alternative characterizations of the p-practical and λ-practical numbers that are often easier to work with.

The main goal of this chapter is to examine the relative sizes of the sets of φ-practical, λ-practical and p-practical numbers. Accordingly, the remainder of the chapter takes the following form. In Section 6.4, we will develop some theory on the structure of λ-practical numbers and show that there are infinitely many λ-practical numbers that are not φ-practical. We will go one step further in Section 6.5 and prove:

Theorem 6.1. *For X sufficiently large, the order of magnitude of λ-practicals in $[1, X]$ that are not φ-practical is $\frac{X}{\log X}$.*

In Sections 6.6 and 6.7, we answer a number of statistical questions concerning the p-practical numbers. For each fixed prime p, we define

$$F_p(X) := \#\{n \leq X : n \text{ is } p\text{-practical}\}.$$

Computational data seems to suggest an estimate for the order of magnitude of $F_p(X)$. In Section 1.2, we examined $F_p(X)/\frac{X}{\log X}$ for $p = 2, 3, 5$ in Tables 1.2 – 1.4. As mentioned in Section 1.2, the fact that the sequence of ratios appears to be bounded strongly suggests the following conjecture:

Conjecture 6.2. *For each rational prime p, $\lim_{X\to\infty} F_p(X)/\frac{X}{\log X}$ exists.*

Proving this may be exceedingly difficult; to understand why, we examine the fate of the practical numbers. An integer n is called *practical* if every integer m with $1 \leq m \leq n$ can be written as a sum of distinct divisors of n. As in Chapter 3 and 4, we define $PR(X)$ to be the count of practical numbers up to X. In spite of the abundance of literature on the practical numbers, it is not even known whether $\lim_{X\to\infty} PR(X)/\frac{X}{\log X}$ exists. In Section 6.7, we work towards the goal of showing that $F_p(X)$ is on the order of $X/\log X$, which given our lower bound for $F(X)$, requires establishing:

Conjecture 6.3. *For each rational prime p, we have*

$$F_p(X) \ll \frac{X}{\log X}.$$

The strongest bound that we have been able to prove in this vein is as follows:

Theorem 6.4. *Let p be a prime number. Assuming that the Generalized Riemann Hypothesis holds, we have $F_p(X) = O\left(X\sqrt{\frac{\log\log X}{\log X}}\right)$.*

6.2 Background and preliminary results

In Chapter 4, we gave the following alternative characterization for the φ-practical numbers, which we state here as a lemma.

Lemma 6.5. *An integer n is φ-practical if and only if every m with $1 \leq m \leq n$ can be written in the form*

$$m = \sum_{d \in \mathcal{D}} \varphi(d),$$

where $\mathcal{D}$ is a subset of divisors of n.

It is not difficult to see Lemma 6.5: since

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

where $\Phi_d(x)$ is the d^{th} cyclotomic polynomial, which is irreducible in $\mathbb{Z}[x]$ with degree $\varphi(d)$, we see that divisors of $x^n - 1$ correspond to subsets of divisors of n.

Recall the upper and lower bounds for $F(X)$ given in (4.2). One of our primary aims in this chapter will be to obtain similar upper bounds for the λ-practical and p-practical numbers. As in the case of the φ-practical numbers, we will find it helpful to have alternative characterizations of the λ-practical and p-practical numbers in terms of their divisors. Let $\ell_a(n)$ denote the multiplicative order of $a \pmod n$ for integers a with $(a, n) = 1$. If $(a, n) > 1$, let $n_{(a)}$ denote the largest divisor of n that is coprime to a, and let $\ell_a^*(n) = \ell_a(n_{(a)})$. In particular, if $(a, n) = 1$ then $\ell_a^*(n) = \ell_a(n)$.

Lemma 6.6. *An integer n is p-practical if and only if every m with $1 \leq m \leq n$ can be written as $m = \sum_{d|n} \ell_p^*(d) n_d$, where n_d is an integer with $0 \leq n_d \leq \frac{\varphi(d)}{\ell_p(d)}$.*

To see the relationship between the two characterizations of p-practical numbers, recall the following well-known proposition (cf. [10, pg. 489, ex.20]):

Proposition 6.7. *The following two cases completely characterize the factorization of $\Phi_d(x)$ over $\mathbb{F}_p$:*

1) If $(d, p) = 1$, then $\Phi_d(x)$ decomposes into a product of distinct irreducible polynomials of degree $\ell_p(d)$ in $\mathbb{F}_p[x]$.

2) If $d = mp^k$, $(m, p) = 1$, then $\Phi_d(x) = \Phi_m(x)^{\varphi(p^k)}$ over $\mathbb{F}_p$.

Thus, the correspondence between the definitions follows from the fact that each cyclotomic polynomial $\Phi_d(x)$ dividing $x^n - 1$ factors into $\varphi(d)/\ell_p^*(d)$ irreducible polynomials of degree $\ell_p^*(d)$ over $\mathbb{F}_p[x]$.

As we will discuss in the next section, the λ-practical numbers can be defined in a similar manner. However, it takes a bit more work to prove this. Before we proceed, we will briefly remark on a second intermediate set that lies between the φ-practicals and p-practicals, which we call the p-adic practical numbers. An integer n is *p-adic practical* if $x^n - 1$ has a divisor of every degree when factored over $\mathbb{Z}_p$, the ring of p-adic integers. We can completely characterize the p-adic practical numbers via the following proposition:

Proposition 6.8. *Let n be a positive integer. Then:*

(1) *If $n = p^k$ with $k \geq 1$, then n is p-adic practical if and only if n is φ-practical, namely if and only if either $p = 2$ or $k = 1$ and $p = 3$.*

(2) *If $(p, n) = 1$, then n is p-adic practical if and only if n is p-practical.*

(3) *If $n = p^k n_0$, where $(p, n_0) = 1$, then n is p-adic practical if and only if for every integer m with $1 \leq m \leq n$, we can write*

$$\sum_{d|n} \ell_p^*(d) \varphi(p^{v_p(d)}) n_d,$$

where $v_p(d)$ is the exact power of p dividing d and $0 \leq n_d \leq \frac{\varphi(d)}{\ell_p^*(d)\varphi(p^{v_p(d)})}$.

The proof of Proposition 6.8 follows immediately from well-known results on the factorization of cyclotomic polynomials in $\mathbb{Z}_p[x]$ (cf. [35, pp. 77-79]).

6.3 An alternative characterization for the λ-practical numbers

Just as we showed that the φ-practical and p-practical numbers have alternative characterizations that resemble the definition of a practical number, we can also show that the λ-practical numbers have such a characterization. Let $\lambda(n)$ denote the universal exponent of the multiplicative group of integers modulo n. We will show that the following theorem gives a criterion for an integer n to be λ-practical that is equivalent to the definition that we gave in Section 1:

Theorem 6.9. *An integer n is λ-practical if we can write every integer m with $1 \leq m \leq n$ in the form $m = \sum_{d|n} \lambda(d)m_d$, where m_d is an integer with $0 \leq m_d \leq \frac{\varphi(d)}{\lambda(d)}$.*

Before giving the proof, however, we will pause to ponder a related question. We can think of the set of integers n that are "p-practical for all primes p" as the intersection between all of the sets of integers that are p-practical. In addition to describing the intersection of these sets, we can also describe their union.

Proposition 6.10. *For each prime p, let S_p be the set of p-practical numbers. Then*

$$\cup_{i=1}^{\infty} S_p = \mathbb{Z}_+.$$

Proof. If $n = 1$ then n is φ-practical, hence it is p-practical for all primes p. If $n > 1$, then we can write $n = p_1^{e_1} \cdots p_k^{e_k}$, with $p_1 < p_2 < \cdots < p_k$ and $e_i \geq 1$ for $1 = 1, ..., k$. Let $p_l^{e_l} = \max(p_1^{e_1}, \cdots, p_k^{e_k})$. Since $n > 1$, then n will always have a maximal prime power

dividing it. From Lemma 6.28, $p_l^{e_l}$ is p_l-practical. Since $p_l^{e_l} > p_i^{e_i}$ for all $i \neq l$, then $p_i \leq p_l^{e_l} + 1$. Thus, by Lemma 6.26, n is p_l-practical. $\square$

In fact, we can prove a stronger result: it turns out that each integer n is p-practical for infinitely many values of p. Namely, for a given n, Dirichlet's Theorem on Primes in Arithmetic Progressions [32, p. 119] implies that there are infinitely many primes p for which $p \equiv 1 \pmod{n}$. In other words, $\ell_p(n) = 1$ for infinitely many primes p, so $x^n - 1$ splits completely into linear factors in $\mathbb{F}_p[x]$ for infinitely many primes p. This argument implies that each integer n is p-practical for a positive proportion of the p's. We could also observe that, if $p \equiv -1 \pmod{n}$, then $\ell_p(n) = 2$, hence all of the irreducible factors of $x^n - 1$ have degree at most 2. Dirichlet's Theorem also guarantees the existence of infinitely many such primes. We remark that there are integers n for which the set of primes $p \equiv \pm 1 \pmod{n}$ are the only primes for which $x^n - 1$ has a divisor of every degree ($n = 5$ is the smallest such integer).

We will now show that $\cap_{i=1}^{\infty} S_p$ is precisely the set of integers satisfying the conditions given in Definition 6.9. In order to do so, we will need the following results from elementary number theory (cf. [21, Theorem 4.2] and [24, proof of Proposition 4.2]):

Lemma 6.11. *If p is an odd prime and $e \in \mathbb{Z}_+$, then $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is cyclic.*

Lemma 6.12. *Let q be an odd prime and suppose that $0 \leq f \leq e$. If a is a generator of $(\mathbb{Z}/q^e\mathbb{Z})^\times$, then a also generates $(\mathbb{Z}/q^f\mathbb{Z})^\times$.*

Lemma 6.13. *For all positive integers n, there exists a prime p such that $\ell_p^*(d) = \lambda(d)$ for all $d \mid n$.*

Proof. First, we will consider the case where $n = q^e$, where q is an odd prime. Each divisor of n is of the form $d = q^f$, with $0 \leq f \leq e$. Since $(\mathbb{Z}/q^f\mathbb{Z})^\times$ is cyclic, there must be some element $a \in (\mathbb{Z}/q^e\mathbb{Z})^\times$ such that $\ell_a^*(q^e) = \lambda(q^e)$. By Lemma 6.12, a is also a generator for $(\mathbb{Z}/q^f\mathbb{Z})^\times$, i.e. $\ell_a^*(q^f) = \lambda(q^f)$. By Dirichlet's Theorem on Primes in an Arithmetic

Progression, there exists a prime $p \equiv a \pmod{q^e}$. Thus, we can certainly find a prime p with $\ell_p^*(q^f) = \lambda(q^f)$ for all f with $0 \leq f \leq e$.

If $n = 2^e$, we observe that, when $p = 3$, we have $\ell_p^*(2^j) = \lambda(2^j)$ for all $j \geq 1$. Hence, $\ell_3^*(d) = \lambda(d)$ for all divisors d of 2^e.

Now we consider the case where $n = q_1^{e_1} \cdots q_k^{e_k}$, $k \geq 2$. Each $d \mid n$ can be written in the form $d = q_1^{f_1} \cdots q_k^{f_k}$, where $0 \leq f_i \leq e_i$ holds for $i = 1, ..., k$. For each i, let a_i be a primitive root $\pmod{q_i^{e_i}}$. (Note: If $q_1 = 2$, we can take $a_1 = 3$ by the previous case). Since $q_1, ..., q_k$ are pairwise relatively prime then, by the Chinese Remainder Theorem, there exists an integer x with

$$\begin{aligned} x &\equiv a_1 \pmod{q_1^{e_1}} \\ &\vdots \\ x &\equiv a_k \pmod{q_k^{e_k}}. \end{aligned}$$

By Dirichlet's Theorem on Primes in Arithmetic Progression, there exists a prime p with $p \equiv x \pmod{n}$. In other words, $\ell_p^*(q_i^{e_i}) = \lambda(q_i^{e_i})$ for $i = 1, ..., k$. By Lemma 6.12, we have $\ell_p^*(q_i^{f_i}) = \lambda(q_i^{f_i})$ for all f_i with $0 \leq f_i \leq e_i$. Therefore, since $q_1, ..., q_k$ are pairwise relatively prime, we have

$$\ell_p^*(q_1^{f_1} \cdots q_k^{f_k}) = \operatorname{lcm}[\ell_p^*(q_1^{f_1}), \cdots, \ell_p^*(q_k^{f_k})] = \operatorname{lcm}[\lambda(q_1^{f_1}), \cdots, \lambda(q_k^{f_k})] = \lambda(q_1^{f_1} \cdots q_k^{f_k}).$$

□

Below, we provide the proof of Theorem 6.9.

Proof. If n is λ-practical then, by Lemma 6.13, there exists a prime p' such that $\ell_{p'}^*(d) = \lambda(d)$ for all $d \mid n$. Since n is p-practical for all primes p then, in particular, n is p'-practical, i.e.

for all integers m with $1 \leq m \leq n$, we have

$$m = \sum_{d|n} \ell^*_{p'}(d) n_{p'}(d),$$

where $n_{p'}(d)$ is an integer satisfying $0 \leq n_{p'}(d) \leq \frac{\varphi(d)}{\ell^*_{p'}(d)}$. Thus, for all m with $1 \leq m \leq n$, we have

$$m = \sum_{d|n} \lambda(d) n_{p'}(d),$$

since $\ell^*_{p'}(d) = \lambda(d)$ for all $d \mid n$. Since it is necessarily the case that $0 \leq n_{p'}(d) \leq \frac{\varphi(d)}{\ell^*_{p'}(d)} = \frac{\varphi(d)}{\lambda(d)}$, then n satisfies the condition given in Definition 6.9.

On the other hand, suppose that every integer m with $1 \leq m \leq n$ can be written in the form $m = \sum_{d|n} \lambda(d) m_d$, where m_d is an integer satisfying $0 \leq m_d \leq \frac{\varphi d}{\lambda(d)}$. By definition, $\lambda(d) = \max_{a \in (\mathbb{Z}/d\mathbb{Z})^\times} \ell^*_a(d)$. Since $\ell^*_a(d) \leq \lambda(d)$ for all a in $(\mathbb{Z}/d\mathbb{Z})^\times$, then certainly every m with $1 \leq m \leq n$ can be written in the form $m = \sum_{d|n} \ell^*_p(d) n_d$, where p is any rational prime and $0 \leq n_d \leq \frac{\varphi(d)}{\ell^*_p(d)}$. Thus, n is λ-practical. □

6.4 The relationship between φ-practical and λ-practical numbers

In this section, we will examine the relationship between φ-practical and λ-practical numbers. We begin by reminding the reader of some useful results on the φ-practical numbers. In Chapter 4, we proved the following necessary condition for an integer n to be φ-practical:

Lemma 6.14. *Suppose that $n = p_1^{e_1} \cdots p_k^{e_k}$ is φ-practical, where $p_1 < p_2 < \cdots < p_k$ and $e_i \geq 1$ for $i = 1, ..., k$. Define $m_i = p_1^{e_1} \cdots p_i^{e_i}$ for $i = 0, ..., k-1$. Then, the inequality $p_{i+1} \leq m_i + 2$ must hold for all i.*

We say that an integer n is *weakly φ-practical* if it satisfies the conditions given in Lemma 6.14. We note that the inequality in Lemma 6.14 also gives a necessary condition

for a positive integer n to be λ-practical. Namely, if $p_{i+1} > m_i + 2$ for some i such that $0 \leq i \leq k-1$ then, since $\lambda(p_{i+1}) = \varphi(p_{i+1}) = p_{i+1} - 1$, we have $\lambda(p_{i+1}) > m_i + 1$. Since $m_i = \sum_{d|m_i} \lambda(d)\frac{\varphi(d)}{\lambda(d)}$, then $m_i + 1$ cannot be written as a sum of $\lambda(d)$'s, so such an n would not be λ-practical. Thus, we have proven the following:

Lemma 6.15. *Every λ-practical number is weakly φ-practical.*

The converse to Lemma 6.15 is false. For example, $n = 9$ is weakly φ-practical but not λ-practical. However, we can show that the converse holds for even integers and for squarefree integers. In order to complete these proofs, we will need the following lemma on the structure of λ-practical numbers.

Lemma 6.16. *Let $n = mp$, where m is λ-practical, $p \leq m + 2$ and $(p, m) = 1$. Then n is λ-practical. Moreover, if $n = p^k m$ with $k \geq 2$, then n is λ-practical if $p \leq m + 1$.*

The proof of Lemma 6.16 is virtually identical to the proof of Lemma 4.1 in Chapter 4. The idea is to use the characterization of λ-practical numbers given in Theorem 6.9 to show that every integer $l \in [1, n]$ can be expressed in the form

$$l = \sum_{d|m} \lambda(d) m_d,$$

with $0 \leq m_d \leq \frac{\varphi(d)}{\lambda(d)}$. In order to check that this holds when $n = mp$, we observe that if every $l \in [1, n]$ can be written in the form

$$l = (p-1)Q + R, \ 0 \leq Q, R \leq m \tag{6.1}$$

then, using our hypothesis that m is λ-practical, we have

$$l = \sum_{d|m} (p-1)\lambda(d) m_d + \sum_{d|m} \lambda(d) m'_d, \tag{6.2}$$

where $0 \leq m_d, m'_d \leq \frac{\varphi(d)}{\lambda(d)}$. We can use the facts that $\lambda(p) = p - 1$ and $\lambda(p_1^{e_1} \cdots p_k^{e_k}) =$

$\text{lcm}[\lambda(p_1^{e_1}), ..., \lambda(p_k^{e_k})]$ to show that we can re-write (6.2) in the following manner:

$$l = \sum_{d|m} \lambda(pd) m_{pd} + \sum_{d|m} \lambda(d) m'_d,$$

where $0 \leq m_{pd} \leq \frac{\varphi(pd)}{\lambda(pd)}$ and $0 \leq m'_d \leq \frac{\varphi(d)}{\lambda(d)}$. Thus, the proof boils down to showing that every $l \in [1, n]$ can be expressed as in (6.1), which follows from breaking $[1, n]$ into subintervals of the form $[(p-1)Q, (p-1)Q + m]$ and using the hypothesis that $p \leq m + 2$ to show that the subintervals cover the full interval. The higher power case is similar, but requires induction on the power of the prime p.

Proposition 6.17. *Let n be an even integer. Then n is weakly φ-practical if and only if n is φ-practical if and only if n is λ-practical.*

Proof. We will begin by showing that an even integer n is weakly φ-practical if and only if it is φ-practical. If n is even and weakly φ-practical, then we can write $n = p_1^{e_1} \cdots p_k^{e_k}$, where $2 = p_1 < p_2 < \cdots < p_k$ and $e_i \geq 1$ for $i = 1, ..., k$. We will use induction on the number of distinct prime factors of n to show that n is φ-practical. For our base case, we observe that 2^{e_1} is φ-practical for all positive values of e_1. For our induction hypothesis, we assume that $m = p_1^{e_1} \cdots p_{k-1}^{e_{k-1}}$ is φ-practical. Since m is even and p_k is odd, then $p_k \leq m+2$ implies that $p_k \leq m + 1$. Thus, by Lemma 4.9, $mp_k^{e_k}$ is φ-practical. The other direction follows immediately from Lemma 4.5. The proof for λ-practicals is the same, this time using Lemma 6.16 instead of Lemma 4.9. □

The conditions given in Lemma 6.14 for an integer n to be weakly φ-practical are necessary, but not sufficient, for n to be φ-practical. When n is squarefree, we have shown (cf. Corollary 4.2 in Chapter 4) that these notions are equivalent. There is an analogous situation for λ-practical numbers.

Proposition 6.18. *Let n be a squarefree integer. Then n is λ-practical if and only if it is φ-practical.*

Proof. We showed in Corollary 4.2 of Chapter 4 that a squarefree integer is φ-practical if and only if it is weakly φ-practical. From Lemma 6.15, every λ-practical number is weakly φ-practical. The other direction of the proof is trivial, as all φ-practical numbers are automatically λ-practical. □

While it is easy to see that all φ-practical numbers are λ-practical, the converse does not hold. In fact, we can show that there are infinitely many counterexamples:

Proposition 6.19. *There are infinitely many λ-practical numbers that are not φ-practical.*

Proof. Let $X \geq 1$ be a real number. Let $n = 45 \cdot \prod_{23<p\leq X} p$. It follows from Bertrand's Postulate that every prime $p \mid n$ with $p \nmid 45$ satisfies $p \leq m + 2$, where m is the product of 45 and all of the primes $23 < q < p$. Then, since 45 is λ-practical, it follows from Lemma 6.16 that n is λ-practical. However, n is not φ-practical, since $x^{45} - 1$ has no divisor of degree 22 and all other primes $p \mid n$ are greater than 23, so $\lambda(p) > 22$. Thus, as we let X tend to infinity, we see that this method produces an infinite family of λ-practical numbers that are not φ-practical. □

6.5 Density considerations for λ-practical numbers

In this section, we will answer some density questions concerning the λ-practical numbers. We will begin by reminding the reader of the method of proof in (4.2), which will be a model for some of the arguments that we will use to bound the number of λ-practical integers up to X. The key to proving the upper bound in (4.2) was to use Proposition 6.17 in order to show that all even φ-practical numbers are practical. To handle the case of odd φ-practicals, we observed that, for every odd integer n in $(0, X]$, there exists a unique positive integer l such that $2^l n$ is in the interval $(X, 2X]$. Moreover, we showed that $2^l n$ is φ-practical if n is φ-practical. As a result, we were able to construct a one-to-one map from the set of odd φ-practical numbers in $(1, X]$ to a subset of the even φ-practical numbers in $(X, 2X]$.This

allowed us to directly compare the size of the set of φ-practical numbers with the size of the set of practical numbers, which we knew to be $O(X/\log X)$ from [34, Theorem 2].

We can use the same argument to show that the upper bound given in (4.2) will also serve as an upper bound for the number of λ-practical numbers up to X. The only modification needed is to use Proposition 6.17 to show that all even λ-practical numbers are practical. On the other hand, Lemma 6.15 show that, if n is an odd λ-practical number, then it is weakly φ-practical. Thus, for $l \geq 1$, $2^l n$ is weakly φ-practical, since multiplying a weakly φ-practical integer n by a power of 2 will not prevent its prime divisors from satisfying the inequalities from Lemma 6.14. Therefore, we can use the argument given above for the odd φ-practicals to obtain the same upper bound for the number of λ-practicals up to X.

In order to obtain a lower bound, we simply observe that the set of φ-practical numbers is properly contained within the set of λ-practical numbers. Hence, the lower bound that we gave in Chapter 4 for the φ-practical numbers will also serve as a lower bound for the λ-practical numbers. As a result, we have:

Theorem 6.20. *Let $F_\lambda(X) = \#\{n \leq X : n \text{ is } \lambda\text{-practical}\}$. Then, there exist positive constants c_3 and c_4 such that*

$$c_3 \frac{X}{\log X} \leq F_\lambda(X) \leq c_4 \frac{X}{\log X},$$

for all $X \geq 2$.

Note that the argument above shows that we may, in fact, take $c_3 = c_1$ and $c_4 = c_2$. However, this does not imply that $F(X) - F_\lambda(X) = o(\frac{X}{\log X})$. In fact, we can show that $F_\lambda(X) - F(X) \gg \frac{X}{\log X}$. Before we prove this result, we remind the reader of some definitions and lemmas used in the lower bound argument for the φ-practical numbers in Chapter 4, which will be useful in this scenario as well.

Let $1 = d_1(n) < d_2(n) < \cdots < d_{\tau(n)}(n) = n$ denote the increasing sequence of divisors

of a positive integer n. We define

$$T(n) = \max_{1 \le i < \tau(n)} \frac{d_{i+1}(n)}{d_i(n)}.$$

Definition 6.21. An integer n is called 2-*dense* if n is squarefree and $T(n) \le 2$.

Note that any 2-dense number $n > 1$ is even. Let

$$D(X) = \#\{1 \le n \le X : n \text{ is 2-dense}\}.$$

In [34], Saias proved the following upper and lower bounds for $D(X)$:

Lemma 6.22 (Saias)**.** *There exist positive constants κ_1 and κ_2 such that*

$$\kappa_1 \frac{X}{\log X} \le D(X) \le \kappa_2 \frac{X}{\log X}$$

for all $X \ge 2$.

In Chapter 4, we gave the following modification on the definition of 2-dense:

Definition 6.23. A 2-dense number n is *strictly* 2-*dense* if $\frac{d_{i+1}}{d_i} < 2$ holds for all i satisfying $1 < i < \tau(n) - 1$.

We showed (cf. Lemma 5.4 in Chapter 4 that the strictly 2-dense integers have an important relationship with the φ-practical numbers:

Lemma 6.24. *Every strictly 2-dense number is φ-practical.*

Recall that we showed in Proposition 6.19 that there are infinitely many λ-practicals that are not φ-practical. We will use the lemmas on 2-dense and strictly 2-dense numbers in order to strengthen this result.

Theorem 6.25. *For X sufficiently large, there exists a positive constant c_5 such that $F_\lambda(X) - F(X) \ge c_5 \frac{X}{\log X}$.*

Proof. We begin by recalling an argument given in Chapter 4. Let $n = mpj$, where m is a 2-dense integer, p is a prime satisfying $m < p < 2m$, and j is an integer that has the following properties: $j \leq X/mp$, $P^-(j) > p$ and mpj is 2-dense. Let $C > 16$ be an integer that is chosen to be large relative to the size of the constant κ_1 from Lemma 6.22. For each integer $k > C$, we consider those 2-dense numbers $m \in (2^{k-1}, 2^k]$. Since $m < p < 2m$, we must have $p \in (2^{k-1}, 2^{k+1})$. We say that n has an *obstruction at* k if m and p land within these intervals, i.e., if p is a prime in our construction that might prevent n from being strictly 2-dense. In Theorem 5.11 in Chapter 4, we showed that, if C is large enough, the number of 2-dense integers with obstructions at $k > C$ is negligible relative to the full count of 2-dense integers. Thus, consider the set

$$\mathcal{N} = \{n \leq X : n \text{ is 2-dense with no obstructions at } k > C\}.$$

For an appropriate choice of $C \geq 5$, we have

$$\#\mathcal{N} \geq \kappa \frac{X}{\log X},$$

where $\kappa > 0$ is some absolute constant. As in Chapter 4, we define a function $f : \mathcal{N} \to \mathbb{Z}_+$ to be a function that maps each element $n \in \mathcal{N}$ to its largest 2-dense divisor with all prime factors less than or equal to 2^C. Let $\mathcal{M} = \mathrm{Im} f$. The Pigeonhole Principle guarantees that there is some $m_0 \in \mathcal{M}$ that has at least

$$\frac{\#\mathcal{N}}{\#\mathcal{M}} \geq \frac{\kappa}{4^{2^C}} \frac{X}{\log X}$$

elements in its preimage, since the Chebyshev bound (cf. [32, pg. 108]) implies that $\prod_{p \leq 2^C} p \leq 4^{2^C}$. In other words, $m_0 = f(n)$ for at least the average number of integers in a pre-image.

Now, for each $n \in \mathcal{N}$ with $f^{-1}(m_0) = n$, let

$$n' = \frac{15 \cdot 29^5}{\gcd(2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23, m_0)} \, n \prod_{\substack{29 < p \leq 2^C \\ p \text{ prime} \\ p \nmid m_0}} p.$$

Since n is 2-dense, it must be the case that $3 \mid n$, hence $3^2 \| n'$. Also, we must have $5 \| n'$, since if $5 \mid n$ then $5 \mid m_0$, so it is removed in the denominator of n'. Thus, the only 5 that appears in the factorization of n' is the one dividing 15. Now, n' does not have any other prime factors smaller than 29, since if n is divisible by a prime $q < 29$, then $q \mid m_0$, hence $q \mid \gcd(2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23, m_0)$. Thus, n' is not φ-practical, since the absence of small primes (aside from the divisors of 45) makes it so that $x^n - 1$ has no divisor of degree 22. However, we will show that n' is λ-practical. Now, let

$$l = n \prod_{\substack{29 < p \leq 2^C \\ p \text{ prime} \\ p \nmid m_0}} p.$$

Since n is 2-dense then $2 \mid n$. Moreover, if we enumerate the prime factors of l in increasing order, where p_i is the i^{th} smallest, then Bertrand's postulate implies that all of the primes p_i dividing l that are greater than 29 satisfy $p_{i+1} \leq 2p_i$. Thus, they satisfy the inequality given in Lemma 6.14 as well. Let

$$r = \frac{15 \cdot 29^5}{\gcd(2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23, m_0)},$$

so $n' = l \cdot r$. Multiplying l by r does not prevent the primes greater than or equal to 29 from satisfying the inequality from Lemma 6.14, since $29^5 > \frac{1}{3} \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$, so that $r > 1$. In other words, if a prime factor p of n' satisfies $p \leq m + 2$, then it is certainly the case that $p \leq mr + 2$. Thus, we have just shown that n' has the following structure: $n' = 45M$, where $P^-(M) = 29$ and all of the prime factors of $45M$ satisfy the inequality from Lemma

6.14. Since 45 is λ-practical, then Lemma 6.16 implies that n' is λ-practical. Now, since we multiplied every n in the pre-image of m_0 by the same number, there is a one-to-one correspondence between λ-practical numbers up to $r \cdot 4^{2^C} X$ that we have constructed and the 2-dense numbers in the pre-image of m_0. As a result, at least $\frac{\kappa}{4^{2^C}} \frac{X}{\log X}$ of the integers up to $r \cdot 4^{2^C} X$ are λ-practical. □

Note: By Lemma 6.15, all of the λ-practical numbers that we have constructed in the proof of Theorem 6.25 are weakly φ-practical. As a result, this argument also shows that, for X sufficiently large, there are $\gg \frac{X}{\log X}$ weakly φ-practicals in $[1, X]$ that are not φ-practical.

6.6 The relationship between λ-practical and p-practical numbers

Our next endeavor will be to describe the relationship between p-practical and λ-practical numbers. We begin with the following analogue of Lemma 6.15, which is proven in the same manner as its predecessor.

Lemma 6.26. *Let $n = mq$, where m is p-practical and q is a prime satisfying $\ell_p^*(q) \leq m+1$, with $(q, m) = 1$. Then n is p-practical. Moreover, if $n = mq^k$ where $k \geq 2$, then n is p-practical if $\ell_p^*(q) \leq m$.*

We can use Lemma 6.26 to prove our first result relating λ-practical and p-practical numbers:

Proposition 6.27. *For each prime p, there are infinitely many p-practicals that are not λ-practical.*

Proof. Case 1: If $p = 2$, let $n = 21 \cdot \prod_{7<q\leq x} q$. Since 21 is 2-practical and since each prime q_0 in the product over q satisfies the inequality $q_0 \leq \prod_{7<q<q_0} q + 2$, then n is 2-practical by Lemma 6.26. However, n is not λ-practical, since we cannot write 4 in the form $\sum_{d|n} \lambda(d) m_d$

with $0 \leq m_d \leq \frac{\varphi(d)}{\lambda(d)}$. Thus, by letting x tend to infinity, we see that this method will generate an infinite family of 2-practical numbers that are not λ-practical.

Case 2: For each prime $p \geq 3$,we will show that there exists a prime $q_0 \neq 3$ dividing $(p^2 + p + 1)$ and, for this q_0, the number $2 \cdot q_0$ is p-practical but not λ-practical. First, observe that if such a prime exists, then $q_0 \mid (p^2 + p + 1)$ implies that $p^3 \equiv 1 \pmod{q_0}$, i.e. $\ell_p^*(q_0) \leq 3$. Thus, since $m_0 = 2$ is p-practical for all primes p and $\ell_p^*(q_0) \leq m_0 + 1$, then $2 \cdot q_0$ is p-practical by Lemma 6.26. However, $2 \cdot q_0$ is not λ-practical, since $q_0 > 3$ implies that $\lambda(q_0) \geq 4$. Thus, we cannot write 3 in the form $\sum_{d|n} \lambda(d) m_d$, with $0 \leq m_d \leq \frac{\varphi(d)}{\lambda(d)}$.

Now, we will prove the existence of a prime q_0 satisfying the conditions given above. The argument boils down to proving that $p^2 + p + 1$ is not a power of 3. In the case where $p = 3$, we have $p^2 + p + 1 = 13$. Suppose that $p > 3$. Then, it must be the case that $p \equiv \pm 1 \pmod 3$. If $p \equiv -1 \pmod 3$, then $p^2 + p + 1 \equiv 1 \pmod 3$, so $p^2 + p + 1$ is not divisible by 3. On the other hand, if $p \equiv 1 \pmod 3$ then, if $p^2 + p + 1$ were a power of 3, the fact that $p > 3$ forces $p^2 + p + 1$ to be divisible by 9. However, the congruence $x^2 + x + 1 \equiv 0 \pmod 9$ has no solutions. □

We remark that we could also have proven the second case in Proposition 6.27 using the following lemma:

Lemma 6.28. *If $n = p^k$ with $k \geq 0$, then n is p-practical.*

Proof. Let $n = p^k$, with $k \geq 0$. Using the binomial theorem, we have $x^{p^k} - 1 = (x-1)^{p^k}$ in $\mathbb{F}_p[x]$. Hence, $x^n - 1$ has a divisor of every degree, so n is p-practical. □

In order to generate an infinite family of p-practical numbers when $p \geq 5$, we could simply have taken $n = p^k$, where k ranges over all positive integers. By Lemma 6.28, n is p-practical. However, when p is in this range, we have $\lambda(p) = p - 1 \geq 4$. In other words, the gap between 1 and $\lambda(p)$ is too large for p^k to be p-practical. In the case where $p = 3$, we can take $n = p^k$ with $k \geq 2$. Then 4 cannot be written in the form $\sum_{d|n} \lambda(d) m_d$ with $0 \leq m_d \leq \frac{\varphi(d)}{\lambda(d)}$.

For each rational prime p, let $F_p(X) = \#\{n \leq X : n \text{ is } p\text{-practical}\}$. We can prove the following theorem on the relative sizes of the sets of p-practical and λ-practical numbers.

Theorem 6.29. *For every rational prime p, there exists a positive constant c_6 such that $F_p(X) - F_\lambda(X) \geq c_6 \frac{X}{\log X}$.*

Proof. This proof is nearly identical to the proof of Theorem 6.25. The main difference is in our construction of n', which varies depending on our choice of p. If $p = 2$, we let

$$n' = \frac{7^2}{\gcd(10, m_0)} \, n \prod_{\substack{7 < q \leq 2^C \\ q \nmid m_0}} q,$$

where C, m_0 and n are defined as in the proof of Theorem 6.25. Then n' is of the form $n' = 21 \cdot m$, where $P^-(m) \geq 7$ and the primes dividing m satisfy the weakly φ-practical conditions. Note that 21 is not λ-practical. Thus, since all of the prime factors of m are at least 7, it follows that n' is not λ-practical. To get the stated result when $p = 2$, we use Lemma 6.26 in place of Lemma 6.15 to show that each n' is 2-practical.

The arguments for $p \geq 3$ follow the same line of reasoning. In the case where $p = 3$, we define

$$n' = \frac{13^4}{\gcd(3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, m_0)} \, n \prod_{\substack{13 < q \leq 2^C \\ q \nmid m_0}} q.$$

In the case where $p \geq 5$, we let

$$n' = \frac{2p^2}{\gcd(6p, m_0)} \, n \prod_{\substack{p < q \leq 2^C \\ q \nmid m_0}} q.$$

□

6.7 Proof of Theorem 6.4

In this section, we present a proof of Theorem 6.4. We shall begin by discussing a few simple lemmas, which will be needed in order to complete the argument. Let n be a positive integer, with $d_1 < d_2 < \cdots < d_{\tau(n)}$ its increasing sequence of divisors. Let $Z \geq 2$. We say that n is Z-dense if $\max_{1 \leq i \leq \tau(n)} \frac{d_{i+1}}{d_i} \leq Z$ holds. The following lemma, due to Saias (cf. [34, Theorem 1]), describes the count of integers with Z-dense divisors.

Lemma 6.30 (Saias)**.** *For $X \geq Z \geq 2$, we have*

$$\#\{n \leq X : n \text{ is } Z\text{-dense}\} \ll \frac{X \log Z}{\log X}. \tag{6.3}$$

The following lemma, due essentially to Friedlander, Pomerance and Shparlinski (cf. [14, Lemma 2]), will also be useful to us.

Lemma 6.31. *Let n and d be positive integers with $d \mid n$. Then, for any rational prime p, we have $\frac{d}{\ell_p^*(d)} \leq \frac{n}{\ell_p^*(n)}$.*

Proof. The result is proven in [14] when $(p, n) = 1$. In the case where $(p, n) > 1$, let $n_{(p)}$ and $d_{(p)}$ represent the largest divisors of n and d that are coprime to p, respectively. Then

$$\frac{d}{d_{(p)}} \leq \frac{n}{n_{(p)}},$$

since the highest power of p dividing d is at most the highest power of p dividing n. After a rearrangement, we have

$$\frac{d}{n} \leq \frac{d_{(p)}}{n_{(p)}} \leq \frac{\ell_p^*(d)}{\ell_p^*(n)},$$

where the final inequality follows from the coprime case. □

We will also need to introduce several additional lemmas from [25]. Throughout the remainder of this section, let $a > 1$ be an integer and let A_q denote the set of primes $p \equiv 1 \pmod{q}$ with $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$.

Lemma 6.32 (Li, Pomerance)**.** *Let $\psi(X)$ be an arbitrary function for which $\psi(X) = o(X)$ and $\psi(X) \geq \log\log X$. The number of integers $n \leq X$ divisible by a prime $p > \psi(X)$ with $\ell_a^*(p) < \frac{p^{1/2}}{\log p}$ is $O(\frac{X}{\log \psi(X)})$.*

Lemma 6.33 (Li, Pomerance)**.** *The number of integers $n \leq X$ divisible by a prime $p \equiv 1 \pmod{q}$ with*

$$\frac{q^2}{4\log^2 q} < p \leq q^2 \log^4 q$$

is $O(\frac{X \log\log q}{q \log q})$.

Below, we present a version of Proposition 1 in Li and Pomerance's paper [25]. As in [25], our lemma will make use of Lemma 5.5; thus, it will depend on the validity of the Generalized Riemann Hypothesis.

Lemma 6.34. *(GRH) Let a be a positive integer. Let $\psi(X)$ be defined as in Lemma 6.32. The number of integers $n \leq X$ with $P(\frac{\lambda(n)}{\ell_a^*(n)}) \geq \psi(X)$ is $O(\frac{X \log\log \psi(X)}{\log \psi(X)})$.*

Proof. Suppose that $n \leq X$ and $q = P(\lambda(n)/\ell_a^*(n)) \geq \psi(X)$. We may assume that X is large, so a is not a q^{th} power and $\psi(X) > a$. Moreover, as we will now show, it must be the case that either $q^2 \mid n$ or $p \mid n$ for some $p \in A_q$. Observe that

$$q \mid \frac{\lambda(n)}{\ell_a^*(n)} \mid \frac{\operatorname{lcm}_{p^e||n}[\lambda(p^e)]}{\operatorname{lcm}_{p^e||n}[\ell_a^*(p^e)]} \mid \operatorname{lcm}_{p^e||n}\left[\frac{\lambda(p^e)}{\ell_a^*(p^e)}\right].$$

In particular, q must divide $\frac{\lambda(p^e)}{\ell_a^*(p^e)}$ for some prime p. If $q = p$, then $q \mid \lambda(p^e)$ implies that $e \geq 2$, so $q^2 \mid n$. If $q \neq p$, then $q \mid \frac{\lambda(p)}{\ell_a^*(p)}$, so $p > q > \psi(X) > a$. Thus, $\ell_a^*(p) = \ell_a(p) \mid \frac{p-1}{q}$, so $p \mid a^{\frac{p-1}{q}} - 1$, which implies that $p \in A_q$.

To handle the case where $q^2 \mid n$, we observe that

$$\begin{aligned}\#\{n \leq X : q^2 \mid n \text{ for some prime } q \geq \psi(X)\} &\leq \sum_{\substack{q \geq \psi(X) \\ q \text{ prime}}} \left\lfloor \frac{X}{q^2} \right\rfloor \\ &\leq X \sum_{\substack{q \geq \psi(X) \\ q \text{ prime}}} \frac{1}{q^2} \ll \frac{X}{\psi(X)}.\end{aligned}$$

Thus, we may assume that n is divisible by a prime $p \in A_q$ with $p > a$.

By Lemma 6.32, we may assume that $\ell_a^*(p) \geq p^{1/2}/\log p$. However, since $p \in A_q$ implies that $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$, then $\ell_a(p) \leq \frac{p-1}{q}$, so $p > \frac{q^2}{(4\log^2 q)}$. Thus, we can use Lemmas 6.33 and 5.5 to deal with the remaining values of $n \leq X$. In particular, we have

$$\#\{n \leq X : p \mid n \text{ for some } p \in A_q \text{ with } p > q^2/(4\log^2 q)\} \tag{6.4}$$

$$\leq \#\{n \leq X : p \mid n \text{ for some } p \equiv 1 \pmod{q} \text{ with } p \in (\frac{q^2}{4\log^2 q}, q^2\log^4 q]\} \tag{6.5}$$

$$+ \#\{n \leq X : p \mid n \text{ for some } p \in A_q \text{ with } p \geq q^2\log^4 q\} \tag{6.6}$$

$$\ll \frac{X\log\log q}{q\log q} + \frac{X}{q\log q} + \frac{X\log\log X}{q^2}, \tag{6.7}$$

where the final inequality follows from Lemmas 6.33 and 5.5. Since our hypotheses specify that $q \geq \psi(X)$, then the bound given in (6.7) implies

$$\begin{aligned}
&\#\{n \leq X : q \geq \psi(X) \text{ and } p \mid n \text{ for some } p \in A_q\} \\
&\ll X \sum_{q \geq \psi(X)} \left(\frac{\log\log q}{q\log q} + \frac{\log\log X}{q^2} \right) \\
&\ll \frac{X\log\log\psi(X)}{\log\psi(X)}.
\end{aligned}$$

□

We will use Lemma 6.34 in order to prove the following.

Lemma 6.35. *(GRH) Let θ be a constant satisfying $\frac{1}{10} \leq \theta \leq \frac{9}{10}$. Let $Y = e^{110(\log X)^\theta(\log\log X)^2}$. For all $a > 1$ and X sufficiently large, uniformly in θ, we have*

$$\#\{n \leq X : \ell_a^*(n) \leq \frac{X}{Ye^{(\log X)^\theta}}\} \ll \frac{X}{(\log X)^\theta \log\log X}. \tag{6.8}$$

Before we prove Lemma 6.35, we will introduce three additional lemmas, the first of which is due to Friedlander, Pomerance and Shparlinski [14] and the last of which is due to

Luca and Pollack [26].

Lemma 6.36. *For sufficiently large numbers X and for $\Delta \geq (\log\log X)^3$, the number of positive integers $n \leq X$ with*

$$\lambda(n) \leq n \exp(-\Delta)$$

is at most $X \exp(-0.69(\Delta \log \Delta)^{1/3})$.

Corollary 6.37. *Let θ be as in Lemma 6.35. For sufficiently large X, the number of positive integers $n \leq X$ with*

$$\lambda(n) \leq \frac{X}{e^{(\log X)^\theta}}$$

is at most $X/e^{(\log X)^{\theta/3}}$.

Proof. Trivially, there are at most $X/\exp((\log X)^{\theta/2})$ values of $n \leq X/\exp((\log X)^{\theta/2})$ with $\lambda(n) \leq X/\exp((\log X)^\theta)$. On the other hand, if $X/\exp((\log X)^{\theta/2}) < n \leq X$, then $X \leq n \exp((\log X)^{\theta/2})$. Thus, for large X, we have

$$\begin{aligned} \# \left\{ \frac{X}{e^{(\log X)^{\theta/2}}} < n \leq X : \lambda(n) \leq \frac{X}{e^{(\log X)^\theta}} \right\} &\leq \# \left\{ n \leq X : \lambda(n) \leq \frac{n e^{(\log X)^{\theta/2}}}{e^{(\log X)^\theta}} \right\} \\ &< \# \left\{ n \leq X : \lambda(n) \leq \frac{n}{e^{\frac{1}{2}(\log X)^\theta}} \right\}. \end{aligned}$$

Applying Lemma 6.36 with $\Delta = \frac{1}{2}(\log X)^\theta$, we see that this quantity is at most $X/\exp(2(\log X)^{\theta/3})$. Therefore,

$$\# \left\{ n \leq X : \lambda(n) \leq \frac{X}{e^{(\log X)^\theta}} \right\} \leq \frac{X}{e^{(\log X)^{\theta/2}}} + \frac{X}{e^{2(\log X)^{\theta/3}}} \leq \frac{X}{e^{(\log X)^{\theta/3}}}.$$

□

Lemma 6.38. *But for $O(\frac{X}{(\log X)^3})$ choices of $n \leq X$, we have*

$$\Omega(\varphi(n)) < 110(\log\log X)^2.$$

We will use these lemmas in the proof of Lemma 6.35, which we present below.

Proof. Let θ be such that $\frac{1}{10} \leq \theta \leq \frac{9}{10}$, let $B = e^{(\log X)^\theta}$ and let $u(n)$ denote the B-smooth part of $\lambda(n)$. Let Y be defined as in the statement of Lemma 6.35. If $\lambda(n)$ has a large B-smooth part, say $u(n) > Y$, then so does $\varphi(n)$, since $u(n)$ must divide $\varphi(n)$ as well. First, we will estimate the number of $n \leq X$ for which $u(n) > Y$. Let $\Omega(u(n)) = k$. By definition, all prime factors of $u(n)$ are at most $e^{(\log X)^\theta}$. Thus, we have

$$Y < u(n) \leq (e^{(\log X)^\theta})^k.$$

Solving for k, we obtain $k \geq 110(\log\log X)^2$. However, Lemma 6.38 implies that $k < 110(\log\log X)^2$ except for $O(\frac{X}{(\log X)^3})$ values of $n \leq X$. Hence, we can conclude that there are at most $O(\frac{X}{(\log X)^3})$ values of n for which the B-smooth part of $\lambda(n)$ is larger than Y. Thus, using Lemma 6.37, we have

$$\begin{aligned}\#\{n \leq X : \frac{\lambda(n)}{u(n)} \leq \frac{X}{Ye^{(\log X)^\theta}}\} &\leq \#\{n \leq X : \lambda(n) \leq \frac{X}{e^{(\log X)^\theta}}\} + \#\{n \leq X : u(n) > Y\} \\ &\ll \frac{X}{e^{(\log X)^{\theta/3}}} + \frac{X}{(\log X)^3}.\end{aligned}$$

However, if we take $\psi(X) = Y\exp\{(\log X)^\theta\}$ then we can use Lemma 6.34 to show that, for all but $O(\frac{X}{(\log X)^\theta \log\log X})$ choices of $n \leq X$, we have $\frac{\lambda(n)}{u(n)} \mid \ell_a^*(n)$. Therefore, we have

$$\ell_a^*(n) \geq \frac{\lambda(n)}{u(n)} > \frac{X}{Ye^{(\log X)^\theta}},$$

except for at most $O(\frac{X}{(\log X)^\theta \log\log X})$ values of $n \leq X$. □

We will need the following elementary lemma in order to complete our argument.

Lemma 6.39. *Let $X \geq 2$ and let $\kappa \geq 1$. Then, we have*

$$\#\{n \leq X : \tau(n) \geq \kappa\} \ll \frac{1}{\kappa} X \log X.$$

Proof. We observe that

$$\sum_{n \leq X} \tau(n) = \sum_{n \leq X} \sum_{d|n} 1 \leq X \sum_{d \leq X} \frac{1}{d} \ll X \log X.$$

The number of terms in the sum on the left-hand side of the equation that are $\geq \kappa$ is $\ll \frac{1}{\kappa} X \log X$. □

Now we have the tools needed to prove Theorem 6.4. Below, we present its proof.

Proof. Let n be a positive integer with divisors $d_1 < d_2 < \cdots < d_{\tau(n)}$. Let p be a rational prime with $p \nmid n$. Let θ and Y be as in Lemma 6.35. In (6.3), set $Z = Y^2$. Assume that n is not in the set of size $O(X \log Y^2 / \log X)$ of integers with Y^2-dense divisors. Then there exists an index j with

$$\frac{d_{j+1}}{d_j} > Y^2. \tag{6.9}$$

Moreover, we can use Lemma 6.39 to show that

$$\#\{n \leq X : \tau(n) > Y/e^{(\log X)^\theta}\} \ll \frac{X e^{(\log X)^\theta} \log X}{Y}. \tag{6.10}$$

As a result, we will assume hereafter that $\tau(n) \leq Y/e^{(\log X)^\theta}$. Examining the ratios $\frac{d_{k+1}}{d_k}$, we remark that it is always the case that $d_1 = 1$ and $d_2 = P^-(n)$; hence, we have

$$\#\{n \leq X : \frac{d_2}{d_1} > Y^2\} = \sum_{\substack{n \leq X \\ P^-(n) > Y^2}} 1 \ll X \prod_{q \leq Y^2} \left(1 - \frac{1}{q}\right),$$

where the final inequality follows from applying Brun's Sieve (cf. [18, Theorem 2.2]). By Mertens' Theorem (cf. [32, Theorem 3.15]), we have

$$X \prod_{q \leq Y^2} \left(1 - \frac{1}{q}\right) \ll \frac{X}{\log Y}. \tag{6.11}$$

Now, suppose that $k > 1$. On one hand, for all $k > 1$, we have

$$1 + \sum_{l \leq k} \ell_p^*(d_l) \frac{\varphi(d_l)}{\ell_p^*(d_l)} = 1 + \sum_{l \leq k} \varphi(d_l) \leq k d_k \leq Y e^{-(\log X)^\theta} d_k. \tag{6.12}$$

On the other hand, Lemma 6.35 implies that $\ell_p^*(n) > \frac{X}{Y e^{(\log X)^\theta}}$ but for

$$O\left(\frac{X}{(\log X)^\theta \log\log X}\right) \tag{6.13}$$

integers $n \leq X$. For such numbers n, for all $i \geq 1$, we have

$$\ell_p^*(d_{j+i}) \geq \frac{\ell_p^*(n) d_{j+i}}{n} > \frac{d_{j+i}}{Y e^{(\log X)^\theta}} > \frac{d_j Y^2}{Y e^{(\log X)^\theta}} = Y e^{-(\log X)^\theta} d_j \tag{6.14}$$

where the inequalities follow, respectively, from Lemma 6.31, Lemma 6.35 and the assumption that there exists an index j for which (6.9) holds. As a result, we can combine the inequality from (6.12) applied with $k = j$ with(6.14) to show that

$$1 + \sum_{l \leq j} \ell_p^*(d_l) \frac{\varphi(d_l)}{\ell_p^*(d_l)} < \ell_p^*(d_{j+i})$$

holds for all $i \geq 1$. Thus, $x^n - 1$ has no divisor of degree $1 + \sum_{l \leq j} \varphi(d_l)$ in $\mathbb{F}_p[x]$, so n is not p-practical. Therefore, by (6.3), (6.10), (6.11) and (6.13), we have

$$F_p(X) \ll \frac{X \log Y}{\log X} + \frac{X e^{(\log X)^\theta} \log X}{Y} + \frac{X}{\log Y} + \frac{X}{(\log X)^\theta \log\log X}. \tag{6.15}$$

Now, the only significant terms in (6.15) are $\frac{X}{(\log X)^\theta \log\log X}$ and $\frac{X \log Y}{\log X}$. Equating these expressions and using the fact that $Y = e^{110(\log X)^\theta (\log\log X)^2}$, we obtain $\theta = \frac{1}{2} - \frac{3 \log_3 X}{2 \log_2 X}$ as a good choice for θ. Plugging this value of θ into the bound $\frac{X}{(\log X)^\theta \log\log X}$ yields a bound of $O\left(X\sqrt{\frac{\log\log X}{\log X}}\right)$ for the size of the set of p-practicals up to X. □

Appendix A

Appendix: Algorithms for Computations

A.1 Theoretical Framework

The following theorem can be used to devise the most basic algorithms for checking whether an integer is practical, φ-practical, p-practical, etc.

Theorem A.1. *Let $w_1 \leq w_2 \leq \cdots \leq w_k$ be positive integers with $\sum_{i=1}^{k} w_i = s$. Then, every integer in $[1, s]$ can be represented as a subsum of w_i's if and only if for each $i < k$, we have $w_{i+1} \leq 1 + w_1 + \cdots + w_i$.*

Proof. Suppose that $w_{i+1} > 1 + w_1 + \cdots + w_i$ for some $i < k$. Then $1 + w_1 + \cdots + w_i$ cannot be represented as a subsum of w_i's. Since $i < k$ then $1 + w_1 + \cdots + w_i < s$, so not every integer in $[1, s]$ can be written in this manner. On the other hand, suppose that for each $i < k$ we have $w_{i+1} \leq 1 + w_1 + \cdots + w_i$. We proceed by induction on k. For our base case, we take $k = 1$ and then $w_1 = 1$. Then $s = 1$ and it is trivially the case that every integer in $[1, s]$ can be represented as a subsum of w_i's. Now, for $k > 1$, suppose that we can make

all subsums up to $w_1 + \cdots + w_{k-1}$. If $w_k \leq 1 + w_1 + \cdots + w_{k-1}$, then the interval $[1, w_k)$ is covered by subsums of $w_1, ..., w_{k-1}$ and the interval $[w_k, w_1 + \cdots + w_{k-1} + w_k]$ is covered by w_k+ subsums of $w_1, ..., w_{k-1}$. Thus, we can make all subsums up to $w_1 + \cdots + w_k = s$. $\square$

If $d_1 < d_2 < \cdots < d_k$ represents the increasing sequence of divisors of an integer n, then Theorem A.1 says that every integer in $[1, \sigma(n)]$ can be represented as a subsum of d_i's if and only if for each $i < k$, we have $d_{i+1} \leq 1 + d_1 + \cdots + d_i$. Similarly, we can let $w_1 \leq w_2 \leq \cdots \leq w_k$ represent the increasing sequence of totients of divisors of an integer n and use Theorem A.1 to obtain an algorithm for determining whether n is φ-practical.

A.2 Algorithm for computing $F(X)$

In this section, we describe our algorithm for computing the data in Table A.1. The most naive algorithm for determining whether a positive integer n is φ-practical makes use of Theorem A.1. The idea is to start with a sorted list of the totients of divisors of n: $[w_1, w_2, ..., w_{\tau(n)}]$, where $w_1 \leq w_2 \leq \cdots \leq w_{\tau(n)}$. The algorithm starts at the beginning of the list and, for each index i, checks whether

$$w_i \leq w_1 + \cdots + w_{i-1} + 1. \tag{A.1}$$

If this inequality fails at any value of i between 1 and $\tau(n)$, the program halts and returns '0' to signify that n is not φ-practical. Otherwise, the program returns '1', which indicates that n is φ-practical. Unfortunately, this method is not particularly efficient, especially when we attempt to count the φ-practical numbers in $[1, X]$ for large values of X.

To speed up the process of counting the φ-practical numbers, we use a series of tests that help us quickly eliminate the numbers that are poor candidates for being φ-practical. First, we observe that for n to be φ-practical, it must be divisible by 2 or 3; otherwise, there is no way to express 2 as a sum of totients of divisors of n. As a result, we can immediately dismiss all integers n with $\gcd(n, 6) = 1$. Moreover, we can use the weakly φ-practical condition

given in chapter 4 in order to remove some additional candidates from our consideration, since Theorem 6.14 tells us that every φ-practical number must be weakly φ-practical. In fact, we can go on to use the weakly φ-practical condition for a second purpose: namely, to detect all of the even φ-practical numbers (recall that Proposition 6.17 tells us that even integers n are weakly φ-practical if and only if they are φ-practical as well). Thus, after applying the weakly φ-practical condition, we are left with only the odd integers that pass the weakly φ-practical test.

Next, we devise a test that we call the *strongly φ-practical* test. The strongly φ-practical test starts with a list of ordered pairs $[(p_1, e_1), (p_2, e_2), ..., (p_{\omega(n)}, e_{\omega(n)})]$, where $p_1 < p_2 < \cdots < p_{\omega(n)}$ are distinct prime factors of n and $e_1, ..., e_{\omega(n)}$ are the corresponding exponents. As we move through the list of pairs, the strongly φ-practical test performs one of two tasks at each index i:

1) If $e_i = 1$, then the test checks whether the weakly φ-practical condition is satisfied. If it fails, then n cannot be φ-practical.

2) If $e_i > 1$, then the test checks whether p_i satisfies the following inequality:

$$p_i \leq \prod_{j<i} p_j^{e_j} - 2.$$

The strongly φ-practical test arises from applying Lemma 4.9 to odd integers. Namely, Lemma 4.9 tells us that if $n = p^k m$ where $k \geq 2$ and m is φ-practical, then $p \leq m+1$ if and only if n is φ-practical. Since the weakly φ-practical test handles all even values of n, we will only apply the strongly φ-practical condition to odd values of n. However, if n is odd, then p and m are both odd and $m+1$ is even. Thus, in order to apply Lemma 4.9, we only need $p \leq m$. Furthermore, since m is composite, then it is not possible to have $p = m$; as a result, we may assume that $p \leq m - 2$. In the case where $k = 1$, Lemma 4.9 states that the weakly φ-practical condition provides a necessary-and-sufficient condition for mp to be φ-practical.

In our algorithm, if n passes the strongly φ-practical test for all of its ordered pairs

(p_i, e_i), then n is φ-practical. If not, then the strongly φ-practical test is inconclusive, in which case we must apply the naive algorithm to check, once and for all, whether n is φ-practical. Fortunately, by the time that we get around to using the naive algorithm, we have already eliminated a large proportion of the integers between 1 and X from consideration. If $G(X)$ represents the number of integers that are determined to be φ-practical before the program passes to the naive algorithm, then, the following table demonstrates the relationship between $F(X)$ and $G(X)$:

X	$F(X)$	$G(X)$	$F(X) - G(X)$
10^2	28	28	0
10^3	174	166	8
10^4	1198	1148	50
10^5	9301	8716	585
10^6	74461	69972	4489
10^7	635528	598156	37372
10^8	5525973	5168593	357380
10^9	48386047	45131358	3254689

Table A.1: Comparison of φ-practical counts

As one can extrapolate from the column on the right, the φ-practicals that are ultimately detected via the naive algorithm only account for between 4% and 7% of the total number of φ-practicals in each interval.

In what follows, we present the Sage code used in our computations of $F(X)$. First, we write a program that takes an integer n as input and generates a list of ordered pairs of prime factors of n with their exact powers:

```
def factor_list(n):
    f = factor(n)
    return list(f)
```

Note that the output of this function is of the form $[(p_1, e_1), (p_2, e_2), ..., (p_{\omega(n)}, e_{\omega(n)}]$, where $p_1 < p_2 < \cdots < p_{\omega(n)}$. Next, we define the weakly φ-practical function, which takes

an integer n as input and checks whether the weakly φ-practical condition is satisfied. The function returns 1 if n is weakly φ-practical and 0 otherwise.

```
def weakly_phi_practical(n):
    prod=1 #initialize the product at 1
    v=factor_list(n) #set v as the factor list of n
    for k in xrange(0, len(v)): #run over each index in v
        for i in xrange(0,k): #for each value of i < k
            prod*=v[i][0]^(v[i][1])
            #multiply the previous product by p_i^e_i
        if v[k][0] > prod +2: #if p_k fails weak condition
            return 0 #halt and return 0
        prod=1 #reset product to 1 and test the next value of k
    return 1 #return 1 if every value of k satisfies the inequality
```

Next, we define the strongly φ-practical function, which takes an integer n as input and checks whether it satisfies the strongly φ-practical criteria.

```
def strongly_phi_practical(n):
    prod=1 #initialize the product to be 1
    v=factor_list(n) #set v as factor list of n
    for k in xrange(0, len(v)): #run over each index in v
        for i in xrange(0,k): #for each value of i <k
            prod*=v[i][0]^(v[i][1])
            #multiply the previous product by p_i^e_i
        if v[k][1] == 1: #if e_k = 1
            if v[k][0] > prod +2: #if p_k fails weak condition
                return 0 #halt and return 0
        prod=1 #otherwise, reset the product to 1
```

```
        if v[k][1] > 1: #if e_k > 1
            if v[k][0] > prod -2: #if p_k fails strong condition
                return 0 #halt and return 0
            prod=1 #reset the product to 1 and test next value of k
        return 1 #return 1 if every value of k passes the test
```

We define the following helper function, which creates a list of totients of divisors of an integer, listed in increasing order.

```
def increasing_totients(n):
    v=divisors(n) #set v to be the increasing list of divisors of n
    w = [] #initialize w to be the empty list
    for k in xrange(0, len(v)): #run over each index d_k in v
        w.append(euler_phi(v[k])) #add phi(d_k) to w
    return sorted(w) #sort w with totients in increasing order
```

We use all of the previous functions in order to devise the following test, which takes an integer n as input and returns 1 if it is φ-practical and 0 otherwise.

```
def phi_practical(n):
    sum=0 #initialize the sum to be 0
    v=increasing_totients(n) #set v as list of increasing totients
    if gcd(n,6) == 1:
        return 0 #return 0 if (n, 6) = 1
    else:
        if weakly_phi_practical(n) == 0:
            return 0 #return 0 if n is not weakly phi-practical
        else:
            if n % 2 == 0:
                return 1
```

```
                #return 1 if n is even and weakly phi-practical
            else:
                if strongly_phi_practical(n) == 1:
                    return 1 #return 1 if n is strongly phi-practical
                else:
                    for k in xrange(0, len(v)):
                    #run over each index in v
                        sum=0 #initialize the sum to be 0
                        for i in range(0,k):
                            sum=sum + v[i] #add phi(d_i) to previous sum
                        if v[k] > sum + 1: #check naive condition
                            return 0 #return 0 if it fails
    return 1
```

Finally, we use a simple counter in order to compute $F(X)$. Our function takes an integer n as input and returns the number of φ-practicals in $[1, n]$.

```
def count_phi_practical(n):
    c = 1
    for i in xrange(2,n+1):
        if phi_practical(i)==1:
            c = c+1
    return c
```

A.3 Algorithm for computing $F_p(X)$

Here, we discuss the methods used to compute the data in Tables 1.2 – 1.4. We will describe the algorithm used for $F_2(X)$, but it should be noted that the algorithms for $F_3(X)$ and $F_5(X)$ are completely analogous.

We begin by generating a list of the odd part of each divisor of n; that is, for each $d \mid n$, we include $d' = d/2^{\nu_2(d)}$ in our list, where $\nu_2(d)$ represents the exact power of 2 that divides d. Next, we construct a list of ordered pairs $(\ell_2(d'), \varphi(d)/\ell_2(d'))$, where each d' comes from our list of the odd parts of divisors of n. We sort this list of ordered pairs so that they appear in increasing order according to their first components. If two pairs have identical first components, they will be sorted according to their second components. Call this list v and let $v[i][0]$ and $v[i][1]$ represent the first and second components of the i^{th} entry in the list, respectively.

The method for checking whether a number n is 2-practical will thus be to first use the algorithm outlined in the previous section to check if n is φ-practical; if it is, then n is automatically 2-practical. If not, then we go through our list v and check whether each component $v[i][0]$ satisfies $v[i][0] \leq 1 + \sum_{j<i} v[i][0] * v[i][1]$. If this inequality fails for any ordered pair in v, then n is not 2-practical; otherwise, n is included in our count of 2-practicals.

Below, we list the code for our sage computations. Our first order of business is to generate a list of the odd divisors of n.

```
def odd_part(n):
    return n/(2**(valuation(n,2))) #returns the odd part of an integer n

def odd_list(n):
    v=divisors(n) #sets v as the list of divisors of n
    w = [] #initializes w as the empty list
    for k in xrange(0, len(v)): #runs over each index of v
        w.append(odd_part(v[k]))
        #appends the odd part of d_k to w
    return w #returns a list of odd parts of divisors of n
```

Next, we define a function that takes an integer n as input and returns a list of $\ell_2(d)$'s, where the d's range over all odd divisors of n.

```
def orders(n):
    v=odd_list(n) #sets v as the list of odd divisors of n
    w = [] #initializes w as the empty list
    for k in xrange(0, len(v)): #runs over each index of v
        w.append(multiplicative_order(mod(2,v[k])))
        #appends ell_2(d_k) to w
    return w
```

We need both the orders $\ell_2(d)$ and their corresponding multiplicities, $\varphi(d)/\ell_2(d)$, in order to check whether an integer n is 2-practical. The following function computes the list of multiplicities that correspond to $\ell_2(d)$, where d ranges over all divisors of n.

```
def multiplicity_list(n):
    v=divisors(n) #sets v as the list of divisors of n
    w=orders(n) #sets w as the list of orders of odd divisors of n
    x = [] #initializes x as the empty list
    for k in xrange(0, len(v)): #runs over each index of v
        x.append(euler_phi(v[k])/w[k])
        #appends ell_2(d_k)'s multiplicity to x
    return x
```

Next, we construct a list of ordered pairs $(\ell_2(d), \varphi(d)/\ell_2(d))$ where the tuples are listed in increasing order by component. That is, we sort the tuples according to their first component and, if two tuples have identical first component, we sort them so that the second components appear in increasing order.

```
def ordmult_list(n):
    v=orders(n) #sets v as the list of orders of divisors of n
    w=multiplicity_list(n) #sets w as the list of multiplicities
    x = [] #initializes x as the empty list
```

```
    for k in xrange(0, len(v)): #runs over each index of v
        x.append((v[k], w[k]))
        #appends (ell_p(d_k), phi(d_k)/ell_p(d_k)) to x
    return sorted(x, key=lambda tup: tup[0])
    #sorts the list of tuples by component
```

The following function takes a tuple and multiplies its entries.

```
def tuple_prod(v): return v[0]*v[1]
```

Next, we borrow a function from section A.2 that constructs a list of increasing totients of divisors of an integer n.

```
def increasing_totients(n):
    v=divisors(n) #sets v as the list of divisors of n
    w = [] #initializes w as the empty list
    for k in xrange(0, len(v)): #runs over each index of v
        w.append(euler_phi(v[k])) #appends phi(d_k)
    return sorted(w) #sorts totients in increasing order
```

The following function uses the naive algorithm described in section A.2 in order to check whether an input n is φ-practical.

```
def naive_phi_practical(n):
    sum=0 #initializes the sum at 0
    v=increasing_totients(n) #sets v as the list of increasing totients
    for k in xrange(0, len(v)): #runs over each index of v
        sum=0 #initializes the sum at 0
        for i in xrange(0,k): $runs over each i < k
            sum=sum + v[i] #adds the ith totient to previous sum
        if v[k] > sum + 1:
```

```
            return 0 #returns 0 if naive test fails
    return 1 #returns 1 if naive test never fails
```

We are finally equipped to construct a function that determines whether an input n is 2-practical.

```
def two_practical(n):
    if naive_phi_practical(n) == 1:
        return 1 #returns 1 if n is phi-practical
    else:
        sum=0 #initializes the sum at 0
        v=ordmult_list(n) #sets v as the list of tuples
        for k in xrange(0, len(v)): #runs over each index of v
            sum=0 #initializes the sum at 0
            for i in xrange(0,k):
                sum=sum + tuple_prod(v[i])
                #adds the product of the two components in the kth tuple
                #to the previous sum
            if v[k][0] > sum + 1:
                return 0 #returns 0 if naive 2-practical test fails
        return 1 #returns 1 if naive 2-practical test never fails
```

As in section A.2, we can use a simple counter to keep track of the number of 2-practicals as we loop over all integers in a given range.

```
def count_two_practical(n):
    c = 1
    for i in xrange(2,n+1):
        if two_practical(i)==1: c = c+1
    return c
```

Bibliography

[1] G. Bachman, *On the coefficients of ternary cyclotomic polynomials*, J. Number Theory **100** (2003), 104 – 116.

[2] G. Bachman, *Flat cyclotomic polynomials of order three*, Bull. London Math. Soc. **38** (2006), 53 – 60.

[3] A.S. Bang, *Om Ligningen* $\Phi_n(x) = 0$, Nyt Tidsskrift for Mathematik (B) **6** (1895), 6 – 12.

[4] P. T. Bateman, *Note on the coefficients of the cyclotomic polynomials*, Bull. Amer. Math. Soc. **55** (1949), 1180 – 1181.

[5] P. T. Bateman, C. Pomerance, and R. C. Vaughan, *On the size of the coefficients of the cyclotomic polynomial*, Colloq. Math. Soc. Janos Bolyai **34** (1984), 171 – 202.

[6] B. Bzdega, *Bounds on ternary cyclotomic coefficients*, Acta Arith. **144** (2010), no. 1, 5 –16.

[7] M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial* $F_{pqr}(x)$, Amer. Math. Monthly **75** (1968), 370 – 372.

[8] M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial* $F_{pqr}(x)$. *II*, Duke Math. J. **38** (1971), 591 – 594.

[9] D. M. Bloom, *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly **75** (1968), 372 – 377.

[10] D. Dummit, R. Foote, *Abstract algebra*. John Wiley & Sons, Inc., USA, 2004.

[11] P. Erdős, *On the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **52** (1946), 179 – 184.

[12] P. Erdős, *On a Diophantine equation*, Mat. Lapok **1** (1950), 192 – 210.

[13] P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael's lambda function*, Acta Arith. **58** no. 4 (1991), 363 – 385.

[14] J. Friedlander, C. Pomerance, and I. E. Shparlinski, *Period of the power generator and small values of the Carmichael function*, Math. Comp. **70** (2001), 1591 – 1605.

[15] Y. Gallot and P. Moree, *Ternary cyclotomic polynomials having a large coefficient*, J. Reine Angew. Math. **632** (2009), 105 – 125.

[16] R. R. Hall and G. Tenenbaum, *Divisors*. Cambridge University Press, Cambridge, 1988.

[17] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*. 4th ed. Oxford University Press, London, 1968.

[18] H. Halberstam and H.-E. Richert, *Sieve methods*. Academic Press, London, 1974.

[19] M. Hausman and H. N. Shapiro, *On practical numbers*, Comm. Pure Appl. Math. **37** no. 5 (1984): 705 – 713.

[20] C. Hooley, *Artin's conjecture for primitive roots*, J. Reine Agnew. Math. **225** (1967), 209 – 220.

[21] K. Ireland, M. Rosen, *A classical introduction to modern number theory*. Springer, New York, 1990.

[22] N. Kaplan, *Bounds for the maximal height of divisors of* $x^n - 1$, J. Number Theory **129** (2009), 2673 – 2688.

[23] P. Kurlberg and C. Pomerance, *On a problem of Arnold: the average multiplicative order of a given integer*. Preprint.

[24] S. Lang, *Algebra*. Springer, New York, 2002.

[25] S. Li and C. Pomerance, *On generalizing Artin's conjecture on primitive roots to composite moduli*, J. Reine Angew. Math. **556** (2003), 205 – 224.

[26] F. Luca and P. Pollack, *An arithmetic function arising from Carmichael's conjecture*, J. Théorie des Nombres de Bordeaux (to appear).

[27] H. Maier, *The coefficients of cyclotomic polynomials*, Proc. Conf. in Honor of Paul T. Bateman, Progr. Math. **85** (1990), 349 – 366.

[28] H. Maier, *Cyclotomic polynomials with large coefficients*, Acta Arith. **64** (1993), 227 – 235.

[29] M. Margenstern, *Les nombres pratiques; théorie, observations et conjectures*, J. Number Theory **37** (1991), 1 – 36.

[30] A. Migotti, *Aur Theorie der Kreisteilungsgleichung*, Z. B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften, Wien, **87** (1883), 7 – 14.

[31] H. Möller, *Über die Koeffizienten des n-ten Kreisteilungspolynoms*, Math. Z. **119** (1971), 33 – 40.

[32] P. Pollack, *Not always buried deep: a second course in elementary number theory*. Amer. Math. Soc., Providence, 2009.

[33] C. Pomerance and N. Ryan, *Maximal height of divisors of* $x^n - 1$. Illinois J. Math. **51** no. 2 (2007), 597 – 604 (electronic).

[34] E. Saias, *Entiers à diviseurs denses. I.*, J. Number Theory **62** (1997), 163 – 191.

[35] J. P. Serre, *Local fields*. Springer, New York, 1995.

[36] B. M. Stewart, *Sums of distinct divisors*, Amer. J. Math. **76** no. 4 (1954), 779 – 785.

[37] G. Tenenbaum, *Lois de répartition des diviseurs*, 5, J. London Math. Soc. (2) **20** (1979), 165 – 176.

[38] G. Tenenbaum, *Sur un problème de crible et ses applications,* Ann. Sci. École Norm. Sup. (4) **19** (1986), 1 – 30.

[39] R. Thangadurai, *On the coefficients of cyclotomic polynomials,* Cyclotomic Fields and Related Topics, Pune, 1999, Bhaskaracharya Pratishthana, Pune (2000), 311 – 322.

[40] R. C. Vaughan, *Bounds for the coefficients of cyclotomic polynomials*, Michigan Math. J. **21** (1974), 289 – 295.