The distribution of some special arithmetic functions

by

Noah Lebowitz-Lockard

(Under the Direction of Paul Pollack)

Abstract

This thesis discusses three topics related to the distributions of arithmetic functions. The first topic is the distribution function of a polynomial of additive functions. Roughly speaking, the distribution function of an arithmetic function f records how often f lies below a given value. We show that certain polynomials of additive functions with continuous distribution functions also have continuous distribution functions.

The second topic is the range of Euler's totient function. For an irreducible quadratic polynomial P, we prove that for almost all n, the equation $\varphi(m) = P(n)$ has no solutions.

The final topic is additively unique sets of primes. A set S is additively unique if the only multiplicative functions possessing a certain invariant on S are $f(n) = 0$ and $f(n) = n$. We classify the additively unique sets of primes.

Index words: Distribution functions, Arithmetic functions, Euler's totient function, Quadratic polynomials, Additive uniqueness

The distribution of some special arithmetic functions

by

Noah Lebowitz-Lockard

B.A., Dartmouth College, 2013

A Dissertation Submitted to the Graduate Faculty

of The University of Georgia in Partial Fulfillment

of the

Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2019

The distribution of some special arithmetic functions

by

Noah Lebowitz-Lockard

Approved:

Major Professor: Paul Pollack

Committee: Neil Lyall
Akos Magyar
Giorgis Petridis

Electronic Version Approved:

Suzanne Barbour
Dean of the Graduate School
The University of Georgia
May 2019

The distribution of some special arithmetic functions

Noah Lebowitz-Lockard

April 18, 2019

Acknowledgments

First and foremost, I would like to thank my advisor, Paul Pollack. For the last four years, he has been truly exceptional as a mentor. I have learned so much from him and I would not have been able to prove these results without his encouragement.

I would also like to thank Pete L. Clark for his mentorship during the University of Georgia VRG in 2015-2016. I learned a great deal about the process of doing research from this experience. I also thank him for all the advice he has given me about math during my time here.

I also thank Carl Pomerance. My first experience with Carl was doing research with him as an undergraduate. Even after I got to grad school, he has still provided helpful advice and really helped me improve as a number theorist. He has been very influential in my journey into number theory and through grad school.

Finally, I would like to thank my family, who have all been very supportive as I have gone through grad school. In particular, I would like to thank my father, David, for all he has done for me over the years. Thank you all very much.

Contents

Chapter 1

Introduction

This thesis focuses on three distinct topics:

1. Distribution functions of arithmetic functions,
2. Polynomials and the range of the totient function,
3. Additively unique sets of integers.

We provide background for each of these topics.

1.1 Distribution functions of arithmetic functions

In a broad sense, a distribution function records how often a set of real numbers lies below a given value.

Definition. Let X be a random variable in a probability space. The *distribution function* of X is the function

$$F_X : \mathbb{R} \to [0, 1]$$

where $F_X(x)$ is the probability that $X \leq x$.

Note that F_X is non-decreasing and right-continuous. In addition,

$$\lim_{x\to-\infty} F_X(x) = 0 \text{ and } \lim_{x\to\infty} F_X(x) = 1. \tag{1}$$

A theorem from probability [8, Theorem 14.1] states that any non-decreasing, right-continuous function satisfying (1) is the distribution function of some random variable. We restrict our attention to the distribution function of an arithmetic function $f : \mathbb{Z}_+ \to \mathbb{R}$.

Definition. Let f be a real-valued arithmetic function. For each positive integer N, define the function $F_N : \mathbb{R} \to [0, 1]$ by

$$F_N(x) = \frac{\#\{n \le N : f(n) \le x\}}{N}.$$

Suppose that there exists a function F such that

$$\lim_{N\to\infty} F_N(x) = F(x), \tag{2}$$

whenever F is continuous at x. If F is a distribution function, then F is the *distribution function* of f.

Assuming an F satisfying (2) exists, it must be non-decreasing by definition. However, it need not be a distribution function. For example, let f be an unbounded non-decreasing function. Then,

$$\lim_{N\to\infty} F_N(x) = 0$$

for all x, which implies that F is identically 0. Therefore, F is not a distribution function.

For a given arithmetic function f, we may ask two questions:

1. Does f have a distribution function?
2. If f does have a distribution function, is this function continuous?

For certain well-understood arithmetic functions, we may answer these questions. Before we do so, we write a definition.

Definition. A real-valued function f is *additive* (resp. *multiplicative*) if $f(mn) = f(m) + f(n)$ (resp. $f(mn) = f(m)f(n)$) for all coprime m, n.

Throughout this thesis, we extensively use the φ and σ functions, which we define below.

Definition. *Euler's totient function* $\varphi(n)$ is the number of $m \leq n$ which are coprime to n. The *sum-of-divisors function* $\sigma(n)$ adds up all of the divisors of n. For $n = p_1^{e_1} \cdots p_k^{e_k}$ we have

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1), \quad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

One of the first results on distribution functions of arithmetic functions is the following theorem of Schoenberg [54]:

Theorem 1.1.1. *The function $\varphi(n)/n$ possesses a continuous distribution function.*

A few years later, Davenport proved a related result [14] (which Behrend and Chowla obtained independently [6], [12]), answering a question Bessel-Hagen had recently posed [7].

Theorem 1.1.2. *The function $n/\sigma(n)$ possesses a continuous distribution function.*

Let $s(n)$ be the sum of the proper divisors of n (the divisors other than n). We say a number is abundant if $s(n) > n$, deficient if $s(n) < n$, and perfect if $s(n) = n$ (these definitions go back to the ancient Greek mathematician Nicomachus [47, Book I, Chapter XIV], circa 100 AD). A notable corollary of Theorem 1.1.2 is that the abundant and deficient numbers have well-defined densities and that the perfect numbers have density 0 (see [17] for an alternate, elementary proof of this result). Before Theorem 1.1.2 was known, Behrend found bounds on the upper and lower densities of the abundant numbers [5]. The current

bounds on the density Δ of abundant numbers are $0.24761 < \Delta < 0.24766$ [39]. Moreover,

$$A(x) = \Delta x + O\left(\frac{x}{\exp((\log x)^{1/3})}\right),$$

where $A(x)$ is the number of abundant numbers $\leq x$ [40].

In the 1930's, Erdős proved three results on the distribution of additive functions ([18], [20], [21], the last of these discusses Schoenberg's related work in [55]). Note that 1.1.5 superseded 1.1.4, which in turn superseded 1.1.3. In each of the following theorems f is an additive function.

Theorem 1.1.3. *Suppose f satisfies the following conditions:*

1. *$f(n) \geq 0$ for all n.*
2. *For all distinct primes p and q, $f(p) \neq f(q)$.*
3. *The sums*

$$\sum_{|f(p)|>1} \frac{1}{p}, \quad \sum_{|f(p)|\leq 1} \frac{f(p)}{p}$$

converge.

Then, f possesses a distribution function.

Theorem 1.1.4. *Even if f only satisfies Conditions* (1) *and* (3)*, it still possesses a distribution function.*

Theorem 1.1.5. *If f satisfies Condition* (3) *and the sum*

$$\sum_{|f(p)|\leq 1} \frac{f(p)^2}{p}$$

converges, then f possesses a distribution function. This distribution function is continuous

if and only if the following sum diverges:

$$\sum_{f(p)\neq 0} \frac{1}{p}.$$

In 1939, Erdős and Wintner proved the converse of the first part of Theorem 1.1.5. The Erdős-Wintner Theorem [26], one of the founding results of probabilistic number theory, determines when an additive function has a distribution function and when that distribution function is continuous.

Theorem 1.1.6. *The additive function f has a distribution function if and only if the following sums converge:*

$$\sum_{|f(p)|>1} \frac{1}{p}, \quad \sum_{|f(p)|\leq 1} \frac{f(p)}{p}, \quad \sum_{|f(p)|\leq 1} \frac{f(p)^2}{p}.$$

Note that for a positive-valued multiplicative function f, the function $\log f$ is additive. Therefore, the Erdős-Winter Theorem is also a statement about multiplicative functions. (It is straightforward to show that $\log(\varphi(n)/n)$ and $\log(n/\sigma(n))$ satisfy the conditions of the Erdős-Wintner Theorem, giving us Theorems 1.1.1 and 1.1.2.)

Unfortunately, these results tell us nothing about distribution functions of *polynomials* of additive and multiplicative functions. There have been multiple results discussing this problem in specific cases.

Proposition 1.1.7. If $f_1, \ldots, f_k$ are additive functions with distribution functions, then every polynomial in $f_1, \ldots, f_k$ has a distribution function as well ([56, p.63] covers sums of additive functions, but similar techniques work for products).

Theorem 1.1.8 ([28, Theorem 4.1])**.** *Let f be an additive function and g a positive-valued multiplicative function. If f and g have distribution functions and at least one of the distri-*

bution functions is continuous, then $f+g$ has a continuous distribution function. (See [31] for a generalization).

In order to state the results of Chapter 2, we first write the following definition.

Definition. We say that an arithmetic function f *clusters around the real number* u if there exists some $\epsilon > 0$ such that, for every $\delta > 0$, the set

$$\{n : |f(n) - u| < \delta\}$$

has upper density at least ϵ. If f does not cluster around any u, we say that f is *nonclustering.*

If a nonclustering function f has a distribution function F, then F is continuous. However, not all nonclustering functions have distribution functions. One such example is the identity function $f(n) = n$. This function does not have a distribution function because it is unbounded and non-decreasing. However, f is still nonclustering. The author recently proved the following results with Pollack [42] (the second of which was initially a conjecture of Luca and Pomerance [43].) In Section 2.1, we discuss these theorems in more detail.

Theorem 1.1.9. *Let $f_1, \dots, f_k$ be multiplicative functions taking values in the non-zero real numbers and satisfying the following conditions:*

1. *f_1 is nonclustering,*
2. *none of $f_1, \dots, f_k$ cluster around 0,*
3. *for all i, j with $1 \le i < j \le k$, the function f_i/f_j is nonclustering.*

Then, every nontrivial linear combination of $f_1, \dots, f_k$ is nonclustering.

Corollary 1.1.10. The function $(\sigma(n)-n)/(n-\varphi(n))$ has a continuous distribution function strictly increasing on $[1, \infty)$.

In Section 2.2, we prove the following two results. (Whether we may replace "polynomial" with "analytic function" in the first theorem is still open.)

Theorem 1.1.11. *If $f_1, \dots, f_k$ are additive functions for which every nontrivial linear combination has a continuous distribution function, then every nonconstant polynomial in $f_1, \dots, f_k$ has a continuous distribution function.*

Theorem 1.1.12. *The product of additive functions with continuous distribution functions also has a continuous distribution function.*

1.2 Polynomials and the range of the totient function

Let $V(x)$ be the number of $n \leq x$ that lie in the range of Euler's totient function. In 1929, Pillai showed that almost all numbers lie outside the range of the totient function [48], namely that

$$V(x) = O\left(\frac{x}{(\log x)^{(\log 2)/e}}\right).$$

Note that $(\log 2)/e \approx 0.25$. This result was improved multiple times ([19], [23], [24], [53], [44]). We list these results here. (For notational convenience, we let $\log_k x$ be the result of taking the logarithm of x k times.)

$$\begin{aligned}
V(x) &= \frac{x}{(\log x)^{1+o(1)}} && \text{(Erdős, 1935)} \\
V(x) &\ll \frac{x}{\log x} \exp(C_1(\log\log x)^{1/2}) && \text{(Erdős, Hall, 1973)} \\
V(x) &\gg \frac{x}{\log x} \exp(C_2(\log_3 x)^2) && \text{(Erdős, Hall, 1976)} \\
V(x) &\ll \frac{x}{\log x} \exp(C_3(\log_3 x)^2) && \text{(Pomerance, 1986)} \\
V(x) &= \frac{x}{\log x} \exp((C_4 + o(1))(\log_3 x)^2) && \text{(Maier, Pomerance, 1988).}
\end{aligned}$$

Here, $C_1 \approx 3.40$, $C_2 \approx 0.36$, $C_3 \approx 1.18$, $C_4 \approx 0.82$. In 1998, Ford [29] derived a formula for $V(x)$, up to a constant multiple:

$$V(x) = \frac{x}{\log x} \exp(C_4(\log_3 x - \log_4 x)^2 + C_5 \log_3 x - (C_5 + (1/2) - 2C_4) \log_2 x + O(1)),$$

with $C_5 \approx 2.18$.

For a given function f, we may consider how often $f(n)$ lies in the range of the totient function. We write a few notable results on this question in the case where f is a polynomial.

Theorem 1.2.1 ([37, Theorem 1])**.** *Let f and g be integer-valued polynomials. Suppose $\deg f \leq \deg g$ and that f factors completely over $\mathbb{Q}$ with only simple roots. Then,*

$$\#\{n \leq x : \exists m \text{ s.t. } \varphi(f(n)) = g(m)\} \ll \frac{x}{(\log x)^{1/10}}.$$

Theorem 1.2.2 ([49, Theorems 1, 2])**.** *Fix an integer $k > 1$. Conditional on a conjecture of Pomerance [52], the number of $n \leq x$ for which $\varphi(n)$ is a kth power is*

$$\frac{x}{L(x)^{1+o(1)}},$$

where

$$L(x) = \exp\left(\frac{\log x \log_3 x}{\log_2 x}\right).$$

Unconditionally, the number of $n \leq x$ for which $\varphi(n)$ is squarefull (every prime factor is repeated) is at most

$$\frac{x}{L(x)^{1+o(1)}}.$$

We define

$$V_f(x) = \#\{n \leq x : \exists m \text{ s.t. } \varphi(m) = f(n)\}.$$

Pollack and Pomerance [51] (improving on [2], [3], [30, Theorem 1.2]) recently showed that for the function $f(x) = x^2$,

$$\frac{x}{(\log x)^2(\log\log x)^2} \ll V_f(x) \ll \frac{x}{(\log x)^{0.0063}}.$$

Rather than just considering squares, we may broaden our scope to integer-valued polynomials. The main focus of Chapter 3 is the following result. (Though this result only applies to irreducible quadratic polynomials, it is entirely possible that one can generalize it to all nonconstant polynomials.)

Theorem 1.2.3. *For an irreducible quadratic polynomial P with integer coefficients,*

$$V_P(x) = O\left(\frac{x}{(\log x)^{0.0312}}\right).$$

In general, we do not have a method for obtaining unconditional lower bounds for $V_P(x)$. However, it is possible to obtain lower bounds if we assume the Bateman-Horn Conjecture [4], which we write below in a simplified form.

Conjecture 1.2.4. Let $f_1, \ldots, f_k$ be a set of distinct, primitive, irreducible polynomials. If there does not exist a prime p which divides $f_1(n)\cdots f_k(n)$ for all n, then the number of $n \leq x$ for which $f_1(n), \ldots, f_k(n)$ are simultaneously prime is on the order of

$$\frac{x}{(\log x)^k}.$$

Using this result, we can prove the following.

Corollary 1.2.5. Assume the Bateman-Horn Conjecture. If P is a polynomial for which

$P(x)+1$ is primitive and irreducible, then

$$V_P(x) \gg \frac{x}{\log x}.$$

Proof. Let P be a polynomial satisfying these properties. If $P(n)+1$ is prime, then $\varphi(P(n)+1) = P(n)$. Assuming the conjecture, the number of $n \leq x$ for which $P(n)+1$ is prime is on the order of $x/\log x$. Therefore,

$$V_P(x) \gg \frac{x}{\log x}.$$

□

1.3 Additively unique sets of integers

The final chapter of this thesis focuses on a number-theoretic result that does not relate to the previous chapters.

Definition. Let S be a set and $\mathcal{F}$ a family of functions. If there is exactly one element $f \in \mathcal{F}$ satisfying $f(m+n) = f(m) + f(n)$ for all $m, n \in S$, then S is an *additively unique set* (AU set) for $\mathcal{F}$.

Let $\mathcal{F}$ be the set of multiplicative functions that do not vanish on some prime. Spiro proved that the primes are additively unique [58]. (Here, f is the identity function.)

There have been multiple recent results showing that certain sets are AU or are close to being AU, some of which we write here.

Theorem 1.3.1 ([15])**.** *Let f be a multiplicative function for which $f(1) = 1$. If*

$$f(p+n^2) = f(p) + f(n^2)$$

for all primes p and positive integers n, then f is the identity function.

Theorem 1.3.2 ([13]). *The triangular and tetrahedral numbers are both AU. (Whether the k-tetrahedral numbers are AU for all $k > 3$ is still open.)*

Theorem 1.3.3 ([11]). *Let f be a multiplicative function that does not vanish on some odd prime. If $f(p) + f(q) = f(p+q)$ for all odd primes p and q, then f is the identity function or*

$$f(n) = \begin{cases} 1, & \text{if } n \text{ is odd.} \\ 2, & \text{if } n \text{ is even.} \end{cases}$$

In Chapter 4, we strengthen Spiro's result as follows by classifying the additively unique sets of primes.

Theorem 1.3.4. *A set of primes is AU if and only if it contains every prime that is not the larger element of a twin prime pair, and at least one element of $\{5, 7\}$.*

Chapter 2

Distribution functions of arithmetic functions

In Section 2.1, we discuss Theorem 1.1.9 and Corollary 1.1.10. In Section 2.2, we prove Theorems 1.1.11 and 1.1.12.

2.1 Clustering of linear combinations of multiplicative functions

We restate Theorem 1.1.9 [42], which gives us a criterion for a linear combination of multiplicative functions to be nonclustering.

Theorem 2.1.1. *Let $f_1, \dots, f_k$ be multiplicative arithmetic functions taking values in the nonzero real numbers and satisfying the following conditions:*

1. *f_1 is nonclustering,*
2. *none of $f_1, \dots, f_k$ cluster around 0,*
3. *for all $i < j$ with $i, j \in \{1, 2, \dots, k\}$, the function f_i/f_j is nonclustering,*

Then for all nonzero $c_1, \dots, c_k \in \mathbb{R}$, the arithmetic function $c_1 f_1 + \cdots + c_k f_k$ is nonclustering.

Recall that if an arithmetic function f possesses a distribution function F, then F is continuous precisely when f is nonclustering. It is often the case that one can prove that F is well-defined by some general principle, but doing so does not offer any insight into whether F is continuous. Theorem 1.1.9 sometimes provides a convenient way of establishing continuity.

Let $s(n)$ be the sum-of-proper-divisors function, so that $s(n) = \sigma(n) - n$. Let $s_\varphi(n) = n - \varphi(n)$ denote the cototient function. In [43], Luca and Pomerance noted that $s(n)/s_\varphi(n) \geq 1$ for all $n \geq 2$ and showed that the sequence $\{s(n)/s_\varphi(n)\}_{n=2}^{\infty}$ is dense in $[1, \infty)$.

Corollary 2.1.2. The arithmetic function $s(n)/s_\varphi(n)$ possesses a continuous distribution function D_{s/s_φ}. Moreover, $D_{s/s_\varphi}(u)$ is strictly increasing for $u \geq 1$.

Corollary 1.1.10 was conjectured at the end of [43, §1]. Using Theorem 1.1.9, the author and Pollack proved this result [42].

2.2 The distribution function of a polynomial in additive functions

2.2.1 Introduction

Section 2.2 is mainly devoted to proving Theorems 1.1.11 and 1.1.12, which we restate here.

Theorem 2.2.1. *If $f_1, \dots, f_k$ are additive functions for which every nontrivial linear combination has a continuous distribution function, then every nonconstant polynomial in $f_1, \dots, f_k$ has a continuous distribution function.*

Theorem 2.2.2. *The product of additive functions with continuous distribution functions also has a continuous distribution function.*

Before we do so, we restate a result related to Theorem 1.1.11, namely Proposition 1.1.7.

Proposition 2.2.3. If $f_1, \ldots, f_k$ are additive functions with distribution functions, then every polynomial in $f_1, \ldots, f_k$ has a distribution function as well.

Though the principle behind the proof of Proposition 1.1.7 is not new, it is useful to state the result explicitly. Our proof of Proposition 1.1.7 is arithmetic, but the theorem could also be established by analytic means, specifically by first using the method of characteristic functions to show that the vector of arithmetic functions $f_1, \ldots, f_k$ possesses a distribution function.

Theorem 1.1.11 is a continuous analogue of Proposition 1.1.7. It is clear that such a result will require extra hypotheses. For instance, if F is a constant polynomial, then the distribution function of $F(f_1, \ldots, f_k)$ is never continuous. There are also less trivial examples where the distribution function is discontinuous. For instance, let $F(x_1, x_2) = x_1 - x_2$, and let f_1 and f_2 be the same additive function with a continuous distribution function. Then, $F(f_1, f_2) = 0$ has a discontinuous distribution function, even though F is nonconstant. In order to obtain a continuous analogue of Proposition 1.1.7, we need to impose conditions on $f_1, \ldots, f_k$.

Theorem 1.1.9 states that under certain conditions, the sum of multiplicative functions with continuous distribution functions also has a continuous distribution function. Theorem 1.1.12, proved using Theorem 1.1.11, is dual to this.

Proposition 1.1.7 already tells us that polynomials in $f_1, \ldots, f_k$ have distribution functions. In order to prove Theorem 1.1.11, we just need to show these distribution functions are continuous. We rewrite the definition of a clustering function to pinpoint what remains to be shown.

Definition. The arithmetic function f *clusters* around the real number r if there exists an

$\epsilon > 0$ such that for any $\delta > 0$, the upper density of positive integers n for which

$$r - \delta < f(n) < r + \delta$$

is greater than ϵ. In addition, f is *nonclustering* if it does not cluster around any real number.

Let f be an arithmetic function with a distribution function. Note that f is nonclustering if and only if the distribution function of f is continuous. After proving Proposition 1.1.7, we prove Theorem 1.1.11 by showing that if $f_1, \ldots, f_k$ are additive functions for which every nontrivial linear combination is nonclustering, then every nonconstant polynomial in $f_1, \ldots, f_k$ is nonclustering as well. We then use Theorem 1.1.11 and a few supplementary results to prove Theorem 1.1.12. Our approach throughout is heavily influenced by work of Erdős (Theorems 1.1.3-1.1.5).

Throughout Sections 2.2.3.4 and 2.2.4, we use the following results related to the Erdős-Wintner Theorem (the second of which is due to Halász [32]).

Lemma 2.2.4. An additive function f is clustering if and only if

$$\sum_{f(p) \neq 0} \frac{1}{p}$$

converges.

Theorem 2.2.5. *Let f be an additive function. For all $a \in \mathbb{R}$, the number of solutions to the equation $f(n) = a$ with $n \leq x$ is*

$$\ll x \left(\sum_{\substack{p \leq x \\ f(p) \neq 0}} \frac{1}{p} \right)^{-1/2}.$$

Proving one direction is straightforward. If the sum converges, then the density of the set of squarefree numbers n for which $f(p) = 0$ for all p dividing n is

$$\prod_{f(p)=0} \left(1 - \frac{1}{p^2}\right) \prod_{f(p)\neq 0} \left(1 - \frac{1}{p}\right) > 0.$$

If n is squarefree and $f(p) = 0$ for all $p|n$, then $f(n) = 0$. If the sum converges, then f clusters around 0. Elliott and Ryavec's [16, Theorem 7.3] is a stronger statement than the converse.

2.2.2 Existence of the distribution function for a polynomial in additive functions

In this section, we discuss distribution functions, but not clustering. In the remaining sections, we only consider whether or not a function is nonclustering. We explicitly write three definitions that we mentioned in passing in Section 2.1.3.

Definition. The y-smooth part $s_y(n)$ of a number n is the largest divisor of n for which every prime factor is at most y and that the y-rough part of n is $n/s_y(n)$.

Definition. Let S be a set of positive integers. The *upper* and *lower densities* of S are

$$\overline{\mathbf{d}}S = \limsup_{x\to\infty} \frac{\#\{n \leq x : n \in S\}}{x}, \quad \underline{\mathbf{d}}S = \liminf_{x\to\infty} \frac{\#\{n \leq x : n \in S\}}{x}.$$

In addition, the *density* of S is

$$\mathbf{d}S = \lim_{x\to\infty} \frac{\#\{n \leq x : n \in S\}}{x},$$

when this quantity is well-defined.

Definition. The arithmetic function F is *essentially determined by small primes* if for all $\epsilon > 0$,

$$\lim_{y\to\infty} \overline{\mathbf{d}}\{n : |F(n) - F(s_y(n))| > \epsilon\} = 0.$$

Lemma 2.2.6. The sum and product of any two functions that are essentially determined by small primes is essentially determined by small primes as well. In addition, any constant multiple of a function that is essentially determined by small primes is essentially determined by small primes.

Proof. Let f and g be two functions that are essentially determined by small primes. We first show that $f + g$ is essentially determined by small primes as well. For all $\delta, \epsilon > 0$, there exists some $Y > 0$ such that if $y > Y$, then the set of numbers n for which either $|f(n) - f(s_y(n))|$ or $|g(n) - g(s_y(n))|$ is greater than $\epsilon/2$ has upper density at most δ. Thus, the set of numbers n for which $|(f + g)(n) - (f + g)(s_y(n))| > \epsilon$ has upper density at most δ. Hence, $f + g$ is essentially determined by small primes.

We now show that fg is essentially determined by small primes. Fix $\delta, \epsilon > 0$. Because f and g are essentially determined by small primes, there exists a $y_1 > 0$ such that the upper density of numbers n for which

$$\max(|f(n) - f(s_{y_1}(n))|, |g(n) - g(s_{y_1}(n))|) > \epsilon$$

is less than $\delta/3$. For any integer $z > 1$, the set of numbers with a y_1-smooth part that is not a multiple of any zth power greater than 1 is

$$\prod_{p\le y_1} \left(1 - \frac{1}{p^z}\right),$$

which tends to 1 as z goes to infinity. Therefore, there exists a number z for which the set of numbers with a y_1-smooth part that is a multiple of some zth power greater than 1 has an

upper density that is less than $< \delta/3$. Letting y_2 be the product of p^z over all prime $p \leq y_1$, we see that the upper density of numbers with y_1-smooth part $\geq y_2$ is $< \delta/3$.

If the y_1-smooth part of n is less than y_2, then there exists a constant C such that $|f(s_{y_1}(n))|, |g(s_{y_1}(n))| < C$ because $s_{y_1}(n)$ only has a finite number of possible values. Applying our definition of y_1 gives us

$$\overline{\mathbf{d}}\{n : \max(|f(n)|, |g(n)|) \geq C + \epsilon\} < 2\delta/3.$$

Let $\eta > 0$. If y is sufficiently large in terms of δ and η, then the upper density of n for which $|f(n) - f(s_y(n))|$ or $|g(n) - g(s_y(n))|$ is greater than η is less than $\delta/3$. We may assume that

$$|f(n) - f(s_y(n))|, |g(n) - g(s_y(n))| < \eta$$

and

$$|f(n)|, |g(n)| < C + \epsilon$$

because the upper density of inputs n not satisfying both of these properties is less than δ. We now have

$$\begin{aligned}
|f(n)g(n) - f(s_y(n))g(s_y(n))| &= |f(n)(g(n) - g(s_y(n))) + g(s_y(n))(f(n) - f(s_y(n)))| \\
&\leq |f(n)||g(n) - g(s_y(n))| + |g(s_y(n))||f(n) - f(s_y(n)))| \\
&< \eta(|f(n)| + |g(s_y(n))|) \\
&< \eta(|f(n)| + |g(n)| + \epsilon) \\
&< \eta(2C + 3\epsilon).
\end{aligned}$$

Choosing η to satisfy $\eta(2C + 3\epsilon) \leq \epsilon$, we see that for all large enough y, depending on δ and ϵ, the density of n for which $|f(n)g(n) - f(s_y(n))g(s_y(n))|$ is greater than ϵ is less than

δ. Thus, fg is essentially determined by small primes.

Let c be a constant. For any function f that is essentially determined by small primes, we may apply the result for products with one of the functions being the constant function $g(n) = c$. □

In order to show that polynomials in $f_1, \ldots, f_k$ have distribution functions, we use a theorem of Tenenbaum [59, Theorem III.2.2] and a result of Erdős and Wintner [26, p. 719-720].

Theorem 2.2.7. *Let f be an arithmetic function. Suppose that for all $\epsilon > 0$, there exists a function $a_\epsilon : \mathbb{Z}_+ \to \mathbb{Z}_+$ with the following properties:*

(i) $\lim_{\epsilon \to 0} \limsup_{T \to \infty} \overline{\mathbf{d}}\{n : a_\epsilon(n) > T\} = 0$,

(ii) $\lim_{\epsilon \to 0} \overline{\mathbf{d}}\{n : |f(n) - f(a_\epsilon(n))| > \epsilon\} = 0$,

(iii) *for each $a \geq 1$, $\mathbf{d}\{n : a_\epsilon(n) = a\}$ exists.*

Then, f has a distribution function.

Theorem 2.2.8. *An additive function f possesses a distribution function if and only if f is essentially determined by small primes.*

Proposition 2.2.9. Let $f_1, \ldots, f_k$ be additive functions each possessing a distribution function. Then, every polynomial in $f_1, \ldots, f_k$ has a distribution function as well.

Proof. By Theorem 2.2.8, $f_1, \ldots, f_k$ are all essentially determined by small primes. Now Lemma 2.2.6 implies that any polynomial $F(f_1, \ldots, f_k)$ is also essentially determined by small primes.

We now argue, using Theorem 2.2.7, that any arithmetic function essentially determined by small primes has a distribution function. Let g be such a function. For each $\epsilon > 0$, we can choose $y = y_\epsilon$ such that the set of n with $|g(n) - s_y(n)| > \epsilon$ form a set of upper density $< \epsilon$.

Take $a_\epsilon = s_y$. Condition (i) follows from an argument seen already in the proof of Lemma 2.2.6 (in fact, the inner lim sup is always 0), (ii) holds by our choose of a_ϵ, and (iii) is easy: the density of n with y-smooth part s is

$$s \prod_{p \leq y} (1 - (1/p)). \qquad \square$$

2.2.3 Nonclustering polynomials of additive functions

2.2.3.1.0 Forward shift operators

Definition. Let F be a function in the variables $x_1, \ldots, x_k$. For any $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$, we define the *forward shift operator* Ψ by

$$\Psi_{\alpha_1,\ldots,\alpha_k} F(x_1, \ldots, x_k) = F(x_1 + \alpha_1, \ldots, x_k + \alpha_k).$$

Definition. Let $F \in \mathbb{R}[x_1, \ldots, x_n]$. F is a polynomial of *essentially r variables* if there exists some polynomial $G \in \mathbb{R}[\ell_1, \ldots, \ell_r]$ with

$$F(x_1, \ldots, x_n) = G(\ell_1, \ldots, \ell_r)$$

where each ℓ_i is a linear form in $x_1, \ldots, x_n$ and there does not exist such a polynomial in fewer than r variables.

Proposition 2.2.10. Let $F \in \mathbb{R}[x_1, \ldots, x_n]$. If there exist distinct n-tuples $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ with

$$\Psi_{\alpha_1,\ldots,\alpha_n} F = \Psi_{\beta_1,\ldots,\beta_n} F,$$

then F has fewer than n essential variables.

Proof. Let $\mathbf{v} = (\alpha_1, \ldots, \alpha_n)$ and $\mathbf{w} = (\beta_1, \ldots, \beta_n)$. Let $\mathbf{x} = (x_1, \ldots, x_n)$ be an arbitrary

vector in $\mathbb{R}^n$. By assumption,

$$F(\mathbf{x}+\mathbf{v}) = F(\mathbf{x}+\mathbf{w}).$$

We replace $\mathbf{x}$ with $\mathbf{x}-\mathbf{w}$ to obtain

$$F(\mathbf{x}) = F(\mathbf{x}+(\mathbf{v}-\mathbf{w})).$$

We may take this equation and replace $\mathbf{x}$ with $\mathbf{x}+(\mathbf{v}-\mathbf{w})$ as many times as we like so that

$$F(\mathbf{x}) = F(\mathbf{x}+(\mathbf{v}-\mathbf{w})) = F(\mathbf{x}+2(\mathbf{v}-\mathbf{w})) = \cdots = F(\mathbf{x}+n(\mathbf{v}-\mathbf{w})) = \cdots .$$

Define the polynomial

$$P_{\mathbf{x}}(t) = F(\mathbf{x}) - F(\mathbf{x}+t(\mathbf{v}-\mathbf{w})) \in \mathbb{R}[t].$$

We have that $P_{\mathbf{x}}(t) = 0$ identically as a polynomial in t because it is a one variable polynomial that vanishes at all of the integers. So letting $\mathbf{u} = \mathbf{v}-\mathbf{w}$ we have that for all $\lambda \in \mathbb{R}$,

$$F(\mathbf{x}) = F(\mathbf{x}+\lambda\mathbf{u}). \tag{2.1}$$

Because $\mathbf{u} \neq \mathbf{0}$, $\mathbf{u}$ has a nonzero component. We may assume without loss of generality that the last component is not zero. We scale $\mathbf{u}$ so that its last component is 1 and express $\mathbf{u}$ as

$$\mathbf{u} = (u_1, \ldots, u_{n-1}, 1).$$

We plug $\lambda = -x_n$ into (1) to rewrite $F(x_1, \ldots, x_n)$ as

$$\begin{aligned} F(x_1, \ldots, x_n) &= F((x_1, \ldots, x_n) - x_n \mathbf{u}) \\ &= F(x_1 - x_n u_1, \ldots, x_{n-1} - x_n u_{n-1}, 0) \\ &= G(x_1 - x_n u_1, \ldots, x_{n-1} - x_n u_{n-1}), \end{aligned} \tag{2.2}$$

where

$$G(t_1, \ldots, t_{n-1}) = F(t_1, \ldots, t_{n-1}, 0)$$

is a polynomial in $\mathbb{R}[t_1, \ldots, t_{n-1}]$. Note that (2) is a polynomial identity because it holds for all $x_1, \ldots, x_n \in \mathbb{R}^n$. It follows that F has fewer than n essential variables. □

Lemma 2.2.11. Let $F(x_1, \ldots, x_k)$ be a polynomial with r essential variables. Then, any polynomial $G \in \mathbb{R}[\ell_1, \ldots, \ell_r]$ satisfying $F(x_1, \ldots, x_n) = G(\ell_1, \ldots, \ell_r)$ has the same degree as F.

Proof. There exist linear forms $\ell_{r+1}, \ldots, \ell_k$ such that $\{\ell_1, \ldots, \ell_k\}$ is an $\mathbb{R}$-basis for $\oplus_{i=1}^{k} \mathbb{R}\, x_i$. For each x_i, there exist constants $c_{i,1}, \ldots, c_{i,k}$ such that

$$x_i = c_{i,1}\ell_1 + \cdots + c_{i,k}\ell_k.$$

We can replace each x_i in $F(x_1, \ldots, x_k)$ with the corresponding linear combination of ℓ_j's. Consider an arbitrary monomial term

$$x_1^{e_1} \cdots x_k^{e_k} = (c_{1,1}\ell_1 + \cdots + c_{1,k}\ell_k)^{e_1} \cdots (c_{k,1}\ell_1 + \cdots + c_{k,k}\ell_k)^{e_k}$$

Both sides have the same degree, namely $e_1 + \cdots + e_k$. When we go from F to G, each term's degree stays the same. Therefore, the degree of the entire polynomial cannot increase. In other words, $\deg F \geq \deg G$. We may apply a similar argument by switching ℓ_i back to x_i.

We obtain $\deg F \leq \deg G$. Hence, $\deg G = d$. □

Throughout the rest of Section 2.2.3, we focus on additive functions $f_1, \ldots, f_k$ with the property that any linear combination of $f_1, \ldots, f_k$ is nonclustering. In order to manipulate the linear combinations of $f_1, \ldots, f_k$, we need the following lemma.

Lemma 2.2.12. Let $f_1, \ldots, f_k$ be additive functions with the property that any nontrivial linear combination of $f_1, \ldots, f_k$ is nonclustering. Let $\ell_1, \ldots, \ell_r$ be linearly independent elements of $\oplus_{i=1}^{k} \mathbb{R}\, x_i$. Then, every nontrivial linear combination of $\ell_1(f_1, \ldots, f_k), \ldots, \ell_r(f_1, \ldots, f_k)$ is nonclustering as well.

Proof. For notational convenience, we let $\tilde{\ell}_i = \ell_i(f_1, \ldots, f_k)$. Suppose that some nontrivial linear combination of $\tilde{\ell}_1, \ldots, \tilde{\ell}_r$ is clustering. Since $\ell_1, \ldots, \ell_r$ are $\mathbb{R}$-linearly independent, any nontrivial linear combination of $\tilde{\ell}_1, \ldots, \tilde{\ell}_r$ is a nontrivial linear combination of $f_1, \ldots, f_k$. The only clustering linear combination of $f_1, \ldots, f_k$ is 0. So, there exist constants $c_1, \ldots, c_r$ not all zero such that

$$c_1\tilde{\ell}_1 + \cdots + c_r\tilde{\ell}_r = 0.$$

The $\tilde{\ell}_i$ are linearly independent functions of $f_1, \ldots, f_k$. Therefore, any nontrivial linear combination of them is still a nontrivial linear combination of $f_1, \ldots, f_k$. Hence, every nontrivial linear combination of $\tilde{\ell}_1, \ldots, \tilde{\ell}_r$ is nonclustering. □

2.2.3.2.0 The main result

Theorem 2.2.13. *Let $f_1, \ldots, f_k$ be additive functions. If every nontrivial linear combination of $f_1, \ldots, f_k$ is nonclustering, then every nonconstant polynomial in $f_1, \ldots, f_k$ is nonclustering as well.*

Suppose the theorem is false. Then, there exist additive functions $f_1, \ldots, f_k$ for which every nontrivial linear combination is nonclustering and a nonconstant polynomial $F \in$

$\mathbb{R}[x_1, \ldots, x_k]$ such that $F(f_1, \ldots, f_k)$ is clustering. Pick $F, f_1, \ldots, f_k$ so that $d := \deg F$ is minimal.

Suppose F does not depend essentially on k variables. Then we can rewrite $F(x_1, \ldots, x_k)$ as a polynomial $G(\ell_1, \ldots, \ell_r)$, where $\ell_1, \ldots, \ell_r$ are linear forms in $x_1, \ldots, x_k$ and $r < k$. We assume that r is minimal, so that G depends essentially on r variables. Thus, $\ell_1, \ldots, \ell_r$ are linearly independent. By Lemma 2.2.11, F and G have the same degree. By Lemma 2.2.12, every nontrivial linear combination of $\ell_1(f_1, \ldots, f_k), \ldots, \ell_r(f_1, \ldots, f_k)$ is nonclustering. If $F(f_1, \ldots, f_k)$ is clustering, then $G(\ell_1(f_1, \ldots, f_k), \ldots, \ell_r(f_1, \ldots, f_k))$ is clustering. Because we can replace F with G and $f_1, \ldots, f_k$ with $\ell_1(f_1, \ldots, f_k), \ldots, \ell_r(f_1, \ldots, f_k)$, we may assume without loss of generality that F depends essentially on k variables.

Note that $d > 1$ because nontrivial linear combinations of $f_1, \ldots, f_k$ are nonclustering by assumption. For any $u \in \mathbb{R}$ and $\epsilon \in \mathbb{R}_+$, we show that there exists some $\delta \in \mathbb{R}_+$ such that the upper density of n satisfying

$$u - \delta < F(f_1(n), \ldots, f_k(n)) < u + \delta \tag{2.3}$$

is less than 3ϵ.

Let $Y \geq 2$ be a large real number, which we will specify more precisely later. Let $n = st$, where s is the Y-smooth part of n. There exists a $Z_0 := Z_0(\epsilon)$ such that if $Y \geq 2$ and $Z > Z_0$, then the upper density of numbers with Y-smooth part larger than Y^Z is less than ϵ [34, Theorem 07]. Let $Z > Z_0$ be another large real number, which we will also specify more precisely later. We assume that $s \leq Y^Z$ at the cost of discarding a set of upper density $< \epsilon$.

Let $\mathcal{S}$ be the set of n satisfying $|F(f_1(n), \ldots, f_k(n)) - u| < \delta$ with $s \leq Y^Z$. In the definitions below, n and n' have Y-smooth parts s and s', respectively. We split $\mathcal{S}$ into two

pieces $\mathcal{S}_1$ and $\mathcal{S}_2$, where

$$\mathcal{S}_1 = \{n \in \mathcal{S} : \exists\ n' \in \mathcal{S} \text{ with } n/s = n'/s' \text{ and } f_i(s) \neq f_i(s') \text{ for some } i\},$$

$$\mathcal{S}_2 = \mathcal{S} \backslash \mathcal{S}_1.$$

2.2.3.3.0 The upper density of $\mathcal{S}_1$

Theorem 2.2.14. *Let $F, f_1, \ldots, f_k, u, \delta, \epsilon, Y, Z$, and $\mathcal{S}_1 = \mathcal{S}_1(F, f_1, \ldots, f_k, u, \delta, \epsilon, Y, Z)$ be defined as above. Then, there exists some $\delta > 0$ such that $\overline{\mathbf{d}}\mathcal{S}_1 < \epsilon$.*

Proof. For notational convenience, we define $F^*(n)$ as $F(f_1(n), \ldots, f_k(n))$. Recall that $\mathcal{S}$ is the set of n satisfying $|F^*(n) - u| < \delta$ with $s \leq Y^Z$. We show that $\overline{\mathbf{d}}S_1 < \epsilon$ for δ sufficiently small.

Let $n \in \mathcal{S}_1$, and write $n = st$, where s is the Y-smooth part of n. By assumption, there is an $n' \in \mathcal{S}$ with $n' = s't$, $n' \neq n$, where s' is the Y-smooth part of n'. By fixing s and s', we may rewrite $F^*(n) - F^*(n')$ as a function of t. For all $i \leq k$, let $x_i = f_i(t)$, $\alpha_i = f_i(s)$, and $\beta_i = f_i(s')$. We view α_i and β_i as constants with respect to t. Note that

$$\begin{aligned} F^*(n) - F^*(n') &= F(f_1(s) + f_1(t), \ldots, f_k(s) + f_k(t)) - F(f_1(s') + f_1(t), \ldots, f_k(s') + f_k(t)) \\ &= (\Psi_{\alpha_1,\ldots,\alpha_k} F)(f_1(t), \ldots, f_k(t)) - (\Psi_{\beta_1,\ldots,\beta_k} F)(f_1(t), \ldots, f_k(t)). \end{aligned}$$

By Proposition 2.2.10, $P := \Psi_{\alpha_1,\ldots,\alpha_k} F - \Psi_{\beta_1,\ldots,\beta_k} F$ is not identically zero. Recall that $|F^*(n) - u|$ and $|F^*(n') - u|$ are both less than δ because n and n' are both elements of $\mathcal{S}$. By the Triangle Inequality,

$$|P(f_1(t), \ldots, f_k(t))| = |F^*(n) - F^*(n')| < 2\delta.$$

If P is a nonzero constant, then this is impossible for δ sufficiently small. Suppose P

has positive degree. Since $\deg P < d$, the minimality of d implies that $P(f_1, \ldots, f_k)$ is nonclustering. The solutions n to

$$|P(f_1(t), \ldots, f_k(t))| < \delta$$

form a set of upper density $< \epsilon$, for sufficiently small δ. For each pair s, s', there exists a constant $\delta_{s,s'}$ such that if $\delta < \delta_{s,s'}$, then the upper density of $n \in \mathcal{S}_1$ with Y-smooth part s for which there exists some $n' \in \mathcal{S}_1$ with the same Y-rough part as n and Y-smooth part s' is less than ϵ/Y^{2Z}. Let $\delta < \min_{s,s'} \delta_{s,s'}$. Every $n \in \mathcal{S}_1$ corresponds to some pair s, s'. Because there are at most Y^{2Z} such pairs, $\mathcal{S}_1$ has upper density less than ϵ. □

2.2.3.4.0 The upper density of $\mathcal{S}_2$

Let $\mathcal{S}_2 = \mathcal{S}_2(f_1, \ldots, f_k, F, \delta, u, Y, Z)$. We now estimate the upper density of $\mathcal{S}_2$.

Let x be a large real number. For each pair of nonnegative integers U, V, define

$$\mathcal{S}_2(U, V) = \{n \in \mathcal{S}_2 : n \in (x/2^{U+1}, x/2^U], t \in (x/2^{(U+1)+V}, x/2^{U+V}]\}.$$

We have the following equality in which the right-hand union is disjoint:

$$\mathcal{S}_2 \cap [1, x] = \bigcup_{U,V \geq 0} \mathcal{S}_2(U, V).$$

If $n \in \mathcal{S}_2(U, V)$, then

$$2^{V-1} < s = n/t < 2^{V+1}.$$

Every $n \in \mathcal{S}_2$ satisfies $s \leq Y^Z$. If $Y^Z \leq 2^{V-1}$, then $\mathcal{S}_2(U, V)$ is empty. Suppose $Y^Z > 2^{V-1}$. We may bound $\#\mathcal{S}_2(U, V)$. Fix the Y-rough component t and count the number of corresponding n. Call these $n_i = s_i t$ for all $i \leq J$, where J is the number of distinct elements

of $\mathcal{S}_2$ with Y-rough part t. Since $n \notin \mathcal{S}_1$, then for all $1 \leq i \leq k$,

$$f_i(s_1) = f_i(s_2) = \cdots = f_i(s_J).$$

In particular, every $n \in \mathcal{S}_2(U,V)$ corresponding to this particular t has $f_1(s) = d$ for a fixed d. In order to bound the number of possible n, we use Theorem 2.2.5. The number of positive integers $S < 2^{V+1}$ for which $f_1(S) = d$ is $\ll 2^{V+1}/\sqrt{E(2^{V+1})}$ where

$$E(T) = \sum_{\substack{p \leq T \\ f_1(p) \neq 0}} \frac{1}{p}.$$

Note that $E(T)$ diverges as $T \to \infty$ by Lemma 2.2.4.

Hence, for every $\rho > 0$, there exists a positive integer $V_0 = V_0(\rho)$ such that whenever $V \geq V_0$, the number of $S < 2^{V+1}$ satisfying $f_1(S) = d$ is at most $2^{V+1}\rho$, uniformly in d. Let ρ be a real number less than 1. Later on, we will fix ρ more precisely. For a fixed t, the number of corresponding $n \in \mathcal{S}_2(U,V)$ is $\leq 2^{V+1}\rho$ when $V \geq V_0$. Otherwise, it is still at most 2^{V+1}.

In addition, $t \leq x/2^{U+V}$ is Y-rough. The number of possible values of t is

$$\leq \frac{x}{2^{U+V}} \prod_{p \leq Y} \left(1 - \frac{1}{p}\right) + O(2^Y) \leq \frac{x}{2^{U+V} \log Y} + O(2^Y).$$

We can combine these upper bounds into

$$\#\mathcal{S}_2(U,V) \leq \begin{cases} \frac{2x}{2^U \log Y} + O(2^{V+Y}), & \text{if } V < V_0 \\ \frac{2\rho x}{2^U \log Y} + O(2^{V+Y}), & \text{if } V \geq V_0. \end{cases}$$

We sum over U and V. Let $\mathcal{S}_2(U) = \bigcup_V \mathcal{S}_2(U,V)$. As explained above, we only need to

consider V satisfying $2^{V-1} < Y^Z$. Thus,

$$\begin{aligned}\#\mathcal{S}_2(U) &\leq \sum_{\substack{0\leq V<V_0\\ V<\frac{\log(Y^Z)}{\log 2}+1}} \left(\frac{2x}{2^U \log Y} + O(2^{V+Y})\right) + \sum_{\substack{V\geq V_0\\ V<\frac{\log(Y^Z)}{\log 2}+1}} \left(\frac{2\rho x}{2^U \log Y} + O(2^{V+Y})\right)\\ &\leq \left(\frac{2V_0}{\log Y}\right)\frac{x}{2^U} + (4\rho Z)\frac{x}{2^U} + O(2^Y Y^Z).\end{aligned}$$

We sum this over $U \leq \log x/\log 2$ to complete the proof, obtaining

$$\#\mathcal{S}_2 \cap [1,x] \leq \left(\frac{4V_0}{\log Y} + 8\rho Z\right)x + O(2^Y Y^Z \log x).$$

The upper density of $\mathcal{S}_2$ is at most the coefficient of x, giving us

$$\overline{\mathbf{d}}\mathcal{S}_2 \leq \frac{4V_0}{\log Y} + 8\rho Z.$$

Fix $Z > Z_0$ and $\rho = \epsilon/(16Z)$. This allows us to fix $V_0 = V_0(\rho)$. Having done so, we choose Y so that $4V_0/\log Y < \epsilon/8$. Selecting these parameters ensures that the upper density of $\mathcal{S}_2$ is less than ϵ. Given Y and Z, we may choose δ sufficiently small so that the upper density of $\mathcal{S}_1$ and the upper density of solutions of (3) that do not belong to $\mathcal{S}$ are both less than ϵ. Therefore, the upper density of n satisfying (3) is less than 3ϵ.

2.2.4 Products of additive functions

We deduce the following result from Theorem 1.1.11.

Theorem 2.2.15. *Every product of nonclustering additive functions is nonclustering.*

Proof. Let $f_1, \dots, f_k$ be nonclustering additive functions. If every nontrivial linear combination of $f_1, \dots, f_k$ is nonclustering, then we are done by Theorem 1.1.11. Let $F(n) =$

$f_1(n) \cdots f_k(n)$ and $u \in \mathbb{R}$. We show that for all $\epsilon > 0$, there exists a $\delta > 0$ such that

$$\overline{\mathbf{d}}\{n : |F(n) - u| < \delta\} < \epsilon.$$

We assume that some nontrivial linear combination of $f_1, \ldots, f_k$ is clustering. Let m be the largest integer for which there exists a set of m distinct numbers $i_1, \ldots, i_m$ such that every linear combination of $f_{i_1}, \ldots, f_{i_m}$ is nonclustering. Without loss of generality, let these functions be $f_1, \ldots, f_m$. Then, for all $r > m$, there exist constants $c_{r,1}, \ldots, c_{r,m}$ such that

$$f_r - (c_{r,1}f_1 + \ldots + c_{r,m}f_m)$$

is clustering. Let $\mathcal{P}_r$ be the set of all primes p with $f_r(p) \neq c_{r,1}f_1(p) + \cdots + c_{r,m}f_m(p)$.

Lemma 2.2.4 states that if f is a clustering additive function, then the sum of $1/p$ for all p for which $f(p) \neq 0$ converges. For any $r > m$, the sum of $1/p$ over all $p \in \mathcal{P}_r$ is finite. Because $\mathcal{P}$ is the union of the $\mathcal{P}_r$'s, the sum of $1/p$ over all $p \in \mathcal{P}$ is finite. Therefore, there exists a number N_1 such that

$$\sum_{\substack{p > N_1 \\ p \in \mathcal{P}}} \frac{1}{p} < \frac{\epsilon}{4}.$$

Except on a set of upper density $< \epsilon/4$, the N_1-rough part of any integer is not a multiple of any element of $\mathcal{P}$.

There exists a number N_2 such that

$$\sum_{p > N_2} \frac{1}{p^2} < \frac{\epsilon}{4}$$

because the sums of the reciprocals of the squares converges. The set of numbers with an N_2-rough part that is not squarefree has upper density less than $\epsilon/4$. Let $N = \max(N_1, N_2)$ and $n = st$, where s is the N-smooth part of n. Except on a set of upper density less than

$\epsilon/2$, t is squarefree and no prime dividing t belongs to $\mathcal{P}$. If $p|t$, then

$$f_r(p) = c_{r,1}f_1(p) + \cdots + c_{r,m}f_m(p).$$

Because t is squarefree and each f_i is additive,

$$f_r(t) = c_{r,1}f_1(t) + \cdots + c_{r,m}f_m(t).$$

Therefore,

$$\begin{aligned} f_1(n)\cdots f_k(n) &= f_1(n)\cdots f_m(n)f_{m+1}(n)\cdots f_k(n) \\ &= (f_1(s)+f_1(t))\cdots(f_m(s)+f_m(t))(f_{m+1}(s)+f_{m+1}(t))\cdots(f_k(s)+f_k(t)) \\ &= (f_1(s)+f_1(t))\cdots(f_m(s)+f_m(t)) \\ &\quad (f_{m+1}(s)+c_{m+1,1}f_1(t)+\cdots+c_{m+1,m}f_m(t))\cdots \\ &\quad (f_k(s)+c_{k,1}f_1(t)+\cdots+c_{k,m}f_m(t)). \end{aligned}$$

We can write

$$f_1(n)\cdots f_k(n) = F_s(f_1(t),\ldots,f_m(t)),$$

where

$$F_s(x_1,\ldots,x_m) = \prod_{r=1}^{m}(f_r(s)+x_r)\prod_{r=m+1}^{k}(f_r(s)+c_{r,1}x_1+\cdots+c_{r,m}x_m).$$

For each $r \in [m+1,k]$, there is some index i with $c_{r,i} \neq 0$, and so F_s is a nonconstant polynomial in $x_1,\ldots,x_m$. By assumption, every nontrivial linear combination of $f_1,\ldots,f_m$ is nonclustering. Therefore, $F_s(f_1,\ldots,f_m)$ is nonclustering by Theorem 1.1.11.

By repeating an argument from the proof of Lemma 2.2.6, we see that there exists a positive integer z such that the upper density of numbers with N-smooth part $\geq M :=$

$\prod_{p \le N} p^z$ is $< \epsilon/4$. We assume that $s < M$. Because $F_s(f_1, \ldots, f_m)$ is nonclustering, for any $s < M$, there exists a δ_s such that the upper density of numbers n with N-smooth part s and $|F(n) - u| < \delta_s$ is less than $\epsilon/(4M)$ for all $s \le M$. Letting $\delta = \min_{s<M} \delta_s$, we see that the upper density of solutions to $|F(n) - u| < \delta$ for which the N-smooth part is less than M and the N-rough part is squarefree and not a multiple of any element of $\mathcal{P}$ is less than $\epsilon/4$. Therefore, the upper density of solutions to $|F(n) - u| < \delta$ is less than ϵ for δ sufficiently small, which implies that F is nonclustering. $\square$

Chapter 3

Polynomials and the range of the totient function

The central goal of this chapter is to prove Theorem 1.2.3, which we restate here.

Theorem 3.0.1. *For an irreducible quadratic polynomial P with integer coefficients,*

$$V_P(x) = O\left(\frac{x}{(\log x)^{0.0312}}\right).$$

For the rest of this chapter, we let $P(x) = ax^2 + bx + c$.

3.1 Background results

3.1.1 Outline

Suppose $P(n)$ lies in the range of the φ-function. Let p be the largest prime number for which there exists a number m such that $p|m$ and $\varphi(m) = P(n)$. By definition, $p-1|P(n)$. We write $P(n) = (p-1)v$. We choose a number $T = o(x)$, which we will optimize later. There are three cases:

1. $p > 4ax$,

2. $T < p \leq 4ax$,

3. $p \leq T$.

For a given number k, let $\rho(k)$ be the number of solutions to the congruence $P(n) \equiv 0 \bmod k$. Note that ρ is a multiplicative function. Let D be the discriminant of $P(x)$. If a prime q does not divide $2a$, then the solutions to $P(x) \equiv 0 \bmod q$ are

$$x \equiv \frac{-b \pm \sqrt{D}}{2a} \bmod q,$$

assuming D is a quadratic residue mod q. If D is a non-residue, then there are no solutions. Hence, for a given $q \nmid 2aD$,

$$\rho(q) = \begin{cases} 2, & \text{if } \left(\frac{D}{q}\right) = 1, \\ 0, & \text{if } \left(\frac{D}{q}\right) = -1. \end{cases}$$

For all but finitely many q, $q \nmid 2aD$. In order to determine the density of primes which split, ramify, or are inert in $\mathbb{Q}[\sqrt{D}]$, we must write a special case of the Chebotarev Density Theorem [10]. In order to write this result, we need a definition.

Definition. Let L be a finite abelian extension of the number field K with Galois group G. Let $\mathcal{O}_K$ be the ring of algebraic integers of K. For a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ which is unramified in L, let the *Artin symbol* $A(\mathfrak{p})$ be the unique element of $\mathrm{Gal}(L/K)$ with

$$A(\mathfrak{p})(\alpha) \equiv \alpha^{\#\mathcal{O}_K/\mathfrak{p}} \mod \mathfrak{p}\mathcal{O}_L$$

for all $\alpha \in \mathcal{O}_L$.

Theorem 3.1.1 (Chebotarev Density Theorem for abelian extensions, with error term)**.** *Let K, L, and G satisfy the properties of the previous definition and let C be an element of $Gal(L/K)$. Then,*

$$\#\{\mathfrak{p} \in \mathcal{O}_K : N(\mathfrak{p}) \leq x, A(\mathfrak{p}) \in C\} = \frac{\#C}{\#G}\left(\frac{x}{\log x}\right) + O\left(\frac{x}{(\log x)^2}\right),$$

where $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$ in $\mathcal{O}_K$.

Chebotarev showed that the lefthand side is asymptotic to the main term of the righthand side and Artin later found the error term [1, Satz 4]. For a set of primes $S \subseteq \mathcal{O}_K$, we define the density of S as

$$\mathbf{d}(S) = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S : (\mathcal{O}_K/\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in \mathcal{O}_K : (\mathcal{O}_K/\mathfrak{p}) \leq x\}},$$

assuming this limit exists. One corollary of the Chebotarev Density Theorem is that

$$\mathbf{d}(\{\mathfrak{p} \in \mathcal{O}_K : N(\mathfrak{p}) \leq x, A(\mathfrak{p}) \in C\}) = \#C/\#G.$$

If $L/\mathbb{Q}$ is a quadratic extension of discriminant D, then

$$A(p) = \left(\frac{D}{p}\right)$$

for all $p \nmid D$, if we identify $\mathrm{Gal}(L/\mathbb{Q})$ with $\{\pm 1\}$. We only need to the Chebotarev Density Theorem to make the following observations. The sets

$$\left\{q : \left(\frac{D}{q}\right) = 1\right\}, \left\{q : \left(\frac{D}{q}\right) = -1\right\}$$

both have density $1/2$ in the set of primes. More specifically, the sets

$$\left\{q \leq x : \left(\frac{D}{q}\right) = 1\right\}, \left\{q \leq x : \left(\frac{D}{q}\right) = -1\right\}$$

have size

$$\frac{1}{2}\pi(x) + O\left(\frac{x}{(\log x)^2}\right).$$

Using partial summation, we can show that

$$\sum_{\substack{N(\mathfrak{p})\leq x \\ A(\mathfrak{p})\in C}} \frac{1}{N(\mathfrak{p})} = \frac{\#C}{\#G}\log\log x + O(1).$$

We repeatedly use this estimate to bound products such as

$$\prod_{\substack{p\leq x \\ (\frac{D}{p})=1}} \left(1 - \frac{2}{p}\right),$$

where D is a constant.

3.1.2 A lower bound for $\varphi(n)$

We write a lower bound for $\varphi(n)$.

Theorem 3.1.2 ([36, Theorem 328])**.** *We have*

$$\liminf_{n\to\infty} \frac{\varphi(n)\log\log n}{n} = e^{-\gamma},$$

where $\gamma \approx 0.577$ *is the Euler-Mascheroni constant.*

The specific value on the righthand side of the equation is irrelevant for our purposes. We only need the fact that it is a positive constant. Throughout this chapter, we use the following corollary.

Corollary 3.1.3. We have

$$\varphi(n) \gg \frac{n}{\log\log n}.$$

3.1.3 The normal orders of $\omega(n)$ and $\Omega(n)$

This subsection deals with the "typical" sizes of arithmetic functions. Even though certain arithmetic functions vary wildly, they are almost always close to simple functions.

Recall that for a set of integers S, we define the density of S as

$$d(S) = \lim_{x\to\infty} \frac{\#\{n \le x : n \in S\}}{x},$$

when this quantity exists.

Definition. Let f be an arithmetic function. The function g is a *normal order* of f if for every $\epsilon > 0$,

$$(1-\epsilon)g(n) < f(n) < (1+\epsilon)g(n)$$

holds for almost all n (a set of density 1 in the integers).

The normal order theorems in this chapter all pertain to the following functions.

Definition. Let $\omega(n)$ be the number of distinct prime of factors of n and $\Omega(n)$ be the number of (not necessarily distinct) prime factors of n. In addition, for a given y, we let $\omega_y(n)$ and $\Omega_y(n)$ be the numbers of such prime factors which are $\le y$.

For a number n,

$$\omega_y(n) = \sum_{\substack{p|n \\ p\le y}} 1, \quad \Omega_y(n) = \sum_{\substack{p^{e_p}\|n \\ p\le y}} e_p.$$

The first major result on normal orders of arithmetic functions was the Hardy-Ramanujan Theorem ([35], see [61] for an elementary proof.)

Theorem 3.1.4 (Hardy-Ramanujan Theorem)**.** *The function* $\log\log n$ *is a normal order of both* $\omega(n)$ *and* $\Omega(n)$*.*

A similar argument shows that if P is an irreducible polynomial, then $\log\log n$ is also a normal order of $\omega(P(n))$ and $\Omega(P(n))$. The Erdős-Kac Theorem [25] is a generalization of the Hardy-Ramanujan Theorem. These results tell us how often ω and Ω are close to the mean. We close this section with two results about how often they are far from the mean.

Theorem 3.1.5 ([34, Chapter 0])**.** *Fix $\epsilon > 0$ and $\alpha \in [1, 2-\epsilon]$. The number of $n \leq x$ with $\Omega(n) > \alpha \log\log n$ is $O_\epsilon(x(\log x)^{-Q(\alpha)})$ with $Q(\alpha) = \alpha(\log\alpha) - \alpha + 1$.*

For the next theorem, we let M be the class of non-negative multiplicative functions satisfying the following conditions:

1. there exists a positive constant A such that $f(p^n) \leq A^n$ for all prime p and $n \in \mathbb{Z}_+$,
2. for all $\epsilon > 0$, there exists a positive constant $B = B(\epsilon)$ such that $f(n) \leq Bn^\epsilon$ for all $n \in \mathbb{Z}_+$.

Theorem 3.1.6 ([46])**.** *Let $f \in M$, let P be an irreducible polynomial with no fixed prime divisors, and $\alpha, \delta \in (0,1)$. For all $x, y \geq 2$ with $x^\alpha \leq y \leq x$,*

$$\sum_{x-y<n\leq x} f(|P(n)|) \ll y \prod_{p\leq x}\left(1-\frac{\rho(p)}{p}\right)\exp\left(\sum_{p\leq x}\frac{f(p)\rho(p)}{p}\right),$$

provided that $x \geq c||P||^\delta$, where c is a constant depending only on $\deg P$, α, δ, and B, and $||P||$ is the largest absolute value of a coefficient of P.

Fix $z > 1$. We show that $f(n) = z^{\omega(n)} \in M$. Note that $f(n) = z^{\omega(n)}$ is a non-negative multiplicative function. In addition, $f(p^\ell)$ is 1 or z for all p and ℓ. We observe that $f(n) \ll n^\epsilon$ for all $\epsilon > 0$:

$$f(n) = z^{\omega(n)} \ll z^{\log n/\log\log n} = n^{\log z/\log\log n} \ll n^\epsilon.$$

Hence, the previous theorem provides a bound on the sum of $z^{\omega(n)}$ over all $n \leq x$. To give the reader an idea of why such an estimate is useful to us, note that we could use this result

to bound how often $\omega(n)$ is large. For any C, we have

$$\#\{n \leq x : \omega(n) \geq C\} \leq \frac{1}{z^C} \sum_{n \leq x} z^{\omega(n)}.$$

We use an argument of this kind in the proof of Lemma 3.3.3, with $\omega(n)$ replaced with $\omega_T(P(n))$.

3.1.4 Brun's Sieve

Brun created his sieve in 1915 as a way of approaching the Goldbach and Twin Prime Conjectures [9]. Rather than write Brun's Sieve in full generality [35, Theorem 2.1], we instead write a simplified version.

Theorem 3.1.7 (Brun's Sieve)**.** *Fix $A > 0$ and $k \in \mathbb{Z}_+$. To each prime $p \leq x^A$, associate $k_p \leq k$ residue classes mod p. The number of positive integers $n \leq x$ that do not lie in any of these residue classes is*

$$\ll_{k,A} x \prod_{p \leq x^A} \left(1 - \frac{k_p}{p}\right).$$

We highlight an application of Brun's Sieve that will be useful later in this chapter. Let P be a fixed primitive irreducible polynomial ("primitive" means that the gcd of the coefficients is 1). For each prime q, $P(n)$ takes $\rho(q)$ possible values mod q as n ranges over the integers. A notable corollary of Brun's Sieve [35, Theorem 2.6] states that

$$\#\{n \leq x : P(n) \text{ is prime}\} \ll x \prod_{\substack{q < x \\ \rho(q) \neq q}} \left(1 - \frac{\rho(q)}{q}\right).$$

In our case, P is quadratic, which allows us to use the formula for $\rho(q)$ in Section 1. We

deduce that

$$\#\{n \le x : P(n) \text{ is prime}\} \ll x \prod_{\substack{q<x \\ (\frac{D}{q})=1}} \left(1 - \frac{2}{q}\right).$$

3.2 A large factor of the form $p - 1$

Let V_1 be the number of $n \le x$ for which $p > 4ax$.

Theorem 3.2.1. *We have*

$$V_1 = O\left(\frac{x(\log\log x)^5}{(\log x)^{1-(e(\log 2)/2)}}\right).$$

Proof. We write $\varphi(m) = P(n)$ with $p|m$ for some $p > 4ax$. We first bound m. Note that $P(n) = an^2 + bn + c \le 2an^2 \le 2ax^2$ for x sufficiently large. By Corollary 3.1.3, $m \ll x^2 \log\log x$.

Using dyadic intervals, we can show that the number of $m \ll x^2 \log\log x$ with a divisor of the form p^2 with $p > 4ax$ is $O(x \log\log x/\log x)$. Hence, we may assume that p^2 does not divide m. We write $m = pr$ with $p \nmid r$. So, $\varphi(m) = P(n) = (p-1)v$ with $\varphi(r) = v$. Because $p > 4ax$ and $P(n) \le 2ax^2$, $v < x/2$ as well.

We write

$$n \equiv t_1, \ldots, t_{\rho(v)} \bmod v,$$

with $0 \leq t_i < v$ for all $i \leq \rho(v)$. Fix i and let $t = t_i$. Let $n = uv + t$. We have

$$\begin{aligned} p &= \frac{P(n)}{v} + 1 \\ &= \frac{P(uv+t)}{v} + 1 \\ &= \frac{a(uv+t)^2 + b(uv+t) + c}{v} + 1 \\ &= avu^2 + (2at+b)u + \left(\frac{at^2+bt+c}{v} + 1\right). \end{aligned}$$

So, we can recast the problem in terms of u. Given v and a, we look for the number of values of u for which the quadratic expression above is prime, then sum over all v and a. In other words, we want to bound the size of

$$M = M_{v,t} = \{u \leq x/v : R(u) \text{ is prime}\},$$

where

$$R(u) = avu^2 + (2at+b)u + \left(\frac{at^2+bt+c}{v} + 1\right).$$

The discriminant of R is $D - 4av$. If R is reducible, then $D - 4av$ is a square. The number of v for which $D - 4av$ is non-negative is $O_P(1)$. For each value of v, the number of corresponding n is also $O_P(1)$. Because there are $O(1)$ values of n for which R is reducible, we assume that R is irreducible. Brun's Sieve gives us

$$\#M \ll \frac{x}{v} \prod_{\substack{q < x/v \\ \rho_R(q) \neq q}} \left(1 - \frac{\rho_R(q)}{q}\right),$$

where $\rho_R(q)$ the number of solutions to $R(u) \equiv 0 \bmod q$ for a given prime q.

The number of possible n is the sum of $\#M$ over all possible v and t. In addition, v lies in the range of Euler's function. For notational convenience, we let $\sum'$ have the condition

that $D-4av$ is not a square. We have

$$V_1 \ll \sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}}{}' \sum_{\substack{0\le t<v\\ P(t)\equiv 0(v)}} \frac{x}{v} \prod_{\substack{2<q<x/v\\ \rho_R(q)\neq q}} \left(1-\frac{\rho_R(q)}{q}\right).$$

We now bound

$$\sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}}{}' \sum_{\substack{0\le t<v\\ P(t)\equiv 0(v)}} \frac{x}{v} \prod_{\substack{q<x/v\\ \rho_R(q)\neq q}} \left(1-\frac{\rho_R(q)}{q}\right) \ll x \sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}}{}' \frac{\rho(v)}{v} \prod_{\substack{2<q<x/v\\ q\nmid av(D-4av)\\ \left(\frac{D-4av}{q}\right)=1}} \left(1-\frac{2}{q}\right).$$

For the product, we multiply by a similar product over the q dividing $2av(D-4av)$ in order to make it easier to manipulate:

$$x \sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}}{}' \frac{\rho(v)}{v} \prod_{\substack{q<x/v\\ \left(\frac{D-4av}{q}\right)=1}} \left(1-\frac{2}{q}\right) \prod_{\substack{2<q<x/v\\ q\mid av(D-4av)\\ \left(\frac{D-4av}{q}\right)=1}} \left(1-\frac{2}{q}\right)^{-1}.$$

We simplify the second product as follows:

$$\begin{aligned}
\prod_{\substack{q<x/v\\ q\mid av(D-4av)\\ \left(\frac{D-4av}{q}\right)=1}} \left(1-\frac{2}{q}\right)^{-1} &\ll \prod_{q\mid v(D-4av)} \left(1-\frac{1}{q}\right)^{-2} \\
&= \left(\frac{v(D-4av)}{\varphi(v|D-4av|)}\right)^2 \\
&\ll (\log\log(v|D-4av|))^2 \\
&\ll (\log\log v)^2.
\end{aligned}$$

We now have

$$V_1 \ll x \sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}}{}' \frac{\rho(v)(\log\log v)^2}{v} \prod_{\substack{q<x/v\\ \left(\frac{D-4av}{q}\right)=1}} \left(1-\frac{2}{q}\right).$$

For small v it is not difficult to show that $D-4av$ is a quadratic residue mod q for about half of all $q < x/v$. Unfortunately, v may be large enough relative to x that this is not always true. We bound the product from above:

$$\begin{aligned}\prod_{\substack{q<x/v\\ \left(\frac{D-4av}{q}\right)=1}}\left(1-\frac{2}{q}\right) &= \prod_{2<q<x/v}\left(1-\frac{1}{q}\left(1+\left(\frac{D-4av}{q}\right)\right)\right)\prod_{\substack{2<q<x/v\\ q|D-4av}}\left(1-\frac{1}{q}\right)^{-1}\\ &\ll \frac{|D-4av|}{\varphi(|D-4av|)}\prod_{2<q<x/v}\left(1-\frac{1}{q}\right)\prod_{2<q<x/v}\left(1-\frac{1}{q}\left(\frac{D-4av}{q}\right)\right)\\ &\ll \frac{\log\log v}{\log(x/v)}\prod_{2<q<x/v}\left(1-\frac{1}{q}\left(\frac{D-4av}{q}\right)\right).\end{aligned}$$

Therefore,

$$\begin{aligned}V_1 &\ll x\sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}}{}'\frac{\rho(v)(\log\log v)^3}{v\log(x/v)}\prod_{2<q<x/v}\left(1-\frac{1}{q}\left(\frac{D-4av}{q}\right)\right)\\ &\ll x(\log\log x)^3\sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}}{}'\frac{\rho(v)}{v\log(x/v)}\prod_{2<q<x/v}\left(1-\frac{1}{q}\left(\frac{D-4av}{q}\right)\right).\end{aligned}$$

We combine Lemmas 6 and 8 of [51] into one result, which we apply to the Kronecker symbol.

Lemma 3.2.2. For every $\epsilon > 0$, every squarefree integer d, and every real number y,

$$\prod_{2<q\le y}\left(1-\frac{1}{q}\left(\frac{d}{q}\right)\right) = O(d^{\epsilon}).$$

In addition, the number of (not necessarily squarefree) $d \le x$ for which

$$\prod_{2<q\le y}\left(1-\frac{1}{q}\left(\frac{d}{q}\right)\right) \le (\log\log|3d|)^2$$

does not hold for some y is $O(x^\epsilon)$.

If $q \nmid D - 4av$ and d is the squarefree part of $D - 4av$ (the result of dividing $D - 4av$ by its largest square divisor), then

$$\left(\frac{D-4av}{q}\right) = \left(\frac{d}{q}\right).$$

When d is the squarefree part of $D - 4av$,

$$\begin{aligned}
\prod_{2<q\le y}\left(1-\frac{1}{q}\left(\frac{D-4av}{q}\right)\right) &= \prod_{\substack{2<q\le y\\ q\nmid D-4av}}\left(1-\frac{1}{q}\left(\frac{d}{q}\right)\right)\\
&= \prod_{\substack{2<q\le y\\ q\mid D-4av}}\left(1-\frac{1}{q}\left(\frac{d}{q}\right)\right)^{-1}\prod_{2<q\le y}\left(1-\frac{1}{q}\left(\frac{d}{q}\right)\right)\\
&\le \prod_{\substack{2<q\le y\\ q\mid D-4av}}\left(1-\frac{1}{q}\right)^{-1}\prod_{2<q\le y}\left(1-\frac{1}{q}\left(\frac{d}{q}\right)\right)\\
&= \frac{D-4av}{\varphi(|D-4av|)}\prod_{2<q\le y}\left(1-\frac{1}{q}\left(\frac{d}{q}\right)\right)\\
&\ll (\log\log|3(D-4av)|)\prod_{2<q\le y}\left(1-\frac{1}{q}\left(\frac{d}{q}\right)\right).
\end{aligned}$$

For a given squarefree number d, the number of numbers $\le x$ with squarefree part d is $O(x^{1/2})$. For all but $O(x^{(1/2)+\epsilon})$ numbers $v \le x/2$,

$$\prod_{2<q\le y}\left(1-\frac{1}{q}\left(\frac{D-4av}{q}\right)\right) \le (\log\log|3(D-4av)|)^3.$$

Let $S(k)$ be the squarefree part of k. We split our sum into two parts.

Suppose $S(D-4av) \notin \mathcal{D}$:

$$\sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}}{}' \frac{\rho(v)}{v\log(x/v)} \prod_{2<q<x/v}\left(1-\frac{1}{q}\left(\frac{D-4av}{q}\right)\right) \ll (\log\log x)^3 \sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}} \frac{\rho(v)}{v\log(x/v)}.$$

We bound this sum using dyadic intervals:

$$\begin{aligned}
\sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}} \frac{\rho(v)}{v\log(x/v)} &= \sum_{i<\log x/\log 2} \sum_{\substack{2^i<x/v\le 2^{i+1}\\ v\in\varphi(\mathbb{Z}_+)}} \frac{\rho(v)}{v\log(x/v)} \\
&\ll \sum_{i<\log x/\log 2} \frac{2^i}{x\log(2^i)} \sum_{\substack{2^i<x/v\le 2^{i+1}\\ v\in\varphi(\mathbb{Z}_+)}} \rho(v) \\
&\ll \sum_{i<\log x/\log 2} \frac{1}{i}\left(\frac{1}{x/2^i}\right) \sum_{\substack{v<x/2^i\\ v\in\varphi(\mathbb{Z}_+)}} \rho(v).
\end{aligned}$$

We bound the sum of the $\rho(v)$ terms using Hölder's Inequality. Let $A, B > 1$ satisfy $(1/A)+(1/B)=1$. Recall that $V(x)$ is the number of $n \le x$ in the range of φ. For the following equation, we use the fact that $V(x) \ll x/(\log x)^{1-\epsilon}$ for all $\epsilon > 0$. We have

$$\begin{aligned}
\sum_{\substack{v<x/2^i\\ v\in\varphi(\mathbb{Z}_+)}} \rho(v) &\ll \left(\sum_{v<x/2^i} \rho(v)^A\right)^{1/A} \left(\sum_{\substack{v<x/2^i\\ v\in\varphi(\mathbb{Z}_+)}} 1^B\right)^{1/B} \\
&\ll \left(\sum_{v<x/2^i} \rho(v)^A\right)^{1/A} (V(x/2^i))^{1/B} \\
&\ll \left(\sum_{v<x/2^i} \rho(v)^A\right)^{1/A} \left(\frac{x/2^i}{(\log(x/2^i))^{1-\epsilon}}\right)^{1/B}.
\end{aligned}$$

In order to bound the sum of $\rho(v)^A$, we use the first of the following two upper bounds on partial sums of nonnegative multiplicative functions (the $k=1$, $y=x$ cases of [57], [50]).

We use the second bound in Section 3.3.1.

Theorem 3.2.3. *Let $f \in M$, as used in Theorem 3.1.6.*

(a) We have

$$\sum_{n \le x} f(n) \ll \frac{x}{\log x} \exp\left(\sum_{p \le x} \frac{f(p)}{p}\right).$$

(b) In addition,

$$\sum_{p \le x} f(p-1) \ll \frac{x}{(\log x)^2} \exp\left(\sum_{p \le x} \frac{f(p)}{p}\right).$$

We show that $\rho \in M$. For a given prime p, let $p^{\sigma_1} \| D$. It is well-known (see [46, Theorem 53]) that if some coefficient of $P(x)$ is not a multiple of p, then $\rho(p^r) \le \rho(p^{2\sigma_1+1})$. Suppose $P(x) = p^{\sigma_2} Q(x)$ where σ_2 is maximal, i.e. some coefficient of $Q(x)$ is not a multiple of p. For all $r \ge \sigma_2$, $\rho(p^r) = \rho_Q(p^{r-\sigma_2})$ because each solution to the congruence $Q(x) \equiv 0 \bmod p^{r-\sigma_2}$ lifts to a solution of $P(x) \equiv 0 \bmod p^r$. (If $r \le \sigma_2$, then $\rho(p^r) = p^r \le p^{\sigma_2}$). So,

$$\rho(p^r) = \rho_Q(p^{r-\sigma_2}) \le \rho_Q(p^{2(\sigma_1 - 2\sigma_2)+1})$$

because the discriminant of $Q(x)$ is $D/p^{2\sigma_2}$. For all r,

$$\rho(p^r) \le \max(\rho_Q(p^{2(\sigma_1-2\sigma_2+1}), p^{\sigma_2}).$$

For all but finitely many p, $\sigma_1 \le 2$. Thus, $\rho(p^r)$ is bounded by a constant C, giving us (1). We have

$$\rho(n) \le C^{\omega(n)} \ll C^{\log n / \log\log n} = o(n^\epsilon)$$

for all $\epsilon > 0$, implying (2).

Therefore,

$$\begin{aligned}
\sum_{v<x/2^i} \rho(v)^A &\ll \frac{x/2^i}{\log(x/2^i)} \exp\left(\sum_{q<x/2^i} \frac{\rho(q)^A}{q}\right) \\
&\ll \frac{x/2^i}{\log(x/2^i)} \exp\left(\sum_{q|2aD} \frac{q^A}{q} + \sum_{\substack{q<x/2^i \\ q\nmid 2aD \\ \left(\frac{D}{q}\right)=1}} \frac{2^A}{q}\right) \\
&\ll \frac{x/2^i}{\log(x/2^i)} \exp\left(\sum_{\substack{q<x/2^i \\ \left(\frac{D}{q}\right)=1}} \frac{2^A}{q}\right) \\
&\ll \frac{x/2^i}{\log(x/2^i)} \exp(2^{A-1} \log\log(x/2^i)) \\
&\ll (x/2^i)(\log(x/2^i))^{2^{A-1}-1}.
\end{aligned}$$

Plugging this into our earlier inequality gives us

$$\sum_{\substack{v<x/2^i \\ v\in\varphi(\mathbb{Z}_+)}} \rho(v) \ll \left(\frac{x}{2^i}\right)\left(\log\left(\frac{x}{2^i}\right)\right)^{\frac{2^{A-1}-1}{A}-\frac{1}{B}+\frac{\epsilon}{B}} = \left(\frac{x}{2^i}\right)\left(\log\left(\frac{x}{2^i}\right)\right)^{\frac{2^A}{2A}-1+\left(1-\frac{1}{A}\right)\epsilon}.$$

The minimum value of $(2^A/(2A)) - 1$ is $((e\log 2)/2) - 1 < 0$, which occurs at $A = 1/\log 2$. Hence,

$$\sum_{\substack{v<x/2^i \\ v\in\varphi(\mathbb{Z}_+)}} \rho(v) \ll \frac{x/2^i}{(\log(x/2^i))^{1-((e\log 2)/2)-(1-\log 2)\epsilon}},$$

giving us

$$\begin{aligned}\sum_{\substack{v<x/2\\ v\in\varphi(\mathbb{Z}_+)}} \frac{\rho(v)}{v\log(x/v)} &\ll \sum_{i<\log x/\log 2} \frac{1}{i}\left(\frac{1}{x/2^i}\right) \sum_{\substack{v<x/2^i\\ v\in\varphi(\mathbb{Z}_+)}} \rho(v)\\ &\ll \sum_{i<\log x/\log 2} \frac{1}{i(\log(x/2^i))^{1-((e\log 2)/2)-(1-\log 2)\epsilon}}.\end{aligned}$$

For notational convenience, we replace ϵ with $(1-\log 2)\epsilon$. We may now finish off our dyadic interval. In order to bound this sum, we split it into two cases: $i > K$ and $i < K$, with $K = (\log x)^{O(1)}$:

$$\sum_{i<K} \frac{1}{i(\log(x/2^i))^{1-(e(\log 2)/2)-\epsilon}} \ll \sum_{i<K} \frac{1}{i(\log(x/2^K))^{1-(e(\log 2)/2)-\epsilon}} \ll \frac{\log K}{(\log(x/2^K))^{1-(e(\log 2)/2)-\epsilon}},$$

$$\sum_{K<i<\log x/\log 2} \frac{1}{i(\log(x/2^i))^{1-(e(\log 2)/2)-\epsilon}} \ll \sum_{i<\log x/\log 2} \frac{1}{K} \ll \frac{\log x}{K}.$$

Setting the two sums equal to each other suggests choosing $K = (\log x)^{e(\log 2)/2}$. This yields

$$\sum_{\substack{v<x/2\\ S(D-4av)\notin\mathcal{D}}} \sum_t \#M_{v,t} \ll \frac{x}{(\log x)^{1-e(\log 2)/2-\epsilon}}.$$

Suppose $S(D-4av) \in \mathcal{D}$. Let U be a function of x chosen with $U = O(x^\epsilon)$ for all ϵ. Suppose $v \le U$. We want to bound

$$(\log\log x)^3 \sum_{v\le U}{}' \frac{\rho(v)}{v\log(x/v)} \prod_{q<x/v}\left(1-\frac{1}{q}\left(\frac{D-4av}{q}\right)\right).$$

By Lemma 3.2.2, the product above is $O(v^\epsilon)$ for any $\epsilon > 0$. In addition, $\log(x/v) \gg \log x$

because $v \leq U$. We already established that $\rho(v) \ll v^{\epsilon}$. Putting this together, we have

$$\sum_{v \leq U}{}' \frac{\rho(v)}{v \log(x/v)} \prod_{q<x/v} \left(1 - \frac{1}{q}\left(\frac{D-4av}{q}\right)\right) \ll \sum_{v<U} \frac{1}{v^{1-2\epsilon} \log x} \ll \frac{U^{2\epsilon}}{\log x}.$$

Now, we consider the case where $S(D-4av) \in \mathcal{D}$ and $U < v < x/2$. We have

$$\sum_{\substack{U<v<x/2 \\ S(D-4av)\in\mathcal{D}}}{}' \frac{\rho(v)}{v \log(x/v)} \prod_{q<x/v} \left(1 - \frac{1}{q}\left(\frac{D-4av}{q}\right)\right) \ll \sum_{\substack{U<v<x/2 \\ S(D-4av)\in\mathcal{D}}} \frac{1}{v^{1-2\epsilon} \log(x/v)}.$$

Because $v < x/2$, $\log(x/v) \gg 1$. At this point, we use dyadic intervals:

$$\begin{aligned}
\sum_{\substack{U<v<x/2 \\ S(D-4av)\in\mathcal{D}}} \frac{1}{v^{1-2\epsilon}} &\ll \sum_i \sum_{\substack{2^i U<v<2^{i+1}U \\ S(D-4av)\in\mathcal{D}}} \frac{1}{v^{1-2\epsilon}} \\
&\ll \frac{1}{U^{1-2\epsilon}} \sum_i \sum_{\substack{v<2^{i+1}U \\ S(D-4av)\in\mathcal{D}}} \frac{1}{2^{(1-2\epsilon)i}} \\
&\ll \frac{1}{U^{1-2\epsilon}} \sum_i \frac{(2^{i+1}U)^{(1/2)+2\epsilon}}{2^{(1-2\epsilon)i}} \\
&\ll \frac{1}{U^{(1/2)-4\epsilon}} \sum_i \frac{1}{2^{((1/2)-2\epsilon)i}} \\
&\ll \frac{1}{U^{(1/2)-4\epsilon}}.
\end{aligned}$$

We add our sums for $v < U$ and $v \geq U$ together:

$$\sum_{\substack{v<x/2 \\ S(D-4av)\in\mathcal{D}}}{}' \frac{\rho(v)}{v \log(x/v)} \prod_{q<x/v} \left(1 - \frac{1}{q}\left(\frac{D-4av}{q}\right)\right) \ll \frac{U^{2\epsilon}}{\log x} + \frac{1}{U^{(1/2)-4\epsilon}}.$$

We choose U so that

$$\frac{1}{\log x} = \frac{1}{U^{1/2}}.$$

Thus,

$$U = (\log x)^2$$

and

$$\begin{aligned}\sum_{\substack{v<x/2\\ S(D-4av)\in\mathcal{D}}}{}' \frac{\rho(v)(\log\log v)^3}{v\log(x/v)} \prod_{q<x/v}\left(1-\frac{1}{q}\left(\frac{D-4av}{q}\right)\right) &\ll \frac{1}{(\log x)^{1-4\epsilon}} + \frac{1}{(\log x)^{1-8\epsilon}} \\ &\sim \frac{1}{(\log x)^{1-8\epsilon}}.\end{aligned}$$

We have obtained the following bound:

$$V_1 = O\left(\frac{x}{(\log x)^{1-e(\log 2)/2-\epsilon}} + \frac{x(\log\log x)^3}{(\log x)^{1-8\epsilon}}\right) = O\left(\frac{x}{(\log x)^{1-e(\log 2)/2-\epsilon}}\right). \qquad \square$$

3.3 A factor of the form $p-1$ in the interval $(T, 4ax)$

In this section, we assume that $T < p \le 4ax$. In addition, fix a number $A \in (1/2, 1)$. We define V_2 and V_3 as the number of $n \le x$ for which $T < p < 4ax$ and $\Omega_T(p-1) < A\log\log T$ and the number of $n \le x$ for which $T < p < 4ax$ and $\Omega_T(p-1) > A\log\log T$, respectively.

3.3.1 A bound for V_2

Theorem 3.3.1. *For all $A \in (1/2, 1)$, we have*

$$V_2 = O\left(\frac{x}{(\log T)^{A\log A - A + 1}}\right).$$

Proof. Given p, we can bound the number of $n \le x$ for which $p-1$ divides $P(n)$. The

number of $n \leq x$ for which $p-1|P(n)$ is

$$\frac{x\rho(p-1)}{p-1} + O(\rho(p-1)).$$

In order to bound the number of possible n for any given p satisfying the conditions above, we sum over all possible p. We obtain

$$V_2 \leq \sum_{\substack{T<p<4ax \\ \Omega_T(p-1)<A\log\log T}} \left(\frac{x\rho(p-1)}{p-1} + O(\rho(p-1))\right).$$

We have $\rho(p-1) < (1/(4a))x\rho(p-1)/(p-1)$. So, we only need to consider the first term of the sum in order to bound the order of magnitude:

$$V_2 \ll x \sum_{\substack{T<p<4ax \\ \Omega_T(p-1)<A\log\log T}} \frac{\rho(p-1)}{p-1}.$$

Fix a constant $B < 1$. Because $\Omega_T(p-1) < A\log\log T$,

$$B^{\Omega_T(p-1)} > B^{A\log\log T} = (\log T)^{A\log B}.$$

For each prime p in our sum,

$$\frac{B^{\Omega_T(p-1)}}{(\log T)^{A\log B}} > 1.$$

Multiplying every term in our sum by this quantity will increase the sum. Hence,

$$\begin{aligned}\sum_{\substack{T<p<4ax \\ \Omega_T(p-1)<A\log\log T}} \frac{\rho(p-1)}{p-1} &\leq \sum_{\substack{T<p<4ax \\ \Omega_T(p-1)<A\log\log T}} \frac{\rho(p-1)}{p-1}\left(\frac{B^{\Omega_T(p-1)}}{(\log T)^{A\log B}}\right) \\ &\leq \frac{1}{(\log T)^{A\log B}} \sum_{T<p<4ax} \frac{B^{\Omega_T(p-1)}\rho(p-1)}{p-1}.\end{aligned}$$

Let $k = \log 2$. In order to evaluate this sum, we break it into dyadic intervals:

$$\begin{aligned}\sum_{T<p<4ax} \frac{B^{\Omega_T(p-1)}\rho(p-1)}{p-1} &\leq \sum_{0\leq i<k\log(4ax/T)+1} \sum_{2^iT\leq p<2^{i+1}T} \frac{B^{\Omega_T(p-1)}\rho(p-1)}{p-1} \\ &\ll \sum_{0\leq i<k\log(4ax/T)+1} \frac{1}{2^iT} \sum_{2^iT\leq p<2^{i+1}T} B^{\Omega_T(p-1)}\rho(p-1).\end{aligned}$$

By Theorem 3.2.3,

$$\begin{aligned}\sum_{2^iT\leq p<2^{i+1}T} B^{\Omega_T(p-1)}\rho(p-1) &\ll \frac{2^{i+1}T}{\log(2^{i+1}T)} \exp\left(\sum_{p<2^{i+1}T} \frac{B^{\Omega_T(p)}\rho(p)}{p} - \sum_{p<2^iT} \frac{1}{p}\right) \\ &\ll \frac{2^iT}{\log(2^iT)} \exp\left(\sum_{p|2aD} \frac{B}{p} + \sum_{\substack{p\leq T \\ \left(\frac{D}{p}\right)=1}} \frac{2B}{p} + \sum_{\substack{T<p<2^{i+1}T \\ \left(\frac{D}{p}\right)=1}} \frac{2}{p} - \sum_{p<2^iT} \frac{1}{p}\right) \\ &\ll \frac{2^iT}{\log(2^i)} \exp(\log\log(2^{i+1}T) - \log\log(2^iT) - (1-B)\log\log T) \\ &\ll \frac{2^iT}{i} \exp(-(1-B)\log\log T) \\ &\sim \frac{2^iT}{i(\log T)^{1-B}}.\end{aligned}$$

Hence,

$$\sum_{T<p<4ax} \frac{B^{\Omega_T(p-1)}\rho(p-1)}{p-1} \ll \sum_{i<k\log(4ax/T)+1} \frac{1}{i(\log T)^{1-B}} \ll \frac{\log\log x}{(\log T)^{1-B}}.$$

Putting all this together shows us that

$$V_2 \ll \frac{x}{(\log T)^{A\log B - B + 1}}.$$

We fix A and let $B = A$ to make $A \log B - B + 1$ as large as possible. Hence,

$$V_2 = O\left(\frac{x}{(\log T)^{A \log A - A + 1}}\right). \qquad \square$$

Note that $A \log A - A + 1$ is positive for all $A \in (1/2, 1)$.

3.3.2 A bound for V_3

Theorem 3.3.2. *We have*

$$V_3 = O\left(\frac{x}{(\log T)^{(A+(1/2)) \log(A+(1/2)) - A + (1/2)}}\right).$$

To prove this theorem, we must show two preliminary results. Suppose $P(n) = (p-1)(q-1)v$ with $p, q > T$ and $\Omega_T(p-1), \Omega_T(q-1) > A \log\log T$. Then, $\Omega_T(P(n)) > 2A \log\log T$. We bound the number of such n with the following results.

Lemma 3.3.3. For all $\epsilon > 0$, the number of $n \leq x$ for which $\omega_T(P(n)) > (1+\epsilon)\log\log T$ is

$$O\left(\frac{x}{(\log T)^{(1+\epsilon)\log(1+\epsilon) - \epsilon}}\right).$$

Proof. Fix $z > 1$. We bound the sum of $z^{\omega_T(P(n))}$.

By Theorem 3.1.6,

$$\sum_{n \leq x} z^{\omega_T(P(n))} \ll x \prod_{q \leq x} \left(1 - \frac{\rho(q)}{q}\right) \exp\left(\sum_{q \leq x} \frac{z^{\omega_T(q)} \rho(q)}{q}\right).$$

We have

$$\begin{aligned}\sum_{n\le x} z^{\omega_T(P(n))} &\ll x \prod_{\substack{q\le x\\ (\frac{D}{q})=1}} \left(1-\frac{2}{q}\right)\exp\left(\sum_{q|2aD}\frac{z}{q}+\sum_{\substack{q<T\\ (\frac{D}{q})=1}}\frac{2z}{q}+\sum_{\substack{T<q\le x\\ (\frac{D}{q})=1}}\frac{2}{q}\right)\\ &\ll x\left(\frac{1}{\log x}\right)\exp(\log\log x+(z-1)\log\log T))\\ &= x(\log T)^{z-1}.\end{aligned}$$

Let M be the number of $n \le x$ for which $\omega_T(P(n)) > (1+\epsilon)\log\log T$. Then,

$$\sum_{n\le x} z^{\omega_T(P(n))} \ge z^{(1+\epsilon)\log\log T} M = (\log T)^{(1+\epsilon)\log z} M.$$

Combining our two bounds gives us

$$M \ll x(\log T)^{z-(1+\epsilon)(\log z)-1}$$

We can choose z to minimize the exponent. At the minimum, $z = 1+\epsilon$, giving us

$$M \ll \frac{x}{(\log T)^{(1+\epsilon)\log(1+\epsilon)-\epsilon}}.$$ □

Theorem 3.3.4. *For all $C, \delta > 0$, the number of $n \le x$ for which $P(n)$ has a square divisor greater than $(\log T)^C$ is*

$$O\left(\frac{x}{(\log T)^{(1-\delta)C/2}}\right).$$

Proof. Suppose $r^2|P(n)$ with $r^2 > (\log T)^C$. Assume $r^2 \le x^{2-\epsilon}$ for a fixed $\epsilon > 0$. The number of possible $n \le x$ is

$$\sum_{r:(\log T)^C < r^2 \le x^{2-\epsilon}} \left(\frac{x\rho(r^2)}{r^2} + O(\rho(r^2))\right).$$

For all $\epsilon > 0$, $\rho(r^2) \ll r^\delta$. Therefore,

$$\sum_{(\log T)^C < r^2 \le x^{2-\epsilon}} \frac{x\rho(r^2)}{r^2} \ll \sum_{r > (\log T)^{C/2}} \frac{x}{r^{2-\delta}} \sim \frac{x}{(\log T)^{(1-\delta)C/2}}$$

and

$$\sum_{(\log T)^C < r^2 \le x^{2-\epsilon}} \rho(r^2) \ll \sum_{r \le x^{1-(\epsilon/2)}} r^\delta \ll x^{1+\delta-(\epsilon/2)}.$$

If $\epsilon > 2\delta$, then the second sum is smaller than a constant multiple of the first one.

We may assume that $r^2 > x^{2-\epsilon}$. If r has a divisor $d \in ((\log T)^{C/2}, x^{1-(\epsilon/2)}]$, then $P(n)$ has a square divisor in the range $((\log T)^C, x^{2-\epsilon}]$, which we have already discussed. Suppose otherwise. Let p be a prime factor of r. If $p \in (x^{\epsilon/2}, x^{1-(\epsilon/2)}/(\log T)^{C/2}]$, then $r/p \in ((\log T)^{C/2}, x^{1-(\epsilon/2)}]$. We may assume that if $p|r$, then $p \le x^{\epsilon/2}$ or $p > x^{1-(\epsilon/2)}/(\log T)^{C/2}$. If every prime factor is $\le x^{\epsilon/2}$, then r has a divisor in the range $((\log T)^{C/2}, x^{1-(\epsilon/2)}]$. Therefore, the largest prime factor of r is greater than $x^{1-(\epsilon/2)}/(\log T)^{C/2}$. There exists some prime $p > x^{1-(\epsilon/2)}/(\log T)^{C/2}$ such that $p^2|P(n)$. The number of n with this property is

$$\sum_{x^{2-\epsilon}/(\log T)^C < p^2 \ll x^2} \left(\frac{x\rho(p^2)}{p^2} + O(\rho(p^2)) \right).$$

We have already established that the first sum is sufficiently small. In addition,

$$\sum_{x^{2-\epsilon}/(\log T)^C < p^2 \ll x^2} \rho(p^2) \ll \frac{x}{\log x}.$$ □

Corollary 3.3.5. For all $\epsilon < 1.75$, the number of $n \le x$ for which $\Omega_T(P(n)) > (1+\epsilon)\log\log T$ is

$$O\left(\frac{x}{(\log T)^{(1+(\epsilon/2))\log(1+(\epsilon/2))-(\epsilon/2)}} \right).$$

Proof. Let $n \le x$. If $\Omega_T(P(n)) > (1+\epsilon)\log\log T$, then there are two possibilities:

1. $\omega_T(P(n)) > (1 + (\epsilon/2)) \log\log T$,

2. $\Omega_T(P(n)) - \omega_T(P(n)) > (\epsilon/2) \log\log T$.

By Lemma 3.3.3, the number of n satisfying the first condition is

$$O\left(\frac{x}{(\log T)^{(1+(\epsilon/2))\log(1+(\epsilon/2))-(\epsilon/2)}}\right).$$

Suppose $\Omega_T(P(n)) - \omega_T(P(n)) > (\epsilon/2)\log\log T$. Then, $P(n)$ has a square factor greater than $2^{(\epsilon/2)\log\log T} = (\log T)^{\epsilon(\log 2)/2}$. By the previous theorem, the number of n satisfying the second condition is

$$O\left(\frac{x}{(\log T)^{\epsilon(\log 2)/4}}\right).$$

For all $\epsilon < 1.75$,

$$(1 + (\epsilon/2))\log(1 + (\epsilon/2)) - (\epsilon/2) < \epsilon(\log 2)/4.$$

Therefore, the number of $n \leq x$ for which $\Omega_T(P(n)) > (1 + \epsilon)\log\log T$ is

$$O\left(\frac{x}{(\log T)^{(1+(\epsilon/2))\log(1+(\epsilon/2))-(\epsilon/2)}}\right). \qquad \square$$

For the rest of this section, we will let $\epsilon < 1.75$. Suppose there exist $p, q \in (T, 4ax)$ with $\Omega_T(p-1), \Omega_T(q-1) > A\log\log T$ and $(p-1)(q-1)|P(n)$. Then $\Omega_T(P(n)) > 2A\log\log T > (1+\epsilon)\log\log T$ for $\epsilon < 2A - 1$, which we have handled with the previous theorem.

The other possibility is that $m = pr$, where r is T-smooth and $\Omega_T(\varphi(r)) < A\log\log T$. If r is T-smooth, then $v = \varphi(r)$ is T-smooth as well. Therefore, $P(n) = (p-1)v$ with v T-smooth. Hence,

$$P(n) = (p-1)v < 4axT^{A\log\log T}.$$

If $T^{A\log\log T} \ll x^{1-\delta}$ for some $\delta > 0$, then $P(n) = O(x^{2-\delta})$, which would imply that $n =$

$O(x^{1-(\delta/2)})$. We find a value of T for which $T^{A \log\log T}$ is very close to $x^{1-\delta}$. We have

$$A \log T \log\log T = (1-\delta)\log x.$$

An approximate solution is

$$T = \exp\left(\frac{1-\delta}{A}\left(\frac{\log x}{\log\log x}\right)\right).$$

For such T (for all $\delta > 0$),

$$V_3 = O\left(\frac{x}{(\log T)^{(1+(\epsilon/2))\log(1+(\epsilon/2))-(\epsilon/2)}}\right) = O\left(\frac{x}{(\log T)^{(A+(1/2))\log(A+(1/2))-A+(1/2)-\delta}}\right).$$

Note that V_1 is independent of T, whereas V_1 and V_2 decrease as T increases. In order to let T be as large as possible, we use the formula for T above for the rest of the chapter.

3.4 The number p is small

Suppose that if $\varphi(m) = P(n)$, then m is T-smooth. We use an argument similar to the one at the end of the previous section to show that the number of such n is negligible. By Theorem 3.3.4, we may assume that $\Omega_T(P(n)) < A \log\log T$. In addition, $P(n)$ is T-smooth because m is T-smooth. Hence,

$$P(n) < T^{A \log\log T} = o(x).$$

So, we may assume that $n = o(x^{1/2})$. We may ignore such n.

3.5 Optimizing parameters

Here are the bounds we obtained (for all $\delta > 0$):

$$V_1 = O\left(\frac{x}{(\log x)^{1-e(\log 2)/2-\delta}}\right),$$

$$V_2 = O\left(\frac{x}{(\log T)^{A\log A-A+1}}\right),$$

$$V_3 = O\left(\frac{x}{(\log T)^{(A+(1/2))\log(A+(1/2))-A+(1/2)-\delta}}\right).$$

The previous section states that if $\varphi(m) = P(n)$, then we may assume that m is not T-smooth. Therefore, $V_P(x)$ is at most the sum of our upper bounds for V_1, V_2, and V_3.

We now optimize our bounds for V_2 and V_3. As A increases, V_2 increases and V_3 decreases. We set V_2 and V_3 approximately equal:

$$\frac{x}{(\log T)^{A\log A-A+1}} = \frac{x}{(\log T)^{(A+(1/2))\log(A+(1/2))-A+(1/2)}},$$

which implies that

$$A\log A - A + 1 = (A + (1/2))\log(A + (1/2)) - A + (1/2).$$

The solution is $A \approx 0.76$. Plugging in this value shows that

$$V_2 + V_3 \ll \frac{x}{(\log T)^{0.0312-\delta}}.$$

Recall that $T = \exp(((1-\delta)/A)(\log x/\log\log x))$. Therefore,

$$V_P(x) = O\left(\frac{x}{(\log x)^{0.0312-\delta}}\right).$$

Chapter 4

Additively unique sets of prime numbers

Recall from the introduction that a set S is additively unique (AU) if the only multiplicative function f for which $f(m+n) = f(m) + f(n)$ for all $m, n \in S$ is the identity function. Spiro proved the following notable result [58].

Theorem 4.0.1. *The primes are AU.*

In this chapter, we refine the previous theorem to prove Theorem 1.3.4, which we restate here.

Theorem 4.0.2. *A set of primes is AU if and only if it contains every prime that is not the larger element of a twin prime pair, and at least one element of* $\{5, 7\}$.

Our proof of this result is very similar to Spiro's proof of Theorem 4.0.1.

4.1 Preliminary results

To start the proof, we show that the primes listed in Theorem 1.3.4 are necessary. From here on, S will refer to a set of primes.

Lemma 4.1.1. If S is AU, then S contains every prime that is not the larger element of a twin prime pair.

Proof. Let p_0 be a prime that is not the larger element of a twin prime pair. Suppose $p_0 \notin S$. Consider the function

$$f(n) = \begin{cases} 1, & \text{if } n \in \{1, p_0\}, \\ 0, & \text{otherwise.} \end{cases}$$

It is clear that f is multiplicative. Let $p, q \in S$. Then, p and q are primes that are not equal to p_0. If $p_0 = 2$, then $p + q > p_0$. Otherwise, p_0 is odd. If $p + q = p_0$, then p or q must be 2. But, this is impossible because p_0 is not the larger element of a twin prime pair. Hence, $p + q \neq p_0$. So, $f(p + q) = f(p) + f(q) = 0$. Thus, $f \in \mathcal{F}$ even though f is not the identity function. If $p_0 \notin S$, then S is not AU. □

The next lemma would still hold if we replaced 5 and 7 with any twin prime pair $p, p+2$, but this would not give us any new information.

Lemma 4.1.2. If S is AU, then S contains 5 or 7.

Proof. Suppose $5, 7 \notin S$. Consider the function

$$f(n) = \begin{cases} 1, & \text{if } n \in \{1, 7\}, \\ 0, & \text{otherwise.} \end{cases}$$

Once again, f is multiplicative. Let $p, q \in S$. Then, $p, q, p + q \neq 7$ because the only way to express 7 as the sum of two primes is $2 + 5$. So, $f \in \mathcal{F}$. Because f is not the identity function, S is not AU. □

Now that we have the necessity of the primes in Theorem 1.3.4, we may spend the rest of this chapter establishing their sufficiency. Over the next few lemmas, we show that if

$f(m+n) = f(m) + f(n)$ for all m, n in an additively unique set S, then $f(n) = n$ for all $n \leq 23$.

Lemma 4.1.3. If $f(p) + f(q) = f(p+q)$ for all $p, q \in S$, then $f(2) = 2$ and $f(3) = 3$.

Proof. Suppose $f(2) \neq 2$. Let p_0 be a prime that is not the larger element of a twin prime pair. We see that

$$f(2)f(p_0) = f(2p_0) = f(p_0) + f(p_0) = 2f(p_0).$$

Hence, $(f(2) - 2)f(p_0) = 0$. However, $f(2) \neq 2$. Thus, $f(p_0) = 0$.

Suppose $5 \in S$. Then, $f(4) = f(2) + f(2) = 2f(2)$ and $f(5) = f(2) + f(3) = f(2)$. In addition,

$$2f(2)^2 = f(4)f(5) = f(20) = f(3) + f(17) = 0 + 0 = 0.$$

Hence, $f(2) = 0$. If p_0 is the larger element of a twin prime pair, then

$$f(p_0) = f(2) + f(p_0 - 2) = 0,$$

implying that f vanishes on all primes.

Suppose $7 \in S$. Then,

$$f(2)f(7) = f(14) = f(3) + f(11) = 0 + 0 = 0.$$

At least one of $f(2), f(7)$ is zero. Once again, $f(4) = 2f(2)$ and $f(5) = f(2)$. Note that

$$f(20) = f(7) + f(13) = f(7)$$

and

$$f(20) = f(4)f(5) = 2f(2)^2.$$

So, $f(2) = 0$ if and only if $f(7) = 0$. Hence, $f(2) = f(7) = 0$. This implies that f vanishes on the primes, which is impossible. Thus, $f(2) = 2$.

We split the proof of $f(3) = 3$ into two cases, depending on whether $5 \in S$ or $7 \in S$. In both parts, we write $f(n)$ in terms of $f(3)$ for multiple values of n, then use these values to solve for $f(3)$. In addition, we note that $f(4) = 2f(2) = 4$ and $f(5) = f(3) + 2$.

1. Suppose $5 \in S$. We have

$$f(7) = f(2) + f(5) = f(3) + 4,$$

$$f(14) = f(2)f(7) = 2f(3) + 8,$$

$$f(11) = f(14) - f(3) = f(3) + 8,$$

$$f(20) = f(4)f(5) = 4f(3) + 8,$$

$$f(17) = f(20) - f(3) = 3f(3) + 8,$$

$$f(22) = f(2)f(11) = 2f(3) + 16,$$

$$f(22) = f(5) + f(17) = 4f(3) + 10,$$

$$4f(3) + 10 = 2f(3) + 16,$$

$$f(3) = 3.$$

2. Suppose $7 \in S$. We have

$$f(10) = f(2)f(5) = 2f(3) + 4,$$

$$f(7) = f(10) - f(3) = f(3) + 4,$$

$$f(14) = f(2)f(7) = 2f(3) + 8,$$

$$f(11) = f(14) - f(3) = f(3) + 8,$$

$$f(13) = f(2) + f(11) = f(3) + 10,$$

$$f(26) = f(2)f(13) = 2f(3) + 20,$$

$$f(23) = f(26) - f(3) = f(3) + 20,$$

$$f(20) = f(4)f(5) = 4f(3) + 8,$$

$$f(17) = f(20) - f(3) = 3f(3) + 8,$$

$$f(34) = f(2)f(17) = 6f(3) + 16,$$

$$f(34) = f(11) + f(23) = 2f(3) + 28,$$

$$6f(3) + 16 = 2f(3) + 28,$$

$$f(3) = 3.$$ □

We extend this lemma a little further.

Lemma 4.1.4. Using the same conditions as before, $f(n) = n$ for all $n \leq 23$.

Proof. We proceed by induction starting from the fact that $f(n) = n$ for all $n < 5$. If n is not a prime power, then $n = ab$, with $\gcd(a, b) = 1$ and $a, b > 1$. So, $f(n) = f(a)f(b) = n$. We only need to check that $f(n) = n$ when n is a prime power. The only possibilities are $n = 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23$. In both cases of the previous proof, $f(4) = 2f(2)$, $f(5) = f(3) + 2$, $f(7) = f(3) + 4$, $f(11) = f(3) + 8$, and $f(17) = 3f(3) + 8$. Therefore, $f(n) = n$ for all $n \in \{5, 7, 11, 17\}$. Here are the other primes:

$$f(13) = f(11) + f(2) = 13,$$

$$f(19) = f(17) + f(2) = 19,$$

$$f(23) = f(26) - f(3) = f(2)f(13) - f(3) = 23.$$

The only remaining cases are $n = 8, 9, 16$. If $5 \in S$, then

$$f(8) = f(5) + f(3) = 8,$$

$$f(16) = f(11) + f(5) = 16,$$

$$f(9) = \frac{f(45)}{f(5)} = \frac{f(44) + f(1)}{5} = \frac{f(4)f(11) + 1}{5} = 9.$$

If $7 \in S$, then

$$f(8) = \frac{f(24)}{f(3)} = \frac{f(17) + f(7)}{3} = 8,$$

$$f(9) = f(7) + f(2) = 9,$$

$$f(16) = \frac{f(48)}{f(3)} = \frac{f(37) + f(11)}{3} = \frac{(f(40) - f(3)) + 11}{3} = \frac{f(5)f(8) + 8}{3} = 16. \qquad \square$$

In addition to proving that the primes are AU unconditionally, Spiro also found a shorter proof conditional on Goldbach's Conjecture. Similarly, we may prove Theorem 1.3.4 using a variant of Goldbach's Conjecture, which we write here.

Conjecture 4.1.5. If n is a composite prime power other than 4, 8, 9, 49, and 64, then $2n$ is the sum of two primes that are not the larger elements of a twin prime pair.

Theorem 4.1.6. *Assuming the conclusion of Conjecture 4.1.5 for all numbers $2n$ with $n \leq M$, $f(n) = n$ for all $n \leq M$.*

Proof. We already know that $f(n) = n$ for all $n \leq 23$. We proceed by induction. Suppose $f(n) = n$ for all $n < m$ with $23 < m \leq M$. We show that $f(m) = m$. If m is not a prime

power, then $m = ab$ for some relatively prime a, b with $a, b > 1$. Therefore,

$$f(m) = f(a)f(b) = ab = m.$$

If m is the larger element of a twin prime pair, then

$$f(m) = f(2) + f(m-2) = 2 + (m-2) = m.$$

Suppose m is a prime for which $m-2$ is not prime. Then, $m + q \equiv 2 \bmod 4$ for some $q \in \{3, 17\}$. In this case, $(m+q)/2$ is an odd number. Because $(m+q)/2 < m$, we have

$$f(m+q) = f(2)f\left(\frac{m+q}{2}\right) = 2\left(\frac{m+q}{2}\right) = m+q,$$

which implies that

$$f(m) = f(m+q) - f(q) = m.$$

Suppose m is a prime power other than 49 and 64. If m is a power of 2, then $m = p + q$ for some prime p, q with $p-2, q-2$ not prime. By our inductive assumption, $f(m) = m$. Suppose m is an odd prime power. Then, $2m = p + q$ with $p-2, q-2$ not prime. Let $p < q$. Then, $p < m < q < 2m$. We know that $f(p) = p$, so it suffices to show that $f(q) = q$. There exists an $r \in \{3, 17, 23, 29\}$ such that $q + r \equiv 4 \bmod 8$. Thus,

$$f(q) + f(r) = f(q+r) = f(4)f\left(\frac{q+r}{4}\right) = q + r.$$

We obtain $f(q) = q$ and $f(m) = m$.

Finally, we consider $n = 49$ and $n = 64$:

$$f(49) = \frac{f(196)}{f(4)} = \frac{f(179) + f(17)}{4} = \frac{(f(182) - f(3)) + 17}{4} = \frac{f(2)f(7)f(13) + 14}{4} = 49,$$

$$f(64) = \frac{f(192)}{f(3)} = \frac{f(187) + f(5)}{3} = \frac{f(11)f(17) + f(5)}{3} = 64. \qquad \square$$

4.2 An unconditional proof

Computational tests show that Conjecture 4.1.5 holds for all prime powers less than 10^{16}. Therefore, $f(n) = n$ for all $n \leq 10^{16}$. Our goal for the rest of this chapter is to show that $f(n) = n$ for all n. First, we show that $f(n) = n$ on a specific set H containing the primes. Then, we show that if n is the smallest number satisfying $f(n) \neq n$, then there exists a number m with $\gcd(m, n) = 1$ and $mn = p + q$ with p, q prime and $p - 2, q - 2$ prime. This will imply that $f(n) = n$ by induction.

Theorem 4.2.1. *Let*

$$H = \{n : v_p(n) \leq 1 \text{ if } p > 1000;\ p^{v_p(n)+1} < 10^9 \text{ if } p < 1000\}.$$

Then, $f(n) = n$ for all $n \in H$.

The following lemma is a variant of [58, Lemma 5]. Throughout the proof of the lemma, we use $\pi_2(x)$ to refer to the number of twin prime pairs with smaller element at most x.

Lemma 4.2.2. For every prime $p > 10^{16}$, there is an odd prime $q < p$ with $q - 2$ not prime such that $p + q \in H$.

Proof. Let $p > 10^{16}$ be prime and $N(p)$ be the number of primes $q < p$ such that $p + q \in H$. In the proof of [58, Lemma 10], Spiro showed that if $p > 10^{10}$, then

$$N(p) \geq 0.3\frac{p-1}{\log(p-1)}.$$

We may put upper bounds on $\pi_2(x)$. Using Brun's Sieve, we have

$$\pi_2(x) \ll \frac{x}{(\log x)^2}.$$

A special case of the Bateman-Horn Conjecture [7] states that

$$\lim_{x\to\infty} \pi_2(x) \left(\frac{x}{(\log x)^2}\right)^{-1} = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \approx 0.66.$$

(The *twin prime constant* is the product above.) Even if we could prove the Bateman-Horn Conjecture, this result would be insufficient as we would not know how quickly the lefthand side of the equation approaches 0.66. We use an explicit result. Suppose $p > 10^{16}$. By [38, Theorem 5.14],

$$\pi_2(p) \leq 7.68 \frac{p}{(\log p)^2}.$$

Because $p > 10^{16}$, $\log p > 36.8$, implying that

$$\pi_2(p) \leq 0.21 \frac{p}{\log p}.$$

For $p > 10^{16}$,

$$\frac{p-1}{\log(p-1)} \left(\frac{p}{\log p}\right)^{-1} = \left(1 - \frac{1}{p}\right) \frac{\log p}{\log(p-1)} > 1 - \frac{1}{p} > 1 - 10^{-16}.$$

Therefore,

$$N(p) \geq 0.3 \frac{p-1}{\log(p-1)} > 0.3(1 - 10^{-16)}) \frac{p}{\log p} > 0.29 \frac{p}{\log p},$$

which gives us

$$N(p) - \pi_2(p) > 0.08 \frac{p}{\log p} \geq 0.08 \frac{10^{16}}{\log(10^{16})} = 2.17 \cdot 10^{13}.$$

Because this difference is greater than 1, there exists an odd prime $q < p$ with $q - 2$ not prime such that $p + q \in H$. □

We can now prove Theorem 4.2.1.

Proof of Theorem 4.2.1. We proceed by induction on H. Let $m \in H$ with $m > 10^{16}$. Assume that $f(n) = n$ for all $n \in H$ with $n < m$. Assume that m is not a prime power. Then, $f(m) = f(a)f(b)$ with $\gcd(a, b) = 1$ and $a, b > 1$. Note that $a, b \in H$ because the exponents of their prime factors are at most as large as they are in m.

Suppose m is a prime power. Then, $m = p^\alpha$ for some prime p. If $p < 1000$, then $p^\alpha < 10^9$, which is impossible. Thus, $p > 1000$. In this case, $\alpha = 1$. Hence, m is prime. If $m - 2$ is prime, then $f(m-2) = m-2$ because $m-2 \in H$. Therefore, $f(m) = f(m-2)+f(2) = m$.

Suppose $m-2$ is composite. There exists an odd prime $q < m$ with $q-2$ not prime such that $m + q \in H$. Clearly, $m + q$ is even. However, $m + q$ is not a power of 2 because every power of 2 in H is less than 10^9. We may write $m+q = 2^k r$ with r odd and $r \in H$. Because $r < m$,

$$f(m) = f(m + q) - f(q) = f(2^k)f(r) - f(q) = 2^k r - q = (m + q) - q = m. \qquad \square$$

Now that we know that $f(n) = n$ for all $n \in H$, we may show that $f(n) = n$ for all n.

Proof of Theorem 1.3.4. We prove the statement for all $n \notin H$. Suppose n is not a multiple of 3. Then, the set of even elements $r \in H$ for which $r \equiv 1 \bmod 3$ and $\gcd(r, n) = 1$ has positive density [41, §174] because H contains all squarefree numbers. Almost all even numbers m can be expressed as a sum of two primes [27]. However, it is also almost always the case that $m - 2$, $m - 3$, and $m - 5$ are composite. Therefore, almost all even numbers

can be expressed as the sum of two primes greater than 5. We have

$$rn = p + q$$

with p, q primes greater than 5 for some r. Because $rn \equiv 1 \bmod 3$, we have $p, q \equiv 2 \bmod 3$. This implies that p and q are not the larger elements of twin prime pairs. Hence,

$$f(r)f(n) = f(rn) = f(p + q) = f(p) + f(q).$$

Because $p, q, r \in H$, $f(p) = p$, $f(q) = q$, and $f(r) = r$. Therefore, $f(n) = n$.

Since f is multiplicative, we only need to show that $f(n) = n$ for all powers of 3 to finish the proof. Let $n = 3^\alpha$. Let p be a prime congruent to 1 mod 3 that is not the larger element of a twin prime pair (such as 37). By Dirichlet's Theorem, there exists a prime q satisfying $3^\alpha \parallel p + q$. Then, $p + q = 3^\alpha r$ with $3 \nmid r$. In addition, p and q are not the larger elements of twin prime pairs. Hence, $f(3^\alpha) = 3^\alpha$. Therefore, f is the identity function. □

Bibliography

[1] E. Artin, Über eine neue Art von L-Reihen, Abh. Math. Sem. Univ. Hamburg **3** (1924), 89–108.

[2] W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, Multiplicative structure of values of Euler's function, in *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, A. J. van der Poorten, ed., Fields Inst. Comm. **41** (2004), 29–47.

[3] W. D. Banks and F. Luca, Power totients with almost primes, Integers **11** (2011), 307–313.

[4] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, Math. Comp. **16** (1962), 363–367.

[5] F. Behrend, Über numeri abundantes I, II, S.-Ber. Preuß Akad. Wiss., math.-nat. Kl. (1932), 322–328; (1933), 119–127.

[6] F. Behrend, Three reviews; of papers by Chowla, Davenport, and Erdős, Jahrbuch Fortschr. Math. **60** (1935), 146–149.

[7] E. Bessel-Hagen, Zahlentheorie, in *Repertorium der höheren Mathematik*, 2nd ed., Vol. 1, B. G. Teubner, Leipzig, 1929, 1458–1574.

[8] P. Billingsley, *Probability and Measure*, 3rd ed., Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, New York, NY, 1995.

[9] V. Brun, Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare, Archiv for Math. og Naturvid. **B34:8** (1915).

[10] N. G. Chebotarev, Opredelenie plotnosti sovokupnosti prostykh chisel, prinadlezhashchikh zadannomu klassu podstanovok, Izv. Ross. Akad. Nauk **17** (1923), 205–250.

[11] K.-K. Chen and Y.-G. Chen, On $f(p) + f(q) = f(p + q)$ for all odd primes p and q, Publ. Math. Debrecen, **76:4** (2010), 425–430.

[12] S. Chowla, On abundant numbers, J. Indian Math. Soc. **1** (1934), 41–44.

[13] P. V. Chung and B. M. Phong, Additive uniqueness sets for multiplicative functions, Publ. Math. Debrecen **55:3-4** (1999), 237–243.

[14] H. Davenport, Über numeri abundantes, Sitzungsber. Preuss. Akad. Wiss., Phys.-Math. Kl. **6** (1933), 830–837.

[15] J.-M. De Koninck, I. Kátai, and B. M. Phong, A new characteristic of the identity function, J. Number Theory, **63** (1997), 325–338.

[16] P. D. T. A. Elliott, *Probabilistic Number Theory I: Mean-Value Theorems*, Grundlehren der mathematischen Wissenschaften, vol. 239, Springer-Verlag, New York, NY, 1979.

[17] P. Erdős, On the density of the abundant numbers, J. London Math. Soc. **9** (1934), 278–282.

[18] P. Erdős, On the density of some sequences of numbers, J. London Math. Soc. **10** (1935), 120–125.

[19] P. Erdős, On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function, Quart. J. Math., Oxford Ser. **6** (1935), 205–213.

[20] P. Erdős, On the density of some sequences of numbers, II, J. London Math. Soc. **12** (1937), 7–11.

[21] P. Erdős, On the density of some sequences of numbers, III, J. London Math. Soc. **13** (1938), 119–127.

[22] P. Erdős, On the distribution function of additive functions, Ann. Math. (2) **47** (1946), 1–20.

[23] P. Erdős and R. R. Hall, On the values of Euler's φ-function, Acta Arith. **22** (1973), 201–206.

[24] P. Erdős and R. R. Hall, Distinct values of Euler's φ-function, Mathematika **23** (1976), 1–3.

[25] P. Erdős and M. Kac, The Gaussian law of errors in the theory of number theoretic functions, Amer. J. Math. **62** (1940), 738–742.

[26] P. Erdős and A. Wintner, Additive arithmetical functions and statistical independence, Amer. J. Math. **61** (1939), 713–721.

[27] T. Estermann, On Goldbach's problem: Proof that almost all even positive integers are sums of two primes, Proc. London Math. Soc. **(2) 44** (1938), 307–314.

[28] M. B. Fein and H. N. Shapiro, Continuity of the distribution function of the sum of an additive and multiplicative arithmetic function, Comm. Pure Appl. Math. **40** (1987), 779–801.

[29] K. Ford, The distribution of totients, Ramanujan J. **2** (1998), 67–151, updated version available as arXiv:1104.3264 [math.NT].

[30] T. Freiberg, Products of shifted primes simultaneously taking perfect power values, J. Aust. Math. Soc. (special issue dedicated to Alf van der Poorten) **92** (2012), 145–154.

[31] J. Galambos and I. Kátai, The continuity of the limiting distribution of a function of two additive functions, Math. Z. **204** (1990), 247–252.

[32] G. Halász, On the distribution of additive arithmetic functions, Acta Arith. **27** (1975), 143–152.

[33] H. Halberstam and H.-E. Richert, *Sieve Methods*, London Mathematical Society Monographs 4, Academic Press, London, 1974.

[34] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 1988.

[35] G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, Quart. J. Math. **48** (1917), 76–92.

[36] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, Oxford, 2008.

[37] D. E. Iannucci and F. Luca, Triangular numbers whose sum of divisors is also triangular, Acta Arith. **129** (2007), 23–40.

[38] D. Klyve, Explicit bounds on twin primes and Brun's constant, *PhD thesis*, Dartmouth College, 2007.

[39] M. Kobayashi, On the density of abundant numbers, *PhD thesis*, Dartmouth College, 2010.

[40] M. Kobayashi and P. Pollack, The error term in the count of abundant numbers, Mathematika **60** (2014), 43–65.

[41] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen, II*, 2nd ed., Chelsea Publ. Co., New York, NY, 1953.

[42] N. Lebowitz-Lockard and P. Pollack, Clustering of linear combinations of multiplicative functions, J. Number Theory **180** (2017), 660–672.

[43] F. Luca and C. Pomerance, Local behavior of the composition of the aliquot and cototient functions, in *Analytic Number Theory, Modular Forms, and q-Hypergeometric Series: In Honor of Krishna Alladi's 60th Birthday*, G. E. Andrews and F. Garvan, eds., Springer Proc. Math. Stat. 221, Springer, Cham, 2017, 477–495.

[44] H. Maier and C. Pomerance, On the number of distinct values of Euler's φ-function, Acta Arith. **49** (1988), 263–275.

[45] T. Nagell, *Introduction to Number Theory*, 2nd ed., Chelsea, New York, NY, 1964.

[46] M. Nair, Multiplicative functions of polynomial values in short intervals, Acta Arith. **62:3** (1992), 257–269.

[47] Nicomachus, *Introduction to Arithmetic*, tr. M. L. D'Ooge; with studies in Greek arithmetic, F. E. Robbins and L. C. Karpinski, Macmillan, New York, NY, 1926.

[48] S. S. Pillai, On some functions connected with $\varphi(n)$, Bull. Amer. Math. Soc. **35** (1929), 832–836.

[49] P. Pollack, How often is Euler's totient a perfect power?, J. Number Theory **197** (2019), 1–12.

[50] P. Pollack, Nonnegative multiplicative functions on sifted sets, and the square roots of -1 modulo shifted primes, accepted by Glasgow Math. J.

[51] P. Pollack and C. Pomerance, Square values of Euler's function, Bull. London Math. Soc. **46** (2014), 403–414.

[52] C. Pomerance, Popular values of Euler's function, Mathematika **27** (1980), 84–89.

[53] C. Pomerance, On the distribution of values of Euler's function, Acta Arith. **47** (1986), 63–70.

[54] I. J. Schoenberg, Über die asymptotische Verteilung reeller Zahlen mod 1, Math. Z. **28** (1928), 171–200.

[55] I. J. Schoenberg, On asymptotic distributions of arithmetical functions, Trans. Amer. Math. Soc. **2** (1936), 315–330.

[56] H. N. Shapiro, Addition of functions in probabilistic number theory, Comm. Pure Appl. Math. **26** (1973), 55–84.

[57] P. Shiu, A Brun-Titchmarsh theorem for multiplicative functions, J. Reine Angew. Math. **313** (1980), 161–170.

[58] C. A. Spiro, Additive uniqueness sets for arithmetic functions, J. Number Theory **42** (1992), 232–246.

[59] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.

[60] E. C. Titchmarsh, A divisor problem, Rend. Circ. Math. Palermo **54** (1930), 414–429.

[61] P. Turán, Über einige Verallgemeinerungen eines satzes von Hardy und Ramanujan, J. London Math. Soc. **9** (1934), 274–276.