ALGEBRAIC AND ANALYTIC PROPERTIES OF ARITHMETIC FUNCTIONS

MARK SCHACHNER

Abstract. When considered as an algebraic space, the set of arithmetic functions equipped with the operations of pointwise addition and Dirichlet convolution exhibits many nontrivial properties. In this paper, we delineate and prove several of these properties, and consider ways to quantify the behavior of certain functions.

Contents

1. Introduction

Consider a function $\varrho : \mathbb{N} \to \mathbb{N}$ given by the recursive definition

$$\varrho(n) = \begin{cases} 1, & \text{if } n = 1; \\ \displaystyle\sum_{d|n, d<n} \varrho(d), & \text{if } n > 1. \end{cases}$$

This function, defined on the natural numbers, is an example of an arithmetic function. It exhibits erratic behavior in many ways: for example, for values of n with few prime factors it remains small, but it quickly grows arbitrarily large if n has many prime factors. However, using the techniques of analytic number theory, the behavior of this and related functions can be quantitatively studied. In this paper, we examine the properties of various important arithmetic functions and consider the space of such functions, equipped with the operations of addition, multiplication, and Dirichlet convolution. We also deduce several facts about the existence and properties of roots of polynomials with arithmetic functions as coefficients.

2. The Space of Arithmetic Functions

In this section we introduce the concept of an arithmetic function, and define a space of arithmetic functions with several operations. We then isolate a few specific functions which will be of use later.

Definition 2.1. An *arithmetic function* is a complex-valued function which is defined on the natural numbers, i.e., a function of the form $f : \mathbb{N} \to \mathbb{C}$.

These functions are also known as number-theoretic functions, which is indicative of their interpretation as encodings of specific properties of the natural numbers.

Definition 2.2. In this paper, we denote the set of arithmetic functions as $\mathbb{A}$. We also equip $\mathbb{A}$ with the operation $+ : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ given by, for $f, g \in \mathbb{A}$, $(f + g)(n) = f(n) + g(n)$ for all $n \in \mathbb{N}$.

Throughout this paper, we will denote arbitrary arithmetic functions by f, g, h, as well as A_k for $k \in \mathbb{N}$. Later, we will define polynomial functions from $\mathbb{A}$ to itself, which will commonly be denoted $\mathbf{F}, \mathbf{G}, \mathbf{H}$. We also define one other binary operation on $\mathbb{A}$, which is important enough to merit its own definition.

Definition 2.3. Let $f, g \in \mathbb{A}$. The *Dirichlet convolution* (or simply *convolution*) of f, g, denoted $f * g$, is the function given by, for each $n \in \mathbb{N}$,

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right),$$

or, equivalently,

$$(f * g)(n) = \sum_{ab=n} f(a) g(b).$$

These two definitions are equivalent via the substitution $a = d$, $b = \frac{n}{a} = \frac{n}{d}$.

The following elements of $\mathbb{A}$ are important in the study of arithmetic functions:

Definition 2.4.

(i) The *identity function* $\varepsilon \in \mathbb{A}$ is given by, for each $n \in \mathbb{N}$,

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

(ii) The *constant functions* $\mathbf{0}, \mathbb{1} \in \mathbb{A}$ are given by $\mathbb{1}(n) = 1$ and $\mathbf{0}(n) = 0$ for each $n \in \mathbb{N}$.

(iii) The *divisor function* $\sigma_i \in \mathbb{A}$, defined for each $i \in \mathbb{C}$, is given by

$$\sigma_i(n) = \sum_{d|n} d^i.$$

for each $n \in \mathbb{N}$. In this paper we denote σ_0 by τ and σ_1 by σ.

Note that, while convolution will play a role similar to multiplication in this paper, the function $\mathbb{1}$ is not the identity with respect to convolution.

3. $\mathbb{A}$ is an Integral Domain

First, we develop arithmetic on $\mathbb{A}$ and prove several statements regarding its algebraic structure.

Lemma 3.1. *The operation $*$ is commutative, associative, and distributive over addition.*

Proof. First, we show that convolution is commutative. To observe this, we use the second definition from Definition 2.3:

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{ab=n} g(a)f(b) = (g * f)(n).$$

To show that convolution is associative, we again use the second definition:

$$\begin{aligned}(f * (g * h))(n) &= \sum_{ab=n} f(a) \cdot (g * h)(b) \\ &= \sum_{ab=n} \left(f(a) \sum_{cd=b} g(c)h(d) \right) \\ &= \sum_{acd=n} f(a)g(c)h(d) \\ &= \sum_{ed=n} \sum_{ac=e} f(a)g(c)h(d) \\ &= ((f * g) * h)(n).\end{aligned}$$

Lastly, we show that convolution distributes over addition:

$$\begin{aligned}(f * (g + h))(n) &= \sum_{ab=n} f(a) \cdot (g + h)(b) \\ &= \sum_{ab=n} f(a)g(b) + f(a)h(b) \\ &= \sum_{ab=n} f(a)g(b) + \sum_{ab=n} f(a)h(b) \\ &= (f * g)(n) + (f * h)(n).\end{aligned}$$

□

We next prove an important result about the role of ε with respect to Dirichlet convolution:

Lemma 3.2. *The function $\varepsilon \in \mathbb{A}$ is the identity element with respect to Dirichlet convolution, i.e., $\varepsilon * f = f * \varepsilon = f$ for all $f \in \mathbb{A}$.*

Proof. Fix some $f \in \mathbb{A}$, and observe that, for all $n \in \mathbb{N}$,

$$\begin{aligned}(f * \varepsilon)(n) &= \sum_{d|n} f(d) \cdot \varepsilon\left(\frac{n}{d}\right) \\ &= f(n)\varepsilon(1) + \sum_{d|n, d<n} f(d) \cdot \varepsilon\left(\frac{n}{d}\right) \\ &= f(n),\end{aligned}$$

since $\varepsilon\left(\frac{n}{d}\right) = 0$ when $d < n$. That $\varepsilon * f = f * \varepsilon = f$ follows from Lemma 3.1. □

We can now make the following important statement about $\mathbb{A}$:

Theorem 3.3. *The set $\mathbb{A}$, along with the operations $+$ and $*$, forms a commutative ring.*

Proof. Pointwise addition is trivially commutative and associative, and has the identity element $\mathbf{0} \in \mathbb{A}$, where $\mathbf{0}(n) = 0$ for all $n \in \mathbb{N}$. Furthermore, for any $f \in \mathbb{A}$ we define $-f$ as the function such that $(-f)(n) = -(f(n))$ for each $n \in \mathbb{N}$; this represents the additive inverse of the element f. From Lemma 3.1 and Lemma 3.2, we have that convolution is commutative, associative, and has an identity element $\varepsilon \in \mathbb{A}$. Lastly, from Lemma 3.1, we have that convolution distributes over addition. □

There, is, however, additional algebraic structure on $\mathbb{A}$ with respect to convolution as demonstrated by the following lemma:

Lemma 3.4. *Suppose $f \in \mathbb{A}$. Then there exists $f^{-1} \in \mathbb{A}$ such that $f * f^{-1} = \varepsilon$ if and only if $f(1) \neq 0$.*

Proof. To show the forward direction, let $f \in \mathbb{A}$ and suppose that there exists $f^{-1} \in \mathbb{A}$ such that $f * f^{-1} = \varepsilon$. Observe that $f(1)f^{-1}(1) = (f * f^{-1})(1) = \varepsilon(1) = 1$, so $f^{-1}(1) = \frac{1}{f(1)}$. Hence $f(1) \neq 0$.

To show the backward direction, fix $f \in \mathbb{A}$ such that $f(1) \neq 0$. We will show that $g(n)$ can be uniquely defined such that $(f * g)(n) = \varepsilon(n)$, proceeding by induction on n :

Base Case. Let $n = 1$ and $g(1) = \frac{1}{f(1)}$. Since $f(1) \neq 0$, we have $g(1)$ is well-defined, and this definition satisfies

$$(f * g)(1) = f(1)g(1) = 1 = \varepsilon(1).$$

Furthermore, any value of $g(1)$ which satisfies the above must equal $\frac{1}{f(1)}$, so this $g(1)$ is defined uniquely.

Inductive Step. Fix $n \in \mathbb{N}$ and suppose that for each $k < n$ we have that $g(k)$ is well-defined and unique. We now define $g(n)$ as follows:

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d>1} f(d)g\left(\frac{n}{d}\right).$$

Observe that $g(n)$ is well-defined for each $n \in \mathbb{N}$, since $f(1) \neq 0$ and $\frac{n}{d} \in \mathbb{N}$, $\frac{n}{d} < n$, so $g\left(\frac{n}{d}\right)$ is uniquely defined by the inductive hypothesis for each $d \mid n, d > 1$. Now, we show $f * g = \varepsilon$. We have two cases: $n = 1$ and $n > 1$. If $n = 1$, then as before $(f * g)(n) = f(1)g(1) = \varepsilon(n)$. If $n > 1$, then

$$\begin{aligned}
(f * g)(n) &= \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \\
&= f(1)g(n) + \sum_{d|n, d>1} f(d)g\left(\frac{n}{d}\right) \\
&= f(1)g(n) - f(1)g(n) \\
&= 0 \\
&= \varepsilon(n).
\end{aligned}$$

Thus g is the unique arithmetic function such that $f * g = \varepsilon$, so for each $f \in \mathbb{A}$ where $f(1) \neq 0$, we can let $f^{-1} = g$ so that $f * f^{-1} = \varepsilon$. Again, that $f^{-1} * f = \varepsilon$ follows from the commutativity of Dirichlet convolution. □

Motivated by Lemma 3.4, we make the following definition:

Definition 3.5. A function $f \in \mathbb{A}$ is called *invertible* if $f(1) \neq 0$.

Using this property we can deduce additional algebraic structure on $\mathbb{A}$:

Theorem 3.6. *The set $\mathbb{A}$ has no zero divisors, i.e., if $f, g \in \mathbb{A}$ and $f * g = \boldsymbol{0}$, then at least one of $f = \boldsymbol{0}, g = \boldsymbol{0}$ holds.*

Proof. We prove the contrapositive, that is, if $f, g \neq \mathbf{0}$ then $f * g \neq \mathbf{0}$. Suppose $f, g \neq \mathbf{0}$; we have that the sets $M = \{n \in \mathbb{N} \mid f(n) \neq 0\}$ and $N = \{n \in \mathbb{N} \mid g(n) \neq 0\}$ are nonempty. Let m, n be the least elements of M, N respectively, and consider the evaluation of $f * g$ at mn :

$$(f * g)(mn) = \sum_{ab=mn} f(a)g(b).$$

Now, each term on the right is of the form $f(a)g(b)$ where $ab = mn$. For each of these terms, we have either $a = m$ and $b = n$, in which case $f(a)g(b) = f(m)g(n) \neq 0$, or one of $a < m, b < n$, in which case $f(a)g(b) = 0$ since we assumed m, n were the least elements of M, N. Thus there is exactly one nonzero term on the right side, so the right side is nonzero; hence the left side must also be nonzero, so $f * g \neq \mathbf{0}$. □

The combination of Theorems 3.3 and 3.6 gives the following result:

Theorem 3.7. *The set $\mathbb{A}$, along with the operations of pointwise addition and Dirichlet convolution, forms an integral domain.*

Note that, since the condition that $f(1) \neq 0$ is weaker than the condition that $f \neq \mathbf{0}$, Theorem 3.7 and Lemma 3.4 do not imply that $\mathbb{A}$ is a field. Indeed, the existence of elements in $\mathbb{A}$ without inverses under convolution will have consequences when we consider roots of polynomials in $\mathbb{A}$.

4. Möbius Inversion and Related Results

In this section, we define an arithmetic function introduced by Möbius in 1832, and prove several results regarding its relationship with other arithmetic functions.

Definition 4.1. The *Möbius function* $\mu \in \mathbb{A}$ is given by, for each $n \in \mathbb{N}$,

$$\mu(n) = \begin{cases} -1 & \text{if } n \text{ is a product of an odd number of distinct primes;} \\ 1 & \text{if } n \text{ is a product of an even number of distinct primes;} \\ 0 & \text{otherwise.} \end{cases}$$

Equivalently, if n is divisible by the square of a prime number, then $\mu(n) = 0$; otherwise, $\mu(n) = (-1)^{\omega(n)}$, where $\omega(n)$ denotes the number of prime factors of n.

To discuss the following results more concisely, we need the following lemma, which solidifies the connection between divisor sums and convolution:

Lemma 4.2. *For any $f \in \mathbb{A}$, $(f * \mathbb{1})(n) = \sum_{d|n} f(d)$.*

Proof. By definition, $(f * \mathbb{1})(n) = \sum_{d|n} f(d)\mathbb{1}\left(\frac{n}{d}\right)$. Since $\mathbb{1}(n) = 1$ for all $n \in \mathbb{N}$, the lemma follows. □

Some results which follow from Lemma 4.2 are:

(i) $\mathbb{1} * \mathbb{1} = \tau$ (see Definition 2.4)
(ii) $\underbrace{\mathbb{1} * \mathbb{1} * \cdots * \mathbb{1}}_{\text{n times}} = \tau_n$ (see Definition 6.3)
(iii) $\mathbb{1} * N = \sigma$, where $N(n) = n$ for all $n \in \mathbb{N}$

Since μ is invertible, it is natural to ask what its inverse is under Dirichlet convolution. The below theorem gives the surprising answer:

Theorem 4.3. $\mu * \mathbb{1} = \varepsilon$.

The following lemma will prove useful to prove Theorem 4.3:

Lemma 4.4. *Let S be a finite nonempty set. Then the sets $\{S' \subset S : |S'|$ is even$\}$ and $\{S' \subset S : |S'|$ odd$\}$ have the same cardinality.*

Proof. We have two cases: $|S|$ is odd and $|S|$ is even. If $|S|$ is odd, then we construct a bijection as follows: Fix some subset of $S' \subset S$. Trivially, $|S'| + |S \setminus S'| = |S|$, and, since $|S|$ is odd, this implies that $|S'|$ and $|S \setminus S'|$ have opposite parity. Thus each subset of S corresponds to exactly one other subset of S such that every even-sized subset corresponds to an odd-sized subset, and vice versa. Hence we have a bijection between the set of even-sized subsets of S and odd-sized subsets of S.

If $|S|$ is even, then we first fix some element $p \in S$. We construct a function f from the power set of S to itself as follows: for any subset S' of S, $p \in f(S')$ if and only if $p \in S'$, and for each element $k \in S \setminus \{p\}$, we have $k \in f(S')$ if and only if $k \notin S'$. Now, f is a bijection and has the property that if S' has n elements, then $f(S')$ has either $(|S|+1)-n$ or $(|S|-1)-n$ elements, depending on whether $p \in S'$. However, since $|S|$ is even, both $|S|+1$ and $|S|-1$ are odd, so $|S'|+|f(S')|$ is odd for each $S' \subset S$. Similarly to the above, this implies that $|S'|$ and $|f(S')|$ have opposite parity; hence we again have a bijection between the even- and odd-sized subsets of S. Thus the lemma is proved. □

Now, we move on to the proof of Theorem 4.3.

Proof of Theorem 4.3. If $n = 1$, then $(\mu * \mathbb{1})(n) = \mu(1) = 1 = \varepsilon(n)$ as required, so suppose $n > 1$. By Lemma 4.2, $\mathbb{1} * \mu = \sum_{d|n} \mu(d)$, so we need to show that the sum of $\mu(d)$ across all of the divisors d of n is equal to $\varepsilon(n)$. Since $\mu(n) = 0$ unless n is squarefree, we need only consider the sum across all squarefree divisors of n. Consider the set $P_n = \{p_1, p_2, \ldots, p_m\}$ of distinct prime factors of n; choosing a squarefree divisor of n is equivalent to choosing some subset of P_n. Observe that, for any subset A of P_n, the value of μ at the squarefree divisor which A represents is 1 if $|A|$ is even and -1 if $|A|$ is odd. Since $n > 1$ we have P_n is nonempty, so by Lemma 4.4 P_n has an equal number of even- and odd-sized subsets. Thus each positive 1 in the sum is canceled by a -1 and the sum of μ across all subsets of P_n is zero. The theorem follows. □

Since Theorem 4.3 states that the Möbius function is the inverse of the constant function $\mathbb{1}$ under Dirichlet convolution, it is often called Möbius inversion, although the name is also given to the following corollary:

Corollary 4.5 (Möbius Inversion)**.** *Let $f, g \in \mathbb{A}$ such that for any $n \in \mathbb{N}$ we have*

$$f(n) = \sum_{d|n} g(d). \tag{4.6}$$

Then

$$g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right). \tag{4.7}$$

Proof. By Lemma 4.2, (4.6) is equivalent to $f = g * \mathbb{1}$. Convolving on both sides by μ, we obtain $f * \mu = g * \mathbb{1} * \mu = g$ by Theorem 4.3. By definition this is equivalent to eq. (4.7). □

As an application of Dirichlet convolution and Möbius inversion, we return to our function ϱ from Section 1. We have, for all n,

$$\varrho(n) = \varepsilon(n) + \sum_{d|n, d<n} \varrho(d).$$

So

$$\begin{aligned} 2\varrho(n) &= \varepsilon(n) + \sum_{d|n} \varrho(d) \\ &= \varepsilon(n) + (\varrho * \mathbb{1})(n). \end{aligned}$$

Thus we have

$$\begin{aligned} & 2\varrho = \varepsilon + \varrho * \mathbb{1} \\ \Rightarrow \quad & (2\varrho) * \mu = \varepsilon * \mu + \varrho * \mathbb{1} * \mu \\ \Rightarrow \quad & 2(\varrho * \mu) = \mu + \varrho \\ \Rightarrow \quad & -\varrho(n) = \mu(n) + (-2)\varrho(n) + \sum_{d|n, d>1} (-2)\mu(d)\varrho\left(\frac{n}{d}\right) \\ \Rightarrow \quad & \varrho(n) = \mu(n) + \sum_{d|n, d>1} (-2)\mu(d)\varrho\left(\frac{n}{d}\right). \end{aligned} \tag{4.8}$$

By evaluating eq. (4.8) at $\frac{n}{d}$ and substituting for $\varrho\left(\frac{n}{d}\right)$, we obtain

$$\begin{aligned} \varrho(n) = \mu(n) &+ \sum_{d_1|n, d_1>1} (-2)\mu(d_1)\mu\left(\frac{n}{d_1}\right) \\ &+ \sum_{d_1|n, d_1>1} \sum_{d_2|\frac{n}{d_1}, d_2>1} (-2)^2\mu(d_1)\mu(d_2)\varrho\left(\frac{n}{d_1 d_2}\right). \end{aligned}$$

Repeating this process of substitution, we arrive at

$$\varrho(n) = \mu(n) + \sum_{\substack{d_1 d_2 \ldots d_m = n \\ d_1, d_2, \ldots, d_{m-1} > 1}} (-2)^m \prod_{i \le m} \mu(d_i) \cdot \mu\left(\frac{n}{d_1 d_2 \ldots d_m}\right),$$

which is a non-recursive definition for ϱ. In general, for each $k \in \mathbb{C}$ we can define a function $\varrho_k \in \mathbb{A}$ which satisfies the functional equation

$$k\varrho_k = (k-1)\varepsilon + \varrho_k * \mathbb{1},$$

where the factor $(k-1)$ is included so $\varrho_k(1) = 1$ for all $k \in \mathbb{C}$. By a similar argument to the above, the solution to this functional equation is given by

$$\varrho_k(n) = \mu(n) + \sum_{\substack{d_1 d_2 \dots d_m = n \\ d_1, d_2, \dots, d_{m-1} > 1}} \left(\frac{k}{1-k}\right)^m \prod_{i \leq m} \mu(d_i) \cdot \mu\left(\frac{n}{d_1 d_2 \dots d_m}\right),$$

a fact which has as a corollary $\varrho_0 = \mu$. Thus Möbius inversion can be useful in determining solutions to functional equations involving Dirichlet convolution.

5. Polynomials in $\mathbb{A}$

In this section, we develop the theory of polynomials in $\mathbb{A}$, and deduce several results about the existence and properties of their roots. We begin with several definitions.

Definition 5.1. Let $f \in \mathbb{A}$. We denote the repeated convolution $\underbrace{f * f * \cdots * f}_{\text{n times}}$ by f^{*n}, and set $f^{*0} = \varepsilon$.

Definition 5.2.

(i) A *polynomial in* $\mathbb{A}$ is an expression of the form

$$\sum_{i=0}^{n} A_i * X^{*i} = A_0 + A_1 * X + A_2 * X^{*2} + \cdots + A_n * X^{*n},$$

where $A_0, A_1, \dots, A_n \in \mathbb{A}$ such that $A_n \neq \mathbf{0}$ and X is an indeterminate.

(ii) The natural number n is called the *degree* of the polynomial.

(iii) The elements $A_0, A_1, \dots, A_n$ are called the *coefficients* or *coefficient functions* of the polynomial, with A_n specifically called the *leading coefficient*.

(iv) If $\mathbf{F}$ is a polynomial in $\mathbb{A}$ and $\mathbf{F}(g) = \mathbf{0}$ for some $g \in \mathbb{A}$, we call g a *root* of $\mathbf{F}$.

We denote the set of polynomials in $\mathbb{A}$ by $\mathbb{A}[X]$.

Since $\mathbb{A}$ is a ring, $\mathbb{A}[X]$ inherits the operations of addition, pointwise multiplication and Dirichlet convolution defined over $\mathbb{A}$, so for any polynomials $\mathbf{F}, \mathbf{G} \in \mathbb{A}[X]$ we let $(\mathbf{F} + \mathbf{G})(X) = \mathbf{F}(X) + \mathbf{G}(X)$ and $(\mathbf{F} * \mathbf{G})(X) = \mathbf{F}(X) * \mathbf{G}(X)$.

Theorem 5.3. *Let $A_0, A_1 \in \mathbb{A}$ such that A_1 is invertible. Then the polynomial $\boldsymbol{F}(X) = A_0 + A_1 * X$ has a single unique root.*

Proof. Since A_1 is invertible, there exists a unique arithmetic function A_1^{-1} such that $A_1 * A_1^{-1} = \varepsilon$. Let $g = -A_0 * A_1^{-1}$. Now $\mathbf{F}(g) = \mathbf{0}$. Also, this root is unique because any root g of $\mathbf{F}$ must satisfy $-A_0 * A_1^{-1} = g$, and the inverse of A_1 is unique by Lemma 3.4. □

There is also an analog to the quadratic formula for polynomials in $\mathbb{A}$ with all coefficients invertible. To prove this, we first need the following lemma:

Lemma 5.4. *Let $f \in \mathbb{A}$ be invertible. Then there exist exactly two functions $g_1, g_2 \in \mathbb{A}$ such that $g_1 * g_1 = g_2 * g_2 = f$.*

Proof. For each natural number n, let $L(n)$ denote the sum of the exponents in the prime factorization of n. (For instance, since $288 = 2^5 \cdot 3^2$, we have $L(288) = 5+2 = 7$.) We will show that we can always uniquely define $g_1(n), g_2(n)$ by induction on $L(n)$.

Base Case. Let $L(n) = 0$, so $n = 1$. If we define $g_1(1)$ as the principal square root of $f(1)$ and $g_2(1)$ as the negative square root of $f(1)$, then we have that $(g_1 * g_1)(1) = f(1) = (g_2 * g_2)(1)$. Moreover, any function h which satisfies $(h * h)(1) = f(1)$ must satisfy $h(1)^2 = f(1)$, so g_1, g_2 are both well-defined and the only functions which satisfy the required property if $L(n) = 0$.

Inductive Step. Suppose that for some $n \in \mathbb{N}$ we have that if $L(s) \leq n$ then $g_1(s), g_2(s)$ are uniquely well-defined. Fix some $m \in \mathbb{N}$ such that $L(m) = n+1$ and let

$$g_1(m) = \frac{1}{2g_1(1)} \left(f(m) - \sum_{\substack{d \mid m \\ 1<d<m}} g_1(d) g_1\left(\frac{m}{d}\right) \right), \tag{5.5}$$

$$g_2(m) = \frac{1}{2g_2(1)} \left(f(m) - \sum_{\substack{d \mid m \\ 1<d<m}} g_2(d) g_2\left(\frac{m}{d}\right) \right) \tag{5.6}$$

We first show that the above definitions are well-defined. We have defined $g_1(1), g_2(1)$ to be the principal and negative square roots of $f(1)$; since $f(1) \neq 0$ by hypothesis, we thus have that $2g_1(1), 2g_2(1) \neq 0$. Next, observe that for all $d \mid m$ such that $1 < d < m$ we have $L(d), L(\frac{m}{d}) < L(m) = n + 1$, so by our inductive hypothesis the above expressions are well-defined. Furthermore, since a rearrangement of the above yields

$$f(m) = \sum_{d \mid m} g_i(d) g_i\left(\frac{m}{d}\right) = (g_i * g_i)(m),$$

for $i = 1, 2$, any function $h \in \mathbb{A}$ which satisfies $h * h = f$ must satisfy one of (5.5),(5.6). Thus g_1 and g_2 are uniquely well-defined for any $k \in \mathbb{N}$ such that $d(k) = n + 1$. Hence the inductive proof is complete. □

As the above lemma shows, for an invertible function $f \in \mathbb{A}$, the "principal Dirichlet square root" (written g_1 above) is well-defined; going forward we denote this by $f^{*1/2}$. This square root has many of the same properties as the usual square root; in particular, $f^{*1/2} * g^{*1/2}$ is a square root of $f * g$ for all invertible $f, g \in \mathbb{A}$.

It is also important to note that, while Lemma 5.4 states that all invertible functions have square roots under convolution, there exist non-invertible functions both with and without square roots. As an example of a non-invertible function with a square root, consider the class of functions δ_k given by, for each $n, k \in \mathbb{N}$,

$$\delta_k(n) = \begin{cases} 1 & \text{if } n = k, \\ 0 & \text{otherwise.} \end{cases}$$

Then the function δ_{k^2}, which is only invertible if $k = 1$, has δ_k as a square root under convolution. As an example of a non-invertible function without a square root, consider the function $\mathbb{1} - \varepsilon$, which evaluates to 0 if $n = 1$ and 1 otherwise. Suppose for contradiction that this function has a square root $s \in \mathbb{A}$. Since $s(1)s(1) = (s * s)(1) = (\mathbb{1} - \varepsilon)(1) = 0$, we must have $s(1) = 0$. But this implies

$$1 = (\mathbb{1} - \varepsilon)(2) = (s * s)(2) = s(1)s(2) + s(2)s(1) = 0,$$

a contradiction. Hence s cannot exist.

Theorem 5.7 (Quadratic Formula)**.** *Let $A, B, C \in \mathbb{A}$ such that A and $B^{*2} - 4A * C$ are invertible. Then there exist exactly two roots $f_1, f_2 \in \mathbb{A}$ of the polynomial*

$$A * X^{*2} + B * X + C, \tag{5.8}$$

and these functions are given by

$$f_1 = (-B + (B^{*2} - 4A * C)^{*1/2}) * (2A)^{-1},$$
$$f_2 = (-B - (B^{*2} - 4A * C)^{*1/2}) * (2A)^{-1}.$$

Proof. The majority of the proof is completely analogous to the usual derivation of the quadratic formula, rearranging (5.8) to obtain

$$(f - B * (2A)^{-1})^{*2} = (B^{*2} - 4A * C) * (4A^{*2})^{-1}. \tag{5.9}$$

Since the right side is invertible, so is the left side, so by Lemma 5.4 we can take the Dirichlet square root of both sides, and arrive at the formula specified by the theorem. □

We now turn to proving the general case, a partial analog of the Fundamental Theorem of Algebra for $\mathbb{A}$.

Definition 5.10. Let $\mathbf{F} \in \mathbb{A}[X]$ be given by

$$\mathbf{F}(X) = \sum_{i=0}^{n} A_i * X^{*i} = A_0 + A_1 * x + \cdots + A_n * X^{*n}.$$

The *formal derivative* of $\mathbf{F}$ is denoted $\mathbf{F}'$ and given by

$$\mathbf{F}'(X) = \sum_{i=1}^{n} iA_i * X^{*n-1} = A_1 + 2A_2 * X + \cdots + nA_n * X^{*n-1}.$$

Definition 5.11. Let $\mathbf{F} \in \mathbb{A}[X]$. The *base polynomial* of $\mathbf{F}$, denoted $P_{\mathbf{F}}$, is the polynomial over $\mathbb{C}$ whose coefficients are the coefficient functions of $\mathbf{F}$ evaluated at 1, i.e., if $\mathbf{F}(X) = A_0 + A_1 * X + \cdots + A_n * X^{*n}$, then $P_{\mathbf{F}}(x) = A_0(1) + A_1(1)x + \cdots + A_n(1)x^n$.

The formal derivative and base polynomial of a polynomial over $\mathbb{A}$ interact in the following important way:

Lemma 5.12. *Let $\boldsymbol{F} \in \mathbb{A}[X]$. Then $P_{\boldsymbol{F}'} = (P_{\boldsymbol{F}})'$, where the prime on the right-hand side denotes the derivative in the usual sense.*

Proof. Suppose $\mathbf{F}(X) = A_0 + A_1 * X + \cdots + A_n * X^{*n}$. The coefficients of $\mathbf{F}'$ are then $A_1, 2A_2, 3A_3, \ldots, nA_n$, so we have

$$P_{\mathbf{F}'}(x) = A_1(1) + 2A_2(1)x + \cdots + nA_n(x)^{n-1}. \tag{5.13}$$

Also, since $P_{\mathbf{F}}(x) = A_0(1) + A_1(1)x + \cdots + A_n(1)x^n$, taking the derivative as usual yields

$$P'_{\mathbf{F}}(x) = A_1(1) + 2A_2(1)x + \cdots + nA_n(1)x^{n-1},$$

which is identical to eq. (5.13). □

Given this fact, we make the following statement, the main theorem of this section:

Theorem 5.14. *Let $\boldsymbol{F} \in \mathbb{A}[X]$ be a polynomial over $\mathbb{A}$ of degree at least 1 such that $P_{\boldsymbol{F}}$ has a root in $\mathbb{C}$ of multiplicity 1. Then $\boldsymbol{F}$ has a root $g \in \mathbb{A}$.*

Proof. The proof runs similarly to those of Lemmas 3.4 and 5.4, in that we will show that for any $n \in \mathbb{N}$ we can well-define $g(n)$ such that $\mathbf{F}(g)(n) = 0$, inducting on $L(n)$.

Base Case. Let $L(n) = 0$, so $n = 1$. By hypothesis $P_{\mathbf{F}}$ has a simple root $r \in \mathbb{C}$; let $g(1) = r$. Now, we have

$$\begin{aligned}\mathbf{F}(g)(1) &= A_0(1) + A_1(1)g(1) + \cdots + A_n(1)g(1)^n \\ &= P_{\mathbf{F}}(g(1)) \\ &= 0.\end{aligned}$$

Inductive Step. Suppose that for some $n \in \mathbb{N}$ we have that if $L(s) \leq n$ then $g(s)$ is well-defined. Fix some $m \in \mathbb{N}$ such that $L(m) = n + 1$ and let

$$\begin{aligned}g(m) = -\frac{1}{\mathbf{F}'(g)(1)}\Bigg(&\left(\sum_{j=0}^{n} A_j(m)g(1)^j\right) \\ &+\Bigg(\sum_{\substack{d_1 d_2 \ldots d_{n+1} = m \\ d_1, d_2, \ldots, d_{n+1} \neq m}} \frac{A_0(d_1)g(d_2 d_3 \ldots d_{n+1})}{\tau_n(m/d_1)} \\ &\qquad + \frac{A_1(d_1)g(d_2)g(d_3 \ldots d_{n+1})}{\tau_{n-1}(m/(d_1 d_2))} \\ &\qquad + \cdots \\ &\qquad + \frac{A_0(d_1)g(d_2)g(d_3)\ldots g(d_{n+1}))}{\tau_1(1)}\Bigg)\Bigg),\end{aligned} \tag{5.15}$$

where $\tau_k(n)$ counts the number of ways to write n as a product of k natural numbers. We first justify that this lengthy definition is well-defined. By Lemma 5.12,

$$\begin{aligned}\mathbf{F}'(g)(1) &= P_{\mathbf{F}'}(g(1)) \\ &= (P_{\mathbf{F}})'(g(1)).\end{aligned}$$

Since $g(1)$ is a root of $P_{\mathbf{F}}$ of multiplicity 1, we can not have that $(P_{\mathbf{F}})'(g(1)) = 0$. Next, observe that, in the second summation, g is always evaluated at a proper divisor of m; since $L(d) < L(m)$ for all proper divisors d of m, by our inductive hypothesis g is well-defined wherever it is evaluated in eq. (5.15). Lastly, since $\tau_k(n) > 0$ for all $n, k \in \mathbb{N}$, each of the fractions in the second summation is well defined. Thus $g(m)$ exists and is uniquely defined for each $m \in \mathbb{N}$.

We now show that, under the definition provided by eq. (5.15), $\mathbf{F}(g)(m) = 0$ for all $m \in \mathbb{N}$. We begin by multiplying both sides of eq. (5.15) by $-\mathbf{F}'(g)(1)$ and adding $g(m) \cdot \mathbf{F}'(g)(1)$ to both sides. This yields

$$0 = \left(\sum_{i=1}^{n} iA_i(1)g(1)^{i-1}g(m)\right) + \left(\sum_{j=0}^{n} A_j(m)g(1)^j\right) + \left(\sum_{\substack{d_1 d_2 \dots d_{n+1} = m \\ d_1, d_2, \dots, d_{n+1} \neq m}} \frac{A_0(d_1)g(d_2 d_3 \dots d_{n+1})}{\tau_n(m/d_1)} + \cdots + \frac{A_0(d_1)g(d_2)g(d_3)\dots g(d_{n+1}))}{\tau_1(1)}\right). \tag{5.16}$$

Now, by using the fact that $\tau_k(n)$ counts the number of ways to write n as a product of k natural numbers, we can represent the third sum by

$$\left(\sum_{\substack{d_1 d_2 = m \\ d_1, d_2 \neq m}} A_1(d_1)g(d_2)\right) + \left(\sum_{\substack{d_1 d_2 d_3 = m \\ d_1, d_2, d_3 \neq m}} A_1(d_1)g(d_2)g(d_3)\right) + \cdots + \left(\sum_{\substack{d_1 d_2 \dots d_{n+1} = m \\ d_1, \dots, d_{n+1} \neq m}} A_1(d_1)g(d_2)\dots g(d_{n+1})\right).$$

Lastly, observe that each of the terms in the first and second summations of eq. (5.16) corresponds to exactly one of the factorizations $d_1, d_2, \dots, d_{n+1}$ where $d_k = m$ for some $1 \leq k \leq n+1$; that is, the first and second sums are exactly the "extra" terms we excluded when we specified that $d_1, d_2, \dots d_{n+1} \neq m$. Combining these facts, we can rewrite eq. (5.16) as

$$\begin{aligned} 0 = A_0(m) &+ \left(\sum_{d_1 d_2 = m} A_1(d_1)g(d_2)\right) + \left(\sum_{d_1 d_2 d_3 = m} A_1(d_1)g(d_2)g(d_3)\right) \\ &+ \cdots + \left(\sum_{d_1 d_2 \dots d_{n+1} = m} A_1(d_1)g(d_2)\dots g(d_{n+1})\right) \\ &= A_0(m) + (A_1 * g)(m) + (A_2 * g^{*2})(m) + \cdots + (A_n * g^{*n})(m), \end{aligned}$$

which is our desired result. □

By repeated application of Theorem 5.14, we also have the following corollary:

Corollary 5.17. *Let $\boldsymbol{F} \in \mathbb{A}[X]$ such that $P_{\boldsymbol{F}}$ has n simple roots. Then $\boldsymbol{F}$ has at least n roots, counted with multiplicity.*

Note that we have shown that the existence of a simple root of $P_{\mathbf{F}}$ is a sufficient condition for $\mathbf{F}$ to have a root, but this condition is by no means necessary. The complexity in finding a necessary and sufficient condition for $\mathbf{F}$ to have a root stems largely from the existence of non-invertible arithmetic functions, as we stated in Section 3.

6. The Growth of Arithmetic Functions

Having examined the elements of $\mathbb{A}$ algebraically, we now consider them analytically, and explore several techniques for quantifying their behavior.

We begin with a definition which will form the core of this section:

Definition 6.1. Let $f, g \in \mathbb{A}$. We say f is an *average order* of g if

$$\lim_{x\to\infty} \frac{\sum\limits_{n\leq x} f(n)}{\sum\limits_{n\leq x} g(n)} = 1.$$

Average orders allow one to "smooth out" the erratic behavior of an arithmetic function, in the sense that arithmetic functions with unpredictable growth often have average orders with predictable growth.

As a classical example, we present the following proof of an average order of τ, the divisor-counting function:

Theorem 6.2. *The function* $\log(n)$ *is an average order of* τ.

Proof. We wish to find a function $f \in \mathbb{A}$ which satisfies the asymptotic formula

$$\sum_{n\leq x} f(n) \sim \sum_{n\leq x} \tau(n).$$

Since $\tau(n) = \sum\limits_{ab=n} 1$, this can be rewritten as

$$\sum_{n\leq x} f(n) \sim \sum_{ab\leq x} 1.$$

We will follow Dirichlet's proof, a method now commonly called the Dirichlet hyperbola method. Observe that the right-hand side can be interpreted as counting the number of lattice points under the hyperbola $ab = x$ (See Fig. 1).

In order to enumerate these points, we divide the figure into three overlapping sectors: where $a \leq \sqrt{x}$, where $b \leq \sqrt{x}$, and where $a, b \leq \sqrt{x}$. We then subtract off the overlap to obtain the formula:

$$\begin{aligned}
\sum_{n\leq x} \tau(n) &= \sum_{ab\leq x} 1 \\
&= \sum_{a\leq\sqrt{x}} \sum_{b\leq\frac{x}{a}} 1 + \sum_{b\leq\sqrt{x}} \sum_{a\leq\frac{x}{b}} 1 - \sum_{a,b\leq\sqrt{x}} 1 \\
&= \sum_{a\leq\sqrt{x}} \left\lfloor \frac{x}{a} \right\rfloor + \sum_{b\leq\sqrt{x}} \left\lfloor \frac{x}{b} \right\rfloor - \left\lfloor \sqrt{x} \right\rfloor^2 \\
&= 2x \sum_{a\leq\sqrt{x}} \left\lfloor \frac{1}{a} \right\rfloor - \left\lfloor \sqrt{x} \right\rfloor^2 \\
&= O(x \log x).
\end{aligned}$$

Since $x \log x = \sum\limits_{n\leq x} \log x$, we obtain that

$$\lim_{x\to\infty} \frac{\sum\limits_{n\leq x} \log(x)}{\sum\limits_{n\leq x} \tau(n)} = 1.$$

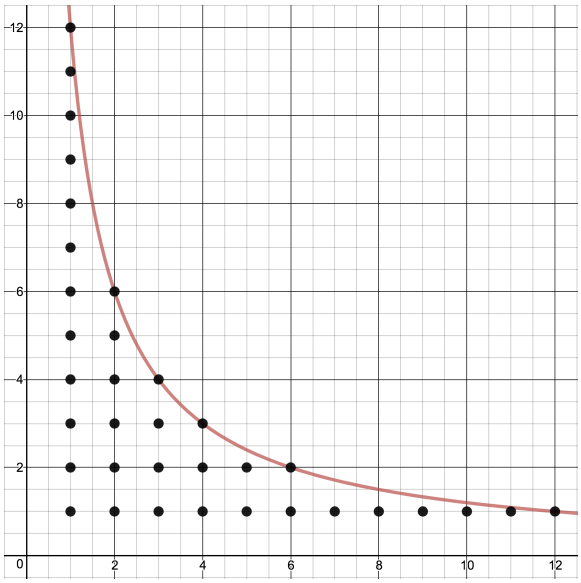

FIGURE 1. The sum of $\tau(n)$ over all $n \leq x$ can be interpreted as counting the lattice points under the hyperbola $ab = x$. Here $x = 12$ and the number of points is 35.

Hence $\log n$ is an average order for τ.

□

The above argument is in fact generalizable to a class of arithmetic functions which we now define:

Definition 6.3. The *k-th Piltz function* τ_k, defined for each $k \in \mathbb{N}$, counts the number of ways to express n as an ordered product of k natural numbers. For example, $\tau_3(6) = 9$ because

$$\begin{aligned} 6 &= 1 \cdot 1 \cdot 6 \\ &= 1 \cdot 6 \cdot 1 \\ &= 6 \cdot 1 \cdot 1 \\ &= 1 \cdot 2 \cdot 3 \\ &= 1 \cdot 3 \cdot 2 \\ &= 2 \cdot 1 \cdot 3 \\ &= 2 \cdot 3 \cdot 1 \\ &= 3 \cdot 1 \cdot 2 \\ &= 3 \cdot 2 \cdot 1. \end{aligned}$$

(To justify the reuse of notation, observe that τ as defined in Definition 2.4(iii) is equal to τ_2.) Additionally, for each $k \in \mathbb{N}$, the *k-th divisor summatory function*

is denoted D_k and given by the sum

$$D_k(x) = \sum_{n \leq x} \tau_k(n).$$

By considering the sum as an enumeration of the number of k-dimensional lattice points in $\mathbb{R}^k$ under the hyperbolic surface $a_1 a_2 ... a_k = x$, it can be shown that

$$D_k(x) = xP_k(\log x) + \Delta_k(x),$$

where P_k is a polynomial of degree $k-1$ and Δ_k is an error term. Thus $(\log n)^{k-1}$ is an average order for τ_k.

One can use similar techniques to bound the values of arithmetic functions, as demonstrated by the following analysis of the behavior of ϱ:

Theorem 6.4.

(i) For all $x > 3$, $\sum_{n \leq x} \varrho(n) \leq (x-1)^{\lfloor \log_2(x) \rfloor}$.
(ii) For all $x \in \mathbb{N}$, $\sum_{n \leq x} \varrho(n) \geq x(\log x - 1)$.

Proof. (i) For $x \in \mathbb{N}$, let $P(x) = \sum_{n \leq x} \varrho(n)$. First, observe that since

$$\begin{aligned} \varrho(n) &= \sum_{\substack{d|n \\ d<n}} \varrho(d) \\ &= \sum_{\substack{d_1|n \\ d_1<n}} \sum_{\substack{d_2|d_1 \\ d_2<d_1}} \varrho(d_2) \\ &= \dots \\ &= \sum_{\substack{d_1|n \\ d_1<n}} \sum_{\substack{d_2|d_1 \\ d_2<d_1}} \cdots \sum_{\substack{d_{s-1}|d_s \\ d_{s-1}<d_s}} 1, \end{aligned}$$

we may characterize ϱ combinatorially as the number of ordered factorizations of n. Thus, $P(x)$ counts the number of ordered tuples of natural numbers (excluding 1 in each tuple and including the empty tuple $\{\emptyset\}$) whose product does not exceed x. Since the maximum length of such a tuple is $\lfloor \log_2(x) \rfloor$ (as long as $x \geq 4$) and each natural number in such a tuple must be less than or equal to x, we may thus bound $P(x)$ above by $(x-1)^{\lfloor \log_2(x) \rfloor}$.

(ii) As above, we will use the combinatorial interpretation of ϱ and P. Fix $x \in \mathbb{N}$. Of length 0, there is one tuple whose product is at most x, and of length 1 there are $x-1$ tuples whose product is at most x. Also, for each $n \leq x$, there are $\left\lfloor \frac{x}{n} \right\rfloor - 1$ tuples of length 2 whose product is at most x. Summing these

three terms together, we obtain that

$$\begin{aligned} P(x) &\geq 1 + (x-1) + \sum_{n \leq x} \left(\left\lfloor \frac{x}{n} \right\rfloor - 1 \right) \\ &= \sum_{n \leq x} \left\lfloor \frac{x}{n} \right\rfloor \\ &\geq \left(\sum_{n \leq x} \frac{x}{n} \right) - x \\ &\geq x \log x - x \\ &= x(\log x - 1). \end{aligned}$$

□

While these are loose bounds, this example demonstrates the basic methods which can be used to treat arithmetic functions analytically.

Acknowledgments. I am very grateful to my mentors, Billy Lee and Karl Schaefer, for their help and for encouraging my pursuit of these topics. I also want to thank Daniil Rudenko for a thoroughly engaging Apprentice curriculum, as well as for his input on the combinatorial side of my research.

References

[1] Apostol, T. M. (2010). Introduction to analytic number theory. New York: Springer.
[2] Tenenbaum, G. (2015). Introduction to analytic and probabilistic number theory. Providence: American Mathematical Society.
[3] Snellman, J. (2002). The ring of arithmetical functions with unitary convolution: Divisorial and topological properties. Research Reports in Mathematics, 4.
[4] Huxley, M. N. (2003). Exponential sums and lattice points III. Proceedings of the London Mathematical Society, 87(3), 591-609.
[5] Hardy, G. H. (1917). On Dirichlet's divisor problem. Proceedings of the London Mathematical Society, 2(1), 1-25.