Properties of Arithmetical Functions

Zack Clark

Math 336, Spring 2016

1 Introduction

Arithmetical functions, as defined by Delany [2], are the functions $f(n)$ that take positive integers n to complex numbers. A variety of such functions have useful number-theoretic properties that include (but not limited to): producing the number of positive divisors of n, the sum of positive divisors of n, and the sum of squares and four squares.

In this paper, I will summarize the key results shown by Delany that focus on proving facts about the group of units of a commutative ring of certain useful arithmetical functions. To that end, this paper will include a brief introduction to terminology and notation, such as basic principles of the ring of arithmetical functions, the Dirichlet Product, multiplicative functions, and antimultiplicative functions.

I will then proceed with an algebraic description of the group of units from the scalars, multiplicative functions, and antimultiplicative functions. From there, I will provide some details in which those two groups of functions can be viewed as complementary subspaces of a rational vector space. I will then use the Bell series of an arithmetical function f and its applications in studying completely multiplicative functions, showing the linear independence of multiplicative functions, and that there is an uncountable set of linearly independent of the product of special functions.

To conclude the paper, I will briefly discuss the Möbius function and Möbius inversion formula and how they can be applied to Fourier series.

2 Definitions and Background Information

To begin, I will define three arithmetical functions with interesting number theory properties:

$\tau(n) =$ the number of positive divisors of n

$\sigma(n) =$ the sum of positive divisors of n ($Also\ known\ as\ the\ Euler\ totient\ function$)

$\phi(n) =$ the number of positive integers $\mathrm{k} \leq \mathrm{n}$ such that $\mathrm{gcd(k, n)\ =\ 1}$.

These functions form a commutative ring with unity under pointwise addition; that is, $(f + g)(n) = f(n) + g(n)$ for positive integer n. Additionally, they satisfy unity under Dirichlet multiplication (or Dirichlet convolution), for which Apostol[1, Chapter 2] provides a definition and proof of commutativity and associativity.

Definition 1 *If f and g are two arithmetical functions, the Dirichlet Product is defined to be the arithmetical function j where*

$$j(n) = (f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$$

Theorem 1 *For any arithmetical functions f, g, h, we have*

$$\begin{aligned} f * g &= g * f && (commutative\ law) \\ (f * g) * h &= f * (g * h) && (associative\ law). \end{aligned}$$

Proof. The commutative property is evident from noting that $\sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{ab=n} f(a)g(b)$. For associativity, let $A = g*h$ and consider $f*A = f*(g*h)$. Then

$$\begin{aligned} (f * A)(n) &= \sum_{ad=n} f(a)A(d) \\ &= \sum_{ad=n} f(a) \sum_{bc=d} g(b)h(c) \\ &= \sum_{abc=n} f(a)g(b)h(c) \end{aligned}$$

If one lets $B = f * g$ and consider $B * h$ then $(B * h)(n)$ produces the same formula. Therefore $f*A = B*h$, so Dirichlet multiplication is associative. □

The Dirichlet product has a multiplicative identity given by an arithmetical function.

Definition 2

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & if\ n = 1 \\ 0 & otherwise \end{cases}$$

is the identity function, where for all f, $I * f = f * I = f$

The identity function allows us to formally define an inverse for an arithmetical function f and even give an explicit formula for it, provided certain conditions are satisfied.

Theorem 2 *Let f be an arithmetical function such that $f(1) \neq 0$. There is a unique arithmnetical inverse f^{-1}, called the Dirichlet inverse of f, where*

$$f * f^{-1} = f^{-1} * f = I.$$

For $n >$ 1, f^{-1} is given by

$$f^{-1}(1) = \frac{1}{f(1)},\ f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f(\frac{n}{d}) f^{-1}(d)$$

Proof. See Apostol[1, p. 30]. □

Both the Dirichlet product and the inverse formula generalizes nicely for a prime power, $p^k, k > 0$, and are given by

$$(f * g)(p^k) = \sum_{i=0}^{k} f(p^i) g(p^{k-i}), f^{-1}(p^k) = \frac{-1}{f(1)} \sum_{i=0}^{k-1} f(p^{k-i}) f^{-1}(p^i)$$

In this paper, we will pay particular attention to a subset of arithmetical functions that are multiplicative.

Definition 3 *An arithmetical function f that is multiplicative has the properties $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever gcd(m, n) = 1. A multiplicative function is uniquely determined by its value on prime powers, i.e.*

$$f(p_1^{k_1} \cdots p_r^{k_r}) = \prod_{i=1}^{r} f(p_i^{k_i})$$

3 Group of Units and Vector Spaces

3.1 Scalars, Multiplicative Functions, and Antimultiplicative Functions

The goal now is to show that the group of units for the invertible arithmetical functions f is the direct sum of three subgroups. First, consider $U = \{f : f(1) \neq 0\}$, $C = \{cI : c \in \Re, c \neq 0\}$, and $U_1 = \{f : f(1) = 1\}$. Clearly, $C, U_1 \subset U$ with $C \cap U_1 = \{I\}$. If $f \in U$ and $c = f(1)$, then $f(cI)*(\frac{1}{c}f)$ (which follows since $(cf)(n) = cf(n)$) where $cI \in C$ and $\frac{1}{c}f \in U_1$. Therefore $U = C \oplus U_1$.

Next, I will sketch Delany's [2, p. 87] proof that the multiplicative subgroup and antimultiplicative subgroup of U will complete the direct sum.

Definition 4 *An antimultiplicative function f satisfies the following two conditions*

$$f(1) = 1, f(p^k) = 0 \text{ for } p^k \text{ a prime power with } k > 0.$$

Let U_m to be the subgroup of multiplicative functions in U and take the complement of U_m in U_1 to be antimultiplicative. Denote this subgroup by U_A. U_A is a nonempty subgroup of U_1 since $I \in U_A$. Additionall, for $f, g \in U_A$ with $k > 0$, we have that $f * g, f^{-1} \in U_A$ using the properties described in Definition 4 and the generalized formulas for the Dirichlet Product and inverse.

Given $f \in U_1$, define g to be a multiplicative function and let $h = f * g^{-1}$. For $k > 0, h(p^k) = I(p^k) = 0$, and hence $f = g * h$ where $g \in U_m$ and $h \in U_A$. Therefore, $U_1 = U_m \oplus U_A$, and hence, $U = C \oplus U_m \oplus U_A$.

3.2 Vector Space $(U_1, *)$

To fully describe (U_1), a few more pieces of terminology must be presented.

Definition 5 *A group G is called an abelian group, if for every pair of elements $a, b \in G$, $ab = ba$ holds.* [1, p. 129]

Definition 6 *An abelien group is divisible if for each $g \in G$ and each positive integer n, there is an $x \in G$ such that $nx = g$.*

Definition 7 *A divisible abelian group in which x is unique is considered torsion-free. If an abelian group is a divisible torsion-free group, it can be viewed as a vector space over the rationals.*

The abelian group $(U_1, *)$ is a divisible torsion-free group, which leads to our next theorem proved in [2, p. 90].

Theorem 3 *For $f \in U_1$, and $\frac{m}{n} \in \mathbb{Q}$, let $f^{(m/n)}$ denote the unique $g \in U_1$ such that $g^{(n)} = f^{(m)}$. Defining scalar multiplication $\mathbb{Q} \times U_1 \to U_1$ by $(q, f) \to f^{(q)}$ makes the group $(U_1, *)$ a vector space over $\mathbb{Q}$.*

This theorem leads us to a description of the structure of U_m, and as $U = C \oplus U_m \oplus U_A$, the theorem also provides a description of U/U_m.

To study the linear independence of such groups of multiplicative functions, we will examine what is known as the Bell Series of an arithmetical function f. Before doing so, I will define several multiplicative functions as in [2].

$$\epsilon^{(m)}(n) = \sum_{d_1 \cdots d_m = n} 1, \epsilon^{(m)}(p^k) = \sum_{p^{k_1} \cdots p^{k_m} = p^k} 1$$

$$\mu^{(m)}(p^k) = \epsilon^{(-m)}(p^k), \mu^{(-m)}(p^k) = \epsilon^{(m)}(p^k)$$

4 Bell Series

Definition 8 *If f is an arithmetical function and p is a prime number, then the Bell series of f with respect to p is given by the power series*

$$f_p(X) = \sum_{k=0}^{\infty} f(p^k) X^k$$

Maclaurian series carry over to Bell series, and in particular several geometric series are useful in proving linear independence:

$$\begin{aligned} \epsilon_p(X) &= 1 + X + X^2 + \ldots = \frac{1}{1-X} \text{ (Ring of formal power series)} \\ (\epsilon_a)_p(X) &= 1 + p^\alpha X + p^{2\alpha} X^2 + \ldots = \frac{1}{1-p^\alpha X} \\ \lambda_p(X) &= 1 - X + X^2 - \ldots = \frac{1}{1+X} \text{ (Liouville } \lambda) \end{aligned}$$

The following theorem states the property of Bell series that makes them such a useful tool for studying multiplicative functions.

Theorem 4 *Consider two arithmetical functions f and g and let $h = f * g$. Then*

$$h(p^n) = f_p(X) g_p(X)$$

Proof.

$$\begin{aligned} f_p(X) g_p(X) &= \left(\sum_{i=0}^{\infty} f(p_i) X^i \right) \left(\sum_{k=0}^{\infty} g(p_k) X^k \right) \\ &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} f(p^i) g(p^{k-i}) \right) X^k \\ &= \sum_{k=0}^{\infty} (f * g)(p^k) X^k = (f * g)_p(X) \end{aligned}$$

□

This result allows for Bell series for $I, \epsilon, \tau, \phi, \lambda, etc.$ to be easily calculated by

considering them as the product of functions with known Bell series.
If an arithemtical function f is completely multiplicative, then by definition $f(p^k) = f(p)^k$ and f is determined by its values on the primes. Using Bell series, we see that $f_p(X) = \frac{1}{1-f(p)X}$. From this result follows a way of calculating rational powers of completely multiplicative functions, with the proof being provided on [2, p. 94].

Proposition 1 *If f is completely multiplicative and $q \in \mathbb{Q}$, then $f^{(q)} = \epsilon^{(q)} f$. When $n = p_1^{k_1} \cdots p_r^{k_r}$,*

$$f^{(q)}(n) = f(n) \prod_{i=1}^{r} \binom{q + k_i - 1}{k_i}$$

Now, we will be able to make very striking claims about the linear independence in U_m.

5 Linear Independence

The following proposition and theorem are the primary results of [2], and consequently, they will be presented in detail.

5.1 In the Reals

A lemma proven in [2] will be necessary to follow the results about linear independence.

Lemma 1 *Suppose $\prod_{i=1}^{r} P_i(X)^{m_i} = 1$, where P_i are nonconstant polynomials, not necessarily distinct, and the m_i are integers. If some P_k is relatively prime to all the others, then $m_k = 0$.*
Additionally, for $\prod_{i=1}^{r}(1 - C_i X)^{-m_i} = 1$ with C_i nonzero constants, if some C_k is different from all the others, then $m_k = 0$.

Consider a set $W \in U_1$ to be a vector space. W is linearly dependent if and only if there exist distinct functions $f_1, \ldots, f_r \in W$ and rationals $q_1, /ldots, q_r$ (not all zero) such that $f_1^{q_1} * \cdots * f_r^{q_r} = I$. By letting N be a positive integer such that $m_i = q_i N$ are integers, then $f_1^{m_1} * \cdots * f_r^{m_r} = I$. In U_m this can occur if and only if $\prod_{i=1}^{r}(f_i)_p(X)^{m_i} = 1$ for each prime.

Proposition 2 *The functions $\{\epsilon_\alpha\lambda_\beta : \alpha, \beta, \in \mathbb{R}, \beta \neq 0\}$ are linearly independent.*

Proof. Suppose $f_1^{m_1} * \cdots * f_r^{m_r} = I$ with m_i being integers. Using Bell series, we see that

$$\prod_{i=1}^{r}(1 - p^{\alpha_i}\beta_i X)^{-m_i} = 1$$

for every prime p. Define $C_i(p) = p^{\alpha_i}\beta_i$ and consider all $C_i(p) = C_j(p)$ where $i \neq j$. Each equation has a solution with no more than one p. Hence, there are a finite number of solutions altogether, so therefore there is a prime such that $C_i(p)$ are all different. By Lemma 1 then, each m_i is zero. □

5.2 Now to $\mathbb{C}$

The results for real-valued α, β is a special case, and can be extended to the complex plane. The main difference in the two cases is that unlike on the reals, $C_i(p) = C_i(p)$ does not have at most one solution, since for $\alpha, \beta \in \mathbb{C}$ it is possible for $p^\alpha = q^\alpha$ when p, q are distinct primes. However, as discussed in [2], by the fundamental theorem of arithmetic, there are most two primes such that $p^\alpha = \beta$. Using this fact, the generalized of Proposition 2 can be proven.

Theorem 5 *The functions $\{\epsilon_\alpha\lambda_\beta : \alpha, \beta, \in \mathbb{C}, \beta \neq 0\}$ are linearly independent.*

Proof. For the same C_i as in Proposition 2, examine $C_i(p) = C_j(p), i \neq j$. This equality simplifies to $p^{\alpha_i - \alpha_i} = \frac{\beta_j}{\beta_i}$. There are no solutions when $\alpha_i = \alpha_j$ since that would imply $\beta i = \beta_j$ as well. As stated above, when $\alpha_i \neq \alpha_j$ there are at most two solutions. Therefore, there are at most a finite number of solutions altogether, so there is one that makes all $C_i(p)$. By Lemma 1, all the exponents m_i are zero. □

To conclude the paper, I will discuss a multiplicative function briefly mentioned by Delany, along with its applications to the Zeta function and Fourier series.

6 Möbius Function

Definition 9 *The Möbius function $\mu(n)$ is defined by:*

$$\mu(n) = \begin{cases} 1 & if\ n = 1 \\ (-1)^r & if\ n\ is\ the\ product\ of\ r\ distinct\ primes \\ 0 & otherwise \end{cases}$$

By using the Dirichlet product, one can find a very useful formula that allows us to relate the Riemann Zeta function to this multiplicative function.

Theorem 6

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \qquad Re(s) > 1$$

Proof. Consider $F(s) = \sum_1^\infty \frac{f(n)}{n^s}$ and $G(s) = \sum_1^\infty \frac{g(n)}{n^s}$ where both f and g are multiplicative. Then both series are absolutely convergent for $Re(s) > 1$ and $F(s)G(s) = \sum_1^\infty \frac{h(n)}{n^s}$ where h is the Dirichlet product of $f * g*$ (see [1, 228]). Take $f(n) = 1$ and $g(n) = \mu(n)$, then $h(n) = I(n)$ and we obtain:

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1$$

Noting that $\zeta(s) \neq 0$ on $Re(s) > 1$ completes the proof. □

This relationship between the Möbius function and the Riemann Zeta function can be used to prove, as in [3, 46], the following definition of the *Möbius Inversion Formula.*

Definition 10 *Suppose that $f(n)$ and $F(n)$ are two multiplicative functions that satisfy the relationship*

$$F(n) = \sum_{d|n} f(d).$$

Then the Möbius Inversion Formula states that f is given by

$$f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d})$$

and the converse is also true.

6.1 Application to Fourier Series

It is possible to find explicit formulas for the Möbius inversions of Fourier series [4, 4]. Consider the Fourier expansion of the real-valued function f

$$f(x) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n x}$$

where the Fourier coefficients $a(n)$ are arithmetical functions.

Definition 11 *Let b be an arithmetical function and $f(x)$ defined as above. Then the "generalized" Dirichlet product is given by*

$$\begin{aligned}(b \odot f)(x) &= \sum_{m=1}^{\infty} b(m) \sum_{n=1}^{\infty} a(n) e^{2\pi i n x} = \sum_{m,n=1}^{\infty} a(n) b(m) e^{2\pi i n x} \\ &= \sum_{l=1}^{\infty} (\sum_{mn=l}^{\infty} a(n) b(n)) e^{2\pi i l x} = \sum_{l=1}^{\infty} (a * b)(l) e^{2\pi i l x}\end{aligned}$$

$(b \odot f)(x)$, therefore, is the Fourier series whose coefficients are given by the Dirichlet product of a and b. If we assume a is invertible, then we see that $(a^{-1} \odot f)(x) = e^{2\pi i x}$ by the Möbius Inversion Formula. Analogous formulas for $sin(2\pi x)$ and $cos(2\pi x)$ can be found by considering the real and imaginary components of f. The application of the Mbius inversion to Fourier series has resulted in numerous applications in physics, including finding arithmetic Fourier transforms and inverse Lattice problems.

Fourier coefficients that are completely multiplicative offer the best case in which strong approximations of inversion formulas. Unfortunately, this is not condition does not happen in general. A rather surprising result is that completely multiplicative Fourier coefficients occur for (but not only) for the Bernoulli polynomials. It is useful to consider periodic extensions of these polynomials, however.

Definition 12 *Let x be any real number and $k \geq 1$, and let $\{x\} = x - \lfloor x \rfloor$. Then the $[0,1]$ periodic extensions to (R) of $B_k(x)$ are given by the infinite series*

$$B_{2k}\{(x)\} = \frac{2(-1)^{k-1}(2k)!}{(2\pi)^{2k}} \sum_{n=1}^{\infty} \frac{cos(2\pi nx)}{n^{2k}},$$

$$B_{2k+1}\{(x)\} = \frac{2(-1)^{k-1}(2k+1)!}{(2\pi)^{2k+1}} \sum_{n=1}^{\infty} \frac{sin(2\pi nx)}{n^{2k+1}}.$$

I will conclude by stating one final theorem that defines an explicit formula for *sine* and *cosine* in terms of the Bernoulli periodic extensions and the Möbius function. The proof of these equalities can be found on [5, 6].

Theorem 7 *For every $k \geq$* and $x \in \mathbb{R}$,

$$cos(2\pi x) = \frac{(-1)^{k-1}(2\pi)^{2k}}{2(2k)!} \sum_{n=1}^{\infty} \frac{\mu(n) B_{2k}\{(nx)\}}{n^{2k}}$$

$$sin(2\pi x) = \frac{(-1)^{k-1}(2\pi)^{2k+1}}{2(2k+1)!} \sum_{n=1}^{\infty} \frac{\mu(n) B_{2k+1}\{(nx)\}}{n^{2k+1}}$$

The connection between the Bernoulli polynomials and the Riemann zeta function is clear. In fact, by setting x = 0, an alternative proof of Theorem 6 can be derived fairly easily.

References

[1] Tom Apostol. *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976

[2] James E. Delany. *Groups of Arithmetical Functions.* Mathematics Magazine, 78(2), 83-97, 2005.

[3] Karatsuba A. A. Karatsuba, and S.M. Voronin. *The Riemann-Zeta Function.* Walter de Gruyter, Berlin; New York, 1992

[4] Luis M. Navas, Francisco J. Ruiz, Juan L. Varona. *The Möbius inversion formula for Fourier series applied to Bernoulli and Euler polynomials.* Journal of Appoximation Theory, 163, 22-40, 2011.