Groups of Arithmetical Functions

JAMES E. DELANY, *Emeritus*
California Polytechnic State University
San Luis Obispo, CA 93407
jdelany@calpoly.edu

An *arithmetical function* is a mapping from the positive integers to the complex numbers. The more interesting ones involve some number-theoretic property, such as

$\tau(n) =$ the number of positive divisors of n,
$\sigma(n) =$ the sum of the positive divisors of n, and
$\phi(n) =$ the number of positive integers $k \leq n$ such that $\gcd(k, n) = 1$.

A typical introductory number theory book includes a chapter on these functions, showing that they form a commutative ring with unity under pointwise addition

$$(f + g)(n) = f(n) + g(n)$$

and *Dirichlet multiplication*

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

Here the sum is taken over all positive integer divisors d of n. This somewhat surprising choice of a product is quite fruitful, allowing one to obtain interesting number-theoretic formulas from simple computations in the ring. In particular, the useful functions mentioned above can all be expressed in terms of two simple elements of this ring.

In this MAGAZINE, Berberian [**2**] discussed (among other things) the group of units of this ring. He showed that τ, σ, and ϕ can be expressed in terms of two very simple functions and proved that those two functions are linearly independent. In this article we extend his pair to an uncountably infinite set. In the process, we present answers to other questions posed in his article, including a description of the structure of the group of units.

In the interest of accessibility, most of the discussion is confined to real-valued arithmetical functions. Except for a bit of abelian group theory, the algebraic ideas come from introductory linear algebra and abstract algebra. For many readers the only novel concept will be Bell series, a powerful tool developed by E. T. Bell in the early twentieth century.

NOTATION. The symbols $\mathbb{P}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ will denote the positive integers, nonnegative integers, integers, rational numbers, real numbers, and complex numbers, respectively.

Background

We develop some basic principles of the ring of arithmetical functions. Our presentation is self-contained, but the reader desiring more information may consult various introductory number theory books, such as Niven and Zuckerman [**6**, Chapter 4] or Rosen [**7**, Chapter 7]. Apostol [**1**, Chapter 2] is particularly helpful.

First, the Dirichlet product can also be expressed as

$$(f * g)(n) = \sum_{d_1 d_2 = n} f(d_1) g(d_2) \tag{1}$$

where the sum extends over all ordered pairs of positive divisors of n whose product is n. Extending this notation, the associative law states that

$$\big(f * (g * h)\big)(n) = \big((f * g) * h\big)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3).$$

The Dirichlet product is particularly easy to evaluate at a prime power, p^k:

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

The multiplicative identity of the ring is

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

To determine the group of units, we ask which arithmetical functions are invertible, in the sense of the Dirichlet product. As long as $f(1) \neq 0$, we can obtain f^{-1} inductively: $f^{-1}(1) = 1/f(1)$ and, when $n > 1$,

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

Again, the formula simplifies for a prime power, p^k, $k > 0$:

$$f^{-1}(p^k) = -\frac{1}{f(1)} \sum_{i=0}^{k-1} f^{-1}(p^i) f(p^{k-i}). \tag{2}$$

Scalar multiplication is defined as usual: $(cf)(n) = cf(n)$. Equation (1) makes it clear that $(cf) * g = f * (cg) = c(f * g)$.

Of particular interest are the functions that are *multiplicative*, those having the properties that $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$. The functions I, τ, σ, and ϕ are all multiplicative. The multiplicative functions form a subgroup of the group of units [**1**, Section 2.10]. A multiplicative function is uniquely determined by its values on the prime powers: if $p_1, \ldots, p_r$ are distinct primes, then

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

EXAMPLE. For each real α, the function ε_α defined by $\varepsilon_\alpha(n) = n^\alpha$ is multiplicative. In fact, it is *totally multiplicative* or *completely mutiplicative* in that $\varepsilon_\alpha(mn) = \varepsilon_\alpha(m)\varepsilon_\alpha(n)$ for all $m, n \in \mathbb{P}$. Then ε_α^{-1} must also be multiplicative, so $\varepsilon_\alpha^{-1}(1) = 1$ and it suffices to compute $\varepsilon_\alpha^{-1}(p^k)$, where p is a prime and k is a positive integer. From (2) we have $\varepsilon_\alpha^{-1}(p) = -\varepsilon_\alpha^{-1}(1)\varepsilon_\alpha(p) = -p^\alpha$. A routine induction, again using (2), shows that $\varepsilon_\alpha^{-1}(p^k) = 0$ when $k \geq 2$. Now suppose that $n > 1$ has prime factorization $n = p_1^{k_1} \cdots p_r^{k_r}$. Then $\varepsilon_\alpha^{-1}(n) = \prod_{i=1}^{r} \varepsilon_\alpha^{-1}(p_i^{k_i})$. This is zero if any one of the

k_i exceeds one. If each $k_i = 1$ we have $n = \prod_{i=1}^{r} p_i$ and $\varepsilon_\alpha^{-1}(n) = \prod_{i=1}^{r} \varepsilon_\alpha^{-1}(p_i) = \prod_{i=1}^{r}(-p_i^\alpha) = (-1)^r n^\alpha$. In summary, we have proved

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

The functions ε, ε_1, and μ Note that $\varepsilon_0(n) = 1$ and $\varepsilon_1(n) = n$ for all n. These functions play a key role; in fact, ε_0 and ε_1 are the two functions featured by Berberian in his article [**2**]. The function ε_0 occurs so often that we let $\varepsilon = \varepsilon_0$. Despite their importance, there is little agreement on notation, as seen in Table 1.

TABLE 1: Notation for I, ε, and ε_1

Author(s)	I	ε	ε_1
Apostol [**1**]	I	u	N
Berberian [**2**]	u	γ	ε
McCarthy [**5**]	δ	ζ	ζ_1
Niven and Zuckerman [**6**]	I	U	E
Rosen [**7**]	ι	ν	–

We can express τ, σ, and ϕ in terms of ε and ε_1 using the following idea: Suppose f is an arithmetical function and let

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} f(d)\varepsilon(n/d) = (f * \varepsilon)(n),$$

showing that $F = f * \varepsilon$. Since $\tau(n) = \sum_{d|n} 1$ and $\sigma(n) = \sum_{d|n} d$ we have

$$\tau = \varepsilon * \varepsilon$$

$$\sigma = \varepsilon_1 * \varepsilon.$$

There is a pretty equation involving Euler's ϕ function, the third on our initial list of examples:

$$\sum_{d|n} \phi(d) = n. \tag{3}$$

To see this, note that $\phi(d)$ equals the number of reduced fractions having denominator d in the interval $(0, 1]$. If we partition the set $\{1/n, 2/n, \ldots, n/n\}$ according to the denominators of the fractions in reduced form, the sum adds the cardinalities of these equivalence classes, and this total must be n. In terms of the Dirichlet product, (3) says $\phi * \varepsilon = \varepsilon_1$, or

$$\phi = \varepsilon_1 * \varepsilon^{-1}.$$

Thus τ, σ, and ϕ are each expressible in terms of ε and ε_1.

The Möbius function $\mu = \varepsilon^{-1}$ appears often, as in $\phi = \varepsilon_1 * \mu$. Taking $\alpha = 0$ in the formula for ε_α^{-1} yields

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

The *Möbius inversion formula* [**1**, p. 32] states that if $F(n) = \sum_{d|n} f(d)$ then $f(n) = \sum_{d|n} F(d)\mu(n/d)$. In our setting this reduces to the assertion that if $F = f * \varepsilon$ then $f = F * \varepsilon^{-1}$.

The group of units

Our initial goal is to obtain an algebraic description of the group of units. We begin by showing it is the direct sum of three subgroups: the scalars, the multiplicative functions, and a group to be defined momentarily.

First we split off the scalar functions.

Let $U = \{f \mid f(1) \neq 0\}$, $U_1 = \{f \mid f(1) = 1\}$, and $C = \{cI \mid c \in \mathbb{R}, c \neq 0\}$. Then C and U_1 are subgroups of U and $C \cap U_1 = \{I\}$. If $f \in U$ and $c = f(1)$ then $f = (cI) * (\frac{1}{c} f)$ with $cI \in C$ and $\frac{1}{c} f \in U_1$. Thus $U = C \oplus U_1$.

There are many important functions for which $f(1) \neq 1$.

EXAMPLE. (SUMS OF SQUARES) Hardy and Wright [**4**, p. 314] used $r_k(n)$ to denote the number of k-tuples $(a_1, a_2, \ldots, a_k)$ of integers for which $a_1^2 + a_2^2 + \cdots + a_k^2 = n$. The two most familiar cases are r_2 and r_4. It turns out that each is a scalar times a multiplicative function. In the first case, $r_2(n) = 4 \sum_{d|n} \chi(n)$, where χ is the completely multiplicative function given by

$$\chi(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ (-1)^{(n-1)/2} & \text{if } n \text{ is odd} \end{cases}$$

[**4**, p. 241]. Thus $r_2 = 4I * \chi * \varepsilon$, and $\chi * \varepsilon$ is multiplicative.

Lagrange showed that every positive integer is expressible as the sum of four squares, so r_4 is always positive. One formula is

$$r_4(n) = 8 \sum_{d|n, 4\nmid d} d$$

[**4**, p. 314]. Defining the multiplicative function f by

$$f(n) = \begin{cases} 0 & \text{if } 4 \mid n \\ n & \text{otherwise,} \end{cases}$$

we have $r_4(n) = 8 \sum_{d|n} f(d)$, and $r_4 = 8I * f * \varepsilon$ with $f * \varepsilon$ multiplicative.

The first few values of r_2 and r_4 are shown in Table 2. One reason these functions get special attention is that they can be related to factorization in the Gaussian integers and integer quaternions, respectively [**4**, Chapter 20].

TABLE 2: Number of ways to express n as the sum of two or four squares

n	1	2	3	4	5	6	7	8	9	10	11	12
χ	1	0	−1	0	1	0	−1	0	1	0	−1	0
$r_2 = 4I * \chi * \varepsilon$	4	4	0	4	8	0	0	4	4	8	0	0
f	1	2	3	0	5	6	7	0	9	10	11	0
$r_4 = 8I * f * \varepsilon$	8	24	32	24	48	96	64	24	104	144	96	96

Antimultiplicative functions Let U_M denote the subgroup of multiplicative functions in U. The desired complement of U_M in U_1 consists of functions we will call *antimultiplicative*, meaning $f(1) = 1$ and $f(p^k) = 0$ whenever p^k is a prime power with $k > 0$. Let U_A be the set of such functions.

To begin with, U_A is a subgroup of U_1. It is nonempty since $I \in U_A$. If $f, g \in U_A$ and $k > 0$ then $(f * g)(p^k) = \sum_{i=0}^{k} f(p^i)g(p^{k-i}) = \sum_{i=0}^{k} 0 = 0$ so $f * g \in U_A$. When $k > 0$ we also have $f^{-1}(p^k) = -\sum_{i=0}^{k-1} f^{-1}(p^i)f(p^{k-i}) = -\sum_{i=0}^{k-1} 0 = 0$ so $f^{-1} \in U_A$. Thus U_A is a group.

It is clear that $U_M \cap U_A = \{I\}$. We would like to be able to separate an arithmetical function into multiplicative and antimultiplicative pieces. Given $f \in U_1$, define g by

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

and let $h = g^{-1} * f$. Then $g \in U_M$ and we claim $h \in U_A$. For $k > 0$, we compute $h(p^k) = (g^{-1} * f)(p^k) = \sum_{i=0}^{k} g^{-1}(p^i)f(p^{k-i}) = \sum_{i=0}^{k} g^{-1}(p^i)g(p^{k-i}) = (g^{-1} * g)(p^k) = I(p^k) = 0$. Thus $f = g * h$ with $g \in U_M$ and $h \in U_A$, so $U_M \oplus U_A = U_1$.

EXAMPLE. Von Mangoldt's Λ function [**1**, p. 32] is given by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k,\ p \text{ prime}, k > 0 \\ 0 & \text{otherwise.} \end{cases}$$

It is useful in studying the distribution of primes. Although Λ is not a unit, e^{Λ} is in U_1. Let

$$f(n) = e^{\Lambda(n)} = \begin{cases} p & \text{if } n = p^k,\ p \text{ prime}, k > 0 \\ 1 & \text{otherwise.} \end{cases}$$

Now let us compute the multiplicative component of f. It turns out to involve the *core* of an integer, which is the product of its distinct prime divisors: $\gamma(p_1^{k_1} \cdots p_r^{k_r}) = p_1 \cdots p_r$. From the definition, the multiplicative part of f is the function g given by

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

Table 3 shows the first few values of e^{Λ}, its multiplicative component γ, and its antimultiplicative component $\gamma^{-1} * e^{\Lambda}$. It is instructive to compute a few examples to verify that $f = g * h$.

TABLE 3: Multiplicative and antimultiplicative components of e^{Λ}

n	1	2	3	4	5	6	7	8	9	10	11	12
$e^{\Lambda} = f$	1	2	3	2	5	1	7	2	3	1	11	1
$\gamma = g$	1	2	3	2	5	6	7	2	3	10	11	6
$\gamma^{-1} * e^{\Lambda} = h$	1	0	0	0	0	−5	0	0	0	−9	0	5

This completes the first step in the description of the group of units: $U = C \oplus U_M \oplus U_A$.

Powers It is actually possible to regard U_1 as a rational vector space in which U_M and U_A are complementary subspaces. This vector space structure is somewhat surprising, as it does not involve addition, but instead entails raising units to rational powers with respect to the Dirichlet product. For $f \in U$ let $f^{(0)} = I$, $f^{(1)} = f$, $f^{(2)} = f * f$, etc. When m is a negative integer let $f^{(m)} = (f^{-1})^{(-m)}$. Needless to say, these powers obey the usual laws of exponents. The associative law extends to m factors as

$$(f_1 * \cdots * f_m)(n) = \sum_{d_1 \cdots d_m = n} f_1(d_1) \cdots f_m(d_m).$$

When $f_1 = \cdots = f_m = f$ this reduces to

$$f^{(m)}(n) = \sum_{d_1 \cdots d_m = n} f(d_1) \cdots f(d_m).$$

As an example, consider powers of ε and $\mu = \varepsilon^{-1}$. If m is a positive integer then

$$\varepsilon^{(m)}(n) = \sum_{d_1 \cdots d_m = n} \varepsilon(d_1) \cdots \varepsilon(d_m) = \sum_{d_1 \cdots d_m = n} 1.$$

In other words, this counts the number of ways to express n as the product of m positive divisors, taking the order of the factors into account. Since ε is multiplicative, $\varepsilon^{(m)}$ is also multiplicative and it suffices to determine it on prime powers. Here

$$\varepsilon^{(m)}(p^k) = \sum_{p^{k_1} \cdots p^{k_m} = p^k} 1 = \sum_{k_1 + \cdots + k_m = k} 1,$$

where each $k_i \in \mathbb{N}$. The number of ways to express k as the sum of m nonnegative integers is $\binom{m+k-1}{m-1}$. To see this, form a row of $m + k - 1$ 1s, choose $m - 1$ of them to be replaced by $+$ signs; regrouping gives an expression for k as desired. For instance, if $k = 5$ and $m = 3$, the row 1 1 1 1 1 1 1 could become 1 1 + +1 1 1, leading to $5 = 2 + 0 + 3$. Thus,

$$\varepsilon^{(m)}(p^k) = \binom{m+k-1}{m-1} = \binom{m+k-1}{k}.$$

We claim that $\mu^{(m)}(p^k) = (-1)^k \binom{m}{k}$ for $m \geq 0$. To begin with, $I(p^k) = (-1)^k \binom{0}{k}$. The induction step follows from $\mu^{(m+1)} = \mu * \mu^{(m)}$ and the identity

$$\binom{m}{k} + \binom{m}{k-1} = \binom{m+1}{k}.$$

When $m < 0$,

$$\mu^{(m)}(p^k) = \varepsilon^{(-m)}(p^k) = \binom{-m+k-1}{k} = (-1)^k \binom{m}{k}.$$

In other words, the formula for positive m also works for negative m. Similarly, if $m < 0$, then

$$\varepsilon^{(m)}(p^k) = \mu^{(-m)}(p^k) = (-1)^k \binom{-m}{k} = \binom{m+k-1}{k},$$

just as in the case $m \geq 0$. In summary,

PROPOSITION 1. *If m is an integer and $n = p_1^{k_1} \cdots p_r^{k_r}$ then*

$$\varepsilon^{(m)}(n) = \mu^{(-m)}(n) = \prod_{i=1}^{r} \binom{m + k_i - 1}{k_i}$$

and

$$\mu^{(m)}(n) = \varepsilon^{(-m)}(n) = \prod_{i=1}^{r} (-1)^{k_i} \binom{m}{k_i}.$$

Furthermore, when $m > 0$, $\varepsilon^{(m)}(n)$ equals the number of ways to express n as the product of m positive integers, taking the order of the factors into account.

For example, $\tau(n) = \varepsilon^{(2)}(n) = \prod_{i=1}^{r} \binom{1+k_i}{k_i} = \prod_{i=1}^{r} (1 + k_i)$.

EXERCISE. For $m \geq 0$ show that $\varepsilon_\alpha^{(m)} = \varepsilon_\alpha \varepsilon^{(m)}$. More generally, if f is any arithmetical function then $(\varepsilon_\alpha f)^{(m)} = \varepsilon_\alpha f^{(m)}$. Here $\varepsilon_\alpha f$ denotes ordinary multiplication.

Elements of finite order Does U_1 have any elements of finite order? A group is said to be *torsion-free* if the only element of finite order is the identity. The group U_1 is torsion-free.

To see this, assume $f^{(m)} = I$ with $m > 0$. Suppose $n > 1$ and $f(d) = 0$ for all $1 < d < n$. Then

$$0 = f^{(m)}(n) = \sum_{d_1 \cdots d_m = n} f(d_1) \cdots f(d_m).$$

The only summands that might not be zero are those in which one of the factors d_i equals n and the rest equal 1. Then $0 = f^{(m)}(n) = mf(n)$ and $f(n) = 0$.

The next step in defining rational powers is to show the existence of roots. In a torsion-free abelian group, roots are unique when they exist. In our situation the reasoning is that if $f^{(m)} = g^{(m)}$ then $(f * g^{-1})^{(m)} = I$, and since U_1 is torsion-free, $f * g^{-1} = I$ and $f = g$.

Roots What happens when we try to construct roots? Suppose $g \in U_1$ and m is a positive integer. We are looking for $f \in U_1$ such that $f^{(m)} = g$. To begin with, $f(1) = 1$. For $n > 1$,

$$g(n) = f^{(m)}(n) = \sum_{d_1 \cdots d_m = n} f(d_1) \cdots f(d_m).$$

Separating out the summands involving $f(n)$ gives

$$g(n) = mf(n) + \sum_{\substack{d_1 \cdots d_m = n \\ d_1, \ldots, d_m < n}} f(d_1) \cdots f(d_m)$$

and solving for $f(n)$ we get

$$f(n) = \frac{1}{m} \left(g(n) - \sum_{\substack{d_1 \cdots d_m = n \\ d_1, \ldots, d_m < n}} f(d_1) \cdots f(d_m) \right).$$

Thus $f(n)$ can be determined inductively, and it is unique.

When $f^{(m)} = g$ we write $g^{(1/m)} = f$.

EXAMPLE. Let us find $\varepsilon^{(1/2)}$ and $\varepsilon^{(1/3)}$. Let f be the function such that $f^{(2)} = \varepsilon$. The preceding formula tells us

$$f(p) = (1/2)(1 - 0) = 1/2$$
$$f(p^2) = (1/2)(1 - f(p)^2) = 3/8$$
$$f(p^3) = (1/2)(1 - 2f(p)f(p^2)) = 5/16$$

These values of $\varepsilon^{(1/2)}(p^k)$ are displayed in Table 4. The mth root of a multiplicative function is also multiplicative, for reasons to be explained soon. This allows us to compute the remaining displayed values of $\varepsilon^{(1/2)}$. Similar calculations yield the indicated values of $\varepsilon^{(1/3)}$.

TABLE 4: Dirichlet roots of ε

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varepsilon^{(1/2)}$	1	1/2	1/2	3/8	1/2	1/4	1/2	5/16	3/8	1/4	1/2	3/16
$\varepsilon^{(1/3)}$	1	1/3	1/3	2/9	1/3	1/9	1/3	14/81	2/9	1/9	1/3	2/27

The vector space $(U_1, *)$ Before describing the structure of U_1, we review some properties of abelian groups, bearing in mind that they are normally discussed using additive notation. An abelian group $(G, +)$ is said to be *divisible* if for each $g \in G$ and each $n \in \mathbb{P}$ there is an $x \in G$ such that $nx = g$. If G is torsion-free, x will be unique. This allows one to view G as a vector space over $\mathbb{Q}$ by letting $(m/n)g$ be the unique solution to $nx = mg$. We have shown that $(U_1, *)$ is a divisible torsion-free group, so we can view it as a vector space over the rationals.

For a thorough discussion of divisible groups, see Fuchs [**3**, Chapter IV]. Divisible groups have some extremely nice properties. A subgroup of a divisible group is a direct summand if and only if it is divisible. Since U_M and U_A are complementary summands of the group U_1, they are divisible subgroups and therefore complementary subspaces when U_1 is regarded as a vector space. In particular, this implies that the nth root of a multiplicative function is multiplicative (as asserted in constructing Table 4) and that the nth root of an antimultiplicative function is antimultiplicative. In summary,

THEOREM 1. *For $f \in U_1$ and $m/n \in \mathbb{Q}$ 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 $\mathbb{Q}$. Furthermore, U_M and U_A are complementary subspaces: $U_1 = U_M \oplus U_A$.*

This result answers two questions posed by Berberian [**2**]. It describes the structure of the group U_M of multiplicative functions and, since $U = C \oplus U_M \oplus U_A$, it also describes the quotient group U/U_M.

He also showed that the two functions ε and ε_1 are linearly independent, and posed the problem of finding a third. In order to study independence, we introduce a new tool.

Bell series

With each arithmetical function we associate a family of formal power series called *generating functions* that distills much of the information about the function. If f is an arithmetical function and p is a prime, then the *Bell series of f with respect to p* is

the formal power series

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

Discussions of the basic ideas of these series can be found in Apostol [**1**, p. 43] and McCarthy [**5**, p. 60]. When speaking of Bell series we often omit the phrase "for each prime p." The statement $I_p(X) = 1$ is intended to mean that this is true for each prime p.

Formulas involving Maclaurin series carry over to Bell series. The geometric series is especially useful. For example,

$$\varepsilon_p(X) = 1 + X + X^2 + \cdots = 1/(1 - X),$$

meaning that $1 + X + X^2 + \cdots = (1 - X)^{-1}$ in $\mathbb{R}[[X]]$, the ring of formal power series. More generally,

$$(\varepsilon_\alpha)_p(X) = 1 + p^\alpha X + p^{2\alpha}X^2 + \cdots = 1/(1 - p^\alpha X).$$

Another well-known function is the Liouville λ [**1**, p. 37] given by

$$\lambda(p_1^{k_1} \cdots p_r^{k_r}) = (-1)^{k_1+\cdots k_r}.$$

Here $\lambda(p^k) = (-1)^k$ and

$$\lambda_p(X) = 1 - X + X^2 - X^3 + \cdots = 1/(1 + X).$$

The calculation of the series for γ is only slightly more complicated:

$$\gamma_p(X) = 1 + pX + pX^2 + pX^3 + \cdots = 1 + \frac{pX}{(1 - X)} = \frac{1 - (1 - p)X}{1 - X}.$$

The feature of Bell series that makes them so valuable is that $(f * g)_p(X) = f_p(X)g_p(X)$. This follows from the rule for multiplying power series:

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

Bell series are most useful in studying multiplicative functions. If $f, g \in U_M$ then, since a multiplicative function is determined by its values on prime powers, $f = g$ if and only if $f_p(X) = g_p(X)$ for each prime p. On the other hand, they are useless when it comes to antimultiplicative functions: $f \in U_1$ is antimultiplicative if and only if $f_p(X) = 1$ for each prime p. If $f \in U_1$, then the Bell series of f equals the Bell series of its multiplicative component.

The multiplicative property implies that if $m \in \mathbb{N}$ then $(f^{(m)})_p(X) = f_p(X)^m$. When $f \in U$ we have $(f^{-1})_p(X)f_p(X) = I_p(X) = 1$ so $(f^{-1})_p(X) = f_p(X)^{-1}$. Then $f_p^{(m)}(X) = f_p(X)^m$ when m is a negative integer as well.

Table 5 lists a few Bell series and illustrates some basic properties: μ and ε are inverses, and their series are reciprocals; σ and ϕ illustrate the product rule; τ is an example of a power.

TABLE 5: Selected Bell series

f	$f_p(X)$
I	1
μ	$1 - X$
ε	$1/(1 - X)$
ε_1	$1/(1 - pX)$
$\tau = \varepsilon * \varepsilon$	$1/(1 - X)^2$
$\sigma = \varepsilon * \varepsilon_1$	$1/\big((1 - X)(1 - pX)\big)$
$\phi = \mu * \varepsilon_1$	$(1 - X)/(1 - pX)$
γ	$\big(1 - (1 - p)X\big)/(1 - X)$
λ	$1/(1 + X)$

What about Bell series of rational powers? Suppose $f \in U_1$ and $f_p(X) = F(X) = 1 + \sum_{k=1}^{\infty} a_k X^k$. If m is a positive integer, there is a unique $g \in U_1$ for which $g^{(m)} = f$, in which case $g_p(X)^m = f_p(X)$. On the other hand, there is a unique series $G(x) = 1 + \sum_{k=1}^{\infty} b_k X^k$ such that $G(X)^n = F(X)$: its coefficients can be calculated inductively and are uniquely determined. Then $g_p(X)$ must equal $G(X)$, so there is no ambiguity in writing $(f^{(1/n)})_p(X) = f_p(X)^{1/n}$ or, for that matter, $(f^{(m/n)})_p(X) = f_p(X)^{m/n}$.

Completely multiplicative functions We illustrate the value of Bell series by using them to determine rational powers of completely multiplicative functions. As noted earlier, each ε_α has this property. Two more examples are Liouville's λ and the χ used in computing r_2. We can generalize the former to λ_β, $\beta \neq 0$, by letting

$$\lambda_\beta(p_1^{k_1} \cdots p_r^{k_r}) = \beta^{k_1 + \cdots k_r}.$$

Each λ_β is completely multiplicative, as are all the products $\varepsilon_\alpha \lambda_\beta$.

If f is completely multiplicative, then $f(p^k) = f(p)^k$ and f is determined by its values on the primes. In that case the Bell series are

$$f_p(X) = \sum_{k=0}^{\infty} f(p^k) X^k = \sum_{k=0}^{\infty} f(p)^k X^k = 1/(1 - f(p)X).$$

For example, $(\varepsilon_\alpha \lambda_\beta)_p(X) = \sum_{k=0}^{\infty} p^{k\alpha} \beta^k X^k = 1/(1 - p^\alpha \beta X)$.

Calculating rational powers of completely multiplicative functions involves binomial series. Many calculus students know that, for $s \in \mathbb{R}$,

$$(1 + x)^s = 1 + \sum_{k=1}^{\infty} \binom{s}{k} x^k$$

where $\binom{s}{k} = s(s - 1) \cdots (s - k + 1)/k!$, even when s is not an integer [**8**, p. 809]. This series converges for $|x| < 1$. In our setting, namely the power series ring $\mathbb{R}[[X]]$, defining $(1 + X)^s$ to mean the series $1 + \sum_{k=1}^{\infty} \binom{s}{k} X^k$ extends the binomial theorem for integer exponents to real exponents in a manner consistent with the ring operations.

Replacing s by $-s$ and X by $-CX$ yields the formula

$$(1 - CX)^{-s} = 1 + \sum_{k=1}^{\infty} \binom{-s}{k} (-1)^k (CX)^k.$$

But

$$\binom{-s}{k}(-1)^k = \binom{s+k-1}{k},$$

so

$$(1 - CX)^{-s} = 1 + \sum_{k=1}^{\infty} \binom{s+k-1}{k} C^k X^k.$$

For example, if q is rational then

$$(\varepsilon^{(q)})_p(X) = (1 - X)^{-q} = \sum_{k=0}^{\infty} \binom{q+k-1}{k} X^k$$

and

$$\varepsilon^{(q)}(p^k) = \binom{q+k-1}{k}.$$

Thus Proposition 1 extends to rational powers:

$$\varepsilon^{(q)}(p_1^{k_1} \cdots p_r^{k_r}) = \prod_{i=1}^{r} \binom{q+k_i-1}{k_i}. \tag{4}$$

EXAMPLE. $\varepsilon^{(1/2)}(p^k) = \binom{k-1/2}{k}$ where

$$\begin{aligned}\binom{k-\frac{1}{2}}{k} &= \frac{(k-\frac{1}{2})(k-\frac{3}{2})\cdots(\frac{1}{2})}{k!}\left(\frac{2^k}{2^k}\right) \\ &= \frac{(1)(3)\cdots(2k-1)}{2^k k!},\end{aligned}$$

so $\varepsilon^{(1/2)}(p) = 1/2$, $\varepsilon^{(1/2)}(p^2) = 3/8$, and $\varepsilon^{(1/2)}(p^3) = 5/16$, just as in Table 4. We could also write

$$\begin{aligned}\varepsilon^{(1/2)}(p^k) &= \left(\frac{(1)(3)\cdots(2k-1)}{2^k k!}\right)\left(\frac{(2)(4)(6)\cdots(2k)}{2^k k!}\right) \\ &= \frac{1}{4^k}\binom{2k}{k}.\end{aligned}$$

Similarly

$$\varepsilon^{(1/3)}(p^k) = \binom{k-\frac{2}{3}}{k} = \frac{(1)(4)(7)\cdots(3k-2)}{3^k k!}.$$

As in Table 4, $\varepsilon^{(1/3)}(p) = 1/3$, $\varepsilon^{(1/3)}(p^2) = 2/9$, and $\varepsilon^{(1/3)}(p^3) = 14/81$.

When f is completely multiplicative,

$$\begin{aligned}(f^{(q)})_p(X) = f_p(X)^q &= (1 - f(p)X)^{-q} \\ &= \sum_{k=0}^{\infty} \binom{q+k-1}{k} f(p)^k X^k \\ &= \sum_{k=0}^{\infty} \varepsilon^{(q)}(p^k) f(p^k) X^k \\ &= (\varepsilon^{(q)} f)_p(X).\end{aligned}$$

In other words, $f^{(q)} = \varepsilon^{(q)} f$. Then, from the formula (4) for $\varepsilon^{(q)}$, we obtain

PROPOSITION 2. *If f is completely multiplicative and $q \in \mathbb{Q}$ then $f^{(q)} = \varepsilon^{(q)} f$. When $n = p_1^{k_1} \cdots p_r^{k_r}$,*

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

Linear independence With Bell series at our disposal, we can obtain some sweeping results about linear independence in U_M. In the sense of this vector space, a set $\mathcal{F} \subseteq U_1$ is linearly dependent if and only if there exist distinct functions $f_1, \ldots, f_r \in \mathcal{F}$ and rationals $q_1, \ldots, q_r$, not all zero, such that $f_1^{(q_1)} * \cdots * f_r^{(q_r)} = I$. In that case, let N be a positive integer such that all the $m_i = q_i N$ are integers. Then $f_1^{(q_1 N)} * \cdots * f_r^{(q_r N)} = I^{(N)}$, or $f_1^{(m_1)} * \cdots * f_r^{(m_r)} = I$. In other words, it suffices to consider integer exponents. In U_M we have $f_1^{(m_1)} * \cdots * f_r^{(m_r)} = I$ if and only if $\prod_{i=1}^{r} (f_i)_p(X)^{m_i} = 1$ for each prime p. The following is useful in dealing with such products.

LEMMA 1. *Suppose $\prod_{i=1}^{r} P_i(X)^{m_i} = 1$, where the 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 $m_k = 0$.*

In particular, when $\prod_{i=1}^{r} (1 - C_i X)^{-m_i} = 1$, where the C_i are nonzero constants, if some C_k is different from all the others, then $m_k = 0$.

Proof. Rewrite the equation as

$$\prod_{m_i < 0} P_i(X)^{-m_i} = \prod_{m_j \geq 0} P_j(X)^{m_j}$$

to obtain polynomials on both sides of the equation. If P_k is relatively prime to the others and $m_k \neq 0$, then P_k divides one side but not the other, a contradiction. ∎

Before offering our principal result on independence, we illustrate the ideas involved with a special case.

PROPOSITION 3. *The functions $\{\varepsilon_\alpha \lambda_\beta \mid \alpha, \beta \in \mathbb{R}, \beta \neq 0\}$ are linearly independent.*

Proof. Suppose $f_1^{(m_1)} * \cdots * f_r^{(m_r)} = I$, where the m_i are integers, $f_i = \varepsilon_{\alpha_i} \lambda_{\beta_i}$, and the f_i are all distinct. We must show that each m_i is zero. In terms of Bell series we have $\prod_{i=1}^{r} (f_i)_p(X)^{m_i} = 1$ for every prime p, or

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

Let $C_i(p) = p^{\alpha_i}\beta_i$. Consider all the equations $C_i(p) = C_j(p)$ with $i \neq j$. Each equation is satisfied by at most one prime p: if a solution to $p^{\alpha_i}\beta_i = p^{\alpha_j}\beta_j$ does exist it can only be $p = (\beta_j/\beta_i)^{1/(\alpha_i-\alpha_j)}$. Thus there are at most a finite number of solutions altogether, so there must be a prime that makes the $C_i(p)$ all different. Lemma 1 then implies that each m_i is zero. ∎

EXERCISE. (POWERS OF γ) For $\alpha \in \mathbb{R}$ show that

$$(\gamma^\alpha)_p(X) = \frac{1-(1-p^\alpha)X}{1-X}$$

and that $\{\gamma^\alpha \mid \alpha \in \mathbb{R}\}$ is a linearly independent set.

Extension to $\mathbb{C}$ All of the foregoing extends to complex-valued arithmetical functions. In this setting $\varepsilon_\alpha(n) = n^\alpha = e^{\alpha \ln n}$. The function λ_β needs no special consideration since the exponents involved are all integers. The only delicate point arises in the proof of the preceding proposition, where we used the fact that each equation $C_i(p) = C_j(p)$, $i \neq j$, had at most one solution. This is not the case in the complex numbers, since it is possible to have $p^\alpha = q^\alpha$ for distinct primes p, q. For instance, if $\alpha = 2\pi i/\ln(3/2)$, then $(3/2)^\alpha = e^{\alpha \ln(3/2)} = e^{2\pi i} = 1$ and $3^\alpha = 2^\alpha$.

On the other hand, if $\alpha, \beta \in \mathbb{C}$ and $\alpha \neq 0$, there are at most two primes p such that $p^\alpha = \beta$. To see this, suppose that p, q, r are distinct primes and $p^\alpha = q^\alpha = r^\alpha = \beta$. Then $(p/q)^\alpha = (p/r)^\alpha = 1$. Taking logarithms, $\alpha \ln(p/q) = 2k\pi i$ and $\alpha \ln(p/r) = 2l\pi i$ with k and l integers. The equation $\alpha l \ln(p/q) = \alpha k \ln(p/r)$ quickly leads to $p^l r^k = p^k q^l$ and the fundamental theorem of arithmetic implies that $k = l = 0$. But in that case, $\alpha \ln(p/q) = \alpha \ln(p/r) = 0$, an impossibility, since $\alpha \neq 0$ and p, q, r are distinct.

We are now in a position to state our main result on independence. Berberian [**2**] proved that ε and ε_1 are independent. But $\varepsilon = \varepsilon_0\lambda_1$ and $\varepsilon_1 = \varepsilon_1\lambda_1$ are just two members of the following uncountable independent set.

THEOREM 2. *The functions $\{\varepsilon_\alpha\lambda_\beta \mid \alpha, \beta \in \mathbb{C}, \beta \neq 0\}$ are linearly independent.*

Proof. Proceed as in the proof of Proposition 3. The equation $C_i(p) = C_j(p)$, $i \neq j$, reduces to $p^{\alpha_i-\alpha_j} = \beta_j/\beta_i$. When $\alpha_i = \alpha_j$ there are no solutions, since we can't also have $\beta_i = \beta_j$. When $\alpha_i \neq \alpha_j$ there are at most two solutions, as we have just seen. Once again, we only need to avoid a finite number of primes to find one that makes all the $C_i(p)$ distinct, so Lemma 1 again implies that all the exponents are zero. ∎

The functions gcd($m, \cdot$) As a final application we consider some functions involving the greatest common divisor. For $m, n \in \mathbb{P}$ let $G_m(n) = \gcd(m, n)$. Each G_m is multiplicative. These functions are not independent: $G_2 * G_3 = G_1 * G_6$, for example. Bell series allow us to uncover such relations.

PROPOSITION 4. *Let (a, b) and $[a, b]$ denote the gcd and lcm of a and b.*

1. *$G_a * G_b = G_{(a,b)} * G_{[a,b]}$ for all $a, b \in \mathbb{P}$.*
2. *If $(a, b) = 1$ then $G_{ab} = \mu * G_a * G_b$.*
3. *If $m = m_1 m_2 \cdots m_r$ and the m_i are pairwise relatively prime then*

$$G_m = \mu^{(r-1)} * G_{m_1} * \cdots * G_{m_r}.$$

4. *If the prime factorization of m is $p_1^{k_1} \cdots p_r^{k_r}$ then*

$$G_m = \mu^{(r-1)} * G_{p_1^{k_1}} * \cdots * G_{p_r^{k_r}}.$$

Proof. First note that if h is the largest integer such that $p^h \mid m$ then

$$(G_m)_p(X) = 1 + pX + p^2X^2 + \cdots + p^{h-1}X^{h-1} + p^hX^h + p^hX^{h+1} + p^hX^{h+2} + \cdots$$
$$= \frac{1 - p^hX^h}{1 - pX} + \frac{p^hX^h}{1 - X} = \frac{1 - X - (p^{h+1} - p^h)X^{h+1}}{(1 - pX)(1 - X)}.$$

Call this $g(p, h, X)$. Now suppose $a, b \in \mathbb{P}$. For a given prime p let p^h be the highest power of p dividing a and let p^k be the highest dividing b. Then $(G_a * G_b)_p(X) = g(p, h, X)g(p, k, X)$. The highest power dividing (a, b) is p^m, where $m = \min(h, k)$, and the highest dividing $[a, b]$ is p^M, with $M = \max(h, k)$. Here $(G_{(a,b)} * G_{[a,b]})_p(X) = g(p, m, X)g(p, M, X)$. But either $h \le k$, $m = h$, and $M = k$, or $k \le h$, $m = k$, and $M = h$. In either case $g(p, h, X)g(p, k, X) = g(p, m, X)g(p, M, X)$. Thus $(G_a * G_b)_p(X) = (G_{(a,b)} * G_{[a,b]})_p(X)$ for all p, and $G_a * G_b = G_{(a,b)} * G_{[a,b]}$.

Noting that $G_1 = \varepsilon$, we have $G_a * G_b = \varepsilon * G_{ab}$ when $(a, b) = 1$. This implies the second equation. The third equation comes from repeated application of the second, and the fourth is a special case of the third. ∎

As an example, $G_{12} * G_{18} = G_6 * G_{36} = \mu^{(2)} * G_2 * G_3 * G_4 * G_9$.

This naturally raises the question of independence. In fact it can be shown that the functions $\{G_{q^k} \mid q \text{ prime}, k \in \mathbb{P}\}$ are linearly independent. Noting that $(G_{q^k})_p(X) = 1/(1 - X)$ if $p \ne q$, and

$$(G_{p^k})_p(X) = \frac{1 + (p - 1)X + (p^2 - p)X^2 + \cdots + (p^k - p^{k-1})X^k}{1 - X},$$

we could eventually establish the assertion by applying Lemma 1 to the numerators of the latter expressions, as in the proof of Proposition 3. The details of the argument, though interesting, are lengthy enough to divert us from the focus of this article so we will not pursue this point.

Further investigation Interesting areas of research lie in many directions.

- A systematic survey of multiplicative functions would be in order, in which the Bell series of families of functions are used to study their dependence relations in the rational vector space U_M. An excellent source of such families is McCarthy [**5**].
- What about the group of functions we have termed antimultiplicative? We haven't said anything about these, leaving the topic for readers to pursue.
- Is U_1 actually a vector space over $\mathbb{R}$ or even $\mathbb{C}$? For completely multiplicative f the right side of the formula in Proposition 2 for $f^{(q)}$ can be evaluated if q is real or even complex. What problems arise when one tries to extend exponentiation to real or complex exponents?

The study of algebraic properties of the ring of arithmetical functions offers research opportunities at many levels. A *Mathematica* notebook that facilitates experimentation with these functions is available at the MAGAZINE website, `www.maa.org/pubs/mathmag.html`.

REFERENCES

1. Tom M. Apostol, *Introduction to Analytic Number Theory,* Springer-Verlag, New York, 1976.
2. S. K. Berberian, *Number-Theoretic Functions via Convolution Rings,* this MAGAZINE, **65**, 1992, 75–90.
3. László Fuchs, *Infinite Abelian Groups,* Academic Press, New York, 1970.

4. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* 5th ed., Clarendon Press, Oxford, 1979.
5. Paul J. McCarthy, *Introduction to Arithmetical Functions,* Springer-Verlag, New York, 1986.
6. Ivan Niven and Herbert S. Zuckerman, *An Introduction to the Theory of Numbers,* 4th ed., John Wiley & Sons, New York, 1980.
7. Kenneth H. Rosen, *Elementary Number Theory and Its Applications,* 4th ed., Addison Wesley Longman, Reading, Massachusetts, 2000.
8. James Stewart, *Calculus,* 5th ed., Brooks/Cole, Belmont, California, 2003.

Letter to the Editor: Sury on Binet

In "A Parent of Binet's Formula?," October 2004, B. Sury asks if there is "a more natural motivation explaining the polynomial identity"

$$\sum_{i\geq 0}(-1)^i\binom{n-i}{i}(XY)^i(X+Y)^{n-2i} = X^n + X^{n-1}Y + \cdots + XY^{n-1} + Y^n.$$

Here is a simple combinatorial explanation of this identity.

The $\binom{n-i}{i}$ term counts the ways to tile a strip of length n with i dominoes of length two and $n-2i$ squares of length one (since such a strip has $n-i$ tiles altogether, from which we choose i of them to be dominoes). Now imagine that we are tiling a strip of length n with squares and dominoes but our squares can be colored in $X+Y$ ways, say X of the colors are *light* and Y of colors are *dark*. Also we will allow both halves of our dominoes to be colored, but the left half is always given a light color and the right half is given a dark color. Thus each domino can be colored in XY ways. Hence the number of tilings with exactly i dominoes (and thus $n-2i$ squares) would be

$$\binom{n-i}{i}(XY)^i(X+Y)^{n-2i}.$$

The total number of tilings is the sum of the above expression over all values of i (to be nonzero, we must have $0 \leq i \leq n/2$).

The left side of the polynomial identity is the number of colored tilings with an even number of dominoes minus the number of colored tilings with an odd number of dominoes. I claim that this difference is "almost zero" since there is an easy way to change the parity of the number of dominoes in "practically every" colored tiling. Specifically, for any tiling, look for the first occurrence of either A) a colored domino or B) a light square followed by a dark square.

If the first such occurrence is a colored domino then chop that domino in half to produce a light square followed by a dark square, producing a tiling of type B. If the first such occurrence is of type B, then join the colored squares together to form a domino, thus creating a tiling of type A. Notice that when we go from A to B or from B to A, we change the parity of the number of dominoes. Thus practically every tiling of type A holds hands with a tiling of type B and vice versa.

What are the exceptions? Simply those tilings that have no dominoes and never have a light square followed by a dark square. Such tilings consist of i dark squares followed by $n-i$ light squares for some $0 \leq i \leq n$, which can be done Y^iX^{n-i} ways. In total, the number of tilings with no light-dark pattern is $X^n + X^{n-1}Y + \cdots + XY^{n-1} + Y^n$, as desired.

——ART BENJAMIN
HARVEY MUDD COLLEGE
CLAREMONT, CA 91711