ARTICLES

Number-Theoretic Functions via Convolution Rings

S. K. BERBERIAN
University of Texas
Austin, TX 78712

For Peter John Durbin

We've all met and befriended at least one of the 'number-theoretic functions' τ, σ, φ: for a positive integer n,

$\tau(n) =$ the number of divisors of n,
$\sigma(n) =$ the sum of the divisors of n,
$\varphi(n) =$ the number of integers k $(1 \leqslant k \leqslant n)$ that are relatively prime to n.

Here 'divisor' means positive integral divisor; and to say that k is relatively prime to n—usually written $(k, n) = 1$—means that 1 is the only common divisor of k and n. For example,

$$\tau(6) = |\{1,2,3,6\}| = 4$$

(vertical bars around a finite set count the number of elements of the set),

$$\sigma(6) = 1 + 2 + 3 + 6 = 12,$$

and $\varphi(6) = |\{1,5\}| = 2$.

There is a beautiful formula that relates these three functions:

$$\varphi * \tau = \sigma.$$

What does it mean? The left side alludes to a way of combining two functions to form a third—a law of composition for functions. Here's how we evaluate the function $\varphi * \tau$ at a positive integer n: We take a divisor d of n, form the product $\varphi(d)\tau(n/d)$ (so to speak, n/d is the divisor of n 'complementary to d'), and we sum these products over all possible divisors d of n. For example,

$$\begin{aligned}(\varphi * \tau)(6) &= \varphi(1)\tau(6) + \varphi(2)\tau(3) + \varphi(3)\tau(2) + \varphi(6)\tau(1)\\ &= 1\cdot 4 + 1\cdot 2 + 2\cdot 2 + 2\cdot 1 = 12,\end{aligned}$$

which equals $\sigma(6)$ (a miracle!). Try it for $n = 12$.

Why does it work? One way to see it would be to derive formulas for φ, τ, and σ and verify that the equation is true (in the last section, we give a one-line proof). Both aspects—deriving the formulas and verifying the equation—call on a property of the functions that is not readily apparent: They are multiplicative. This means that

$$\tau(mn) = \tau(m)\tau(n) \quad \text{whenever } (m, n) = 1,$$

and similarly for the functions σ and φ (all of these facts will be proved below). In view of the Fundamental Theorem of Arithmetic (factorization into powers of primes, unique apart from the order of the factors), this reduces the computation of, say, $\varphi(n)$, to the computation of $\varphi(p^k)$, where p is prime and k is a positive integer. For example,

$$\begin{aligned}\varphi(60) &= \varphi(2^2\cdot 3\cdot 5) = \varphi(2^2)\varphi(3\cdot 5)\\ &= \varphi(4)\varphi(3)\varphi(5) = 2\cdot 2\cdot 4 = 16.\end{aligned}$$

To reduce the verification of $(\varphi * \tau)(n) = \sigma(n)$ to the case that $n = p^k$, we need to know that $\varphi * \tau$ is also multiplicative. And therein lies the tale....

The functions τ, σ, φ, and a host of other interesting functions live in a fascinating ring A. The elements of A are the functions $f\colon \mathbb{P} \to \mathbb{Z}$, where $\mathbb{P}$ is the set of positive integers and $\mathbb{Z}$ is the ring of integers:

$$\mathbb{P} = \{1,2,3,\dots\}, \qquad \mathbb{Z} = \{0,\pm 1,\pm 2,\pm 3,\dots\}.$$

Functions f, g in A are added 'pointwise',

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

and their product $f * g$, called the *convolution* of f and g, is defined by the formula

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

(the sum extends over all *positive* integral divisors d of n). We will see that A, equipped with the operations $f+g$ and $f*g$, is a commutative ring with a unity element u (the only computation of any substance is the associative law for convolution). The set of units (= invertible elements) of the ring A is a group, called the *group of units* of A and denoted U_{A}:

$$\mathrm{U}_{\mathrm{A}} = \{f \in \mathrm{A}\colon f * g = u \text{ for some } g \in \mathrm{A}\}.$$

It turns out that the units of A are the functions $f \in \mathrm{A}$ such that $f(1) = \pm 1$. A function $f \in \mathrm{A}$ will be called *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$. The group of units includes all of the multiplicative functions f (simply because $f(1) = 1$). The centerpiece of the theory is the following theorem:

The multiplicative functions form a **subgroup** *of the group of units of* A.

Some of the preliminaries will be presented in slightly greater generality: We will look at convolution rings $\mathrm{A} = \mathrm{A}_{\mathrm{R}}(\mathrm{S})$ of functions $f\colon \mathrm{S} \to \mathrm{R}$, for certain monoids S and for certain rings R.[1] The motive is twofold: to clear the air of irrelevant special properties of the monoid $\mathrm{S} = \mathbb{P}$ and the ring $\mathrm{R} = \mathbb{Z}$, and to point the way for further exploration. The reader who prefers to leave the generality for another day can substitute $\mathbb{P}$ for S, and $\mathbb{Z}$ for R; very little substance (and none of the fun) will be lost by doing so. With or without the generality, the topic is technically within the reach of (and, judging from my experience, greatly enjoyed by) an undergraduate class in abstract algebra, toward the end of the semester. This article is written in the hope of encouraging students and teachers to give it a try.

[1] The exposition is inspired by that of G. Hochschild, *Perspectives of Elementary Mathematics* (Springer-Verlag, 1983), Chapter 2.

1. Counting Divisors (The Function τ)

In the first two sections we prove a core of facts from number theory 'with our bare hands' (no fancy techniques); these pertain to the functions τ and φ described in the introduction.

LEMMA. *For each positive integer n, write D_n for the set of positive integral divisors of n:*

$$\mathrm{D}_n = \{x \in \mathbb{P}: x|n\}.$$

For every pair of positive integers m and n, the formula $f(x,y)=xy$ defines a surjective mapping $f\colon \mathrm{D}_m \times \mathrm{D}_n \to \mathrm{D}_{mn}$.

Proof. If x and y are divisors of m and n, respectively, then xy is a divisor of mn, thus the formula $f(x,y)=xy$ does indeed define a mapping $f\colon \mathrm{D}_m \times \mathrm{D}_n \to \mathrm{D}_{mn}$; it remains to prove that f is surjective. Assuming $z|mn$, we seek a factorization $z=xy$ with $x|m$ and $y|n$. Say $mn=tz$. Let $x=(m,z)$ (the greatest common divisor of m and z) and write $m=xm_1$, $z=xz_1$. We have

$$(xm_1)n = mn = tz = t(xz_1),$$

so $m_1 n = tz_1$. Since $z_1|m_1 n$ and $(z_1, m_1)=1$ we have $z_1|n$, and the desired factorization $z=xy$ is obtained by setting $y=z_1$.

THEOREM 1. *If m and n are relatively prime positive integers, then the mapping $f\colon \mathrm{D}_m \times \mathrm{D}_n \to \mathrm{D}_{mn}$ of the lemma is bijective.*

Proof. In view of the lemma, it suffices to show that f is injective. Assuming $xy=x'y'$, where x, x' are divisors of m, and y, y' are divisors of n, we must show that $x=x'$ and $y=y'$. Since $x|m$, $y'|n$ and $(m,n)=1$, we have also $(x,y')=1$; but x divides $xy=x'y'$, so necessarily $x|x'$. Similarly $x'|x$, so $x=x'$; then $y=y'$ by cancellation.

Remark. The converse of Theorem 1 is true: If f is injective then $(m,n)=1$. (Hint: Assuming $(m,n)=d>1$, show that f is not injective. Write $m=m_1 d$, $n=n_1 d$ and look at $m_1 n = mn_1$.)

Definition 1. For every positive integer n, the *number* of (positive integral) divisors of n is denoted $\tau(n)$; thus $\tau(n)=|\mathrm{D}_n|$, where $\mathrm{D}_n=\{k \in \mathbb{P}: k|n\}$.

Examples. $\tau(6)=4$ because $D_6=\{1,2,3,6\}$; $\tau(1)=1$; for $n>1$, $\tau(n)\geqslant 2$ because n has at least the divisors 1 and n; $\tau(7)=2$ because $\mathrm{D}_7=\{1,7\}$; $\tau(n)=2 \Leftrightarrow n$ is a prime number.

The key property of τ:

THEOREM 2. $\tau(mn)=\tau(m)\tau(n)$ *whenever* $(m,n)=1$.

Proof. If $(m,n)=1$ then, by Theorem 1, $|\mathrm{D}_{mn}| = |\mathrm{D}_m \times \mathrm{D}_n| = |\mathrm{D}_m| \cdot |\mathrm{D}_n|$.

Definition 2. A function $f\colon \mathbb{P} \to \mathbb{Z}$ is called a *number-theoretic function*; f is said to be *multiplicative* if $f(1)=1$ and if $f(mn)=f(m)f(n)$ whenever $(m,n)=1$.

Remark. If $f(mn)=f(m)f(n)$ whenever $(m,n)=1$ and if $f(1)\neq 1$, then f is identically zero. (Look at $f(n\cdot 1)=f(n)f(1)$.)

Multiplicativity is a powerful tool for computation:

Corollary. *If n is a positive integer with prime-power factorization*

$$n = p_1^{k_1} \cdots p_r^{k_r}$$

(where $p_1, \ldots, p_r$ are distinct primes and $k_1, \ldots, k_r$ are positive integers) then

$$\tau(n) = \prod_{i=1}^{r} (k_i + 1).$$

Proof. By Theorem 2, it suffices to show that $\tau(p^k) = k + 1$ when p is prime and k is a positive integer. The set of divisors of p^k is $\{1, p, p^2, \ldots, p^k\}$.

2. Euler's φ-function

According to the definition in the introduction,

$$\varphi(n) = |\{k \in \mathbb{P}: 1 \leqslant k \leqslant n, (k, n) = 1\}|.$$

The derivation of the properties of φ is expedited by finding another formula for it.

Lemma 1. *If n is an integer greater than 1, $\mathbb{Z}_n = \mathbb{Z}/(n)$ is the ring of integers modulo n and $\mathrm{U}_{\mathbb{Z}_n}$ is the group of units of $\mathbb{Z}_n$, then the order of $\mathrm{U}_{\mathbb{Z}_n}$ is $\varphi(n)$.*

Proof. For any integer k, write $\bar{k} = k + (n)$ for the equivalence class of k modulo n, where $(n) = \mathbb{Z}n$ is the set of all integral multiples of n. By Euclid's algorithm for calculating the greatest common divisor, k and n are relatively prime if and only if $1 = rk + sn$ for suitable integers r and s. On passing to quotients modulo n, this means that $\bar{1} = \bar{r}\bar{k}$ for some integer r, that is, $\bar{k}$ is invertible in the quotient ring $\mathbb{Z}_n$. Thus, as k runs over the integers from 1 to $n - 1$ that are relatively prime to n, $\bar{k}$ runs over the group of units of $\mathbb{Z}_n$.

Lemma 2. *If m and n are relatively prime integers greater than 1, then $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ are isomorphic as rings.*

Proof. Define a mapping $f\colon \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by the formula $f(k) = (k + (m), k + (n))$; this is easily seen to be a ring homomorphism, with kernel $(m) \cap (n) = ([m, n])$, where $[m, n]$ is the least common multiple of m and n. Since $mn = (m, n)[m, n]$ and $(m, n) = 1$ we have $mn = [m, n]$, thus the kernel of f is (mn). By the First Isomorphism Theorem, passage to quotients modulo the kernel yields a monomorphism $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$. But

$$|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = |\mathbb{Z}_m \times \mathbb{Z}_n|,$$

so the mapping is necessarily surjective.

Remark. With notations as in Lemma 2, if a and b are any two integers then there exists an integer k such that $k + (m) = a + (m)$ and $k + (n) = b + (n)$ (that's the meaning of surjectivity in the preceding proof); in other words $k \equiv a \pmod{m}$ and $k \equiv b \pmod{n}$. In this form, the lemma is known as the Chinese Remainder Theorem.

Lemma 3. *If R and S are rings with unity and $\mathrm{R} \times \mathrm{S}$ is the product ring, then $\mathrm{U}_{\mathrm{R} \times \mathrm{S}} = \mathrm{U}_{\mathrm{R}} \times \mathrm{U}_{\mathrm{S}}$.*

Proof. Products in $\mathrm{R} \times \mathrm{S}$ are defined by the formula $(x, y)(x', y') = (xx', yy')$; such a product is equal to the unity element $(1, 1)$ if and only if $xx' = 1$ and $yy' = 1$.

THEOREM 3. *If m and n are relatively prime positive integers, then $\varphi(mn)=\varphi(m)\varphi(n)$.*

Proof. If $m=1$ or $n=1$ the equation is trivial. Suppose m and n are $\geqslant 2$. In view of Lemmas 1–3, the asserted equation is immediate from the formula for the number of elements in a product set.

On the way to a formula for actually computing $\varphi(n)$:

LEMMA 4. *For integers $a, b_1, \ldots, b_r$,*

$$(a, b_1 \cdots b_r)=1 \quad \Leftrightarrow \quad (a, b_i)=1 \quad \textit{for all } i.$$

Proof. In words, an integer is relatively prime to each of a list of integers if and only if it is relatively prime to their product. For $a=0$ or $a=\pm 1$ the asserted equivalence is trivial. Assuming $a \geqslant 2$, write $u_i=b_i+(a)$ for the class of b_i modulo a. By the proof of Lemma 1, the assertion is that

$$u_1 \cdots u_r \text{ is a unit of } \mathbb{Z}_a \quad \Leftrightarrow \quad u_1, \ldots, u_r \text{ are units of } \mathbb{Z}_a,$$

which is obviously true.

THEOREM 4. *If n is a positive integer with prime-power factorization $n=p_1^{k_1} \cdots p_r^{k_r}$, then*

$$\varphi(n)=\prod_{i=1}^{r}\left(p_i^{k_i}-p_i^{k_i-1}\right).$$

Proof. By Theorem 3 we need only show that $\varphi(p^k)=p^k-p^{k-1}$ for p prime and k a positive integer. Let $1 \leqslant a \leqslant p^k$. By Lemma 4,

$$(a, p^k)=1 \quad \Leftrightarrow \quad (a, p)=1;$$

since p is prime, this means that

$$(a, p^k)>1 \quad \Leftrightarrow \quad (a, p)=p \quad \Leftrightarrow \quad a \text{ is a multiple of } p.$$

Let $\mathrm{X}=\{a \in \mathbb{P}\colon 1 \leqslant a \leqslant p^k\}$, a set with p^k elements. The elements of X that are multiples of p form a subset $\mathrm{Y}=\{p, 2p, 3p, \ldots, p^{k-1}p\}$ with p^{k-1} elements. Thus, for $a \in \mathrm{X}$,

$$(a, p^k)=1 \quad \Leftrightarrow \quad a \in \mathrm{X}-\mathrm{Y},$$

where $\mathrm{X}-\mathrm{Y}$ is a set with p^k-p^{k-1} elements.

3. Monoids of Finite Type

A *semigroup* (written multiplicatively) is a nonempty set S with a binary operation $x \cdot y$ (or simply xy) that is associative ($xy \cdot z=x \cdot yz$ for all x, y, z). A *monoid* is a semigroup having an element 1 that is neutral for the operation ($1x=x1=x$ for all x). The data for a monoid is conveniently expressed as a triple $(\mathrm{S}, \cdot, 1)$. A monoid is *cancellative* if $xy=xz$ (or $yx=zx$) implies $y=z$, and *commutative* if $xy=yx$ for all x, y.

Example. The monoid $(\mathbb{P},\cdot,1)$ of positive integers under multiplication is both cancellative and commutative. It also has the following property, which is crucial for our discussion.

Definition 3. A monoid $(S,\cdot,1)$ is said to be of *finite type* if each element of S has only finitely many factorizations in S; in other words, for each $x \in S$, the set of ordered pairs $\{(y,z) \in S \times S\colon x = yz\}$ is finite. (This set contains at least the ordered pairs $(1,x)$ and $(x,1)$.)

Example 1. In the monoid $(\mathbb{P},\cdot,1)$, $ab = n \Leftrightarrow a|n$ and $b = n/a$, so

$$\{(a,b)\colon ab = n\} = \{(a,n/a)\colon a|n\},$$

a set with $\tau(n)$ elements.

Example 2. Let $S = F_1[t]$ be the set of all *monic* (leading coefficient 1) polynomials with coefficients in a field F. With ordinary polynomial multiplication as the law of composition and the constant polynomial 1 as neutral element, S is a commutative and cancellative monoid. It is of finite type because each monic polynomial is factorable uniquely (apart from order) as a product of powers of a finite list of irreducible monic polynomials. (If p,q are irreducible monic polynomials and $p|q$, then $p = q$.)

Example 3. Let $S = \{1,t,t^2,t^3,\dots\}$, t an indeterminate, with $t^it^j = t^{i+j}$ as the operation (where $t^0 = 1$). This is essentially the monoid $(\mathbb{N},+,0)$ in multiplicative disguise, where $\mathbb{N} = \{0,1,2,3\dots\}$.

Definition 4. An element x of a monoid S is said to be a *unit* if there is an element $x' \in S$ (necessarily unique) such that $xx' = x'x = 1$. The set U_S of all units of S is a group (called, naturally, the group of units of S).

Examples. For the monoid $(\mathbb{P},\cdot,1)$, the group of units is $\{1\}$; for $(\mathbb{Z},\cdot,1)$ it is $\{1,-1\}$; for $(\mathbb{Z},+,0)$ it is $\mathbb{Z}$ (here the notation is 'additive'); for $(F,\cdot,1)$, where F is a field, it is $F - \{0\}$; for the monoid $F_1[t]$ of Example 2, it is $\{1\}$; for $(R,\cdot,1)$, where R is a ring with unity, the group of units is the set of invertible elements of R. A group is a monoid all of whose elements are units.

Remark. If $(S,\cdot,1)$ is a monoid of finite type, then its group of units is finite. (Proof: The set of all ordered pairs (x,y) with $xy = 1$ is finite; the units of S are among the first coordinates of such pairs.) It follows that an infinite group—for example $(\mathbb{Z},+,0)$—is not a monoid of finite type.

4. Rings of Functions on Monoids of Finite Type

In this section $(S,\cdot,1)$ is a monoid of finite type and R is any ring with unity. (In Section 5 we specialize to $S = \mathbb{P}$; in Sections 6 and 7, $S = \mathbb{P}$ and the ring R is required to be commutative; in the final Section 8, we throw in the towel and assume that $S = \mathbb{P}$ and $R = \mathbb{Z}$.)

Definition 5. The set of all functions $f\colon S \to R$ will be denoted $A_R(S)$, briefly A. For f, $g \in A$, $f = g$ means that $f(x) = g(x)$ for all $x \in S$.

Two operations must be defined to make A a ring: *addition* (along with concepts of 'zero' and 'negatives') and *multiplication*. The definitions pertaining to addition are as follows:

Definition 6. For $f, g \in \mathrm{A}$ the *sum* $f+g$ of f and g, and the *negative* $-f$ of f, are defined 'pointwise':

$$(f+g)(x) = f(x) + g(x), \qquad (-f)(x) = -f(x)$$

for all $x \in \mathrm{S}$. The *zero* element of A is the constant function $0\colon \mathrm{S} \to \mathrm{R}$ defined by $0(x) = 0$ for all $x \in \mathrm{S}$, where the 0 on the right side is the zero element of the ring R.

LEMMA 1. *For the operations of Definition* 6, $(\mathrm{A}, +, 0)$ *is an abelian group.*

The proof of the lemma is straightforward and elementary. The multiplicative structure of A is more subtle.

Definition 7. For $f, g \in \mathrm{A}$ we define a function $f * g \in \mathrm{A}$, called the *convolution* of f and g, by the formula

$$(f*g)(x) = \sum_{yz=x} f(y)g(z)$$

for all $x \in \mathrm{S}$. (The sum on the right is finite because only finitely many ordered pairs (y, z) qualify.)

Example. If $\mathrm{S} = \mathbb{P}$ (under multiplication) then

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

where d runs over all positive integral divisors of n (the sum has $\tau(n)$ terms). When n is a prime p, there are only two terms: $(f*g)(p) = f(1)g(p) + f(p)g(1)$.

The proof that Definition 7 makes A a ring with unity (commutative when S and R are commutative) is arranged in a series of lemmas.

LEMMA 2. *For all* $f, g, h \in \mathrm{A}$, $f*(g+h) = f*g + f*h$ *and* $(f+g)*h = f*h + g*h$.

Proof. This is a straightforward consequence of the definitions and the distributive laws in the ring R.

LEMMA 3. *For all* $f, g, h \in \mathrm{A}$, $(f*g)*h = f*(g*h)$.

Proof. For all $x \in \mathrm{S}$,

$$\begin{aligned}[f*(g*h)](x) &= \sum_{yz=x} f(y)(g*h)(z) \\ &= \sum_{yz=x} f(y) \sum_{st=z} g(s)h(t) \\ &= \sum_{y\cdot st=x} f(y)\cdot g(s)h(t),\end{aligned}$$

summed over all triples (y, s, t) for which $y \cdot st = x$; similarly,

$$[(f*g)*h](x) = \sum_{ys\cdot t=x} f(y)g(s)\cdot h(t),$$

summed over all triples (y, s, t) for which $ys \cdot t = x$. Since $y \cdot st = ys \cdot t$ and $f(y)\cdot g(s)h(t) = f(y)g(s)\cdot h(t)$ (because the operations in S and R are associative), we see that $[f*(g*h)](x) = [(f*g)*h](x)$ for all $x \in \mathrm{S}$.

From Lemmas 1–3 we know that A is a ring. The unity element u of A is defined as follows:

Definition 8. The function u: $\mathrm{S} \to \mathrm{R}$ is defined by $u(1_{\mathrm{S}}) = 1_{\mathrm{R}}$ and $u(x) = 0$ for $x \neq 1_{\mathrm{S}}$. (Writing 1 for the identity element of either S or R, the definition can be expressed in 'Kronecker delta' notation: $u(x) = \delta_{x,1}$.)

LEMMA 4. *With u as in Definition* 8, $f * u = u * f = f$ *for all* $f \in \mathrm{A}$.

Proof. Let $x \in \mathrm{S}$. In the formula

$$(f * u)(x) = \sum_{yz = x} f(y)u(z),$$

$u(z)$ is 0 unless $z = 1$. The only possible nonzero term on the right side corresponds to the factorization $x1 = x$, so $(f * u)(x) = f(x)u(1) = f(x)1 = f(x)$. This shows that $f * u = f$; similarly $u * f = f$.

LEMMA 5. *If* S *and* R *are commutative then* $f * g = g * f$ *for all* $f, g \in \mathrm{A}$.

Proof. In the formula

$$(f * g)(x) = \sum_{yz = x} f(y)g(z),$$

interchanging y and z—then $f(z)$ and $g(y)$—yields the formula for $(g * f)(x)$. The interchanges are permissible by the assumed commutativity.

Summarizing Lemmas 1–5:

THEOREM 5. *If* S *is a monoid of finite type and* R *is a ring with unity, then* $\mathrm{A} = \mathrm{A}_{\mathrm{R}}(\mathrm{S})$ *is a ring with unity for the pointwise sum and the convolution product, where the unity element* u *is the function defined by* $u(x) = \delta_{x,1}$. *If, moreover,* S *and* R *are commutative, then* A *is a commutative ring.*

5. The Group of Units in a Convolution Ring

In this section, $\mathrm{A} = \mathrm{A}_{\mathrm{R}}(\mathbb{P})$; that is, the monoid is specialized to $(\mathbb{P}, \cdot, 1)$ but R can still be any ring with unity.

THEOREM 6. *A function* $f \in \mathrm{A}$ *is a unit of* A *if and only if* $f(1)$ *is a unit of* R, *that is,*

$$\mathrm{U}_{\mathrm{A}} = \{f \in \mathrm{A}\colon f(1) \in \mathrm{U}_{\mathrm{R}}\}.$$

Proof. Suppose f is a unit of A, say $f * g = g * f = u$. Since $1 = 1 \cdot 1$ is the only factorization of 1, we have $1 = u(1) = (f * g)(1) = f(1)g(1)$. Similarly $g(1)f(1) = 1$, so $f(1)$ is a unit of R (with inverse $g(1)$).

Conversely, assuming $f \in \mathrm{A}$ with $f(1)$ invertible in R, we must show that f has a convolution inverse. This will be done by constructing functions g and h in A such that $g * f = u$ and $f * h = u$ (then $g = h$ by the associative law for convolution). The functions g and h will be constructed recursively (whence the restriction to the monoid of positive integers).

We seek a function $g \in \mathrm{A}$ satisfying the relation

$$(*) \qquad \sum_{d \mid k} g(d)f(k/d) = u(k)$$

for all $k \in \mathbb{P}$. For $k=1$ this calls for $g(1)f(1)=1$. Define $g(1)=f(1)^{-1}$. Let $n>1$ and assume inductively that $g(k)$ has been defined for all $k<n$ in such a way that $(*)$ holds for $1 \leqslant k < n$. The relation $(*)$ calls for $g(n)$ to satisfy the condition

$$\sum_{d|n,\, d<n} g(d)f(n/d) + g(n)f(1) = 0,$$

where, by the induction hypothesis, all terms of the summation on the left have already been defined. We take this as a cue to *define* $g(n)$ by the formula

$$g(n) = \Big(-\sum_{d|n,\, d<n} g(d)f(n/d)\Big)f(1)^{-1}.$$

This completes the construction of $g \in \mathrm{A}$ such that $g * f = u$.

Similarly, if $h \in \mathrm{A}$ is defined recursively by the formulas $h(1)=f(1)^{-1}$ and

$$h(n) = f(1)^{-1}\Big(-\sum_{d|n,\, d>1} f(d)h(n/d)\Big),$$

then $f * h = u$.

Remark 1. With notations as in the theorem, define $\Phi\colon \mathrm{A} \to \mathrm{R}$ by $\Phi(f)=f(1)$, that is, Φ is 'evaluation at 1.' From $(f * g)(1) = f(1)g(1)$ we see readily that Φ is a ring homomorphism of A onto R. The assertion of the theorem is that $\mathrm{U}_{\mathrm{A}} = \Phi^{-1}(\mathrm{U}_{\mathrm{R}})$. Incidentally, $\mathrm{Ker}\,\Phi = \{f \in \mathrm{A}\colon f(1)=0\}$ and $\mathrm{A}/\mathrm{Ker}\,\Phi \cong \mathrm{R}$. (Remember polynomial rings and the evaluation map $p \mapsto p(0)$?)[2]

Remark 2. When $f(1)=1$ the recursive formula for the convolution inverse f^{-1} of f simplifies to

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

If $n=p^k$ (p prime, k a positive integer), this can be written

$$f^{-1}(p^k) = -\sum_{i=0}^{k-1} f^{-1}(p^i)f(p^{k-i});$$

in particular, $f^{-1}(p) = -f(p)$, $f^{-1}(p^2) = -f(p^2)+f(p)^2$ and $f^{-1}(p^3) = -f(p^3) + f(p)f(p^2) + f(p^2)f(p) - f(p)^3$.

6. The Subgroup of Multiplicative Functions

We now specialize to the case that $\mathrm{A} = \mathrm{A}_{\mathrm{R}}(\mathbb{P})$, where R is a *commutative* ring with unity. The classical terminology in Section 1 is extended to cover R-valued functions:

Definition 9. A function $f\colon \mathbb{P} \to \mathrm{R}$ is said to be *multiplicative* if $f(1)=1$ and $f(mn)=f(m)f(n)$ whenever m and n are relatively prime.

[2] However, the formula of Theorem 6 is false for rings of polynomial functions. The more pertinent ring is the 'ring of formal power series' (G. Hochschild, op. cit., p. 22), for which Theorem 6 *is* true (with the multiplicative monoid $\mathbb{P}$ replaced by the additive monoid $\mathbb{N}$—and $f(1)$ by $f(0)$).

Some easy examples: $f=$ the constant function 1; $f=u$ the unity element of A. The next theorem is a powerful tool for generating and analyzing further examples.

THEOREM 7. *The multiplicative functions $f \in \mathrm{A}$ form a subgroup of the group of units of* A.

Proof. If $f \in \mathrm{A}$ is multiplicative then $f(1)=1$, so $f \in \mathrm{U}_{\mathrm{A}}$ by Theorem 6. Assuming $f, g \in \mathrm{A}$ are multiplicative, we have to show that $f * g$ and f^{-1} are also multiplicative. At any rate,

$$(f*g)(1)=f(1)g(1)=1 \quad \text{and} \quad f^{-1}(1)=f(1)^{-1}=1.$$

Assuming $(m, n)=1$ we must show that

$$(f*g)(mn)=(f*g)(m)(f*g)(n) \qquad 1^\circ$$

$$f^{-1}(mn)=f^{-1}(m)f^{-1}(n). \qquad 2^\circ$$

The proof of 1° is straightforward; notation is 90% of the battle. The proof of 2°, based on 1°, is devious.

Proof of 1°. We note for later use that every divisor of m is relatively prime to every divisor of n. By definition,

$$(*) \qquad (f*g)(mn)=\sum_{yz=mn} f(y)g(z).$$

Also,

$$(f*g)(m)=\sum_{rs=m} f(r)g(s),$$

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

so

$$\begin{aligned}(f*g)(m)(f*g)(n) &= \sum_{rs=m}\sum_{ab=n} f(r)g(s)\cdot f(a)g(b)\\ &= \sum_{rs=m}\sum_{ab=n} f(r)f(a)\cdot g(s)g(b)\end{aligned}$$

(by the commutativity of R). Since r, s are divisors of m, and a, b are divisors of n, we have

$$f(r)f(a)=f(ra) \quad \text{and} \quad g(s)g(b)=g(sb)$$

by the multiplicativity of f and g, therefore

$$(**) \qquad (f*g)(m)(f*g)(n)=\sum_{rs=m,\, ab=n} f(ra)g(sb).$$

The strategy of the proof is to set up a one-to-one correspondence between the terms of $(*)$ and $(**)$ in such a way that corresponding terms are equal. Let

$$\mathrm{V}=\{(y,z)\in\mathbb{P}^2\colon yz=mn\}=\{(y,mn/y)\colon y\,|\,mn\}$$

(a set with $\tau(mn)$ elements) and let

$$\mathrm{W}=\{(r,s,a,b)\in\mathbb{P}^4\colon rs=m \text{ and } ab=n\}$$

$$= \{(r, m/r, a, n/a) : r|m \text{ and } a|n\}$$

(a set with $\tau(m)\tau(n)$ elements). Since $\tau(mn) = \tau(m)\tau(n)$ (Theorem 2), V and W have the same number of elements. The earlier equations can be written

$$(*) \qquad (f*g)(mn) = \sum_{(y,z)\in \mathrm{V}} f(y)g(z),$$

$$(**) \qquad (f*g)(m)(f*g)(n) = \sum_{(r,s,a,b)\in \mathrm{W}} f(ra)g(sb).$$

If $(r,s,a,b)\in \mathrm{W}$ then $ra\cdot sb = rs\cdot ab = mn$, therefore $(ra, sb)\in \mathrm{V}$; thus, the formula

$$\theta(r,s,a,b) = (ra, sb)$$

defines a mapping θ: $\mathrm{W}\to\mathrm{V}$. Moreover, if $w=(r,s,a,b)\in \mathrm{W}$ and $v = \theta(w) = (ra, sb)$, then the term $f(ra)g(sb)$ of $(**)$ corresponding to w is equal to the term of $(*)$ corresponding to $v=\theta(w)$. It remains to show that the mapping θ is bijective, and since $|\mathrm{W}| = |\mathrm{V}|$ we need only show that it is injective.

Suppose $\theta(r,s,a,b) = \theta(r',s',a',b')$, that is, $(ra,sb) = (r'a', s'b')$; then

$$ra = r'a' \quad \text{and} \quad sb = s'b',$$

where r, r', s, s' are divisors of m, and a, a', b, b' are divisors of n (thus every element of the first list is relatively prime to every element of the second). From $r|r'a'$ and $(r,a')=1$ we conclude that $r|r'$; similarly $r'|r$, so $r=r'$ and then $a=a'$ by cancellation. Similarly $s=s'$ and $b=b'$, thus $(r,s,a,b)=(r',s',a',b')$. This completes the proof that $f*g$ is multiplicative.

Proof of 2°. The idea of the proof is to define a (suitable) function $h\in \mathrm{A}$ that is visibly multiplicative and then show (using 1°) that $h = f^{-1}$.

Define $h(1)=1$. If $n>1$ and

$$n = p_1^{k_1}\cdots p_r^{k_r}$$

is its prime-power factorization, define

$$h(n) = f^{-1}(p_1^{k_1})\cdots f^{-1}(p_r^{k_r});$$

h is defined unambiguously because, by the commutativity of R, the expression on the right is invariant under any permutation of the primes $p_1,\dots,p_r$.

We assert that h is multiplicative. Suppose $m>1$, $n>1$ with $(m,n)=1$. The primes $q_1,\dots,q_t$ occurring in m are different from the primes $p_1,\dots,p_r$ occurring in n; thus if

$$m = q_1^{j_1}\cdots q_t^{j_t} \quad \text{and} \quad n = p_1^{k_1}\cdots p_r^{k_r}$$

then

$$mn = q_1^{j_1}\cdots q_t^{j_t}\cdot p_1^{k_1}\cdots p_r^{k_r}$$

is the prime-power factorization of mn. Therefore

$$\begin{aligned} h(mn) &= f^{-1}(q_1^{j_1})\cdots f^{-1}(q_t^{j_t})\cdot f^{-1}(p_1^{k_1})\cdots f^{-1}(p_r^{k_r}) \\ &= h(m)h(n) \end{aligned}$$

by the definition of h.

Since f and h are multiplicative, $f * h$ is multiplicative by the first part of the proof. We assert that $f * h = u$. Indeed, $(f * h)(1) = f(1)h(1) = 1 = u(1)$ and, for p prime and $k \in \mathbb{P}$,

$$\begin{aligned}(f*h)(p^k) &= \sum_{i+j=k} f(p^i)h(p^j) = \sum_{i+j=k} f(p^i)f^{-1}(p^j)\\ &= (f*f^{-1})(p^k) = u(p^k) \qquad (=0),\end{aligned}$$

therefore $(f * h)(n) = u(n)$ for all $n > 1$ by the multiplicativity of $f * h$ and u.

But $f * h = u$ implies $h = f^{-1}$, thus f^{-1} has been identified with a function h known to be multiplicative.

Remarks (optional). A moment's thought about the construction of h in the proof of 2° persuades us that the values of a multiplicative function can be specified arbitrarily on the set of prime-powers p^k. Let's capture this idea in a convenient notation. Let Λ be the set of all prime numbers, $\mathbb{N}$ the set of all nonnegative integers. For every function β: $\Lambda \times \mathbb{N} \to \mathrm{R}$ such that $\beta(p,0) = 1$ for all $p \in \Lambda$, there exists a unique multiplicative function $f_\beta \in \mathrm{A}$ such that $f_\beta(p^k) = \beta(p,k)$ for all p and k.

Write $\mathscr{B}$ for the set of all such functions β, and M_A for the set of all multiplicative functions $f \in \mathrm{A}$; the correspondence $\beta \mapsto f_\beta$ defines a bijection $\mathscr{B} \to \mathrm{M}_\mathrm{A}$. (Since M_A is a subgroup of U_A (Theorem 7), $\mathscr{B}$ acquires a group structure via the bijection ('transport of structure'). Problem: Find a formula for the group law of $\mathscr{B}$.) One can identify $\mathscr{B}$ with the set $\mathscr{F}(\Lambda \times \mathbb{P}, \mathrm{R})$ of all functions $\Lambda \times \mathbb{P} \to \mathrm{R}$ (a set sometimes denoted $\mathrm{R}^{\Lambda \times \mathbb{P}}$). This answers, in a nebulous way, the question of 'how many' multiplicative functions there are.

7. The Möbius Function μ

Let's revert for a moment to the general case $\mathrm{A} = \mathrm{A}_\mathrm{R}(\mathrm{S})$, where $(\mathrm{S}, \cdot, 1)$ is any monoid of finite type and R is any ring with unity. The element $u \in \mathrm{A}$ is the neutral element for the convolution product (Lemma 4 of §4). There is a second 'product' on A that makes it a ring: the pointwise product fg, where $(fg)(x) = f(x)g(x)$ for all $x \in \mathrm{S}$. For the pointwise product, the neutral element is the 'constant function 1':

Definition 10. The function γ: $\mathrm{S} \to \mathrm{R}$ is defined by $\gamma(x) = 1$ for all $x \in \mathrm{S}$.

When $\mathrm{S} = \mathbb{P}$, γ is a unit of A for the convolution product (Theorem 6) and γ is multiplicative in the sense of Definition 9. If, moreover, R is commutative then, although γ is itself a boring function, its convolution inverse is interesting:

THEOREM 8. *If* $\mathrm{A} = \mathrm{A}_\mathrm{R}(\mathbb{P})$, *where* R *is a commutative ring with unity, and if* $\mu = \gamma^{-1}$, *then*

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

Proof. Since $\mu(1) = \gamma(1)^{-1} = 1$, by Remark 2 of §5 we have, for $n > 1$,

$$\mu(n) = -\sum_{d|n,\, d<n} \mu(d)\gamma(n/d) = -\sum_{d|n,\, d<n} \mu(d).$$

In particular, for p prime and $k \in \mathbb{P}$,

$$\mu(p^k) = -\sum_{i=0}^{k-1} \mu(p^i).$$

Thus $\mu(p) = -\mu(1) = -1$ and

$$\begin{aligned}\mu(p^{k+1}) &= -\sum_{i=0}^{k} \mu(p^i) = -\sum_{i=0}^{k-1} \mu(p^i) - \mu(p^k)\\ &= \mu(p^k) - \mu(p^k) = 0.\end{aligned}$$

Summarizing: $\mu(1) = 1$, and if p is a prime then $\mu(p) = -1$ and $\mu(p^k) = 0$ for $k \geqslant 2$. Since μ is multiplicative (Theorem 7) the formula for $\mu(n)$ in the statement of the theorem follows at once from the prime-power factorization of n.

The function μ of Theorem 8 is called the *Möbius function*. Its role in number theory rests on two mappings $\mathrm{A} \to \mathrm{A}$ defined as follows:

Definition 11. For $f \in \mathrm{A} = \mathrm{A}_{\mathrm{R}}(\mathbb{P})$, R a commutative ring with unity, the functions $f', f^\circ \in \mathrm{A}$ are defined by the formulas

$$f'(n) = \sum_{d \mid n} f(d)\mu(n/d), \qquad f^\circ(n) = \sum_{d \mid n} f(d).$$

Thus $f^\circ(n)$ is the sum of $f(d)$ over all divisors d of n. In view of Theorem 8, $f'(n)$ is a 'weighted sum' (weights ± 1) of the $f(d)$ for which n/d is either 1 or a product of distinct primes.

The mappings $f \mapsto f'$ and $f \mapsto f^\circ$ are 'linear' in an appropriate sense. For example, $(f+g)' = f' + g'$ and $(rf)' = rf'$ for $r \in \mathrm{R}$, where, by definition, $(rf)(x) = rf(x)$ for all $x \in \mathrm{S}$. Looking at the formulas in Definition 11, it seems a miracle that these mappings are mutually inverse.

THEOREM 9 (Möbius inversion formulas). *Let* $\mathrm{A} = \mathrm{A}_{\mathrm{R}}(\mathbb{P})$, *where* R *is a commutative ring with unity. For all* $f \in \mathrm{A}$, $f'^\circ = f$ *and* $f^{\circ\prime} = f$.

Proof. From Definition 11 it is clear that $f' = f * \mu$ and $f^\circ = f * \gamma$, so the asserted formulas are immediate from $\mu = \gamma^{-1}$.

8. The Classical Case

Having indulged in some harmless and possibly helpful generality (it made the proofs no harder) we settle down to the classical case that motivated it all: $\mathrm{A} = \mathrm{A}_{\mathbb{Z}}(\mathbb{P})$, the convolution ring of integer-valued functions on the monoid $(\mathbb{P}, \cdot, 1)$ of positive integers under multiplication.

The fact that $(\mathbb{P}, \cdot, 1)$ is a submonoid of $(\mathbb{Z}, \cdot, 1)$ yields an important dividend: The insertion mapping

$$\varepsilon : \mathbb{P} \to \mathbb{Z}, \qquad \varepsilon(n) = n \quad \text{for all } n \in \mathbb{P},$$

is an element of the ring A and is trivially multiplicative. This completes the cast of characters for our discussion:

$$u, \gamma, \varepsilon, \tau, \sigma, \varphi.$$

A common thread of neutrality runs through the first three. Thus u is neutral for the convolution product of A, γ is neutral for the pointwise product, and ε is as neutral as it can be for composition: For every $f \in \mathrm{A}$ the composition $f \circ \varepsilon$ makes sense and $f \circ \varepsilon = f$.

THEOREM 10. *$\tau = \gamma * \gamma$ and $\sigma = \varepsilon * \gamma$.*

Proof. For all positive integers n,

$$(\gamma * \gamma)(n) = \sum_{d \mid n} \gamma(d)\gamma(n/d) = \sum_{d \mid n} 1 = \tau(n)$$

and

$$(\varepsilon * \gamma)(n) = \sum_{d \mid n} \varepsilon(d)\gamma(n/d) = \sum_{d \mid n} d \cdot 1 = \sigma(n).$$

An interesting by-product of the formula $\sigma = \varepsilon * \gamma$ is that ε and γ are multiplicative (obvious), therefore σ is multiplicative (not obvious!) by Theorem 7.

THEOREM 11. *$\varphi * \gamma = \varepsilon$.*

Proof. All functions in sight are multiplicative, so we need only show that $(\varphi * \gamma)(n) = \varepsilon(n)$ for $n = p^k$ (p prime, $k \in \mathbb{P}$). Citing the formula for φ (Theorem 4) at the appropriate step, we have

$$\begin{aligned}(\varphi * \gamma)(p^k) &= \sum_{i=0}^{k} \varphi(p^i)\gamma(p^{k-i}) = \sum_{i=0}^{k} \varphi(p^i) \\ &= \varphi(1) + \sum_{i=1}^{k} (p^i - p^{i-1}) \\ &= 1 + (p^k - 1) = p^k = \varepsilon(p^k).\end{aligned}$$

THEOREM 12. *$\varphi * \tau = \sigma$.*

Proof.[3] Citing Theorems 10 and 11, we have

$$\varphi * \tau = (\varepsilon * \gamma^{-1}) * (\gamma * \gamma) = \varepsilon * \gamma = \sigma.$$

From the formulas $\tau = \gamma * \gamma$, $\sigma = \varepsilon * \gamma$, $\varphi = \varepsilon * \gamma^{-1}$, we see that all of the functions under discussion belong to the subgroup $\langle \gamma, \varepsilon \rangle$ of $\mathrm{U_A}$ generated by γ and ε (where $\mathrm{U_A}$ is the group of units of A). This subgroup is worth dwelling on.

In general, if G is a group and a, b are elements of G such that $ab = ba$, then the mapping $\mathbb{Z}^2 \to \mathrm{G}$ defined by $(m, n) \mapsto a^m b^n$ is a homomorphism of groups. Its range is therefore the subgroup $\langle a, b \rangle$ generated by a and b, thus $\langle a, b \rangle = \{a^m b^n \colon m, n \in \mathbb{Z}\}$.

Let's apply this to a pair of elements f, g of the abelian group $\mathrm{U_A}$. But first we need a distinctive notation for 'convolution powers': Let's write $f^{(n)}$ for the convolution nth power of f ($n \in \mathbb{Z}$), that is,

$$f^{(0)} = u,\ f^{(1)} = f,\ f^{(n+1)} = f^{(n)} * f \text{ for } n \in \mathbb{P},$$

[3] It is striking that a single formula links these functions. Doesn't it remind you of $e^{\pi i} + 1 = 0$?

and $f^{(-n)} = (f^{-1})^{(n)}$ for $n \in \mathbb{P}$. The subgroup of $\mathrm{U_A}$ generated by f and g is

$$\langle f, g\rangle = \{f^{(m)} * g^{(n)} \colon m, n \in \mathbb{Z}\},$$

and the mapping $(m, n) \mapsto f^{(m)} * g^{(n)}$ is a group homomorphism of $\mathbb{Z}^2$ onto $\langle f, g\rangle$. We are going to show that this is an isomorphism when $f = \gamma$ and $g = \varepsilon$.

LEMMA. *If $f \in \mathrm{U_A}$ and $f(1) = 1$ then $f^{(k)}(p) = kf(p)$ for all primes p and all $k \in \mathbb{Z}$.*

Proof. Fix a prime p and consider the mapping $\lambda \colon \mathbb{Z} \to \mathbb{Z}$ defined by $\lambda(k) = f^{(k)}(p)$. In particular, $\lambda(1) = f(p)$. For all integers j and k,

$$\begin{aligned}\lambda(j+k) &= f^{(j+k)}(p) = (f^{(k)} * f^{(j)})(p)\\ &= f^{(k)}(1)f^{(j)}(p) + f^{(k)}(p)f^{(j)}(1)\\ &= 1\cdot\lambda(j) + \lambda(k)\cdot 1 = \lambda(j) + \lambda(k);\end{aligned}$$

this shows that λ is a group homomorphism, so

$$\lambda(k) = k\lambda(1) \quad \text{for all } k \in \mathbb{Z},$$

in other words $f^{(k)}(p) = kf(p)$ for all $k \in \mathbb{Z}$.

THEOREM 13. *The mapping $\mathbb{Z}^2 \to \langle\gamma, \varepsilon\rangle$ defined by $(m, n) \mapsto \gamma^{(m)} * \varepsilon^{(n)}$ is an isomorphism of groups, thus $\langle\gamma, \varepsilon\rangle \cong \mathbb{Z}^2$.*

Proof. It remains only to prove injectivity of the mapping. Assuming $\gamma^{(m)} * \varepsilon^{(n)} = u$, we have to show that $m = n = 0$. For *every* prime p, we have

$$\begin{aligned}0 = u(p) &= (\gamma^{(m)} * \varepsilon^{(n)})(p)\\ &= \gamma^{(m)}(1)\varepsilon^{(n)}(p) + \gamma^{(m)}(p)\varepsilon^{(n)}(1)\\ &= 1\cdot\varepsilon^{(n)}(p) + \gamma^{(m)}(p)\cdot 1\\ &= n\varepsilon(p) + m\gamma(p) \quad \text{(by the lemma)}\\ &= np + m,\end{aligned}$$

whence it is obvious that $m = n = 0$.

In conclusion, here are some prospects for further exploration.

1. The functions γ and ε are, so to speak, 'independent'; they generate a subgroup of $\mathrm{U_A}$ (more precisely, of $\mathrm{M_A}$) of 'rank 2'. That's an open invitation to find an interesting multiplicative function f such that γ, ε, f generate a subgroup of rank 3 (and why stop at 3?).[4]

2. The constant function γ is boring, but its convolution inverse $\mu = \gamma^{-1}$ proved to be interesting. How about the inverses of the other functions? For example, $\tau^{-1} = \mu * \mu$ by Theorem 10. From the formula for μ (Theorem 8) it is easy to derive the formula (for p prime)

$$\tau^{-1}(p^k) = \begin{cases} 0 & \text{if } k \geqslant 3,\\ 1 & \text{if } k = 2,\\ -2 & \text{if } k = 1.\end{cases}$$

[4] A good place to start would be to browse through P. J. McCarthy's *Introduction to Arithmetical Functions* (Springer-Verlag, 1986), where a host of intriguing special functions are discussed.

Since τ^{-1} is multiplicative (Theorem 7), it follows that if $n = p_1^{k_1} \cdots p_r^{k_r}$ is the prime-power factorization of n, then $\tau^{-1}(n) = 0$ if $k_i \geqslant 3$ for some i, otherwise $\tau^{-1}(n) = (-2)^m$, where $m \geqslant 0$ is the number of indices i for which $k_i = 1$.

The formulas for ε^{-1}, φ^{-1} and σ^{-1} are equally accessible (use Remark 2 following Theorem 6).

3. Theorems 10 and 11 invite exploration of convolution formulas for other pairs of functions, in particular convolution squares. One of them is nice—$\varepsilon * \varepsilon = \tau \cdot \varepsilon$ (the pointwise product!)—but $\tau * \tau$, $\varphi * \varphi$ and $\sigma * \sigma$ seem to be messy.

4. From Theorem 13 we know the 'structure' of the subgroup $\langle \gamma, \varepsilon \rangle$ of the group $\mathrm{M_A}$ of multiplicative functions. What is the 'structure' of $\mathrm{M_A}$? The remarks at the end of Section 6 are a start, but not totally satisfying. When that's settled, the groups $\mathrm{U_A}$ and $\mathrm{U_A}/\mathrm{M_A}$ beckon—and what more can we say about the ring A?

5. Abandoned in Section 3 but not forgotten is the monoid $\mathrm{S} = \mathrm{F}_1[t]$ of monic polynomials with coefficients in a field F (§3, Example 2). Its group of units is $\{1\}$. Could the proof of Theorem 6 be adapted to S by inducting on degree? The ring $\mathrm{A_R(S)}$ with $\mathrm{R} = \mathrm{F}[t]$ invites exploration (in particular, S is a submonoid of R).

6. What about monoids S that are not necessarily of finite type? They can be admitted, at the cost of considering only functions $f\colon \mathrm{S} \to \mathrm{R}$ of 'finite support' (i.e., vanishing at all but finitely many points of S) so as to assure the existence of the sums defining convolutions.[5] At first glance, we seem to have lost the functions $\tau, \varphi, \ldots$ that motivated it all; however, thinking of τ as an infinite sequence

$$(\tau(1), \tau(2), \tau(3), \ldots),$$

we surely recapture its essence by considering the totality of all of its 'finite truncates'

$$(\tau(1), \ldots, \tau(n), 0, 0, 0, \ldots).$$

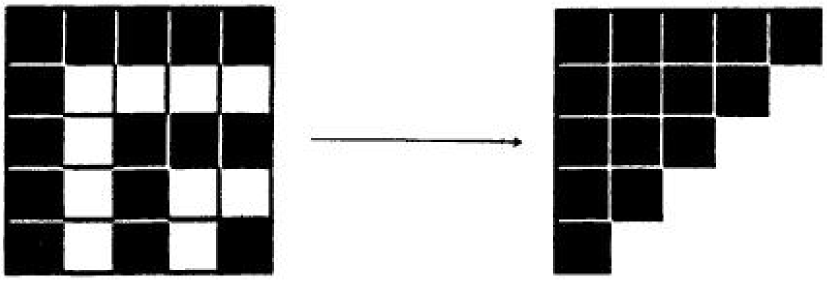
Should we have started with such rings in the first place?

7. An integral domain is a commutative ring with unity having no divisors of zero (if $x \neq 0$ and $y \neq 0$ then $xy \neq 0$). Exercise: If R is an integral domain, then so is the convolution ring $\mathrm{A_R}(\mathbb{P})$.

[5] Such convolution rings are called 'monoidal algebras', generalizing the more familiar 'group algebras.'

Proof without Words: Alternating Sum of Squares = Triangular Number

$$n^2 - (n-1)^2 + \cdots + (-1)^{n-1}(1)^2 = \sum_{k=0}^{n} (-1)^k (n-k)^2 = \frac{(n)(n+1)}{2}$$



—Stephen L. Snover
University of Hartford
W. Hartford, CT 06117