Canad. Math. Bull. Vol. **16** (1), 1973

TOTALLY MULTIPLICATIVE FUNCTIONS IN REGULAR CONVOLUTION RINGS

BY
K. L. YOCOM([1])

1. **Introduction.** McCarthy [4] generalized a necessary and sufficient condition for an arithmetic function to be totally multiplicative to the incidence algebra on a partially ordered set. Several equivalent conditions for an arithmetic function to be totally multiplicative are known [1], [2]. In this paper we generalize several of these (and some apparently new ones) to the regular convolution rings of Narkiewicz [5]. We also investigate the prime factorization of arithmetic functions in a certain subring of some of these regular convolution rings.

2. **Generalized totally multiplicative functions.** The incidence algebra $F(+, *, \circ)$ of a locally finite partially ordered set $S(\leq)$ is the set of all functions f from $S\times S$ into a field with $f(x, y)=0$ if $x \not\leq y$. The operations in $F(+, *, \circ)$ are defined by

$$\begin{aligned}(f+g)(x, y) &= f(x, y)+g(x, y),\\ (f\circ g)(x, y) &= fg(x, y) = f(x, y)g(x, y)\\ (f * g)(x, y) &= \sum (f(x, z)g(z, y): x \leq z \leq y).\end{aligned}$$

McCarthy [4] proved the following:

(I). If $f\in F$ then

(1) $$f(x, z)f(z, y) = f(x, y) \quad \text{for all} \quad x \leq z \leq y$$

if and only if

(2) $$f(g * h) = fg * fh \quad \text{for all} \quad g, h \in F.$$

If $S(\leq)$ is the set of natural numbers N ordered by divisibility we can associate with each arithmetic function f a function $f' \in F$ defined by $f'(x, y)=f(y/x)$ if $x \mid y$ and $f'(x, y)=0$ otherwise. The subset F' of F thus determined forms a subalgebra of F and (I) is seen to be a generalization of

(II). If f is an arithmetic function then

(3) $$f(x)f(y) = f(xy) \quad \text{for all} \quad x, y \in N$$

if and only if

(4) $$f(g * h) = fg * fh \quad \text{for all arithmetic functions } g \text{ and } h.$$

Received by the editors May 5, 1971 and, in revised form, August 18, 1971.
([1]) This work was supported by NSF Science Faculty Fellowship 60210.

https://doi.org/10.4153/CMB-1973-023-2 Published online by Cambridge University Press

Here $*$ denotes Dirichlet convolution defined by

$$(g * h)(n) = \sum (f(d)g(n/d) : d \mid n) \quad \text{for} \quad n \in N.$$

Condition (3) is the usual definition of a totally multiplicative function f. Carlitz [2] observed that (3) is equivalent to

$$f\tau = f * f \tag{5}$$

where $\tau(n)$ is the number of divisors of n. If $\nu(n)=1$ for all $n \in N$ then $\tau = \nu * \nu$ and (5) becomes

$$f(\nu * \nu) = f\nu * f\nu \tag{6}$$

which is (4) with $g=h=\nu$. This suggests a generalized version of (II) with (4) replaced by (6). If we define $\nu \in F$ by $\nu(x, y)=1$ if $x \leq y$ then (I) is no longer valid with (2) replaced by (6) as the following example shows. Let $S(\leq)$ be the lattice shown in Fig. 1 and define $f \in F$ by

$$f(x, y) = \begin{cases} 0 & \text{if} \quad (x, y) = (a, b) \\ -1 & \text{if} \quad (x, y) = (a, x_1) \\ 1 & \text{otherwise.} \end{cases}$$

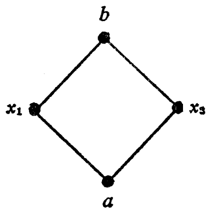

Figure 1.

Then f satisfies (6) but not (1) since $f(a, x_1)f(x_1, b) = -1 \neq f(a, b)$. A generalization is possible to the regular convolution rings of arithmetic functions. These rings are obtained by replacing Dirichlet convolution by another convolution as follows. Let C be a mapping from N to the subsets of N such that $C(n) \subset D(n)$ the set of divisors of n and define the C-convolution $*_C$ of two arithmetic functions f and g by

$$(f *_C g)(n) = \sum (f(d)g(n/d) : d \in C(n)).$$

Let A denote the set of arithmetic functions. Then $A(+, *_C)$ is called a *regular convolution ring* if

(a) $A(+, *_C)$ is a commutative ring,

(b) f and g multiplicative implies $f *_C g$ is multiplicative,

(c) ν has an inverse μ_C under $*_C$ such that $\mu_C(p^\alpha)=0$ or -1 if p is a prime and $\alpha \geq 1$.

https://doi.org/10.4153/CMB-1973-023-2 Published online by Cambridge University Press

Narkiewicz [5] showed that $A(+, *_C)$ is regular if and only if

(i) $d \in C(n)$ implies $n/d \in C(n)$,

(ii) $1, n \in C(n)$ for each $n \in N$,

(iii) $d \in C(m)$ and $m \in C(n)$ if and only if $d \in C(n)$ and $m/d \in C(n/d)$,

(iv) $(m, n)=1$ implies $C(mn)=\{de : d \in C(m), e \in C(n)\}$,

(v) for each prime power $p^\alpha > 1$ there is a divisor $t=t_C(p^\alpha)$ of α such that

$$C(p^\alpha) = \{1, p^t, p^{2t}, \ldots, p^{rt}\}$$

where $rt=\alpha$ and $p^t \in C(p^{2t})$, $p^{2t} \in C(p^{3t})$, $\ldots$.

We shall assume hereafter that $A(+, *_C)$ is a regular ring. The function $\nu *_C \nu$ shall be denoted by τ_C. Note that $\tau_C(n)$ is the cardinality of $C(n)$.

Definition. A function $f \in A$ will be called *C-multiplicative* if for each $n \in N$

$$f(d)f(n/d) = f(n) \quad \text{for all} \quad d \in C(n). \tag{7}$$

Lemma 1. *If $f \in A$ then f is C-multiplicative if and only if for each $n \in N$*

$$f(n) = f(\pi p^\alpha) = \pi f(p^t)^{\alpha/t} \tag{8}$$

where $n=\pi p^\alpha$ is the canonical factorization of n into prime powers and $t=t_C(p^\alpha)$.

Proof. First note that $m=\pi p^\beta \in C(n)$ if and only if each $\beta \le \alpha$ and $t_C(p^\beta)=t_C(p^\alpha)$. This follows from (iv) and (v) above.

Let f be C-multiplicative and proceed by induction on $\tau_C(n)$. $\tau_C(n)=1$ implies $n=1$ and by (7) $f(1)^2=f(1)$ so $f(1)=0$ or 1. But $f(1)=0$ implies $f(n)=f(1)f(n)=0$ so f is identically zero and (8) is satisfied in this case. Thus let $f(1)=1$. $\tau_C(n)=2$ implies $C(n)=\{1, n\}$, $n=p^\alpha$, $t_C(p^\alpha)=\alpha$ and (8) is satisfied. Now suppose (8) holds for all m with $2 \le \tau_C(m) < \tau_C(n)$. Then there is a $d \in C(n)$, $1<d<n$, say $d=\pi p^\beta$. Then by (7) and the induction hypothesis

$$\begin{aligned} f(n) = f(\pi p^\alpha) &= f(\pi p^\beta) f(\pi p^{\alpha-\beta}) \\ &= \pi f(p^t)^{\beta/t} \pi f(p^t)^{(\alpha-\beta)/t} \\ &= \pi f(p^t)^{\alpha/t} \end{aligned}$$

and the induction is complete. Conversely if f satisfies (8) and $d \in C(n)$ with $d=\pi p^\beta$, $n=\pi p^\alpha$ then

$$\begin{aligned} f(n) = \pi f(p^t)^{\alpha/t} &= \pi f(p^t)^{\beta/t} \pi f(p^t)^{(\alpha-\beta)/t} \\ &= f(\pi p^\beta) f(\pi p^{\alpha-\beta}) = f(d) f(n/d). \end{aligned}$$

We now generalize (II).

Theorem 1. *For $f \in A$ the following are equivalent:*

(a) *f is C-multiplicative,*

(b) *$f(g *_C h)=fg *_C fh$ for all $g, h \in A$,*

(c) $f(g *_C g) = fg *_C fg$ *for some C-multiplicative g which is never zero,*
(d) $f\tau_C = f *_C f$,
(e) $f(\nu *_C g) = f *_C fg$ *for some* $g \in A$ *which is strictly positive.*

Proof. We give a cyclic proof for the equivalence of (a) through (d).

(a) implies (b): If f is C-multiplicative then

$$\begin{aligned}(fg *_C fh)(n) &= \sum (f(d)g(d)f(n/d)h(n/d) : d \in C(n)) \\ &= f(n)(g *_C h)(n).\end{aligned}$$

(b) implies (c): Take $g=h$ to be C-multiplicative and never zero.

(c) implies (d): If g is C-multiplicative and never zero and $f(g *_C g) = fg *_C fg$ then $f(g *_C g) = gf(\nu *_C \nu) = gf\tau_C = g(f *_C f)$ and g can be cancelled to yield (d).

(d) implies (a): From (d) we have $f(1) = f(1)^2$ so $f(1)=0$ or 1. First assume $f(1)=0$. Then if $\tau_C(n)=2$, (d) implies $2f(n) = 2f(1)f(n) = 0$ and $f(n)=0$. Suppose inductively that $f(m)=0$ for all m with $2 \leq \tau_C(m) < \tau_C(n)$. Then by (d) and the induction hypothesis

$$\begin{aligned}f(n)\tau_C(n) &= \sum (f(d)f(n/d) : d \in C(n)) \\ &= 2f(1)f(n) + \sum (f(d)f(n/d) : d \in C(n),\ 1 < d < n) = 0.\end{aligned}$$

Thus $f \equiv 0$ and is C-multiplicative. Now assume $f(1)=1$. Then (8) holds for $\tau_C(n)=1$ or 2 and supposing (8) true for all m with $2 \leq \tau_C(m) < \tau_C(n)$, (d) gives

$$f(n)\tau_C(n) = 2f(n) + \sum (f(d)f(n/d) : d \in C(n),\ 1 < d < n)$$

and hence

$$f(n)(\tau_C(n)-2) = (\tau_C(n)-2)\pi f(p^t)^{\alpha/t}$$

and by the lemma, f is C-multiplicative.

Condition (b) with $g=\nu$ and h a positive function gives (e). The proof that (e) implies (a) is similar to the above proof that (d) implies (a) and we omit it. This completes the proof of the theorem.

If for each $n \in N$, $C(n) = D(n)$, the set of all divisors of n then a C-multiplicative function is totally multiplicative while if $C(n) = U(n) = \{d : d \mid n,\ (d, n/d) = 1\}$ for all $n \in N$, then C is unitary convolution and a C-multiplicative function is a multiplicative function, i.e. $(m, n) = 1$ implies $f(mn) = f(m)f(n)$.

The ring $A(+, *_C)$ has a unity ε defined by $\varepsilon(1)=1$ and $\varepsilon(n)=0$ for $n>1$. An element $f \in A(+, *_C)$ is a unit (i.e. has an inverse f^{-1} under $*_C$) if and only if $f(1) \neq 0$ [5]. A number $n \in N$ is called *C-primitive* if $n \neq 1$ and $C(n) = \{1, n\}$. Thus n is C-primitive if and only if $n = p^\alpha$ for $\alpha \geq 1$ and $t_C(p^\alpha) = \alpha$. The value of μ_C, the inverse of ν, at $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ is given by

$$\mu_C(n) = \begin{cases} 1 & \text{if } \quad n = 1, \\ (-1)^r & \text{if each } p_i^{\alpha_i} \text{ is } C \text{ primitive}, \qquad 1 \leq i \leq r, \\ 0 & \text{if some } p_i^{\alpha_i} \text{ is not } C \text{ primitive}, \quad 1 \leq i \leq r. \end{cases}$$

https://doi.org/10.4153/CMB-1973-023-2 Published online by Cambridge University Press

Apostol [1] recently gave several conditions under which a multiplicative function will be totally multiplicative. We now generalize these conditions in the following theorems.

THEOREM 2. (a) *If $f \in A$ is C-multiplicative and $f(1) \neq 0$ then*

$$(fg)^{-1} = fg^{-1} \tag{9}$$

for all $g \in A$ with $g(1) \neq 0$.

(b) *If f is multiplicative and* (9) *holds for $g=\nu$, $g^{-1}=\mu_C$ then f is C-multiplicative.*

Proof. (a) By Theorem 1,

$$fg *_C fg^{-1} = f(g *_C g^{-1}) = f\varepsilon = \varepsilon$$

so that $(fg)^{-1} = fg^{-1}$ as required ($f\varepsilon = \varepsilon$ since $f(1) \neq 0$ implies $f(1)=1$).

(b) Since f is multiplicative it is sufficient by Lemma 1 to show that $f(p^\alpha) = f(p^t)^{\alpha/t}$ where $\alpha \geq 1$, $t = t_C(p^\alpha)$. Letting $\alpha = rt$, the case when $r=1$ is clear. For $r \geq 2$ using the properties of μ_C we have

$$\begin{aligned} 0 = f *_C f^{-1}(p^\alpha) &= f *_C f\mu_C(p^\alpha) \\ &= f(p^{rt}) - f(p^{(r-1)t})f(p^t), \end{aligned}$$

and thus $f(p^{rt}) = f(p^{(r-1)t})f(p^t)$ and inductively $f(p^\alpha) = f(p^t)^{\alpha/t}$

As a corollary to Theorem 2, we have

THEOREM 3. *If f is multiplicative and $f(1) \neq 0$ then f is C-multiplicative if and only if*

$$f^{-1} = f\mu_C. \tag{10}$$

Another characterization is

THEOREM 4. *If f is multiplicative and $f(1) \neq 0$ then f is C-multiplicative if and only if*

$$f^{-1}(p^\alpha) = 0 \tag{11}$$

for all nonprimitives p^α.

Proof. If f is C-multiplicative and $f(1) \neq 0$ then by Theorem 3, $f^{-1}(p^\alpha) = f(p^\alpha)\mu_C(p^\alpha) = 0$ if p^α is not primitive. Conversely let f be multiplicative, $f(1) \neq 0$ and $f^{-1}(p^\alpha) = 0$ if p^α is not primitive. Let $p^\alpha = p^{rt}$ with $t = t_C(p^\alpha)$. Then

$$f *_C f^{-1}(p^t) = f(p^t) + f^{-1}(p^t) = 0$$

and thus

$$f^{-1}(p^t) = -f(p^t). \tag{12}$$

https://doi.org/10.4153/CMB-1973-023-2 Published online by Cambridge University Press

Next for $r \geq 2$

$$f * f^{-1}(p^{rt}) = f(p^{rt}) + f(p^{(r-1)t}) f^{-1}(p^t) = 0$$

with (12) gives

$$f(p^{rt}) = f(p^{(r-1)t}) f(p^t)$$

and thus by induction on r

$$f(p^{rt}) = f(p^t)^r$$

and by Lemma 1, f is C-multiplicative.

The proofs of Theorems 2 and 4 were modeled on Apostol's proofs of the corresponding theorems in [1]. The following theorem corresponds to Apostol's Theorem 8. We have weakened his condition on the function G in (b) and note that his proof of (b) still goes through. The proof we give is then modeled on his proof.

THEOREM 5. (a) *If* $g, G \in A$ *satisfy*

$$g = G *_C \mu_C \tag{13}$$

then

(a) *if* f *is C-multiplicative with* $f(1) \neq 0$ *then*

$$fG *_C f^{-1} = fg, \tag{14}$$

(b) *If* f *is multiplicative*, $f(1) \neq 0$ *and if* (14) *holds for some* G *with* $G(1)=1$ *and for each* $p^\alpha > 1$, $G(p^\alpha) \neq 1$ *then* f *is C-multiplicative.*

Proof. (a) By Theorem 3, $f^{-1} = f\mu_C$ and thus using Theorem 1,

$$fG *_C f^{-1} = fG *_C f\mu_C = f(G *_C \mu_C) = fg.$$

(b) By Theorem 4, it suffices to show that $f^{-1}(p^\alpha)=0$ if p^α is not primitive. For $p^\alpha = p^{2t}$, $t \geq 1$, p^t primitive, (14) gives

$$f^{-1}(p^{2t}) + f(p^t)G(p^t)f^{-1}(p^t) + f(p^{2t})G(p^{2t}) = f(p^{2t})g(p^{2t}).$$

Using (12) and (13) this becomes

$$f^{-1}(p^{2t}) = G(p^t)(f(p^t)^2 - f(p^{2t})).$$

But $f *_C f^{-1}(p^{2t}) = 0 = f(p^{2t}) + f(p)f^{-1}(p) + f^{-1}(p^{2t})$ and (12) imply

$$f(p^t)^2 - f(p^{2t}) = f^{-1}(p^{2t})$$

so that

$$f^{-1}(p^{2t}) = G(p^t) f^{-1}(p^{2t})$$

and since $G(p^t) \neq 1$ we have $f^{-1}(p^{2t}) = 0$. Now let $p^\alpha = p^{rt}$, p^t primitive, $r \geq 3$ and suppose $f^{-1}(p^{jt}) = 0$ for $2 \leq j < r$. Then by (14)

$$f(p^\alpha)g(p^\alpha) = f^{-1}(p^\alpha) + f^{-1}(p^{\alpha-t})G(p^{\alpha-t})f^{-1}(p^t) + f(p^\alpha)G(p^\alpha).$$

https://doi.org/10.4153/CMB-1973-023-2 Published online by Cambridge University Press

Again using (12) and (13) this reduces to

$$f^{-1}(p^\alpha) = G(p^{\alpha-t})(f(p^t)f(p^{\alpha-t})-f(p^\alpha)).$$

The induction hypothesis gives

$$f *_C f^{-1}(p^\alpha) = f(p^\alpha)+f(p^{\alpha-t})f^{-1}(p^t)+f^{-1}(p^\alpha) = 0$$

which with (12) gives $f(p^t)f(p^{\alpha-t})-f(p^\alpha)=f^{-1}(p^\alpha)$ so that

$$f^{-1}(p^\alpha) = G(p^{\alpha-t})f^{-1}(p^\alpha)$$

and since $G(p^{\alpha-t})\neq 1$ we have $f^{-1}(p^\alpha)=0$ and this completes the proof.

3. **A subring of** $A(+, *_C)$. It is easily seen that $A(+, *_C)$ will have proper divisors of zero if $C\neq D$ [5]. The ring $A(+, *_D)$ has no proper zero divisors and is in fact a unique factorization domain [3]. In the ring $F(+, *)$ of incidence functions of a locally finite partially ordered set $S(\leq)$ a subalgebra $G(+, *)$ has been studied [6], [7], [9]. The set G consists of all $f\in F$ with the property that $[x, y]\simeq[u, v]$ implies $f(x, y)=f(u, v)$, i.e. f is constant on each class of order-isomorphic intervals in S. If we take $S=N$ ordered by $m\leq_C n$ if $m\in C(n)$ then there is a natural imbedding of $A(+, *_C)$ in $F(+, *)$. Simply correspond each $f\in A$ to $f'\in F$ defined by $f'(x, y)=f(y/x)$ if $x\in C(y)$ and denote by A' the resulting subring of F. Then let $B'=A'\cap G$ and let $B=\{f\in A:f'\in B'\}$. Then $B(+, *_C)$ is a subring of $A(+, *_C)$ and is described by

$$B = \{f\in A: C(m)\simeq C(n) \text{ implies } f(m) = f(n)\}.$$

In the following we will use the notations

$$A_C = A(+, *_C) \quad\text{and}\quad B_C = B(+, *_C).$$

It is this subring B_C which we wish to investigate. First we note that $C(m)\simeq C(n)$ if and only if $m=n=1$ or when $m, n>1$ are factored into prime powers,

$$m = p_1^{r_1t_1}\cdots p_k^{r_kt_k}, \qquad n = q_1^{r_1't_1'}\cdots q_l^{r_l't_l'}$$

where $p_i^{t_i}$ and $q_j^{t_j'}$ are primitives then $k=l$ and in some arrangement $r_i=r_i'$, $1\leq i\leq k$. This follows from the fact that $C(m)$ is the direct product of the chain $C(p_i^{r_it_i})=\{1, p_i^{t_i}, \ldots, p_i^{r_it_i}\}$, $1\leq i\leq k$. It follows from a theorem of Scheid [7,s Theorem 1] that B_C is an integral domain if

(III). For each prime power $p^\alpha>1$ with $C(p^\alpha)=\{1, p^t, p^{2t}, \ldots, p^{rt}=p^\alpha\}$ there are infinitely many primes q such that for some $\beta\geq 1$, $C(q^\beta)=\{1, q^{t'}, q^{2t'}, \ldots, q^{rt'}=q^\beta\}$, i.e. the chain $C(q^\beta)$ is of the same length as $C(p^\alpha)$.

In the cases $C=U$ and $C=D$ we have $U(m)\simeq U(n)$ if and only if $\omega(m)=\omega(n)$, $D(m)\simeq D(n)$ if and only if $\omega(m)=\omega(n)$ and if $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, $n=q_1^{\beta_1}\cdots q_k^{\beta_k}$ then in some order $\alpha_i=\beta_i$, $1\leq i\leq k$. Here $\omega(n)$ is the number of distinct prime divisors of n. Both B_U and B_D satisfy (III) and thus are integral domains.

https://doi.org/10.4153/CMB-1973-023-2 Published online by Cambridge University Press

THEOREM 6. (a) *The ring B_U contains only one prime π (up to associates) and each nonzero $f \in B_U$ can be written uniquely in the form*

$$f = u *_U \pi^{\omega(N(f))} \tag{15}$$

where u is a unit in B_U and $N(f)$ is given by

$$N(f) = \min\{n : f(n) \neq 0\}. \tag{16}$$

(b) *The ring B_D contains infinitely many nonassociated primes and each nonzero $f \in B_D$ factors into a finite number of primes.*

Proof. (a) First suppose $f \in B_U$ is a unit. Then $N(f)=1$ and if we agree that $\pi^0=\varepsilon$ (15) holds in this case. Now suppose $f \in B_U$ is nonzero and a nonunit. Then since $f(n)$ depends only on $\omega(n)$, $N(f)=2 \cdot 3 \cdots p_k$ where p_k is the k^{th} prime in their natural order. It is easily verified that

$$N(g *_U h) = N(g)N(h) \tag{17}$$

for all nonzero $g, h \in B_U$. Now let $\pi(n)=1$ if n is a prime power $p^\alpha>1$ and $\pi(n)=0$ otherwise. Then $N(\pi)=2$ and π is a prime by (17). Then define $\pi^{k+1}=\pi^k *_U \pi$ for $k=1, 2, \ldots$ and establish inductively that $\pi^k(n)=k!$ if $\omega(n)=k$, $\pi^k(n)=0$ otherwise. Let $f_r = f(n)$ if $\omega(n)=r$, $N(f)=2 \cdot 3 \cdot \cdots \cdot p_k$ so that $\omega(N(f))=k$, and $f_r=0$ for $r<k$. Now solve the equation $f=u *_U \pi^k$ for u_r, $r=0, 1, 2, \ldots$ as follows. Let n satisfy $\omega(n)=k+r$. Then

$$\begin{aligned} f(n) = f_{k+r} = u *_U \pi^k(n) &= \sum (\pi^k(d)u(n/d) : d \in U(n)) \\ &= \sum (k!u(n/d) : d \in U(n),\ \omega(d) = k) \\ &= k!\binom{k+r}{r} u_r = (k+r)!u_r/r! \end{aligned}$$

and hence

$$u_r = r!f_{k+r}/(k+r)!, \qquad r = 0, 1, 2, \ldots,$$

and this uniquely determines u. Notice that we have a "power series" representation for $f \in B_u$

$$f = f_0 + f_1\pi + f_2\pi^2/2! + \cdots + f_k\pi^k/k! + \cdots.$$

(b) For a nonzero $f \in B_D$ we define $N(f)$ by (16) and (17) remains valid with $*_U$ replaced by $*_D$, i.e.

$$N(g *_D h) = N(g)N(h) \tag{18}$$

for all nonzero $g, h \in B_D$. Also f is a unit if and only if $N(f)=1$. Using (18) we can easily prove that f factors into a finite number of primes for if f is not prime then $f=g * h$ where g, h are nonunits and (18) implies $N(g)$, $N(h)$ are less than $N(f)$ so either g is a prime or it factors, and continuing in this way the process terminates in a finite number of steps and produces a prime factorization of f. Since $f \in B_D f(q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}) = f(2^{\alpha_1} 3^{\alpha_2} \cdots p_k^{\alpha_k})$ where p_k is the k^{th} prime in their natural

https://doi.org/10.4153/CMB-1973-023-2 Published online by Cambridge University Press

order. Thus $N(f)$ will be of the form

$$2^{\alpha_1}3^{\alpha_2}\cdots p_k^{\alpha_k}, \qquad \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k \geq 1$$

and f will be prime if $N(f)=2\cdot 3\cdots p_k$. Thus if we define $\pi_k(n)=1$ if n is square free and $\omega(n)=k$, $\pi_k(n)=0$ otherwise, then π_k is a prime in B_D for $k=1,2,\ldots$ and we have exhibited an infinite set of nonassociated primes.

There are several open questions remaining. If B_C is an integral domain, (a) Can a norm N be defined on B_C such that $N(f*_C g)=N(f)N(g)$ for all nonzero $f,g\in B_C$? (b) Does unique factorization hold in B_C (B_D in particular)? (c) Must Scheid's condition (III) hold on C? i.e. is his condition necessary for B_C to be an integral domain?

We give an affirmative answer to (a) in a special case.

THEOREM 7. *Let k be a fixed positive integer and suppose for each prime p, C satisfies*

$$C(p^k) = \{1, p, p^2, \ldots, p^k\},$$
$$C(p^\alpha) = \{1, p^\alpha) \quad \textit{for all} \quad \alpha > k.$$

Then there is a norm $N(f)$ on B_C satisfying

$$N(f *_C g) = N(f)N(g)$$

for all nonzero $f, g\in B_C$.

Proof. For each $n\in N$ define

$$\begin{aligned} r_k(n) &= Nbr\{p : p^k \mid n \text{ and } p^{k+1} \nmid n\}\\ r_{k-1}(n) &= Nbr\{p : p^{k-1} \mid n,\ p^k \nmid n\}\\ &\cdots\\ r_2(n) &= Nbr\{p : p^2 \mid n,\ p^3 \nmid n\}\\ r_1(n) &= Nbr\{p : p \mid n,\ p^2 \nmid n \text{ or } p^\alpha \mid n \text{ for some } \alpha > k\}.\end{aligned}$$

Then for a nonzero $f\in B_C$, define

$$\begin{aligned} r_k^{(f)} &= \min\{r_k(n) : f(n) \neq 0\},\\ r_{k-1}^{(f)} &= \min\{r_{k-1}(n) : r_k(n) = r_k^{(f)}, f(n) \neq 0\},\\ &\cdots\\ r_1^{(f)} &= \min\{r_1(n) : r_i(n) = r_i^{(f)},\ 2 \leq i \leq k, f(n) \neq 0\},\end{aligned}$$

and for $n_f\in N$ satisfying $r_i(n_f)=r_i^{(f)}$ for $1\leq i\leq k$ define

$$N(f) = \tau_C(n_f).$$

Note that $C(m)\simeq C(n)$ if and only if

$$r_i(m) = r_i(n) \quad \text{for} \quad 1 \leq i \leq k.$$

Now let f,g be nonzero elements of B_C, and suppose $n_0\in N$ satisfies $r_i(n_0)=r_i^{(f)}+r_i^{(g)}$ for $1\leq i\leq k$. Suppose $d\in C(n_0)$ and that $f(d)g(n_0/d)\neq 0$. Then $r_k(d)\geq r_k^{(f)}$

https://doi.org/10.4153/CMB-1973-023-2 Published online by Cambridge University Press

and $r_k(n_0/d) \geq r_k^{(g)}$. Since $r_k(n_0)=r_k(d)+r_k(n_0/d)=r_k^{(f)}+r_k^{(g)}$ we must have $r_k(d)=r_k^{(f)}$, $r_k(n_0/d)=r_k^{(g)}$. Continuing in this way we get $r_i(d)=r_i^{(f)}$, $r_i(n_0/d)=r_i^{(g)}$ for $1 \leq i \leq k$ and thus

$$(f *_C g)(n_0) = \sum (f(d)g(n_0/d): d \in C(n_0),\ r_i(d) = r_i^{(f)},\ r_i(n_0/d) = r_i^{(g)},\ 1 \leq j \leq k)$$
$$= f(n_f)g(n_g)\binom{r_k(n_0)}{r_k^{(f)}}\binom{r_{k-1}(n_0)}{r_{k-1}^{(f)}}\cdots\binom{r_1(n_0)}{r_1^{(f)}} \neq 0$$

Also note that $\tau_C(n_0)=\tau_C(n_f)\tau_C(n_g)=N(f)N(g)$ and all that remains is to show that $N(f *_C g)=\tau_C(n_0)$. Let $h=f *_C g$ and suppose $h(n)\neq 0$. Then $r_k(n)\geq r_k^{(f)}+r_k^{(g)}$ and since $h(n_0)=0$ we have $r_k^{(h)}=r_k^{(f)}+r_k^{(g)}=r_k(n_0)$. Continuing we get $r_i^{(h)}=r_i^{(f)}+r_i^{(g)}=r_i(n_0)$ for $1\leq i\leq k$ and thus $N(f)=\tau_C(n_0)$.

With the norm $N(f)$ introduced in the above proof we still have $N(f)=1$ if and only if f is a unit and thus $N(f)$ a prime integer for $f \in B_C$ implies f is a prime. We can then exhibit a few primes in B_C as follows. Let p be a prime $\leq k+1$ and define

$$\pi_p(n) = \begin{cases} 1 & \text{if } \ r_{p-1}(n) = 1, \quad r_i(n) = 0 \ \text{ for } \ 1 \leq i \leq k, \ \ i \neq p-1 \\ 0 & \text{otherwise.} \end{cases}$$

Then π_p is a prime in B_C with $N(\pi_p)=p$.

References

1. T. M. Apostol, *Some properties of completely multiplicative functions*, Amer. Math. Monthly **78** (1971), 266–271.
2. L. Carlitz, *Problem E2268*, Amer. Math. Monthly **77** (1970), p. 1107.
3. E. D. Cashwell, and C. J. Everett, *The ring of number theoretic functions*, Pacific J. Math. **9** (1956), 975–985.
4. P. J. McCarthy, *Arithmetical functions and distributivity*, Canad. Math. Bull. **13** (1970), 491–496.
5. W. Narkiewicz, *On a class of arithmetical convolutions*, Colloq. Math. **10** (1963), 81–94.
6. H. Scheid, *Über ordnungstheoretische functionen*, J. Reine Angew. Math. **238** (1969), 1–13.
7. ———, *Functionen über lokal endlichen halbordnungen*, *I*, Monatsh. Math. **74** (1970), 336–347.
8. ———, *Einige ringe zahlentheoretisher functionen*, J. Reine Angew. Math. **237** (1968), 1–11.
9. David Smith, *Incidence functions as generalized arithmetic functions*, *I*, Duke Math. J. **36** (1967), 617–637.

University of Wyoming,
Laramie, Wyoming