ON SOME ARITHMETIC CONVOLUTIONS

M. V. Subbarao, University of Alberta

0. Introduction. In this paper we first review some of the known arithmetical convolutions with particular reference to a class of convolutions which may be called Lehmer's ψ-products. These products are general enough to include as special cases the well known Dirichlet and unitary products and other Narkiewicz-type products. We indicate a few new cases of ψ-products, and in particular study in some detail a new convolution, called "exponential convolution", which is a variant of Lehmer's ψ-product.

For arbitrary arithmetic functions α, β, this is defined by the equations

$$(\alpha \odot \beta)(1) = \alpha(1)\beta(1),$$

and if $n > 1$ has the canonical form

$$n = p_1^{a_1} \cdots p_r^{a_r},$$

then

$$(\alpha \odot \beta)(n) = \prod_{\substack{b_j c_j = a_j \\ j = 1,\ldots,r}} \alpha(\pi p_j^{b_j})\beta(\pi p_j^{c_j}).$$

This is unlike most known arithmetical convolutions. For example, it is not of the form

$$\sum_{d|n} \alpha(d)\beta(n/d)$$

or of the form

$$\sum_{a \leq n} \alpha(a)\beta(n-a).$$

Yet it is commutative and associative. For $n > 1$, among the divisors over which it is summed, the smallest is not 1, but the core of n, namely the product of the distinct prime factors of n.

We obtain some of the simplest properties associated with this convolution. For example, calling d an exponential divisor of $n = p_1^{a_1}\cdots p_r^{a_r}$ if $d = p_1^{b_1}\cdots p_r^{b_r}$ where $b_j | a_j$, and denoting the number of such divisors by $\tau^{(e)}(n)$, we obtain fairly satisfactory results for the order of $\tau^{(e)}(n)$. For example,

$$\overline{\lim_{n\to\infty}} \log \tau^{(e)}(n) \log\log n/\log n = \tfrac{1}{2}\log 2.$$

Analogous to the Dirichlet divisor problem, we have here the corresponding divisor problem for exponential divisors, namely to find the exact order of the error function for the summatory function

$$T(x) = \sum_{n \le x} \tau^{(e)}(n).$$

We can show that $T(x) = Ax + E(x)$ where $E(x) = O(x^{\frac{1}{2}+\epsilon})$ for every positive ϵ. But the exact order of $E(x)$ is still an open question.

The commutative semigroup of arithmetic functions defined by the exponential convolution $\odot$ has zero divisors. Whether the sub-semigroup formed by the non-zero-divisors has the unique factorization property is another of the unsolved problems associated with this convolution. Some other problems appear in the last section.

1. Definitions and Notations. By an arithmetic function $\alpha(n)$ we mean a complex-valued function defined for all positive integers n (and in some cases for $n = 0$ also). We denote the set of positive integers by Z, the set of arithmetic functions by S, and arbitrary arithmetic functions by α, β, γ. We write $n, m, a, b, c, a_1, \ldots, a_r, b_1, \ldots, b_r, c_1, \ldots, c_r$ to mean always positive integers, while $h_1, h_2, \ldots$ represent non-negative integers. We denote the sequence of all primes by $q_1, q_2, \ldots,$ so that $q_1 = 2, q_2 = 3,$ etc. Also $p_1, p_2, \ldots, p_r$ denote arbitrary primes. If $n > 1$, its canonical form is always assumed to be

$$n = p_1^{a_1}\cdots p_r^{a_r}. \tag{1.1}$$

Note that every $n \geq 1$ has the unique representation

$$n = q_1^{h_1} q_2^{h_2} \cdots, \tag{1.2}$$

where all but a finite number of the h's are zero.

Let (a,b) and $[a,b]$ denote, respectively, the g. c. d. and l. c. m. of a and b.

An arithmetic function α is said to be multiplicative if

$$\alpha(ab) = \alpha(a)\alpha(b)$$

for all a, b such that $(a,b) = 1$. The notion of multiplicativity can be generalized or specialized in many ways.

An illustration of each kind is provided by the following definitions (which we require later on).

An arithmetic function $\alpha(n)$ is said to be

(1.3) semi-multiplicative [29] if for all a and b,

$$\alpha(a)\alpha(b) = \alpha((a,b))\alpha([a,b]);$$

(1.4) exponentially multiplicative if α is multiplicative and, whenever $(a,b) = 1$,

$$\alpha(p^{ab}) = \alpha(p^a)\alpha(p^b)$$

for all primes p.

There are several other classes of arithmetic functions including completely multiplicative, completely unmultiplicative and almost multiplicative (Goldsmith [22, 23]).

2. Some types of convolutions.

Given two arithmetic functions α and β, their sum (also called natural sum) is defined by

$$(\alpha + \beta)(n) = \alpha(n) + \beta(n) \qquad (n \in Z).$$

However, their product may be defined in several ways, thus giving rise to different types of arithmetical convolutions. Among the simplest and most widely known are the following three:

(2.1) Natural product $\alpha\beta$ (also written as $\alpha \times \beta$) defined by

$$(\alpha\beta)(n) = \alpha(n)\beta(n);$$

(2.2) Dirichlet product $\alpha\cdot\beta$ given by

$$(\alpha\cdot\beta)(n) = \sum_{ab=n} \alpha(a)\beta(b);$$

(2.3) Unitary product $\alpha * \beta$ defined by

$$(\alpha * \beta)(n) = \sum_{\substack{ab=n \\ (a,b)=1}} \alpha(a)\beta(b).$$

The theory of arithmetic functions connected with Dirichlet convolutions was first investigated by E. T. Bell [1, 2, 3, 4], and later extensively by R. Vaidyanathaswamy [42, 43], who also introduced the convolution now known as unitary product. This convolution was later extensively studied, among others, by Eckford Cohen [12]. The ring $(S,+,\cdot)$ has the unique factorization property, as was shown by Cashwell and Everett [8], but the ring $(S,+,*)$ is not even an integrity domain.

(2.4) The l. c. m. product $\alpha \oplus \beta$ of α and β is defined by

$$(\alpha \oplus \beta)(n) = \sum_{[a,b]=n} \alpha(a)\beta(b).$$

This convolution was studied in detail by D. H. Lehmer [25]. In view of Von Sterneck's theorem [24, p. 955] that if $\gamma = \alpha \oplus \beta$, then

$$\left(\sum_{a|n} \alpha(a)\right)\left(\sum_{a|n} \beta(a)\right) = \left(\sum_{a|n} \gamma(a)\right), \tag{2.5}$$

the calculation of l. c. m. products is essentially reduced to that of Dirichlet and natural products, since if μ is the Möbius function, we have from (2.5),

$$\gamma = (\alpha\cdot E)(\beta\cdot E)\cdot\mu \tag{2.6}$$

where E is the arithmetical function defined by

$$E(n) = 1 \quad \text{for all } n \in Z. \tag{2.7}$$

(2.8) The Cauchy product of α and β is given by

$$\sum_{\substack{a+b=n \\ a \geq 0}} \alpha(a)\beta(b) \qquad (n \in Z).$$

We here require that $\alpha(n)$ and $\beta(n)$ be defined for $n = 0$ also.

The Cauchy product was studied by several authors including E. T. Bell [1] and Eckford Cohen [10, 11]. The set S with natural sum and Cauchy product is an integrity domain in which there is essentially a single prime α defined by $\alpha(1) = 1$, $\alpha(n) = 0$ $(n \neq 1)$.

(2.9) The Lucas-Carlitz product. Recently, L. Carlitz [6, 7] introduced this product which is analogous to the Cauchy product. Let p be a fixed prime and put

$$n = n_0 + n_1 p + n_2 p^2 + \cdots \quad (0 \leq n_j < p),$$

$$r = r_0 + r_1 p + r_2 p^2 + \cdots \quad (0 \leq r_j < p).$$

Then, a result dating back to Lucas (see [6], p. 583) states that

$$\binom{n}{r} = \binom{n_0}{r_0}\binom{n_1}{r_1}\binom{n_2}{r_2}\cdots \pmod{p}. \tag{2.10}$$

Hence the binomial coefficient $\binom{n}{r}$ is relatively prime to p if and only if

$$0 \leq r_j \leq n_j \qquad (j = 0, 1, 2, \ldots). \tag{2.11}$$

Using this fact, Carlitz defines the new product of α and β by the expression

$$\sum \alpha(a)\beta(n-a),$$

where the sum is restricted to those a that satisfy (2.11). (Here $\alpha(0)$, $\beta(0)$ are assumed to be defined.) Carlitz calls this the Lucas product of α and β. However, since Lucas did not even think of a convolution based on (2.10), it would be more appropriate to call this the the Lucas-Carlitz product. Carlitz has an unproved conjecture regarding the zero divisors of the ring constituted by S, natural addition and Lucas-Carlitz multiplication [6].

(2.12) Narkiewicz's convolution [28]. For each positive n, let A_n be a non-empty set of positive divisors of n. For each $\alpha, \beta \in S$, the product $\alpha \circ \beta$ is defined by Narkiewicz by the relation

$$(\alpha\circ\beta)(n) = \sum_{\substack{ab=n \\ a \in A_n}} \alpha(a)\beta(b).$$

Narkiewicz gives conditions on A_n under which this convolution is commutative and associative and shows that the semigroup $(S,\circ)$ has an identity element if and only if $\{1,n\} \subseteq A_n$ for every $n \in Z$, and then the identity element is the arithmetic function η defined by

$$(2.13) \qquad \eta(n) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}$$

Further, Narkiewicz shows that the units of $(S,\circ)$ are those $\alpha \in S$ for which $\alpha(1) \neq 0$. Also, the convolution $\circ$ preserves multiplicativity (that is, $\alpha\circ\beta$ is multiplicative whenever α and β are) if and only if

$$A_{mn} = A_m \times A_n \qquad (m,n \in Z),$$

where $A_m \times A_n$ represents the set

$$\{ab:\ a \in A_m,\ \ b \in A_n\}.$$

All these properties hold of course in the case of Dirichlet and unitary convolutions.

There are some unsolved problems about this convolution such as in [28, p. 87].

The Narkiewicz product is not general enough to include the convolutions defined by the l. c. m., Cauchy, Lucas-Carlitz or natural products.

(2.14) The k-product (Gioia and Subbarao [19, 38, 39]) of α and β is defined by

$$\sum_{ab=n} \alpha(a)\beta(b)k((a,b))$$

where the function k satisfies the condition for associativity, namely,

(2.15) $$k((a,b))k((ab,c)) = k((a,bc))k((b,c))$$

for all $a, b, c \in Z$. The commutativity of the product is automatic. The k-product convolution appears to be the first generalization in the literature involving a kernel. It extends in an elegant manner many of the nice properties and identities associated with Dirichlet and unitary products. We refer to [19, 38, 39] for details.

The k-product is further generalized by T. M. K. Davison [15] as follows.

(2.16) Davison's product of α and β is given by

$$\sum_{ab=n} \alpha(a)\beta(b)A(a,b)$$

where $A(a,b)$ is a function of the two variables a and b, instead of being a function of their g. c. d. as in (2.14). See also Gesely [18].

(2.17) Remark. It is possible to construct a variety of interesting special cases of the products (2.12), (2.14) and (2.16). As examples which should be worthy of a detailed study, we mention the following.

(2.18) The Semi-unitary product of α and β may be defined by

$$\sum_{\substack{ab=n \\ (a,b)_*=1}} \alpha(a)\beta(b).$$

Here $(a,b)_*$, called the semi-unitary g. c. d. of a to b, is the largest divisor of a which is a unitary divisor of b. (c is called a unitary divisor of b if $c|b$ and $(c,b/c) = 1$.)

(2.19) Bi-unitary product of α and β, denoted by $\alpha{*}{*}\beta$, may be defined by

$$\sum_{\substack{ab=n \\ (a,b)_{**}=1}} \alpha(a)\beta(b),$$

where $(a,b)_{**}$ denotes the largest positive integer which is a unitary divisor of both a and b.

In fact some divisor functions related to these convolutions are already considered respectively by Chidambaraswamy [9] and Suryanarayana [41].

Some interesting convolutions that await detailed study, all special cases of (2.12) and (2.16), are defined by the following products:

(2.20)
$$\sum_{\substack{ab=n \\ \gamma(a)=\gamma(n)}} \alpha(a)\beta(b);$$

(2.21)
$$\sum_{\substack{ab=n \\ \gamma(a)=\gamma(b)}} \alpha(a)\beta(b);$$

(2.22)
$$\sum_{\substack{ab=n \\ (a,b)_k^*=1}} \alpha(a)\beta(b).$$

Here $\gamma(a)$, the core of a, denotes the product of the distinct prime factors of a; and $(a,b)_k^*$ denotes the greatest k-th power divisor of a which is a unitary divisor of b. (See [34].)

We shall not refer to several other convolutions, in the literature, such as those associated with the work of L. Weisner [44], G. C. Rota [32], H. H. Crapo [14], D. A. Smith [35, 36, 37], D. L. Goldsmith [22, 23], as well as E. Cohen's convolution of arithmetic functions of finite abelian groups [13]. It should be pointed out that the bibilography at the end of the paper gives only an illustrative list of some of the work done on convolutions.

3. The Lehmer ψ-product $\alpha \circ \beta$. All the convolutions listed above, with the exception of (2.12) and (2.14), are special cases of the so called ψ-products of D. H. Lehmer developed in [24, 26]. Lehmer's important paper [24] on these products, published in 1932, does not seem to have received adequate attention. For this reason, and also because we later introduce a variant of a Lehmer ψ-product, we shall mention it in some detail.

Let $\psi(x,y)$ be a positive integral-valued function defined for a prescribed set T of ordered pairs (x,y), $x,y \in Z$. The ψ-product $\alpha \circ \beta$ of α and β is defined by

$$(3.1) \qquad (\alpha \circ \beta)(n) = \sum_{\psi(a,b)=n} \alpha(a)\beta(b) \qquad (n \in Z).$$

Lehmer assumes that ψ satisfies the following postulates.

(3.2) Postulate I. For each $n \in Z$, $\psi(a,b) = n$ has a finite number of solutions.

(3.3) Postulate II. $\psi(a,b) = \psi(b,a)$.

(3.4) Postulate III. $\psi(a,\psi(b,c)) = \psi(\psi(a,b),c)$.

These ensure that $\alpha \circ \beta$ is defined by a finite sum and that $\circ$ is commutative and associative.

(3.5) Postulate IV. For any $n \in Z$, $\psi(a,1) = n \Rightarrow a = n$.

This ensures that the semigroup $(S,\circ)$ has the identity element $\eta(n)$ defined in (2.13).

If $\psi(x,y) = n$ has a solution x for some y, then x is called a ψ-divisor of n, and x and y are called conjugate ψ-divisors of n. Let $d(n)$ denote the largest ψ-divisor of n, and

$$\delta_1(n),\ \delta_2(n),\ \ldots,\ \delta_r(n)$$

be the ψ-conjugates of $d(n)$.

Lehmer assumes another postulate, namely,

(3.6) Postulate V. The equation $d(n) = m$ has for each $m > 0$ one and only one solution $m = n$ and $d(1) = 1$.

He then derives a number of theorems such as the following:

(3.7) The semigroup $(S,\bigcirc)$ has the identity η given by (2.13).

(3.8) α is a unit in $(S,\bigcirc)$ if and only if

$$\sum_{k=1}^{r(n)} \alpha(\delta_k(n)) \neq 0 \qquad (n = 1, 2, \ldots).$$

Lehmer then develops a calculus of ψ-convolution introducing notions such as ψ-multiplicative functions. We shall not go into these details.

Among the examples Lehmer gave of his ψ-products is the product of two functions α, β defined by

$$(\alpha \bigcirc \beta)(1) = \alpha(1)\beta(1),$$

and if $n > 1$ is given by (1.1), then

$$(3.9) \qquad (\alpha \bigcirc \beta)(n) = \sum_{\substack{b_i c_i = a_i + 1 \\ i = 1,\ldots,r}} \alpha\Big(\prod_i p_i^{b_i - 1}\Big)\, \beta\Big(\prod_i p_i^{c_i - 1}\Big).$$

(3.10) Remark. By varying Lehmer's Postulates I to V on $\psi(x,y)$, it is possible to construct convolutions which vary from Lehmer's products. In particular, the author has replaced Postulate IV by the following:

$$\psi(n,y) = n \Rightarrow y = \gamma(n)$$

where $\gamma(n)$ denotes the core of n with $\gamma(1) = 1$. We shall not go into the details of the new results obtained, but shall consider in detail a special convolution with this property. We call this "exponential convolution" and study it in the next section.

4. Exponential convolution. For arbitrary α and β, we define their exponential product, denoted by $\alpha \odot \beta$, as follows:

$$(\alpha \odot \beta)(1) = \alpha(1)\beta(1);$$

$$(4.1)\qquad (\alpha \odot \beta)(n) = \sum_{\substack{b_j c_j = a_j \\ j = 1,\ldots,r}} \alpha\Big(\prod p_j^{b_j}\Big)\, \beta\Big(\prod p_j^{c_j}\Big), \qquad n > 1,$$

where $n > 1$ has the representation given in (1.1).

(4.2) Remark. This convolution is clearly commutative and associative. This is not of Narkiewicz type, not being of the form $\sum \alpha(d)\beta(n/d)$. In fact, it is not a Lehmer-type product, because it violates his Postulate IV in (3.5).

(4.3) Exponential divisors. If $n = p_1^{a_1}\cdots p_r^{a_r}$, by an exponential divisor of n, we mean a divisor of the form

$$d = p_1^{b_1}\cdots p_r^{b_r}, \qquad (b_j | a_j,\ \ j = 1,\ \ldots,\ r).$$

We call the divisor $p_1^{a_1/b_1}\cdots p_r^{a_r/b_r}$ the exponential conjugate of d.

We now state some of our results about this convolution.

(4.4) Theorem. (i) The system $(S,\odot)$ is a commutative semigroup with identity element $|\mu|$ (where $|\mu|$ is the arithmetic function defined by $|\mu(n)|$, $\mu(n)$ being the Möbius function).

(ii) The units of $(S,\odot)$ are those α for which $\alpha(n) \neq 0$ whenever n is a product of distinct primes, and $\alpha(1) \neq 0$.

(iii) The semigroup $(S,\odot)$ has an infinity of zero divisors. An element α of $(S,\odot)$ is a non-zero-divisor only if, given any finite number of primes $p_1,\ \ldots,\ p_r$, there exist corresponding positive integers $a_1,\ \ldots,\ a_r$ such that

$$\alpha\Big(p_1^{a_1}\cdots p_r^{a_r}\Big) \neq 0.$$

(iv) $(S,\odot)$ has no non-trivial nilpotent elements.

Proof. Result (i) is easily proved. For if $p_1,\ \ldots,\ p_r$ are distinct primes, and α any arithmetic function,

$$(\alpha \odot \mu)(p_1\cdots p_r) = \alpha(p_1\cdots p_r)\,|\mu(p_1\cdots p_r)|$$

$$= \alpha(p_1\cdots p_r).$$

If $n = p_1^{a_1}\cdots p_r^{a_r}$ and $a_1\cdots a_r > 1$, then

$$(\alpha\cdot|\mu|)(n) = \sum_{\substack{b_i c_i = a_i \\ i = 1,\ldots,r}} \alpha\left(\prod p_i^{b_i}\right) \left|\mu\left(\prod p_i^{c_i}\right)\right|$$

$$= \alpha(n)\,|\mu(p_1\cdots p_r)|,$$

since, recalling the definition of $\mu(n)$, the only non-vanishing term in the sum on the right corresponds to the case $c_1 = \cdots = c_r = 1$.

Thus $|\mu|$ is an identity element of $(S,\odot)$, but there cannot be more than one identity.

To prove (ii), first we note that the condition is necessary. For if we denote the inverse of α by α^{-1} whenever it exists, we have for distinct primes $p_1, \ldots, p_r$,

$$1 = |\mu(p_1\cdots p_r)| = (\alpha \odot \alpha^{-1})(p_1\cdots p_r)$$

$$= \alpha(p_1\cdots p_r)\alpha^{-1}(p_1\cdots p_r),$$

which implies that $\alpha(p_1\cdots p_r) \neq 0$.

On the other hand, suppose that $\alpha(p_1\cdots p_r) \neq 0$ for every finite set of primes $p_1, \ldots, p_r$, and $\alpha(1) \neq 0$. We can construct $\alpha^{-1}(n)$ for all n by induction on n. Thus the relation $\alpha(1)\alpha^{-1}(1) = 1$ gives $\alpha^{-1}(1) = 1/\alpha(1)$. Similarly $\alpha^{-1}(2) = 1/\alpha(2)$.

Take any $n = p_1^{a_1}\cdots p_r^{a_r} > 2$ and assume that $\alpha^{-1}(m)$ is known for all $m < n$. Then from the relation

$$|\mu(n)| = (\alpha \odot \alpha^{-1})(n)$$

$$= \alpha(p_1\cdots p_r)\alpha^{-1}(n) + \sum_{\substack{b_i c_i = a_i \\ b_1\cdots b_r > 1}} \alpha\left(\prod p_i^{b_i}\right) \alpha^{-1}\left(\prod p_i^{c_i}\right),$$

we can solve for $\alpha^{-1}(n)$ uniquely.

The proof of (iii) is as follows. The stated condition for α to be a non-zero-divisor is necessary. For suppose there exist primes $p_1, \ldots, p_r$ $(r > 0)$ such that

$$\alpha\left(p_1^{a_1} \cdots p_r^{a_r}\right) = 0$$

for all positive integers $a_1, \ldots, a_r$. Define the function β as follows:

$$\beta(p_1 \cdots p_r) = 1,$$

$$\beta(n) = 0, \qquad n \neq p_1 \cdots p_r.$$

Then

$$(\alpha \odot \beta)(n) = 0 \quad \text{for all} \quad n \in Z,$$

showing that α is a zero divisor.

Remark. The question whether the above condition is also sufficient for a non-zero-divisor remains open.

To prove (iv), we proceed as follows. Suppose there is an α such that

$$\alpha^{(k)} \equiv \alpha \odot \alpha^{(k-1)} \equiv 0.$$

Then we show that

$$\alpha(n) \equiv 0. \tag{4.8}$$

This clearly holds for $n = 1$, and also whenever n is square-free, since then

$$\alpha^{(k)}(n) = (\alpha(n))^k.$$

We next show that (4.8) holds for N_a of the form

$$N_a = p_1^a p_2 \cdots p_r \qquad (a > 0).$$

We proceed by induction on a, this being true for $a = 1$. Assume that $\alpha(N_a) \neq 0$ and $\alpha\left(p_1^{a_1} p_2 \cdots p_r\right) = 0$ for $a_1 < a$. Then

$$\alpha^{(2)}\left(p_1^{a^2} p_2\cdots p_r\right) = (\alpha\cdot\alpha)\left(p_1^{a^2} p_2\cdots p_r\right)$$
$$= \alpha(N_a)\,\alpha(N_a)$$
$$\neq 0$$

Let b be the smallest positive integer for which

$$\alpha^{(2)}(p_1^b p_2\cdots p_r) \neq 0.$$

Then

$$\alpha^{(3)}\left(p_1^{ab} p_2\cdots p_r\right) = (\alpha \odot \alpha^{(2)})\left(p_1^{ab} p_2\cdots p_r\right)$$
$$= \alpha\left(p_1^{a} p_2\cdots p_r\right)\ \alpha^{(2)}\left(p_1^{b} p_2\cdots p_r\right)$$
$$\neq 0.$$

Continuing this argument, we produce an n such that $\alpha^{(k)}(n) \neq 0$, leading to a contradiction. Hence $\alpha(N_a) = 0$ for $a = 1, 2, \ldots$.

We now continue the induction successively on $a_2, a_3, \ldots$ to show that $\alpha\left(p_1^{a_1} p_2^{a_2} p_3\cdots p_r\right) = 0$, etc, and thus for any integer $n = p_1^{a_1}\cdots p_r^{a_r}$, completing the proof.

(4.9) Exponential analogue of Möbius function. Let us define $\mu^{(e)}(n)$, the exponential analogue of the Möbius function, as follows:

$$\mu^{(e)}(1) = 1$$

and for $n > 1$ given by (1.1),

$$\mu^{(e)}(n) = \mu(a_1)\cdots\mu(a_r).$$

Clearly, $\mu^{(e)}(n)$ is a multiplicative function and also exponentially multiplicative (see (1.4)). We can also verify that if $E(n)$ is the function which equals 1 for all n, then its exponential inverse is $\mu^{(e)}(n)$. It follows that for any α and β,

$$\alpha = \beta \odot E \quad \Leftrightarrow \quad \beta = \alpha \odot \mu^{(e)}.$$

We know that in $(S,\cdot)$ the semi-multiplicative functions form a semigroup [30] and the multiplicative functions a group. We note the following analogous result without proof.

(4.10) In $(S,\odot)$ the set of all unit multiplicative functions form a group.

5. The connection between exponential convolution and Dirichlet convolution. The Dirichlet convolution of arithmetic functions $\alpha(n)$ of a single argument can be extended to functions $\alpha(n_1,\ldots,n_k)$ of k arguments, k being an arbitrary finite number. In fact such an extension was already considered by Vaidyanathaswamy in [43].

If S_k denotes the set of all arithmetic functions $\alpha(n_1,\ldots,n_k)$ of k arguments, we define the Dirichlet product $\alpha\cdot\beta$ by

$$(\alpha\cdot\beta)(n_1,\ldots,n_k) = \sum_{\substack{a_j b_j = n_j \\ j=1,\ldots,k}} \alpha(a_1,\ldots,a_k)\,\beta(b_1,\ldots,b_k).$$

The system $(S_n,\cdot)$ is a commutative semigroup having as the identity the arithmetic function η_k given by

$$\eta_k(n_1,\ldots,n_k) = \begin{cases} 1, & n_1 = \cdots = n_k = 1; \\ 0, & \text{otherwise.} \end{cases}$$

The units of $(S_n,\cdot)$ are those functions α for which $\alpha(1,\ldots,1) \neq 0$. It can be shown that the system $(S_n,+,\cdot)$ is a commutative ring, and in fact a domain of integrity. Following the method of Cashwell and Everett [8], one can study the unique factorization property for $(S_n,+,\odot)$.

The Möbius function for $(S_n,\cdot)$ is the function $\mu(n_1,\ldots,n_k)$ defined by

$$\mu(n_1,\ldots,n_k) = \mu(n_1)\cdots\mu(n_k).$$

(See [43, sec. 4].

We wish to point out that some of these results can be extended to the set $\overline{S}$ of complex-valued arithmetic functions $\overline{\alpha} = \overline{\alpha}(\overline{h})$ whose arguments $\overline{h}$ are vectors of the form

$$\overline{h} = (h_1, h_2, \ldots),$$

where $h_1, h_2, \ldots$ are non-negative integers all but a finite number of which are zero. We denote the set of all such vectors by $\overline{Z}$.

Let

$$\overline{s} = (s_1, s_2, \ldots), \tag{5.1}$$

$$\overline{t} = (t_1, t_2, \ldots) \tag{5.2}$$

be two such vectors. We then define that $\overline{s}$ and $\overline{t}$ are of the "same type" if and only if

$$s_j = 0 \Leftrightarrow t_j = 0 \qquad (j = 1, 2, \ldots).$$

If $\overline{s}$ and $\overline{t}$ are of the same type and are given by (5.1) and (5.2), we define the vector $\overline{s}\overline{t}$ as follows:

$$\overline{s}\overline{t} = (s_1 t_1, s_2 t_2, \ldots). \tag{5.3}$$

It should be noted that the vector $\overline{s}\overline{t}$ is not defined unless $\overline{s}$ and $\overline{t}$ are of the same type.

Let $\overline{\alpha}, \overline{\beta}, \in \overline{S}$. We define their Dirichlet product, denoted by $\overline{\alpha}\cdot\overline{\beta}$, by the relation

$$(\overline{\alpha}\cdot\overline{\beta})(\overline{h}) = \sum_{\overline{s}\overline{t}=\overline{h}} \overline{\alpha}(\overline{s})\overline{\beta}(\overline{t}) \qquad (\overline{h} \in Z_o).$$

We recall the definition $\eta(n)$ given in (2.13) and extend it by defining $\eta(0) = 1$. For $\overline{h} = (h_1, \ldots)$, we define the function $\overline{\eta}$ by

$$\overline{\eta}(\overline{h}) = \eta(h_1)\eta(h_2)\cdots . \tag{5.4}$$

Finally, we write $|\overline{h}|$ for $\max_j h_j$, whenever it exists. We now have the following result.

We can now define $\overline{\eta}$ alternately as

$$\overline{\eta}(\overline{h}) = \begin{cases} 1, & |\overline{h}| \le 1, \\ 0, & |\overline{h}| > 1. \end{cases} \tag{5.5}$$

(5.6) <u>Theorem</u>. $(\overline{S},\cdot)$ is a commutative semigroup for which

(i) the identity element is $\overline{\eta}$;

(ii) the units are those $\overline{\alpha}$ for which

$$\overline{\alpha}(\overline{h}) \ne 0 \quad \text{for} \quad |\overline{h}| \le 1;$$

(iii) if $\overline{E} \in \overline{S}$ is defined by $\overline{E}(\overline{h}) = \overline{1}$ for all $\overline{h} \in \overline{Z}$, and if $\overline{\mu}$ is the inverse of $\overline{E}$ (so that $\overline{\mu}(\overline{h})$ is the Möbius function of $(\overline{S},\cdot)$), $\overline{\mu}$ is given by

$$\overline{\mu}(\overline{h}) = \mu(h_1)\mu(h_2)\cdots, \qquad \overline{h} = (h_1,h_2,\ldots), \tag{5.7}$$

with the convention that $\mu(0) = 0$.

The proof is similar to that for the semigroup $(S,\cdot)$, and is omitted.

We next recall that any $n \in Z$ has the representation given in (1.2), so that the mapping

$$n \longleftrightarrow \overline{h} = (h_1,h_2,\ldots)$$

is one-to-one on Z onto $\overline{Z}$. Further, to each $\alpha \in S$, there corresponds in a one-to-one manner the element $\overline{\alpha}$ in $\overline{S}$ given by

$$\alpha(n) \longleftrightarrow \overline{\alpha}(\overline{h}), \qquad n = q_1^{h_1}q_2^{h_2}\cdots, \quad \overline{h} = (h_1,h_2,\ldots). \tag{5.8}$$

Further, this correspondence preserves the semigroup operation, that is, if

$$\alpha \longleftrightarrow \overline{\alpha}, \quad \beta \longleftrightarrow \overline{\beta},$$

then

$$\alpha \odot \beta \longleftrightarrow \overline{\alpha}\cdot\overline{\beta}.$$

Thus we have proved the following result.

(5.9) <u>Theorem</u>. The semigroups $(S,\odot)$ and $(\bar{S},\cdot)$ are isomorphic to each other.

(5.10) <u>Remark</u>. From the mapping given in (5.8), we could at once deduce the results (i), (ii) of Theorem (4.4) and the results in (4.9) from Theorem (5.6).

6. <u>The order and average order of $\tau^{(e)}(n)$</u>. We have already defined $\tau^{(e)}(n)$ to be the number of exponential divisors of n, $\tau^{(e)}(1) = 1$.

If $n > 1$ has the representation (1.1), we have

$$\tau^{(e)}(n) = \tau(a_1)\tau(a_2)\cdots\tau(a_r), \tag{6.1}$$

$\tau(a)$ denoting the number of divisors of n. We now prove:

(6.2) <u>Theorem</u> (Erdös).

$$\overline{\lim_{n\to\infty}} \frac{\log \tau^{(e)}(n) \log\log n}{\log n} = \tfrac{1}{2}\log 2.$$

<u>Proof</u>. We first prove that for any given $\epsilon > 0$, there are infinitely many positive integers m for which

$$\tau^{(e)}(m) > 2^{(1-\epsilon)\log m/2\log\log m}.$$

Let $m = q_1^2 q_2^2 \cdots q_k^2$, where $q_1, \ldots, q_k$ are the first k primes. Then by the prime number theorem, $\frac{1}{2}\log m \sim y$ where $y = q_k$, and $k = \pi(q_k) = \pi(y) \sim y/\log y$, where $\pi(x)$ = number of primes $\le x$. Hence

$$\begin{aligned}\log \tau^{(e)}(m) &= k\log 2\\ &\sim (\log 2)y/\log y\\ &\sim (\log 2)\tfrac{1}{2}\log m/\log\log m,\end{aligned}$$

from which we get the inequality stated above.

To complete the proof of the theorem, it remains only to show that given any $\epsilon > 0$,

$$\tau^{(e)}(n) < 2^{(1+\epsilon)\log n/2\log\log n} \qquad (n > n_0(\epsilon)).$$

Put

$$F(n) = \max_{1 \le m \le n} \tau^{(e)}(m)$$

and assume that t is the smallest integer for which $\tau^{(e)}(t) = F(n)$.

Put $t = t_1 t_2$ where all the prime factors of t_1 are less than $\log n/(\log\log n)^2$ and all prime factors of t_2 are $\ge \log n/(\log\log n)^2$. We have

$$\tau^{(e)}(t_1) < \left(\frac{\log n}{\log 2}\right)^{\log n/(\log\log n)^3} < 2^{\epsilon \log n/2 \log\log n}$$

for all $n \ge n_o(\epsilon)$, because t_1 has fewer than $(1+\epsilon)\log n/(\log\log n)^3$ prime factors and the exponent of each prime factor in the canonical form of t_1 is $< \log n/\log 2$.

Let us now look at t_2. Put $t_2 = p_1^{b_1} \cdots p_r^{b_r}$, where $p_1, \ldots, p_r$ are consecutive primes $\ge \log n/(\log\log n)^2$. We have

$$b_1 + \cdots + b_r \le (1 + o(1)) \log n/\log\log n$$

since $n \ge t_2 \ge p_1^{b_1+\cdots+b_r}$, or $b_1 + \cdots + b_r \le \log n/\log p_1$. We can assume that all the b_j's are > 1 and are even, since if b is odd, there is an even $c < b$ with $\tau(c) \ge \tau(b)$ (recall the minimal nature of t) and if $b = 1$, it makes no contribution to $\tau(n)$.

Now, if we have even numbers whose sum is given, their product is maximal if all are 2, as can be easily proved, for instance, by induction. Thus

$$\tau^{(e)}(t_2) = \prod_{j=1}^{r} \tau(b_j) \le \prod_{j=1}^{r} b_j$$

$$\le 2^{(1 + o(1))\log n/2 \log\log n},$$

which is what we set out to establish. Theorem (6.2) is thus proved.

<u>Remark</u>. The result of the theorem may be compared with the well known result:

$$\overline{\lim_{n\to\infty}} \frac{\log \tau(n) \log\log n}{\log n} = \log 2 .$$

(6.3) <u>Theorem</u>. Let

$$T(x) = \sum_{n \le x} \tau^{(e)}(n) .$$

Then

$$T(x) = Ax + O(x^{\frac{1}{2}} \log x)$$

where

$$A = \prod_p \left\{1 + (1-p^{-1}) \sum_{k=2}^{\infty} (p^k-1)^{-1}\right\}.$$

<u>Proof</u>. Let

$$f(s) = \sum_{n=1}^{\infty} \frac{\tau^{(e)}(n)}{n^s} .$$

This is regular for $\sigma = \mathrm{Re}(s) > 1$. Since $\tau^{(e)}(n)$ is multiplicative, on using (6.1),

$$f(s) = \prod_p \left\{1 + \tau(1)p^{-s} + \tau(2)p^{-2s} + \cdots \tau(a)p^{-as} + \cdots\right\}$$

$$= \prod_p \left\{1 + \frac{p^{-s}}{1-p^{-s}} + \frac{p^{-2s}}{1-p^{-2s}} + \cdots\right\}$$

$$= \prod_p (1-p^{-s})^{-1}\varphi(s)$$

$$= \zeta(s)\varphi(s)$$

where $\zeta(s)$ is the Riemann zeta function and

$$\varphi(s) = \prod_p \left\{1 + (1-p^{-s}) \sum_{k=2}^{\infty} (p^{ks}-1)^{-1}\right\}.$$

Clearly, $\varphi(s)$ is regular for $\sigma > \frac{1}{2}$. An application of Ikehara's theorem now gives

(6.5) $$\lim_{x\to\infty} \left(\frac{T(x)}{x}\right) = \varphi(1) = A.$$

The usual contour integration method, applied to (6.4), gives the order estimate of the error term of the theorem after considerable laborious calculations. The details will be given elsewhere.

(6.6) Remark. We can extend (6.5) as follows:

Let

$$T^{(k)}(x) = \sum_{n \le x} [\tau^{(e)}(n)]^k.$$

Then

$$\lim_{x\to\infty} \left(\frac{T^{(k)}(x)}{x}\right) \text{ exists for every } k \text{ and } = A_k,$$

where

$$A_k = \prod_p \left\{1 + \sum_{n=2}^{\infty} \left[(\tau(n))^k - (\tau(n-1))^k\right] p^{-n} \right\}.$$

Another result of interest is as follows. Let an integer n be said to be exponentially square-free if in its canonical form each exponent is square-free, with the convention that 1 is taken to be exponentially square-free. Let $Q^{(e)}(x)$ denote the number of exponentially square-free integers $\le x$. Then we have

(6.7) Theorem. $$Q^{(e)}(x) = Bx + O(x^{\frac{1}{2}})$$

where

$$B = \prod_p \left(1 - \sum p^{-as} + \sum p^{-bs}\right),$$

where a ranges over all non-square-free numbers for which $a-1$ is square-free, and b ranges over all square-free numbers for which $b-1$ is non-square-free.

Proof. We proceed as in the proof of (6.3) and use a result of H. Delange [16], namely, if $\alpha(n)$ is a multiplicative arithmetic function with $\alpha(n) = 0$ or 1, and for primes p, $\alpha(p) = 1$, then

$$\sum_{n \le x} \alpha(n) = Cx + o(x^{\frac{1}{2}}),$$

c being a constant.

7. Exponentially perfect numbers. Many of the usual problems associated with Dirichlet convolution have their counterparts in exponential (or, in fact, any other) convolution. As an example, we mention the question of determination of all exponentially perfect numbers, which by definition are positive integers n for which

$$\sigma^{(e)}(n) = 2n,$$

where $\sigma^{(e)}(n)$ denotes the sum of the exponential divisors of n. An example of such a number is 36. It is easy to see that there exist an infinity of them; for if m is exponentially perfect, so is mk (called the associate of m) where k is any square-free integer relatively prime to m.

Some examples of exponentially perfect numbers are:

$$2^2.3^3.5^2; \quad 2^3.3^2.5^2; \quad 2^4.3^2.11^2;$$
$$2^6.3^2.7^2.13^2; \quad 2^7.3^2.5^2.7^2.13^2;$$
$$2^8.3^2.5^2.7^2.139^2.$$

We raise the following questions.

(7.1) Is there an odd exponentially perfect number?

(7.2) Are there an infinity of exponentially perfect numbers such that no two of them are associates of each other?

We obtained some necessary conditions for an odd integer to be exponentially perfect, which will be published elsewhere.

8. Remark. We finally remark that to every given convolution of arithmetic functions, one can define the corresponding exponential convolution and study the properties of arithmetical functions which arise therefrom. For example, one can study the exponential unitary

convolution,and in fact, the exponential analogue of any Narkiewicz-type convolution, among others.

9. Acknowledgement. The author is thankful to Professor P. Erdös for sending his proof of Theorem (6.2) and to Dr. Suryanarayana for his help in the preparation of the list of references.

REFERENCES

1. E. T. Bell, On Liouville's theorems concerning certain numerical functions, Bull. Amer. Math. Soc. 19 (1912), 164-166.

2. E. T. Bell, Euler Algebra, Trans. Amer. Math. Soc. 25 (1923), 135-154.

3. E. T. Bell, Outline of a theory of arithmetical functions in their algebraic aspects, J. Indian Math. Soc. 17 (1928), 249-260.

4. E. T. Bell, Factorability of numerical functions, Bull. Amer. Math. Soc. 37 (1931), 251-253.

5. L. Carlitz, Rings of arithmetic functions, Pacific J. Math. 14 (1964), 1165-1171.

6. L. Carlitz, Arithmetic functions in an unusual setting, Amer. Math.Monthly 73 (1966), 582-590.

7. L. Carlitz, Arithmetical functions in an unusual setting II, Duke Math. J. 34 (1967), 757-759.

8. E. D. Cashwell and C. J. Everett, The ring of number-theoretic functions, Pacific J. Math. 9 (1959), 975-985.

9. J. Chidambaraswamy, Sum functions of unitary and semi-unitary divisors, J. Indian Math. Soc. 31 (1967), 117-126.

10. E. Cohen, Rings of arithmetic functions, Duke Math. J. 19 (1952), 115-129.

11. E. Cohen, Rings of arithmetic functions II: The number of solutions of quadratic congruences, Duke Math. J. 21 (1954), 9-28.

12. E. Cohen, Unitary products of arithmetical functions, Acta Arith. 7 (1961), 29-38.

13. E. Cohen, Arithmetical functions of finite Abelian groups, Math. Ann. 142 (1961), 165-182.

14. H. H. Crapo, The Möbius function of a lattice, J. Combinatorial Theory 1 (1966), 126-131.

15. T. M. K. Davison, On arithmetic convolutions, Canad. Math. Bull. 9 (1966), 287-296.

16. H. Delange, Sur certaines functions additives á valeur entiers, Acta Arith. 16 (1969/70), 195-206.

17. P. Erdös, (Private communication to the author).

18. G. Gesely, A generalized arithmetic composition, Amer. Math. Monthly 74 (1967), 1216-1217.

19. A. A. Gioia, The k-product of arithmetic functions, Canad. J. Math. 17 (1965), 970-976.

20. A. A. Gioia, On an identity for multiplicative functions, Amer. Math. Monthly 69 (1962), 988-991.

21. A. A. Gioia, Generalized Dirichlet products of number theoretic functions. Ph.D. Thesis, University of Missouri, 1964.

22. D. L. Goldsmith, On the multiplicative properties of arithmetic functions, Pacific J. Math. 27 (1968), 283-304.

23. D. L. Goldsmith, A generalized convolution for arithmetic functions, Duke Math. J. 38 (1971), 279-283.

24. D. H. Lehmer, Arithmetic of double series, Trans. Amer. Math. Soc. 33 (1931), 945-457.

25. D. H. Lehmer, A new calculus of numerical functions, Amer. J. Math. 53 (1931), 843-854.

26. D. H. Lehmer, Polynomials for the n-ary composition of numerical functions, Amer. J. Math. 58 (1936), 563-572.

27. P. J. McCarthy, Regular arithmetical convolutions, Portugal. Math. 10 (1963), 81-94.

28. W. Narkiewicz, On a class of arithmetical convolutions, Colloq. Math. 10 (1963), 81-94.

29. J. Popken, On convolutions in number theory, Indag. Math. 17 (1955), 10-15.

30. D. Rearick, Semi multiplicative functions, Duke Math. J. 33 (1966), 49-54.

31. D. Rearick, Operations on algebras of arithmetic functions, Duke Math. J. 35 (1968), 761-766.

32. G. C. Rota, On the foundations of combinatorial theory I. Theory of Möbius functions, Z. Wahrscheinlichkeitstheorie und Verw. 2 (1964), 340-368.

33. R. Siva Ramakrishna, Contributions to the study of multiplicative arithmetic functions, (to appear).

34. V. Sivaramprasad and D. Suryanarayana, Sum functions of k-ary and semi-k-ary divisors, J. Austral. Math. Soc. (to appear).

35. D. A. Smith, Incidence functions as generalized arithmetic functions I, Duke Math. J. 34 (1967), 617-633.

36. D. A. Smith, Incidence functions as generalized arithmetic functions II, Duke Math. J. 36 (1969), 15-30.

37. D. A. Smith, Incidence functions as generalized arithmetic functions III, Duke Math. J. 36 (1969), 353-367.

38. M. V. Subbarao and A. A. Gioia, Generalized Dirichlet products of arithmetical functions (abstract), Notices Amer. Math. Soc. 10 (1963), No. 7, p. 661.

39. M. V. Subbarao and A. A. Gioia, Identities for multiplicative functions, Canad. Math. Bull. 10 (1967), 65-73.

40. M. Sugunamma, Contributions to the study of general arithmetic functions, Ph.D. Thesis, Sri Venkateswara University, Tirupati, India, 1965.

41. D. Suryanarayana, The number of bi-unitary divisors of an integer, Proceedings of a Conference on the Theory of Arithmetic Functions, Kalamazoo, 1971.

42. R. Vaidyanathaswamy, The identical equations of the multiplicative function, Bull. Amer. Math. Soc. 36 (1930), 762-772.

43. R. Vaidyanathaswamy, The theory of multiplicative arithmetical functions, Trans. Amer. Math. Soc. 33 (1931), 579-662.

44. L. Weisner, Abstract theory of inversion of finite series, Trans. Amer. Math. Soc. 38 (1935), 474-484.