Canad. Math. Bull. Vol. **20** (3), 1977

ON AN ARITHMETIC CONVOLUTION

BY
J. HANUMANTHACHARI

1. **Introduction and notation.** In this paper the congruence $(f\circ g)(n)\equiv 0 \pmod n$ and the functional equation $f\circ f\circ\cdots\circ f=g$, are studied, where $\circ$ is an exponential regular convolution. For definitions, see below.

We recall that an arithmetic convolution C is a map from the set N of positive integers into the power set $\mathscr{P}(N)$ such that for each $n\in N$, $C(n)$ is a set of divisors of n. Following Narkiewicz [1], we say that C is regular if and only if

(i) the statements "$d\in C(m)$ and $m\in C(n)$" and "$d\in C(n)$, and $(m/d)\in C(n/d)$" are equivalent;

(ii) $d\in C(n)$ implies $(n/d)\in C(n)$

(iii) $1, n\in C(n)$ for all $n\in N$;

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

(v) for every prime power $p^a>1$, the set $C(p^a)$ is of the form $\{1, p^t, p^{2t},\ldots, p^{rt}=p^a\}$, with some $t\neq 0$, and more over $p^t\in C(p^{2t})$, $p^{2t}\in C(p^{3t}),\ldots$

We note that the Dirichlet convolution D, where $D(n)$ is the set of all positive divisors of n, and the unitary convolution U, where $U(n)$ is the set of all positive divisors d of n such that $(d, n/d)=1$, are regular.

Let $\mathscr{A}$ be the set of all arithmetic functions. We now introduce

DEFINITION 1.1. For f, $g\in A$, the exponential regular C-convolution of f and g, denoted by $f\circ g$, is defined by

$$(f\circ g)(1)=f(1)g(1)$$

and if $n>1$ has the canonical form

$$n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r} \tag{1.1}$$

then,

$$(f\circ g)(n)=\sum f\left(\prod_{i=1}^r p_i^{b_i}\right)g\left(\prod_{i=1}^r p_i^{c_i}\right),$$

where the summation is over $b_i\in C(a_i)$ such that $b_ic_i=a_i$, $i=1,2,\ldots,r$.

It is obvious that $\langle\mathscr{A},\circ\rangle$ is a commutative semi-group with $|\mu|$, as the identity, where μ is the Möbius function. We also recall that an arithmetic function f is said to be multiplicative if $f(mn)=f(m)f(n)$, for all m, n such that $(m,n)=1$ and further it is said to be exponentially multiplicative if in addition whenever

Received by the editors, in revised form, May 12, 1976

https://doi.org/10.4153/CMB-1977-046-9 Published online by Cambridge University Press

$(a, b)=1$, $f(p^{ab})=f(p^a)f(p^b)$ for all primes p [4]. We also note the following (for proofs, see [4]).

LEMMA 1.1 *The units of $\langle \mathcal{A}, \circ\rangle$ are those f for which $f(1)\neq 0$ and $f(n)\neq 0$ whenever n is a product of distinct primes.*

LEMMA 1.2. *If $f, g \in \mathcal{A}$ are exponentially multiplicative, then $f\circ g$ is also exponentially multiplicative.*

LEMMA 1.3. *If $f\in\langle \mathcal{A}, \circ\rangle$ is exponentially multiplicative and f^{-1} exists, then f^{-1} is also exponentially multiplicative.*

2. **A congruence for a class of arithmetic functions.** In this section we obtain a necessary and sufficient condition under which the congruence

$$(f\circ g)(n)\equiv 0 \pmod n \tag{2.1}$$

holds for all positive integers n, where f and g are integral valued arithmetic functions and f is a unit exponentially mulitplicative function in $\langle \mathcal{A}, \circ\rangle$. Our result is akin to Subbarao's result [Theorem 1,2]. We write $F(n)$ for the left member of (2.1).

If f and g are multiplicative, then so is F. In this case (2.1) holds for all n if and only if $F(p^a)\equiv 0 \pmod{p^a}$ for all primes p and all integers $a>0$. Further if f and g are exponentially multiplicative, then from Lemma 1.2, F is exponentially multiplicative. In this case the congruence (2.1) cannot hold for all n. For, suppose $F(n)\neq 0$ for some n given by (1.1), then $F(p_1p_2\cdots p_r)=1$ and hence $F(p_1p_2\cdots p_r)\not\equiv 0 \pmod{p_1p_2\cdots p_r}$. However we have the following.

THEOREM 2.1. *If f and g are integral valued arithmetic functions and f is a unit exponentially multiplicative function in $\langle \mathcal{A}, \circ\rangle$ then (2.1) holds for all positive integers n if and only if*

$$\sum f(p^b)g(p^c m)\equiv 0 \pmod{p^a} \qquad (b\in C(a), bc=a) \tag{2.2}$$

for all primes p and all positive integers a and m with $(p, m)=1$.

Proof. (2.1) holds when $n=1$ trivially. We can assume that $n>1$. Write $n=p^a m$, where p is a prime such that $(p, m)=1$. Taking $m=\prod_{j=1}^{s} q_j^{\alpha_j}$, and using the exponential multiplicativity of f, we may write

$$F(n)=\sum_1 f\Big(\prod q_j^{\beta_j}\Big)\sum_2 f(p^b)g\Big(p^c\prod q_j^{\gamma_j}\Big),$$

where $\sum_1$ is the summation over all $\beta_j\in C(\alpha_j)$ satisfying that $\beta_j\gamma_j=\alpha_j$ $j=1,2,\ldots,s$, and $\sum_2$ is the summation over all $b\in C(a)$ such that $bc=a$. If (2.2) holds for all prime divisors of n, then

$$F(n)\equiv 0 \pmod n$$

We now prove that condition (2.2) is also necessary for (2.1) to hold.

Let us assume that (2.1) holds for all positive integers n. Since f is a unit exponentially multiplicative function, from Lemma 1.3, f^{-1} is exponentially multiplicative. Setting $n=p^a m$, with the same conditions on p, a, m what is mentioned earlier, writing $g=f^{-1}\circ F$, using exponentially multiplicative property of f^{-1} and noting that $|\mu(p^e)|=1$ or 0 according as $e=1$ or $e>1$, we may write

$$\sum f(p^b)g(p^c m)=\sum f^{-1}\Big(\prod q_j^{\beta_j}\Big)F\Big(p^a\prod q_j^{\gamma_j}\Big) \tag{2.3}$$

where $b\in C(a)$, with $bc=a$; and $\beta_j\in C(\alpha_j)$, with $\beta_j\gamma_j=\alpha_j$ $j=1,2,\ldots,s$

In view of (2.1), $F(p^a\prod q_j^{\gamma_j})\equiv 0 \pmod{p^a\prod q_j^{\gamma_j}}$, which implies that $F(p^a\prod q_j^{\gamma_j})\equiv 0 \pmod{p^a}$ for every $\prod q_j^{\gamma_j}$ which is of course relatively prime to p^a, yielding (2.2).

3. **An arithmetical equation.** The object of this section is to find certain solutions of the functional equation

$$f^{(s)}=g$$

for a given unit exponentially multiplicative function g, where $f^{(s)}=f\circ f\circ\cdots\circ f$ is the sth iterate of f. This is analogous to a result of Subbarao [3]. For n given by (1.1)

$$f^{(s)}(n)=\sum f\Big(\prod p_i^{b_{1i}}\Big)\cdots f\Big(\prod p_i^{b_{si}}\Big),$$

where the summation is over $b_{1i}\in C(a_i)$, $b_{2i}\in C(a_i/b_{1i}),\ldots,b_{(s-1)i}\in C(a_i/b_{1i}\cdots b_{(s-2)i})$ such that $b_{1i}b_{2i}\cdots b_{si}=a_i$, $i=1,2,\ldots,r$.

In view of Lemma 1.2, the exponential multiplicativity of f implies that of $f^{(s)}$. But the converse of this is not true. For example, choose $f=\mu$ and $C=D$. Though $\mu^{(2)}$ is exponentially multiplicative, μ is not exponentially multiplicative. In fact $\mu^{(2s)}$ is exponentially multiplicative. The following conditional converse is useful in the sequel.

LEMMA 3.1. *If $f^{(s)}$ is a unit exponentially multiplicative function, then f is a unit exponentially multiplicative function if and only if $f(1)=1$ and $f(\gamma(n))=1$ for every n, where $\gamma(n)$ is the product of distinct prime factors of n.*

Proof. Since $f^{(s)}(1)=(f(1))^s$ and $f^{(s)}(\gamma(n))=(f(\gamma(n)))^s$, it is clear that $f^{(s)}$ is a unit if and only if f is a unit. Suppose, the exponential multiplicativity of $f^{(s)}$ also implies the exponential multiplicativity of f. Then $f(1)=1$ and $f(\gamma(n))=1$ for every n. Now assume that $f^{(s)}$ is a unit exponentially multiplicative with $f(1)=1$ and $f(\gamma(n))=1$ for every n. Suppose there is a pair of relatively prime positive integers m and n such that $f(mn)\neq f(m)f(n)$. From the well ordering principle, there exists a pair of relatively prime positive integers with this property such that their product is the smallest element in the set of all such products. Let m_1, n_1 be this pair. If m_2 and n_2 are relatively prime positive integers such that $m_2n_2<m_1n_1$, then $f(m_2n_2)=f(m_2)f(n_2)$. It is obvious that

neither m_1 nor n_1 is equal to 1. Let $m_1=\prod_{i=1}^{k} p_i^{\alpha_i}$ and $n_1=\prod_{j=1}^{t} q_j^{\beta_j}$ Then,

$$f^{(s)}(m_1n_1)=sf(m_1n_1)(f(\gamma(m_1n_1)))^{s-1} -sf(m_1)f(n_1)(f(\gamma(m_1)))^{s-1}(f(\gamma(n_1)))^{s-1} +\sum_1 f\left(\prod p_i^{\delta_{1i}}\right)\cdots f\left(\prod p_i^{\delta_{si}}\right) \times\sum_2 f\left(\prod q_j^{\Delta_{1j}}\right)\cdots f\left(\prod q_j^{\Delta_{sj}}\right) \tag{3.1}$$

where $\sum_1$ is the summation over $\delta_{1i}\in C(\alpha_i),\ldots,\delta_{(s-1)i}\in(\alpha_i/\delta_{1i}\cdots\delta_{(s-2)i})$ such that $\delta_{1i}\cdots\delta_{si}=\alpha_i$, $i=1,2,\ldots,k$ and $\sum_2$ is the summation over $\Delta_{1j}\in C(\beta_j),\ldots,\Delta_{(s-1)j}\in C(\beta_j/\Delta_{1j}\cdots\Delta_{(s-2)j})$ such that $\Delta_{1j}\cdots\Delta_{sj}=\beta_j$, $j=1,2,\ldots,t$. Using $f(\gamma(n))=1$ for every n and the multiplicativity of $f^{(s)}$ in (3.1), we get $f(m_1n_1)=f(m_1)f(n_1)$. This leads to the multiplicativity of f. Similarly, using (iv) and the exponential multiplicativity of $f^{(s)}$, $f(p^{ab})=f(p^a)f(p^b)$ for every prime p whenever $(a,b)=1$.

THEOREM 3.1. *Let g be a unit exponentially multiplicative function. Then the equation $f^{(s)}=g$ has a unit exponentially multiplicative solution. Denoting this solution by h, $f^{(s)}=g$ has a countably infinite number of solutions given by*

$$f(n)=\omega(n)h(n), \tag{3.2}$$

where $\omega(n)$ is an s-th root of unity such that $\omega(n)=\omega(\gamma(n))$.

Proof. Since g is a unit exponentially multiplicative function from the equation $f^{(s)}=g$, one has $(f(1))^s=1$ and $(f(\gamma(n)))^s=1$ for every n. Let the solution corresponding to the case $f(1)=1$ and $f(\gamma(n))=1$ for every n be denoted by h. Then from Lemma 3.1, h is a unit exponentially multiplicative function. Using the mathematical induction, h is determined for any $n=\prod_{j=1}^{v} p_j^{a_j}$ by the equation,

$$g(n)=sh(n)+\sum h\left(\prod p_j^{b_{1j}}\right)\cdots h\left(\prod p_j^{b_{sj}}\right) \tag{3.3}$$

where $\sum$ is the summation over $b_{1j}\in C(a_j),\ldots,b_{(s-1)j}\in C(a_j/b_{1j}\cdots b_{(s-2)j})$ such that $b_{1j}\cdots b_{sj}=a_j$, $j=1,2,\ldots,v$ and $b_{kj}\neq a_j$ for at least one value of $j=1,2,\ldots,v$ and for every $k=1,2,\ldots,s$. Now it is clear that f given by (3.2) satisfies the equation $f^{(s)}=g$.

ACKNOWLEDGEMENT. The author is indebted to Prof. M. V. Subbarao, Professor of Mathematics of the University of Alberta, Edmonton and to the referee for their valuable suggestions in the preparation of the final form of the paper.

REFERENCES

1. W. Narkiewicz, *On a class of arithmetical convolutions* Colloq. Math., **10** (1963), 81–94.

2. M. V. Subbarao, *A congruence for a class of arithmetic functions*, Canad. Math. Bull., **9** (1966), 571–574.

3. ——, *A class of arithmetical equations*, Niew Archief voor wiskunde **(3), 15** (1967), 211–217.

4. ——, *On some arithmetic convolutions*, proc. of the Conference on arithmetic functions (April 1971), Lecture notes in maths. **251,** The theory of arithmetic functions, Springer-Verlag, 247–271.

DEPARTMENT OF MATHEMATICS,
SRI VENKATESWARA UNIVERSITY,
TIRUPATI 517502 (A.P.) INDIA.