Annales Univ. Sci. Budapest., Sect. Comp. 22 (2003) 95-101

ON MULTIPLICATIVE FUNCTIONS SATISFYING CONGRUENCE PROPERTIES

J. Fehér (Pécs, Hungary)

Dedicated to Professor Karl-Heinz Indlekofer on the occasion of his 60th birthday

Abstract. We call the function $f : \mathbb{N} \to \mathbb{Z}$ KH-multiplicative ($f \in \in KH\mathcal{M}$) if for fixed appropriate positive numbers K, H, for any pair of primes $P \neq Q$ such that $P, Q > H$ we have

$$|f(PQ) - f(P)f(Q)| < K.$$

In this paper we prove the following theorem: Let $f \in KH\mathcal{M}$, s be a fixed positive integer and assume that

$$f(n^s + m) \equiv f(m) \pmod{n}$$

holds for every $m, n \in \mathbb{N}$. Then $f(n) = n^\alpha$, $\alpha \in \mathbb{N}_0$.

1. Introduction

The funtion $f : \mathbb{N} \to \mathbb{Z}$ is called multiplicative ($f \in \mathcal{M}$) if the condition

$$(*) \qquad f(nm) = f(n)f(m)$$

Research partially supported by the Hungarian National Foundation for Scientific Research Grant T031877.

is satisfied for all pairs $n, m \in \mathbb{N}$, $(n, m) = 1$. The f is completely multiplicative ($f \in \mathcal{M}^*$), iff (*) holds for all pairs $n, m \in \mathbb{N}$. The function $f(n) = n^\alpha$ ($\alpha \in \mathbb{N}_0$) is multiplicative and has many nice properties. For example:

$$(**) \qquad (n+m)^\alpha \equiv m^\alpha \pmod{n} \quad (\forall n, m \in \mathbb{N}).$$

As it was noticed by M.V. Subbarao (1966), the property (**) holds only for power funtions among all multiplicative functions, namely we have

Theorem A. (M.V. Subbarao, 1966 [8]) *If $f \in \mathcal{M}$ and*

$$f(n+m) \equiv f(m) \pmod{n} \quad (\forall n, m \in \mathbb{N}),$$

then $f(n) = n^\alpha$ ($\alpha \in \mathbb{N}_0$).

Let $M, N \subset \mathbb{N}$, and for $f : \mathbb{N} \to \mathbb{Z}$ assume

$$(1) \qquad f(n+m) \equiv f(m) \pmod{n} \quad (\forall n \in N, \forall m \in M).$$

First let us remind a few variants of Theorem A. In them all f satisfy the condition (1).

Theorem B. (A. Iványi, 1972 [5]) *If $f \in \mathcal{M}^*$, $N = \mathbb{N}$, $M = \{m\}$ and $f(m) \neq 0$, then $f(n) = n^\alpha$ ($\alpha \in \mathbb{N}_0$).*

The latter result was improved, namely we have

Theorem B'. (B.M. Phong and J. Fehér, 1985 [7]) *If $f \in \mathcal{M}$, $N = \mathbb{N}$, $M = \{m\}$ and $f(m) \neq 0$, then $f(n) = n^\alpha$ ($\alpha \in \mathbb{N}_0$).*

Theorem C. (I. Joó and B.M. Phong, 1992 [6]) *If $f \in \mathcal{M}$, $N = \{n \mid n \in \mathbb{N}, A \mid n\}$, $M = \{B\}$, $(A, B) = 1$ and $f(B) \neq 0$, then there are a real valued Dirichlet character $\chi \pmod{A}$ and $\alpha \in \mathbb{N}_0$, such that $f(n) = \chi(n) n^\alpha$ ($\forall n \in \mathbb{N}$, $(n, A) = 1$).*

Definition. (M.V. Subbarao, 1985 [9]) The function $f : \mathbb{N} \to \mathbb{Z}$ is called quasi multiplicative ($f \in Q\mathcal{M}$) if $f(np) = f(n)f(p)$ hold for all primes p and all $n \in \mathbb{N}$ such that $p \not| n$.

Theorem D. (J. Fabrykowski and M.V. Subbarao, 1988, [1]) *If $f \in Q\mathcal{M}$, $M = \mathbb{N}$ and $N = \mathcal{P}$ ($= \{\text{primes}\}$), then $f(n) = n^\alpha$ ($\alpha \in \mathbb{N}_0$).*

The authors of Theorem D conjectured, that the conclusion remains true also in the cases when N is substituted by an infinite subset of primes. This conjecture was partly proved, namely we have

Theorem E. (J. Fehér and B.M. Phong, 2000 [4]) *If $f \in Q\mathcal{M}$, $N = \{p \mid p \in \mathcal{P}, p > K\}$, and $M = \mathbb{N}$, then $f(n) = n^\alpha$ ($\alpha \in \mathbb{N}_0$).*

Theorem F. (J. Fehér, 1994, [2]) *If $f \in \mathcal{M}$, $N = \{n^2 \mid n \in \mathbb{N}\}$, $M = \{1\}$, then $f(2) = 2^\beta$ and $f(q^K) = q^{K\alpha(q)}$ for all primes of the form $q = 4k + 1$.*

Notice that the function f occuring in Theorem F satisfies also the following condition:

$$ab \in H \Rightarrow f(ab) = f(a)f(b),$$

where

$$H := \{2^\varepsilon \prod_i q_i^{h_i} \mid \varepsilon = 0, 1; \quad q_i \in \mathcal{P}, q_i \equiv 1 \pmod 4\}.$$

If $f \in \mathcal{M}$, $N = \{n^2 \mid n \in \mathbb{N}\}$, $M = \mathcal{P}$, and there is a prime p_0, such that $f(p_0) \neq 0$, then it can be proved [3] that

$$|f(p^K)| = p^{\alpha(p,K)} \quad (\forall p \in \mathcal{P}).$$

Moreover, we expect that the latter f is of the form $f(n) = n^\alpha$ ($\alpha \in \mathbb{N}_0$), but to prove this, seems to be not so easy.

2. KH-multiplicative functions

Definition. Let K, H be arbitrary fixed positive numbers. We call the function KH-multiplicative ($f \in KH\mathcal{M}$) if $f(1) = 1$ and for all primes $P, Q > > H$, $P \neq Q$

$$|f(PQ) - f(P)f(Q)| < K.$$

It is clear that $\mathcal{M}^* \subset \mathcal{M} \subset Q\mathcal{M} \subset KH\mathcal{M}$. In what follows, we would like to demonstrate the strength of the congruence property (1).

Theorem 1. *Assume $M = \mathbb{N}$ and N fulfills the conditions: for all pairs $k, m \in \mathbb{N}$ there are $A, B \in N$ such that*

(α) $A, B > k$,

(β) $(A, B) = (AB, m) = 1$.

If the function $f \in KH\mathcal{M}$ satisfies the condition (1), then f is completely multiplicative.

Proof. Since $M = \mathbb{N}$, the condition (1) easily implies

$$f(hn + m) \equiv f(m) \pmod n \quad (\forall n \in N, \forall h, m \in \mathbb{N}). \tag{2}$$

Let a, b be arbitrary fixed natural numbers. Let us fix $A, B \in N$ so that $A, B > H$,

$$A, B > K + |f(ab) - f(a)f(b)|,$$

and also assume that $(A, B) = (AB, ab) = 1$. The latter condition implies that the congruence

$$Ax + 1 \equiv a \pmod{B}$$

can be solved and that all solutions are of the form $x = x_0 + MB$ $(M \in \mathbb{Z})$. Since $(AB, AM_0 + 1) = (B, AM_0 + 1) = (B, a) = 1$, we can choose $w \in \mathbb{N}$ such that the number $P = WAB + AM_0 + 1$ is prime. Further, let Q be a prime of the form $Q = LAB + b$. Then

$$\begin{cases} P = W_1A + a = W_2B + 1 \quad (W_1, W_2 \in \mathbb{N}), \\ Q = L_1A + b = L_2B + b \quad (L_1, L_2 \in \mathbb{N}). \end{cases} \tag{3}$$

The condition (2) gives

$$\left.\begin{matrix} f(P) \equiv f(a) \\ f(Q) \equiv f(b) \end{matrix}\right\} \pmod{A} \Rightarrow f(P)f(Q) \equiv f(a)f(b) \pmod{A}.$$

On the other hand $PQ = TA + ab \Rightarrow f(PQ) \equiv f(ab) \pmod{A}$. These imply

$$A | f(PQ) - f(P)f(Q) - (f(ab) - f(a)f(b)) = \triangle.$$

A is so chosen that $P, Q > H$, hence

$$|\triangle| < K + |f(ab) - f(a)f(b)| < A,$$

that is possible only if $\triangle = 0$.

Consequently

$$f(PQ) - f(P)f(Q) = f(ab) - f(a)f(b).$$

The condition fulfilled by B shows that the latter equation is true also for $a = 1$. This implies that $f(PQ) - f(P)f(Q) = 0$, hence $f(ab) = f(a)f(b)$.

Remark. For example, the N-as follows satisfy the conditions of Theorem 1 : $N = \mathbb{N}$, $N = \mathcal{P}^*(\subset \mathcal{P}$, infinite), $N = \{2^p - 1 \mid p \in \mathcal{P}\}, \ldots$. Consequently, the Theorems A, D, E remain true also under more general condition of KH-multiplicity.

3. An application

Theorem 2. *Let $s \in \mathbb{N}$ be fixed. Assume that $f \in KH\mathcal{M}$ and*

$$f(n^s + m) \equiv f(m) \pmod{n} \quad (\forall n, m \in \mathbb{N}). \tag{4}$$

Then $f(n) = n^\alpha$ $(\alpha \in \mathbb{N}_0)$.

For the proof we need two lemmas.

Lemma 1. *If an f satisfies the conditions of Theorem 2, then f is completely multiplicative.*

Proof. A slight modification of the proof of Theorem 1.

Lemma 2. *For any prime $\pi > 2$ there exist infinitely many primes Q such that Q is a primitive root $\pmod{\pi^\ell}$ for all $\ell = 1, 2, \ldots$.*

Proof. Well known.

Proof of Theorem 2. The condition (4) easily implies

$$f(kn^s + m) \equiv f(m) \pmod{n} \quad (\forall k, n, m \in \mathbb{N}). \tag{5}$$

Let $p \neq q$ be primes. There are $x, y \in \mathbb{N}$, such that

$$px \equiv q^s y + 1. \tag{6}$$

Using (5) this implies

$$f(p)f(x) \equiv 1 \pmod{q},$$

hence $f(p) = (-1)^{h(p)} p^{\alpha(p)}$ $(\forall p \in \mathcal{P})$.

Let π, Q be as in Lemma 2 and let P be a prime $P \neq \pi$, $P \neq Q$. Then for all $\ell = 1, 2, \ldots$ there exists $h(\ell) \in \mathbb{N}$ such that

$$P \cdot Q^{h(\ell)} \equiv \quad (\mathrm{mod}\ \pi^{\ell s}), \tag{7}$$

hence by (5) we see that

$$(-1)^{\varepsilon(P) + h(\ell)\varepsilon(Q)} P^{\alpha(P)} Q^{\alpha(Q)} \equiv 1 \pmod{\pi^\ell}. \tag{8}$$

From (7) we see immediately that

$$P^{\alpha(Q)} \cdot Q^{h(\ell)\alpha(Q)} \equiv 1 \pmod{\pi^\ell}. \tag{9}$$

(8) and (9) imply

$$(-1)^{\varepsilon(P)+h(\ell)\varepsilon(Q)}P^{|\alpha(Q)-\alpha(P)|}-1\equiv 0 \pmod{\pi^{\ell}}.$$

Since the modulus can be arbitrary large, the latter congruence can hold if and only if $\alpha(P)=\alpha(Q)=\alpha$ and

$$\varepsilon(P)+h(\ell)\varepsilon(Q)\equiv 0 \pmod 2. \tag{10}$$

We have to show that $\varepsilon(P)$ is even. First, we show that the parity of $h(\ell)$ does not depend on ℓ. The condition (7) implies that for arbitrary $\ell_1,\ell_2\in\mathbb{N}$ we have

$$Q^{|h(\ell_1)-h(\ell_2)|}\equiv 1 \pmod{\pi}. \tag{11}$$

As Q is primitive $\pmod{\pi}$, (11) shows that $2|\pi-1|h(\ell_1)-h(\ell_2)$ consequently $h(\ell_1)$ and $h(\ell_2)$ have the same parity. After that it is enough to show that for any prime P there is π such that $2\mid h(1)=h$.

If $o(P)\mid\dfrac{\pi-1}{2}$, then h is even. Indeed, (7) (for $\ell=1$) implies

$$P^{o(P)}\cdot Q^{ho(P)}\equiv Q^{ho(P)}\equiv 1 \pmod{\pi}.$$

As Q is primitive $\pmod{\pi}$ we have $\pi-1|o(P)\cdot h|h\cdot\dfrac{\pi-1}{2}\Rightarrow 2\mid h$. To finish the proof it is enough to show that for any P prime, there is a prime $\pi>2$ such that $o(P)\mid\dfrac{\pi-1}{2}$.

For this notice that

(α) if $2<P\neq 2^T+1$ than $2<\pi\mid P-1$ $\left(\text{hence } o(p)=1\mid\dfrac{\pi-1}{2}\right)$,

(β) if $P=2^T+1$ $(T\geq 1)$ than $2<\pi\mid P^3-1$ $\left(\text{hence } o(p)=3\mid\dfrac{\pi-1}{2}\right)$,

(γ) if $P=2$ than $\pi=7$ $\left(\text{hence } o(2)=3\mid\dfrac{\pi-1}{2}=3\right)$.

These show (using (10)) that $f(P)=P^{\alpha}$ $(\forall P\in\mathcal{P})$, consequently $f(n)=n^{\alpha}$.

References

[1] **Fabrykowski J. and Subbarao M.V.,** A class of arithmetic functions satisfying a congruence property, *J. Madras University. Section B,* **51** (1988), 48-51.

[2] **Fehér J.,** On integer valued multiplicative and additive arithmetical functions, *Annales Univ. Sci. Budapest. Sect. Comp.,* **14** (1994), 39-45.

[3] **Fehér J.,** (Unpublished manuscript) (2002)

[4] **Fehér J. and Phong B.M.,** On a problem of Fabrykowski and Subbarao concerning quasi multiplicative funtions satisfying a congruence property, *Acta Math. Hungar.,* **89** (1-2) (2000), 149-159.

[5] **Iványi A.,** On multiplicative functions with congruence property, *Annales Univ. Sci. Budapest. Sect. Math.,* **15** (1972), 133-137.

[6] **Joó I. and Phong B.M.,** Arithmetical functions with congruence properties, *Annales Univ. Sci. Budapest. Sect. Math.,* **35** (1992), 151-155.

[7] **Phong B.M. and Fehér J.,** Note on multiplicative functions satisfying a congruence property, *Annales Univ. Sci. Budapest. Sect. Math.,* **33** (1990), 261-265.

[8] **Subbarao M.V.,** Arithmetic functions satisfying congruence property, *Canad. Math. Bull.,* **9** (1966), 143-146.

[9] **Subbarao M.V.,** *On some arithmetic functions satisfying a congruence property,* Amer. Math. Soc. Abstract, 86 T-11-54 (1986).

J. Fehér
Department of Mathematics
University of Pécs
Ifjúság u. 6.
H-7624 Pécs, Hungary