Annales Univ. Sci. Budapest., Sect. Comp. 24 (2004) 247-252

ON MULTIPLICATIVE FUNCTIONS SATISFYING CONGRUENCE PROPERTIES II.

J. Fehér (Pécs, Hungary)

Dedicated to Professor Imre Kátai on the ocassion of his 65th birthday

1. Introduction

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

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

is satisfied for all pairs $n,m\in\mathbb{N}$, $(n,m)=1$. The f is completely multiplicative ($f\in\mathcal{M}^*$), if $(*)$ 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:

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

As it was noticed by M.V. Subbarao (1966), namely we have

Theorem A. (M.V. Subbarao, 1966 [5]) *If $f\in\mathcal{M}$ and*

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

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

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

$$(*\,*\,*)\qquad f(n+m)\equiv f(m)\pmod n\ (\forall n\in N,\ \forall m\in M).$$

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

Research partially supported by the Hungarian National Foundation for Scientific Research under grant T031877 and the fund of Applied Number Theory Research Group of the Hungarian Academy of Sciences.

Theorem B. (A. Iványi, 1972 [2]) *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 C. (B.M. Phong and J. Fehér, 1985 [4]) *If* $f \in \mathcal{M},\ N = \mathbb{N},\ M = \{m\}$ *and* $f(m) \neq 0$ *then* $f(n) = n^\alpha$ $(\alpha \in \mathbb{N})$.

Theorem D. (I. Joó and B.M. Phong, 1992 [3]) *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* χ (mod A) *and* $\alpha \in \mathbb{N}_0$, *such that* $f(n) = \chi(n)n^\alpha$ $(\forall n \in \mathbb{N},\ (n, A) = 1)$.

Theorem E. (J. Fehér, 1994, [1]) *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 Theorme E satisfies also the following condition:

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

where

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

In this paper we prove the following theorem.

Theorem. *Let* $f : \mathbb{N} \to \mathbb{Z}$ *be a multiplicative function. Assume that for all primes* p *and* $n \in \mathbb{N}$

$$f(n^2 + p) \equiv f(p) \pmod n. \tag{1}$$

Then: if there is a prime p_0 *such that* $f(p_0) \neq 0$, *then*

$$|f(q^k)| = q^{\alpha(q^k)}$$

for all q *primes and* $k \in \mathbb{N}$.

2. Lemmas

The proof of Theorem is based on the four lemmas as follows.

Lemma 1. *Let* $A, B, C \in \mathbb{N},\ (A, B) = 1$. *Then the diophantine equation*

$$Ax - By = 1$$

has got the solution (x, y) *such that* $(x, c) = 1$.

Proof. Let (x_0, y_0) be a solution, $c = \prod_{i=1}^{s} p_i^{\alpha_i} \prod_{j=1}^{r} q_j^{\beta_j}$ be the primepower-decomposition of c, where $p_i \mid x_0$, and $q_j \nmid x_0$. Then the pair

$$x = x_0 + B(p_1 \dots p_s + 1)(q_1 \dots q_r),$$
$$y = y_0 + A(p_1 \dots p_s + 1)(q_1 \dots q_r)$$

is a solution satisfying the condition $(C, X) = 1$.

Lemma 2. *Let* p_0, ρ_0 *be two (not equal) odd primes such that* $\left(\frac{-p_0}{\rho_0}\right) = -1$. *Then there are infinitely many odd primes* q *such that* $\left(\frac{-p_0}{q}\right) = \left(\frac{-q}{\rho_0}\right) = 1$.

Proof. Let $q = 4Mp_0 + 1$ $(M \in \mathbb{N})$. Then the condition $\left(\frac{-p_0}{q}\right) = 1$ (where $(\cdot)$ is the Jacobi symbol) is fulfilled for all M. The diophantine equation

$$4Mp_0 + 1 = -1 + \rho_0 L$$

has a solution and its solutions are: $M = M_0 + \rho_0 N$, $L = L_0 + 4p_0 N$. Using we get

$$q = 4p_0\rho_0 N + 4p_0 M_0 + 1 = 4\rho_0 p_0 N + \rho_0 L_0 - 1 \quad (N \in \mathbb{N}),$$

and this shows that $\left(\frac{-q}{\rho_0}\right) = 1$. The condition $(4\rho_0 p_0,\ 4p_0 M_0 + 1) = 1$ implies that among q-s there are infinitely many primes.

Lemma 3. *Let* $2 < q$ *be a prime such that* $q \nmid A$ *and* $p \neq q$ *a prime such that* $\left(\frac{-p}{q}\right) = 1$. *Then for all* $\alpha \in \mathbb{N}$ *there exist* $x, u \in \mathbb{N}$ *such that*

$$q^\alpha u p = x^2 A^2 + p, \quad (q, u) = (p, u) = 1.$$

Proof. Let T and v be positive integers such that

$$q^\alpha v = A^2 \cdot T + 1. \tag{2}$$

The relation (2) shows that $\left(\frac{T}{q}\right) = \left(\frac{-1}{q}\right) \Rightarrow \left(\frac{Tp}{q}\right) = \left(\frac{-p}{q}\right) = 1$, hence there is $x_0 \in \mathbb{N}$ such that

$$x_0^2 \equiv Tp \pmod{q^{\alpha+1}}. \tag{3}$$

The numbers $x = x_0 + kq^{\alpha+1}$ are also solutions of (3), hence we can choose the k so that $p|x$. So we can assume that in (3) $p|x_0$. By the Lemma 1, we can choose v satisfying (2) and also $(v, pq) = 1$. The relation (3) shows that, denoting

$$L := \frac{x_0^2 - Tp}{q^\alpha}, \quad u^* := vp + LA^2,$$

we get $q|L,\ q\not| v$ and so $q\not| u^*$. The relation (2) implies

$$q^\alpha vp = TpA^2 + p. \tag{4}$$

From this we see that

$$q^\alpha vp = q^\alpha(u^* - LA^2) = q^\alpha \left(\frac{x_0^2 - Tp}{q^\alpha} A^2\right) = q^\alpha u^* - x_0^2 A^2 + TpA^2,$$

and (4) also implies that $q^\alpha u^* = x_0^2 A^2 + p$. Here $p \mid x_0$ implies $p \| X_0^2 A_2 + p$ and this in turn implies $u^* = up,\ p\not| u$.

One can prove (in a similar way) the following

Lemma 4. *Let $2\not| A$ and $\alpha \in \mathbb{N}$. Then there are infinitely many primes $p > 2$ such that*

$$2^\alpha up = x^2 A^2 + p, \quad (u, 2p) = 1. \tag{5}$$

3. Proof of the theorem

Assume that f fulfills the conditions of the theorem. First we show that $f(p) \neq 0$ for all primes p.

Let p, q be primes such that $p \neq q,\ p \neq p_0,\ q \neq p_0,\ q^k \| f(p_0)$ and assume

$$pu\,p_0 = x^2 q^{2(k+1)} + p_0,\ (u, pp_0) = 1.$$

Then

$$f(p)f(u)f(p_0) \equiv f(p_0) \pmod{q^{k+1}},$$

which implies

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

showing that $f(p) \neq 0$.

By the Lemmas 2, 3, 4 we see that

(α) $p_0 = 2 \Rightarrow f(11) = 0$.

$p \neq p_0$ and $p \neq 11$ and $\left(\frac{-11}{p}\right) = 1 \Rightarrow f(p) \neq 0$,

$p \neq p_0$ and $p \neq 11$ and $\left(\frac{-11}{p}\right) = -1 \Rightarrow \exists q$ prime, for which $\left(\frac{-11}{q}\right) = \left(\frac{-q}{p}\right) = 1$, and so $f(11) \neq 0 \Rightarrow f(q) \neq 0 \Rightarrow f(p) \neq 0$.

(β) $2 < p_0$ and $2 < p \neq p_0$ and $\left(\frac{-p_0}{p}\right) = 1 \Rightarrow f(p) = 0$,

$2 < p_0$ and $2 < p \neq p_0$ and $\left(\frac{-p_0}{p}\right) = -1 \Rightarrow \exists q > 0$ prime, for which $\left(\frac{-p_0}{q}\right) = \left(\frac{-q}{p}\right) = 1$, and so

$f(p_0) \neq 0 \Rightarrow f(q) \neq 0 \Rightarrow f(p) \neq 0$.

Finally, let q^α be a given power of the prime q, and a prime ρ, such that $\rho \neq q$. Then there are $u, x \in \mathbb{N}$ and a prime $p(\neq q)$, such that

$$q^\alpha up = x^2\rho^{2k} + p, \quad (u, pq) = 1.$$

From this we see that

$$f(q^\alpha)f(u)f(p) \equiv f(p) \pmod{p^k}. \tag{6}$$

For $f(p) \neq 0$ $\exists s \in \mathbb{N}_0$, $\rho^s \| f(p)$. Assuming that $k > s$ the relation (6) shows that

$$f(q^\alpha)f(u) \equiv 1 \pmod{\rho},$$

consequently $\rho \not| f(q^\alpha)$.

4. Remarks

(a) It seems that the function f satisfying the conditions of the Theorem as well as the congruence (1) are power functions. It seems to us that to prowe the independence of $\alpha(p^k)$ upon k and p is not easy task.

(b) If for some prime p_0, $f(p_0) = 0$, then obviously $f(p) = \{\circ\}$. In this case there is a solution f of (1) such that $f \in \mathcal{M}\backslash\mathcal{M}^*$. An example of such function:

$$f(1) = 1,\ f(9) = 2 \quad \text{and} \quad f(n) = 0 \text{ if } n \neq 1, 9.$$

References

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

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

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

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

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

(Received April 20, 2004)

J. Fehér
Department of Mathematics
Janus Pannonius University
Ifúság útja 6.
H-7624 Pécs, Hungary