Annales Univ. Sci. Budapest., Sect. Comp. 14 (1994) 39-45

ON INTEGER VALUED MULTIPLICATIVE AND ADDITIVE ARITHMETICAL FUNCTIONS

J. Fehér (Pécs, Hungary)

Dedicated to Professor Karl-Heinz Indlekofer
on the occasion of awarding to him the degree
"Doctor honoris causa"

1. Introduction

Let $\mathcal{M}$ and $\mathcal{M}^*$ denote the family of all integer valued multiplicative and completely multiplicative functions, respectively. Furthermore let $\mathcal{A}$ be the set of all integer valued additive functions.

In 1966 M.V. Subbarao [5] proved the following: If $f \in \mathcal{M}$ and we have

$$f(n+m) \equiv f(m) \pmod{n} \tag{1}$$

for each couple (n, m) then necessarily

$$f(n) = n^{\alpha} \qquad (\forall n \in \mathbb{N}) \tag{2}$$

for a suitable integer $\alpha \geq 0$.

In [3] A. Iványi established that if $f \in \mathcal{M}^*$ and (1) holds for some fixed m for all values of n then f is also of the form (2). This result was sharpened by B.M. Phong and the author [2] by showing that the relations $f \in \mathcal{M}$, $f(m) \neq 0$ and (1) for some m and for all n imply (2), too. Finally B.M. Phong and I. Joó [1] proved the following: If $f \in \mathcal{M}$, $A \geq 1$, $B \geq 1$ and $C \neq 0$ are fixed integers and for all $n \in \mathbb{N}$ we have

$$f(An+B) \equiv C \pmod{n} \tag{3}$$

then there exists a real Dirichlet character $\chi_A \pmod{A}$ such that

$$f(n) = \chi(n) n^{\alpha} \tag{4}$$

for all $n \in \mathbb{N}$ with $(n, A) = 1$ where $\alpha \geq 0$ is a suitable integer.

The following question is raised naturally: Let us fix $T \in \mathbb{Z}$ and $P(x) \in \mathbb{Z}[x]$ with $deg\ P \geq 1$ and $P(n) > 0$ $(n = 1, 2, \ldots)$. Assume $f \in \mathcal{M}$ or alternatively $f \in \mathcal{A}$. What can be stated about f if

$$(5) \qquad f(P(n)) \equiv T \pmod{n} \quad (n = 1, 2, \ldots)?$$

In the present paper we are going to prove the following

Theorem 1. *Let $f \in \mathcal{M}$ and suppose*

$$(6) \qquad f(n^2 + 1) \equiv 1 \pmod{n^2} \quad (\forall n \in \mathbb{N}).$$

Then $f(2) = 2^{\nu}$, $f(q^{\alpha}) = q^{\alpha\mu(q)}$ whenever q is a prime with $q \equiv 1 \pmod{4}$.

Define $H := \left\{ 2^{\varepsilon} \prod_i q_i^{\alpha_i} \mid \varepsilon = 0, 1; \quad q_i \equiv 1 \pmod{4} \quad primes \right\}$.

Theorem 2. *Let $g \in \mathcal{A}$ and assume*

$$(7) \qquad g(n^2 + 1) \equiv 0 \pmod{n} \quad (\forall n \in \mathbb{N}).$$

Then g is completely additive on the set H in the sense that $a, b \in H$ implies always $g(ab) = g(a) + g(b)$.

2. Lemmas

Lemma 1. *Let $q \equiv 1 \pmod{4}$ be a prime or let $q = 2$. Suppose $P \not\equiv 0 \pmod{q}$ is an integer and let $\alpha = 1$ if $q = 2$. Then there exists a couple $(x, u) \in \mathbb{N}^2$ such that*

$$(8) \qquad q^{\alpha} u = x^2 P^2 + 1 \quad \text{and} \quad u \not\equiv 0 \pmod{q}.$$

Proof. If $q = 2$ then any odd x suits our requirements. Let $q \equiv 1 \pmod{4}$ be a prime. Since $P \not\equiv 0 \pmod{q}$, we can choose $(v, T) \in \mathbb{N}^2$ such that

$$(9) \qquad q^{\alpha} v = TP^2 + 1 \quad \text{and} \quad (v, T) = 1.$$

Since (9) implies $\left(\frac{T}{q}\right) = 1$, there exists $x \in \mathbb{N}$ with $x^2 \equiv T \pmod{q^{\alpha+1}}$. Let $k = \dfrac{x^2 - T}{q^{\alpha}}$, $u = v + kP^2$. Then $(u, q) = (v, q) = 1$ and $q^{\alpha} u = x^2 P^2 + 1$.

Lemma 2. *Let $q \equiv 1 \pmod 4$ be a prime, $uq^\alpha = A^2+1$ $(\alpha \in \mathbb{N})$, $u \not\equiv 0 \pmod q$. Then the equation*

$$x^2 - (A^2+1)y^2 = A^2 \tag{10}$$

admits a solution such that $A|x$, $A|y$, $y^2+1 = vq$, $v \not\equiv 0 \pmod q$ and $(u,v)=1$.

Proof. Let $uq^\alpha = A^2+1$ $(= d)$, $u \not\equiv 0 \pmod q$. Then the Pell equation

$$x^2 - (A^2+1)y^2 = 1 \tag{11}$$

has a solution (x_0, y_0) satisfying

$$x_0 \not\equiv 0 \pmod q, \quad y_0 \not\equiv 0 \pmod q \quad \text{and} \quad u|y_0. \tag{12}$$

It is well-known that the couples (x_n, y_n) defined by

$$\begin{aligned} x_n &= \sum_{i=0}^{\infty} \binom{n}{2i} d^i y_0^{2i} x_0^{n-2i} \\ y_n &= \sum_{i=0}^{\infty} \binom{n}{2i+1} d^i y_0^{2i+1} x_0^{n-2i-1} = n y_0 x_0^{n-1} + B_n d \end{aligned} \tag{13}$$

are solutions of (11). It is clear that (X_n, Y_n) is a solution of (10) for $X_n = Ax_n$, $Y_n = Ay_n$. From (13) it follows

$$Y_n^2 + 1 = (Any_0x_0^{n-1})^2 + 2y_0x_0^{n-1}A^2B_n dn + C_nq^2 + 1.$$

Let $n = s(q^2-1)+1$. Then $d = uq^\alpha$ and, by Fermat's theorem,

$$Y_n^2 + 1 \equiv (Ay_0)^2(s-1)^2 + 1 \pmod q. \tag{14}$$

The case $\alpha > 1$

If $\alpha > 1$ then we have also (14) (*mod* q^2). Choose a positive integer such that

$$(Ay_0)^2(s_0-1)^2 + 1 \begin{cases} \equiv 0 \pmod q, \\ \not\equiv 0 \pmod{q^2}. \end{cases} \tag{15}$$

Then (X_n, Y_n) suits our requirements for $n = s_0(q^2-1)+1$.

The case $\alpha = 1$

Suppose that s_0 satisfies (15) and let $s = s_0 + mq$. Then for $n = n(m) = (s_0 + mq)(q^2 - 1) + 1$ we have

$$Y_{n(m)}^2 + 1 = G_m q \equiv (Ay_0)^2 (s_0 - 1 + mq)^2 x_0^{2(s_0+mq)(q^2-1)} + 1 +$$

$$+2A_{y_0}^2(-(s_0 - 1) - mq) x_0^{(s_0+mq)(q^2-1)} uqB_n \qquad (\text{mod } q^2).$$

According to the Euler–Fermat theorem, here we have

$$\begin{aligned} x_0^{2s_0(q+1)(q-1)} &= Lq + 1, \\ x_0^{2m(q+1)q(q-1)} &= L_m q^2 + 1, \\ x_0^{s_0(q+1)(q-1)} &= Dq + 1, \\ x_0^{m(q+1)q(q-1)} &= D_m q^2 + 1 \end{aligned}$$

and hence

$$G_m q \equiv Mq + (Ay_0)^2(s_0 - 1)Lq + 2(Ay_0)^2(s_0 - 1)mq -$$

$$-2Ay_0(Dq + 1)[(s_0 - 1) + mq]uB_n q \qquad (\text{mod } q^2).$$

On the other hand

$$B_n \equiv \binom{n}{3} y_0^3 x_0^{n-3} \equiv -\frac{s_0(s_0^2 - 1)}{6} y_0^3 x_0^{q-3} \qquad (\text{mod } q)$$

and hence

$$G_m \equiv T \cdot m + E \quad (\text{mod } q) \quad \text{where} \quad T \equiv 2(Ay_0)^2(s_0 - 1) \not\equiv 0 \quad (\text{mod } q).$$

Thus we can achieve $q | G_m$. Notice that (X_n, Y_n) suits our requirements if $n = (s_0 + mq)(q^2 - 1) + 1$ and $G_m \not\equiv 0 \ (\text{mod } q)$.

Lemma 3. *Every prime number* $q = 4k + 1$ *admits a representation* $q = \prod_i (4x_i^2 + 1)^{l_i} \quad (x_i, l_i \in \mathbb{Z})$.

Proof. (See I. Kátai [4])

3. Proof of Theorem 1

(a) Let $q = 2$ or $q \equiv 1 \pmod 4$ and suppose $\alpha = 1$ if $q = 2$. Furthermore let p be a prime with $p | f(q^\alpha)$. We show that $q = p$. Assume $q \neq p$. Then by Lemma 1 the condition $uq^\alpha = x^2p^2 + 1$, $u \not\equiv 0 \pmod q$ can be satisfied. Hence, by (6), it follows $f(u)f(q^\alpha) \equiv 1 \pmod p$ which is impossible because $p | f(q^\alpha)$.

(b) Let $q \equiv 1 \pmod 4$ be a prime, $\alpha \geq 1$ an integer, $P \not\equiv 0 \pmod q$, $uq^\alpha = t^2P^2 + 1 = A^2 + 1$, $u \not\equiv 0 \pmod q$. Let (X, Y) be a solution of the equation $x^2 - (A^2+1)y^2 = A^2$ satisfying the conditions of Lemma 2. Then

$$l^2P^2 + 1 = x^2 + 1 = (A^2+1)(y^2+1) = uq^\alpha v,$$

$$(u, q) = (v, q) = (u, v) = 1$$

and therefore, by (6),

$$f(u)f(v)f(q^{\alpha+1}) \equiv 1 \pmod P. \tag{16}$$

On the other hand, since $uq^\alpha = A^2 + 1 = t^2P^2 + 1$ and $(u, q) = 1$, (6) implies

$$f(u)f(q^\alpha) \equiv 1 \pmod P, \tag{17}$$

and since $vq = y^2 + 1 = h^2P^2 + 1$ and $(v, q) = 1$, by (6),

$$f(v)f(q) \equiv 1 \pmod P. \tag{18}$$

From (16), (17) and (18) we get

$$f(u)f(v)f(q^{\alpha+1}) \equiv f(u)f(v)f(q^\alpha)f(q) \pmod P. \tag{19}$$

Since $(P, u) = (P, v) = 1$ by (a) we have $(P, f(u)) = (P, f(v)) = 1$. Thus (19) entails

$$f(q^{\alpha+1}) \equiv f(q^\alpha)f(q) \pmod P. \tag{20}$$

Since P can be arbitrarily large, from (20) we obtain

$$f(q^{\alpha+1}) = f(q^\alpha)f(q) \qquad (\alpha = 1, 2, \ldots). \tag{21}$$

Comparing (a) and (21) we deduce $|f(q^\alpha)| = q^{\alpha\mu(q)}$.

(c) It remains to check that $f(q) > 0$. Let p, q be primes of the form $4k+1$ and assume $f(p) = -p^{\nu}$. By Lemma 3 we have $pq^2 \prod_i (4x_i^2 + 1) = \prod_j (4y_j^2 + 1)$. Hence (6) and the complete multiplicativity imply

$$-p^{\nu} q^{2\mu} \equiv 1 \pmod 4. \tag{22}$$

On the other hand

$$p^{\nu} q^{2\mu} \equiv 1 \pmod 4. \tag{23}$$

Comparing (22) and (23) we see that

$$p^{|\mu-\nu|} + 1 \equiv 0 \pmod 4,$$

which is impossible since $p \equiv 1$ $(mod\ 4)$. Finally $2 \cdot 5^2 = 7^2 + 1$ and the assumption $f(2) = -2^{\nu}$ imply similarly

$$2^{|\nu-\mu|} + 1 \equiv 0 \pmod 7$$

which is also impossible.

4. Proof of Theorem 2

Let $q \equiv 1$ $(mod\ 4)$ be a prime, $\alpha \geq 1$, $P \not\equiv 0$ $(mod\ q)$. Then, with the notations of the proof of Theorem 1, from (7) we obtain

$$g(u) + g(q^{\alpha}) \equiv 0 \pmod P, \tag{24}$$

$$g(v) + g(q) \equiv 0 \pmod P, \tag{25}$$

$$g(u) + g(v) + g(q^{\alpha+1}) \equiv 0 \pmod P. \tag{26}$$

The proof of (24), (25) and (26) is analogous to our previous considerations. Hence we get finally

$$g(q^{\alpha+1}) = g(q^{\alpha}) + g(q).$$

References

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

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

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

[4] **Kátai I.**, Some problems in number theory, *Studia Sci.Math.Hung.*, **16** (1981), 289-295.

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

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