Annales Univ. Sci. Budapest., Sect. Comp. 22 (2003) 49-67

ON ARITHMETICAL FUNCTIONS SATISFYING CONGRUENCE PROPERTIES

Bui Minh Phong (Budapest, Hungary)

Dedicated to Professor Karl-Heinz Indlekofer on his 60th anniversary

I. Introduction

An arithmetical function $f(n) \not\equiv 0$ is said to be multiplicative if $(n,m) = 1$ implies
$$f(nm) = f(n)f(m)$$
and it is called completely multiplicative if this equation holds for all pairs of positive integers n and m. In the following we denote by $\mathcal{M}$ and $\mathcal{M}^*$ the set of all integer-valued multiplicative and completely multiplicative functions, respectively. For each positive integer $\mathcal{D}$ let $\mathcal{M}^*_{\mathcal{D}}$ be the set of all arithmetical functions f for which $f(nm) = f(n)f(m)$ is satisfied for all $n,\ m$ coprime to $\mathcal{D}$. Let $I\!N$ be the set of all positive integers and $\mathcal{P}$ be the set of all primes. In the following, (m,n) denotes the greatest common divisor of the integers $m,\ n$ and $m \parallel n$ denotes that m is a unitary divisor of n, i.e. that $m|n$ and $(\frac{n}{m}, m) = 1$.

In 1966 M.V. Subbarao [12] proved the following assertion: If $f \in \mathcal{M}$ satisfies

$$(1) \qquad f(n+m) \equiv f(m) \pmod n \quad \text{for all} \quad n,m \in I\!N,$$

then there is a non-negative integer α such that

$$(2) \qquad f(n) = n^{\alpha} \quad \text{for all} \quad n \in I\!N.$$

The research was financially supported by the Hungarian National Foundation for scientific research under grant OTKA T043657.

A. Iványi [3] extended this result proving that if $f \in \mathcal{M}^*$ and (1) holds for a fixed $m \in I\!N$ and for all $n \in I\!N$, then $f(n)$ has also the same form (2). In [9] we improved the results of Subbarao and Iványi mentioned above by proving that if $M \in I\!N$, $f \in \mathcal{M}$ satisfy the conditions $f(M) \neq 0$ and

$$f(n+M) \equiv f(M) \pmod{n} \quad \text{for all} \quad n \in I\!N,$$

then (2) holds. Later, in the papers [5], [7] and [11] we obtained some generalizations of this result, namely we have shown the following theorems:

Theorem A. ([7]) *If the integers $A > 0$, $B > 0$, $C \neq 0$, $N > 0$ with $(A, B) = 1$ and $f \in \mathcal{M}$ satisfy the relation*

$$f(An+B) \equiv C \pmod{n} \quad \textit{for all} \quad n \geq N,$$

then $f(B) = C$ and there are a non-negative integer α, a real-valued Dirichlet character $\chi \pmod{A}$ such that

$$f(n) = \chi(n)n^\alpha \quad \textit{for all} \quad n \in I\!N,\ (n, A) = 1.$$

Theorem B. ([11]) *Let A, B, D be positive integers with conditions*

$$(A, B) = 1 \quad \textit{and} \quad (A, D, 2) = 1.$$

If a function $f \in \mathcal{M}$ and an integer $C \neq 0$ satisfy the congruence

$$f(An+B) \equiv C \pmod{n} \quad \textit{for all} \quad n \in I\!N,\ (n,\ D) = 1,$$

then $f(B) = C$ and there are a non-negative integer α, a real-valued Dirichlet character $\chi \pmod{A}$ such that

$$f(n) = \chi(n)n^\alpha$$

holds for all $n \in I\!N$, $(n, A) = 1$.

Another characterization of n^α by using congruence property was found by A. Iványi [3], namely he proved that if $f \in \mathcal{M}$ satisfies the relation

$$f(n+m) \equiv f(n) + f(m) \pmod{n} \quad \text{for all} \quad n, m \in I\!N, \tag{3}$$

then $f(n)$ is a power of n with positive integer exponent. It is proved in [6] that this result continues to hold even if the relation (3) is valid for all $m \in \mathcal{P}$ instead of for all $m \in I\!N$. Recently in a joint paper with J. Fehér [10] we gave all solutions f of the congruence (3) under the conditions that $f \in \mathcal{M}^*$ and the relation (3) holds for a fixed $m \in \mathbb{N}$ and for all $n \in \mathbb{N}$. For further results and generalizations of this topics we refer to the works [2], [4], [8] and [11].

Our purpose in this paper is to prove the following

Theorem. *Let A, B be positive integers with conditions*

$$(A, B) = 1 \quad \textit{and} \quad (A, 2) = 1.$$

Assume that a function $f \in \mathcal{M}$ and an integer $C \neq 0$ satisfy the congruence

$$f(An + B) \equiv f(An) + C \pmod{n} \quad \textit{for all} \quad n \in \mathbb{N}. \tag{4}$$

We have

(I) If there is a prime power $\pi^e > 1$ such that $(\pi, A) = 1$ and $f(\pi^e) = 0$, then

(a) $\pi = 2$ and $f(An) = -1$ for all $n \in \mathbb{N}$, $(n, 2) = 1$,

(b) $C = 1$ and $f(2^\gamma) = 0$ for all $\gamma \in \mathbb{N}$ in the case $(B, 2) = 1$,

(c)

$$f(2^\gamma) = \begin{cases} 1 & \textit{if } \gamma < \alpha, \\ 2 - f(2^\alpha) & \textit{if } \gamma > \alpha, \end{cases} \quad \textit{and} \quad f(2^\alpha) = \begin{cases} 2 & \textit{if } e > \alpha, \\ 0 & \textit{if } e = \alpha \end{cases}$$

in the case $2^\alpha \parallel B$ with $\alpha \in \mathbb{N}$, furthermore $e \geq \alpha$, $f(A) = -1$, $C = 2$,

(II) If $f(n)f(Am) \neq 0$ for all $n, m \in \mathbb{N}$, $(n, A) = 1$ and

$$|f(n)| = 1 \quad \textit{for all} \quad n \in \mathbb{N}, \qquad n \equiv 1 \pmod{D}$$

holds for some fixed $D \in \mathbb{N}$, then

(i) $f(A) + C = 1$ and $f(An) = f(A)$ for all $n \in \mathbb{N}$ in the case when $f(A^m) \neq -1$ for some $m \in \mathbb{N}$,

(ii) $f(n) = 1$ for all $n \in \mathbb{N}$, $(n, 2A) = 1$ and

$$f\left(2^{\alpha+\gamma}\right) = C - f\left(2^\alpha\right) \quad \textit{for all} \quad \gamma \in \mathbb{N},$$

where $2^\alpha \parallel B$, $\alpha \geq 0$. Furthermore, if $\alpha > 0$, then $C = 2$ and $f(2^\delta) = 1$ for $\delta < \alpha$.

(III) If $f(n)f(Am) \neq 0$ for all $n, m \in \mathbb{N}$, $(n, A) = 1$ and $|f(N)| > 1$ for some $N \in \mathbb{N}, (N, A) = 1$, then there are a non-negative integer α and a real-valued Dirichlet character $\chi \pmod{A}$ such that

$$f(n) = \chi(n) n^\alpha$$

holds for all $n \in \mathbb{N}$, $(n, A) = 1$.

II. The proof of (I)

Lemma 1. *Assume that the conditions of the theorem are satisfied. If there is a prime power $\pi^e > 1$ such that $(\pi, A) = 1$ and $f(\pi^e) = 0$, then*

(a) $\pi = 2 \quad \text{and} \quad f(An) = -1 \quad \text{for all} \quad n \in I\!N, \quad (n,2) = 1.$

(b) *If $(B,2) = 1$, then $C = 1$ and $f(2^\gamma) = 0$ for all $\gamma \in I\!N$.*

(c) *If $2^\alpha \parallel B$ with $\alpha \in I\!N$, then $e \geq \alpha$, $f(A) = -1$, $C = 2$,*

$$f(2^\gamma) = \begin{cases} 1 & \text{if } \gamma < \alpha, \\ 2 - f(2^\alpha) & \text{if } \gamma > \alpha, \end{cases} \quad \text{and} \quad f(2^\alpha) = \begin{cases} 2 & \text{if } e > \alpha, \\ 0 & \text{if } e = \alpha. \end{cases}$$

Proof. Assume that a prime power $\pi^e > 1$ satisfies the conditions $(\pi, A) = 1$ and $f(\pi^e) = 0$. First we prove that

$$f(A) \neq 0. \tag{5}$$

and

$$F(n) := \frac{f(An)}{f(A)} = \chi_\pi(n) \quad \text{for all} \quad n \in I\!N, \ (n,\pi) = 1. \tag{6}$$

It is easy to check that for each prime $P > \max(A, B, \pi^e, |C|)$ one can find positive integers x, y such that $\pi^e x = APy + B$ and $(x, \pi) = (y, AP) = 1$. By (4), we have

$$0 = f(\pi^e) f(x) = f(\pi^e x) = f(APy + B) \equiv f(A) f(P) f(y) + C \pmod{P},$$

which shows (5).

Let n_0 be a positive integer for which $An_0 + B \equiv \pi^e \pmod{\pi^{e+1}}$. We get from (4) that

$$0 = f[A(\pi^{e+1}n + n_0) + B] \equiv f[A(\pi^{e+1}n + n_0)] + C \pmod{\pi^{e+1}n + n_0} \tag{7}$$

holds for all $n \in I\!N$. Let M be any positive integer with $M \equiv 1 \pmod{\pi^{e+1}}$. By (7), for each $n \in I\!N, (\pi^{e+1}n + n_0, AM) = 1$ we have

$$-Cf(AM) \equiv f(AM) f[A(\pi^{e+1}n + n_0)] = f(A)[f(AM) f(\pi^{e+1}n + n_0)] =$$

$$= f(A)f[AM(\pi^{e+1}n+n_0)] \equiv -Cf(A) \pmod{\pi^{e+1}n+n_0}$$

is satisfied . Thus we have shown that

$$(8) \qquad f(AM) = f(A) \quad \text{for all} \quad M \equiv 1 \pmod{\pi^{e+1}}.$$

Repeating the argument used in the proof of Lemma 19.3 of [1], in order to prove (6), we shall deduce from the (5) and (8) that

$$F(n) = F(m) \quad \text{if} \quad n \equiv m \pmod{\pi}, \quad (nm,\pi)=1$$

and

$$F(nm) = F(n)F(m) \quad \text{for all} \quad n,m \in I\!N, \quad (nm,\pi)=1,$$

and so (6) is true.

Indeed, if $(n,\pi)=1$ and $n \equiv m \pmod{\pi}$, then there is a positive integer x for which $nx \equiv mx \equiv 1 \pmod{\pi^{e+1}}$ and $(x,\ Anm)=1$. From (8) we have

$$f(An)f(x) = f(Anx) = f(A) = f(Amx) = f(Am)f(x) \neq 0,$$

therefore $f(An) = f(Am)$.

Now let $n,\ m \in I\!N$ with $(nm,\pi)=1$. Then there are positive integers $u,\ v$ such that $nu \equiv 1 \pmod{\pi^{e+1}}$ and $mv \equiv 1 \pmod{\pi^{e+1}}$ and $(u, Anm) = (v,\ Anmu) = 1$. Therefore, by (8) we get

$$f(A) = f(Anu) = f(An)f(u), \quad f(A) = f(Amv) = f(Am)f(v)$$

and

$$f(A) = f(Anmuv) = f(Anm)f(u)f(v),$$

which imply $f(A)f(Anm) = f(An)f(Am)$. Thus, the proof of (6) is completed.

Assume now that $(\pi,B)=1$. Then for each $\gamma \in I\!N$, by (4) and (6) we have

$$f(A\pi^\gamma n+B) = \frac{1}{f(A)} f[A(A\pi^\gamma n+B)] = \chi_\pi(A\pi^\gamma n+B) = \chi_\pi(B) = f(B),$$

and so

$$f(A\pi^\gamma n) \equiv f(B) - C \pmod{n} \quad \text{for all} \quad n \in I\!N.$$

This with $n \equiv 1 \pmod{A\pi}$, $n \to \infty$ implies

$$f(A\pi^\gamma n) = f(\pi^\gamma)f(An) = f(\pi^\gamma)f(A)\chi_\pi(n) = f(A\pi^\gamma)$$

and
$$f(A\pi^\gamma) = f(B) - C \quad \text{for all} \quad \gamma \in I\!N.$$
This relation with $\gamma = e$ shows that
$$f(\pi^\gamma) = \frac{f(B) - C}{f(A)} = 0 \quad \text{for all} \quad \gamma \in I\!N$$
and so
$$F(n) = \chi_\pi(n) \quad \text{and} \quad F(An+B) \equiv f(A)F(n)+C \pmod n \quad \text{for all} \quad n \in I\!N.$$
Hence, Lemma 1 of [10] gives
$$\pi = 2, \quad f(A) = -1, \quad C = 1, \quad (2, AB) = 1$$
and
$$F(n) = \chi_2(n) \quad \text{for all} \quad n \in I\!N.$$
The part (b) of Lemma 1 is proved.

Next assume that $\pi^\alpha \parallel B$ with $\alpha \in I\!N$. First we note that $e \geq \alpha$. Indeed, if $e < \alpha$, then for all $n \in I\!N$, $(n, \pi) = 1$, we have
$$0 = f(\pi^e) f\Big(An + \frac{B}{\pi^e}\Big) = f(A\pi^e n + B) \equiv$$
$$\equiv f(A\pi^e n) + C = f(\pi^e) f(An) + C = C \pmod n$$
which contradicts to $C \neq 0$.

By (4) and (6), we have
$$f(An + B) = \frac{1}{f(A)} f\left[A(An + B)\right] = \chi_\pi(An + B) =$$
$$= \chi_\pi(A)\chi_\pi(n) \equiv f(A)\chi_\pi(n) + C \pmod n$$
for all $n \in I\!N$, $(n, \pi) = 1$, which implies, similarly as above, that

(9) $$\chi_\pi(n) = 1 \quad \text{and} \quad f(An) = f(A) \quad \text{for all} \quad n \in I\!N,\ (n, \pi) = 1,$$

furthermore

(10) $$f(A) + C = 1.$$

We note from (9) that

$$f(n)=1 \quad \text{for all} \quad n\in I\!N,\ (n,\ A\pi)=1. \tag{11}$$

Let $\gamma>\alpha$ be an integer. Then by (4) and (11) we get

$$f(\pi^\alpha)=f(\pi^\alpha)f\Big(A\pi^{\gamma-\alpha}n+\frac{B}{\pi^\alpha}\Big)=f(A\pi^\gamma n+B)\equiv$$

$$\equiv f(A\pi^\gamma n)+C \pmod n \quad \text{for all} \quad n\in I\!N.$$

This and (11) with $n\to\infty,\ \ (n,A\pi)=1$ implies

$$f(\pi^\gamma)=\frac{f(\pi^\alpha)-C}{f(A)} \quad \text{for all}\ \ \gamma\in I\!N,\ \gamma>\alpha. \tag{12}$$

Let $\delta<\alpha$ be a positive integer. Then by (4) and (11), we infer that

$$f(\pi^\delta)=f(\pi^\delta)f\Big(An+\frac{B}{\pi^\delta}\Big)=f(A\pi^\delta n+B)\equiv$$

$$\equiv f(A\pi^\delta n)+C \pmod n \quad \text{for all} \quad n\in I\!N,\quad (n,\pi)=1.$$

This and (11) with $n\to\infty,\ \ (n,A\pi)=1$ give $f(A\pi^\delta)=f(\pi^\delta)-C$, from which and (10) we get $f(\pi^\delta)=1$ for all $\delta<\alpha$.

Next we shall prove that $f(A)=-1$ and $C=2$. As we have shown above, there is a positive constant K such that $|f(An+B)|<K$, $|f(An)|<K$ for all $n\in I\!N$. Thus

$$|f(An+B)-f(An)-C|<2K+|C|:=G \quad \text{for all} \quad n\in I\!N,$$

consequently

$$f(An+B)=f(A)f(n)+C \quad \text{for all} \quad n\in I\!N,\quad n\ge G,\quad (n,A)=1.$$

By using induction on k, the last relation shows that

$$f\Big(A^kn+B\left(A^{k-1}+\ldots+A+1\right)\Big)=f(A)^kf(n)+C\left[f(A)^{k-1}+\ldots+f(A)+1\right]$$

is valid for all integers $k\in I\!N$, $n>G$, $(n,A)=1$. Therefore this with $n=\pi^e t>G,\ (t,A\pi)=1$ implies that

$$\Big|\ C\left[f(A)^{k-1}+\ldots+f(A)+1\right]\ \Big|\le K \quad \text{for all} \quad k\in I\!N.$$

Since $f(A)$ is an integer and $f(A) \neq 0$, $f(A) \neq 1$, the last relation implies $f(A) = -1$.Therefore it follows from (10) that $C = 2$.

Finally, we prove that $\pi = 2$.

Assume that $\pi \geq 3$. Let $B = \pi^\alpha B'$. Then for each integer $\gamma \geq \alpha$ there is a positive integer N_0 such that $(A\pi^{\gamma-\alpha}N_0 + B',\ \pi) = (N_0,\ \pi) = 1$. Then

$$\left(A\pi^{\gamma-\alpha}(\pi m + N_0) + B',\ A\pi\right) = 1,$$

therefore (11) implies

$$f[A\pi^\gamma(\pi m + N_0) + B] = f\left(\pi^\alpha[A\pi^{\gamma-\alpha}(\pi m + N_0) + B']\right) =$$

$$= f\left(\pi^\alpha\right) f\left(A\pi^{\gamma-\alpha}(\pi m + N_0) + B'\right) = f\left(\pi^\alpha\right).$$

By (4) and (9), we have

$$f\left(\pi^\alpha\right) \equiv f[A\pi^\gamma(\pi m + N_0)] + C = f(\pi^\gamma) f[A(\pi m + N_0)] + C =$$

$$= f(\pi^\gamma) f(A) + C \pmod{\pi m + N_0},$$

which gives

$$f\left(\pi^\alpha\right) = f(\pi^\gamma) f(A) + C \quad \text{for all} \quad \gamma \geq \alpha.$$

This relation with $\gamma = e$ shows that $f\left(\pi^\alpha\right) = C$, therefore $f(\pi^\gamma) = 0$ for all $\gamma \geq \alpha$. But $f\left(\pi^\alpha\right) = C = 2$, which is a contradiction. Thus we have proved that $\pi = 2$.

By applying (12) for the case $\gamma = e > \alpha$, we have

$$0 = f(\pi^e) = \frac{f(\pi^\alpha) - C}{f(A)} = 2 - f(\pi^\alpha),$$

which gives (c).

Lemma 1 is proved.

III. The proof of (III) in the particular case

Lemma 2. *Assume that the conditions of the theorem are satisfied and* $f(n) \neq 0$ *for all* $n \in I\!N$, $(n, A) = 1$. *If there are a prime* $p|A$ *and a non-negative integer* a *such that* $f(Ap^a) = 0$, *then there are a non-negative integer* α *and a real-valued Dirichlet character* $\chi_A \pmod{A}$ *such that*

$$f(n) = \chi_A(n) n^\alpha \quad \textit{for all} \quad n \in I\!N,\ (n, A) = 1.$$

Proof. Assume that there are a prime $p|A$ and a non-negative integer a such that $f(Ap^a)=0$. Let $p^b \parallel A$.

By (4), we have

$$f(Ap^a n+B) \equiv f(Ap^a n)+C=C \pmod{n} \quad \text{for all} \quad n \in I\!N,\ (n,p)=1.$$

Since $(A,B)=(p,2)=1$, this relation with Theorem B implies that there are a non-negative integer α and a real-valued Dirichlet character $\chi_{Ap^a} \pmod{Ap^a}$ such that

$$(13)\quad f(n)=\chi_{Ap^a}(n)n^\alpha \quad \text{for all} \quad n \in I\!N,\ (n,A)=1 \quad \text{and} \quad f(B)=C \neq 0.$$

First we consider the case when $\alpha=0$. We shall prove that in this case

$$(14)\qquad f(Am+1)=f(Am)+1$$

and

$$(15)\qquad f(Ap^a m)=0$$

hold for all $m \in I\!N$.

Let m is a positive integer. Then by (13) we get that

$$f(Amn+B)=f(Am+B) \quad \text{and} \quad f(Amn)+C=f(Am)f(n)+C=f(Am)+C$$

hold for all $n \in I\!N$, $n \equiv 1 \pmod{Ap^a}$, which with (4) proves that $f(Am+$ $+B)=f(Am)+C$ for all $m \in I\!N$. It clear that (14) follows directly from this relation and (13). Since $f(B)=f(Ap^a m+B)=f(Ap^a m)+C=f(Ap^a m)+$ $+f(B)$, we have $f(Ap^a m)=0$ and so (15) is proved.

Next we show

$$(16)\qquad f(An)=0 \quad \text{for all} \quad n \in I\!N.$$

To see (16), first we consider the case when $b \geq a$. By using (13) and (14) we have

$$[f(An)+1][f(Akn)+1]=f(An+1)f(Akn+1)=f\Big[An\,(Akn+k+1)\Big]+1,$$

and so

$$(17)\qquad f\Big[An\,(Akn+k+1)\Big]=f(An)f(Akn)+f(Akn)+f(An)$$

are satisfied for all $k,\ n \in I\!N$. By taking $k \equiv -1 \pmod{p^a}$ in (17), one can deduce from (15) that

$$f(An)f(Akn) + f(Akn) + f(An) = f\Big[An\,(Akn + k + 1)\Big] = 0$$

for all $n \in I\!N$. Therefore

$$f(AN)f(AkN)f(n)^2 + [f(AN) + f(AkN)]f(n) = 0$$

and so

$$f(AN)f(AkN)f(n) + f(AN) + f(AkN) = 0$$

holds for all $N, n \in I\!N$, $(n, A) = 1$. Hence we have used the fact $f(n) \neq 0$ for all $n \in I\!N, (n, A) = 1$. If $f(AN) + f(AkN) \neq 0$, then $f(AN)f(AkN) \neq 0$, consequently $f(n) = 1$ for all $n \in I\!N$, $(n, A) = 1$. Thus (16) follows from (14). If $f(AN) + f(AkN) = 0$, then $f(AN)f(AkN) = f(AN) + f(AkN) = 0$, therefore

$$f(AN) = 0 \quad \text{for all} \quad N \in I\!N.$$

Thus (16) is proved for $b \geq a$.

Let now $b < a$. In order to see (16) it is enough to prove that $f(Ap^{a-b}) = 0$. By taking $n = p^{a-b}t$, $(t, A) = 1$ and $k \equiv -1 \pmod{p^b}$, we have $Ap^a | An\,(Akn + k + 1)$, therefore by (15) and (17) we get

$$f(Ap^{a-b})f(Akp^{a-b})f(t) + f(Ap^{a-b}) + f(Akp^{a-b})] = 0,$$

which, as above, implies that either (16) or $f(Ap^{a-b}) = 0$. The proof of (16) is finished. Therefore Lemma 2 follows from (4), (16) and Theorem A.

Now we consider the case when $\alpha > 0$. Let $f(n) := \mathcal{F}(n)n^\alpha$ for all $n \in I\!N$. It is clear that $\mathcal{F} \in \mathcal{M}_A^*$ and $\mathcal{F}(n) = \chi_{Ap^\alpha}(n)$ for all $n \in I\!N, (n, A) = 1$. We infer from (4) that $\mathcal{F}(An + B)B^\alpha \equiv C \pmod{n}$, therefore

$$\mathcal{F}(Am + B)B^\alpha = \mathcal{F}(Amn + B)B^\alpha \equiv C \pmod{n}$$

holds for all $n \in I\!N, n \equiv 1 \pmod{Ap^\alpha}$. This shows that $\mathcal{F}(Am + B)B^\alpha = = C = f(B) = \mathcal{F}(B)B^\alpha$, consequently $\mathcal{F}(Am + B) = \mathcal{F}(B)$ for all $m \in I\!N$. Hence we have $\mathcal{F}(n) = \chi_A(n)$ for some real-valued Dirichlet character (mod A).

Lemma 2 is proved.

IV. The proof of (II)

Lemma 3. *Assume that the conditions of the theorem are satisfied, furthermore*

$$f(n) \neq 0 \quad \text{for all} \quad n \in I\!N, \quad (n, A) = 1. \tag{18}$$

and

$$f(An) \neq 0 \quad \text{for all} \quad n \in I\!N. \tag{19}$$

If there is a positive integer D such that

$$|f(n)| = 1 \quad \text{for all} \quad n \in I\!N, \quad n \equiv 1 \pmod{D},$$

then the following assertions hold:
(i) If $f(A^m) \neq -1$ for a some $m \in I\!N$, then $f(A) + C = 1$,

$$f(An) = f(A) \;\; \text{for all} \;\; n \in I\!N$$

and

$$f(n) = 1 \;\; \text{for all} \;\; n \in I\!N, \; (n, A) = 1.$$

(ii) If $f(A^m) = -1$ for all $m \in I\!N$, then

$$f(n) = 1 \;\; \text{for all} \;\; n \in I\!N, \; (n, 2A) = 1,$$

and

$$f\left(2^{\alpha+\gamma}\right) = C - f\left(2^{\alpha}\right) \quad \text{for all} \;\; \gamma \in I\!N,$$

where $2^\alpha \parallel B$, $\alpha \geq 0$. Furthermore, if $\alpha > 0$, then $C = 2$ and $f(2^\delta) = 1$ for $\delta < \alpha$.

Proof. First we note that if $|f(n)| = 1$ for all $n \in I\!N$, $\quad n \equiv 1 \pmod{D}$, then

$$|f(n)| = 1 \quad \text{for all} \quad n \in I\!N, \quad (n, \;\; D) = 1, \tag{20}$$

Since $(A, B) = 1$, there is $N_0 \in I\!N$ satisfying the following relations $(2AN_0 + B, \; D) = 1$ and $(N_0, D) = 1$. Then for all $m \in I\!N$, $\;m \equiv 1 \pmod{D}$, we have $(2AN_0m + B, D) = (2AN_0 + B, \; D) = 1$, therefore from (4) and (20), one can infer that

$$1 = f(2AN_0m + B)^2 \equiv \Big[f\left(2AN_0m\right) + C\Big]^2 \equiv$$

$$\equiv f(2AN_0m)^2 + 2Cf(2AN_0m) + C^2 =$$

$$= f(2AN_0)^2 + 2Cf(2AN_0m) + C^2 \pmod{m},$$

consequently

$$f(2AN_0m) \equiv 1 - C^2 - f(2AN_0)^2 \pmod{m}$$

holds for all $m \in I\!N$, $m \equiv 1 \pmod{D}$. Since C and $f(2AN_0)$ are non-zero integers, we have $1 - C^2 - f(2AN_0)^2 \neq 0$. As we have seen in the proof of (8) in Lemma 1, the above congruence implies that $f(2AN_0m) = f(2AN_0)$ for all $m \in I\!N$, $m \equiv 1 \pmod{D}$. On the other hand, this relation also holds for all N_0 satisfying $(2AN_0 + B, D) = (N_0, D) = 1$ and for all $m \in I\!N$, $m \equiv 1 \pmod{D}$. Hence we have

$$f(2Am) = f(2A) \text{ for all } m \in I\!N, \quad m \equiv 1 \pmod{D},$$

consequently

(21) $$f(n) = \chi_{2AD}(n) \text{ for all } (n, 2AD) = 1$$

where χ_{2AD} is a suitable real-valued character $\pmod{AD}$.

By taking $n = 2DLt$ in (4), where $L, t \in I\!N$, $t \equiv 1 \pmod{2AD}$, we get from (21) that

$$f(B) = f(B)f(2ADLt + 1) = f(2ABDLt + B) \equiv$$

$$\equiv f(2ABDLt) + C = f(2ABDL)f(t) + C = f(2ABD) + C \pmod{t},$$

consequently

$$f(2ABDL) = f(B) - C = f(2ABD) \quad \text{for all} \quad L \in I\!N.$$

This with (21) shows that

$$|f(n)| < K \quad \text{for all} \quad n \in I\!N,$$

where K is some constant. Thus from (4) we infer that

(22) $$f(An + B) = f(An) + C \quad \text{for all} \quad n \in I\!N, \quad n > G := 2K + |C|.$$

First we get easily from (22) that

(23) $$f(A^m n + B) = f(A^m n) + C \quad \text{for all} \quad n \in I\!N, \quad n > G,$$

and

$$f\Big((A^m)^k n + B\left((A^m)^{k-1} + \ldots + A^m + 1\right)\Big) = \tag{24}$$

$$= \left(f(A^m)\right)^{k-1} f(A^m n) + C\left[\left(f(A^m)\right)^{k-1} + \ldots + f(A^m) + 1\right]$$

are valid for all integers $k, m, n \in I\!N$, $n > G$.

If $f(A^m) \neq -1$ for some positive integer m. Since $|f(n)| < K$ for all $n \in I\!N$, therefore (24) implies

$$\left|\frac{f(A^m)^{k-1}[(f(A^m)-1)f(A^m n) + Cf(A^m)] - C}{f(A^m) - 1}\right| \leq K$$

for all $k, n \in I\!N$, $n > G$, and so

$$f(A^m n) = \frac{Cf(A^m)}{1 - f(A^m)}$$

holds for all $n \in I\!N, n > G$. One can easily check from this relation that $f(A^m n) = f(A^m)$ also satisfied for all $n \in I\!N$. Hence $f(n) = 1$ for all $n \in$ $\in I\!N$, $(n, A) = 1$, which with (22) shows that $f(An) = C - f(An + B) = C - 1$ for all $n \in I\!N$, $n > G$, consequently $f(An) = f(A)$ for all $n \in I\!N$. Thus the part (i) of Lemma 3 is proved.

To complete the proof of Lemma 4, it remains to consider the case when

$$f(A^m) = -1 \quad \text{for all} \quad m \in I\!N. \tag{25}$$

In this case, applying (24) with $k = 2$, we have

$$f\Big(A^{2m} n + B\left(A^m + 1\right)\Big) = -f(A^m n) \tag{26}$$

for all integers $m, n \in I\!N$, $n > G$. Let

$$\mu := \begin{cases} 1 & \text{if } 2 \mid B \\ 2 & \text{if } 2 \nmid B \end{cases} \quad \text{and} \quad R_m := A^m + 1 \quad (m \in I\!N).$$

Since $(A, 2) = 1$, for each positive integer m there is a positive integer t_m such that $(R_m, A^{2m} t_m + B) = (R_m, t_m + B) = 1$, $(AR_m, t_m) = \mu$ and $(AR_m, \frac{t_m}{\mu}) = 1$. By considering $n = R_m\left(AR_m t + t_m\right)$ and taking into account (26), it follows from (25) that

$$f(R_m) f\left[A^{2m}\left(AR_m t + t_m\right) + B\right] = \frac{f\left(\mu R_m\right)}{f(\mu)} f\left(AR_m t + t_m\right)$$

for all $m, t \in I\!N$, $t > G$. This combined with (22) and (25) implies

$$\left[\frac{f(\mu R_m)}{f(R_m)f(\mu)} + 1\right] f(AR_m t + t_m) = C$$

for all $m, t \in I\!N$, $t > G$. Hence we get from Lemma 19.3 of [1] that

$$f \in \mathcal{M}^*{}_{AR_m} \ \text{ and } \ f(n) = \chi_{AR_m}(n) \ \text{ for all } \ n, m \in I\!N, (n, AR_m) = 1.$$

Since $(R_1, R_2) = (A+1, A^2+1) = 2$, the above relation gives

$$(27) \qquad f \in \mathcal{M}^*{}_{2A} \ \text{ and } \ f(n) = \chi_{2A}(n) \ \text{ for all } \ n \in I\!N, (n, 2A) = 1.$$

Let $2^\alpha \parallel B$. Applying (22) and (27) with $n = 2^{\alpha+\gamma}m,\ \gamma \geq 1$, we have

$$f\left(2^{\alpha+\gamma}Am\right) = f\left[2^\alpha\left(2^\gamma Am + \frac{B}{2^\alpha}\right)\right] - C = f(2^\alpha) f\left(\frac{B}{2^\alpha}\right) - C$$

for all $m \in I\!N$. This shows that

$$f(n) = 1 \ \text{ for all } \ n \in I\!N,\ (n, 2A) = 1$$

and

$$f\left(2^{\alpha+\gamma}\right) = C - f\left(2^\alpha\right) \quad \text{for all} \ \ \gamma \in I\!N.$$

Finally, we consider the case when $\alpha > 0$. In this case we have $(A+B, 2) = 1$, and so $1 = f(A+B) = f(A) + C = -1 + C$, which gives $C = 2$. If $\delta < \alpha$, then $f(2^\delta) = f(A2^\delta + B) = f(A2^\delta) + C = -f(2^\delta) + 2$, consequently $f(2^\delta) = 1$. Thus the part (ii) of Lemma 3 is proved.

The proof of Lemma 3 is completed.

V. The proof of (III). Lemmas

Lemma 4. *Assume that the conditions of the theorem are satisfied and there are a prime π, infinitely many positive integers $\alpha_1 < \alpha_2 < \dots$ and $\beta_1 < \beta_2 < \dots$ such that*

$$\pi^{\beta_i} \parallel f(\pi^{\alpha_i}) \quad (i = 1, 2, \dots).$$

Then

$$f(B) = C \ \text{ and } \ f \in \mathcal{M}^*{}_{A\pi}.$$

Proof. We assume that a prime π and the sequences $\{\alpha_k\}_{k=1}^{\infty}$, $\{\beta_k\}_{k=1}^{\infty}$ of positive integers satisfy $\pi^{\beta_i} \parallel f(\pi^{\alpha_i}) \quad (i=1,2,\ldots)$.

Let $\pi^\alpha \parallel A,\ \pi^\beta \parallel B$ and $A=\pi^\alpha A',\ B=\pi^\beta B'$. Since $\alpha_1<\alpha_2<\ldots$, we can assume that $\alpha_i-\beta_i>\alpha+\beta$ for all $i>i_0$.

Let $n,\ m\in I\!N,\ (nm,\ A\pi)=1$. It is easy to check from the Chinese Remainder Theorem that for all positive integers $i>j$ with $\alpha_j>\alpha+\beta$, there are $x,\ y,\ u$ and v such that

$$nx=A\pi^{\alpha_i-\alpha-\beta}y+1,\quad (x,\ nmB)=1,\ \ (y,\ \pi)=1,$$

and

$$mu=Av\pi^{\alpha_j-\alpha}+B,\quad (u,\ nmx)=1,\ \ (v,\ \pi)=1.$$

Therefore, by (4), we get

$$f(nB)f(x)=f(nxB)\equiv f(AB\pi^{\alpha_i-\alpha-\beta}y)+C=$$

$$=f(A'B'y)f(\pi^{\alpha_i})+C\equiv C \bmod \pi^{\beta_i},$$

$$f(m)f(u)=f(mu)\equiv f(Av\pi^{\alpha_j-\alpha})+C=f(A'v)f(\pi^{\alpha_j})+C\equiv C \pmod{\pi^{\beta_j}},$$

and

$$f(nm)f(x)f(u)=f(nmxu)\equiv$$

$$\equiv f\Big[A\pi^{\alpha_j-\alpha}\left(A\pi^{\alpha_i-\alpha-\beta}yv+B\pi^{\alpha_i-\alpha_j-\beta}y+v\right)\Big]+C\equiv C \pmod{\pi^{\beta_j}},$$

consequently

$$f(nB)f(m)\equiv Cf(nm) \pmod{\pi^{\beta_j}}.$$

This shows that

$$f(nB)f(m)=Cf(nm)$$

holds for all $n,\ m\in I\!N,\ (nm,A\pi)=1$. Thus $f(B)=C$ and

$$f(nm)=f(n)f(m)\quad \text{for all}\quad n,\ m\in I\!N,\ (nm,A\pi)=1.$$

Lemma 4 is proved.

Lemma 5. *Assume that a multiplicative function f satisfies the condition $f(n)\neq 0$ for all $n\in I\!N$ and H is a positive integer. If the relations*

(28) $$f(H(k+1))f(Hk(k+1))=f(H(k+1)^2)f(Hk)$$

and

(29) $$f(H(k+1)) + f(Hk(k+1)) = f(H(k+1)^2),$$

hold for all $k \in I\!N$, *then*

(30) $$f(Hn) = nf(H) \quad \textit{holds for all} \quad n \in I\!N.$$

Proof. It is obvious that (30) holds for $n = 1$. From (28) and (29) we have

(31) $$f(H(k+1))f(Hk(k+1)) = [f(H(k+1)) + f(Hk(k+1))]\, f(Hk),$$

which with $k = 1$ proves (30) for $n = 2$.

Assume that (30) is true for all $n < N$, where $N \geq 3$. Since $f \in \mathcal{M}$ and $(N-1, N) = 1$, one can check from our assumption that

$$f(H(N-1)N) = \frac{f(H(N-1))f(HN)}{f(H)} = (H-1)f(HN).$$

Applying (31) with $k = N-1$, we infer from the last relation that

$$f(HN)(N-1)f(HN) = [f(HN) + (N-1)f(HN)]\,(N-1)f(H).$$

Hence $f(HN) = Nf(H)$ and so Lemma 5 is proved.

VI. The proof of the Theorem.

Assume that $f(n) \neq 0$ and $f(Am) \neq 0$ for all $n, m \in I\!N$, $(n, A) = 1$ and $|f(N)| > 1$ for a some $N \in I\!N, (N, A) = 1$.

For each $k \in I\!N$, $k > 1$ let $P = P(k)$ be a positive integer for which $2|ABkP(k)$ and let $\mathcal{H} := \mathcal{H}(k, P)$ denote the set of those $n \in I\!N$ which subjected to the following properties:

(32) $$\begin{cases} (ABkPn+1, k+1) = 1, \\ (2ABkPn+1, k-1) = 1, \\ (n, ABk(k^2-1)P) = 1. \end{cases}$$

An application of the Chinese Remainder Theorem and the definition of $P(k)$ shows that $\mathcal{H} \neq \emptyset$.

For each $n \in \mathcal{H}$, by (4) we have

$$f(B)f(AB(k+1)Pn+1)f(AB^2k(k+1)Pn+B) =$$

$$= f(AB^2(k+1)Pn+B)f(AB^2k(k+1)Pn+B) \equiv$$

$$\equiv \left[f(AB^2(k+1)P)f(n)+C\right]\left[f(AB^2k(k+1)P)f(n)+C\right] =$$

$$= f(AB^2(k+1)P)f(AB^2k(k+1)P)f(n)^2 +$$

$$+Cf(AB^2k(k+1)P)f(n)+Cf(AB^2(k+1)P)f(n)+C^2 \pmod{n},$$

and

$$f(B)f(AB(k+1)Pn+1)f(AB^2k(k+1)Pn+B) =$$

$$= f(B)f\Big(AB^2(k+1)^2Pn(ABkPn+1)+B\Big) \equiv$$

$$\equiv f(AB^2(k+1)^2P)f(AB^2kP)f(n)^2+Cf(AB^2(k+1)^2P)f(n)+Cf(B) \pmod{n}.$$

These imply

(33) $$Xf(n)^2+Yf(n) \equiv C^2 - Cf(B) \pmod{n} \quad \text{for all} \quad n \in \mathcal{H},$$

where

$$X = X(k,P) = f(AB^2(k+1)P)f(AB^2k(k+1)P) - f(AB^2(k+1)^2P)f(AB^2kP)$$

and

$$Y = Y(k,P) = Cf(AB^2k(k+1)P) + Cf(AB^2(k+1)P) - Cf(AB^2(k+1)^2P).$$

Let $D = D(k,P) = AB^4k(k^2-1)P$. It is clear that

$$nm \in \mathcal{H} \quad \text{for all} \quad n \in \mathcal{H} \quad \text{for all} \quad m \equiv 1 \pmod{D}.$$

Thus, by the above relation we get

$$Xf(n)^2f(m)^2+Yf(n)f(m) \equiv C^2 - Cf(B) \pmod{n},$$

consequently

(34) $$[f(m)^2 - f(m)]Yf(n) \equiv (C^2 - Cf(B))[f(m)^2-1] \pmod{n}$$

for all $n \in \mathcal{H}$ and for all $m \equiv 1 \pmod{D}$, $(n, m) = 1$.

If $f(m)^2-1=0$ for all $m\equiv 1 \pmod D$, then we get a contradiction by using Lemma 3 and the fact $|f(N)|>1$. Therefore there is an $m\in I\!N$ such that $m\equiv 1 \pmod D$, and $[f(m)^2-1][f(m)^2-f(m)]\neq 0$. If $C\neq f(B)$, then $Y\neq 0$ and there are infinitely many $n\in\mathcal{H}$ such that $(n,m)=1$. It follows from (34) that

$$(C^2-Cf(B))[f(m)^2-1]f(m)\equiv[f(m)^2-f(m)]Yf(n)f(m)\equiv$$

$$\equiv(C^2-Cf(B))[f(m)^2-1] \pmod n,$$

which shows that $f(m)=1$, which is impossible.

Assume now that $C=f(B)$. Then we get from (34) that

$$[f(m)^2-f(m)]Yf(n)\equiv 0 \pmod n \ \text{ for all } \ n\in\mathcal{H}. \tag{35}$$

If $Y\neq 0$, then we infer from (35) that there are primes $\pi_1,\pi_2\in\mathcal{H}$, $\pi_1\neq\pi_2$ and

$$[f(m)^2-f(m)]Yf(\pi_i^{\varphi(D)t+1})\equiv 0 \pmod{\pi_i^{\varphi(D)t+1}} \ \text{ for all } \ t\in I\!N$$

hold for $i=1,2$. Hence, Lemma 4 implies that $f\in\mathcal{M}_A^*$.

Repeating the argument used above, using the fact $f\in\mathcal{M}_A^*$, one can deduce that

$$[f(m)^2-f(m)]Yf(n)\equiv 0 \pmod n \ \text{ for all } \ n\in I\!N,\ (n,A)=1.$$

Since $[f(m)^2-f(m)]Y\neq 0$, this congruence shows that $f(n)\equiv 0 \pmod n$ for all $n\in I\!N$, $(n,A)=1$. The proof of (III) follows from (4) and Theorem B.

Finally, assume that $C=f(B)$ and $Y=0$. Then we get from (33) that $Xf(n)^2\equiv 0 \pmod n$ for all $n\in\mathcal{H}$. Similarly as above, the proof of Theorem is finished for the case when $X\neq 0$. Now let $X=Y=0$. Then Lemma 5 shows that

$$f(2AB^2n)=nf(2AB^2) \ \text{ for all } \ n\in I\!N.$$

This combined with Lemma 4 implies $f\in\mathcal{M}_A^*$, consequently $f(An)= = nf(A)$ for all $n\in I\!N$ and $f(n)=n$ for $n\in I\!N, (n,A)=1$.

Theorem is proved.

References

[1] **Elliott P.D.T.A.,** *Arithmetic functions and integers products*, Grund. der Math. Wiss. **272**, Springer, 1985.

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

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

[4] **Joó I.,** Arithmetical functions satisfying a congruence property, *Acta Math. Hungar.,* **63** (1994), 1-21.

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

[6] **Phong B.M.,** Multiplicative functions satisfying a congruence property, *Periodica Math. Hungar.,* **26** (1991), 123-128.

[7] **Phong B.M.,** Multiplicative functions satisfying a congruence property V., *Acta Math. Hungar.,* **62** (1993), 81-87.

[8] **Phong B.M.,** Quasi multiplicative functions with congruence property, *Acta Acad. Paed. Agriensis, Sect. Math.,* **25** (1998), 55-59.

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

[10] **Phong B.M. and Fehér J.,** Note on multiplicative functions satisfying congruence property II., *Math. Pannon.,* **10** (1) (1999), 133-138.

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

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

Bui Minh Phong
Department of Computer Algebra
Eötvös Loránd University
Pázmány Péter sét. 1/C
H-1117 Budapest, Hungary
bui@compalg.inf.elte.hu