Acta Sci. Math., 55 (1991), 301—307

Note on multiplicative functions satisfying a congruence property

I. JOÓ

1. An arithmetical function $f(n)\neq 0$ is said to be multiplicative if $(n, m)=1$ implies

$$f(nm)=f(n)f(m)$$

and it is called completely multiplicative if the above equation holds for all pairs of positive integers n and m. In the following let $\mathcal{M}$ and $\mathcal{M}^*$ denote the set of integer-valued multiplicative and completely multiplicative functions, respectively.

In 1966 M. V. SUBBARAO [3] proved that if $f\in\mathcal{M}$ and f satisfies the relation

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

for every positive integers n and m, then $f(n)$ is a power of n with non-negative integer exponent. In 1972 A. IVÁNYI [1] showed that if $f\in\mathcal{M}^*$ and (1) holds for a fixed m and every n, then $f(n)$ also has the same form. Recently, B. M. PHONG and J. FEHÉR [2] extended the results of Subbarao and Iványi mentioned above, proving that if $f\in\mathcal{M}$ and (1) holds for a fixed m with $f(m)\neq 0$ and for every positive integer n, then there is a non-negative integer a such that

$$f(n)=n^a \quad (n=1, 2, \ldots).$$

In this paper we shall give a characterization of those elements $f\in\mathcal{M}$ which satisfy

$$f(pn+M)\equiv f(M) \pmod{n}$$

for every positive integer n, where p is a fixed prime, M is a fixed positive integer with the conditions $(p, M)=1$ and $f(M)\neq 0$.

We prove the following

Theorem. *Let p be a prime, M be a positive integer for which $(p, M)=1$. Moreover let $f\in\mathcal{M}$ with $f(M)\neq 0$. If f satisfies the relation*

$$f(pn+M)\equiv f(M) \pmod{n} \tag{2}$$

Received August 11, 1989 and in revised form January 30, 1990.

for every positive integer n, then either

$$f(n) = n^a \tag{3}$$

or

$$f(n) = \left(\frac{n}{p}\right) \cdot n^a \tag{4}$$

for all positive integers n which are prime to p, where $a \geqq 0$ *is an integer and* $\left(\frac{n}{p}\right)$ *denotes the Legendre symbol.*

Example. All solutions $f \in \mathcal{M}$ of the following congruence

$$f(5n+1) \equiv 1 \pmod{n} \quad (n = 1, 2, \ldots)$$

are

$$f(n) = n^a \quad \text{for all } n \text{ prime to } 5$$

or

$$f(n) = \left(\frac{n}{5}\right) n^a = \begin{cases} n^a & \text{if } n \equiv \pm 1 \pmod 5 \\ -n^a & \text{if } n \equiv \pm 2 \pmod 5, \end{cases}$$

where a is a non-negative integer.

2. Lemmas

Lemma 1. *Assume that p, M and f satisfy the conditions of Theorem and* (2) *holds for every positive integer n. If Q is a prime for which* $(Q, pM) = 1$, *then*

$$f(Q^k) = f(Q)^k \quad (k = 1, 2, \ldots). \tag{5}$$

Proof. Let Q be a prime with $(Q, pM) = 1$. We prove (5) by induction on k.

It is obvious that (5) holds for $k = 1$. Assume that (5) is true for k and prove it for $k+1$, and (5) will be proved.

Let q be a prime for which

$$q > QM|f(M)|. \tag{6}$$

Then there exist positive integers x and y such that

$$Q^k x = 1 + pqy \quad \text{and} \quad (x, QM) = 1.$$

Applying (2) with $n = qyM$, we get

$$f(Q^k)f(x)f(M) = f(Q^k xM) = f(M + pqyM) \equiv f(M) \pmod q,$$

which with (6) implies

$$f(Q^k)f(x) \equiv 1 \pmod q. \tag{7}$$

On the other hand, using the fact $(QM, pxq)=1$ we can choose positive integers u and v such that

$$Qu = M+pxqv \quad \text{and} \quad (u, Q) = 1.$$

Then, we have

$$f(Q^{k+1})f(xu) = f(Q^{k+1}xu) = f[Q^k x)(Qu)] =$$
$$= f[Q^k x(M+pxqv)] = f[MQ^k x+px^2qvQ^k] =$$
$$= f\big(M+pq(My+x^2vQ^k)\big) \equiv f(M) \pmod q$$

and

$$f(Q)f(xu) = f(Qxu) = f[x(M+pxqv)] = f(x)f(M+pxqv) \equiv fx)f(M) \pmod q.$$

These give

$$f(Q^{k+1})f(x)f(M) \equiv f(Q)f(M) \pmod q$$

which, using (6), implies

$$f(Q^{k+1})f(x) \equiv f(Q) \pmod q. \tag{8}$$

From (7) we get that $f(x)\not\equiv 0 \pmod q$, and so (7) and (8) imply that

$$f(Q^{k+1}) \equiv f(Q^k)f(Q) \pmod q.$$

This shows that

$$f(Q^{k+1}) = f(Q^k)f(Q) = f(Q)^{k+1},$$

since there are infinitely many primes q satisfying (6). Thus (5) is proved for $k+1$. Lemma 1 is proved.

Lemma 2. *Assume that p, M and f satisfy the conditions of Theorem and* (2) *holds for every positive integer n. Then there exists a non-negative integer a such that*

$$|f(n)| = n^a \tag{9}$$

for all positive integers n which are prime to p.

Proof. We first prove that there exists a non-negative integer a such that

$$|f(n)| = n^a \quad \text{if} \quad (n, pM) = 1. \tag{10}$$

In order to prove (10) it is enough to show that

$$f(Q) = \pm Q^{a(Q)} \tag{11}$$

for each prime Q coprime to pM, where $a(Q)\geqq 0$ is an integer, furthermore if P, Q are distinct primes with $(PQ, pM)=1$, then

$$a(P) = a(Q). \tag{12}$$

Let Q be a prime for which $(Q, pM)=1$. Assume that there is a prime $q\neq Q$ and $q|f(Q)$. Then, by Lemma 1, we have

$$q^s|f(Q)^s = f(Q^s) \quad (s = 1, 2, \ldots). \tag{13}$$

For each positive integers s there are positive integers $t=t(s)$ and $h=h(s)$ such that

$$Q^s t = M + pq^s h, \quad (Q, t) = 1.$$

Then we get from (2) and (13) that

$$0 \equiv f(Q^s)f(t) = f(Q^s t) = f(M + pq^s h) \equiv f(M) \pmod{q^s},$$

holds for every s, which implies $f(M)=0$. This is a contradiction and so (11) holds.

Now let P, Q be distinct primes for which $(PQ, pM)=1$. Then, by using (11) we have

$$f(P) = \pm P^{a(P)}, \quad f(Q) = \pm Q^{a(Q)}.$$

Assume that $a(P) \geqq a(Q)$ and let $d=a(P)-a(Q)$. Since p is a prime and $(PQ, p)=1$, we have

$$(PQ^s)^{2(p-1)} \equiv 1 \pmod{p} \quad (s = 1, 2, \ldots)$$

and so we get from (2) that

$$f(M) \equiv f[(PQ^s)^{2(p-1)}M] = f(P)^{2(p-1)}f(Q)^{2s(p-1)}f(M) =$$

$$= P^{2d(p-1)}(PQ^s)^{2(p-1)a(Q)}f(M) \equiv P^{2d(p-1)}f(M) \mod \left(\frac{(PQ^s)^{2(p-1)}-1}{p}\right)$$

holds for every positive integer s, consequently

$$P^{2d(p-1)}f(M) = f(M)$$

This shows that $d=a(P)-a(Q)=0$, which implies (12). From (11) and (12) it follows that (10) holds.

Now we prove (9).

By using (10), in order to prove (9) it is enough to show that

$$|f(q^k)| = q^{ka} \quad (k = 1, 2, \ldots) \tag{14}$$

holds for all prime divisors q of M, where a is a non-negative integer determined in (10).

Let m be a positive integer for which

$$(m, pM) = 1. \tag{15}$$

Then we have $(pm+M, pM)=1$ and so from (2) and (10) we get

$$f(M) \equiv f(M+pm) = \pm(M+pm)^a \equiv \pm M^a \pmod{m},$$

which, as $m \to \infty$ with $(m, M)=1$, implies that

$$|f(M)| = M^a, \tag{16}$$

where a is an integer given in (10).

Let q be a prime divisor of M and $q^{k_0} \| M$. Let $k \leqq k_0$. Then there exist infinitely many positive integers m such that

$$\left(pm + \frac{M}{q^k}, pM\right) = 1.$$

For these m using (2) and (10), we have

$$f(M) \equiv f(pq^k m + M) = f(q^k) f\left(pm + \frac{M}{q^k}\right) = \pm f(q^k)\left(pm + \frac{M}{q^k}\right)^a \equiv$$

$$\equiv \pm f(q^k)\left(\frac{M}{q^k}\right)^a \pmod{m},$$

which implies

$$f(M) = \pm f(q^k)\frac{M^a}{q^{ka}}. \tag{17}$$

Thus, by (16) and (17), it follows that (14) holds for $k \leqq k_0$.

Now let $k > k_0$. Then there exists a prime $Q_0 = Q_0(k)$ such that

$$q^{k-k_0} Q_0 \equiv 1 \pmod{p}, \quad (Q_0, pM) = 1. \tag{18}$$

From (2), (10) and (18) we get that

$$f(M) \equiv f[q^{k-k_0} Q_0^{1+(p-1)t} M] = f(Q_0)^{1+(p-1)t} f(q^{k-k_0} M) =$$

$$= \pm Q_0^{a(1+(p-1)t)} f(q^{k-k_0} M) \left(\mod \frac{q^{k-k_0} Q_0^{1+(p-1)t} - 1}{p}\right)$$

holds for every positive integer t. Thus, we have

$$f(q^{k-k_3} M) = \pm q^{a(k-k_3)} f(M),$$

which, using the fact that (14) holds for every positive integer $k \leqq k_0$, implies that

$$f(q^k) = \pm q^{a(k-k_0)} f(q^{k_0}) = \pm q^{ak}.$$

It follows that (14) holds for every positive integer $k > k_0$, and this completes the proof of Lemma 2.

Lemma 3. *Assume p, M and f satisfy the conditions of Theorem and* (2) *holds for every positive integer n. Then we have*

$$f(nM) = n^a f(M)$$

for each quadratic residue $n \pmod{p}$, i.e. for $\left(\frac{n}{p}\right) = 1$, where a is the same integer as in Lemma 2.

Proof. Assume that $(n,p)=1$ and $\left(\frac{n}{p}\right)=1$, i.e. the quadratic congruence

$$z^2 \equiv n \pmod{p}$$

is solvable. It is clear that there exists a prime $Q_1=Q_1(n)$ such that

$$nQ_1^2 \equiv 1 \pmod{p} \quad \text{and} \quad (Q_1, pM) = 1. \tag{19}$$

Let $s(t)=1+(p-1)t$. Then, from (2) and (19) we get that

$$f(nQ_1^{2s(t)}M) \equiv f(M)\left(\mathrm{mod}\,\frac{nQ_1^{2s(t)}-1}{p}\right) \tag{20}$$

holds for every positive integer t. Since $(Q_1, pM)=1$, from Lemmas 1 and 2 we have

$$f(nQ_1^{2s(t)}M) = f(Q_1)^{2s(t)}f(nM) = Q_1^{2as(t)}f(nM)$$

which with (19) implies that

$$n^a f(M) \equiv n^a Q_1^{2as(t)} f(nM) \left(\mathrm{mod}\,\frac{nQ_1^{2s(t)}-1}{p}\right)$$

holds for every positive integer t. The last congruence shows that

$$f(nM) = n^a f(M)$$

since $nQ_1^{2s(t)}-1 \to \infty$ as $t \to \infty$. Thus, Lemma 3 is proved.

3. Proof of Theorem

Assume that p, M and f satisfy the conditions of Theorem and (2) holds for every positive integer n. At first we obtain from Lemma 2 that

$$f(n) = \pm n^a \quad \text{if} \quad (n,p) = 1, \tag{21}$$

where $a \geqq 0$ is an integer and from Lemma 3 that

$$f(n) = n^a \quad \text{if} \quad (n, pM) = 1, \left(\frac{n}{p}\right) = 1. \tag{22}$$

First we shall prove that our theorem holds for all n coprime to pM. Assume that $f(n) \neq n^a$ on the set of integers n with $(n, pM)=1$. We prove that

$$f(n) = \left(\frac{n}{p}\right) n^a \quad \text{if} \quad (n, pM) = 1. \tag{23}$$

It is obvious that (23) follows from (22) in the case $\left(\frac{n}{p}\right)=1$. Since $f(n) \neq n^a$ on

the set of integers n coprime to pM, hence there exists a positive integer n_0 such that

$$f(n_0) = -n_0^a \quad \text{and} \quad (n_0, pM) = 1. \tag{24}$$

It follows from (22) and (24) that $\left(\frac{n_0}{p}\right) = -1$.

If $(n, pM)=1$ and $\left(\frac{n}{p}\right) = -1$, then $\left(\frac{n_0 n}{p}\right) = 1$ and so from (22), (24), and Lemma 1 we obtain

$$-n_0^a f(n) = f(n_0)f(n) = f(nn_0) = (nn_0)^a.$$

This shows that

$$f(n) = -n^a = \left(\frac{n}{p}\right) n^a.$$

Thus, (23) is proved.

Using (23) and the method which was used in the proof of Lemma 2 (see the proof of (14)), one can deduce that if $q|M$ then

$$f(q^k) = q^{ka} \quad (k = 1, 2, \ldots)$$

in the case when $f(n)=n^a$ for all n coprime to pM and

$$f(q^k) = \left(\frac{q^k}{p}\right) q^{ka} \quad (k = 1, 2, \ldots)$$

in the case when $f(n)=\left(\frac{n}{p}\right) n^a$ for all n coprime to pM.

The theorem is proved.

References

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

[2] B. M. Phong and J. Fehér, Note on multiplicative functions with congruence property,

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

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
REÁLTANODA U. 13—15
H-1053 BUDAPEST
HUNGARY