REDUCED RESIDUE SYSTEMS AND A PROBLEM FOR MULTIPLICATIVE FUNCTIONS

Bui Minh Phong (Budapest, Hungary)

To the memory of Imre Környei To the memory of Béla Kovács

Abstract. It is proved that if F, $G: IN \to \{0, 1\}$ are completely multiplicative functions such that G(an+b)=F(An+B) is satisfied for some integers a>0, b, A>0, B with $\Delta=Ab-aB\neq 0$ and for every positive integer n, then either F(An+B)=G(an+b)=0 for all $n\in IN$ or F(n)=G(m)=1 for all $n,m\in IN$, $(n,A'\Delta)=(m,a'\Delta)=1$, where $a'=\frac{a}{(a,b)}$ and $A'=\frac{A}{(A,B)}$.

1. Introduction and results

Notations. Let \mathbb{N} denote the set of all positive integers. The letters p, q, π with and without suffixes denote prime numbers. (m, n) denotes the greatest common divisor of the integers m and n. Here $m \mid\mid n$ denotes that m is an unitary divisor of n, i.e. that $m\mid n$ and $(\frac{n}{m}, m) = 1$. For each $n \in \mathbb{N}$ we denote by n^* the product of all prime divisors of n. Let P(n) denote the greatest prime divisor of n. Let \mathcal{M} (\mathcal{M}^*) be the set of complex-valued multiplicative (completely multiplicative) functions.

P.Erdős proved in 1946 [2] that if $f: \mathbb{N} \to \mathbb{R}$ is an additive function such that $\Delta f(n) := f(n+1) - f(n) = o(1)$ as $n \to \infty$, then f(n) is a constant multiple of $\log n$. This assertion has been generalized in several directions (e.g. see [1]). The characterization of multiplicative functions $f: \mathbb{N} \to \mathbb{C}$

Research (partially) supported by Hungarian National Foundation for Scientific Research, grant No. 2153 and T 020295.

under suitable regularity conditions even in the simplest case $\Delta f(n) = o(1)$ is much harder. More than 15 years ago I.Kátai stated as a conjecture that $f \in \mathcal{M}$, $\Delta f(n) = o(1)$ as $n \to \infty$ imply that either f(n) = o(1) or $f(n) = n^s \ (n \in \mathbb{N}), \ 0 \le \operatorname{Re} s < 1$. This was proved by E.Wirsing in a letter to Kátai (September 3, 1984) and in a recent paper [14]. It is not hard to deduce from Wirsing's theorem that if $f, g \in \mathcal{M}$, g(n+1) - f(n) = o(1) as $n \to \infty$, then either f(n) = o(1), or $f(n) = g(n) \ (n \in \mathbb{N})$, and in the last case $f(n) = n^s \ (n \in \mathbb{N}), \ 0 \le \operatorname{Re} s < 1$.

Recently, improving the above results, we proved in [9] that if $k \in \mathbb{N}$ is given and $f, g \in \mathcal{M}$ satisfy the condition

$$g(n+k)-f(n)=o(1)$$
 as $n\to\infty$,

then either f(n)=o(1) as $n\to\infty$ or there are $F,\ G\in\mathcal{M}$ and a complex constant s such that

$$f(n) = n^s F(n), \quad g(n) = n^s G(n), \quad 0 \le \text{Re } s < 1$$

and

$$G(n+k) = F(n)$$

are satisfied for all $n \in \mathbb{N}$. In [7]-[8], by using the result of [4], the equation G(n+k) = F(n) is solved completely.

The general case concerning the characterization of those $f,\ g\in\mathcal{M}$ for which

$$g(an + b) - Ef(An + B) = o(1)$$
 as $n \to \infty$,

where a>0, b, A>0, B are fixed integers and E is a complex constant, seems to be a hard problem. The main difficulty is that we are unable to determine all those F, $G\in\mathcal{M}$ for which G(an+b)=EF(An+B) $(n\in\mathbb{I}\!N)$ is satisfied, even under the assumption that the values are taken from the set $\{0, 1\}$. The above question was solved in [11]-[12] for B=0 under the conditions |f(n)|=|g(n)|=1 $(n\in\mathbb{I}\!N)$. A similar result was obtained in [13] under the conditions f=g, |g(n)|=1 $(n\in\mathbb{I}\!N)$, g(n+b)-g(n)=o(1) as $n\to\infty$, (n,b)=1. Recently, N.L.Bassily and I.Kátai [6] showed that if f, $g\in\mathcal{M}$ satisfying g(2n+1)-Df(n)=o(1) $(n\to\infty)$ with some constant $D\neq 0$, then either f(n)=o(1) $(n\to\infty)$ and g(m)=o(1) $(m\to\infty)$, (m,2)=1 or D=f(2), $f(n)=n^s$, $0\leq \mathrm{Re} s<1$, and f(n)=g(n) for odd integers n.

In order to determine those multiplicative functions f, g which satisfy the relation g(an + b) - Ef(An + B) = o(1) as $n \to \infty$, the first problem is to give all solutions of multiplicative functions F and G for which G(an + b) = F(An + B) $(n \in \mathbb{N})$ is satisfied under the assumptions that the values are taken from the set $\{0, 1\}$. Excluding the case G(an + b) = F(An + B) = 0 for

all $n \in \mathbb{N}$, the solution of the last equation will use a result concerning the characterization of suitable reduced residue systems.

For fixed integers a > 0, b, A > 0 and B with $\Delta := Ab - aB \neq 0$, we shall denote by S = S(a, b; A, B) the subset of positive integers which is subjected to the following properties:

(1) if
$$x, y \in S$$
 and $(x, y) = 1$, then $xy \in S$,

(2) if
$$x \in \mathcal{S}$$
 and $y \parallel x$, then $y \in \mathcal{S}$,

and

(3)
$$an + b \in S$$
 if and only if $An + B \in S$.

It is obvious that if $f \in \mathcal{M}$ and f(an+b) = Ef(An+B) is satisfied for all $n \in IV$, then the set $S_f := \{n \in IV \mid f(n) \neq 0\}$ satisfies the conditions (1)-(3).

Our purpose in this paper is to prove

Theorem 1. Let S = S(a, b; A, B) be a set subjected to the conditions (1)-(3). If there are a prime π and positive integers $w = w(\pi)$, M such that

$$(4) \qquad (\pi, aA) = 1,$$

(5)
$$\{\pi^w, \ \pi^{w+1}, \ \pi^{w+2}, \ldots\} \subseteq \mathcal{S},$$

and

$$(6) AM + B \in \mathcal{S},$$

then we have

$$\{ n \mid (n, d\Delta) = 1 \} \subseteq S,$$

where d = (a, A).

Theorem 2. If $F \in \mathcal{M}^*$ and $G \in \mathcal{M}^*$ such that

$$G(an + b) = F(An + B)$$
 for all $n \in \mathbb{N}$,

and the set of values of F(An + B) and of G(an + b) is contained in $\{0, 1\}$, where a > 0, b, A > 0, B are integers with $\Delta := Ab - aB \neq 0$, then one of the following assertions holds:

(i)
$$F(An + B) = G(an + b) = 0$$
 for all $n \in \mathbb{N}$,

(ii)
$$F(n) = G(m) = 1$$
 for all $n, m \in \mathbb{N}$, $(n, A'\Delta) = (m, a'\Delta) = 1$, where $a' = \frac{a}{(a,b)}$ and $A' = \frac{A}{(A,B)}$.

2. Lemmas

The proof of Theorem 1 is based on Lemmas 1-2.

Lemma 1. If there are a prime q and a positive integer M for which (q, aA) = 1, $AM + B \in \mathcal{S}$ and

$$\{1, q, q^2, \ldots\} \subseteq \mathcal{S},$$

then

$$\{ n \mid (n, d\Delta N) = 1 \} \subseteq S,$$

where d = (a, A) and $N = N_q$ is a positive integer defined by $q^{\varphi(aA)} = aAN_q + 1$ and $\varphi(\cdot)$ denotes the Euler-function.

Proof. Assume that the set S = S(a, b; A, B) satisfies the conditions (1)-(3), furthermore there are a prime q and a positive integer M for which (q, aA) = 1, $AM + B \in S$ and (7) holds. First, by using (3), we can assume that $\Delta = Ab - aB > 0$. Let

$$q^{\varphi(aA)} = aAN + 1.$$

Since

$$(aAN + 1)(an + b) = a[(aAN + 1)n + bAN] + b,$$

it follows from (1)-(3) and (7) that

$$An + B \in S$$
 if and only if $A[(aAN + 1)n + bAN] + B \in S$,

which implies

(8)
$$An + B \in S$$
 if and only if $(aAN + 1)(An + B) + A\Delta N \in S$.

It is clear from (7) that $(aAN+1)^{k-1} \in \mathcal{S}$ holds for all positive integers k, and so by using the fact $AM+B \in \mathcal{S}$ and (8), we have

(9)
$$(aAN+1)^k(AM+B) + A\Delta N \in \mathcal{S}$$

for all positive integers k. Let $AM + B + A\Delta N = q^C D$, where C is a non-negative integer and (D, aAN + 1) = (D, q) = 1. It follows from (7) that

$$q^C \in \mathcal{S}.$$

On the other hand, since (D, aAN + 1) = 1 it follows from the Euler-Fermat theorem and (9) that

$$D \parallel \left((aAN + 1)^{\varphi(D^2)} - 1 \right) (AM + B) + (AM + B + A\Delta N)$$

and

$$((aAN + 1)^{\varphi(D^2)} - 1)(AM + B) + (AM + B + A\Delta N) =$$

$$= (aAN + 1)^{\varphi(D^2)}(AM + B) + A\Delta N \in \mathcal{S}.$$

These relations, together with (2), imply

$$(11) D \in \mathcal{S}.$$

Thus, by (1), (10) and (11), we have

$$AM + B + A\Delta N \in \mathcal{S}$$

from which

$$(12) A\Delta Nm + (AM + B) \in \mathcal{S}$$

is satisfied for all positive integers m. Let p be a prime number which is prime to $A\Delta N$, and let α be a positive integer. Then there is a positive integer m for which the congruence

(13)
$$A\Delta Nm + (AM + B) \equiv p^{\alpha} \pmod{p^{\alpha+1}}$$

holds. Thus, it follows from (1)-(3), (12) and (13) that $p^{\alpha} \in \mathcal{S}$, i.e

$${n \mid (n, A\Delta N) = 1} \subseteq S.$$

To complete the proof of Lemma 1 it is enough to show that

(14)
$$\{n \mid (n, a\Delta N) = 1\} \subseteq \mathcal{S}.$$

Let p be a prime number which is prime to $a\Delta N$, and let α be a positive integer. By (3) and the fact $AM + B \in \mathcal{S}$, we also have $aM + b \in \mathcal{S}$. Let $e = e(p, \alpha)$ be a positive integer for which

$$(aAN + 1)^{e}(aM + b) := aM' + b > a\Delta N p^{\alpha + 1}.$$

It is clear that $aM' + b \in S$. As we proved in the proof of (9), these relations imply that

 $(aAN+1)^k(aM'+b) - a\Delta N \in \mathcal{S}$

holds for all positive integers k. The last relation, as the proof of (12), implies that

$$aM' + b - a\Delta Nm \in \mathcal{S}$$

holds for all positive integers m for which $aM' + b - a\Delta Nm > 0$.

On the other hand, we can choose a positive integer m_0 for which

(17)
$$aM' + b - a\Delta N m_0 \equiv p^{\alpha} \pmod{p^{\alpha+1}},$$

$$0 < m_0 \le p^{\alpha+1}$$

hold. The last relation with (15) and (16) shows that $aM' + b - a\Delta N m_0 > 0$ and

$$aM' + b - a\Delta N m_0 \in \mathcal{S}$$
.

Finally, by using (2) and (17), we have $p^{\alpha} \in \mathcal{S}$. Thus (14) is proved.

The proof of Lemma 1 is finished.

Lemma 2. Assume that all conditions of Theorem 1 are satisfied. Then there is a prime q such that (q, aA) = 1 and

$$\{1, q, q^2, \ldots\} \subseteq \mathcal{S}.$$

Proof. By (4), we have $(\pi, aA) = 1$, and so

$$\pi^{w\varphi(aA)} = aAN_{\pi} + 1.$$

where w is the positive integer defined in (5).

As in the proof of Lemma 1, one can deduce that

if
$$An + B \in \mathcal{S}$$
, then $(aAN_{\pi} + 1)(An + B) + A\Delta N_{\pi} \in \mathcal{S}$,

which, using the following assertions

$$(aAN_{\pi}+1)^{k-1}(An+B) \in \mathcal{S}, \text{ if } An+B \in \mathcal{S}, k \in \mathbb{N},$$

and

$$(aAN_{\pi} + 1)^{k-1}(An + B) \equiv B \pmod{A},$$

implies that

(19) if
$$An + B \in \mathcal{S}$$
, then $(aAN_{\pi} + 1)^{k}(An + B) + A\Delta N_{\pi} \in \mathcal{S}$

holds for all positive integers k.

By (5), (19) and using the argument used in the proof of (12), we also have

(20) if
$$An + B \in \mathcal{S}$$
, then $\pi^{w\varphi(aA)t}(An + B + A\Delta N_{\pi}) \in \mathcal{S}$

for all $t \in IN$.

It is well-known from [15] that

$$P(\pi^{w\varphi(aA)t} - 1) \to \infty$$
 as $t \to \infty$,

where P(y) denotes the greatest prime divisor of y. This shows that there are a positive integer T and a prime q such that

(21)
$$q \mid \pi^{w\varphi(aA)T} - 1 \text{ and } (q, aA\Delta N_{\pi}) = 1.$$

Now we deduce that (18) holds for such a q.

Let q be a prime satisfying (21) and let $\Pi := \pi^{w\varphi(aA)T}$. Let us choose t = T in (20), using (4)-(6) we have

if
$$AM + B \in \mathcal{S}$$
, then $\Pi(AM + B + A\Delta N_{\pi}) \in \mathcal{S}$,

consequently

(22)
$$\Pi \left[\Pi^m (AM + B) + A\Delta N_\pi \frac{\Pi^m - 1}{\Pi - 1} \right] \in \mathcal{S}$$

holds for all positive integers m. Then it is easily seen that there is a positive integer m(q) such that

$$q \parallel G_{m(q)} := \Pi \left[\Pi^{m(q)} (AM + B) + A\Delta N_{\pi} \frac{\Pi^{m(q)} - 1}{\Pi - 1} \right],$$

furthermore

$$q \parallel R_q := \frac{\Pi^q - 1}{\Pi - 1}.$$

It is proved in [10, Theorem 4.1] that the last conditions imply that for each positive integer α there exists a positive $m(q^{\alpha})$ for which

$$q^{\alpha} \parallel G_{m(q^{\alpha})} := \Pi \left[\Pi^{m(q^{\alpha})} (AM + B) + A\Delta N_{\pi} \frac{\Pi^{m(q^{\alpha})} - 1}{\Pi - 1} \right].$$

This together with (22) completes the proof of (18), and so Lemma 2 is proved.

3. Proof of Theorem 1

Assume that the conditions of Theorem 1 hold. By Lemma 2, we can assume that $w = w(\pi) = 0$ in the condition (5), i.e. all conditions of Lemma 1 are satisfied with $q = \pi$. Let

$$\pi^{\varphi(aA)} = aAN_{\pi} + 1.$$

Thus, by Lemma 1, we have

$$\{ n \mid (n, d\Delta N_{\pi}) = 1 \} \subset \mathcal{S},$$

where d = (a, A).

Let $N_{\pi}=N_{\pi}^{'}N_{\pi}^{''}$ and $\Delta=\Delta^{'}\Delta^{''}$, where $(N_{\pi}^{'},N_{\pi}^{''})=(\Delta^{'},\Delta^{''})=$ = $(aA,\Delta^{'}N_{\pi}^{'})=1$ and all prime divisors of $\Delta^{''}N_{\pi}^{''}$ are divisors of aA. Since $(aA,\Delta^{'}N_{\pi}^{'})=1$, there are $N_{1}\in I\!\!N$ and $N_{2}=aAt+1$ such that

$$aAN_1+1\equiv -1\pmod{\Delta^{'}N_{\pi}^{'}}$$
 and $aA(aAt+1)+1\equiv -1\pmod{\Delta^{'}N_{\pi}^{'}},$

furthermore the numbers $aAN_i + 1$ (i = 1, 2) are primes. It is clear from (23) that for the numbers $aAN_i + 1$ (i = 1, 2) all conditions of Lemma 1 are satisfied, furthermore

$$(24) (N_{\pi}, N_1, N_2) = (N_{\pi}' \cdot N_{\pi}'', N_1, N_2)|2.$$

One can deduce from Lemma 1 that

$${n \mid (n, d\Delta N_{\pi}) = 1} \cup {n \mid (n, d\Delta N_{1}) = 1} \cup {n \mid (n, d\Delta N_{2}) = 1} \subseteq S,$$

which with (24) implies

$$(25) {n \mid (n, 2d\Delta) = 1} \subset \mathcal{S}.$$

Thus, the proof of Theorem 1 is completed in the case when $2|\Delta$.

Assume now that $(2, \Delta) = 1$. If aA is an even number, then

$$\left(2aA,\ 2\Delta'\right)=2\mid (aA+2).$$

So, we can choose a positive integer t such that

$$aA(2t+1)+1 \equiv -1 \pmod{2\Delta'}$$
 and $aA(2t+1)+1$ is prime.

Let $N_3 = 2t + 1$. We infer from Lemma 1 and (25) that

$${n \mid (n, 2d\Delta) = 1} \cup {n \mid (n, d\Delta N_3) = 1} \subseteq \mathcal{S},$$

which gives

$${n \mid (n, d\Delta) = 1} \subseteq S.$$

Now let $2 \not\mid aA\Delta$. Then we can assume that $a \equiv A \equiv B \equiv 1 \pmod{2}$, $b \equiv 0 \pmod{2}$. Thus, for each non-negative integer α , we can find a positive integer n_0 such that

(26)
$$an_0 + b \equiv 2^{\alpha} \pmod{2^{\alpha+1}}.$$

It is clear that $2|n_0$. Since $d\Delta$ is odd and n_0 is even, an application of the Chinese Remainder Theorem shows that in this case there exists a positive integer n_1 for which

(27)
$$(a2^{\alpha+1}n_1 + an_0 + b, d\Delta) = (A2^{\alpha+1}n_1 + An_0 + B, 2d\Delta) = 1.$$

It follows from (25) and (27) that

$$A\left[2^{\alpha+1}n_1+n_0\right]+B\in\mathcal{S},$$

which with (3) and (26) shows that $2^{\alpha} \in \mathcal{S}$. Thus

$$\{1,2,2^2,\ldots\}\subseteq\mathcal{S},$$

and the proof of Theorem 1 is complete.

4. Proof of Theorem 2

Assume that $F \in \mathcal{M}^*$ and $G \in \mathcal{M}^*$ satisfy the equation

(28)
$$G(an+b) = F(An+B) \quad \text{for all} \quad n \in IN$$

and the set of values of F(An+B) and of G(an+b) is contained in $\{0, 1\}$, where a>0, b, A>0, B are integers with $\Delta:=Ab-aB\neq 0$. Assume that (i) is not true, i.e. there is a positive integer M such that

(29)
$$G(aM + b) = F(AM + B) = 1.$$

It is obvious that in this case we may assume that (a, b) = (A, B) = 1. Let p be a prime, p|aM + b. Then (p, a) = 1, and so for each $t \in IN$ we have

(30)
$$P_t := p^{\varphi(a)t} = aT_t + 1, \quad G(P_t) = 1.$$

Hence, by (28), we infer that

$$F(An + B) = G(an + b) = G(P_t)G(an + b) = G[P_t(an + b)] =$$

(31)
$$= G[a(P_t n + bT_t) + b] = F[A(P_t n + bT_t) + B]$$

is satisfied for all $n, t \in IN$. Let

$$\mathcal{S}_F := \{n \in \mathbb{N} \mid F(n) = 1\} \text{ and } \mathcal{S}_G := \{n \in \mathbb{N} \mid G(n) = 1\}.$$

It follows from (29) and (31) that

$$A(P_tM + bT_t) + B \in S_F$$
 for all $t \in \mathbb{N}$,

which, using Theorem 1, implies

$$(32) IN_t := \{ n \in IN \mid (n, A\Delta T_t) = 1 \} \subseteq S_F \text{ for all } t \in IN.$$

An application of the Chinese Remainder Theorem shows that there exists a positive integer m_0 for which

$$(am_0 + 1, A\Delta T_1) = 1$$
 and $(m_0, T_1) = 2$.

Hence, by repeating the argument we used in the proof of (32), we get

$$\{ n \in IN \mid (n, A\Delta m_0) = 1 \} \subseteq S_F,$$

which together with (32) implies

$$\{ n \in \mathbb{N} \mid (n, 2A\Delta) = 1 \} \subseteq \mathcal{S}_F.$$

The deduction of the following assertion

$$\{ n \in \mathbb{I} N \mid (n, 2a\Delta) = 1 \} \subseteq \mathcal{S}_G$$

is very similar to the above argument. We omit this part of the proof.

If $2 \mid aA\Delta$, then (ii) is proved. Let $2 \not| aA\Delta$, and so $2 \not| B-b$. Assume that $2 \mid B$ and $2 \not| b$. Since G(aM+b)=F(AM+B)=1 and $2 \mid (aM+b)(AM+B)$, therefore either F(2)=1 or G(2)=1. It can be easily shown from (33)-(34) that (ii) is true in both cases. Thus, this completes the proof of (ii). Theorem 2 is proved.

References

- [1] Elliott P.D.T.A., Arithmetic functions and integer products, Grund. der Math. Wiss. 272, Springer, 1985.
- [2] Erdős P., On the distribution function of additive functions, Ann. Math., 47 (1946), 1-20.
- [3] **Kátai I.**, Multiplicative functions with regularity properties I, Acta Math. Hungar., 42 (3-4) (1983), 295-308.
- [4] Kátai I., Arithmetical functions satisfying some relations, Acta Sci. Math., 55 (1991), 249-268.
- [5] Kátai I., Research problems in number theory II., Ann. Univ. Sci. Bud. Sect. Comp., 16 (1996), 223-251.
- [6] Bassily N.L. and Kátai I., On the pairs of multiplicative functions satisfying some relations, Aequationes Math., 55 (1998), 1-14.
- [7] Fehér J., Kátai I. and Phong B.M., On multiplicative functions satisfying a special relation, Acta Sci. Math. (Szeged), 64 (1998), 49-57.
- [8] Kátai I. and Phong B.M., On some pairs of multiplicative functions correlated by an equation, New Trends in Probability and Statistics, Vol.

- 4. Analytic and Probabilistic Methods in Number Theory, TEV, Vilnius, 1997, 191-203.
- [9] **Kátai I. and Phong B.M.,** A characterization of n^s as a multiplicative function, *Acta Math. Hungar.* (accepted)
- [10] Kiss P. and Phong B. M., Divisibility properties in second order recurrences, *Publ. Math. Debrecen*, 26 (1979), 187-197.
- [11] Phong B.M., A characterization of some arithmetical multiplicative functions, Acta Math. Hungar., 63 (1) (1994), 29-43.
- [12] **Phong B.M.**, A characterization of the some unimodular multiplicative functions, *Publ. Math. Debrecen* (to appear)
- [13] Tang Yuansheng, A reverse problem on arithmetic functions, J. Number Theory, 58 (1996), 130-138.
- [14] Wirsing E., Tang Yuansheng and Shao Pintsung, On a conjecture of Kátai for additive functions, J. Number Theory, 56 (1996), 391-395.
- [15] Shorey T.N. and Tijdeman R., Exponential diophantine equations, Cambridge Univ. Press, 1986.

Bui Minh Phong

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