

REDUCED RESIDUE SYSTEMS AND A PROBLEM FOR MULTIPLICATIVE FUNCTIONS II.

Bui Minh Phong (Budapest, Hungary)

Abstract. It is proved that if multiplicative functions F and G , integers $a > 0$, b , $A > 0$, B with $\Delta = Ab - aB \neq 0$ and a non-zero complex number C satisfy the equation $G(an + b) = CF(An + B)$ for every positive integer n , then either the set

$$\{n \in \mathbb{N} \mid G(an + b) = CF(An + B) \neq 0\} \text{ is finite}$$

or $F(n)G(m) \neq 0$ for all positive integers n, m with $(n, 2A\Delta) = (m, 2a\Delta) = 1$, furthermore for all integers $\alpha, \beta \geq 1$

$$G(2^\alpha) \neq 0 \text{ if and only if } F[(A, B)] \neq 0$$

and

$$F(2^\beta) \neq 0 \text{ if and only if } G[(a, b)] \neq 0.$$

1. Introduction

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 $m \parallel n$ denotes that m is a unitary divisor of n , i.e. that $m|n$ and $(\frac{n}{m}, m) = 1$. Let \mathcal{M} (\mathcal{M}^*) be the set of complex-valued multiplicative (completely multiplicative) functions.

It was financially supported by OTKA 2153 and by MÖB-DAAD PPP-Ungarn 1998/1999.

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

$$g(an + b) - Cf(An + B) = o(1) \quad \text{as } n \rightarrow \infty,$$

where $a > 0, b, A > 0, B$ are fixed integers with $\Delta = Ab - aB \neq 0$ and C is a non-zero complex constant, is not given yet. In order to give the solution of this relation, the first problem is to give all solutions of multiplicative functions F and G for which the equation

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

is satisfied under the assumption that the values are taken from the set $\{0, 1\}$. Excluding the case $G(an + b) = F(An + B) = 0$ for all large integers n , the solution of this equation will use a result concerning the characterization of suitable reduced residue systems. For results and related problems of the above equation with $b = 0$, we refer to papers [1]-[7] and [9]-[11]. In a recent paper [11] we proved the following

Lemma 1. *Assume that a function $F \in \mathcal{M}$ satisfies the equation*

$$F(an + b) = CF(An + b) \quad \text{for all } n \in \mathbb{N},$$

where $a > 0, b, A > 0, B$ are fixed integers with $\Delta = Ab - aB \neq 0$ and C is a non-zero complex constant. If there are a prime π and positive integers $w = w(\pi), M$ such that $(\pi, aA) = 1, F(AM + B) \neq 0$ and

$$F(m) \neq 0 \quad \text{for all } m \in \{\pi^w, \pi^{w+1}, \pi^{w+2}, \dots\},$$

then we have

$$F(n) \neq 0 \quad \text{for all } n \in \mathbb{N}, (n, \Delta) = 1.$$

Our purpose in this paper is to prove the following

Theorem 1. *Let $a > 0, b, A > 0$ and B be integers with $\Delta := Ab - aB \neq 0$. If $F, G \in \mathcal{M}$ satisfy*

$$(1) \quad G(an + b) = CF(An + B) \quad \text{for all } n \in \mathbb{N}$$

with a non-zero complex number C , then either the set

$$(2) \quad \{n \in \mathbb{N} \mid G(an + b) = F(An + B) \neq 0\} \text{ is finite}$$

or

(A) In the case $2 \mid aA\Delta$

$$(3) \quad F(n)G(m) \neq 0 \text{ for all } n, m \in \mathbb{N}, \quad (n, A\Delta) = (m, a\Delta) = 1.$$

(B) In the case $2 \nmid aA\Delta$

$$F(n)G(m) \neq 0 \text{ for all } n, m \in \mathbb{N}, \quad (n, 2A\Delta) = (m, 2a\Delta) = 1,$$

furthermore for all integers $\alpha, \beta \geq 1$

$$G(2^\alpha) \neq 0 \text{ if and only if } F[(A, B)] \neq 0$$

and

$$F(2^\beta) \neq 0 \text{ if and only if } G[(a, b)] \neq 0.$$

The case $F = G$ can be formulated as

Theorem 2. Let $a > 0, b, A > 0$ and B be integers with $\Delta := Ab - aB \neq 0$. If $F \in \mathcal{M}$ satisfies

$$(4) \quad F(an + b) = CF(An + B) \text{ for all } n \in \mathbb{N}$$

with a non-zero complex number C , then either the set

$$(5) \quad \mathcal{K}_F(a, b, A, B) := \{n \in \mathbb{N} \mid F(an + b) = F(An + B) \neq 0\} \text{ is finite}$$

or

$$(6) \quad F(n) \neq 0 \text{ for all } n \in \mathbb{N}, \quad (n, \Delta) = 1.$$

First we prove Theorem 2, then we can reduce the general case to it.

2. Proof of Theorem 2

In this section we assume that $a > 0, b, A > 0$ and B are integers with $\Delta := Ab - aB \neq 0$ and the function $F \in \mathcal{M}$ satisfies (4). Let

$$\mathcal{S} = \mathcal{S}_F := \{n \in \mathbb{N} \mid F(n) \neq 0\}.$$

The basic idea of the proof is to show that if (5) does not hold, then there is a prime q for which

$$(7) \quad (q, aA) = 1 \quad \text{and} \quad \{1, q, q^2, \dots\} \subseteq \mathcal{S}.$$

Then we apply Lemma 1 to get (6).

Lemma 2. *Assume that a function $F \in \mathcal{M}$ satisfies (4) and the set $\mathcal{K}_F(a, b, A, B)$ is infinite. Then there is a prime q for which (7) holds.*

Proof. Since the set $\mathcal{K}_F(a, b, A, B)$ is infinite, there is an infinite sequence $n_1 < n_2 < \dots$ such that

$$F(an_i + b) = CF(An_i + B) \neq 0 \quad \text{for} \quad i = 1, 2, \dots$$

First, we assume that a function $F \in \mathcal{M}$ is of finite support, that is

$$F(p^\alpha) = 0 \quad (\alpha = 1, 2, \dots) \quad \text{if} \quad p \notin \mathcal{B} = \{p_1, p_2, \dots, p_r\},$$

where p_1, p_2, \dots, p_r are primes.

In this case, one can deduce from the multiplicativity of F and (4) that all the prime divisors of the numbers $An_i + B$, $an_i + b$ are from the set \mathcal{B} , furthermore

$$A(an_i + b) - a(An_i + B) = \Delta,$$

which contradicts to a well-known theorem of Thue (e.g. see [12]).

Thus, we may assume that F is not of finite support, i.e. there is an infinite sequence of primes $\pi_1 < \pi_2 < \pi_3 < \dots$ and suitable exponents α_j such that

$$\{\pi_1^{\alpha_1}, \pi_2^{\alpha_2}, \pi_3^{\alpha_3}, \dots\} \subseteq \mathcal{S}.$$

Then there are a positive integer ℓ , $(\ell, aA) = 1$ and an infinite sequence of prime powers

$$\{q_1^{\gamma_1}, q_2^{\gamma_2}, \dots\} \subseteq \{\pi_1^{\alpha_1}, \pi_2^{\alpha_2}, \pi_3^{\alpha_3}, \dots\} \subseteq \mathcal{S},$$

for which $q_j^{\gamma_j} \equiv \ell \pmod{aA}$ and $q_j^{\gamma_j} > \Delta$. We shall prove that for each number $AM + B \in \mathcal{S}$ there exist a positive integer Q and a prime q for which

$$(8) \quad Q \in \mathcal{S}, \quad (Q, 2\Delta(AM + B)) = 1, \quad Q \equiv 1 \pmod{aA}$$

and

$$(9) \quad q|Q + 1, \quad (q, 2aA\Delta) = 1$$

are satisfied.

Using Euler-Fermat theorem, it follows from the condition $q_j^{\gamma_j} \equiv \ell \pmod{aA}$ ($j = 1, 2, \dots$) that there are infinite many positive integers $Q_0 < Q_1 < Q_2 < \dots$ for which (8) is true, i.e.

$$Q_i \in \mathcal{S}, \quad (Q_i, 2\Delta(AM + B)) = 1 \quad \text{and} \quad Q_i \equiv 1 \pmod{aA}$$

for all $i \geq 0$, furthermore

$$(Q_i, Q_j) = 1 \quad \text{for all} \quad i \neq j.$$

Let $\mathcal{N}(2aA\Delta)$ denote the set of those positive integers which are products of prime power divisors p^α , $p|2aA\Delta$. Assume that (9) is not true for the above numbers Q_1, Q_2, \dots , i.e.

$$Q_i + 1 = x_i, \quad Q_0 Q_i + 1 = y_i \quad \text{with} \quad x_i, y_i \in \mathcal{N}(2aA\Delta) \quad (i = 1, 2, \dots).$$

Hence

$$Q_0 Q_i \in \mathcal{S}, \quad (Q_0 Q_i, 2\Delta(AM + B)) = 1, \quad Q_0 Q_i \equiv 1 \pmod{aA}$$

and

$$Q_0 x_i - y_i = Q_0 - 1 \quad \text{with} \quad x_i, y_i \in \mathcal{N}(2aA\Delta)$$

are satisfied for all $i \in \mathbb{N}$, which contradicts to a theorem of Thue (e.g. see [12]). Thus, we have proved that there exist a positive Q and a prime q for which (8) and (9) are satisfied.

Let Q, q be such numbers for which (8) and (9) hold. Then, we obtain

$$\text{if } AM + B \in \mathcal{S}, \quad \text{then} \quad Q(AM + B) = A \left(QM + B \frac{Q-1}{A} \right) + B \in \mathcal{S},$$

and so

$$Q \left[a \left(QM + B \frac{Q-1}{A} \right) + b \right] = a \left(Q^2 M + BQ \frac{Q-1}{A} + b \frac{Q-1}{a} \right) + b \in \mathcal{S}.$$

Thus we have proved that

$$\text{if } AM + B \in \mathcal{S}, \quad \text{then} \quad A \left(Q^2 M + (aBQ + Ab) \frac{Q-1}{aA} \right) + B \in \mathcal{S}.$$

This implies that

$$G_m := A \left(Q^{2m} M + (aBQ + Ab) \frac{Q-1}{aA} \frac{Q^{2m}-1}{Q^2-1} \right) + B \in \mathcal{S}$$

holds for all positive integers m . Since q satisfies (9), one can deduce that there is a positive integer $m(q)$ such that

$$q \parallel G_{m(q)},$$

furthermore

$$q \parallel R_q := \frac{Q^{2q} - 1}{Q^2 - 1}.$$

It is proved in [8, Theorem 4.1] that the last two conditions imply that for each positive integer α there exists a positive $m(q^\alpha)$ for which

$$q^\alpha \parallel G_{m(q^\alpha)} = A \left(Q^{2m(q^\alpha)} M + (aBQ + Ab) \frac{Q - 1}{aA} \frac{Q^{2m(q^\alpha)} - 1}{Q^2 - 1} \right) + B.$$

This together with the fact $G_{m(q^\alpha)} \in \mathcal{S}$ completes the proof (7). Lemma 2 is proved.

Finally, Theorem 2 is immediately follows from Lemma 1 and Lemma 2.

3. Proof of Theorem 1

Assume that the functions $F, G \in \mathcal{M}$ satisfy (1), where $a > 0$, b , $A > 0$, B are integers with $\Delta := Ab - aB \neq 0$ and C is a non-zero complex number. Let

$$\mathcal{S}_F := \{ n \in \mathbb{N} \mid F(n) \neq 0 \} \quad \text{and} \quad \mathcal{S}_G := \{ n \in \mathbb{N} \mid G(n) \neq 0 \}.$$

Lemma 3. *If (2) does not hold, then F and G are not finite support.*

Proof. Since (2) does not hold, there is an infinite sequence $N_1 < N_2 < \dots$ such that

$$(10) \quad G(aN_i + b) = CF(AN_i + B) \neq 0 \quad \text{for } i = 1, 2, \dots$$

Assume that the function F is a finite support, that is

$$F(p^\alpha) = 0 \quad (\alpha = 1, 2, \dots) \quad \text{if } p \notin \mathcal{C} = \{p_1, p_2, \dots, p_r\},$$

where p_1, p_2, \dots, p_r are primes. Similarly as in the proof of Theorem 2, one can deduce from the theorem of Thue that in this case G is not a finite support. Thus, there are primes $\pi_1 < \pi_2 < \pi_3 < \dots$ and $q_1 < q_2 < q_3 < \dots$ such that

$$(11) \quad \{\pi_1^{\alpha_1}, \pi_2^{\alpha_2}, \pi_3^{\alpha_3}, \dots\} \subseteq \mathcal{S}_F$$

$$(12) \quad \{q_1^{\beta_1}, q_2^{\beta_2}, q_3^{\beta_3}, \dots\} \subseteq \mathcal{S}_G,$$

hold for suitable exponents α_j and β_j ($j \in \mathbb{N}$). Let M be a positive integer such that $G(aM + b) = CF(AM + B) \neq 0$. If we write

$$(aM + b)^2(AM + B)^2m + M$$

in the place of n , then we can write the equation (1) in the form

$$(13) \quad G(Um + 1) = F(Vm + 1) \text{ for all } m \in \mathbb{N},$$

where $U = a(aM + b)(AM + B)^2$ and $V = A(AM + B)(aM + b)^2$. As we showed in the proof of Theorem 2, the conditions (11) and (12) imply that there are a positive integer $Q \in \mathcal{S}_G$ with $Q \equiv 1 \pmod{U}$ and infinite positive integers $Q_0 < Q_1 < Q_2 < \dots$ for which

$$Q_i \in \mathcal{S}_F \text{ and } Q_i \equiv 1 \pmod{QV}$$

for all $i \geq 0$, furthermore

$$(Q_i, Q_j) = 1 \text{ for all } i \neq j.$$

From (13) we infer that

$$\begin{aligned} G(Q)F(QVm + 1) &= G(Q)G(QUm + 1) = \\ &= G \left[U \left(Q^2m + \frac{Q-1}{U} \right) + 1 \right] = F \left[V(Q^2m + \frac{Q-1}{U}) + 1 \right] \end{aligned}$$

and $F(Q_i) = F(QVm_i + 1) \neq 0$ for all integers $i \geq 0$. Therefore from Theorem 2 we have

$$\{ n \in \mathbb{N} \mid (n, \delta) = 1 \} \subseteq \mathcal{S}_F,$$

where

$$\delta = QV(V - U) \frac{Q-1}{U} = AQ \frac{Q-1}{a} (aM + b)^2 \Delta.$$

Let us now consider $n = \frac{\delta}{A}(AM + B)m + M$ and taking into account (1), one can see that

$$\begin{aligned} & G(aM + b)G[Q(Q - 1)(AM + B)(aM + b)\Delta m + 1] = \\ & = G\left[a\left(\frac{\delta}{A}(AM + B)m + M\right) + b\right] = CF(AM + B)F(\delta m + 1) \neq 0 \end{aligned}$$

for all $m \in \mathbb{N}$. Consequently

$$\{n \in \mathbb{N} \mid (n, \delta') = 1\} \subseteq \mathcal{S}_G,$$

where

$$\delta' = Q(Q - 1)(AM + B)(aM + b)\Delta.$$

Finally, let π be a positive integer for which

$$(14) \quad \pi \equiv 1 \pmod{aA} \quad \text{and} \quad (\pi, \delta\delta') = 1.$$

It is obvious that $x^k \in \mathcal{S}_F \cap \mathcal{S}_G$ for all $x \mid \pi$ and $k \in \mathbb{N}$. Therefore, we infer from (1)

$$\begin{aligned} CG(\pi)F(An + B) &= G(\pi)G(an + b) = G\left[a\left(\pi n + b\frac{\pi - 1}{a}\right) + b\right] = \\ &= CF\left[A\left(\pi n + b\frac{\pi - 1}{a}\right) + B\right] \end{aligned}$$

and

$$\begin{aligned} F(\pi)G(an + b) &= CF(\pi)F(An + B) = CF\left[A\left(\pi n + B\frac{\pi - 1}{A}\right) + B\right] = \\ &= G\left[a\left(\pi n + B\frac{\pi - 1}{A}\right) + b\right]. \end{aligned}$$

On the other hand, by (10) we have $AN_i + A \in \mathcal{S}_F$ and $aN_i + b \in \mathcal{S}_G$ for all $i \in \mathbb{N}$, and so Theorem 2 with the last relations shows that

$$(15) \quad \left\{n \in \mathbb{N} \mid \left(n, A\frac{\pi - 1}{aA}\Delta\right) = 1\right\} \subseteq \mathcal{S}_F$$

and

$$(16) \quad \left\{n \in \mathbb{N} \mid \left(n, a\frac{\pi - 1}{aA}\Delta\right) = 1\right\} \subseteq \mathcal{S}_G.$$

An application of the Chinese Remainder Theorem shows that there is a positive integer K such that

$$\left(aAK + 1, aA \frac{\pi - 1}{aA} \Delta \right) = 1 \quad \text{and} \quad \left(K, \frac{\pi - 1}{aA} \right) \mid 2.$$

Repeating the argument used in the proof of (15) and (16), we also have

$$\{ n \in \mathcal{IN} \mid (n, AK\Delta) = 1 \} \subseteq \mathcal{S}_F \quad \text{and} \quad \{ n \in \mathcal{IN} \mid (n, aK\Delta) = 1 \} \subseteq \mathcal{S}_G,$$

which with (15) and (16) gives

$$(17) \quad \{ n \in \mathcal{IN} \mid (n, 2A\Delta) = 1 \} \subseteq \mathcal{S}_F$$

and

$$(18) \quad \{ n \in \mathcal{IN} \mid (n, 2a\Delta) = 1 \} \subseteq \mathcal{S}_G.$$

It is easily seen that if $aA\Delta$ is even, then (17) and (18) imply (3) and Theorem 1 is proved.

Now let $(aA\Delta, 2) = 1$. Then we can assume that $a \equiv A \equiv B \equiv 1 \pmod{2}$, $b \equiv 0 \pmod{2}$. Thus, for positive integers α, β we can find a positive integer n_0, n_1 such that

$$(19) \quad an_0 + b \equiv 2^\alpha \pmod{2^{\alpha+1}} \quad \text{and} \quad An_1 + B \equiv 2^\beta \pmod{2^{\beta+1}}.$$

It is clear that $2 \mid n_0, 2 \nmid n_1$. Since $aA\Delta$ is odd, an application of the Chinese Remainder Theorem shows that in this case there exists a positive integer n_2, n_3 for which

$$(20) \quad (a'2^{\alpha+1}n_2 + a'n_0 + b', 2a\Delta) = (A'2^{\alpha+1}n_2 + A'n_0 + B', 2A\Delta) = 1$$

and

$$(21) \quad (a'2^{\alpha+1}n_3 + a'n_1 + b', 2a\Delta) = (A'2^{\alpha+1}n_3 + A'n_1 + B', 2A\Delta) = 1,$$

where $A = (A, B)A', B = (A, B)B', a = (a, b)a'$ and $b = (a, b)b'$. It follows from (1), (17), (18), (20) and (21) that for all integers $\alpha, \beta \geq 1$ we have

$$2^\alpha \in \mathcal{S}_G \quad \text{if and only if} \quad (A, B) \in \mathcal{S}_F$$

and

$$2^\beta \in \mathcal{S}_F \quad \text{if and only if} \quad (a, b) \in \mathcal{S}_G.$$

Thus, the proof of Theorem 1 is complete.

References

- [1] **Kátai I.**, Arithmetical functions satisfying some relations, *Acta Sci. Math.*, **55** (1991), 249-268.
- [2] **Kátai I.**, Research problems in number theory II., *Ann. Univ. Sci. Budapest., Sect. Comp.*, **16** (1996), 223-251.
- [3] **Bassily N.L. and Kátai I.**, On the pairs of multiplicative functions satisfying some relations, *Aequationes Math.*, **55** (1998), 1-14.
- [4] **Fehér J., Kátai I. and Phong B. M.** , On multiplicative functions satisfying a special relation, *Acta Sci. Math. (Szeged)*, **64** (1998), 49-57.
- [5] **Kátai I. and Phong B. M.** , On some pairs of multiplicative functions correlated by an equation, *New Trends in Probability and Statistics*, Vol. 4 (1997), *Analytic and Probabilistic Methods in Number Theory*, TEV, Vilnius, Lithuania, 191-203.
- [6] **Kátai I. and Phong B. M.** , On some pairs of multiplicative functions correlated by an equation II, *Aequationes Math.*, **59** (2000), 287-297.
- [7] **Kátai I. and Phong B. M.** , A characterization of n^s as a multiplicative function, *Acta Math. Hungar.*, **87** (2000), 317-331.
- [8] **Kiss P. and Phong B. M.**, Divisibility properties in second order recurrences, *Publ. Math. Debrecen*, **26** (1979), 187-197.
- [9] **Phong B. M.**, A characterization of some arithmetical multiplicative functions, *Acta Math. Hungar.*, **63** (1) (1994), 29-43.
- [10] **Phong B. M.**, A characterization of the some unimodular multiplicative functions, *Publ. Math. Debrecen*, **57** (2000), 339-366.
- [11] **Phong B. M.**, Reduced residue systems and a problem for multiplicative functions, *Ann. Univ. Sci. Budapest., Sect. Comp.*, **19** (1999), 34-46.
- [12] **Shorey T. N. and Tijdeman R.** , *Exponential diophantine equations*, Cambridge Univ. Press, 1986.

(Received December 16, 1999)

Bui Minh Phong

Department of Computer Algebra

Eötvös Loránd University

Pázmány Péter sét. 1/D

H-1117 Budapest, Hungary

bui@compalg.inf.elte.hu