A CONGRUENCE FOR A CLASS OF ARITHMETIC FUNCTIONS

M.V. Subbarao

(received May 11, 1966)

1. Introduction. There is considerable literature concerning the century old result that for arbitrary positive integers a and m,

$$\sum_{d \mid m} \mu(d)\, a^{m/d} \equiv 0 \pmod{m}, \tag{1.1}$$

where $\mu(m)$ is the usual Möbius function. For earlier work on this we refer to L.E. Dickson [4, pp. 84-86] and L. Carlitz [1, 2]. Another reference not noted by the above authors is R. Vaidyanathaswamy [6], who noted that the left member of (1.1) represents the number of special fixed points of the m th power of a rational transformation of the n th degree. Recently Carlitz [1, 2] considered a generalization of (1.1) and obtained necessary and sufficient conditions for the congruence

$$\sum_{d \mid m} \mu(d)\, g(m/d) \equiv 0 \pmod{m} \tag{1.2}$$

to hold, where $g(m)$ is an arbitrary arithmetic function. This in turn was further generalized by P. C. McCarthy [5] who obtained necessary and sufficient conditions for the validity of the congruence

$$\sum_{d^k \mid m} \mu(d)\, g(m/_{d}k) \equiv 0 \pmod{m}$$

where $k \geq 1$ is a given integer.

It is the purpose of this note to consider these results in a more general setting and raise the question: Given two arithmetic functions $f(m)$ and $g(m)$, of which the former is multi-

Canad. Math. Bull. vol. 9, no. 5, 1966

https://doi.org/10.4153/CMB-1966-070-4 Published online by Cambridge University Press

plicative, under what conditions does the congruence

$$(1.3) \qquad \sum_{d|m} f(d)\, g(m/d) \equiv 0 \pmod{m}$$

hold for all positive integers m? We obtain necessary and sufficient conditions for (1.3) to hold, from which the results of Carlitz and McCarthy referred to earlier follow as special cases.

2. Throughout what follows we assume that $f(m)$ and $g(m)$ are integral valued. We write $F(m)$ for the left member of (1.3) and recall the well known fact that $F(m)$ is multiplicative provided both $f(m)$ and $g(m)$ are so, but that this no longer holds if only $f(m)$ is multiplicative. It follows that if both $f(m)$ and $g(m)$ are multiplicative, (1.3) holds if and only if we have

(2.1) $\quad F(p^a) \equiv 0 \pmod{p^a}$ for all primes p and all integers $a > 0$.

If $f(m)$ alone is multiplicative and $g(m)$ is note, the condition (2.1) is still obviously necessary for the validity of (1.3) for all m, but is no more sufficient, as can be seen, for example, on setting

$$f(m) = \mu(m);\ g(1) = 1,\ g(n) = n^2 + 1\ (n > 1).$$

However we have the following

THEOREM 1. If $g(m)$ is multiplicative, the congruence (1.3) holds for all positive integers m if and only if for all primes p and all positive integers a and b with $(b, p) = 1$ we have

$$(2.2) \qquad \sum_{t=0}^{a} f(p^t)\, g(p^{a-t} b) \equiv 0 \pmod{p^a}.$$

Proof. To prove the "if" part, we can assume that $m > 1$ since (1.3) holds trivially for $m = 1$. Let p be a prime divisor of m and $p^a \| m$, so that we can write $m = p^a n$ where $(p, n) = 1$. We have

https://doi.org/10.4153/CMB-1966-070-4 Published online by Cambridge University Press

$$F(m) = \sum_{d|n} \sum_{t=0} f(p^t d)\, g(p^{a-t} n/d)$$

$$= \sum_{d|n} f(d) \sum_{t=0}^{a} f(p^t)\, g(p^{a-t} n/d) .$$

Since $(p, n/d) = 1$, the inner sum $\equiv 0 \pmod{p^a}$ on using (2.2). Using a similar argument for each prime divisor of m we obtain $F(m) \equiv 0 \pmod{m}$, as is to be shown.

We next assume (1.3) to hold for all m and derive (2.2). First we observe that, $f(m)$ being multiplicative, $f(1) \neq 0$ and the (Dirichlet) inverse function $\bar{f}^{1}(m)$ exists and is completely characterized by the properties:

i) $\bar{f}^{1}(m)$ is multiplicative;

ii) for all primes p and all integers $a \geq 0$,

$$(2.3) \qquad (f \cdot \bar{f}^{1})(p^t) = \sum_{t=0}^{a} f(p^t)\, \bar{f}^{1}(p^{a-t}) = \begin{cases} 1, & \text{if } a = 0 \\ 0, & \text{if } a > 0 \end{cases} .$$

Recalling the definition of $F(m)$ we have

$$g(m) = \sum_{d|m} F(d)\, \bar{f}^{1}(m/d)$$

for all $m > 0$. Setting, in particular, $m = p^a n$ where p is an arbitrary prime, n an arbitrary integer > 0 prime to p and a an arbitrary non-negative integer, one obtains, on using the multiplicativity of $\bar{f}^{1}(m)$.

$$g(p^a n) = \sum_{t=0}^{a} \bar{f}^{1}(p^{a-t}) \sum_{d|n} F(p^t d)\, \bar{f}^{1}(n/d).$$

Using similar relations for $g(p^{a-1} n), \ldots, g(n)$, we have

$$(2.4) \quad \sum_{t=0}^{a} f(p^t)\, g(p^{a-t} n) = \sum_{t=0}^{a} f(p^t) \sum_{\kappa=0}^{a-t} \bar{f}^{1}(p^{a-t-\kappa}) \sum_{d|n} F(p^\kappa d) \bar{f}^{1}(n/d).$$

https://doi.org/10.4153/CMB-1966-070-4 Published online by Cambridge University Press

Rearranging the terms, the right member becomes

$$\sum_{t=0}^{a} (f \cdot \bar{f}^{1})(p^{t}) \sum_{d|n} F(p^{a-t}d)\, \bar{f}^{1}(n/d)$$

which, in view of (2.3), reduces to

$$\sum_{d|n} F(p^{a}d)\bar{f}^{1}(n/d).$$

Since by assumption (1.3) holds for all m, we have $F(p^{a}d) \equiv 0 \pmod{p^{a}}$, showing that the left member of (2.4) is $\equiv 0 \pmod{p^{a}}$ and thus completing the proof of the theorem.

REFERENCES

1. L. Carlitz, An arithmetic function. Bull. Amer. Math. Soc. 43, (1937), pages 271-276.

2. L. Carlitz, Note on an arithmetic function. Amer. Math. Monthly, 59, (1952), pages 386-387.

3. E.D. Cashwell and C.J. Everett, The ring of number theoretic functions. Pacific J. of Math. 9, (1959), pages 975-985.

4. L.E. Dickson, History of the Theory of Numbers. Vol. I.

5. P.J. McCarthy, On an arithmetic function. Monatsh Math. 63, (1959), pages 228-230.

6. R. Vaidyanathaswamy, Collected papers, Madras University.

University of Alberta, Edmonton.

https://doi.org/10.4153/CMB-1966-070-4 Published online by Cambridge University Press