# ARITHMETIC FUNCTIONS SATISFYING A CONGRUENCE PROPERTY

M. V. Subbarao

(received October 20, 1965)

1. Introduction. This note proves (in the theorem below) a conjecture made by the author last year through the pages of the Departmental Problem Book. This arose in connection with some other investigations of arithmetic functions.

THEOREM. Let $f(n)$ be an integer-valued arithmetic function satisfying:

(1.1) $f(mn) = f(m)f(n)$ for all $(m, n) = 1$;

(1.2) $f(n+k) \equiv f(n) \pmod{k}$ for all positive integers $n$ and $k$

Then either $f(n) \equiv 0$ or $f(n) = n^r$ for a non-negative integer $r$.

Recently Leo Moser showed the author a proof, sent him by Ron Graham and credited [2] to Jon Folkman for the special case when $f(n)$ is a completely multiplicative function (i.e., $f(mn) = f(m)f(n)$ for all $m$ and $n$). Our proof given here naturally involves some arguments the need for which do not arise in Folkman's special case.*

2. Proof of the theorem. If $f(1) = 0$, then $f(n) = f(n)f(1) = 0$ for all $n$. If $f(k) = 0$ for $k > 1$, given an integer $m$, there exist an infinity of primes $p$ satisfying $(p, k) = (p, m) = 1$. For each such $p$, by Dirichlet's theorem, there exists an infinity of primes $q$ so that $(q, k) = 1$ and $kq \equiv m \pmod{p}$. Hence $0 = f(k)f(q) = f(kq) \equiv f(m) \pmod{p}$,

* After completing this paper, the author received from Folkman a proof of the theorem when $f$ is multiplicative. His proof is however on somewhat different lines.

giving $f(m) = 0$.

Suppose now that $f(n)$ never vanishes. From (1.1) we have $f(1) = 1$. For a prime $p$ and $a > 0$ we can set $f(p^a) = mp^r$ where $r \geq 0$ and $(m, p) = 1$. Clearly $m = \pm 1$, for otherwise, if $q$ is any prime divisor of $|m|$, there is by Dirichlet's theorem a prime $t$ for which $(t, p) = (t, q) = 1$ and $p^a t \equiv 1 \pmod{q}$, and this leads to the absurdity that

$$1 = f(1) = f(p^a t) \equiv mp^r f(t) \pmod{q}.$$

We next show that for $p$ fixed, the value of $m$ is independent of $a$. Writing, for $a > 0, b > 0$, $f(p^a) = m_a p^{r_a}$; $f(p^b) = m_b p^{r_b}$, $d = |a - b|$, $R = |r_a - r_b|$, the relation $f(p^a) \equiv f(p^b) \pmod{|p^a - p^b|}$ shows that $r_a$ and $r_b$ are both $= 0$ or both $> 0$, and further either $p^r m_a - m_b$ or $m_a - p^R m_b$ is $\equiv 0 \pmod{p^d - 1}$. It follows that $m_a = m_b$ for all $a, b$ for which $|a - b| > 2$, and hence for all positive $a$ and $b$.

Keep the prime $p$ fixed. Corresponding to every prime $q \neq p$, there is a prime $t$ such that $(t, p) = (t, q) = 1$ and $pt \equiv 1 \pmod{q}$. Thus

$$m_1^2 p^{2a_1} (f(t))^2 = (f(pt))^2 \equiv (f(1))^2 = 1$$

$$\equiv f(p)f(t) \equiv f(p^2 t)f(t) = f(p^2)(f(t))^2$$

$$\equiv m_2 p^{a_2} (f(t))^2 \pmod{q},$$

so that for every prime $q \neq p$,

$$m_2 p^{a_2} - m_1^2 p^{2a_1} \equiv 0 \pmod{q}.$$

It follows that $m_2 p^{a_2} = m_1^2 p^{2a_1}$. Since we already know that $m_1 = m_2$, this shows that $m_2 = m_1^2$ and hence $m_1 = m_2 = 1$.



https://doi.org/10.4153/CMB-1966-017-7 Published online by Cambridge University Press

We also have $a_2 = 2a_1$. If now we suppose $a_n = na_1$ for an integer $n \geq 1$ where $f(p^n) = p^{a_n}$, we have for all primes $q \neq p$,

$$p^{a_{n+1}} (f(t))^{n+1} = f(p^{n+1} t)\ (f(t))^n$$

$$\equiv f(p^n)(f(t))^n = p^{na_1} (f(t))^n = (f(pt))^n$$

$$\equiv 1 \equiv (f(pt))^{n+1} \equiv p^{(n+1)a_1} (f(t))^{n+1} \pmod{q}.$$

This gives $a_{n+1} = (n+1)\, a_1$ and proves by induction on $k$ that $a_k = ka_1$ for all $k \geq 1$.

To prove the theorem it only remains to show that if, for any two distinct primes $p$ and $q$, $f(p) = p^a$ and $f(q) = q^b$, then $b = a$. Assuming, for definiteness, $p > q$ and writing $d = |a - b|$, and $N = p^{d+k} q - 1 > 1$, where $k$ is any integer $\geq 1$, we have $p^{d+k} q \equiv 1 \pmod{N}$, giving

$$p^{a(d+k)} q^b = f(p^{d+k} q) \equiv f(1) = 1 \equiv p^{(d+k)a} q^a \pmod{N}.$$

Hence $q^d \equiv 1 \pmod{N}$. Now $0 \leq q^d - 1 < N$ so that $d = 0$, and the theorem follows.

3. Remarks. I. Property (1.2) is equivalent to

$$f(n+p^a) = f(n) \pmod{p^a}, \tag{3.1}$$

for $a, n = 1, 2, 3, \ldots$, and all primes $p$.

For, if $p$ and $q$ are distinct primes and $a \geq 0$, $b \geq 0$, we have, on using (3.1),

$$f(n) \equiv f(n+p^a) \equiv f(n+2p^a) \equiv f(n+3p^a) \equiv \ldots \equiv f(n+p^a q^b) \pmod{p^a}$$

and similarly

$$f(n) \equiv f(n+p^a q^b) \pmod{q^b}.$$

Hence $f(n) \equiv f(n+p^a q^b) \pmod{p^a q^b}$. An easy induction process extends this property to (1.2). The reverse implication is trivial.

https://doi.org/10.4153/CMB-1966-017-7 Published online by Cambridge University Press

II. The theorem fails if the multiplicative property of $f(n)$ is replaced by the property that $f(1) = 1$ and $f(mn) \geq f(m)\, f(n)$ for all $m, n \geq 1$. This is shown by the counter example $f(n) = n^a(2n^a - 1)$ where $a$ is any positive integer. It is of interest to know if one can formulate a property weaker than multiplicativity for which the theorem still holds.

In Memory of my Teacher, Professor K. Ananda Rau.

## REFERENCES


1. J. Folkman, Private communication.

2. M. V. Subbarao, A Class of Arithmetical Equations, (to appear).



University of Alberta (Edmonton)





https://doi.org/10.4153/CMB-1966-017-7 Published online by Cambridge University Press