ON THE FUNCTIONAL EQUATION $F(mn)F((m, n)) = F(m)F(n)f((m, n))$

TOM M. APOSTOL AND HERBERT S. ZUCKERMAN

1. Introduction. Let f be a completely multiplicative arithmetical function. That is, f is a complex-valued function defined on the positive integers such that

$$f(mn) = f(m)f(n)$$

for all m and n. We allow the possibility that $f(n) = 0$ for all n. (If f is not identically zero then we must have $f(1) = 1$.) Given such an f we wish to study the problem of characterizing all numerical functions F which satisfy the functional equation

$$F(mn)F((m, n)) = F(m)F(n)f((m, n)) , \tag{1}$$

where (m, n) denotes the greatest common divisor of m and n. When $f(n) = n$ for all n, Equation (1) is satisfied by the Euler ϕ function since we have

$$\phi(mn)\phi((m, n)) = \phi(m)\phi(n)(m, n) .$$

More generally, it is known (see [1], [2]) that an infinite class of solutions of (1) is given by the formula

$$F(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)g\left(\frac{n}{d}\right),$$

where μ is the Möbius function and g is any multiplicative function, that is,

$$g(mn) = g(m)g(n) \quad \text{whenever } (m, n) = 1 .$$

Some work on a special case of this problem has been done by P. Comment [2]. In the case $f(1) = 1$ he has investigated those solutions F of (1) which have $F(1) \neq 0$ and which satisfy an additional condition which he calls "property O": If there exists a prime p_0 such that $F(p_0) = 0$ then $F(p_0^\alpha) = 0$ for all $\alpha > 1$. Comment's principal theorem states that F is a solution of (1) with property O and with $F(1) \neq 0$ if, and only if, F satisfies the two equations

$$F(mn)F(1) = F(m)F(n) \quad \text{whenever } (m, n) = 1$$

and

Received May 28, 1963.

$$F(p^\alpha) = F(p)f(p)^{\alpha-1} \quad \text{for all primes } p \text{ and all } \alpha \geqq 1 .$$

In this paper we study the problem in its fullest generality. In the case of greatest interest, $F(1) \neq 0$, we obtain a complete classification of all solutions of (1).

2. The solutions of (1) with $f(1) = 0$. If the given f has $f(1) = 0$ then f is identically zero and Equation (1) reduces to

$$F(mn)F((m, n)) = 0 \tag{2}$$

for all m, n. To characterize the solutions of (2) we introduce the following concept.

DEFINITION 1. A (finite or infinite) set $A = \{a_1, a_2, a_3, \cdots\}$ of positive integers is said to have property P if no a_i is divisible by any a_j^2.

Two simple examples of sets with property P are the set of primes and the set of products of distinct primes. The solutions of (2) may now be characterized as follows:

THEOREM 1. *A numerical function F satisfies* (2) *if, and only if, there exists a set A with property P such that $F(n) = 0$ whenever $n \notin A$.*

Proof. Let $A = \{a_1, a_2, a_3, \cdots\}$ be a set with property P. Define $F(a_1), F(a_2), F(a_3), \cdots$, in an arbitrary fashion and define $F(n) = 0$ if $n \notin A$. We shall prove that F satisfies (2).

Choose two integers m and n and let $d = (m, n)$. If $d \notin A$ then $F(d) = 0$ and (2) holds. If $d \in A$ then $mn \notin A$ since $d^2 \mid mn$. In this case we have $F(mn) = 0$ and again (2) holds. Therefore F satisfies (2) in all cases.

To prove the converse, assume F satisfies (2) and let A be the set of integers n such that $F(n) \neq 0$. We shall prove that A has property P. Choose any element b in A. If b were divisible by k^2 for some k in A, say $b = qk^2$, then we could take $m = qk, n = k$ in (2) to obtain

$$F(b)F(k) = 0$$

which is impossible since both b and k are in A. Therefore A has property P and the proof of Theorem 1 is complete.

3. The solutions of (1) with $f(1) = F(1) = 1$. Since we have characterized all solutions of (1) when $f(1) = 0$ we assume from now on that $f(1) \neq 0$ which means $f(1) = 1$. We divide the discussion in two parts according as $F(1) \neq 0$ or $F(1) = 0$. In the first case we introduce $G(n) = F(n)/F(1)$ and we see that (1) is equivalent to

$$G(mn)G((m, n)) = G(m)G(n)f((m, n))$$

with $G(1) = 1$. This means that the case with $F(1) \neq 0$ reduces to the case $F(1) = 1$. In this case we make a preliminary reduction of the problem as follows.

THEOREM 2. *Assume $f(1) = 1$. A numerical function F satisfies (1) with $F(1) = 1$ if, and only if, F is multiplicative and satisfies the equation*

$$F(p^{a+b})F(p^b) = F(p^a)F(p^b)f(p^b) \tag{3}$$

for all primes p and all integers $a \geqq b \geqq 1$.

Proof. Assume F satisfies (1). Taking coprime m and n in (1) we find $F(mn) = F(m)F(n)$, so F is multiplicative. Taking $m = p^a$, $n = p^b$ in (1) we obtain (3).

To prove the converse, assume F is a multiplicative function satisfying (3) for primes p and $a \geqq b \geqq 1$. Choose two positive integers m and n. If $(m, n) = 1$, Equation (1) is satisfied because it simply states that F is multiplicative. Therefore, assume $(m, n) = d > 1$ and use the prime-power factorizations

$$m = \prod_{i=1}^{\infty} p_i^{a_i}, \qquad n = \prod_{i=1}^{\infty} p_i^{b_i}, \qquad d = \prod_{i=1}^{\infty} p_i^{c_i}$$

where $a_i \geqq 0$, $b_i \geqq 0$, $c_i = \min(a_i, b_i)$, the products being extended over all primes. Since F is multiplicative we have

$$\begin{aligned} F(mn)F(d) &= \prod_{i=1}^{\infty} F(p_i^{a_i+b_i})F(p_i^{c_i}) \\ &= \prod_{0 \leqq b_i \leqq a_i} F(p_i^{a_i+b_i})F(p_i^{b_i}) \cdot \prod_{0 \leqq a_i < b_i} F(p_i^{a_i+b_i})F(p_i^{a_i}) . \end{aligned}$$

The factors corresponding to $b_i = 0$ or $a_i = 0$ are

$$\prod_{0 = b_i \leqq a_i} F(p_i^{a_i}) \cdot \prod_{0 = a_i < b_i} F(p_i^{b_i}) = \prod_{a_i b_i = 0} F(p_i^{a_i})F(p_i^{b_i})f(p_i^{c_i})$$

since $F(1) = f(1) = 1$. For the remaining factors we apply (3) to each product and we obtain

$$\begin{aligned} F(mn)F(d) &= \prod_{0 \leqq b_i \leqq a_i} F(p_i^{a_i})F(p_i^{b_i})f(p_i^{b_i}) \cdot \prod_{0 \leqq a_i < b_i} F(p_i^{a_i})F(p_i^{b_i})f(p_i^{a_i}) \\ &= \prod_{i=1}^{\infty} F(p_i^{a_i})F(p_i^{b_i})f(p_i^{c_i}) = F(m)F(n)f(d) . \end{aligned}$$

This completes the proof of Theorem 2.

We turn now to the problem of finding all solutions of (3). If p is a prime for which $f(p) = 0$, then for this prime (3) becomes

$$F(p^{a+b})F(p^b) = 0 \quad \text{whenever } a \geqq b \geqq 1 . \tag{4}$$

For a fixed p the solutions of (4) may be characterized as follows:

THEOREM 3. *An arithmetical function F satisfies* (4) *for a given prime p if, and only if, there exists an integer $c \geqq 1$ such that*

$$F(p^i) = 0 \quad \text{for}^1 \ 1 \leqq i \leqq c - 1 \quad \text{and for } i \geqq 2c . \tag{5}$$

Proof. Assume F satisfies (5) for some $c \geqq 1$. Choose two integers a and b with $a \geqq b \geqq 1$. If $b \leqq c - 1$ then (5) implies $F(p^b) = 0$ so (4) is satisfied. If $b \geqq c$ then $a + b \geqq 2b \geqq 2c$ so $F(p^{a+b}) = 0$ and (4) is again satisfied.

To prove the converse, assume F is an arithmetical function satisfying (4) for some prime p. If $F(p^t) = 0$ for all integers $t \geqq 1$ then (5) holds with $c = 1$. Otherwise, we let c be the smallest $t \geqq 1$ for which $F(p^t) \neq 0$. Then $F(p^i) = 0$ for all $i \leqq c - 1$. Now take any $i \geqq 2c$ and write $i = a + c$ where $a \geqq c$. Taking $b = c$ in (4) we find $F(p^i) = 0$ for $i \geqq 2c$. Therefore (5) is satisfied for this choice of c and the proof of Theorem 3 is complete.

We consider next those primes p for which $f(p) \neq 0$. For such p the problem of solving (3) may be reduced as follows:

THEOREM 4. *Let p be a prime for which $f(p) \neq 0$. An arithmetical function F satisfies* (3) *if, and only if, there exists an arithmetical function g* (which may depend on p) *such that*

$$F(p^a) = g(a)f(p)^a \quad \text{for all } a \geqq 1 , \tag{6}$$

where g satisfies the functional equation

$$g(a + b)g(b) = g(a)g(b) \quad \text{for all } a \geqq b \geqq 1 . \tag{7}$$

Proof. Assume there exists a function g satisfying (7) and let $F(p^a) = g(a)f(p)^a$. Then if $a \geqq b \geqq 1$ we have

$$F(p^{a+b})F(p^b) = g(a + b)f(p)^{a+b}g(b)f(p)^b$$

and

$$F(p^a)F(p^b)f(p^b) = g(a)f(p)^a g(b)f(p)^b f(p)^b .$$

[1] If $c = 1$ the inequality $1 \leqq i \leqq c - 1$ is vacuous; in this case it is understood that (5) is to hold for all $i \geqq 2$.

Using (7) we see that F satisfies (3).

To prove the converse, assume F satisfies (3) and let

$$g(a) = \frac{F(p^a)}{f(p)^a}$$

for $a \geqq 1$. From (3) we see at once that g satisfies (7), so the proof of Theorem 4 is complete.

Next we determine all the solutions of the functional equation (7).

THEOREM 5. *Assume g is an arithmetical function satisfying (7). Then there exists an integer $k \geqq 1$, a divisor d of k, and a complex number C such that*

$$(8) \quad g(n) = 0 \quad \textit{for } 1 \leqq n \leqq k - 1 , \quad \textit{and for } n \geqq k, n \not\equiv 0 \pmod d ,$$

$$(9) \qquad g(n) = C \quad \textit{for } n \geqq k, n \equiv 0 \pmod d .$$

Conversely, choose any integer $k \geqq 1$, any divisor d of k, and any complex number C. For those n satisfying $n \geqq k$ and $n \equiv 0 \pmod d$ let $g(n) = C$, and let $g(n) = 0$ for all other n. Then this g satisfies (7).

Proof. Assume g satisfies (7). If g is identically zero then (8) and (9) hold with any choice of k and d and with $C = 0$. If g is not identically zero, let k be the smallest positive integer n for which $g(n) \neq 0$ and let $C = g(k)$. Then $g(n) = 0$ for $1 \leqq n \leqq k - 1$. If $n \geqq 2k$ we may write $n = k + r, r \geqq k$, and use (7) with $a = r, b = k$ to obtain the periodicity relation

$$(10) \qquad g(k + r) = g(r) \quad \text{for } r \geqq k .$$

In particular, $g(2k) = g(k)$. Therefore, to completely determine g we need only consider $g(n)$ for n in the interval $k + 1 \leqq n \leqq 2k - 1$. If $g(n) = 0$ for all n in this interval then $g(n) = 0$ for all $n \not\equiv 0 \pmod k$ and (8) and (9) hold with $d = k, C = g(k)$. Suppose, then, that $g(n) \neq 0$ for some n in the interval $k + 1 \leqq n \leqq 2k - 1$ and let $k + d$ be the smallest such n. Then $1 \leqq d \leqq k - 1$. We prove next that $d \mid k$, that $g(n) = 0$ if $n \not\equiv 0 \pmod d$, and that $g(n) = C$ if $n \equiv 0 \pmod d$.

For this purpose we define a new function h by the equation

$$h(n) = \frac{g(n + k)}{g(k)} \quad \text{for } n \geqq 0 .$$

Then the periodicity property (10) implies

$$(11) \qquad h(n + k) = h(n) \quad \text{if } n \geqq 0 .$$

We also have

(12) $$h(0) = h(k) = 1,\ h(n) = 0 \quad \text{if } 1 \leqq n < d,\ h(d) \neq 0 .$$

Now for $n \geqq 0$ we have

$$h(n + d) = h(n + d + 2k) = \frac{g(n + d + 3k)}{g(k)} \quad \text{and} \quad h(d) = \frac{g(d + k)}{g(k)} ,$$

Since $n + 2k > d + k > 1$ we may use (7) with $a = n + 2k$, $b = d + k$, to obtain

$$\begin{aligned} h(n + d)h(d) &= \frac{g(n + d + 3k)g(d + k)}{g(k)^2} \\ &= \frac{g(n + 2k)g(d + k)}{g(k)^2} = h(n + k)h(d) = h(n)h(d) . \end{aligned}$$

Since $h(d) \neq 0$ this implies

(13) $$h(n + d) = h(n) \quad \text{if } n \geqq 0 .$$

Using (13) along with (12) we find

$$h(n) = 0 \quad \text{if } n \not\equiv 0 \pmod{d},\ h(n) = 1 \quad \text{if } n \equiv 0 \pmod{d} .$$

Also, $d \mid k$ since $h(k) = 1$. This implies that $g(n) = 0$ if $n \not\equiv 0 \pmod{d}$, and that $g(n) = g(k) = C$ if $n \equiv 0 \pmod{d}$.

Now we prove the converse. Given $k \geqq 1$, a divisor d of k, and a complex number C, define g as indicated in (8) and (9). We must prove that this g satisfies (7). Choose integers a and b with $a \geqq b \geqq 1$. If $a \leqq k - 1$ then $b \leqq k - 1$ and $g(a) = g(b) = 0$ so (7) is satisfied. Suppose, then, that $a \geqq k$. We consider two cases: (i) $a \not\equiv 0 \pmod{d}$, and (ii) $a \equiv 0 \pmod{d}$.

If $a \not\equiv 0 \pmod{d}$ we have $g(a) = 0$ and the right member of (7) vanishes. If $a + b \not\equiv 0 \pmod{d}$ then $g(a + b) = 0$. If $a + b \equiv 0 \pmod{d}$ then $b \not\equiv 0 \pmod{d}$ and $g(b) = 0$. Therefore we always have $g(a + b)g(b) = 0$ so the left member of (7) also vanishes. This settles case (i).

In case (ii), $a \equiv 0 \pmod{d}$, we again consider the two alternatives $a + b \not\equiv 0 \pmod{d}$, $a + b \equiv 0 \pmod{d}$. If $a + b \not\equiv 0 \pmod{d}$ then $b \not\equiv 0 \pmod{d}$ and both sides of (7) vanish. If $a + b \equiv 0 \pmod{d}$ then $b \equiv 0 \pmod{d}$ so $g(a) = g(b) = g(a + b) = C$ and Equation (7) is satisfied. This completes the proof of Theorem 5.

Theorems 2 through 5 give us a complete classification of all solutions of (1) in the case $f(1) = F(1) = 1$.

4. The case $f(1) = 1$, $F(1) = 0$. In this case any F which satisfies (1) must also satisfy

(14) $$F(m)F(n) = 0 \quad \text{whenever } (m, n) = 1 .$$

These functions may be characterized by means of sets of integers with the following property.

DEFINITION 2. A (finite or infinite) set $S = \{k_1, k_2, k_3, \cdots\}$ of positive integers will be said to have property Q if $1 < k_i < k_{i+1}$ and $(k_i, k_j) > 1$ for all i and j.

For example, the set of all multiples of a given integer $k_1 > 1$ has property Q, but there are more complicated sets with this property.

THEOREM 6. *A numerical function F satisfies* (14) *if, and only if, there exists a set S with property Q such that $F(n) = 0$ whenever $n \notin S$, and $F(n) \neq 0$ whenever $n \in S$.*

Proof. Assume F satisfies (14). Then $F(1) = 0$. If F is identically zero the theorem holds with S the empty set. If F is not identically zero there is a smallest integer $k_1 > 1$ with $F(k_1) \neq 0$. The set $\{k_1\}$ has property Q. If $F(n) = 0$ for all $n > k_1$ we may take $S = \{k_1\}$. Otherwise there exists a smallest integer $k_2 > k_1$ with $F(k_2) \neq 0$. The set $\{k_1, k_2\}$ has property Q because (14) implies $(k_1, k_2) > 1$. If $F(n) = 0$ for all $n > k_2$ we may take $S = \{k_1, k_2\}$. If $F(n) \neq 0$ for some $n > k_2$ we let k_3 be the smallest such n. Then (14) implies $(k_1, k_3) > 1$ and $(k_2, k_3) > 1$ so the set $\{k_1, k_2, k_3\}$ has property Q. Continuing in this way we obtain a set $S = \{k_1, k_2, k_3, \cdots\}$ (finite or infinite) with the properties indicated in the theorem.

To prove the converse, choose any set S with property Q, assign arbitrary nonzero values to the elements of S and let $F(n) = 0$ if $n \notin S$. To show that F satisfies (14), choose integers m and n with $(m, n) = 1$. Both m and n cannot be in S since S has property Q. Therefore at least one of m or n is not in S so at least one of $F(m)$ or $F(n)$ is zero. This completes the proof of Theorem 6.

Since Theorem 6 characterizes all solution of (14), all solutions of the more general equation (1) with $F(1) = 0$ must be found among those described in Theorem 6. For those solutions F of (14) which also satisfy (1) more can be asserted about the set S on which F does not vanish. We shall treat only the case in which f is never zero. In this case, if we write $G(n) = F(n)/f(n)$, Equation (1) is equivalent to

$$G(mn)G((m, n)) = G(m)G(n) . \tag{15}$$

In other words, if f never vanishes the problem reduces to the case in which f is identically 1. Moreover, $G(n) = 0$ if, and only if, $F(n) = 0$ so the set S on which G does not vanish is the same as that on which F does not vanish. For those G satisfying (15) with $G(1) = 0$ we shall prove:

THEOREM 7. *Let G be a solution of* (15) *with* $G(1) = 0$ *and let* $S = \{k_1, k_2, \cdots\}$ *be a set with property Q such that* $G(n) \neq 0$ *if, and only if,* $n \in S$. *Then S contains mn and (m, n) whenever it contains m and n. Moreover, every element in S is a multiple of k_1. If* $tk_1^a \in S$ *for some* $t \geqq 1, a \geqq 1$, *then G is constant on the subset* $\{tk_1^a, tk_1^{a+1}, tk_1^{a+2}, \cdots\}$.

Proof. If $m \in S, n \in S$, then $G(m) \neq 0$ and $G(n) \neq 0$. Therefore Equation (15) implies $G(mn) \neq 0$ and $G((m, n)) \neq 0$, so S contains mn and (m, n). Let $d = (k_i, k_1)$. Then $d \in S$ so $d = k_1$ since k_1 is the smallest member of S. Therefore each k_i in S is a multiple of k_1, as asserted.

If $tk_1^a \in S$, let $S(t) = \{tk_1^a, tk_1^{a+1}, tk_1^{a+2}, \cdots\}$. This is a subset of S. Taking $m = k_1$ and $n = tk_1^{a+r}$ in Equation (15) we find $G(tk_1^{a+r+1}) = G(tk_1^{a+r})$ so G is constant on $S(t)$.

BIBLIOGRAPHY

1. Douglas R. Anderson and T. M. Apostol, *The evaluation of Ramanujan's sum and generalizations*, Duke Math. J., **20** (1953), 211-216.

2. P. Comment, *Sur L'équation fonctionelle* $F(nm)F((n, m)) = F(n)F(m)f((m, n))$, Bull. Res. Council of Israel, Sect. F7F (1957/58) pp. 14-20.

CALIFORNIA INSTITUTE OF TECHNOLOGY AND
UNIVERSITY OF WASHINGTON