THE ITERATION OF CERTAIN ARITHMETIC FUNCTIONS

IVAN NIVEN

1. Introduction. For $n \geqslant 3$ define $C(n)$ to be the integer j such that $\phi^{(j)}(n) = 2$, where $\phi^{(j)}(n)$ denotes the jth iterate of the Euler ϕ-function. Define $C(1) = C(2) = 0$. This function has been studied by S. S. Pillai [1], with the notation $R(n)$ for $1 + C(n)$ if $n \geqslant 2$, and $R(1) = 0$. H. Shapiro [2] has also investigated this function, proving the basic relations

$$C(ab) = C(a) + C(b) \text{ or } C(ab) = C(a) + C(b) + 1, \tag{1}$$

the second equation holding when a and b are both even, otherwise the first.

It was suggested to the writer by Morgan Ward that a function analogous to $C(n)$ can be obtained by iteration of $\lambda(n)$, the least positive exponent so that

$$a^{\lambda(n)} \equiv 1 \pmod n \tag{2}$$

for every a which is prime to n. Thus for $n \geqslant 1$ we define $g(n)$ as the least positive integer j such that $\lambda^{(j)}(n) = 1$, where $\lambda^{(j)}(n)$ is the jth iterate of the λ-function. We now prove the following results.

THEOREM 1. *If* $(a, b) = 1$, *then* $g(ab) = \max \{g(a), g(b)\}$.

THEOREM 2. *For* $n \geqslant 1$, $g(2^{2n}) = g(2^{2n+1}) = n + 1, g(p^n) = n - 1 + g(p)$ *where p is any odd prime.*

The method of deriving functions $C(n)$ and $g(n)$ from $\phi(n)$ and $\lambda(n)$ can be generalized to obtaining $F(n)$ from any $f(n)$ which has the property $f(n) < n$ for $n > k$, where k is a constant. It might be expected that $F(n)$ would have a property similar to (1) whenever $f(n)$ was multiplicative, that is, whenever $f(ab) = f(a)f(b)$ for relatively prime a and b. That this is not so can be seen readily by taking $f(n)$ to be the number of divisors of n. Similarly, Theorem 1 is not implied merely by the functional relation of $\lambda(n)$, namely

$$\lambda(ab) = \text{l.c.m. } \{\lambda(a), \lambda(b)\} \text{ whenever } (a, b) = 1. \tag{3}$$

In §2 we shall prove Theorems 1 and 2, and the next two theorems in §3 and §4.

THEOREM 3. $\limsup \{C(n + 1) - C(n)\} = \limsup \{g(n + 1) - g(n)\}$
$= \limsup \{C(n) - g(n)\} = \infty$,

THEOREM 4. $\liminf \{C(n + 1) - C(n)\} = \liminf \{g(n+1) - g(n)\} = -\infty$,
$\liminf \{C(n) - g(n)\} = -1$.

Received September 4, 1949.

https://doi.org/10.4153/CJM-1950-037-0 Published online by Cambridge University Press

2. The fundamental results for $g(n)$. It is known that for any odd prime p,

$$\lambda(p^n) = \phi(p^n) = p^{n-1}(p-1), \tag{4}$$

$$\lambda(2^n) = \tfrac{1}{2}\phi(2^n) = 2^{n-2} \text{ for } n \geqslant 3; \quad \lambda(4) = 2; \quad \lambda(2) = 1. \tag{5}$$

Together with (3), these imply

$$\lambda(m)|\lambda(n) \text{ whenever } m|n. \tag{6}$$

Now Theorem 1 clearly holds if $a = 1$, and we use mathematical induction, assuming the result for $g(n)$ with $n < ab$. Ignore the trivial cases where $g(a) = g(b) = 1$, or where $a = 1$ or $b = 1$. We have

$$g(n) = 1 + g(\lambda(n)) \quad \text{for } n > 2, \tag{7}$$

and so

$$g(ab) = 1 + g(\lambda(ab)) = 1 + g\{\text{l.c.m. } (\lambda(a), \lambda(b))\}. \tag{8}$$

Also $\lambda(a) < a$, $\lambda(b) < b$, so that $ab >$ l.c.m. $(\lambda(a), \lambda(b)) = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, these primes being arranged so that $g(p_1^{\alpha_1}) \geqslant g(p_i^{\alpha_i})$ $(i = 2, 3, \ldots, r)$. Thus by (6) and the induction hypothesis, (8) becomes $g(ab) = 1 + g(p_1^{\alpha_1})$. Without loss of generality we may assume that $p_1^{\alpha_1}$ is a divisor of $\lambda(a)$, so that $g(p_1^{\alpha_1}) = g(\lambda(a)) \geqslant g(\lambda(b))$, whence $g(a) \geqslant g(b)$ by (7). Hence we have $g(ab) = 1 + g(\lambda(a)) = g(a) = \max\{g(a), g(b)\}$.

To prove Theorem 2, we note that the first part is established by (5). And the second part can be obtained by use of mathematical induction, (4), (7) and Theorem 1. Thus for $n \geqslant 2$,

$$g(p^n) = 1 + g(\lambda(p^n)) = 1 + g\{p^{n-1}(p-1)\} = 1 + g(p^{n-1}).$$

3. Proof of Theorem 3. We shall in this and the following section make use of two results of Pillai [1, Theorems 1 and 3] which can be summarized thus:

$$[\log_2 n] \geqslant C(n) \geqslant \log_3 n/2. \tag{9}$$

Since $4^{3^k} - 1$ or $(1+3)^{3^k} - 1$ is divisible by 3^k we can write, using (9) and (1) and the fact that $C(3^k) = k$,

$$\begin{aligned} C(4^{3^k} - 1) &= C(3^k) + C\{(4^{3^k} - 1)/3^k\} \\ &< k + \log_2\{(4^{3^k} - 1)/3^k\} \\ &< k + 2{\cdot}3^k - k\log_2 3. \end{aligned}$$

Also $C(2^j) = j - 1$ and so we have

$$C(4^{3^k}) - C(4^{3^k} - 1) > 2{\cdot}3^k - 1 - k - 2{\cdot}3^k + k\log_2 3 = k\log_2(3/2) - 1.$$

This establishes the first part of Theorem 3.

By (4) and (5) we have $g(n) \leqslant C(n) + 1$, and so (9) implies

$$g(n) \leqslant 1 + [\log_2 n]. \tag{10}$$

Now $(3^k + 1, 3^k - 1) = 2$ and we apply Theorem 1 to get

https://doi.org/10.4153/CJM-1950-037-0 Published online by Cambridge University Press

$$g(3^{2k}-1) \leqslant 1 + \max\{g(3^k+1), g(3^k-1)\}$$
$$\leqslant 2 + \log_2(3^k+1) < 3 + k\log_2 3.$$

From this it follows that

(11) $$g(3^{2k}) - g(3^{2k}-1) > 2k + 1 - 3 - k\log_2 3,$$

which proves the second part of Theorem 3.

The last part of Theorem 3 can be obtained by taking n to be the product of the first k primes, and using (1), Theorem 1, (9) and (10).

4. Proof of Theorem 4. By (9) we see that

(12) $$C(3^j+1) \geqslant j.$$

Next we prove that

(13) $$C(3^{2^k}-1) \geqslant 2^k + k - 1$$

by mathematical induction. Using (1) and (12) we have

$$C(3^{2^k}-1) = C(3^{2^{k-1}}+1) + C(3^{2^{k-1}}-1) + 1$$
$$\geqslant 2^{k-1} + 2^{k-1} + k - 2 + 1.$$

Having proved (13), we see that it implies

$$C(3^{2^k}) - C(3^{2^k}-1) \leqslant 2^k - 2^k - k + 1 = -k + 1,$$

which establishes the first part of Theorem 4.

We now discuss $g(n+1) - g(n)$ with $n = (3^{2k}-1)^2$, k odd. Thus $3^{2k} \equiv 9 \pmod{16}$ and $3^{2k} \equiv -1 \pmod 5$, so that $3 \nmid n$, $5 \nmid n$, $2^6 \mid n$, $2^7 \nmid n$. So for large k we have $g(n) = g(p^{2j})$ where p is some odd prime > 5 and $p^j < 3^k + 1$ so that $j < 1 + k\log_p 3$. Using (10) we have

(14) $$g(n) = g(p^{2j}) = 2j - 1 + g(p) < 2j + \log_2 p < 2 + 2k\log_p 3 + \log_2 p.$$

Considering the last expression as a function of a continuous variable p on the range $(7, 3^k)$, with k constant, we see that it is a maximum for $p = 3^k$, so that (14) implies $g(n) < 4 + k\log_2 3$. Hence we have

$$g(n+1) - g(n) > g\{3^{2k}(3^{2k}-2)\} - 4 - k\log_2 3$$
$$\geqslant g(3^{2k}) - 4 - k\log_2 3$$
$$= 2k + 1 - 4 + k\log_2 3.$$

This proves the second part of Theorem 4, and the final part is a consequence of the two results $g(n) \geqslant C(n) + 1$ and $g(3^k) = k + 1 = 1 + C(3^k)$.

References

[1] S. S. Pillai, *On a function connected with $\phi(n)$*, Bull. Amer. Math. Soc., vol. 35 (1929), 837-841.

[2] Harold Shapiro, *An arithmetic function arising from the ϕ function*, Amer. Math. Monthly, vol. 50 (1943), 18-30.

University of Oregon