NOTE ON EULER'S φ-FUNCTION

BY R. D. CARMICHAEL

Two correspondents have recently called my attention to the fact that the supposed proof of the following theorem, which I gave some years ago,* is not adequate:

THEOREM I. *For a given number n, the equation $\varphi(x) = n$ either has no solution or it has at least two solutions.*

So far I have been unable to supply a proof of the theorem, though it seems probable that it is correct. I am therefore compelled to allow it to stand in the status of a conjectured or empirical theorem.

Let us examine the hypothesis that there exists a value ν of n such that $\varphi(x) = \nu$ has one and just one solution. It is easy to derive certain necessary properties of x. In the first place, x is even, since otherwise $2x$ would also be such that $\varphi(2x) = \nu$. Again, x is divisible by 4, since otherwise $\varphi(x/2)$ would be equal to ν. Let us then denote the value of x by $4s$. We shall prove the following theorem.

THEOREM II. *If $4s$ has the factor $p_0^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, where p_0 $(= 2)$, p_1, p_2, $\cdots$, p_k are distinct prime numbers, and if the quotient of $4s$ by this factor is prime to the factor, and if $p_0^{\gamma_0}p_1^{\gamma_1}\cdots p_k^{\gamma_k} + 1$ is a prime number q, where for a given i, $0 < \gamma_i < \alpha_i$, then $4s$ has the factor q^2.*

The proof is almost immediate. For we have

$$\varphi(2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}) = \varphi(2^{\alpha_0-\gamma_0}p_1^{\alpha_1-\gamma_1}p_2^{\alpha_2-\gamma_2}\cdots p_k^{\alpha_k-\gamma_k}q),$$

so that we should have two solutions of the equation $\varphi(4s) = \nu$ unless s contains the factor q. Similarly, it may be shown that s contains the factor q^2, since otherwise the first power of q could be omitted by appropriately raising certain (or all)

* This BULLETIN, vol. 13 (1907), p. 241. The theorem is also stated as an exercise in my *Theory of Numbers*, p. 36; it was its presence here that led each correspondent to the discovery of the error.

of the exponents on the p's without affecting the value of the φ-function.

In the same way we may prove the following theorem.

THEOREM III. *If s is divisible by a prime of the form $2^k + 1$ it is divisible by the square of this prime.*

For if $4s = 2^{\alpha_0}(2^k + 1)s_1$, where s_1 is prime to $2(2^k + 1)$, we have

$$\varphi(4s) = 2^{\alpha_0 - 1}2^k \cdot \varphi(s_1) = \varphi(2^{k+\alpha_0}s_1),$$

contrary to the hypothesis that the solution is unique.

From Theorem II, it follows that s has the factor 3^2, thence that it has the factor 7^2, and thence that it has the factor 43^2.

Now suppose that s does not have the factor 3^3. Then since $\varphi(2^{\alpha_0} \cdot 3^2) = 2^{\alpha_0} \cdot 3 = \varphi(2^{\alpha_0 - 1} \cdot 13)$, if $\alpha_0 > 1$, it is readily shown that s has the factor 13^2. For this case, then, $4s$ has the factor $2^2 \cdot 3^2 \cdot 7^2 \cdot 13^2 \cdot 43^2$. We may now apply Theorem II successively to show that $4s$ has the factors 79^2, 547^2, 3319^2, 1854763^2. It appears possible to determine in the same way still other factors of $4s$. Those obtained are sufficient to show that $4s$ has at least 38 digits.

If $4s$ contains the factor 3^3, then it follows from Theorem II that it has the factors 19^2, 127^2. Then $4s$ has the factor $2^2 \cdot 3^3 \cdot 7^2 \cdot 19^2 \cdot 43^2 \cdot 127^2$. Applying Theorem II successively we may show that $4s$ has the factors 2287^2, 101347^2, 304039^2. It appears possible to determine in the same way still other factors of $4s$. Thence it is easy to see that $4s$ in this case has at least 41 digits.

Hence, if the empirical Theorem I is not valid, the unique solution x (which would then exist for at least one value of n) must contain at least 38 digits. Moreover, it is easy to increase this number of necessary digits for these exceptional solutions. Hence it seems probable that the empirical theorem is true.

THE UNIVERSITY OF ILLINOIS.