SOME REMARKS ON A PAPER OF McCARTHY[1)]

P. Erdös

(received March 3, 1958)

As usual we denote the number of integers not exceeding n and relatively prime to n by Euler's ϕ function $\phi(n)$. Lehmer[2)] calls the $\phi(n)$ integers

$$1 = a_1 < a_2 < \ldots < a_{\phi(n)} = n - 1$$

the totatives of n.

Denote by $\phi(k, \ell, n)$ the number of a's satisfying

$$n\ell/k < a_i < n(\ell + 1)/k \qquad n > k.$$

If $n\ell \equiv 0 \pmod k$ or $n(\ell + 1) \equiv 0 \pmod k$ then, since $n > k$, $(n\ell/k, n) > 1$ and $(n(\ell + 1)/k, n) > 1$ respectively. Thus $\phi(k, \ell, n)$ is the number of totatives of n satisfying

$$n\ell/k \leq a_i \leq n(\ell + 1)/k.$$

If

$$\phi(k, \ell, n) = \phi(n)/k, \quad \ell = 0, 1, 2, \ldots, k-1 \tag{1}$$

Lehmer[2)] says that the totatives are uniformly distributed with respect to k. To shorten the notation we say that T(n, k) holds in this case. Lehmer[2)] further calls n exceptional with respect to k if either n is divisible by k^2 or n has a prime factor of the form $kx + 1$. He shows that for all exceptional n, T(n, k) holds.

In a recent note McCarthy[1)] proves that if k is a prime then T(n, k) holds if and only if n is exceptional with respect to k. However, if k is not squarefree there is an integer $n > k$ which is not exceptional and for which T(n, k) holds. He further asks if the second half of his theorem remains true if k is not a prime but is squarefree. We are going to prove this in this note.

It is clear that if $T(n, k)$ holds then $\phi(n) \equiv 0 \pmod{k}$. We are going to show that if $k \neq p$ or $k \neq 2p$, p odd, then this condition is not sufficient, i.e. there exists an integer n for which $\phi(n) \equiv 0 \pmod{k}$ but $T(n, k)$ does not hold. Lehmer[2] observes that $n = 21$, $k = 4$ show that $\phi(n) \equiv 0 \pmod{k}$ is not sufficient that $T(n, k)$ holds.

It would be of interest to determine all the integers n for which $T(n, k)$ holds but this problem we can solve only for very special values of k.

THEOREM 1. **Let k be any integer which is not a prime. Then there are infinitely many n which are not exceptional and for which $T(n, k)$ holds.**

First assume $k = p^{\alpha}$, $\alpha > 1$. Then we can take $n = Ap^{\alpha+1}$.

Assume next $k \neq p^{\alpha}$. Then $k = ab$ where $(a, b) = 1$, $a > 1$, $b > 1$. By the well-known theorem of Dirichlet on primes in arithmetic progressions, there are infinitely many primes p and q such that

$$p \equiv 1 \pmod{a}, \quad p \equiv -1 \pmod{b}; \quad q \equiv -1 \pmod{a}, \quad q \equiv 1 \pmod{b}.$$

Clearly $n = pq$ is not exceptional. Now we show that (1) holds. It will be sufficient to show that for every ℓ with $1 \leq \ell \leq k$ the number of integers $m < \frac{\ell n}{k}$ satisfying $(m, n) = 1$ equals

$$(2) \qquad \frac{\ell \phi(n)}{k} = \frac{\ell(p-1)(q-1)}{k}.$$

The number of such integers clearly equals

$$(3) \qquad \left[\frac{\ell pq}{k}\right] - \left[\frac{\ell p}{k}\right] - \left[\frac{\ell q}{k}\right] + \left[\frac{\ell}{k}\right] = \frac{\ell(p-1)(q-1)}{k} - \varepsilon_1 + \varepsilon_2 + \varepsilon_3 - \varepsilon_4$$

where

$$\varepsilon_1 = \frac{\ell pq}{k} - \left[\frac{\ell pq}{k}\right], \quad \varepsilon_2 = \frac{\ell p}{k} - \left[\frac{\ell p}{k}\right],$$

$$\varepsilon_3 = \frac{\ell q}{k} - \left[\frac{\ell q}{k}\right], \quad \varepsilon_4 = \frac{\ell}{k} - \left[\frac{\ell}{k}\right].$$

We must show

(4) $$\varepsilon_1 - \varepsilon_2 - \varepsilon_3 + \varepsilon_4 = 0.$$

When $\ell = k$, $\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon_4 = 0$ and we are done.

Assume $\ell < k$. Since $pq \equiv -1 \pmod k$, we have

$$\varepsilon_1 = \frac{\ell pq}{k} - \left[\frac{\ell pq}{k}\right] = \frac{k-\ell}{k}, \quad \varepsilon_4 = \frac{\ell}{k}$$

or

$$\varepsilon_1 + \varepsilon_4 = 1.$$

Clearly $0 < \varepsilon_2 < 1$ and $0 < \varepsilon_3 < 1$. Hence $0 < \varepsilon_2 + \varepsilon_3 < 2$ and $-1 < \varepsilon_1 - \varepsilon_2 - \varepsilon_3 + \varepsilon_4 < 1$; but $\varepsilon_1 - \varepsilon_2 - \varepsilon_3 + \varepsilon_4$ is the difference of two integers and therefore itself an integer. This proves (4) and completes the proof.

In McCarthy's paper the example $k = 6$, $n = 9$ is given. Here 9 is a power of a prime, it is not exceptional with respect to 6, and $T(9, 6)$ holds. We now show that this situation can occur if and only if

(5) $$k = p^{\alpha} b, \quad p \equiv 1 \pmod b, \ n = p^{\alpha+i}, \ 1 \leq i < \infty$$

$(i < \alpha$ if $b = 1)$.

Clearly, if (5) is satisfied then n is not exceptional. Furthermore we have in this case that the number of integers $m \leq \ell n/k$ with $(m, n) = 1$ equals

$$\left[\frac{\ell n}{k}\right] - \left[\frac{\ell n}{kp}\right] = \frac{\ell}{k}\phi(n) - \varepsilon_1 + \varepsilon_2 \quad (1 \leq \ell \leq k);$$

but $\phi(n) \equiv 0 \pmod k$ implies $\varepsilon_1 - \varepsilon_2$ is an integer with $0 < \varepsilon_1 < 1$, $0 < \varepsilon_2 < 1$ so that $\varepsilon_1 - \varepsilon_2 = 0$. Hence (5) also implies that $T(n, k)$ holds.

Suppose conversely that $n = p^{\beta}$, $T(n, k)$ holds and n is not exceptional with respect to k. Put $k = p^{\alpha} b$, $(p, b) = 1$.

If $b = 1$, clearly $\alpha > \beta/2$ (since n is not exceptional). Thus we may assume $b > 1$. Since $T(n, k)$ holds we must have

$$\phi(n) = p^{\beta-1}(p-1) \equiv 0 \pmod{p^{\alpha} b},$$

or $\alpha < \beta$ and $p \equiv 1 \pmod{b}$ as stated.

Suppose that $k = 2p$ (p odd), n is not exceptional with respect to k, and $T(n, k)$ holds. First of all we must have $\phi(n) \equiv 0 \pmod{2p}$. Furthermore n can have no prime factor $\equiv 1 \pmod{p}$; for such a factor would have to be $\equiv 1 \pmod{2p}$ and n would be exceptional. Thus $n \equiv 0 \pmod{p^2}$. Conversely, if $n \equiv 0 \pmod{p^2}$ and $n \not\equiv 0 \pmod{4}$ then $T(n, k)$ holds and n is not exceptional. Thus if $k = 2p$, $\phi(n) \equiv 0 \pmod{k}$ is necessary and sufficient for $T(n, k)$ to hold. Now we prove

THEOREM 2. If $k \neq p$ and $k \neq 2p$ (p odd), then there always exists an n for which $\phi(n) \equiv 0 \pmod{k}$ and $T(n, k)$ does not hold.

If $k = 4$ we can take $n = 21$ (this is Lehmer's example). If $k = 8$ we can take $n = 35$. Every other k can be factored in the form

$$k = ab, \quad a > 2, \quad b > 2.$$

It is not difficult to see that for such k there exist infinitely many primes p and q satisfying

$$(6) \qquad p \equiv 1 \pmod{a}, \quad p \equiv 1 \pmod{b}, \ pq \equiv -1 \pmod{k},$$

$$\frac{p}{k} - \left[\frac{p}{k}\right] > \frac{1}{2}, \quad \frac{q}{k} - \left[\frac{q}{k}\right] > \frac{1}{2}$$

Put $n = pq$; clearly $\phi(n) \equiv 0 \pmod{k}$ and n is not exceptional. Now, as in (3),

$$\phi(k, 1, n) = \frac{(p-1)(q-1)}{k} - \varepsilon_1 + \varepsilon_2 + \varepsilon_3 - \varepsilon_4.$$

Since $pq \equiv -1 \pmod{k}$, $\varepsilon_1 + \varepsilon_4 < 1$. But by the second line of (6), $\varepsilon_2 + \varepsilon_3 > 1$; thus, since $\varepsilon_1 - \varepsilon_2 - \varepsilon_3 + \varepsilon_4$ is an integer, it must be -1 and

$$\phi(k, 1, n) = \frac{(p-1)(q-1)}{k} + 1.$$

Hence (1) is not satisfied and the proof of Theorem 2 is complete.

Let k be an integer, $n = pq$ not exceptional with respect to k and $n \not\equiv -1 \pmod{k}$. I conjecture that $T(n, k)$ does not hold, but I have not been able to decide this question.

FOOTNOTES

1. Amer. Math. Monthly, 64 (1957), 585-586.

2. Canad. J. of Math. 7 (1955), 347-357.