# REMARKS AND CORRECTIONS TO MY PAPER "SOME REMARKS ON A PAPER OF McCARTHY"

P. Erdős

(communicated by P. Scherk)

(received October 20, 1959)

Denote by $\phi(k,t,n)$ the number of integers $m$ for which

$$nt/k < m < n(t+1)/k, \quad (n, m) = 1 .$$

If $\phi(k,t,n) = \phi(n)/k$ for every $0 \leq t < k$ we shall say, following Lehmer, that $T(n,k)$ holds. In my paper with the above title I prove the following

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

De Bruijn kindly pointed out that my proof given in the above paper has many misprints and is incomplete. To correct it would require consideration of several special cases, thus we give a slightly different proof.

First we prove the following

LEMMA. Let $k \neq p$, $k \neq 2p$ and $k \neq 30$. Then there are two integers $u$ and $v$ satisfying

$$(1) \qquad 1 \leq u < k, \quad 1 \leq v < k, \quad (u,k) = (v,k) = 1,$$

$$(u - 1)(v - 1) \equiv 0 \pmod{k}, \quad u + v > k.$$

Assume first that $k$ is not squarefree. Then $t^2 \mid k$ for some $t > 1$. Put $u = v = k - k/t + 1$. Clearly (1) is satisfied.

Assume next that $k$ is squarefree. Put $k = p_1 p_2 \cdots p_r, p_1 < p_2 < \cdots < p_r$. Assume first $r > 2$. Define $u$ as the greatest integer satisfying

$$x \equiv 1 \pmod{p_r}, \quad (x,k) = 1, \quad 1 \leq x < k. \tag{2}$$

The number of integers satisfying (2) clearly equals

$$\frac{k}{p_r} \prod_{i=1}^{r-1} \left(1 - \frac{1}{p_i}\right) \geq \frac{p_1 p_2 \cdots p_{r-1}}{r} \geq p_1$$

since $\prod_{i=1}^{r-1} \left(1 - \frac{1}{p_i}\right) \geq \frac{1}{r}$, $r > 2$ and $p_{r-1} \geq r$.

Thus not all the integers $1 + yp_r$, $0 \leq y \leq \frac{k}{p_r} \prod_{i=1}^{r-1} \left(1 - \frac{1}{p_i}\right)$, can be relatively prime to $k$ since at least one of them is a multiple of $p_1$. Hence there clearly exists an integer satisfying (2) which is not less than $k \prod_{i=1}^{r-1} \left(1 - \frac{1}{p_i}\right) + 1$, or

$$u \geq k \prod_{i=1}^{r-1} \left(1 - \frac{1}{p_i}\right) + 1 > \frac{p_1 p_2 \cdots p_r}{r}. \tag{3}$$

Define $v$ as the greatest integer satisfying

$$x \equiv 1 \pmod{p_1 p_2 \cdots p_{r-1}}, \quad (x,k) = 1, \quad 1 \leq x < k. \tag{4}$$

Clearly at least one of the integers $k - p_1 p_2 \cdots p_{r-1} + 1$, $k - 2p_1 p_2 \cdots p_{r-1} + 1$ satisfies (4), or

$$v \geq k - 2p_1 p_2 \cdots p_{r-1} + 1. \tag{5}$$

Clearly $(u - 1)(v - 1) \equiv 0 \pmod{k}$, $(u,k) = (v,k) = 1$. Thus to prove our lemma we only have to show that $u + v > k$. Hence by (3) and (5) we have to show that

$$\frac{p_1 p_2 \cdots p_r}{r} > 2 p_1 p_2 \cdots p_{r-1}$$

or

$$p_r > 2r.$$

Since $r > 2$ and $k \neq 30$ the only squarefree integer $k = p_1 \ldots p_r$ for which $p_r > 2r$ is not satisfied is $210 = 2.3.5.7$. and here $u = 43$, $v = 181$ satisfies (1).

If $r = 2$, we have $k = p_1p_2$, $2 < p_1 < p_2$. Here we put $u = p_1p_2 - p_1 + 1$ and $v = p_2 + 1$ or $2p_2 + 1$, thus (1) is satisfied, which completes the proof of the lemma.

It is easy to see that if $k = p$, $k = 2p$ or $k = 30$ the lemma does not hold.

Now we can prove our theorem. By the well known theorem of Dirichlet there are infinitely many primes $p$ and $q$ satisfying $p \equiv u \pmod{k}$, $q \equiv v \pmod{k}$. Put $n = pq$. We have

$$\phi(k, 0, n) = (p-1)(q-1)/k - \varepsilon_1 + \varepsilon_2 + \varepsilon_3 - \varepsilon_4$$

where

$$\varepsilon_1 = pq/k - [pq/k], \qquad \varepsilon_2 = p/k - [p/k] = u/k,$$

$$\varepsilon_3 = q/k - [q/k] = v/k, \quad \varepsilon_4 = 1/k - [1/k] = 1/k.$$

Clearly $\varepsilon_1 \leq (k-1)/k$. Thus $\varepsilon_1 + \varepsilon_4 \leq 1$. By (1) $\varepsilon_2 + \varepsilon_3 = (u + v)/k > 1$ and $\phi(n) = (p-1)(q-1) \equiv 0 \pmod{k}$, thus $-\varepsilon_1 + \varepsilon_2 + \varepsilon_3 - \varepsilon_4$ is an integer. Since it is greater than 0 it must be 1, thus $\phi(k, 0, n) = \phi(n)/k + 1$ or $T(n,k)$ does not hold, which proves our theorem for all $k \neq 30$. If $k = 30$ take $n = 77$. Here $\phi(30, 1, 77) = 0$, which shows that $T(77, 30)$ fails to hold and our theorem is proved.

I would like to call attention to the conjecture which I stated at the end of my paper and which I can not prove though its proof is perhaps very simple: Let $k$ be an integer, $n = pq$, $\phi(n) \equiv 0 \pmod{k}$ but $p \not\equiv 1 \pmod{k}$, $q \not\equiv 1 \pmod{k}$. Then $T(n,k)$ does not hold.

## REFERENCE

1. P. Erdős, Some remarks on a paper of McCarthy, Canad. Math. Bull. 1 (1958), 71-75.